ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИУТУ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ»»

Тези доповідей

27 жовтня 2023

м. Київ

Редакційна колегія:

Віталій САВЧЕНКО– д.т.н., професор, директор Навчально-наукового інституту захисту інформації Державного університету інформаційно-комунікаційних технологій .

Галина ГАЙДУР– д.т.н., професор, завідувач кафедри Інформаційної та кібернетичної безпеки Державного університету інформаційно-комунікаційних технологій.

Андрій КОЖУХІВСЬКИЙ – д.т.н., професор, професор кафедри Інформаційної та кібернетичної безпеки Державного університету інформаційно-комунікаційних технологій.

Сергій ГАХОВ – к.військ.н., доцент, доцент кафедри Інформаційної та кібернетичної безпеки Державного університету інформаційно-комунікаційних технологій.

Віталій МАРЧЕНКО – д.ф., доцент, доцент кафедри Інформаційної та кібернетичної безпеки Державного університету інформаційно-комунікаційних технологій.

Рекомендовано до друку Вченою радою Навчально-наукового інституту захисту інформації Державного університету інформаційно-комунікаційних технологій (протокол № 3 від 16.10.2023 р.)

Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 27 жовтня 2023 року). Навчально-науковий інститут захисту інформації, Державний університет інформаційно-комунікаційних технологій . Київ, 2023. 394 с.

Збірник призначений для науковців, викладачів, докторантів, аспірантів і студентів закладів вищої освіти, фахівців з інформаційної та кібернетичної безпеки, працівників органів державної влади та місцевого самоврядування. Редакційна колегія не несе відповідальності за зміст матеріалів, що опубліковані у збірнику. Тези подані в авторській редакції та відображають персональну позицію учасників конференції

.

Зміст

Андрущенко Максим Вікторович
студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

ВИКЛИКИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРНИХ СЕРЕДОВИЩАХ

Технології, які змінюються, і загрози, що розвиваються, роблять IT-безпеку ще складнішою. Компанії та організації впроваджують хмарні технології, нові методи розробки та оновлені підходи щодо архітектури додатків. Однак кіберзлочинці також переходять до атак на хмарні інфраструктури, про що свідчать щорічні звіти Cisco, IBM, Microsoft, OWASP. Проте, при належній політиці та впровадженні управління хмарними даними та системами можна ефективно захистити ресурси організації.

Хмарні середовища зазвичай будуються за моделлю спільної відповідальності: постачальник послуг, такий як Amazon Web Services, відповідає за безпеку використовуваної інфраструктури, а клієнти відповідають за захист компонентів програм, робочих навантажень та віртуальних машин. Це означає, що IT-спеціалісти та розробники працюють над підвищенням безпеки своїх частин системи та дотриманням найкращих практик від свого постачальника послуг [1].

Один із викликів, з якими стикаються організації, особливо ті, які лише починають використовувати хмарні ресурси – це відсутність розуміння того, як працює хмарна інфраструктура та її відмінності від локальних систем та мереж. IT-персонал повинен бути ознайомлений із ризиками недостатньо захищених хмарних розгортань і знати конфігураційні особливості постачальника послуг. Багато чинників можуть спричинити атаки на робочі станції, пропускну здатність, навантаження та додатки, включаючи неправильні конфігурації, неправильне використання технологій, відсутність досвіду роботи з хмарними системами або навіть дії розробників та хмарних інженерів. Загалом, компоненти хмарних систем взаємопов'язані, що робить потенційні вектори атак складними для визначення. Тому розуміння безпеки як спільної відповідальності має вирішальне значення.

Хмарні технології спрямовані на вирішення сучасних викликів та завдань, що пов’язані з інформаційною безпекою, політиками та конфігураціями мережі, моніторингом програм та додатків. Варто зазначити, що впровадження хмарних технологій також призводить до появи нових проблем. Початківцям в IT іноді важко зрозуміти складність реалізації хмарних концепцій. Кожен постачальник послуг має свої особливості, тому спеціалісти повинні бути ознайомлені з конкретними концепціями хмарного провайдера[2]. Також хмарні послуги можуть бути реалізовані у вигляді стандартних інтернет-сервісів та протоколів для спрощення їхнього використання клієнтами, як показано на рис.1.

Компанії та організації взаємодіють з хмарними продуктами, які включають в себе сервіси від різних вендорів та провайдерів, кожен із яких має свої власні особливості та протоколи. Своєю чергою, це ускладнює налаштування безпеки, які часто важко відстежувати або навіть розуміти[3].

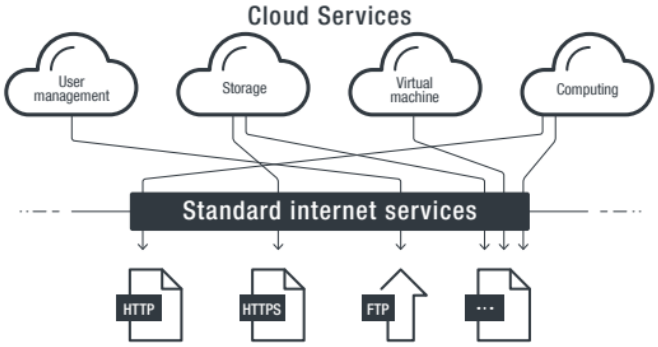


Рис.1. Представлення стандартних інтернет-сервісів і протоколів

Захист додатків та робочих навантажень у хмарі значно відрізняється від захисту локальних мереж. Некоректні конфігурації хмарних послуг створюють для організацій ризики, як криптоджекінг, електронний скіммінг та викрадання даних. Контейнерні технології в хмарі, якщо їх залишити відкритими, також створюють подібні ризики. Нарешті, некоректне управління обліковими записами та даними, нехтуванням вимог щодо конфіденційності інформації призводить до витоку та фінансових витрат, які стрімко зростатимуть, коли загрози рухаються через хмарний стек.

Постачальники хмарних послуг, такі як AWS, часто пропонують опції для керування безпекою через зручний і чистий API. Практики DevOps повинні використовувати можливість програмно створити безпечну хмарну програму з більш високим рівнем безпеки, ніж традиційні рішення. Крім того, спеціалізовані технології безпеки для хмарних послуг можуть забезпечити ще більш складний та багаторівневий рівень захисту, ніж те, що пропонують постачальники хмарних послуг. Сценарії розгортання в хмарі, такі, як AWS CloudFormation, надають уявлення про те, як кожна частина програми поєднується разом і де слід шукати некоректні або відсутні елементи управління безпекою або журналів. Це також можна використовувати для визначення місць, де потрібні додаткові інструменти безпеки, такі як Deep Security [4].

Висновок. Хмарні рішення допомагають компаніям реалізовувати все нові підходи щодо задоволення потреб клієнтів. Однак потрібно чітко підкреслити те, що організації повинні розуміти основні загрози та виклики, з якими вони будуть зіштовхуватися в хмарному середовищі.

Перелік посилань:

1. AWS General Reference. «Manage IAM User Access Keys Properly». [Електронний ресурс] - Режим доступу: https://docs.aws.amazon.com/en_pv/general/latest/gr/aws-access-keys-best-practices.html#iam-useraccess-keys.

2. Scott Ikeda. «Sans Institute Cloud Security Survey Reveals Top Threats, Which Surprisingly Are Not DDoS Attacks.» [Електронний ресурс] - Режим доступу: https://www.cpomagazine.com/cybersecurity/2019-sans-institute-cloud-security-survey-reveals-top-threats-which-surprisingly-are-not-ddos-attacks/.

3. Amazon Web Services. «Introducing Amazon S3 Block Public Access» [Електронний ресурс] - Режим доступу: https://aws.amazon.com/about-aws/whatsnew/2018/11/introducing-amazon-s3-block-public-access/.

4. Trend Micro Security News. «Imperva Data Breach Caused by Stolen AWS API Key.» [Електронний ресурс] - Режим доступу: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/imperva-data-breach-caused-by-stolen-aws-api-key.

Асман Олександр Ярославович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ЗАБЕЗПЕЧЕННЯ ВІД РИЗИКІВ ВИКОРИСТАННЯ ВІРТУАЛЬНОЇ ВАЛЮТИ ПІД ЧАС ВИКОНАННЯ ТРАНЗАКЦІЙ

Основна мета даної роботи полягає в аналізі та оцінці механізмів забезпечення від ризиків, пов'язаних з використанням віртуальної валюти під час виконання транзакцій. Дослідження спрямоване на ідентифікацію найбільш ризикових аспектів використання віртуальних валют, визначення основних проблем, що виникають в процесі транзакцій та встановлення ефективних механізмів мінімізації цих ризиків. Дослідження включає аналіз сучасних методів кібербезпеки, а також вивчення правових та регуляторних аспектів віртуальних валют з метою розроблення рекомендацій для підвищення безпеки та надійності транзакцій з використанням віртуальних валют. Дослідження також спрямоване на виявлення потенційних сценаріїв загроз для систем віртуальних валют та розроблення стратегій їх передбачення та запобігання. Висновки дослідження мають бути практично спрямованими та враховувати глобальний характер використання віртуальних валют, а також рекомендації стосовно майбутнього розвитку законодавства та технологій у сфері криптовалютних транзакцій.

Використання віртуальної валюти під час виконання транзакцій нерозривно пов'язане з рядом потенційних ризиків, які можуть виникнути через її цифрову та децентралізовану природу. Основні ризики використання віртуальної валюти під час транзакцій включають, але не обмежуються, такі аспекти:

Кібербезпека: Зловмисники можуть спробувати здійснити кібератаки на платформи обміну віртуальною валютою, гаманці або використовують соціальні інженерні методи для шахрайства та викрадення віртуальних активів.

Волатильність: Ринок віртуальної валюти відомий своєю високою волатильністю, що може призвести до значних коливань вартості валюти. Це може створювати небезпеку для тих, хто використовує цю валюту для транзакцій.

Легальний статус і регуляція: Багато країн до сих пір не визначили точного статусу віртуальних валют, що може вести до правової невизначеності і недостатньої регуляції, створюючи середовище для зловживань та нелегальних дій.

Технічні проблеми: Відсутність стандартизованих технічних протоколів та проблеми масштабованості можуть викликати технічні збої, що можуть спричинити втрату валюти або недоступність коштів.

Анонімність та використання для злочинних дій: Віртуальна валюта може використовуватися для незаконних дій через свою анонімність, що може створювати проблеми для боротьби зі злочинністю та фінансуванням тероризму.

Втрата доступу до гаманця: Втрата приватного ключа до гаманця може призвести до остаточної втрати віртуальних активів, оскільки не існує централізованого органу, який може відновити доступ до втрачених коштів.

Дослідження цих ризиків та розробка ефективних стратегій їх управління є критично важливою для забезпечення безпечності та надійності транзакцій з використанням віртуальних валют.

Багацький Сергій Петрович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЇ ПРОТИДІЇ ВИТОКАМ ДАНИХ В ОРГАНІЗАЦІЯХ

Запобігти витоку даних стає дедалі складніше через оцифрування документообігу в організаціях. Порушення даних є великою проблемою для сучасного бізнесу, і для запобігання втраті інформації потрібні сучасні засоби. Витоки даних можуть призвести до серйозних фінансових втрат, порушення конфіденційності клієнтів та клієнтської інформації, а також до втрати репутації компанії. Ризик витоку даних можна значно зменшити за допомогою сучасного рішення DLP.

Підприємства з конфіденційними даними можуть зіткнутися з порушенням даних, коли хакери отримують доступ до їхніх конфіденційних центрів обробки даних і можуть копіювати або переміщувати дані без відома компанії.

Наявність надійного місця та надійного програмного забезпечення для запобігання витокам даних може сповіщати компанії про порушення, щоб зменшити витік даних і запобігти їх погіршенню. Крім того, програмне забезпечення для моніторингу може виявляти аномальну поведінку та потенційно запобігати витоку даних [1].

Компанії в інформаційно-інтенсивних галузях повинні безпечно отримувати, надсилати, зберігати та мати доступ до великої кількості інформації. Вони також повинні відповідати приголомшливій кількості відповідних і нормативних вимог.

Що таке запобігання втраті даних (DLP)?

Запобігання втраті даних (DLP — Data loss prevention) — це стратегія пом’якшення загроз для критично важливих даних. DLP зазвичай впроваджується як частина загальної програми захисту даних організації.

DLP захищає конфіденційність даних за допомогою різноманітних програмних засобів і методів, призначених для запобігання несанкціонованому доступу до конфіденційної інформації. Це досягається шляхом класифікації різних типів вмісту в об’єктах даних і застосування автоматичних політик захисту.

Багаторівневі політики DLP гарантують, що конфіденційна інформація залишається за мережевими брандмауерами. Створення плану DLP також дає змогу організаціям переглядати та оновлювати свої політики зберігання та утримання даних, щоб підтримувати відповідність нормативним вимогам [2].

Тенденція віддаленої роботи з дому в поєднанні з більш складними кібератаками підкреслює зростаючий інтерес до DLP.

Чому організація повинна використовувати DLP

Існує багато причин, чому компаніям слід інтегрувати можливості DLP у свою систему кібербезпеки. Інші причини для впровадження заходів безпеки DLP у компанію включають [3]:

1. Деякі компанії не знають, куди зберігаються чи передаються їхні дані.
2. Більшість компаній повинні підтримувати певний рівень безпеки, щоб

відповідати державним і національним законам.

3. Розглядають зовнішні загрози, але не внутрішні загрози.

4. Підготовка до аудиту.

5. Щоб уникнути витоку даних, компаніям необхідно віддавати перевагу запобіганню загрозам до їх виникнення [3].

Інструменти та технології запобігання втраті даних

Існує два типи продуктів DLP: спеціальні та інтегровані.

Спеціальні – це окремі продукти, які є глибокими та складними. Інтегровані продукти є більш простими, працюють з іншими інструментами безпеки щодо застосування політики та дешевші, ніж спеціальні інструменти DLP.

Програмні продукти DLP використовують бізнес-правила для забезпечення дотримання нормативних вимог і класифікації та захисту конфіденційної та важливої інформації. Це означає, що неавторизовані користувачі не можуть випадково чи зловмисно поділитися даними, що становить організаційний ризик.

Сумнівно, що один інструмент задовольнить усі потреби організації щодо запобігання втраті даних. Багато постачальників DLP зосереджені на одній області, тоді як інші мають набори інструментів, які підходять один одному. Компанії можуть зібрати набір найкращих у своєму класі інструментів або використовувати комплексний пакет.

Які є типи запобігання втраті даних?

Мережевий DLP охоплює низку методів безпеки даних. Серед них:

Ідентифікація даних. DLP є корисним, лише якщо йому повідомляють, що є конфіденційним, а що ні. Компанії повинні використовувати автоматизований інструмент виявлення та класифікації даних, щоб забезпечити надійну та точну ідентифікацію та категоризацію даних, а не залишати це рішення людям.

Захист даних у русі. Дані досить часто переміщуються всередині, і зовнішні порушення часто покладаються на це для перенаправлення даних. Програмне забезпечення DLP може допомогти переконатися, що дані в русі не направляються кудись, куди вони не повинні потрапляти [2].

Захист даних у стані спокою. Ця техніка захищає дані, коли вони не переміщуються , наприклад, зберігаються в базах даних, інших програмах, хмарних сховищах, комп’ютерах, мобільних пристроях та інших засобах зберігання.

Кінцева точка DLP. Цей тип функції DLP захищає дані на рівні кінцевих пристроїв — не лише комп’ютерів, але й мобільних телефонів і планшетів. Він може блокувати копіювання даних або шифрувати всі дані під час їх передачі.

Виявлення витоку даних. Ця техніка передбачає встановлення базової лінії нормальної діяльності, а потім активний пошук незвичної поведінки.

Хмарний DLP. Рішення DLP розвинулися для керування та захисту критично важливих даних у додатках типу «програмне забезпечення як послуга» та «інфраструктура як послуга».

Отже, впровадження технологій протидії витокам даних на основі DLP є

надзвичайно важливими для забезпечення протидії витокам даних в організації.

Перелік посилань:
1. Yuri. What Is Data Leak Prevention? | SoftActivity. SoftActivity. URL: https://www.softactivity.com/ideas/what-is-data-leak-prevention/ (дата звернення: 19.10.2023).
2. Kranz G., Patrizio A. What is Data Loss Prevention (DLP)? Everything You Need to Know. *WhatIs.com*. URL: https://www.techtarget.com/whatis/definition/data-loss-prevention-DLP (дата звернення: 19.10.2023).
3. Data Leak Prevention- why is it important?. *Prima Secure*. URL: https://primasecure.com/data-leak-prevention/ (дата звернення: 19.10.2023).

Bakalo Vladyslav
student of National Aviation University, Kyiv, Ukraine

INFORMATION SECURITY AS A BASIC COMPONENT OF EFFICIENT ACTIVITIES

Cyber security is an important part of general security in the sphere of protection of legal and organizational interaction between the state and the citizen, man and society, and the national interests of Ukraine. Directed policy of the state, its executive structures, and activities of enterprises, institutions, and organizations in this area are an integral part of their work.

Globalization in various spheres of activity, including the use of information technologies, requires increased attention to the security component in the organization of interaction between various subjects whose activities are under constant threat.

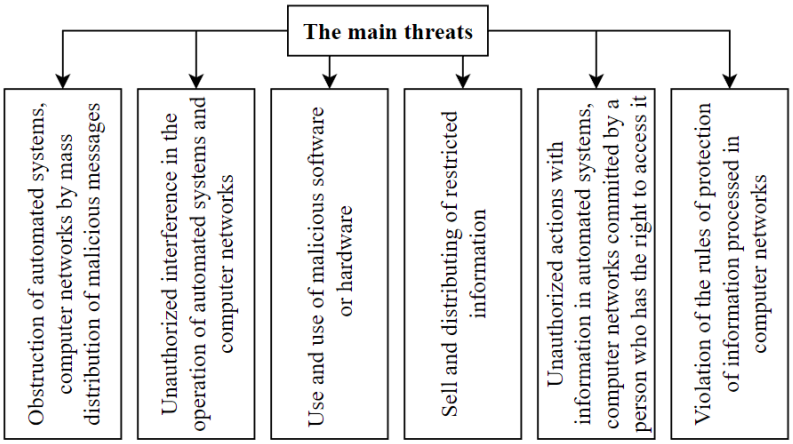


Figure 1 – Cyber threats

To ensure this requirement, it is necessary to integrate the information system with the security system.

This will allow simultaneously protecting information and other resources from viruses, DoS attacks, and DDoS attacks, using all opportunities for their prevention and timely detection. These processes are the basis of management tools, proper knowledge, and understanding of threats.

Checking computers and various media should be a mandatory procedure and an important precaution. Software tools for detecting changes made to data must be installed on computers as necessary to detect changes in executable programs. System maintenance measures are required to maintain the integrity and availability of

services. It is necessary to define daily technological processes for removing backup copies of data, logging events and failures, as well as for monitoring the environment in which the equipment functions. Critical production data and applications should be backed up regularly. To ensure that all mission-critical production data and programs can be recovered after a computer failure or media failure, it is necessary to have adequate backup facilities. Backup procedures for individual systems must meet the requirements of the organization's business continuity plans.

Data security and its preservation directly depend on:

- Classifications;
- Safe disposal;
- Multifactor authorization for administrative access;
- Use of encryption;
- Tracking and registration of access to them.

Ensuring information security means choosing the right vector of its development, aligning it with the company's (organization's) development direction, implementing current control over information policy and team qualifications, managing measures during negative events and eliminating negative consequences.

References:

1. Network security: how Ukraine will regulate cyberspace. But how the new law "On the basic principles of ensuring cyber security of Ukraine" will affect business / A. Krasny, A. Zymarin, I. Myagka, M. Poletaeva [Electronic resource] // mind.ua. 2018. URL: https://mind.ua/openmind/20184620-bezpeka-v-merezhi-yak-ukrayina-regulyuvatime-kiberprostir
2. Spencer Fm. (2017). Public-Private Partnerships (PPP)s for Cybersecurity Infrastructures. DOI: 10.13140/RG.2.2.22703.59044. URL: https://www.researchgate.net/publication/332182533_PublicPrivate_Partnerships_PPPs_for_Cybersecurity_Infrastructures

Барбунов Ярослав Олександрович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕННОГО ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

У сучасному світі, де інформація стала валютою, критично важливою для функціонування підприємств, технологія забезпечення захищеного функціонування інформаційних систем стає необхідністю і викликом одночасно. Зростання обсягів обробки, передачі та зберігання інформації вимагає від підприємств ефективних та сучасних засобів захисту від різноманітних загроз, що небезпечно наближаються з усіх сторін. Інформаційні системи підприємств є місцем, де переплітаються ключові бізнес-процеси, конфіденційна інформація та технології. Однак це також стає об'єктом пристосування для атак та зловживань, які можуть принести серйозні наслідки для бізнесу, якість обслуговування та репутацію підприємства.

Забезпечення захищенного функціонування інформаційної системи підприємства є необхідною умовою для забезпечення стабільності, безпеки та ефективності діяльності підприємства у сучасному цифровому середовищі. Ось кілька ключових причин, чому це настільки важливо:

Конфіденційність даних:

Підприємства зберігають конфіденційні дані, такі як особиста інформація клієнтів, фінансова інформація та комерційні таємниці. Забезпечення захищенного функціонування інформаційної системи гарантує, що ці дані залишаються під надійним захистом від несанкціонованого доступу.

Цілісність даних:

Недоторканність та цілісність даних є ключовими аспектами ефективної роботи підприємства. Забезпечення захищеності допомагає запобігти неправомірним змінам чи втраті даних, що може призвести до серйозних наслідків.

Доступність ресурсів:

Надійне функціонування інформаційної системи гарантує доступність ресурсів для співробітників, клієнтів та інших стейкхолдерів. Перерви в роботі системи можуть призвести до втрати бізнес-можливостей та репутаційних збитків.

Захист від кібератак:

Сучасні підприємства стають об'єктом кібератак та зловживань. Забезпечення захищеності інформаційної системи включає в себе впровадження заходів проти кіберзагроз та ефективне виявлення інцидентів.

Відповідність законодавству:

Багато секторів економіки регулюються законодавством, що вимагає відповідних стандартів захисту інформації. Забезпечення захищеності інформаційної системи допомагає підприємствам відповідати цим нормам та уникати штрафів чи інших юридичних проблем.

Збереження репутації:

Втрата конфіденційності, цілісності чи доступності може призвести до серйозних пошкоджень репутації підприємства. Забезпечення захищеного функціонування є важливим елементом підтримання довіри серед клієнтів та партнерів.

Загальною метою забезпечення захищеного функціонування інформаційної системи є збереження високої якості роботи підприємства та зменшення ризиків, пов'язаних із сучасними викликами в галузі кібербезпеки.

У будь-якій галузі базовий принцип інформаційної безпеки полягає в дотриманні балансу інтересів суб’єкта господарювання, громадянина, суспільства і держави. З урахуванням цього будується система інформаційної безпеки підприємства, яка повинна враховувати можливі загрози і методи захисту інформації. До загроз відносять:

1. Неуважність і недбалість співробітників. Завжди є ймовірність того, що хто-небудь відкриє фішингових лист і впровадить вірус з особистого ноутбука на сервер компанії. Або скопіює файл з конфіденційною інформацією на планшет, флешку або КПК для роботи у відрядженні. І жодна компанія не застрахована від пересилання неуважним співробітником важливих файлів не за тією адресою.

2. Використання піратського ПЗ. Неліцензійні програми не дають захисту від шахраїв, зацікавлених в крадіжці інформації за допомогою вірусів. Володар

неліцензійного ПЗ не отримує технічної підтримки, своєчасних оновлень, що надаються компаніями-розробниками.

3. DDoS-атаки. Distributed-Denial-of-Service – “розподілена відмова від обслуговування” – це потік помилкових запитів від сотень тисяч географічно розподілених хостів, які блокують обраний ресурс одним з двох шляхів. Перший шлях – це пряма атака на канал зв’язку. Другий – атака безпосередньо на сервер ресурсу. Зазвичай подібні атаки використовуються в ході конкурентної боротьби, шантажу компаній або для відвернення уваги системних адміністраторів від деяких протиправних дій.

4. Комп’ютерні віруси. Одна з найнебезпечніших на сьогоднішній день загроз інформаційній безпеці. Це можна пояснити появою нових каналів проникнення вірусів. На першому місці як і раніше залишається електронна пошта, але, як показує практика, віруси здатні проникати і через програми обміну повідомленнями, такі як ICQ та інші. Збільшилася і кількість об’єктів для можливих вірусних атак. Якщо раніше атакам піддавалися в основному сервери стандартних вебслужб, то сьогодні віруси здатні впливати і на міжмережеві екрани, комутатори, мобільні пристрої маршрутизатори. Останнім часом особливо активні стали так звані віруси-шифрувальники.

5. Загрози з боку співвласників бізнесу (легальних користувачів інформації фірми). Такі витоку фахівці називають інсайдерськими.

6. Законодавство. Державні органи наділені правом конфіскувати в ході перевірок обладнання та носії інформації, що завдає збитків компанії. До методів захисту інформації слід віднести:

фізичні засоби захисту інформації (обмеження або повну заборону доступу сторонніх осіб на територію);

базові засоби захисту електронної інформації (численні антивірусні програми, а також системи фільтрації електронної пошти);

використання анти-DDoS (послугу анти-DDoS, пропоновані програмістами);

резервне копіювання даних (особливо актуальною стала послуга віддаленого зберігання різної інформації в «хмарі» дата-центрів);

план аварійного відновлення даних (в ньому обов’язково повинна бути передбачена можливість введення аварійного режиму роботи на період збою, а також всі дії, які повинні бути зроблені після відновлення даних. Сам процес відновлення слід максимально відпрацювати з урахуванням всіх змін системи;

шифрування даних при передачі інформації в електронному форматі (end-to-end protection).

Визначення життєвого циклу інформаційної безпеки підприємства, дослідження основних рівнів інформаційної безпеки підприємства є також важливими аспектами її забезпечення в сучасних умовах їх господарювання.

Перелік посилань:

1. Вітер С.А., Світлишин І.І. Захист облікової інформації та кібербезпека підприємства. Економіка і суспільство: електронне фахове видання. 2017. №11. С 497-502. URL: https://economyandsociety.in.ua/journals/11_ukr/80.pdf (дата звернення: 29.09.2023).

2. Смірнов О.А. Інформаційна безпека в комп'ютерних мережах: навчальний посібник /О.А. Смірнов, С.А. Конопліцька-Слободенюк, К.О. Смірнов, Т.В. Буравченко, Л.І. Смірнова [та інш.]. – Кропивницький : Центральноукраїнський національний університет, 2020. - 295 с. URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/9799/1/Inform_bezp_komp_mer.pdf. (дата звернення: 03.10.2023).
3. .Клименко В. Внутрішні загрози інформаційній безпеці організації / В. Клименко // Вісник НБУ. – 2008. – № 5. – С. 62-63. (дата звернення: 06.10.2023)

Басюк Ілля Богданович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ТА ЗАСОБИ ЗАПОБІГАННЯ ПОШИРЕННЮ ЗАГРОЗ В ПРОМИСЛОВІЙ МЕРЕЖІ IOT ІЗ ВИКОРИСТАННЯМ КОНЦЕПЦІЇ INDUSTRIAL THREAT DEFENCE

У сучасному світі індустріального Інтернету речей (IoT), де виробничі процеси стають все більш цифровизованими, забезпечення безпеки та надійності промислових мереж стає вельми актуальною проблемою. Підвищення кількості з'єднаних пристроїв і розвиток технологій відкривають нові можливості для вдосконалення виробничих процесів, але також і загрози з боку кібератак, які можуть призвести до серйозних проблем та втрат. У цій тезі ми розглядаємо важливість впровадження концепції Industrial Threat Defence для запобігання поширенню кіберзагроз у промислових мережах IoT.

Розглядаємо актуальні загрози, з якими стикаються промислові мережі IoT, включаючи в себе DDoS атаки, атаки на рівень додатків та зловживання даними.

Представляємо концепцію Industrial Threat Defence як стратегічний підхід до захисту мереж IoT у промисловості. Цей підхід включає в себе використання алгоритмів машинного навчання для виявлення аномалій та автоматичне реагування на кібератаки.

Подробно розглядаємо технології та засоби, такі як blockchain для забезпечення цілісності даних, шифрування для захисту конфіденційності та протоколи аутентифікації для перевірки справжності пристроїв.

Розглядаємо практичні аспекти реалізації концепції Industrial Threat Defence у промислових мережах IoT та можливості її вдосконалення для майбутнього.

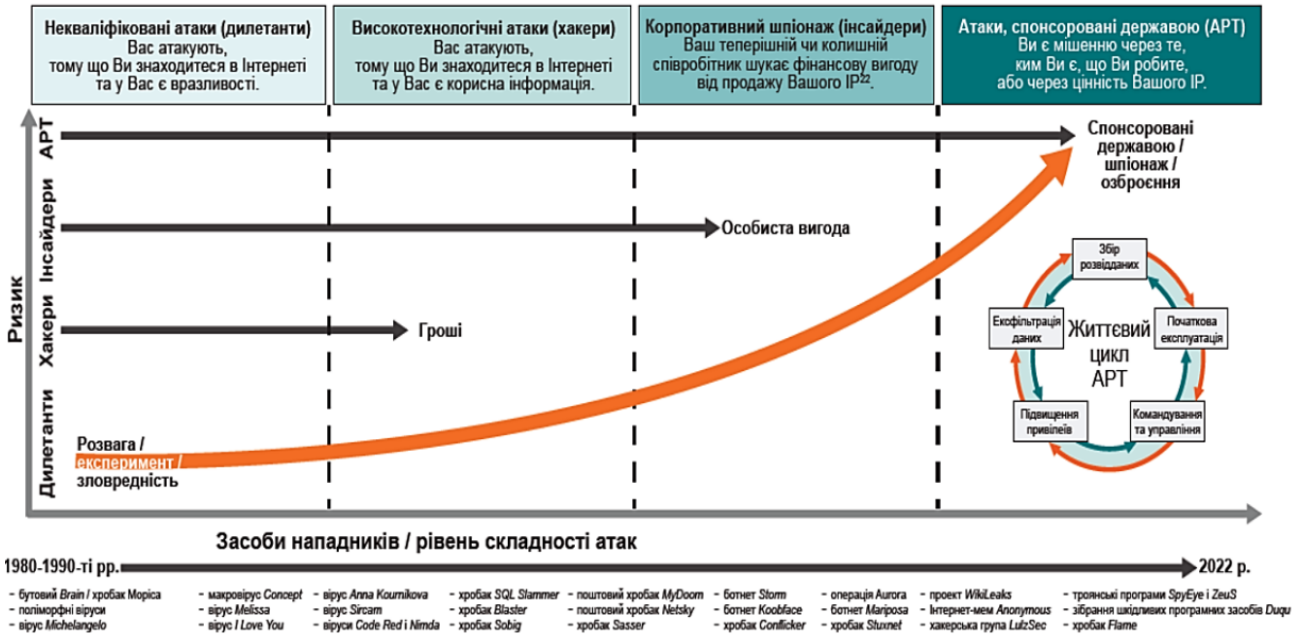


Рис.1. Динаміка розвитку засобів для кібернетичних атак

Перелік посилань:

1. INDUSTRIAL INTERNET OF THINGS, IIOT URL: https://www.it.ua/knowledge-base/technology-innovation/promyshlennyj-internet-veschej (дата звернення: 10.10.2023).
2. ПРОБЛЕМИ ТА ЗАГРОЗИ БЕЗПЕЦІ ІОТ ПРИСТРОЇВ URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/231 (дата звернення: 20.10.2023).
3. РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ОБ'ЄКТІВ ІНТЕРНЕТУ РЕЧЕЙ URL: https://ela.kpi.ua/bitstream/123456789/48855/1/Trokhymenko_magistr.pdf(дата звернення: 23.10.2023).

Катков Юрій Ігорович
доктор технічних наук, професор кафедри комп'ютерних наук, ННІТ, ДУІКТ, Київ, Україна
Березовська Юлія Володимирівна
доктор філософії, доцент кафедри комп'ютерних наук, ННІТ, ДУІКТ, Київ, Україна
Борода Кирил Олександрович
студент групи КНД-41, ННІТ, ДУІКТ, Київ, Україна

РОЗРОБКА КОНСТРУКТОРА ВЕБ-САЙТІВ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ

Однією з найзахоплюючих областей сучасної комп'ютерної науки є штучний інтелект (AI). Це інноваційна галузь, яка створює можливість комп'ютерам і програмам не просто виконувати завдання, аналогічні до людського інтелекту, але й навіть перевершувати їх в деяких аспектах. Задача полягає в тому, щоб надати системам можливість "мислити" та "навчатися" на основі аналізу даних та вивчення закономірностей. Штучний інтелект включає в себе різноманітні методи та техніки, такі як машинне навчання, глибоке навчання, обробка природної мови та багато інших. Він застосовується в різних сферах, включаючи медицину, автономне водіння, фінанси, аналітику та, звісно, веб-розробку [1].

Ключові слова: штучний інтелект, конструктор веб-сайтів, автоматизація, персоналізація, інтерактивність, інновації, виклики, можливості.

1. Актуальність.

Конструктор сайту – це програмне забезпечення для створення сайту у візуальному редакторі без спеціальних знань програмування. Як правило, конструктор сайту це окрема самостійна послуга, але може надаватися як додаткова хостинговими компаніями [3].

Розробка конструктора веб-сайтів з використанням штучного інтелекту відкриває нові перспективи та революціонізує спосіб створення та оптимізації веб-ресурсів. Інтеграція штучного інтелекту у процес веб-розробки дозволяє автоматизувати багато аспектів створення веб-сайтів, підвищити їхню якість та забезпечити відповідність найсучаснішим стандартам. Існує декілька ключових аргументів, які підкреслюють актуальність цього завдання.

Спочатку, спостерігається різке збільшення попиту на веб-сайти. У сучасному світі майже кожна галузь діяльності потребує наявності веб-сайту, незалежно від того, чи маємо ми на увазі бізнес, освіту, культуру або громадські ініціативи. Збільшення числа замовлень на веб-сайти ставить перед розробниками завдання створення їх великої кількості, що може призвести до значних витрат ресурсів, які включають в себе як людський труд, так і час. Розробка конструктора веб-сайтів зі штучним інтелектом дозволить автоматизувати і прискорити цей процес, допомагаючи розробникам зекономити час і зусилля.

По-друге, вимоги до веб-сайтів постійно зростають. Сучасні веб-ресурси повинні відповідати високим стандартам щодо дизайну, функціональності та безпеки. Вони мають бути адаптивними до різних пристроїв, швидкі та надійні. Це робить процес розробки веб-сайтів більш складним і вимагає високого рівня кваліфікації розробників. Використання штучного інтелекту для автоматизації певних аспектів розробки може значно полегшити це завдання і забезпечити високу якість результату.

По-третє, у бізнес-середовищі особливо цінується швидкість та ефективність. Швидкий запуск веб-сайту може вирішити питання конкурентоспроможності, і це означає, що розробники веб-сайтів повинні бути здатні швидко та якісно створювати ресурси. Застосування штучного інтелекту може сприяти прискоренню процесу розробки, забезпечуючи швидкий результат.

Зважаючи на зростаючу важливість штучного інтелекту в веб-розробці, можна виділити ще один важливий аспект: виклики та можливості. Впровадження штучного інтелекту у веб-розробку призводить до різних викликів і відкриває безліч можливостей для подальшого розвитку галузі.

2. Виклики і можливості.

З використанням штучного інтелекту виникають питання етики та безпеки. Розробники повинні враховувати питання конфіденційності та захисту даних користувачів, а також уникати можливих загроз, пов'язаних з автоматизацією.

Застосування штучного інтелекту для створення веб-сайтів вимагає забезпечення високої якості та надійності інтелектуальних систем. Помилки в алгоритмах машинного навчання можуть призвести до негативного впливу на

користувачів.

Розробники повинні знати, як ефективно контролювати та налагоджувати інтелектуальні системи для забезпечення їхньої працездатності та ефективності.

Штучний інтелект дозволяє автоматизувати багато рутинних завдань у веб-розробці, що дозволяє розробникам більше часу приділяти більш складним і творчим аспектам своєї роботи.

За допомогою штучного інтелекту можна створювати веб-сайти, які індивідуалізуються для кожного користувача, враховуючи їхні уподобання та потреби.

Штучний інтелект допомагає в аналізі даних та прогнозуванні тенденцій, що дозволяє вдосконалити веб-сайти та оптимізувати їх для кращої продуктивності.

Інтелектуальні системи можуть надавати можливість користувачам взаємодіяти з веб-сайтами на більш продуктивному рівні, а також надавати корисні відгуки та рекомендації.

Застосування штучного інтелекту в дизайні веб-сайтів може привести до створення стильних та ефективних дизайнів, що привертають користувачів.

3. Персоналізація.

Ще однією ключовою тенденцією є постійний акцент на персоналізації та індивідуальному досвіді користувачів. Користувачі бажають веб-сайти, які відповідають їхнім потребам та надають індивідуальний досвід. Розробка веб-сайтів, яка враховує індивідуальні вимоги кожного клієнта, стає ключовим фактором у задоволенні цих потреб.

Застосування штучного інтелекту у веб-розробці може призвести до значного покращення всіх цих аспектів. Інтелектуальні системи можуть автоматизувати різні аспекти процесу, від генерації дизайну до створення контенту та оптимізації веб-сайтів [4]. Це може включати автоматичну обробку природної мови для створення контенту, рекомендації щодо оптимізації швидкості завантаження та адаптивного дизайну для різних пристроїв. Інтеграція машинного навчання може сприяти аналізу даних та забезпечити індивідуальні рекомендації користувачам щодо покращення їхніх веб-сайтів.

4. Технології та інструменти.

Для розробки конструктора веб-сайтів з використанням штучного інтелекту використовуються сучасні технології та інструменти. Мови програмування, такі як Python та JavaScript, використовуються для реалізації функціональності конструктора та створення інтерактивного веб-інтерфейсу. Фреймворки для машинного навчання, такі як TensorFlow та PyTorch, застосовуються для навчання інтелектуальних моделей аналізу даних та рекомендацій. Мови розмітки, такі як HTML, CSS та JavaScript, використовуються для створення інтуїтивного інтерфейсу конструктора веб-сайтів та забезпечення користувачів зручністю використання. Системи керування базами даних, такі як MySQL або PostgreSQL, забезпечать зберігання

та доступ до структури веб-сайтів та їхніх даних. База даних (database) – сукупність даних, організованих відповідно до концепції, яка описує характеристику цих даних і взаємозв'язки між їх елементами; ця сукупність підтримує щонайменше одну з областей застосування [2].

За допомогою розпізнавання образів та обробки природної мови можливо автоматизувати створення контенту на веб-сайті. Наприклад, система може аналізувати текст та зображення, що відповідають тематиці веб-сайту, і генерувати відповідний контент. Це спростить процес створення вмісту та забезпечить високу швидкість розробки.

5. Приклади використання ШІ для конструкторів веб-сайтів.

Використання штучного інтелекту у веб-розробці дозволить створити інтелектуальний конструктор веб-сайтів, який зробить процес створення та оптимізації веб-ресурсів швидшим і ефективнішим. Користувачі зможуть швидко створювати власні веб-сайти з інтерактивними функціями та стильним дизайном. Система також може надавати рекомендації щодо оптимізації та покращення веб-сайтів, забезпечуючи їх відповідність найсучаснішим стандартам.

Висновок.

Узагальнюючи, розробка конструктора веб-сайтів зі штучним інтелектом є важливою і перспективною ініціативою. Вона дозволяє поєднати потужність штучного інтелекту з сучасними технологіями веб-розробки, створюючи інноваційний інструмент для розробників та користувачів. Такий конструктор веб-сайтів спрощує процес створення веб-ресурсів, підвищує якість та інтерактивність веб-сайтів і відкриває новий рівень технологічного розвитку. Цей інструмент стає ключовим у подоланні сучасних викликів та задоволенні потреб користувачів у надшвидкісному та індивідуалізованому веб-середовищі.

Перелік посилань:

1. Frąckiewicz M. ШІ та розумна мобільність: використання інтелектуальних систем для підключених і автономних транспортних засобів [Електронний ресурс] / Marcin Frąckiewicz // TS2 SPACE. – 7 квітня 2023. – Режим доступу до ресурсу: http://surl.li/mkzed

2. База даних [Електронний ресурс] // Wikipedia. – 31 січня 2023. – Режим доступу до ресурсу: http://surl.li/bqulg

3. Конструктор сайту [Електронний ресурс] // HOSTiQ. – Режим доступу до ресурсу: http://surl.li/mkyyb

4. Вплив штучного інтелекту на веб-розробку: оптимізація процесів та підвищення користувацького досвіду [Електронний ресурс] // TS2 SPACE. – 20 серпня 2023. – Режим доступу до ресурсу: http://surl.li/mkzar

Біляєв Дмитро Андрійович аспірант групи АКЗІ-125,
дтн, проф. Савченко Віталій Анатолійович,
ННІЗІ ДУІКТ, Київ, Україна

МЕТОД ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

Характеризуючи сучасний стан розвитку суспільства, варто звернути увагу на підвищення ролі інформаційних технологій у життєдіяльності окремої людини, суспільства і держави. Бурхливий розвиток інформаційних процесів, провадження нових винаходів, досягнень та технологій обумовило не лише можливості поступального розвитку нашої держави, але і стала фактором зростання кількості злочинів та вдосконалення засобів і способів вчинення злочинних посягань. Розвиток інформаційних систем в Україні, на сучасному етапі, можна охарактеризувати як низький і прийти до висновку, що впроваджені інформаційні системи на сьогодні не здатні в повному обсязі реалізувати своє призначення у процесі діяльності правоохоронних органів. Саме тому, питання вдосконалення інформаційного забезпечення юридичної діяльності набуває особливої актуальності.

Однією з проблем хмарних обчислень є труднощі, що виникають при переході на “хмару”, найбільше це виявляється у двох напрямках:

Економічні витрати з його використання.

Інформаційна безпека, тобто. дані які зберігаються на хмарних сервісах, і при не дотриманні правил алгоритмів безпеки, схильні до ризику втрати інформації[1].

У цьому аспекті існує низка загроз:

Нездатність клієнта хмари самостійно контролювати та проводити аудит безпеки файлів, що обмежує його можливості.

Видалений злом або несанкціоноване проникнення в сервер хмар.

Низький рівень захисту бездіяльних віртуальних машин.

Використання практично виключно парольної автентифікації та застосування не цілком надійних способів відновлення забутих автентифікаційних даних [2].

Щоб мінімізувати всі ризики, потрібно чітко розуміти важливість усіх способів забезпечення конфіденційності та безпеки, особливо приділити увагу функціям шифрування та автентифікації даних усередині хмарного середовища, механізму контролю трафіку між машинами та розмежуванням прав на доступ.

На загальний рівень безпеки впливає вибір моделі розгортання хмарного середовища: приватна хмара, інфраструктура, підготовлена для ексклюзивного використання єдиною організацією; публічна хмара, інфраструктура, призначена для вільного користування широким колом користувачів; громадську хмару, вид інфраструктури, призначений для використання конкретним співтовариством споживачів з організацій, які мають спільні завдання; та гібридна хмара, комбінація із двох або більше різних хмарних інфраструктур [3, 4].

Убезпечити роботу у хмарі можна за допомогою використання гібридного підходу, що поєднує у собі публічні та приватні хмари. Частина даних, які класифікуються організацією як найбільш критичні, залишаються в приватній хмарі, тоді як всі інші дані зберігаються в публічній хмарі.

Використання десктопного серверу управління основними механізмами безпеки забезпечує можливість контролю на рівні кіберфізичних систем, а також дозволяє, при використанні функцій управління у хмарі, забезпечувати можливість створення двоконтурних систем безпеки.

Такий підхід дозволяє створювати системи захисту інформації, які можуть протистояти сучасним цільовим атакам (комплексованим атакам з урахуванням гібридності та синергізму, а також методів соціальної інженерії), отримати об'єктивну оцінку поточного стану захищеності контуру бізнес-процесів, а також формувати завчасно превентивні заходи безпеки.

Список використаних джерел

1. Mahon.E. Transitioning the Enterprise to the Cloud: A Business Approach. Cloudworks Publishing Company; 1st edition. Loudworks Publishing Company, Hudson, Ohio, United States, 2015. p - 178.

2. Mahmood.Z, Puttini.R, Erl.T. Cloud Computing: Concepts, Technology & Architecture. Pearson Education (US), 2013. p -528.

3. Pohasii S. Synergy of building cybersecurity systems / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov, O. Korol, S. Milevskyi, S. Pohasii, A. Tkachov, O. Shmatko, Y. Melenti, O. Sievierinov, S. Ostapov, A. Gavrilova, O. Tsyhanenko, S. Herasimov, E. Nyemkova, B. Tomashevsky, I. Hrod, I. Opirskyy, V. Zvieriev, O. Prokopenko, V. Savchenko, O. Barabash, V. Sobchuk, G. Shuklin, V. Khvostenko, O. Tymochko, M. Pavlenko, A. Trystan, S. Florov // monograph. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. (P. 102 – 147).

4. Коваленко О.С. Огляд проблем та станів хмарних обчислень [Електронний ресурс] // Інформатика, обчислювальна техніка та інженерна освіта. – 2018

Бойко Олександр Олександрович
студент групи УБДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ПЕРСОНАЛОМ У СФЕРІ КІБЕРБЕЗПЕКИ

Сьогодні ефективність управління персоналом грає надзвичайно важливу роль у забезпеченні кібербезпеки. Ефективне управління персоналом може зменшити цей ризик, навчаючи співробітників правилам кібербезпеки та вдосконалюючи їхні навички. Проаналізовані підходи різних дослідників, що стосуються визначення сутності «управління персоналом» визначили складність та багатогранність проблеми формування ефективної системи управління персоналом у сфері кібербезпеки в сучасних умовах. Розкриті шляхи підвищення ефективності управління персоналом, які дозволять якісно організувати кібербезпеку.

Всесвітні кіберзагрози зростають у розмірі та складності. Переважна більшість кібератак сьогодні спрямовані на вразливості, які виникають через людський фактор, такі як соціальний інжиніринг або недбалість персоналу. Внутрішні загрози, такі як зловмисники всередині організації, можуть бути навіть більш небезпечними, ніж зовнішні атаки.

Ефективне управління персоналом стає стратегічно важливим фактором

для забезпечення кібербезпеки, оскільки персонал виступає як перший захист від кіберзагроз і визначає, наскільки успішно організація може захистити свою інформацію та реагувати на інциденти. Ефективне управління персоналом дозволяє швидко мобілізувати та орієнтувати команди для відповіді на кіберінциденти, зменшуючи час реакції на загрози та мінімізуючи шкоду. Правильно підготовлений і мотивований персонал допомагає забезпечити сталість і надійність систем кібербезпеки, зменшуючи ризик людських помилок або недбалості.

В дослідженнях [1,2] ефективність управління персоналом визначає в розрізі 9 функцій управління персоналом за відповідними індикаторами: аналіз та планування персоналу; набір персоналу; відбір персоналу; атестація та оцінювання кадрів; організація трудових відносин; мотивація персоналу; створення умов праці; інформаційне забезпечення; розвиток і навчання персоналу.

Ключовим елементом успішної стратегії забезпечення кібербезпеки організації є правильний підбір персоналу на основі професійних стандартів, які визначають вимоги до знань умінь і навичок на основі КВЕД-2010 «Класифікація видів економічної діяльності» [3] та Національного класифікатору України ДК 003:2010 «Класифікатор професій» [4]. Для цього в організації для фахівців кібербезпеки створюються карти компетенцій (професіограми) – портрет ідеального співробітника, які дозволяють уникнути недоліків підбору і полегшують роботу співробітників відділу кадрів, що зайняті прийомом на роботу.

Важливим аспектом ефективності управління персоналом у сфері кібербезпеки є його підготовка та навчання із застосуванням сучасних технологій та інструментів, таких як системи виявлення та реагування на інциденти (IDS/IPS), SIEM-системи, проведення обов’язкових регулярних тренінгів персоналу щодо дій в непередбачуваних або кризових ситуаціях, пов’язаних з кібербезпекою. Підготовка персоналу може здійснюватись як за планом всередині організації так і на курсах з отриманням сертифікатів, які будуть підтвердженням компетентності та необхідних навичок.

Здобуття сертифікатів у галузі кібербезпеки може підвищити компетентність персоналу та підтвердити їхні навички. Сертифікація може включати такі стандарти, як CISSP, CEH, CompTIA Security+, і багато інших.

CISSP (Certified Information Systems Security Professional) - це міжнародно визнана сертифікація, яка підтверджує знання та навички у галузі інформаційної безпеки. Ця сертифікація була розроблена для професіоналів, які мають досвід у галузі інформаційної безпеки та бажають поглибити свої знання.

CEH (Certified Ethical Hacker) - це сертифікація, яка показує наявність знань та навичок, необхідних для тестування безпеки комп’ютерних систем. Ця сертифікація допоможе зрозуміти, як працюють хакери, щоб краще захистити свою систему.

CompTIA Security+ - це сертифікація, яка показує наявність знань та навичок, необхідних для розуміння основних принципів безпеки комп’ютерних

систем. Ця сертифікація допоможе вам зрозуміти загальну структуру безпеки комп'ютерних систем.

Розробка та впровадження стандартів і процедур у сфері кібербезпеки допомагає створити структурований підхід до управління персоналом. Це може включати плани реагування на інциденти, політики безпеки та моніторинг загроз.

Одним із важливих механізмів підвищення ефективності управління персоналом є розробка та впровадження професійного кодексу кібербезпеки та корпоративного етичного кодексу організації кібербезпеки, в яких визначені етичні правила професійної діяльності.

Також важливим напрямком підвищення ефективності є мотивація персоналу, розроблена система оцінки результативності співробітників.

Загалом, ефективне управління персоналом стає стратегічно важливим фактором для забезпечення кібербезпеки, оскільки персонал виступає як перший захист від кіберзагроз і визначає, наскільки успішно організація може захистити свою інформацію та реагувати на інциденти.

Перелік посилань:

1. Рульєв В.А. Управління персоналом / В. А. Рульєв, С. О. Гуткевич, Т. Л. Мостенська. – Київ: КОНДОР, 2017. – 324 с
2. Дудукало Г.О. Механізм забезпечення ефективності управління персоналом машинобудівних підприємств : автореф. дис. на здобуття наук. ступеня канд. ек. наук : спец. 08.00.04 / Дудукало Г. О. – Київ, 2015. – 20 с.
3. КЛАСИФІКАЦІЯ ВИДІВ ЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ ДК 009:2010. Наказ Держспоживстандарту України від 11.10.2010 N 457 [Електронний ресурс] Режим доступу: URL: https://zakon.rada.gov.ua/rada/show/vb457609-10#Text. (дата звернення – 22.10.23).
4. НАЦІОНАЛЬНИЙ КЛАСИФІКАТОР УКРАЇНИ ДК 003:2010.Класифікатор професій. Наказ Держспоживстандарту України від 28.07.2010 № 327. [Електронний ресурс] Режим доступу: URL: https://zakon.rada.gov.ua/rada/show/va327609-10#Text. (дата звернення – 22.10.23).

Бондар Іван Володимирович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАХИСТУ МЕРЕЖІ ПІДПРИЄМСТВА ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ЗА ДОПОМОГОЮ VPN

Розвиток технологій та збільшення обсягу даних, які зберігаються та передаються в мережі підприємства, робить їх доволі цінними та цікавими для зловмисників. Такі атаки, як DDoS, витік інформації, та інші, можуть завдати серйозної шкоди бізнесу, компанії або підприємству і не тільки. Саме тому, потрібно використовувати VPN як один із способів захисту цих данних від компрометації/злиття/перехоплення зловмисниками.

Технологія VPN дозволяє створити безпечний тунель для передачі даних через незахищену мережу, таку як Інтернет. Вона забезпечує конфіденційність, цілісність та автентифікацію даних, які передаються через мережу. За допомогою VPN, всі дані шифруються, що ускладнює доступ до них навіть для найбільш досвідчених зловмисників.

Чому потрібно створювати віртуальну приватну мережу (VPN).

Через пандемію мільйони співробітників тепер працюють віддалено, тому з початку поширення COVID-19 кількість зареєстрованих кіберзлочинів

збільшилася на 300%. VPN створюють набагато більш безпечне з'єднання між віддаленими комп'ютерами (домашніми мережами або комп'ютерами, використовуваними людьми в дорозі) й іншими «локальними» комп'ютерами і серверами.

Ці мережі, по суті, доступні тільки людям, які повинні мати доступ до ваших систем, включаючи вашу бездротову мережу, і до обладнання, яке є найважливішим у ваших мережевих налаштуваннях. VPN може значно знизити ймовірність того, що хакери знайдуть точку входу і завдадуть шкоди вашій системі.ля атак зловмисники використовують фішинг та методи соціальної інженерії, які змушують співробітників натискати на заражені посилання. Їх надсилають електронною поштою або у повідомленнях месенджерів.

Перелік посилань:

1. Захист локальної мережі URL: https://infotel.ua/zahist-lokalnoi-merezhi (дата звернення: 22.10.2023).
2. Найкраще VPN-рішення для вашого бізнесу URL: https://surfshark.com/uk/vpn-for-business (дата звернення: 23.10.2023).

Бондаренко Євген Вікторович, АСП-11
Державний університет телекомунікацій,
м.Київ

АНАЛІЗ ЗАДАЧ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ КОМЕРЦІЙНОЇ КОМПАНІЇ НА РІВНІ КЛАСТЕРУ

Визначено актуальність та аналіз основних задач при управлінні інформаційною безпекою комерційної на рівні кластеру. Розкрито зміст задач управління інформаційною безпекою комерційної компанії на рівні кластеру.

У сучасному цифровому світі інформаційна безпека є однією з найважливіших складових успіху комерційних компаній. Втрати даних, кіберзлочини та інші загрози можуть суттєво вплинути на фінансові результати та репутацію будь-якої компанії . Управління інформаційною безпекою компанії на рівні кластеру є особливо складним завданням, і тільки з правильною її організацією можна досягти високого рівня результатів. В роботах [1, 2] розглянуто основні задачі при управлінні інформаційною безпекою комерційної компанії на рівні кластеру. Досліджено зміст основних задач при управлінні інформаційною безпекою комерційної компанії на рівні кластеру та проведено аналіз по виявленню недоліків та проблем. Тому, як показує досвід багатьох кластерних компаній , в самих основних задачах управління інформаційною безпекою комерційної компанії на рівні кластеру (див. рис.) завжди будуть присутні особливості по їх виконанню. Основні задачі, які виконуються при управлінні інформаційною безпекою комерційної компанії на рівні кластеру, представлені на рис.1.

Рис.1 Основні задачі, які виконуються при управлінні інформаційною безпекою комерційної компанії на рівні кластеру.

Аналіз поточного стану

Першим кроком в розробці методики підвищення ефективності управління інформаційною безпекою на рівні кластеру є аналіз поточного стану. Компанія повинна оцінити свої існуючі інформаційні системи, ідентифікувати потенційні загрози та слабкі місця. Цей аналіз допоможе визначити основні проблеми та визначити пріоритети для подальших дій.

Розробка стратегії інформаційної безпеки

На основі результатів аналізу поточного стану, кластер має розробити стратегію інформаційної безпеки. Ця стратегія повинна визначити мету і завдання для підвищення ефективності управління інформаційною безпекою та визначити ресурси, які будуть виділені для цього.

Впровадження технологічних рішень

Для підвищення ефективності управління інформаційною безпекою, кластер повинен впровадити відповідні технологічні рішення. Це включає в себе встановлення сучасних систем моніторингу та виявлення загроз, резервне копіювання даних, антивірусне програмне забезпечення та інші інструменти для захисту інформації.

Навчання та підвищення кваліфікації персоналу

Ефективне управління інформаційною безпекою вимагає висококваліфікованого персоналу. Кластер повинен забезпечити навчання та підвищення кваліфікації співробітників, щоб вони могли ефективно виявляти, відстежувати та реагувати на потенційні загрози.

Планування та вправна реакція на інциденти

Незважаючи на всі заходи щодо попередження інцидентів, інформаційна безпека не може бути гарантованою на 100%. Кластер повинен розробити план реагування на інциденти та проводити регулярні навчання для персоналу з питань реагування на кібератаки та інші інциденти.

Моніторинг та аудит інформаційної безпеки

Остаточним кроком є постійний моніторинг та аудит інформаційної безпеки. Кластер повинен встановити механізми для постійного слідкування за станом інформаційної безпеки та регулярного проведення аудитів для

визначення ефективності заходів.

Таким чином, управління інформаційною безпекою комерційних компаній на рівні кластеру на сьогодні є актуальним завданням.

При проведенні подальшої дослідницької діяльності ці перелічені задачі необхідно обов'язково включати в методичні матеріали спрямовані на підвищення ефективності управління інформаційною безпекою.

Перелік посилань:

1. Porter, M. E. (1998). "Clusters and the New Economics of Competition." Harvard Business Review.
2. NIST Special Publication 800-53. (2020). "Security and Privacy Controls for Information Systems and Organizations."
3. Doherty, N. F., & Fulford, H. (2016). "A Reference Model for the Management of Information Security in Small and Medium-Sized Enterprises." Computers & Security.
4. Whitman, M. E., & Mattord, H. J. (2019). "Principles of Information Security."
5. Rouse, M. (2019). "What is Cluster (in data management)? - Definition from WhatIs.com." TechTarget.

Бондаренко Вадим Володимирович, БСДМ-62
Державний університет телекомунікацій,
м. Київ

ТЕХНОЛОГІЯ СТВОРЕННЯ ІНТЕГРОВАНОЇ ПЛАТФОРМИ КІБЕРНАВЧАНЬ ТАКТИЧНОГО РІВНЯ

Проведено аналіз платформ Кібернавчань типу Cyber Range і CTF. Визначено модель, етапи створення та їх реалізація. Сформовано вимоги до створення платформи кібернавчань тактичного рівня.

Кібернавчання – це заходи, які проводяться різними організаціями з метою навчання робітників або персоналу, виконуючи різні сценарії. Кожна організація створює свій власний сценарій по якому різні команди виконують свої функції в рамках одного навчання[1].

На сьогоднішній час існує дві найпопулярніші платформи кібернавчань – Cyber Range і CTF, які практично направлені та поєднують в собі всі дієві методи та функції, необхідні для навчання.. Для реалізації даних платформ по одинці затрачається багато ресурсів та сил, що є не дуже ефективно. Необхідно розглянути архітектуру кожної платформи, сформулювати вимоги та створити гібридну модель, яка буде структурована та реалізована на базі програмного забезпечення з відкритим кодом. Гібридна модель повинна працювати в повному обсязі та виконуватиме всі покладені на неї завдання[2].

Висновки. Сформовано модель інтегрованої платформи кібернавчань тактичного рівня та реалізовано її розгортання. Здійснено випробовування даної платформи на основі виконання вправ по протидії вразливостям. Сформовано звіт, в якому описано всі дії по виконанню вправи, результати та практичні навички, які були при цьому набуті.

Перелік посилань:

1. C. Zimmerman. Ten Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation,

2014.

2. J. Muniz, G. McIntyre, and N. AlFardan. Security Operations Center. Cisco Press, 2016.

Бондарєв Ілля Дмитрович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ОСНОВНІ РИЗИКИ БЕЗПЕКИ ВИКОРИСТАННЯ ЕЦП В ОРГАНІЗАЦІЇ

Використання електронних цифрових підписів в організації, не дивлячись на їх здатність забезпечувати автентичність та цілісність документів, може зіткнутися з ризиками, такими як несанкціонований доступ до ключів підпису, слабка інфраструктура публічних ключів, потенційні вразливості у програмному забезпеченні для створення підписів та недостатнє освічення користувачів щодо правильного використання та зберігання електронних підписів.

Електронний цифровий підпис (ЕЦП) – головні ризики та головні рекомендації щодо їх запобігання

Електронний цифровий підпис (ЕЦП) став ключовим інструментом у сучасному діловому світі, який дозволяє забезпечувати автентичність, цілісність та відмову від заперечення електронних документів. Однак разом із зростанням їх популярності з'являються й нові ризики безпеки.

Несанкціонований доступ до ключів підпису [1]**:**

Якщо приватний ключ користувача потрапляє в руки зловмисника, цей зловмисник може підробляти підпис користувача. Недостатня захистованість ключів, відсутність двофакторної автентифікації та слабкі паролі можуть призвести до витоку ключів.

Слабка інфраструктура публічних ключів (ПКІ):

Якщо Центр Видачі Сертифікатів (ЦВС) компрометовано, це може призвести до видачі недійсних або підроблених сертифікатів. Відсутність належного аудиту та перевірки ЦВС може зробити систему вразливою.

Вразливості у програмному забезпеченні:

Програмне забезпечення, яке використовується для генерації та перевірки ЕЦП, може містити вразливості, що дозволяють атакувати підпис. Оновлення безпеки мають регулярно встановлюватися, щоб запобігти експлуатації відомих вразливостей.

Недостатнє освічення користувачів:

Користувачі можуть не розуміти важливості зберігання приватних ключів у безпечному місці або не знати про необхідність регулярної зміни паролів. Некоректне використання технології ЕЦП може призвести до витоку конфіденційної інформації.

Фізична безпека:

Зберігання приватних ключів на фізичних носіях (наприклад, USB-токенах) може призвести до їх втрати чи крадіжки. Захист від фізичного доступу до обладнання, де зберігаються ключі, є важливим аспектом безпеки ЕЦП.

Для забезпечення ефективного використання ЕЦП організаціям необхідно

регулярно оцінювати та мінімізувати потенційні ризики, а також надавати своїм співробітникам відповідне навчання. Тільки інтегрований підхід до управління ризиками може гарантувати високий рівень безпеки при використанні ЕЦП. Далі наведено основні способи мінімізації ризиків при використанні ЕЦП [2]:

- Сильні паролі та двофакторна автентифікація: Використання складних паролів, які регулярно змінюються, разом з двофакторною автентифікацією, може допомогти зменшити ризик несанкціонованого доступу.
- Зашифроване зберігання: Зберігання приватних ключів у зашифрованому вигляді, щоб захистити їх від несанкціонованого доступу.
- Регулярний аудит ЦВС: Проведення зовнішніх і внутрішніх аудитів Центру Видачі Сертифікатів для перевірки їхньої безпеки та відповідності стандартам.
- Обмежений доступ до ЦВС: Встановлення строгих політик доступу до інфраструктури ПКІ, щоб зменшити ризик компрометації.
- Регулярне оновлення ПЗ: Встановлення останніх патчів безпеки та оновлень для програмного забезпечення, яке використовується для роботи з ЕЦП.
- Тестування на вразливості: Регулярні перевірки програмного забезпечення на наявність вразливостей, щоб виявити та виправити їх вчасно.
- Навчальні програми: Організація регулярних тренінгів та семінарів для співробітників щодо безпечного використання та зберігання ЕЦП.
- Інформаційні кампанії: Розробка та дистрибуція інформаційних матеріалів, які роз'яснюють важливість та основи безпеки ЕЦП.
- Захищене зберігання: Використання сейфів або інших засобів фізичного захисту для зберігання пристроїв, що містять приватні ключі (наприклад, USB-токени).
- Контроль доступу: Обмеження доступу до приміщень та обладнання, де зберігаються ключі, з використанням систем контролю доступу, відеоспостереження та інших механізмів безпеки.

Врахування цих рішень та їх впровадження в організації допоможе зменшити ризики безпеки, пов'язані з використанням електронних цифрових підписів, і підвищити довіру до цифрових транзакцій та документів.

Перелік посилань:

1. NIST Special Publication 800-57. (2016). Recommendation for Key Management – Part 1: General [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
2. NIST Special Publication 800-63B. (2017). Digital Identity Guidelines: Authentication and Lifecycle Management [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

Бригинець Анастасія Андріївна,
студентка групи БСД-41, ННІЗІ ДУТ, Київ, Україна

СТВОРЕННЯ ВІРТУАЛЬНОГО СЕРЕДОВИЩА ДЛЯ ЕМУЛЯЦІЇ КІБЕРАТАК У РАМКАХ ПРОГРАМИ КОРИСТУВАЦЬКОГО КОНТЕНТУ ВІД OFFSEC

У сучасному інформаційному суспільстві, інформаційні системи підприємств стали невід'ємною частиною бізнес-процесів, обліку, управління та інших сфер діяльності. Зростання залежності від інформаційних технологій сприяло інтенсифікації кіберзлочинності, а також збільшенню кількості та складності кібератак. Через це зростає потреба навчання спеціалістів RedTeam та BlueTeam шляхом модуляції реальних атак на дійсні інформаційно-комунікаційні системи. Один із методів реалізації таких навчань є створення віртуальних середовищ для емуляції кібератак, що описано у цій статті.
Ключові слова: вразливе віртуальне середовище, емуляція атак, віртуальна машина, програма користувацького контенту.

Перед початком створення вразливої віртуальної машини необхідно виконати багато досліджень для розробки ідеї для неї. Нижче наведено кілька прикладів можливих джерел інформації:

1. Соціальні мережі, такі як Twitter і LinkedIn, і слідкування за дослідженнями від компаній та спеціалістів, що працюють у сфері кіберзахисту.
2. Отримання оновлень щодо нових уразливостей через Twitter або The Daily Swig від PortSwigger.
3. Перевірка вразливостей через сайти, такі як exploit-db.com і cve.mitre.org.
4. Слідкування за статтями на Exploit Database Security Papers [1].

Усе зводиться до творчого поєднання знайдених уразливостей, щоб створити повноцінну машину. Можна зв'язатися з командою Labs Team у Offensive Security Discord в каналі #user-generated-content, щоб отримати відгук на ваші ідеї перед розпочатком створення машини.

Перед розгортанням вразливої віртуальної машини (ВМ) важливо створити сценарій, що містить такі елементи:

• Foothold для початкового доступу і отримання прапора користувача.
• Підвищення привілеїв для отримання root-користувача.

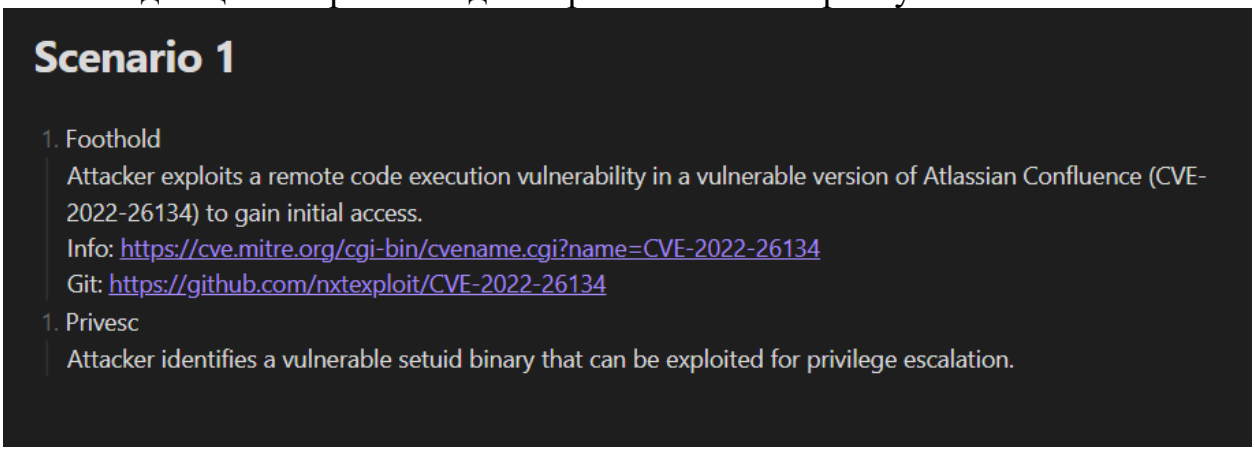


Рис. 1 – Приклад сценарію

Необхідно також переконатися, що машина відповідає вимогам програми

користувацького контенту від OffSec та включає всі відповідні елементи вирівнювання карти MITRE, які можна знайти на https://attack.mitre.org/.

Також слід розглянути різні типи машин та їх застосування. Наприклад:

• T1190 - Експлуатація загальнодоступного застосунку.

• T1059 - Інтерпретатор команд і сценаріїв.

• T1169 - Зловживання механізмом контролю привілеїв: Sudo та кешування Sudo [2].

Техніки - це конкретні методи або дії, які використовуються для реалізації тактик. Кожен метод описує певний підхід або поведінку, пов'язану з кіберзагрозами, і класифікується в рамках тактик.

Після визначення сценарію і вимог слід вибрати гіпервізор, такий як VirtualBox, VMware або Hyper-V, і вибрати вразливий образ ВМ, які містять уразливості для вивчення методів тестування на проникнення.

Далі виконуються різні техніки, такі як встановлення вразливих версій програмного забезпечення, розгортання веб-додатків з уразливостями віддаленого виконання коду, створення вразливих системних конфігурацій.
Це супроводжується створенням облікових записів користувачів, паролів, прапорів і файлів, які відповідають сценарію ВМ.

Важливо також створити покроковий посібник у форматі Markdown, який описує всі необхідні кроки для створення машини та надає інструкції для експлуатації всіх вразливих векторів.

Packer може бути використаний для створення базових образів для розробки машин на основі Vagrant.

Хоча робота зі стандартними образами не є обов'язковою, вона може бути корисною, забезпечуючи стійкість та актуальність образу, спрощуючи процеси розробки та зменшуючи споживання пропускної здатності.

Перелік посилань:
1. GitHub - CsEnox/Art-of-Creating-Machines. GitHub. URL: https://github.com/CsEnox/Art-of-Creating-Machines#art-of-creating-machines (date of access: 28.09.2023).
2. User-Generated Content FAQ. URL: https://help.offsec.com/hc/en-us/articles/360049610511-User-Generated-Content-FAQ (date of access: 28.09.2023).

Бригинець Анастасія Андріївна,
студентка групи БСД-41, ННІЗІ ДУТ, Київ, Україна

МЕТОДОЛОГІЯ ВИКОРИСТАННЯ CRON JOBS ДЛЯ ПРОВЕДЕННЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Cron job - це спосіб планування та виконання скриптів або програмних файлів у визначений час і дату на Unix-подібних системах. Це часто використовується для автоматизації рутинних завдань, таких як резервне копіювання даних, оновлення програм тощо. Проте важливо розуміти, що Cron job виконується з правами власника завдання, а не поточного користувача, і це може призвести до потенційних проблем з безпекою. Далі буде розглянуто конфігурації Cron job, які зберігаються у кронтабах (таблицях Cron), і підкреслено важливість перевірки та моніторингу найближчого часу та дати запуску кожного завдання.

Ключові слова: Cron job, атаки на підвищення привілеїв, кронтаби, автоматизація завдань, безпека системи, права доступу, експлуатація вразливостей.

Cron job використовується для запуску скриптів або виконання двійкових файлів у визначений час. Зазвичай це відбувається з правами власника завдання, а не поточного користувача. Хоча належно налаштовані Cron job не мають вразливостей, в певних умовах вони можуть стати вектором атаки на підвищення привілеїв.

Ідея такого виду атаки досить проста: якщо існує заплановане завдання Cron, яке виконується з правами користувача "root", і атакуюча сторона може змінити скрипт або файл, який буде виконуватися, то цей скрипт виконається з правами "root" [4].

Конфігурації завдань Cron зберігаються у кронтабах (таблицях Cron). Існує можливість переглядати найближчий час та дату запуску кожного завдання. Кожен користувач системи має свій власний файл кронтаба (/etc/crontab) і може запускати певні завдання, навіть якщо він не ввійшов до системи [3].

```
alper@targetsystem:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * * root /home/alper/Desktop/backup.sh

alper@targetsystem:~$
```

Рис. 1 – Приклад вмісту файлу /etc/crontab з можливістю експлуатації вразливості

Під час тестування на проникнення, часто зустрічаються завдання, які запускаються щодня, щотижня або щомісяця.

Утиліту Cron можна повністю налаштувати. Це робиться шляхом редагування файлів кронтаба. Кожен користувач має свій власний кронтаб, який можна редагувати за допомогою команди "crontab -e" під своїм іменем.

На практиці ймовірний такий розвиток подій при експлуатації цієї вразливості: припустимо, що під час дослідження системи, було знайдено деякий скрипт backup.sh, який було видалено, але cron job на нього залишився активним.

```
#
* * * * *  root /antivirus.sh
* * * * *  root antivirus.sh
* * * * *  root /home/karen/backup.sh
* * * * *  root /tmp/test.py
```

Рис. 2 – Активний cron job

З цього можна зробити висновок, що якщо ми створимо зловмисний скрипт з такою ж назвою і в тій самій директорії, то його буде виконано за певний проміжок часу. Реалізувати такі дії можна, виконавши команди для створення і заповнення вмісту файлу (touch і nano/vim відповідно) та додавши, наприклад, reverse shell [1].

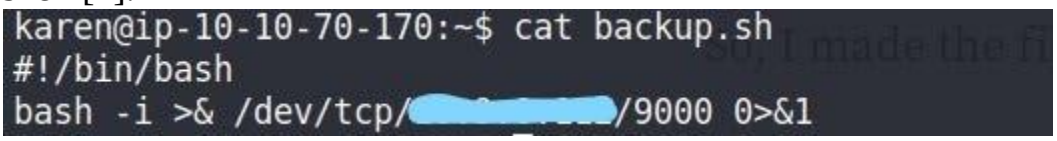


Рис. 3 – Приклад вмісту файлу backup.sh (reverse shell)

Після деякого часу очікування і виконання скрипту, зловмисник зможе отримати root привілеї.

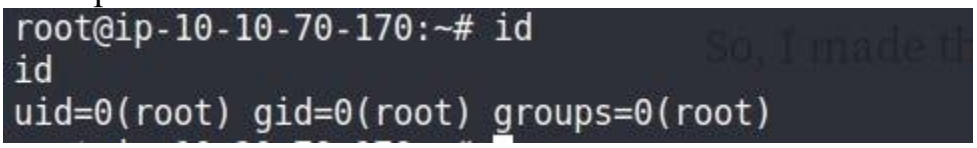


Рис. 4 – Вивід терміналу на стороні зловмисника із запущеним nc listener

Отже, якщо випадково було знайдено існуючий скрипт або завдання, прикріплене до cron jobs, завжди варто витратити час на те, щоб зрозуміти функцію скрипта і те, як використовується будь-який інструмент в контексті безпеки. Наприклад, tar, 7z, rsync і т.д. можна використовувати не за їхнім прямим призначенням, використовуючи функціонал wildcard [2].

Для захисту від зловмисної експлуатації cron jobs, якщо такі наявні у дійсній системі та виконують функцію автоматизації деяких системних завдань, необхідно переконатися, що жоден із наявних автоматизаційних скриптів не може бути змінений непривілейованим користувачем. Також необхідно впевнитись, що усі існуючі Cron скрипти є безпечними.

Перелік посилань:

1. AK A. Privileges Escalation Techniques (Basic to Advanced) in Linux. *Search Medium*. URL: https://infosecwriteups.com/privileges-escalation-techniques-basic-to-advanced-in-linux-973cb62cbe8d.

2. Exploiting the Cron Jobs Misconfigurations (Privilege Escalation) | VK9 Security. *VK9 Security | Ready to improve your hacking skills?*. URL: https://vk9-sec.com/exploiting-the-cron-jobs-misconfigurations-privilege-escalation/ (date of access: 13.10.2023).

3. Linux Privilege Escalation - HackTricks. *HackTricks*. URL: https://book.hacktricks.xyz/linux-hardening/privilege-escalation (date of access: 13.10.2023).

4. TryHackMe | Linux Privilege Escalation. *TryHackMe*. URL: https://tryhackme.com/room/linprivesc (date of access: 13.10.2023).

Брюшинін Назар Сергійович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАХИСТУ ВІД DDOS АТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ НА ОСНОВІ CLOUDFLARE

Ще декілька років тому DDoS-атака була вузькоспеціалізованим терміном, про який знали тільки системні адміністратори та фахівці у сфері мережевої безпеки. Сьогодні DDoS відомий всім — керівникам компаній, які постраждали від такого виду атак, користувачам, які не можуть потрапити на улюблений сайт або отримати звичну послугу, фахівцям, що працюють віддалено тощо. Ці віртуальні атаки стають все більш частими, а страждають від них реальні люди.

DDoS (Distributed Denial of Service) — розподілена атака, спрямована на відмову обладнання в обслуговуванні. Найпростіша DDoS — це надсилання мільйонів пакетів даних з різних комп'ютерів на певний сайт. Чим атакуючих комп'ютерів більше і чим частіше пакети надсилаються, тим швидше заб'ється канал зв'язку, оперативна пам'ять сервера та вільні слоти для з'єднань. В результаті сервер «ляже», коли не зможе обробляти все більше запитів. На екрані користувача це буде виглядати як недоступність сайту, адже сервер не може самостійно фільтрувати, де шкідливі запити, а де — відвідування клієнтів.

CloudFlare — це сервіс, який допомагає захистити сайт від різних мережевих атак, зокрема і DDoS. Принцип роботи полягає в тому, що весь трафік, перш ніж потрапити на цільовий сайт, проходить через сервери CloudFlare, де фільтрується згідно з призначеним для користувача налаштуванням. Для встановлення необхідно змінити DNS-сервери на пропоновані сервісом та активувати захист, вибравши один із запропонованих рівнів — від легкої до високої.

Зручна система моніторингу CloudFlare показує, з яких IP-адрес спостерігається найбільше запитів — швидше за все, це і є комп'ютери, які використовуються зловмисниками. Крім того, можна блокувати одразу підмережі та навіть країни — наприклад, якщо ваш проект розрахований на країни СНД та Європи, азіатські IP (звідки дуже часто і виходить загроза) можна тимчасово заблокувати, поки йде атака. Також є екстрений режим — якщо сайт атакують, включення цього режиму змусить кожного відвідувача сайту пройти автоматичну перевірку. Затримки в декілька секунд вистачить для того, щоб відсікти шкідливі запити, а звичайні клієнти побачать заглушку і почекають, поки перевірка закінчиться.

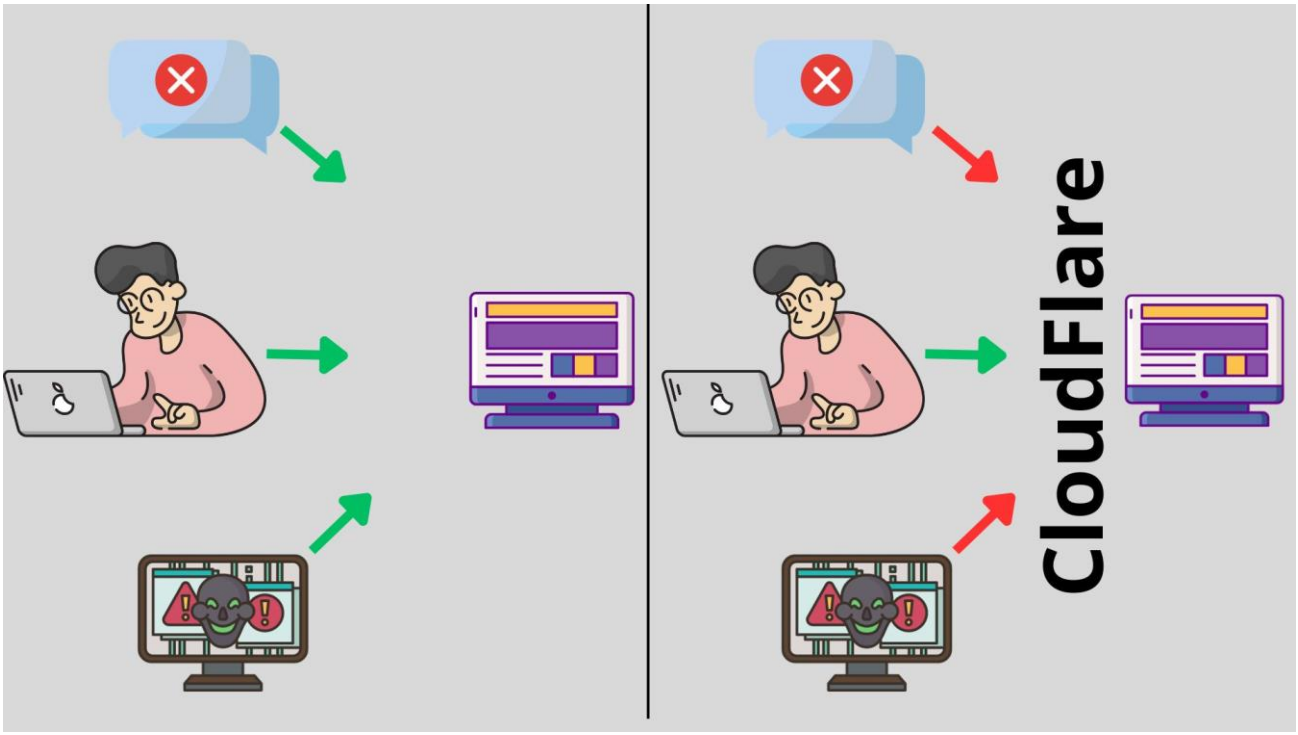


Рис.1. Захист сайту від DdoS-атак.

Перелік посилань:

1. Загрози та можливості CloudFlare: https://datami.ua/zagrozi-ta-mozhlivosti-cloudflare (дата звернення: 08.10.2023).
2. CLOUDFLARE URL: https://www.cloudflare.com (дата звернення: 08.10.2023).

Бугаєнко Нікіта Костянтинович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ЗАГРОЗЛИВОЇ ДІЯЛЬНОСТІ І ПОВЕДІНКИ В IT СЕРЕДОВИЩІ

В сучасному цифровому світі, де кіберзагрози стають все більш складними і вишуканими, ефективна технологія виявлення загрозливої діяльності та аномальної поведінки в інформаційно-технологічному середовищі (IT) відіграє надзвичайно важливу роль у забезпеченні безпеки та стійкості цифрових інфраструктур. Ці технологічні рішення, такі як системи виявлення вторгнень (IDS), системи захисту від вторгнень (IPS), аналіз поведінки користувачів, машинне навчання та штучний інтелект (AI), дозволяють виявляти та реагувати на широкий спектр кіберзагроз, включаючи шкідливе програмне забезпечення, атаки з використанням вразливостей, соціальний інжиніринг та інші форми агресивної кібердіяльності.

Шляхом неперервного моніторингу, аналізу мережевого трафіку, а також використання алгоритмів аналізу великих обсягів даних, ці технології забезпечують раннє виявлення і блокування потенційно шкідливих або аномальних дій в IT середовищі. Постійне оновлення бази знань та

вдосконалення алгоритмів дозволяє підвищувати ефективність виявлення навіть найновіших форм кіберзагроз, забезпечуючи захист від небажаних інцидентів та мінімізуючи ризики для бізнесу та приватності користувачів. В цілому, розробка та застосування високоефективних систем виявлення загрозливої діяльності і поведінки в IT середовищі визначає сучасні стандарти кібербезпеки та відіграє ключову роль у забезпеченні безпеки та стійкості сучасних цифрових інфраструктур.

В технології виявлення загрозливої діяльності і поведінки в інформаційно-технологічному середовищі (IT) також існують певні ризики, які можуть виникнути через хибні спрацювання, недостатню ефективність систем або неправильне їх застосування. Деякі з цих ризиків включають:

- **Помилкові спрацювання:** Виявлення загроз може супроводжуватися помилковими спрацюваннями, коли безшкідливі дії помилково ідентифікуються як загрозливі. Це може вести до блокування легітимних користувачів або систем, що може завдати шкоди бізнесу.
- **Несправність систем:** Технічні проблеми, помилки в програмному забезпеченні або несправність обладнання можуть призвести до недостатнього або неправильного виявлення загроз. Це може викликати просіки в безпеці та призвести до потенційних кібератак.
- **Неправильна конфігурація:** Несправна конфігурація систем виявлення загроз може призвести до пропусків в роботі системи або до її недосяжності, що в свою чергу може створити дірки в кібербезпеці.
- **Недостатня реактивність:** Якщо системи не можуть швидко реагувати на нові загрози та виклики, вони можуть стати неефективними проти сучасних та складних атак.
- **Залежність від штучного інтелекту:** Використання штучного інтелекту та машинного навчання для виявлення загроз може призвести до проблем у випадку, якщо зловмисники використовують атаки з використанням штучного інтелекту для обходу систем безпеки.
- **Проблеми з приватністю:** Деякі методи виявлення загроз можуть порушувати приватність користувачів, що може призвести до конфліктів з законодавством про захист персональних даних.

Для зменшення цих ризиків важливо використовувати комплексні підходи до кібербезпеки, включаючи регулярне оновлення та перевірку систем виявлення загроз, постійне навчання персоналу та впровадження найкращих практик з кібербезпеки.

Щавінський Юрій Віталійович
доцент кафедри УІКБ, ННІЗІ ДУІКТ, Київ, Україна
Будзинський Олександр Володимирович
аспірант, ННІЗІ ДУІКТ, Київ, Україна

ШЛЯХИ УДОСКОНАЛЕННЯ ЗАХИСТУ КОРПОРАТИВНИХ БАЗ ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Зроблений аналіз проблем забезпечення безпеки корпоративних баз даних у сучасних комп'ютерних системах дозволив зробити висновок щодо необхідності пошуку ефективних шляхів удосконалення захисту даних. Досліджені існуючі підходи до захисту даних та запропоновані шляхи для підвищення рівня безпеки корпоративних баз даних, які включають технічні та організаційні пропозиції організаціям при організації комплексної системи інформаційної безпеки. Їх врахування може значно підвищити ефективність захисту корпоративних баз даних в комп'ютерних системах.

Захист корпоративних баз даних є важливим завданням у сфері інформаційної безпеки. Успішна діяльність підприємств сьогодні значною мірою залежить від доступу до даних. Втрата чи недоступність цих даних може призвести до серйозних фінансових втрат та порушення роботи підприємств. У зв'язку з цим, багато країн впроваджують строгі законодавчі вимоги щодо захисту даних, такі як загальний регламент про захист даних (GDPR) в Європі або Каліфорнійська законодавча ініціатива щодо конфіденційності споживачів (CCPA) в США.

Однак, кількість кіберзагроз та атак на корпоративні бази даних з кожним роком зростає в геометричній прогресії, зловмисники вдосконалюють свої техніки та використовують штучний інтелект і квантові обчислення для створення більш складних і розумних атак щоб наносити збитки підприємствам.

Підприємства накопичують все більше даних, включаючи конфіденційну інформацію про клієнтів, фінансову та іншу важливу інформацію. Це робить корпоративні бази даних більш привабливими цілями для зловмисників. Корпоративні дані можуть знаходитися на різних пристроях та серверах у різних частинах світу. Збільшення використання мобільних пристроїв та хмарних технологій розширює поверхню атак і ускладнює захист даних. Виявлені проблеми захисту даних спонукають вітчизняних та зарубіжних науковців до пошуку нових ефективних методів захисту корпоративних баз.

У роботах [1, 2] розглянуто особливості захисту інформаційних ресурсів у корпоративних мережах та системах, а також описано підхід щодо їх оцінки, який дозволяє точніше описувати інформаційні ресурси через характерні для них вразливості, вартість самих ресурсів, а також ранжувати ризики та інформаційні ресурси за ступенем критичності для діяльності організації. Разом з тим, автори відзначають, що користувачі сучасних інформаційних систем належно не усвідомили необхідність системного підходу до питань забезпечення безпеки даних.

В роботі [3] проаналізовані складні та багатогранні причини, починаючи від зовнішніх атак і закінчуючи внутрішніми витоками, від технологічних

лазівок до недоліків управління, а також від нових ризиків, що виникають від нових технологій до нових моделей і повторюваних проблем з безпекою баз даних. Методи захисту конфіденційності здебільшого ґрунтуються на традиційних технологіях анонімізації, нечіткості та криптографії, але мають невеликий успіх у середовищі великих баз даних [4].

Безпека баз даних включає всі аспекти технологій та практик інформаційної безпеки. Безпека баз даних відноситься до ряду інструментів, засобів контролю та заходів, призначених для встановлення та збереження конфіденційності, цілісності та доступності бази даних. Вона повинна враховувати та захищати наступне:

- інформацію в базі даних;
- саму систему управління базами даних (СУБД)
- будь-які пов'язані програми, які приймають участь у обробленні та збереженні даних;
- фізичний (або віртуальний) сервер баз даних та відповідне обладнання;
- обчислювальна та мережева інфраструктура, що використовується для доступу до бази даних.

З метою захисту корпоративних баз даних в комп’ютерних системах, використовують різноманітні методи та засоби, такі як: шифрування, контроль доступу, автентифікація, авторизація, аудит, моніторинг та інші. В умовах постійних кіберзагроз і вразливостей комп'ютерних систем необхідно розробити ефективні способи для забезпечення конфіденційності, цілісності та доступності корпоративних даних.

Одним із шляхів підвищення ефективності захисту є розгортання поряд із брандмауером для бази даних також брандмауерів нового покоління (NGFW) для захисту своїх мереж і брандмауерів веб-додатків для захисту веб-сайтів і додатків, які отримують доступ до бази даних.

Також, для мінімізації внутрішніх загроз, організації повинні проводити перевірку біографічних даних програмістів, підрядників, фахівців з безпеки, адміністраторів баз даних і всіх, хто може отримати доступ до конфіденційної інформації або перенаправити її. Викрадення облікових даних хакерами виглядають для більшості інструментів безпеки як авторизований доступ, доки не буде виявлено незвичайну поведінку. Тому після підтвердження ідентичності співробітників організації повинні впроваджувати інструменти аналізу поведінки користувачів і організацій (UEBA), функції UEBA на інших інструментах безпеки та журнали аудиту для пошуку ознак неналежної або ненормальної поведінки.

Організаціям, які впроваджують менеджери паролів, може знадобитися складніший і частіший термін дії паролів, не турбуючись про те, що користувачі зберігатимуть свої паролі в незахищених або вразливих місцях. Доступ користувачів слід регулярно оновлювати, щоб запобігти доступу застарілих і забутих користувачів або пристроїв.

Резервне копіювання інформації баз даних має бути регулярним і надійно

захищеним. Найкращі практики дотримуються правила резервного копіювання 3-2-1, коли повинно бути три копії даних резервного копіювання, два типи сховища та принаймні одна копія зберігатися за межами сайту та в автономному режимі. Не повинно бути абсолютно ніякого публічного доступу до резервних копій, а резервні копії повинні шифруватися і зберігатися окремо від ключів шифрування.

Пристрої адміністратора повинні бути додатково обмежені використанням звуження IP і MAC-адрес, білого списку або контролю доступу до мережі (NAC).

Мережі повинні контролюватися за допомогою інструментів XDR або систем виявлення та запобігання вторгнень (IDPS). Усі системи безпеки повинні передавати сповіщення інструментам моніторингу інформації та подій безпеки (SIEM), операційним центрам безпеки (SOC) або командам керованого виявлення та реагування (MDR).

Компоненти поставок програмного забезпечення для управління базами даних, такі як бібліотеки з відкритим вихідним кодом, також повинні відслідковуватися та усуватися на наявність вразливостей та оновлень.

Отже, безпека баз даних – це складна справа, яка включає всі аспекти технологій та практик інформаційної безпеки. Удосконалення захисту корпоративних баз даних є важливим завданням в сучасних комп'ютерних системах. Зазначені шляхи, поряд із використанням сучасних методів шифрування, систем постійного моніторингу та двофакторної автентифікації можуть значно підвищити рівень безпеки даних у корпоративних середовищах.

Перелік посилань:

1. Кононова В. О., Грибков С. В., Харкянен О. В. Оцінка засобів захисту інформаційних ресурсів / В. О. Кононова, С.В. Грибков, О.В. Харкянен // Вісник Нац. ун-ту “Львівська політехніка”. – 2014. – № 806. – с. 99–105.

2. Якименко І. З. Критерії оцінки рівня захисту комп’ютерних мереж з врахуванням їх архітектури. // Інформатика та математичні методи в моделюванні, 2013. – Т. 3 – №1 – С. 82–90.

3. S.H. Kim, J. Kwon. How do EHRs and a meaningful use initiative affect breaches of patient information? / Inf. Syst. Res., 30 (4) 2019, pp. 1184-1202. DOI: https://doi.org/10.1287/isre.2019.0858

4. C. Yin, J. Xi, R. Sun, J. Wang. Location privacy protection based on differential privacy strategy for big data in industrial Internet of Things. //IEEE Transactions on Industrial Informatics, 14 (8) 2018, pp. 3628-3636. DOI: https://doi.org/10.1109/TII.2017.2773646

Будзинський Олександр Володимирович
аспірант групи АІКБ-11, ННІЗІ ДУІКТ, Київ, Україна

ЗАХИСТ КОРПОРАТИВНОЇ МЕРЕЖІ ВІД ШКІДЛИВИХ ІНТЕРНЕТ-РЕСУРСІВ

В умовах війни більш гостро постає проблема захисту користувачів від переходу на шкідливі інтернет-ресурси. Сторінки, які містять експлойти, фішинг-сайти, різні дезінформаційні ресурси, що використовуються з метою проведення ворожого ІПСО (інформаційно-психологічна операція) - лише частина з можливих шкідливих інструментів. Ситуацію ускладнює можливість використання та створення скорочених URL, коли назву ресурсу можливо дізнатися лише постфактум.

У сучасних компаніях (особливо в умовах епідемій чи війни) часто співробітники працюють не безпосередньо на робочому місці, а віддалено за допомогою персональних комп'ютерів, ноутбуків чи планшетів. Співробітники компаній, що знаходяться далеко від офісу, працюють з корпоративними додатками та документами, а також ведуть ділове листування, використовуючи корпоративну пошту, підключаючись до незахищених публічних хот-спотів або точок доступу. Крім того, стрімкий розвиток та популяризація хмарних сервісів призвела до того, що все більше користувачів використовує для підвищення продуктивності роботи різні файлові сервери та хмарні платформи, що нерідко порушує корпоративні правила роботи з мережею Інтернет.

Тенденція переходу корпоративних додатків та користувачів до хмарних сервісів робить традиційні засоби захисту периметра мережі менш надійними або й зовсім не ефективними. Компанія Cisco займається розробкою хмарних інструментів для захисту у кібер-просторі, один з досить потужних інструментів отримав назву Cisco Umbrella [1].

Завданням інструменту Cisco Umbrella є відстеження запитів на підключення до інтернет-ресурсів та захист корпоративних користувачів від проникнення шкідливого ПЗ (програмного забезпечення) при доступі до різних об'єктів в мережі інтернет.

Система повністю сканує всі DNS-запити, пропускаючи їх через свої бази та використовуючи алгоритми машинного навчання, ідентифікує відомі та нові DNS-запити. Такий підхід дозволяє надійно захистити корпоративних користувачів, що працюють в Інтернеті та хмарних мережах від фішингових ресурсів, botnet-мереж, проникнення шкідливого коду, що впливає на сервери через DNS-протокол, а також від інших загроз, які використовують DNS-імена у якості фундаменту для створення кібер-атак.

Ключові можливості Umbrella:

- незалежність від розробників обладнання: будь-які DNS-запити можна перевіряти;
- інтеграція з іншими продуктами від компанії Cisco (наприклад, Meraki), а також з іншими розробниками програмного забезпечення;
- контроль за роботою DNS-протоколу у мережі;
- надійний захист користувачів незалежно від Інтернет-провайдера;
- інспекція HTTPS- трафіку та файлів, блокування сайтів;
- контроль доступу до хмарних платформ;
- проактивне блокування загроз, що виникають;
- контроль корпоративних додатків.

Налаштування сервісу є відносно простим для великих корпорацій. Якщо корпоративна поліка інформаційної безпеки дозволяє використання персональних пристроїв для віддаленої роботи, на ньому потрібно встановлювати додаток Cisco AnyConnect, до якого буде під'єднано агент Umbrella та буде перехоплювати всі DNS-запити і направляти їх на довірені ресурси та блокувати доступ до підозрілих та шкідливих, інформуючи про це як

користувача: так і спеціалістів з інформаційної безпеки. Для максимального захисту в периметрі корпоративної мережі потрібно дозволити DNS-запити тільки на ресурси Cisco Umbrella та обмежити доступ до інших DNS-серверів (наприклад, всім відомий ресурс від Google – 8.8.8.8, або ресурс від Cloudflare - 1.1.1.1). А також в консолі управління потрібно вносити публічні адреси, з яких будуть надходити DNS-запити (публична IP-адреса, яку надає провайдер у точці підключення) [2].

На рисунку 1 відображено список поточних DNS-запитів, які можна побачити у консолі управління Cisco Umbrella.

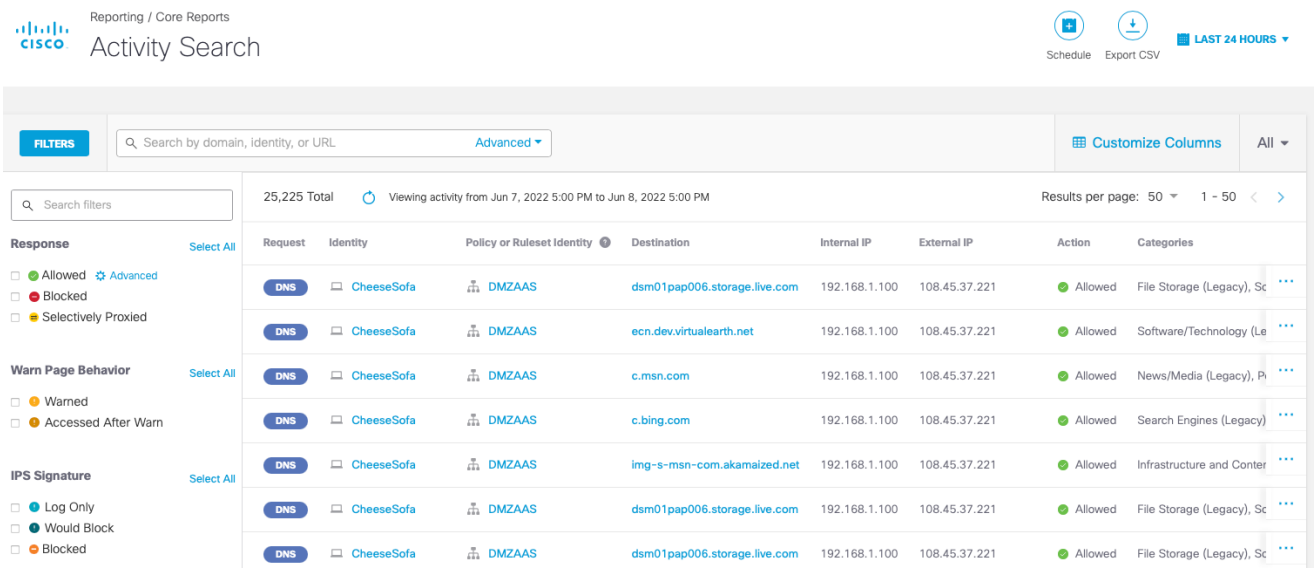


Рис.1. Поточні DNS-запити у консолі Cisco Umbrella

Продукт Cisco Umbrella заснований на проекті OpenDNS та дозволяє захищати не тільки корпоративну мережу, але й домашню. На сторінці OpenDNS потрібно зареєструвати власний обліковий запис. Вказати публічний IP-адрес, який використовується для доступу в Інтернет, та налаштувати правила, які запити блокувати, а які – ні. На домашньому маршрутизаторі вказати публічні IP-адреси DNS-серверів від OpenDNS. Якщо IP-адреса не статична, то на один з домашніх комп'ютерів потрібно встановити програму-агент «OpenDNS-Updater», яка періодично буде оновлювати інформацію на сервері OpenDNS про поточну публічну адресу домашньої мережі [3].

Основна відмінність полягає в тому, що Umbrella та OpenDNS поділяються сайти на дещо різні категорії в залежності від їх змісту. Крім того, OpenDNS оновлює базу даних повільніше за Umbrella. Тому, якщо створено новий шкідливий сайт, швидше від нього буде захищена та мережа, яка використовує Cisco Umbrella.

Cisco Umbrella за рахунок глобального охоплення дозволяє бачити всі запити в Інтернет, блокувати загрози до початку атаки і навіть передбачати їх за рахунок технологій машинного навчання та штучного інтелекту. Інструмент орієнтований на ті організації, які не впевнені, що їхні «периметрові» засоби

захисту ефективно фільтрують DNS-трафік, а також ті організації, які мають співробітників, які працюють віддалено, або мають розгалужену мережу філій із пристроями, що самостійно виходять в Інтернет (банкомати, термінали оплати тощо). Для домашньої мережі можна використовувати продукт OpenDNS.

Перелік посилань:

4. How to Secure Your Remote Workers URL: https://learn-cloudsecurity.cisco.com/umbrella-resources/umbrella/cybersecurity-for-remote-workers-how-to-secure-every-device-everywhere?language=English (дата звернення: 18.10.2023).
5. Cisco Umbrella SIG User Guide URL: https://docs.umbrella.com/umbrella-user-guide/docs (дата звернення: 18.10.2023).
6. OpenDNS Knowledge Base URL: https://support.opendns.com/hc/en-us/categories/204012807-OpenDNS-Knowledge-Base (дата звернення: 18.10.2023).

Бутенко Андрій Сергійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ЗАХИСТ КІНЦЕВИХ ПРИСТРОЇВ НА ОСНОВІ EDR СИСТЕМИ

Кількість загроз і атак на кінцеві пристрої продовжує зростати, а їхня важлива роль у бізнес-процесах і зберіганні конфіденційної інформації робить ефективний захист невід'ємною частиною кібербезпеки. Системи EDR (Endpoint Detection and Response) забезпечують комплексний моніторинг і реагування на загрози, виявляючи навіть найдрібніші аномалії. Це важливо для запобігання витоку даних, втрати та забезпечення безперервності бізнес-процесів. Таким чином, впровадження системи EDR є необхідним для ефективного захисту кінцевих пристроїв в умовах сучасних кіберзагроз.

Що таке EDR?

Виявлення кінцевих точок і реагування (EDR — Endpoint Detection and Response), також відоме як виявлення загроз кінцевих точок і реагування на загрози (EDTR — endpoint detection and threat response), — це рішення безпеки кінцевих точок, яке постійно відстежує пристрої кінцевих користувачів, щоб виявляти та реагувати на кіберзагрози, такі як програми-вимагачі та шкідливі програми [1].

Розроблений Антоном Чувакіним із Gartner, EDR визначається як рішення, яке «записує та зберігає поведінку на рівні кінцевої системи, використовує різноманітні методи аналізу даних для виявлення підозрілої поведінки системи, надає контекстну інформацію, блокує зловмисну активність і забезпечує виправлення для користувачів. пропозиція». Відновити уражені системи».

Gartner визначає виявлення загроз кінцевої точки та реагування на них як інструменти для виявлення та дослідження підозрілої діяльності (та її слідів) у кінцевій точці. Тому такі рішення можна віднести до серії Advanced Threat Protection. Архітектурно рішення полягає в наступному: агент кінцевої точки відстежує події на цьому рівні системи та мережі та/або надсилає інформацію про них на сервери чи хмару для подальшого аналізу та реагувати на виявлені загрози [2].

5 основних функцій EDR

Сьогодні основні можливості та функції виняткових,

високопродуктивних інструментів EDR і платформ захисту кінцевих точок EDR включають (рис. 1):

1. Розширене виявлення загроз і виявлення шкідливих дій.
2. Стримування загрози кібербезпеці на скомпрометованій кінцевій точці.
3. Пошук і розслідування даних про інциденти – сортування попереджень із оповіщенням високої точності.
4. Перевірка підозрілої діяльності та вказівки з усунення.
5. Полювання на загрози для захисту кінцевої точки від майбутніх атак.

Технологія EDR неухильно прогресує, включаючи розширені функції запобігання, а також безперервний моніторинг, виявлення в реальному часі та можливості видимості повного спектру, сортування та реагування [3].

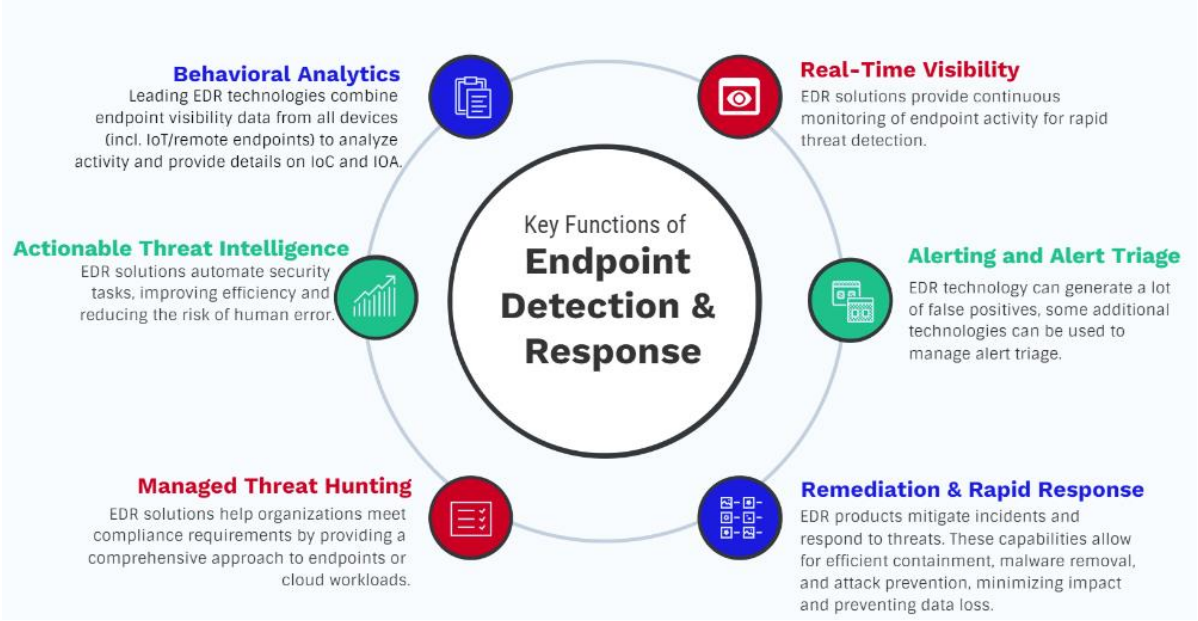


Рис. 1 — Основні функції EDR [3]

Ключові компоненти програмного забезпечення EDR

Більшість найсучасніших інструментів EDR тепер виконують аналіз першопричин усіх підозрілих, аномальних або активно заблокованих загроз за замовчуванням. У кожному разі технологія EDR визначає підозрілі події, а потім генерує сповіщення, які допомагають командам безпеки зупинити загрози та мінімізувати шкоду від атак на кібербезпеку [3].

Основні компоненти можливостей EDR включають:

1. Поведінкова аналітика.
2. Інтелектуальна інформація про загрози.
3. Керований пошук загроз.
4. Видимість у реальному часі.
5. Сповіщення та сортування повідомлень.
6. Рішуче усунення та реагування на інциденти.

Отже, захист кінцевих пристроїв на основі систем EDR є надзвичайно важливим елементом безпеки в сучасній мережі. Оскільки кіберзагрози продовжують зростати в масштабах і складності, недооцінка важливості

ефективного захисту кінцевих точок може мати серйозні наслідки для організацій.

Перелік посилань:

1. Aarness A. What is EDR? Endpoint Detection & Response Defined. crowdstrike.com. URL: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/ (дата звернення: 18.10.2023).
2. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с
3. Open EDR®. What is EDR? Endpoint Detection & Response Explained. URL: https://www.openedr.com/blog/what-is-edr/ (дата звернення: 18.10.2023).

Василенко Віталій Вікторович
студент групи УБДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ПІДХОДИ ДО ПЛАНУВАННЯ І РЕАЛІЗАЦІЇ ЗАХОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Розвиток інформаційної структури підприємств тягне за собою неконтрольоване збільшення кількості інформаційних загроз і вразливостей інформаційних ресурсів. Тому актуальність планування і реалізації заходів інформаційної безпеки підприємств обумовлена сьогодні сучасним розвитком інформаційних технологій, якими користуються кіберзлочинці та зростанням кількості кібератак. Запропонована методика планування заходів інформаційної безпеки підприємства допомагає забезпечити ефективність захисту від кіберзагроз, виконати регуляторні вимоги та зберігати конфіденційність даних.

Сьогодні інформаційна безпека стала невід'ємною частиною успішної діяльності підприємств у сучасному бізнесі. Із збільшенням кількості кібератак на дані підприємств і організацій, які потребують захисту, розповсюдженням шкідливих програм зростає потреба у пошуку ефективних заходів щодо інформаційної безпеки на підприємствах.

Відомості, які є предметом зловживань кіберзлочинців і підлягають захисту від порушення конфіденційності, цілісності та доступності відповідно до вимог нормативно-правових актів, відносять до основних активів підприємств. Сукупність технічних і програмних засобів, призначених для виконання функцій з обробки інформації обмеженого поширення складає допоміжні активи. Тому перед кожним підприємством, як стверджують науковці [1], постає питання комплексного підходу до розробки та впровадження методів і засобів захисту ресурсів інформаційно-комунікаційних систем та мереж підприємств.

Планування інформаційної безпеки на підприємстві - це процес, який включає ряд кроків і послідовності, спрямованих на забезпечення безпеки інформації та інформаційних ресурсів (рис. 1). Така методика допомагає підприємствам створити систему інформаційної безпеки, яка буде ефективно захищати їхню інформацію та інфраструктуру від потенційних загроз. При цьому

імовірність виникнення загроз впливає на величину ризику, розрахованого математично [2]

$$R = \lambda P_T P_V(z), \quad (1)$$

де R – ризик як комплексна величина; λ – розмір збитків, викликаних порушенням безпеки інформаційного активу; P_T – ймовірність виникнення загрози; $P_V(z)$ – функція, яка описує ймовірність реалізації загрози для інформаційного активу в залежності від витрат z на забезпечення захисних заходів.

Рис.1. Методика планування заходів інформаційної безпеки підприємства

Одним із важливих кроків у забезпеченні інформаційної безпеки на підприємстві є розробка політики безпеки яка визначає засади, стандарти та вимоги для збереження конфіденційності, цілісності та доступності інформації та інформаційних ресурсів і повинна бути створена з урахуванням особливостей підприємства та регуляторних вимог [3].

Великим потенціалом для поліпшення інформаційної безпеки на підприємствах є застосування штучного інтелекту. Він може використовуватися для виявлення загроз, автоматичного реагування на них та їх прогнозування, аналізу ризиків, вдосконалення захисту та управління інцидентами.

Таким чином, планування та реалізація заходів інформаційної безпеки залишається актуальним завданням для підприємств, оскільки це допомагає забезпечити захист від кіберзагроз, виконувати регуляторні вимоги та зберігати конфіденційність даних, зберігати неперервність бізнесу та зміцнювати позиції на ринку. Комплексний план інформаційної безпеки має бути адаптованим до конкретних потреб і ризиків підприємства, а також регулярно переглядатися та оновлюватися для ефективного захисту від сучасних кіберзагроз.

Перелік посилань:

1. А. Чунарьова, А. Чунарьов. Система управління інформаційною безпекою на базі міжнародних стандартів серії ISO. / Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2(24) вип., 2012 р. С. 48-52.

2. Карпович І.М., Гладка О.М., Наконечна Ю.А. Аналіз ризиків безпеки інформаційної системи ІТ-підприємства. / Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. Том 31 (70) № 5 2020. С. 69-74. DOI https://doi.org/10.32838/2663-5941/2020.5/12

3. Нечаєва І. А., Дьордій Є. А. Управління ризиками підприємства в секторі іт-послуг як інструмент підвищення його конкурентоспроможності. / Ефективна економіка. 2018. № 12. – URL: http://www.economy.nayka.com.ua/?op=1&z=6797 (дата звернення: 22.10.2023). DOI: https://doi.org/10.32702/2307-2105-2018.12.120

Вершигора Анатолій Миколайович
УБДМ-61, ДУІКТ, Київ, Україна

ЦЕНТР БЕЗПЕКИ SOC: ОСОБЛИВОСТІ ЗАСТОСУВАННЯ НА ПІДПРИЄМСТВАХ МАЛОГО, СЕРЕДНЬОГО ТА ВЕЛИКОГО БІЗНЕСУ

Усі сучасні компанії стикаються з проблемами підтримки ефективного реагування на кіберзагрози, тому центр безпеки SOC має важливе значення для їхньої стратегії протидії кіберризикам. SOC є стратегічною основою, яка дозволяє компанії реагувати та приймати рішення для зменшення ризиків кібербезпеки. Водночас підприємства малого, середнього та великого бізнесу, обираючи підходи до впровадження SOC, мають враховувати такі чинники як обсяги витрат, наявність кваліфікованих фахівців, можливості впровадження передових технологій тощо.

У сучасному світі, де інформаційні технології проникають у всі сфери бізнесу, важливість забезпечення кібербезпеки продовжує зростати. Центри оперативної безпеки (SOC) стали ключовим елементом стратегії захисту для компаній різного розміру. Але як вони впливають на підприємства малого, середнього та великого бізнесу?

Малий бізнес: Для малих компаній основними перешкодами в імплементації SOC часто є вартість та необхідність у кваліфікованих фахівцях. Малі підприємства можуть вирішувати ці проблеми, вдаючись до аутсорсингових SOC-послуг, які надають доступ до передових технологій та експертів без потреби великих інвестицій в інфраструктуру та персонал.

Середній бізнес: Середні підприємства часто знаходяться на перехресті між необхідністю в управлінні складнішими ІТ-інфраструктурами й обмеженими ресурсами. SOC у таких організаціях має бути масштабованим, враховуючи специфічні бізнес-вимоги та загрози, з якими вони стикаються. Розвиток інтегрованих та автоматизованих систем безпеки може сприяти ефективності та зменшенню витрат.

Великий бізнес: Великі корпорації зазвичай мають більше ресурсів і складніші ІТ-інфраструктури, що потребують вишуканої стратегії безпеки. Вони можуть дозволити собі створення внутрішніх SOC, які спроектовані для реагування на конкретні виклики організації та неперервного моніторингу загроз у реальному часі. Важливою є інтеграція з бізнес-процесами та стратегічними цілями компанії [1, 2].

Також слід розглянути шляхи потенційного розвитку SOC:

1. Автоматизація та штучний інтелект: Використання передових технологій, як-от штучний інтелект та машинне навчання, може зробити SOC

більш прогнозованими та ефективними, автоматизуючи рутинні задачі та аналіз великих обсягів даних.

2. Прогресивне навчання персоналу: Враховуючи швидкі зміни кіберзагроз, неперервне професійне розвиток та навчання персоналу є критично важливими для підтримання ефективності SOC.

3. Розширення інтеграції: SOC майбутнього повинні бути ще більш інтегрованими з іншими бізнес-функціями, що забезпечить ширший огляд загроз та більш цілісну стратегію безпеки.

4. Зосередженість на прогнозуванні та відновленні: Наступне покоління SOC буде зосереджене не тільки на виявленні та реагуванні, а й на прогнозуванні потенційних кіберзагроз та стратегіях швидкого відновлення після інцидентів [3].

Забезпечення кібербезпеки є неперервним процесом, який вимагає адаптації до нових загроз та використання передових технологій. Сучасні SOC повинні еволюціонувати у відповідь на ці зміни, щоб захистити важливі активи своїх організацій незалежно від їх розміру або сектору діяльності.

Список використаної літератури:

1. Впровадження SIEM і SOC. URL: https://www.h-x.technology/ua/siem-soc-implementation-ua
2. Securing Success: Why Small and Medium Enterprises (SMEs) Need a Security Operations Center (SOC) URL: https://www.linkedin.com/pulse/securing-success-why-small-medium-enterprises?trk=organization_guest_main-feed-card_feed-article-content
3. Security Operations Center: SOC Ultimate Business Guide. URL: https://www.think-cloud.co.uk/blog/security-operations-center-soc-ultimate-business-guide/

Веселков Нікіта Леонідович
аспіранта групи АІКБ-11, ННІЗІ ДУІКТ, Київ, Україна
Марченко Віталій Вікторович
Доцент кафедри Інформаційної та кібернетичної безпеки, ННІЗІ ДУІКТ, Київ, Україна

МЕТОД ОПТИМІЗАЦІЇ ПРОЦЕСІВ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ В РОЗГАЛУЖЕНИХ SOC КОМАНДАХ

Розглянуто функціональні обов’язки фахівців SOC команди і процеси цих команд під час розслідування. На основі цієї інформації представлені основні методи оптимізації цих процесів.

Ключові слова: SOC, розслідування, фахівців кібербезпеки, оптимізації, NIST.

Центр управління безпекою (SOC) представляє собою централізовану функцію всередині організації, яка використовує ресурси людей, процесів і технологій для постійного контролю та покращення рівня безпеки організації шляхом виконання завдань з превентивного захисту, виявлення, аналізу та реагування на кібербезпекові інциденти. Розслідування кіберінциденту в командах SOC - це комплексний процес, спрямований на виявлення, аналіз, врегулювання та усунення кіберзагрози або інциденту в інформаційній системі. Процес розслідування зазвичай включає в себе такі кроки:

- Виявлення інциденту: SOC команда спостерігає за подіями в мережі та в системах і виявляє підозрілі або аномальні активності, які можуть свідчити про кіберзагрозу. Це може включати в себе моніторинг логів, сенсорів, виявлення вразливостей і аналіз сигналів з систем захисту.
- Збір даних: Коли підозрілий інцидент виявлено, SOC команда розпочинає збирати дані, пов'язані з інцидентом. Це може включати в себе аналіз логів, дампів пам'яті, файлів, мережевих пакетів та інших відомостей, що допомагають встановити природу і масштаб інциденту.
- Аналіз даних: Отримані дані піддаються глибокому аналізу для встановлення того, як саме інцидент стався, хто міг бути залучений і які наслідки це може мати для організації. Завдяки аналізу, команда може визначити, який тип загрози був використаний і чи були компрометовані системи чи даних.
- Ідентифікація винних: На цьому етапі SOC команда намагається визначити винних або здійснює спроби відстежити джерело атаки. Це може включати в себе вивчення сигнатур, методів атак та інших характеристик нападу.
- Врегулювання інциденту: Після виявлення і виокремлення загрози або атаки SOC команда приймає заходи для обмеження поширення інциденту та мінімізації збитків. Це може включати в себе заблокування атакуючих IP-адрес, вимкнення компрометованих облікових записів і інші заходи безпеки.
- Відновлення та запобігання майбутнім інцидентам: SOC команда також працює над відновленням систем до нормального режиму і розробляє плани для запобігання майбутнім інцидентам. Це може включати в себе оновлення політик безпеки, застосування патчів, навчання персоналу та інші заходи.
- Документація і звітність: На завершальному етапі SOC команда докладно документує всі кроки, взяті під час розслідування, та складає звіт, який включає в себе виявлені загрози, заходи, вжиті для їх усунення, і рекомендації щодо подальших дій.

Кожен з даних етапів може бути, а в деяких випадках навіть потребує оптимізації для покращення робочих умов і ефективності процесів фахівців SOC команди. Методи оптимізації процесів SOC включають в себе наступні основні процеси:

- Покращення робочих інструментів (технологічних розробок). Команда може поліпшити власні інструменти які Вони використовують для розслідування і також, придбати або оптимізувати сторонні рішення від вендорів які використовуються в їх роботі.
- Розробка та впровадження технологій машинного навчання. Машинне навчання може допомогти фахівцям SOC команди більш детально аналізувати виявлені події, покращити моніторинг, зменшити час який витрачають фахівці при аналізі інцидентів та поліпшити багато інших рутинних процесів фахівців SOC.

- Доповнення документації та розробка нових нормативних документів. Процес оптимізація наявної документації включає в себе підтримку актуальної документації, що описує процедури і плани відновлення, використання баз даних з інформацією про виявлені загрози та інциденти для аналізу та попередження майбутніх подібних ситуацій, ведення журналів інцидентів для аналізу і покращення дій у майбутньому та інші процеси.
- Покращення досвіду фахівців та комунікації між ними. Фахівці SOC потребують постійного підвищення кваліфікації, як за допомогою стороннього навчання і сертифікації, так і за рахунок внутрішніх процесів навчання, наприклад використання навчальних даних для тренування аналітиків і підвищення їхньої ефективності в розслідуванні інцидентів або проведення після-інцидентного аналізу для визначення, які кроки були ефективними, а які можна поліпшити. Також фахівці потребують оптимізації їх комунікації, наприклад, шляхом організації регулярних зустрічей і тренувань для покращення комунікації та співпраці між співробітниками

Дані методи є загальними і можуть доповнюватися окремим техніками та підходами в залежності від різних факторів у SOC командах, таких як, їх розмір, функціональні обов'язки фахівців, сфера діяльності або кількість клієнтів з якими вони працюють. Оптимізація процесів вкрай необхідна для подібних структур в кібербезпеці, бо саме від таких команд і фахівців залежить стан безпеки інфраструктур компаній та працездатність бізнесу у випадку кіберінцидентів.

Перелік посилань:
1. ISO 18788 Security Operations Management System Training
2. NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response.
3. ISO/IEC 27035:2011

Висотін Микита Дмитрович
студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ WEB-ДОДАТКІВ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

На сьогодні, веб-вразливості справді перевершують по кількості і можливій шкоді будь-які інші проблеми інформаційної безпеки. Більшість зовнішніх атак на корпоративні інформаційні системи націлені саме на вразливості веб-додатків. Багато компаній, навіть з незвичних нам сегментів ринку, повністю переходять в онлайн. А поширення онлайн-платежів тільки підсилює цей тренд. Як показує досвід, там де є онлайн продажі, використання спеціалізованого обладнання для захисту є по-справжньому критичним та необхідним.

Серед основних загроз на рівні з використанням програмних вразливостей, зловмисники активно використовують і фішингові інструменти, які побудовані на

помилках людей. Від цього нам нікуди не втекти, однак спеціалісти з інформаційної безпеки також не сидять склавши руки. Сьогодні на ринку вже доступні ефективні інструменти захисту веб-додатків.

На сам перед виявленням вразливостей в корпоративній інформаційній системі займаються так звані “білі хакери”. Кожний спеціаліст має свій підхід та інструментарій для тестування.

Інструментарій:

- **Acunetix Vulnerability Scanner –** повністю автоматизований out-of-band сканер уразливостей із можливостями Black-Box та Gray-Box аналізу з єдиним відображенням даних. Може бути розгорнутий у хмарі та за клієнта;

- Burp Suite – це програмне забезпечення безпеки, яке використовується для тестування веб-застосунків на проникнення;

- Metasploit Project – проект, присвячений інформаційній безпеці. Створений для надання інформації про вразливість, допомогу у створенні сигнатур для IDS, створення та тестування експлойтів. Найбільш відомий проект Metasploit Framework – зручна платформа для створення та налагодження експлойтів;

- Nmap — вільна утиліта, призначена для різноманітного сканування IP-мереж, що настроюється, з будь-якою кількістю об'єктів, визначення стану об'єктів сканованої мережі;

-и т.д

Більшість вразливостей знаходяться під час ручного тестування SQLinjection,XSS, и т.д.

Цілі в тестуванні безпеки:

-у складних системах, де задіяні багато взаємодій, критично важливі для безпеки функції повинні бути ідентифіковані та ретельно проаналізовані;

-помилки визначені та усунені;

-кількість критичних помилок підтримується на низькому рівні, щоб уникнути непрацездатності системи;

-атрибути безпеки повинні розглядатися як частина всіх рівнів тестування ПЗ.

Додаткову інформацію з безпеки програм можна дізнатися тут: CHECK, ISACA, NIST Guideline, OSSTMM, OWASP Guide.

Принципи безпеки:

Конфіденційність (обмеження або надання доступу до інформації).

Цілісність (можливість відновити дані в повному обсязі у разі їх пошкодження; доступ до зміни інформації тільки певної категорії користувачів).

Доступність (ієрархія рівнів доступу та їх чітке дотримання).

Перелік посилань:

1. Тестування веб-проєктів: основні етапи та поради URL: https://qalight.ua/baza-znaniy/testuvannya-veb-proektiv-osnovni-etapi-ta-poradi/ (дата звернення: 19.10.2023).
2. Pentest URL: https://habr.com/ru/articles/651167/ (дата звернення: 19.10.2023).
3. Acunetix URL: https://corewin.ua/ru/security/acunetix/ (дата звернення: 19.10.2023).

Ворона Олександр Анатолійович, БСДМ-61
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОЇ РОБОТИ ГІБРИДНИХ ПРАЦІВНИКІВ ОРГАНІЗАЦІЇ НА БАЗІ FORTISASE

Визначено мету і основні завдання щодо забезпечення безпечної роботи гібридних працівників організації. Розглянуто зміст технології забезпечення безпечного доступу гібридних працівників організації.

Віддалена робота працівників організацій створює нові вразливості до атак. Порушення безпеки, пов’язані з віддаленою роботою працівників організацій, коштують дорожче. Так, Звіт IBM Cost of a Data Breach 2022 [1] показав, що віддалена робота в усьому світі збільшила середню вартість витоку даних майже на 1 мільйон доларів. Зломи в США з дистанційною роботою коштують на 600 000 доларів більше, ніж у середньому по світу.

Зі збільшенням кількості гібридної робочої сили організації повинні захистити своїх співробітників, які отримують доступ до мережі та додатків як на місці, так і за його межами. Цей перехід до роботи з будь-якого місця (work-from-anywhere, WFA) значно розширив сферу атак, охопивши домашні офіси і мобільних працівників, тим самим збільшуючи складність захисту мережі, додатків і ресурсів. Організації, що мають справу з численними віддаленими офісами і співробітниками, які працюють за принципом WFA, часто стикаються з труднощами в послідовному застосуванні і впровадженні політик безпеки, а також із забезпеченням оптимальної роботи користувачів, незалежно від їхнього мережевого розташування [2].

Захист цього гібридного середовища являє собою унікальний виклик, оскільки зміни відбулися органічно, а не в результаті ретельно спланованої стратегії. Швидке поширення нових мережевих кордонів і залучення співробітників WFA, часто реалізовані як незалежні проекти, створили вразливості, якими охоче користуються кіберзлочинці.

Архітектура сервісу безпечного доступу (secure access service edge, SASE) допомагає протистояти цим загрозам, розширюючи безпечний доступ і високопродуктивне з'єднання для користувачів у будь-якому місці. Однак багато рішень SASE вирішують лише частину проблеми. Вони або не забезпечують кібербезпеку корпоративного рівня для співробітників WFA, або не здатні безперешкодно інтегруватися з низкою фізичних і віртуальних засобів захисту, розгорнутих на кордоні мережі. Або і те, і інше. Результатом є нездатність забезпечити узгоджену політику безпеки і оптимального користувацького досвіду для всіх співробітників.

FortiSASE, створений на основі підходу єдиного постачальника Fortinet (рис. 1), забезпечує комплексне рішення SASE, інтегруючи хмарне підключення до програмно-визначеної глобальної мережі (software-defined wide area network,

SD-WAN) з хмарною службою безпеки (security service edge, SSE), що розширює можливості конвергенції мереж і безпеки від межі мережі до співробітників WFA [2].

FortiSASE був спеціально розроблений, щоб об'єднати мережеві технології та безпеку в інтегроване та адаптивне рішення для забезпечення оптимального та безпечного з'єднання для користувачів WFA. FortiSASE забезпечує безпечний веб-шлюз (secure web gateway, SWG), доступ до мережі з нульовою довірою (zero-trust network access, ZTNA), брокер безпеки хмарного доступу наступного покоління (cloud access security broker, CASB), брандмауер як послугу (Firewall-as-a-Service, FWaaS) як хмарну послугу, а також безпечну SD-WAN з уніфікованим управлінням і веденням журналів.

Стратегія безпечної роботи в мережі, заснована на єдиній операційній системі FortiOS і доповнена послугами безпеки на основі штучного інтелекту FortiGuard, що дозволяє Fortinet об'єднати функції безпеки і роботи з мережею в єдину інтегровану систему, що забезпечує стабільну безпеку і зручність роботи для будь-якого користувача в будь-якій точці світу. FortiSASE дозволяє організаціям захистити доступ до Інтернету, хмарних сховищ і додатків з будь-якої точки світу за допомогою вбудованих засобів кібербезпеки корпоративного рівня та користувацького інтерфейсу.

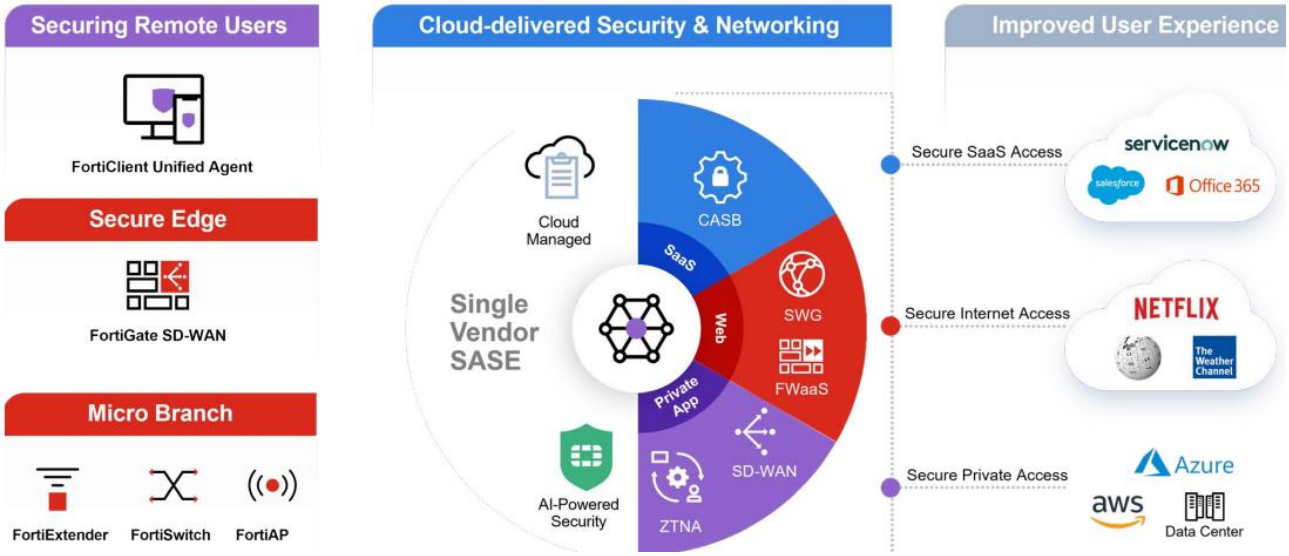


Рис. 1. SASE від одного постачальника з послугами безпеки на основі штучного інтелекту [2]

Отже, інтегроване хмарне рішення SASE захищає користувачів, додатки та кінцеві пристрої, безперешкодно взаємодіючі з рештою активів розподіленої мережі. Цей легкий наскрізний підхід до конвергенції мереж і безпеки забезпечує адаптивну стратегію, необхідну організаціям у сучасному цифровому середовищі, що швидко розвивається. Крім того, з розширенням підходу SASE від одного постачальника, FortiSASE стає найбільш комплексною та інтегрованою пропозицією SASE в галузі. Вона захищає користувачів, доступ, кордони і пристрої в будь-якому місці, забезпечуючи при цьому найвищу

рентабельність інвестицій, послідовну політику безпеки і покращений користувацький досвід. Завдяки підходу до конвергенції безпеки та мережевої конвергенції, FortiSASE забезпечує простий і безпечний перехід до SASE.

Література

1. Cost of a Data Breach Report. IBM. URL: https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258. (дата звернення: 29.09.2023).

2. A Comprehensive SASE Solution to Secure the Hybrid Workforce. Solution Brief. Fortinet. URL: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-fortisase-cloud-delivered-securtiy-to-every-user.pdf. (дата звернення: 29.09.2023).

Врадін Клим Сергійович
Студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

ШТУЧНИЙ ІНТЕЛЕКТ І КІБЕРБЕЗПЕКА

Тема "Штучний інтелект і кібербезпека" стає все більш актуальною зі зростанням застосування штучного інтелекту (ШІ) у кіберсередовищі. Ця сфера дослідження займається дослідженням загроз, пов'язаних з використанням ШІ для кібератак, а також створенням методів та технологій для виявлення та захисту від таких атак. Це критичну проблему в епоху, коли ШІ використовується як інструмент як для кіберзлочинців, так і для захисту кіберсистем.

Штучний інтелект (ШІ) - це область інформатики та комп'ютерних наук, яка займається створенням систем та програм, здатних виконувати завдання, які зазвичай потребують інтелектуальних здібностей людини. Основною метою ШІ є розробка комп'ютерних систем, які можуть аналізувати інформацію, навчатися на основі досвіду, приймати рішення, вирішувати проблеми та виконувати завдання, які раніше могли бути виконані лише людиною.

У найближчому майбутньому штучний інтелект змінить світ. Частково ці зміни будуть позитивними та можуть принести користь людям у таких сферах, як охорона здоров’я, транспорт, поліпшення планування міського простору, але водночас вони можуть бути серйозною загрозою, зокрема в руках терористичних та злочинних груп.

Розвиток штучного інтелекту, що спостерігається нині, в основному обумовлений експоненціальним розвитком в області напівпровідникових технологій. Потужність обчислювальних операцій, пам’яті, каналів передачі даних з часом невідворотно зростає, а наявне обладнання дозволяє розробляти великомасштабні алгоритми штучного інтелекту, які були опрацьовані понад 40 років тому. За кілька доларів ви можете створити комп’ютер, який має потужність колишніх обчислювальних центрів.[2]

Поява штучного інтелекту (AI – artificial intelligence) може стати «найгіршою подією в історії нашої цивілізації», якщо людство не знайде спосіб контролювати його нестримний розвиток. Про це заявив видатний фізик Стівен Хокінг, виступаючи на технологічній конференції Web Summit у Лісабоні, Португалія.

За словами вченого, штучний інтелект можна використовувати для того, щоб зменшити шкоду, яку завдає людство навколишньому середовищу, щоб

викорінити бідність і хвороби, однак майбутнє і досі невизначено.[1]

Також штучний інтелект стає потужним інструментом як для кіберзлочинців, так і для фахівців з кібербезпеки. Можливості ШІ можуть бути використані для автоматизації атак, створення підроблених повідомлень та зловмисних програм, а також для обходу систем виявлення інцидентів.

Обчислювальні системи, що використовують штучний інтелект (ШІ) і машинне навчання, відіграють все більш важливу роль у кібероперація̈х і стали основним напрямком досліджень у сфері кібербезпеки. Оператори служби безпеки повинні бути в курсі всього, що відбувається у вашій системі, і вміти швидко виявляти аномалії, такі як шкідливе програмне забезпечення або неправильні конфігурації, щоб зупинити порушення в сучасному гіперзв'язаному цифровому світі. У цілісному розумінні технології штучного інтелекту можуть допомогти в захисті від програм-вимагачів, соціальної інженерії та шкідливого програмного забезпечення, яке стає все більш витонченим і руйнівним.

Розглянемо сфери, де штучний інтелект може бути сприятливим, та області, де він становить потенційну загрозу. Почнемо з позитивних аспектів. Значною мірою штучний інтелект дійсно автоматизує безліч людських функцій, що призводить до економії часу та ресурсів.

Переваги:

1. Діагностування захворювань;
2. Правова сфера;
3. Аналіз та обробка великого обсягу даних у всіх сферах промисловості, економіки, інших сферах;
4. Допомога технологій штучного інтелекту у космічній сфері та науці;
5. Економія часу;
6. Економія коштів та ефективність застосування в банківській сфері.

Загрози:

1. Масове безробіття;
2. Втрата контролю над штучним інтелектом;
3. Розвиток конфліктів на релігійному, соціальному, економічному підґрунті.

Перелік посилань:

1. Стівен Хокінг: штучний інтелект може стати найгіршим винаходом людства URL: https://mind.ua/news/20178313-stiven-hoking-shtuchnij-intelekt-mozhe-stati-najgirshim-vinahodom-lyudstva
2. Штучний інтелект стане головною загрозою людству URL: https://1news.com.ua/tsikave/shtuchniy-intelekt-stane-golovnoyu-zagrozoyu-lyudstvu.html
3. A Primer On Artificial Intelligence And Cybersecurity URL: https://www.forbes.com/sites/chuckbrooks/2023/09/26/a-primer-on-artificial-intelligence-and-cybersecurity/?sh=2e824bf875d2

Гавриленко Євгеній Дмитрович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ПОДВІЙНІ АТАКИ ВИМАГАННЯ ЯК ОДНА З НАЙБІЛЬШИХ ПРОБЛЕМ КІБЕРБЕЗПЕКИ У 2023 РОЦІ

Впроваджуючи нові IT-рішення та технології, компанії одночасно з цим й створюють нові ризики для безпеки. Кіберзлочинність стає дедалі професійнішою, що в свою чергу призводить до виникнення більш численних, непомітних і витончених загроз. Суб'єкти боротьби з кіберзагрозами щоденно працюють над розробкою, проектуванням і розвитком рішень, які могли б будь-яким чином обійти чи подолати найсучасніші рішення кібербезпеки.

Програми-вимагачі з'явилися як зловмисне програмне забезпечення, яке було зосереджене на вимаганні грошей за допомогою шифрування даних. Відмовляючи легітимним користувачам у доступі до їх даних шляхом шифрування, зловмисники могли вимагати викуп за їх відновлення, і тому зростання загроз від програм-вимагачів стало причиною цілеспрямованих досліджень безпеки, які ставили собі за мету виявлення та усунення цих загроз. Процес шифрування кожного окремого файлу в цільовій системі займає багато часу — і це дає можливість зберегти деякі дані шляхом припинення зловмисного програмного забезпечення до моменту завершення шифрування — що в свою чергу дозволяє компаніям відновити дані з резервних копій, не сплачуючи викупу зловмисникам.

Подвійні атаки вимагання додали крадіжку даних до вже існуючого шифрування даних, а деякі оператори програм-вимагачів навіть перейшли до зосередження виключно на крадіжці даних, повністю пропускаючи процес шифрування. Такі витоки даних програм-вимагачів швидше здійснити, їх важче виявити, а також неможливо виправити за допомогою наявних резервних копій, що робить їх найефективнішим підходом для кіберзлочинців і ще більшою загрозою для корпоративного сектору.

У підсумку, подвійна атака вимагання є різновидом кібератаки, під час якої зловмисники отримують доступ до конфіденційних даних жертви, а не тільки шифрують їх, що в свою чергу підвищує їх шанси на отримання викупу. Стандартні атаки програм-вимагачів лише шифрують дані жертви, а додаткова загроза ексфільтрації робить цю атаку вкрай небезпечною для організацій у всіх галузях.

Взагалі, існує 4 етапи вимагання програм-вимагачів: одиночне вимагання, подвійне вимагання, потрійне вимагання і чотириразове вимагання.

Одиночне вимагання (перший етап багаторазового вимагання) передбачає шифрування. Зловмисники або шифрують цілі системи, або обирають файли, які вважають вкрай важливими. Одиночне вимагання є єдиним методом атаки для таких програм-вимагачів, як WannaCry та CryptoLocker.

Більшість компаній з легкістю долають загрозу шифрування файлів, використовуючи актуальну систему резервного копіювання. Щоб протистояти цьому, оператори зловмисного програмного забезпечення почали впроваджувати ще один етап вимагання, який передбачає отримання несанкціонованого доступу до даних, – тактику, яка набула популярності завдяки таким шкідливим програмам, як Maze та DoppelPaymer. Зловмисники викрадають конфіденційні дані та погрожують оприлюднити їх у "даркнеті" або продають їх на "чорному ринку".

Атака з потрійним вимаганням може приймати дуже різні форми, але зазвичай вона лише ще більше розширює "ігрове поле" для зловмисників. Наприклад, якщо жертва відмовляється платити викуп навіть після загрози, що її конфіденційна інформація буде розголошена, то щоб вчинити додатковий тиск, може бути використана атака зриву служби. AvosLocker є одним із типів програм-вимагачів, що використовують DDoS-атаки як невід'ємну частину свого інструментарію потрійного вимагання.

Кіберзлочинці також можуть спробувати збільшити свої прибутки, використовуючи програми-вимагачі з чотириразовим вимаганням, що впроваджують додатковий рівень, який передбачає контакт із партнерами жертви з метою отримання викупу або іншою підступною тактикою. Наприклад, коли постачальник апаратного забезпечення Quanta відмовився сплачувати викуп групі зловмисників REvil, вони звернули увагу на Apple, яка є одним із клієнтів Quanta.

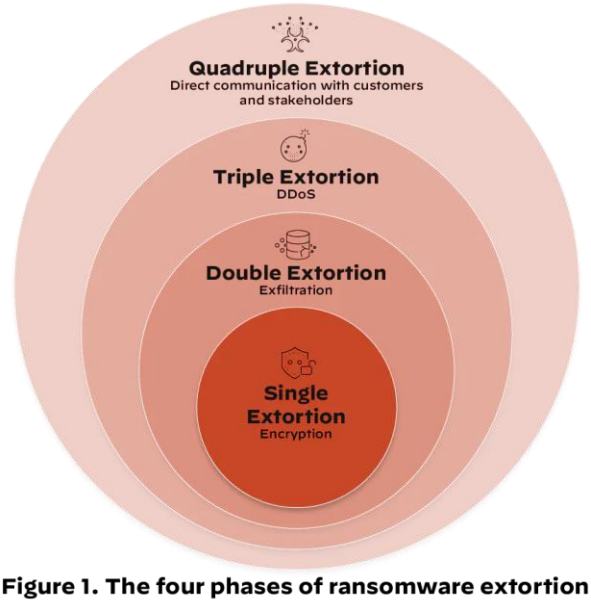


Figure 1. The four phases of ransomware extortion

Рис. 1 – Чотири етапи вимагання програм-вимагачів

Подвійні атаки вимагання можуть завдавати компаніям шкоди,

позбавляючи їх доступу до важливих даних, а також розкриваючи їх конфіденційну інформацію на загал. Люди та компанії повинні вживати профілактичних заходів, аби краще підготуватися до захисту і подальшим відновленням після подібних атак. Захист від подвійних атак вимагання включає наступне:

- **Наявність надійної політики автентифікації та отримання доступу**. Успішність подвійної атаки вимагання в першу чергу залежить від отримання доступу до системи. Заблокувавши систему та автентифікацію користувачів, а також використовуючи надійні протоколи та багатофакторну автентифікацію, компанії значно ускладнюють отримання доступу до системи для зловмисників.
- **Глибокий захист мережі**. Комплексна стратегія глибокого захисту помічає атаки, перш ніж вони стануть небезпечними. Для цього потрібно використовувати комбінацію брандмауерів, інструментів аналізу мережевого трафіку, систем запобігання та виявлення вторгнень, веб-фільтрації та сканування кінцевих точок.
- **Проактивне полювання на загрозу**. Інструменти проактивного полювання на загрози активно шукають можливі загрози, які могли якимось чином обійти укріплення мережі.
- **Навчання з питань кібербезпеки**. Використання соціальної інженерії та фішингових атак є доволі популярним способом проведення подвійних атак вимагання. Потрібно обмежити цей ризик шляхом навчання всіх співробітників і підрядників, які мають доступ до мережі.
- **Використання інструментів захисту від втрати даних**. Інструменти захисту від втрати даних були спеціально створені, аби гарантувати компаніям, що їхня конфіденційна та приватна інформація жодним чином не залишить мережу.
- **Безперебійне резервне копіювання**. Програми-вимагачі спеціалізуються на забороні доступу до даних. Потрібно належним чином підтримувати безперебійне резервне копіювання в безпечному та віддаленому місці, аби підвищити шанси на швидке відновлення даних, якщо подібні атаки будуть мати місце.

Список використаних джерел:

1. Biggest Cyber Security Challenges in 2023 [Electronic Resource]. - Mode of access : URL : https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/biggest-cyber-security-challenges-in-2023. - Title from the screen.
2. What Is Double Extortion Ransomware? [Electronic Resource]. - Mode of access : URL : https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortion-ransomware. - Title from the screen.
3. What is Multi-Extortion Ransomware? [Electronic Resource]. - Mode of access : URL : https://www.paloaltonetworks.com/cyberpedia/what-is-multi-extortion-ransomware. - Title from the screen.
4. double extortion ransomware [Electronic Resource]. - Mode of access : URL : https://www.techtarget.com/searchsecurity/definition/double-extortion-ransomware. - Title from the screen.

Гайдур Ксенія Володимирівна
Студентка групи БСДМ-51, ННІЗІ, ДУІКТ, Київ, Україна

ПРОТИДІЇ ФІШИНГОВИМ АТАКАМ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

Завдяки високому цифровому розвитку інформаційні системи стають невід'ємною частиною організаційної інфраструктури. Однак через доступність та відкритість інтернету з'являються й високоінтелектуальні кіберзагрози, де фішингові атаки виходять на перший план як одна з найпоширеніших загроз.

З розквітом цифрових технологій та інтернету організації отримують доступ до великих джерел знань, покращенні методи зберігання та обробки інформації й не тільки, проте завжди є ті, хто бажає незаконно отримати конфіденційні та персональні дані з подальшим зловмисним використанням. Саме фішинг є одним із найпоширеніших методів викрадення облікових даних, які використовують кіберзлочинці в усьому світі. Перевага такого методу полягає в тому, що його легко замаскувати, а ефективність надзвичайно висока, і що найважливіше – дуже важко звинуватити злочинців, які займаються фішингом, в будь-якому кіберзлочині. Все через те, що жертва фактично надає їм облікові дані сама, без жодного примусу з боку шахраїв, саме тому це навряд чи можна класифікувати як шантаж чи розповсюдження зловмисного програмного забезпечення.

Що з себе представляє фішинг? Фактично це повідомлення надіслане з нібито надійного джерела (типу з банку чи іншого популярного онлайн-сервісу), де буде запропоновано, наприклад, підтвердити ваші дані облікового запису, номер кредитної картки чи іншої конфіденційної інформації. Саме при підтвердженні даних жертва надає про себе інформацію чи дозволяє проникнути в свою інформаційну систему зараженому вірусом файлу, який надалі буде викрадати персональні дані та поширюватись по всій цифровій системі.

Ціль фішингу — отримання цінних даних, які можуть бути продані або використані для зловмисних цілей, таких як вимагання, шантаж, викрадення грошей або особистих даних.

Шляхи фішингу численні, оскільки кіберзлочинці постійно винаходть нові методи виманювання конфіденційної інформації. У минулому для для цього часто використовували неправильно написані або оманливі доменні імена. Сьогодні зловмисники використовують вже більш складні методи, завдяки чому фальшиві сторінки дуже схожі на свої легітимні аналоги.

Організаціям дуже важливо знати як захистись від такого роду загроз тому, що:

- *Поширеність*

Фішингові атаки є поширеними і всепроникаючими загрозами у кібербезпеці. Вони постійно розвиваються, використовуючи вдосконалені тактики для обману. Всезагальна природа цих атак робить їх підкресленою проблемою для осіб, бізнесів і організацій будь-якого розміру.

- *Фінансові та репутаційні наслідки*

Успішні фішингові атаки можуть призвести до несанкціонованого доступу, до фінансових рахунків, шахрайських транзакцій та крадіжки конфіденційної інформації. Крім того, репутаційний збиток від атаки може піддавати сумніву довіру і впливати на становище організації в очах клієнтів, партнерів і зацікавлених сторін.

- *використання вразливостей людини*

Фішингові атаки часто використовують вразливості людей, а не покладаються виключно на технічні вразливості. Техніки соціальної інженерії використовуються для маніпулювання особами та отримання від них конфіденційної інформації або виконання дій, що можуть компрометувати безпеку. Вирішення цього людського елементу вимагає багатокрокового підходу, що включає в себе освіту, обізнаність та навчання.

- *Еволюція технік*

Техніки фішингу постійно змінюються, що робить важким завдання традиційних заходів кібербезпеки наздогнати їх. Зловмисники регулярно адаптують свої тактики для обхіду протоколів безпеки, що робить обов'язковим для організацій впровадження динамічних і адаптивних протидій.

- *Залежність організацій від інформаційних систем*:

В сучасній цифровій епохі організації великою мірою залежать від інформаційних систем для проведення своєї діяльності. Компрометація цих систем через фішингові атаки можуть порушити бізнес-процеси, призвести до порушення конфіденційності даних і призвести до значного періоду недоступності.

Таким чином із зростанням залежності від технологій росте і необхідність вдосконалених захистів від фішингових загроз.

До основних видів фішингових атак відноситься:

- *Фішинг в електронних листах*

Найпоширеніша форма фішингу, атаки якого зловмисники здійснюють, підроблюючи гіперпосилання в електронних листах, щоб обманом примусити користувачів розкрити свої персональні дані.

- *Фішинг за допомогою зловмисних програм*

Атака за допомогою прихованого шкідливого програмного забезпечення. Зустрічаються у «безпечних» здавалося б файлах та у вкладеннях в електронних листах.

- *Цільовий фішинг*

В даному випадку жертвами цільового фішингу є конкретні особи, робочі й особисті дані яких вдалося зібрати зловмисникам. Атаки налаштовані так, щоб можна було легко обійти базові технології кібербезпеки.

- *Полювання на велику здобич*

На відміну від цільового фішингу тут кіберзлочинець обирає так званих поважних осіб (бізнесменів або знаменитостей). Шахраї вишукують відомості про своїх жертв, а потім вичікують слушного моменту, щоб викрасти їхні

облікові дані або іншу делікатну інформацію.

- *Смсшинг*

Цей вид фішингу утворено в результаті поєднання двох слів: "SMS" і "фішинг". Зловмисники надсилають шахрайські SMS-повідомлення начебто від від надійних джерел.

- *Вішинг*

Зловмисники телефонують людям із шахрайських інформаційно-довідкових служб і намагаються визнати в них персональну інформацію. Часто застосовують методи соціотехніки, щоб обманом примусити своїх жертв інсталювати на їхні пристрої шкідливе програмне забезпечення, яке маскується під якусь звичайну програму.

Тож для протидії фішинговим атакам можна надати наступні рекомендації:

1. Дізнаватись про нові методи фішингу.
2. Не надсилати нікому свої облікові дані. У разі необхідності варто перевірти вміст повідомлення, відправника або організацію, яку вони представляють.
3. Не натискати на підозрілі кнопки та посилання. Як правило такі повідомлення містять посилання або вкладення, які завантажаться щойно користувач натисне на кнопку.
4. Регулярно перевіряти облікові записи.
5. Використовувати надійне рішення для захисту від фішингових атак.

Підсумовуючи, протидія фішинговим атакам в інформаційних системах є одним із критичних завдань, яке вимагає комплексного та адаптивного підходу, Оскільки через легкість виконання такі атаки є поширеними та постійно еволюціонують, це вимагає постійного оновлення стратегій від спеціалістів. До того ж заходи протидії, як правило, виходять за межі традиційних засобів забезпечення безпеки. Багатогранний характер фішингу використовує як технічні вразливості, так і людські схильності, що вимагає всебічного механізму захисту. Тобто недостатньо лише встановити захисне програмне забезпечення, а й необхідно регулярно проводити інструктаж зі співробітниками та сповіщати їх про нові види, способи атак та як протидіяти цим загрозам. В результаті подібної атаки організація може втратити не тільки конфіденційні дані, а й довіру клієнтів, що значно вплине на подальший розвиток даної компанії.

Перелік посилань:

1. Поняття фішингу URL: Режим доступу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/ (дата звернення: 13.10.2023).
2. Що таке фішинг? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing (дата звернення: 14.10.2023).
3. Фішинг: методи та приклади атак URL: https://gridinsoft.ua/phishing (дата звернення: 14.10.2023).

Гахов Сергій Олександрович
к.,військ. н., доцент кафедри ІКБ, ННІЗІ ДУІКТ, Київ, Україна
Ганченко Марія Іванівна
аспірнтка групи АІКБ-11, ННІЗІ ДУІКТ, Київ, Україна

МЕТОДИ КЛАСТЕРИЗАЦІЇ ДАНИХ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКУ

Визначається необхідність, актуальність, потенціал удосконалення та підвищення ефективності процесу моніторингу в IPS та IDS системах для виявлення аномалій мережевого трафіку. А також описані переваги, недоліки, можливості та перспективи дослідження, використання і вдосконалення описаного вище процесу за допомогою Штучного Інтелекту та алгоритмів кластеризації даних на основі Машинного Навчання для покращення систем моніторингу, контролю трафіку і підвищення захищеності мережі організації.

Одним із актуальних на сьогодні підходів у протидії аномаліям мережевого трафіку є інтеграція систем моніторингу з методами Штучного Інтелекту та підвищення їх ефективності з використанням алгоритмів Машинного Навчання (далі по тексту — МН), задля автоматизації, прискорення і покращення процесів виявлення, та реагування на аномалії в мережі, такі як: різка зміна об’єму трафіку, незвичайний набір даних, що передаються корпоративною мережею, підозріла поведінка мережевого пристрою і т.д. Серед методів пошуку та виявлення аномалій у наборах даних найбільш досліджуваними є алгоритми кластеризації.

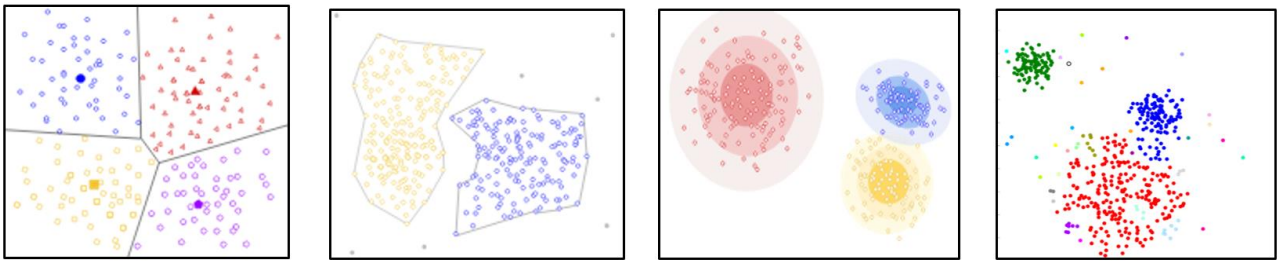
Такі алгоритми МН працюють на основі розподілу наборів даних на кластери (окреслена область даних) і за різними критеріями (визначений простір ознак) виявляють кластери, що є аномаліями (відхилення від прийнятої норми). Прикладом використання може бути вивчення інформації про зв’зки між пакетами даних, які передаються мережею (мають подібні розміри, одне джерело й спільне призначення) для створення кластерів і визначення пакету як аномального, якщо він не належатиме до кластера. Таким чином можуть бути виявлені DDoS атаки (пакети даних мають незвичайний розподіл розмірів), зловмисні програми (незвичайний розподіл джерел і призначення кожного пакета) та незвична поведінка користувачів (незвичайний розподіл часу пересилання пакетів даних).

Різноманітність критеріїв виявлення грунтується на способах виникнення аномалій, іншими словами залежить від типу атаки: [1]

1. Точкові/глобальні аномалії (атаки типу U2R або ж “*user-to-root”*, R2L або “temote-to-local”). Найбільш досліджувані, суть полягає у здатності системи класифікувати окремий екземпляр даних як аномальний по відношенню до решти даних.
2. Контекстуальні аномалії (атака типу “probe”). Залежать від структури набору даних, і визначаються аномалією у певному контексті, як щось малоймовірне.

3. Колективні аномалії (DoS, DDoS атаки). Відхилення від норми декількох кластерів даних по відношенню до переважаючої решти, при окремому розгляді можуть не видавати аномальних ознак.

Ефективність роботи алгоритму кластеризації даних напряму залежить від характеристик їх набору, який може використовуватись для навчання та в подальшому для автоматизації системи виявлення аномалій. Адже схожі об'єкти і структури даних поділяються на групи (екземпляр) таким чином, щоб дані всередині групи були максимально схожими, але дані різних кластерів (набір споріднених за критеріями екземплярів) максимально відрізнялися один від одного. Існує чотири різні методи (див. Рис 1.) створення кластерів: [2]



a) b) c) d)

Рис.1. – Методи кластеризації: a) на основі центроїда; b) на основі щільності; c) на основі розподілу; d) на основі зв’язків.

1. Кластеризація на основі центроїда (див. Рис.1.a.) – k-means (Centroid-based Clustering). [3] Алгоритм, що працює на основі відстані, де кожен об’єкт відноситься до кластера залежно від відстані до центрального об’єкта (центроїд). Основним завданням є ітераційна мінімізація відстані між об’єктом та центроїдом кластера. Для цього визначається кількість кластерів (k – визначається вручну), довільним чином обирається центроїд із групи даних, визначається відстань між центроїдом та точкою даних, обираються найближчі точки даних до кожного центроїда, що і формуватимуть кластер.

Перевагою алгоритму є його зручність для кластеризації великої кількості даних. Значним недоліками є необхідність попереднього визначення кількості кластерів вручну.

2. Кластеризація на основі щільності (див. Рис.1.b.) – DBSCAN (Density-based spatial clustering of applications with noise) [2]. Алгоритм підраховує та визначає відстань (радіус кола — ε-околиця екземпаляра) та кількість граничних об’єктів (мінімально необхідна кількість даних — min pts, що розташовані в ε-околиці клатера) для кожного кореневого об’єкта (ядро - центр екземпляра). Всі об’єкти в околицях ядра (основний екзкмпляр) належать до одного кластера, який може включати інші екземпляри та створювати послідовність із сусідніх екземплярів. Будь-який інший екземпляр, який не задовільняє вищеописаним вимогам щодо відстані та кількості граничних об’єктів вважається аномалією.

Перевагами алгоритму є те, що він: добре працює, коли всі кластери щільні і чітко розділені області; може знаходити кластери будь-якого розміру та форми. Недоліками є те, що алгоритм не працюватиме з кластерами різної щільності та

у випадку великорозмірних даних.

3. Кластеризація на основі розподілу (див. Рис.1.c.) – (Distribution-based Clustering). [4] Алгоритм працює на основі ймовірності нормального або гаусівського розподілу даних.

Перевагами алгоритму є: робота зі штучно створеними даними (синтетичними) та з кластерами різного розміру. Недоліками є: необхідність визначення параметрів, які контролюватимуть складність, аби уникнути створенню моделей розподілу даних; ймовірнісний підхід для розподілу одних даних, який може бути невірним для інших наборів даних.

4. Кластеризація на основі зв'язків (див. Рис.1.d.) – (Connectivity-based Clustering). [4] Робота алгоритму полягає у визначенні кластерів на основі близького розташування точок даних, оскільки близькі точки даних мають більше подібностей ніж віддалені. Алгоритм побудований на понятті ієрархії кластерів, які можуть перетинатись залежно від суб'єктивно обраного параметру відстані.

Перевагами алгоритму є: можливість врахувати якомога більшу кількість інформації про зв'язки між даними, а не лише їх індивідуальні характеристики, та більш ефективно їх розділити на кластери; різноманітність типів даних. Недоліками алгоритму є: неефективність для великих наборів даних; складність інтерпретації, через відсутність чіткості у розумінні того, яким чином здійснювався розподіл на кластери.

Відтак, основними перевагами методів кластеризації є можливість дослідження різних наборів даних та навчання систем на їх основі для виявлення аномалій мережевого трафіку. Недоліками ж та областями для подальших досліджень і вдосконалень є:

– складність чіткого визначення діапазонів екземплярів та меж кластера в цілому;

– недосконаліть виявлення всіх подібностей у наборах даних для правильного окреслення меж кластеру;

– недостатня автоматизація та необхідність людського втручання для визначення параметрів використовуваного методу.

Перелік посилань:

1. A Comprehensive Beginner's Guide to the Diverse Field of Anomaly Detection. [електронний ресурс] – Режим доступу: https://towardsdatascience.com/a-comprehensive-beginners-guide-to-the-diverse-field-of-anomaly-detection-8c818d153995 (дата звернення: 01.10.2023).

2. Based Spatial Clustering of Application with Noise. [електронний ресурс] – Режим доступу:https://medium.com/@tpreethi/dbscan-algorithm-density-based-spatial-clustering-of-application-with-noise-a826538dcb42 (дата звернення: 07.10.2023).

3. K-Means Clustering: A Quick Walkthrough. [електронний ресурс] – Режим доступу: https://medium.com/@aatish_kayyath/k-means-clustering-a-quick-walkthrough-c2e11268a386 (дата звернення: 05.10.2023).

4. Different Types of Clustering Algorithm. [електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/different-types-clustering-algorithm/ (дата звернення: 08.10.2023).

Глотов Володимир Олександрович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАХИСТУ WEB-РЕСУРСІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

Ця стаття розглядає технології захисту веб-ресурсів в інформаційній системі організації. Захист веб-ресурсів є важливим аспектом забезпечення конфіденційності, цілісності та доступності інформації в інформаційних системах підприємства. Стаття розглядає такі аспекти, як використання шифрування для захисту передачі даних через мережу, використання сучасних методів аутентифікації і авторизації, мережеві файрволи, виявлення та захист від зловмисних атак, таких як SQL-ін'єкція, крос-сайтовий скриптінг і DDoS-атаки.

Інформаційні системи сьогодні відіграють важливу роль у функціонуванні більшості організацій. Забезпечення безпеки веб-ресурсів стає надзвичайно актуальною задачею, оскільки порушення безпеки може призвести до серйозних наслідків для бізнесу та клієнтів. У цій доповіді ми розглянемо ключові аспекти технології захисту веб-ресурсів в інформаційній системі організації.

Першим і одним із найважливіших аспектів захисту веб-ресурсів є шифрування даних. Воно дозволяє захистити дані від несанкціонованого доступу під час їх передачі через мережу. Важливими технологіями в цьому контексті є протокол HTTPS для шифрування даних на рівні транспортного рівня та застосування шифрування даних на рівні додатку. Такий підхід забезпечує конфіденційність даних, які обмінюються між користувачами і серверами.

Для забезпечення безпеки веб-ресурсів важливо визначити, хто має доступ до різних функцій та ресурсів. Це досягається через механізми аутентифікації та авторизації. Аутентифікація підтверджує ідентичність користувача, тоді як авторизація визначає, які операції та ресурси доступні користувачу після вдалої аутентифікації. Для цього використовуються різні методи, включаючи багатофакторну аутентифікацію та ролевий доступ.

Однією з головних загроз для веб-ресурсів є різні види кібератак. Важливо мати захист від атак, таких як SQL-ін'єкція, крос-сайтовий скриптінг, DDoS-атаки та інші. Використання мережевих файрволів, систем виявлення і запобігання вторгнення (IDS/IPS), а також регулярне оновлення програмного забезпечення допомагають зменшити ризики вразливостей і атак.

Моніторинг та аудит безпеки важливі для вчасного виявлення і реагування на можливі порушення безпеки. Системи моніторингу дозволяють відслідковувати активність користувачів, реагувати на підозрілі події та вчасно виявляти вторгнення. Аудит дозволяє проводити ретельний аналіз подій та інцидентів для покращення стратегії безпеки.

Найбільша загроза для безпеки інформаційної системи - це люди. Недостатня обізнаність та необережність персоналу може призвести до порушень безпеки. Тому навчання персоналу в галузі кібербезпеки є важливим кроком. Це може включати в себе проведення навчань, обговорення правил безпеки та впровадження строгих політик безпеки.

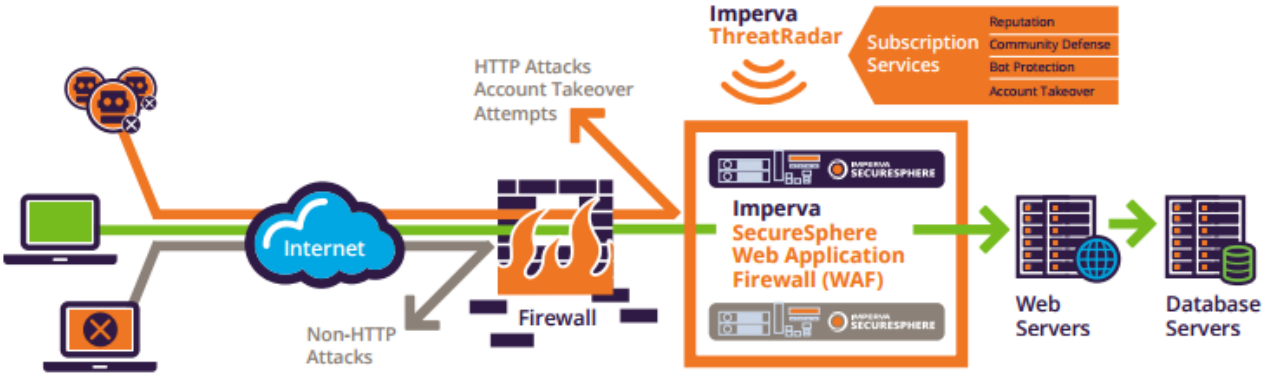


Рис. 1 Imperva SecureSphere Web Firewall Application – один з лідерів в області відображення атак на веб-додатки.

Забезпечення безпеки веб-ресурсів в інформаційній системі організації - це важлива задача, яка вимагає комплексного підходу. Шифрування даних, аутентифікація, авторизація, захист від атак, моніторинг т а аудит безпеки та навчання персоналу є важливими компонентами цього підходу. Правильно розроблена і реалізована стратегія захисту дозволяє не лише запобігти інцидентам безпеки, але і зберегти довіру клієнтів та партнерів, що є надзвичайно важливим для успішної діяльності організації. Необхідно також пам'ятати, що безпека - це постійний процес, і вона повинна постійно адаптуватися до нових загроз і вразливостей. Постійне вдосконалення і оновлення стратегії захисту є необхідним для збереження безпеки веб-ресурсів в інформаційній системі організації. Завдяки вивченню та впровадженню сучасних технологій захисту, організації можуть зменшити ризики порушення безпеки та зберегти надійність своїх веб-ресурсів. Захист інформації і безпека даних стають все більш важливими в умовах зростаючих загроз кібербезпеці, і організації повинні бути готові до їх вирішення.

Перелік посилань:

1. Imperva SecureSphere Web Firewall Application: https://www.imperva.com/products/web-application-firewall-waf/ (дата звернення: 24.10.2023)
2. Захист веб-додатків: чому це важливо? https://itbiz.ua/statti-ta-obzori/zaxist-veb-dodatkiv-chomu-ce-vazhlivo/ (дата звернення: 24.10.2023)

Говоруха Марк Миколайович
Студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ПОРАДИ ЩОДО ЕФЕКТИВНОГО ВИБОРУ ІНСТРУМЕНТУ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА АДМІНІСТРУВАННЯ (IGA) ДЛЯ ЗАХИСТУ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Управління ідентифікацією та адміністрування (IGA) - один з найважливіших елементів системи кібербезпеки. Вони включають управління обліковими записами, правами доступу та управління ризиками. Системи IGA допомагають організаціям оцінювати ризики, пов'язані з доступом до ресурсів, і

приймати рішення про надання прав доступу. Ефективні методи вибору інструменту IGA можуть значно покращити кібербезпеку корпоративних інформаційних систем.

1. Оцінюйте постачальників IGA не тільки за їх традиційними адміністративними можливостями, але й за їхню здатність задовольнити майбутні потреби, пов'язані з хмарними технологіями, штучним інтелектом та машинним навчанням.
2. Враховуйте простоту розгортання та експлуатації в будь-якій оцінці.
3. Розглядайте машинні ідентичності як окремі типи ідентичностей, якими потрібно керувати, як і людськими ідентичностями.
4. Перш ніж почати розглядати різні інструменти IGA, ви повинні спочатку подумати про те, для чого вам потрібен інструмент. Які найважливіші вимоги до безпеки вашої організації? Які функції вам потрібні? Після того, як ви добре зрозумієте свої потреби, ви можете почати звужувати свій вибір.

Перелік посилань:

1. Gartner Identity & Access Management Summit 2024, Grapevine, TX. *Gartner*. URL: https://www.gartner.com/en/conferences/na/identity-access-management-us/featured-topics/identity-governance-and-administration

Голобородько Владислав Сергійович
Студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ

Зростаюча складність загроз потребує інноваційних технічних рішень. Сучасний ландшафт кібербезпеки характеризується постійною еволюцією загроз, які стають все більш складними та витонченими. Ця тенденція справедлива для всіх сфер, від бізнесу та державних установ до особистих користувачів. Ось докладніше розглянемо, чому зростаюча складність загроз потребує інноваційних технічних рішень.

1. Розширені можливості атак

Кіберзлочинці постійно вдосконалюють свої методи атак. Вони використовують арсенал різноманітних інструментів, від шкідливих програм до соціально-інженерних загроз. Злочинці також активно використовують інтелектуальні технології, такі як штучний інтелект, для зламу інформаційних систем. Це робить процес виявлення та запобігання атак набагато складнішим завданням.

2. Специфіка атак на великі обсяги даних

Захист великих обсягів даних, які зберігаються в хмарних обчисленнях, стає все більш важливим завданням. Атаки, спрямовані на великі обсяги даних, можуть призвести до великих втрат інформації та порушення приватності користувачів. Інноваційні технічні рішення потрібні для забезпечення надійного захисту таких обсягів даних.

3. Загрози Інтернету речей (IoT)

Зростаюча кількість підключених пристроїв у мережі Інтернет речей

створює нові можливості для атак. Вразливості IoT-пристроїв можуть використовуватися для створення ботнетів та інших форм атак на масову аудиторію. Це вимагає інноваційних технічних рішень для захисту IoT-екосистеми.

4. Зростання віддаленої співпраці

Зростаюча кількість працівників працює з віддалених місць та використовує мобільні пристрої для доступу до корпоративних ресурсів. Ця віртуальна мобільність створює нові виклики для захисту інформації, оскільки потребує забезпечення безпеки в будь-якому місці та часі.

5. Глобальна природа загроз

Загрози кібербезпеки не мають кордонів. Хакери можуть діяти з будь-якої точки світу, а їх атаки можуть мати глобальний вплив. Це вимагає глобальної співпраці та інноваційних підходів до виявлення та реагування на атаки.

Усі ці фактори демонструють необхідність постійної інновації та розвитку технічних систем захисту інформації. Тільки таким чином можна забезпечити надійний захист в умовах постійно зростаючої складності кіберзагроз.

Перелік посилань:

7. ПРОБЛЕМИ ТА ЗАГРОЗИ БЕЗПЕЦІ IoT ПРИСТРОЇВ URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/231/205

8. The Top 10 IoT Security Threats and Vulnerabilities –Particle Blog. (б.д.). URL: Blog.https://blog.particle.io/the-top-10-iot-security-threats/

9. У Bluetooth знайшли масштабну вразливість. https://nv.ua/ukr/techno/it-industry/u-bluetooth-znajshli-masshtabnu-vrazlivist-2484381.html.

Головко Євген Васильович
студент групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

ОЦІНКА ЕФЕКТИВНОСТІ ЗАСОБІВ ТА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Захист інформаційних ресурсів є одним із пріоритетних завдань безпеки підприємств України, оскільки перехід до інформаційного суспільства змінив статус інформації. Наразі вона може бути як засобом забезпечення безпеки, так і загрозою та небезпекою. За умов постіндустріального етапу інформація перетворилась на стратегічний ресурс економічного і науково-технологічного прогресу. Відтак, захист інформації на підприємствах потребуєдостатнього теоретико-методологічного підґрунтя. Дослідження можливості застосування математичних методів для оцінювання захисту інформації на підприємстві є досить актуальним питанням за сучасних умов розвитку економіки.

На основі аналізу закордонних та вітчизняних праць визначено ключові чинники, які визначають рівень захисту інформації на підприємстві. Можна встановити функціональну залежність між рівнем захисту інформації та факторами впливу на нього у вигляді структурно-логічної схеми. Отже, було розроблено структурно-логічну схему захисту інформації на підприємстві.

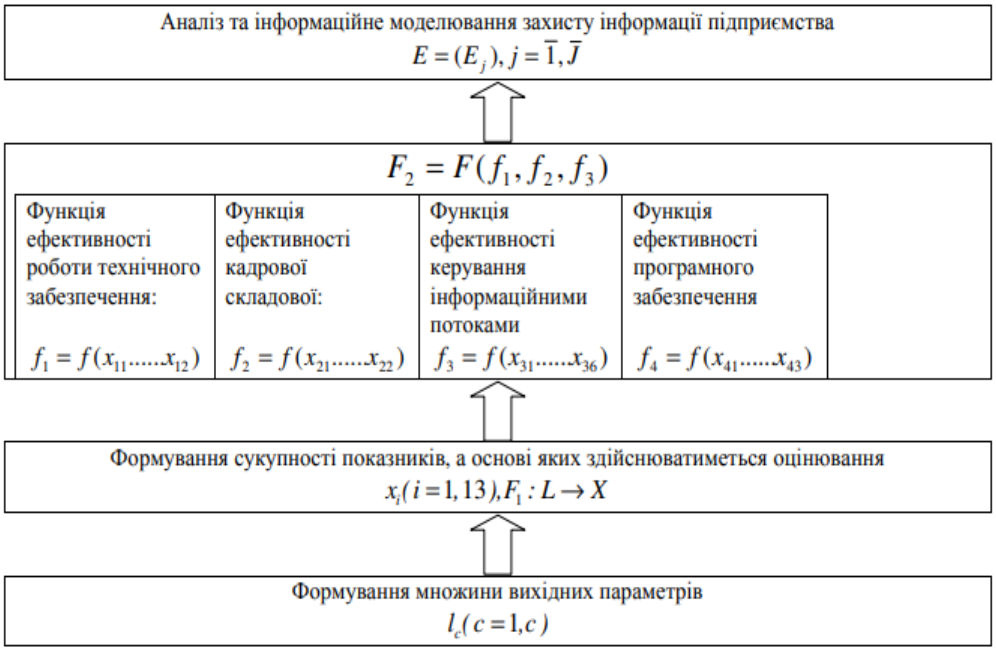


Рис.1. Структура схеми оцінювання рівня захисту інформації на підприємстві

Перелік посилань:

- МЕТОДИЧНИЙ ПІДХІД ДО ОЦІНЮВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВАХ URL: https://praci.vntu.edu.ua/index.php/praci/article/download/6/6/11 [с. 1, 2, 3] (дата звернення: 24.10.2023).

Голубчук Сергій Вікторович, БСДМ-62
Державний університет інформаційно-комунікаційних технологій
м. Київ

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК КОРПОРАТИВНОЇ ІНФРАСТРУКТУРИ НА БАЗІ РІШЕННЯ З ВІДКРИТИМ ВИХІДНИМ КОДОМ WAZUH

Розглянуто основні проблеми та зміст технології забезпечення захисту кінцевих точок корпоративної інформаційної системи за допомогою платформи Wazuh. Розглянуто архітектуру і можливості платформи Wazuh. Розроблено загальні рекомендації щодо управління захистом кінцевих точок корпоративної інформаційної системи.

Кінцеві точки — це фізичні або віртуальні пристрої, які під’єднані до корпоративної комп’ютерної мережі і обмінюються з нею даними. Це можуть бути комп’ютери, мобільні пристрої, сервери, віртуальні машини тощо.

З швидким розвитком комп’ютерних технологій, стрімко розвивається і кіберзлочинність. Згідно звіту FBI IC3 (IC3 - Internet Crime Complaint Center -

Центр скарг на Інтернеті злочини), за останні 5 років ФБР отримало 3.26 млн. скарг про скоєні кібератаки з сумарними збитками 27,6 мільярда доларів, і це статистика лише по Сполученим Штатам. Достатньо поширеним вектором для проведення кібератак є кінцеві точки корпоративних інформаційних систем. Їх захист має важливе значення для забезпечення безпеки корпоративної інфраструктури.

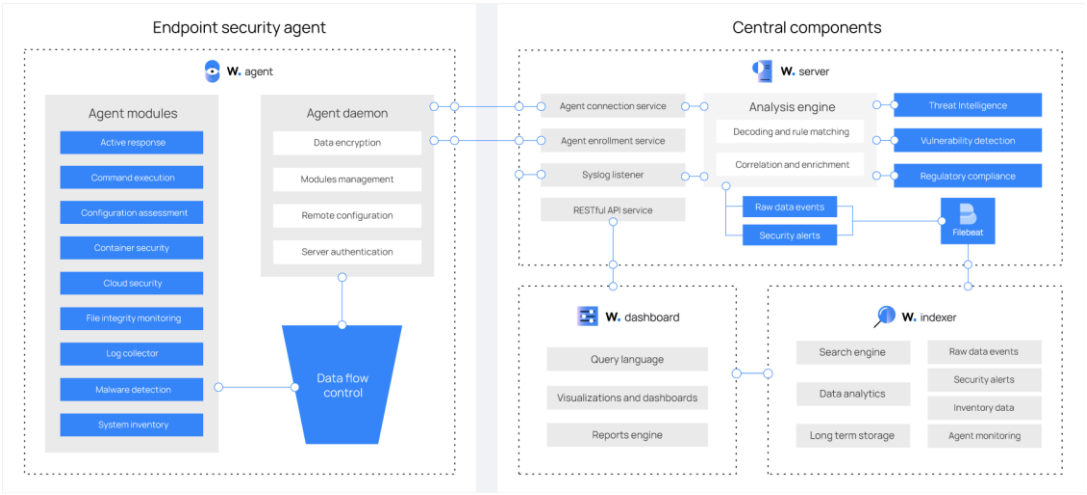
Однією з основних проблем безпеки кінцевих точок, є їх недостатня видимість. Без повної видимості всіх кінцевих точок, виявлення потенційних загроз і реагування на них може бути складним завданням. Ефективне керування загрозами вимагає виявлення і негайного усунення потенційних загроз безпеки та їх пристроїв. Інженери кібербезпеки можуть досягти цього, отримавши доступ до цих пристроїв. Для виявлення інцидентів і своєчасного реагування на них, на кінцевих точках повинні бути розгорнуті рішення безпеки, які налаштовані на збір даних журналу та сповіщень. Ці дані дозволять швидко розпізнавати й усувати будь-які потенційні загрози, забезпечуючи безпеку пристроїв і даних підприємства. Останнім часом в корпоративному сегменті набирає популярність концепція BYOD (Bring your own device), яка дозволяє співробітникам використовувати власні пристрої для вирішення корпоративних задач. Також, багато компаній практикують віддалений режим роботи з доступом до корпоративної інфраструктури. Все це сильно ускладнює забезпечення захисту корпоративних інформаційних систем, тому інженерам кібербезпеки або системним адміністраторам важливо мати в арсеналі інструмент (XDR/SIEM) для аналізу подій безпеки у реальному часі.

Wazuh — це безкоштовна платформа безпеки з відкритим вихідним кодом, яка являє собою сукупність XDR/SIEM системи націленої на захист кінцевих точок в локальних, візуалізованих, контейнерних та хмарних середовищах. XDR (розширене виявлення та реагування) збирає та автоматично співвідносить дані на кількох рівнях безпеки – кінцевої точки, сервера, хмарного робочого навантаження та мережі. Це дає змогу швидше виявляти загрози та покращувати час дослідження та реагування за допомогою аналізу безпеки. Ключовим елементом XDR є EDR (Endpoint Detection and Response). SIEM (Security information and event management) - технологія керування інформацією про безпеку та подіями, яка підтримує виявлення загроз, дотримання вимог і керування інцидентами безпеки за допомогою збору та аналізу (як майже в реальному часі, так і історичних) подій безпеки, а також широкого спектру інших джерел подій і контекстних даних. Основними можливостями є широкий спектр збору та керування подіями журналів, здатність аналізувати події журналів та інші дані з різних джерел, а також операційні можливості (такі як керування інцидентами, інформаційні панелі та звітність).

Wazuh має клієнт-серверну архітектуру і базується на агентах. Агент є модульним і мультиплатформним, тобто підтримує більшість операційних систем (MS Windows, GNU Linux, Unix, macOS). В доповнення до можливостей моніторингу на основі агентів, платформа Wazuh також може контролювати пристрої без агентів, наприклад: брандмауери, комутатори, маршрутизатори і

точки доступу, які здатні відправляти дані журналів через SSH, Syslog або за допомогою своїх API.

Серверна частина Wazuh складається з трьох компонентів: Wazuh індексатор, Wazuh сервер та панель керування Wazuh. Агенти передають дані безпеки кінцевих точок на Wazuh сервер (передача відбувається з використанням TLS шифрування). Ці дані попадають в аналітичну машину, в якій вони аналізуються/декодуються і передаються в Wazuh індексатор для індексації та зберігання. Потім вони із індексатора вони попадають у центральну панель Wazuh.



Мал. 1. Компоненти платформи Wazuh

На кінцевій точці, Wazuh може:

- виявляти прогалини у конфігурації;
- відстежувати активні процеси в системі;
- відстежувати цілісність файлової системи;
- виявляти шкідливе програмне забезпечення (в тому числі, на основі сигнатур);
- виявляти підозрілу активність;
- відстежувати несанкціоноване прослуховування портів;
- збирати log-файли (облікові журнали базових служб та сервісів на машині) та аналізувати їх.
- сканувати програмне забезпечення опираючись на бази загальновідомих вразливостей (CVE);
- проводити регулярні перевірки на відповідність вимогам PCI DSS, HIPAA, GDPR, NIST, CIS тощо;

Загальні рекомендації щодо управління захистом кінцевих точок корпоративної інформаційної системи

Для повноцінного захисту кінцевих точок і корпоративної інфраструктури повинен використовуватись комплексний підхід.

На кожній кінцевій точці має бути:

- встановлено антивірусний захист,
- налаштовано брандмауер;
- розподілені права доступу згідно нормативної документації пов’язаної з інформаційною та кібербезпекою. Кожен користувач має мати лише необхідні для виконання своїх службових обов’язків доступи;
- на мобільних кінцевих точках обов’язкове повнодискове шифрування;
- при роботі співробітників з чутливих даними, обов’язкова наявність на кінцевих точках системи запобігання витоку.
- віддалений доступ виключно використанням VPN;
- сегментація корпоративної мережі;
- обов’язкова аутентифікація всіх кінцевих точок в корпоративній мережі (наприклад 802.1x).

Перелік посилань:
1. Internet Crime Report [Електронний ресурс] / FBI AC3 - 2022 – Режим доступу: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
2. Wazuh documentation [Електронний ресурс] – Режим доступу: https://documentation.wazuh.com/current/index.html

Гончарук Ілля Дмитрович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

КОНЦЕПЦІЯ BRING YOUR OWN DEVICE З ТОЧКИ ЗОРУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНИХ ПІДПРИЄМСТВ

Все більше працівників різних підприємств використовують свої мобільні пристрої для робочих потреб. Це пов'язано з тим, що в наш час обчислювальні потужності таких девайсів майже зрівнялися з потужностями стаціонарних робочих станцій. Поширення сфери хмарних обчислень також накладає свій відбиток - завдяки сучасним потужностям працівник може запустити робочий додаток віддалено на своєму пристрої і виконати роботу швидше та якісніше. Така політика носить назву BYOD. В даній роботі будуть розглянуті основні переваги та виклики, які дана концепція несе для компаній.

BYOD як поширена корпоративна політика повністю сформувалася і отримала розповсюдження в 2011 році. Згідно з опитуваннями Cisco та Ovum, BYOD є глобальним явищем серед великих (1000 і більше) і середніх підприємств Америки, Азії та Європи [1, с.2].

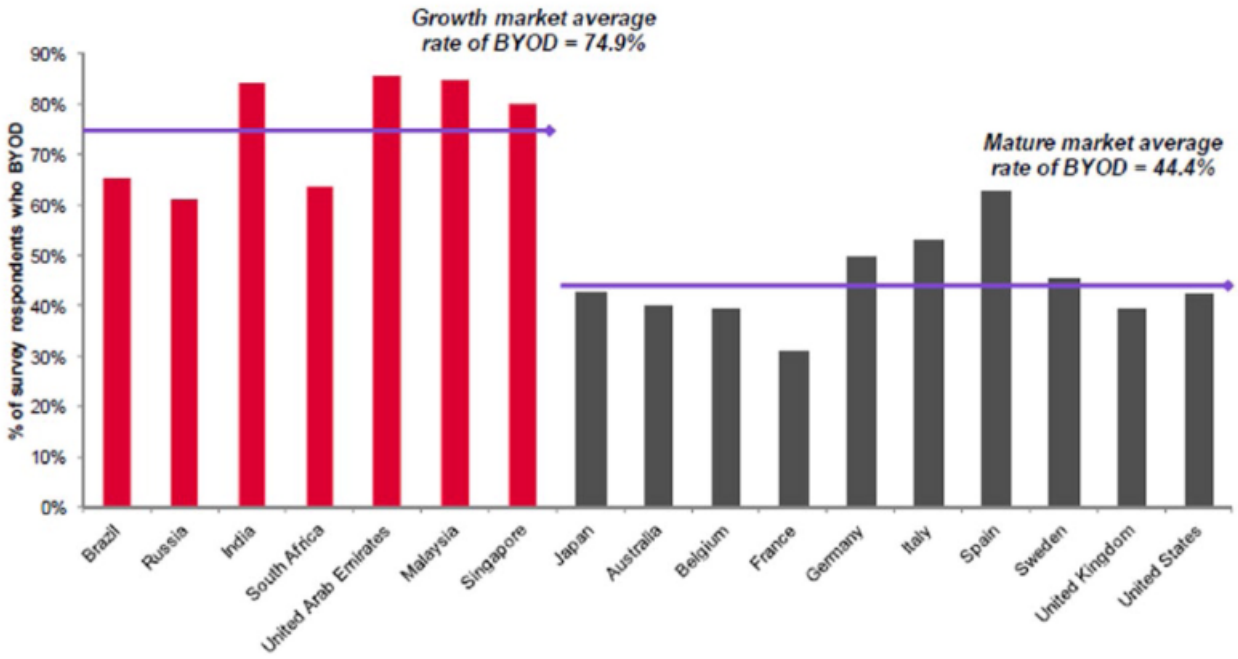


Рис.1 - Поширення BYOD в країнах, що розвиваються (червоні) та розвинених країнах

Як видно з Рис.1, майже 45% працівників розвинених країн використовували свої пристрої на роботі на момент 2012 року. Відсоток розповсюдження BYOD в країнах, що розвиваються, значно вищий — 75%. Це пов'язано з тим, що не всі підприємства цих регіонів можуть надати співробітникам якісні корпоративні пристрої, тому їм доводиться використовувати свої. Відсоток використання BYOD на момент 2018 року сягав 70%, тому можна стверджувати, що дана політика є важливою частиною сучасної офісної культури.

Чому бізнес-структури зацікавлені в використанні концепції BYOD? Ще в 2013-у році BT Group опублікувало опитування, в якому 42% опитуваних зазначило, що в результаті впровадження BYOD їх робоча ефективність підвищилась [2]. Це є наслідком таких причин:

- працівникам простіше працювати з своїми власними пристроями;
- мінімізуються витрати на придбання нового обладнання для бізнесу;
- відкривається можливість для співробітників працювати дистанційно.

З такими перевагами, політика BYOD привносить у бізнес і серйозні виклики до інформаційної безпеки. Як відомо зі звіту Verizon, людський фактор продовжує бути найсуттєвішою причиною витоків даних [3, с.8]. За 2022 рік 82% порушень були пов'язані з людським фактором. Незалежно від того, чи це використання викрадених облікових даних, фішинг, зловживання або просто помилка, люди продовжують відігравати дуже велику роль в інцидентах і порушеннях. Логічно випливає, що внесення концепції BYOD підвищить ризики витоків даних, адже підприємству буде складніше прослідковувати використання робочих пристроїв. Окрім того, має місце і психологічна сторона

— ставлення працівника до корпоративного і власного майна є, безумовно, різним. Отже, ризик того що співробітник, наприклад, натисне на фішингове посилання в електронному листі зростає. Це нанесе шкоду не тільки йому самому, а й може спричинити витік даних в його компанії.

Основні загрози мобільних девайсів перекликаються з поширеними загрозами стаціонарних комп'ютерів. До таких відносяться [4]:

1. Витік даних - дані можуть бути втрачені або піддані впливу, коли пристрої втрачаються або викрадаються, або якщо на особистому пристрої встановлено шкідливе програмне забезпечення. Хоча хмарні технології пом'якшили більшість випадків втрати даних через пошкодження пристроїв, бар'єри безпеки та резервне копіювання мають вирішальне значення для інформаційної безпеки бізнесу.
2. Шкідливі програми - у деяких випадках шкідливі програми можуть отримати контроль над мобільним пристроєм користувача. Це може призвести до стеження, неочікуваних витрат на передачу даних або дивні дзвінки, а також до втрати особистої або робочої інформації. Тому працівники потребують додаткового навчання щодо принципів безпечної роботи з додатками. Таке навчання має включати важливість завантаження контенту лише з магазинів додатків. У багатьох випадках шкідливі додатки завантажуються через «піратські» веб-сайти.
3. Проблеми управління пристроями - з будь-яким мобільним пристроєм, що належить співробітнику або компанії, існують ризики, пов'язані з втратою контролю. Коли кінцевий пристрій виходить за межі будівлі компанії, може бути важко проконтролювати, чи не використовується він у сумнівних безкоштовних бездротових з'єднаннях і чи не буде він загублений або викрадений.
4. Поєднання особистого та ділового використання - з BYOD поєднання ділового та особистого використання неминуче. Роботодавець не може контролювати, чи вирішать його співробітники робити покупки в Інтернеті на сумнівних веб-сайтах і чи не загублять вони свій пристрій. Хоча компанія і може провести інтенсивне навчання щодо найкращих практик безпеки, вона не може гарантувати, що її співробітники не позичатимуть свої пристрої друзям або не використовуватимуть загальнодоступні бездротові з'єднання для збереження даних.
5. Не слід забувати і про DoS та DDoS-атаки, вони також залишаються загрозою і для бізнесу з BYOD-політикою.

Підсумовуючи, концепція BYOD дозволяє працівникам використовувати свої мобільні пристрої для роботи в компанії. Це несе як вагомі переваги, так і суттєві виклики до забезпечення інформаційної безпеки на підприємстві. Підвищується ризик витоку конфіденційної інформації, а керівники бізнесу можуть зіткнутися зі складнощами в управлінні роботи працівників. Щоб пом'якшити чи усунути ризики безпеки в компанії, необхідно:

– здійснювати навчання працівників, що пов'язане з політикою BYOD;

– для полегшення керування використовувати засоби MDM (Mobile device management);

– вибрати модель BYOD, що буде імплементована в бізнес (CYOD, COPE). Дані моделі регулюють наскільки підприємство може контролювати пристрій співробітника;

– на основі моделі розробити та впровадити політику BYOD (пристрої, що можуть використовувати співробітники; додатки можна встановлювати на персональні пристрої; дані, що можуть бути доступні на персональних пристроях; покарання, передбачені за порушення правил).

При впровадженні і дотриманні перелічених заходів безпеки, підприємство мінімізує ризики, пов'язані з концепцією BYOD і отримає від неї суттєві переваги. Це грає суттєву роль для життєдіяльності компанії, адже, як видно з досліджень, до 70% працівників так чи інакше використовує свої власні пристрої на роботі.

Перелік посилань:

1. Morufu Olalere A Review of Bring Your Own Device on Security Issues / Mohd Taufik Abdullah, Ramlan Mahmod, Azizol Abdullah. - Federal University of Technology, Minna. – Nigeria, 2015. – 11 с.

2. BYOD Gives Competitive Advantage, Say IT Managers URL: https://www.prnewswire.com/news-releases/byod-gives-competitive-advantage-say-it-managers-151687995.html (дата звернення 10.10.2023).

3. Data Breach Investigations Report / Verizon. – 2022. – 108 с.

4. The 8 Top BYOD Security Risks URL:https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate (дата звернення 24.10.2023).

Городенцев Андрій Андрійович
Студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

АТАКИ ПРОГРАМ ВИМАГАЧІВ: СУЧАСНИЙ ВИКЛИК КІБЕРБЕЗПЕЦІ

У середовищі кібербезпеки, що швидко розвивається, однією з найактуальніших і найсучасніших проблем є зростання кількості атак з використанням програм-вимагачів. Атаки з використанням програм-вимагачів стають все більш витонченими та масштабними, завдаючи значної фінансової, операційної та репутаційної шкоди приватним особам, компаніям і навіть об'єктам критичної інфраструктури. У цьому документі детально розглядається сучасний стан атак з використанням програм-вимагачів, їхній вплив та стратегії, які застосовують кіберзлочинці та експерти з кібербезпеки для протидії цій поширеній загрозі.

Еволюція атак з використанням програм-здирників

Програми-здирники - це тип шкідливого програмного забезпечення, яке шифрує дані жертви, роблячи їх недоступними, і вимагає викуп, зазвичай у криптовалюті, в обмін на ключ для розшифрування. Хоча атаки з використанням програм-вимагачів з'явилися ще наприкінці 1980-х років, за останні роки вони значно еволюціонували. Сучасні атаки з використанням програм-вимагачів характеризуються застосуванням сучасних методів шифрування, багатовекторних методів атаки та більшою увагою до високопоставлених цілей. Крім того, моделі "програми-вимагачі як послуга" (RaaS) спростили розгортання

атак навіть для менш технічно підготовлених кіберзлочинців, що сприяло їхньому поширенню.

Вплив атак з використанням програм-здирників

Атаки з використанням програм-вимагачів мають далекосяжні наслідки, які по-різному впливають на організації та окремих осіб:

- Фінансові втрати: Виплати викупу, часто в криптовалюті, зростають, і деякі жертви платять значні суми, щоб відновити свої дані. Фінансові наслідки також включають витрати, пов'язані з відновленням, розслідуванням і потенційною юридичною відповідальністю.
- Операційні збої: Атаки вірусів-здирників порушують бізнес-операції, що призводить до простоїв, зниження продуктивності та шкоди репутації компанії. Це може мати каскадний вплив на ланцюжки поставок і відносини з клієнтами.
- Втрата даних: у деяких випадках жертви не можуть відновити свої дані навіть після сплати викупу, що призводить до безповоротної втрати даних.
- Пошкодження репутації: Організації, які стають жертвами атак вірусів-здирників, можуть зазнати репутаційних втрат, підриваючи довіру серед клієнтів, партнерів та зацікавлених сторін.
- Загроза національній безпеці: Постачальники критично важливої інфраструктури також стають мішенню, що викликає занепокоєння з точки зору національної безпеки. Атаки на лікарні, електромережі та інші об'єкти життєзабезпечення можуть мати небезпечні для життя наслідки.

Стратегії кібербезпеки та реагування

Вирішення сучасної проблеми атак з використанням програм-вимагачів вимагає багатогранного підходу:

- Превентивні заходи: Організаціям необхідно інвестувати в надійні заходи кібербезпеки, включаючи регулярне резервне копіювання, сегментацію мережі та навчання співробітників розпізнаванню спроб фішингу та підозрілих дій.
- Правоохоронна діяльність та регулювання: Уряди відіграють більш активну роль у протидії атакам з використанням програм-вимагачів. Правоохоронні органи переслідують кіберзлочинців, а також розробляються нормативні акти, які встановлюють стандарти кібербезпеки для критичної інфраструктури.
- Співпраця: Обмін інформацією та співпраця між державним і приватним секторами є надзвичайно важливими. Такі ініціативи, як проєкт No More Ransom, що пропонує безкоштовні інструменти для розшифрування, демонструють силу колективних зусиль.
- Покращене реагування на інциденти: Організації повинні мати чітко розроблені плани реагування на інциденти, щоб мінімізувати наслідки атаки та швидко відновити роботу.

- Боротьба з програмами-здирниками: Зусилля з відстеження криптовалютних платежів, здійснених операторам програм-вимагачів, набирають обертів, що потенційно ускладнює для злочинців виконання їхніх вимог.
- Поінформованість про кібербезпеку: Підвищення обізнаності громадськості про ризики програм-вимагачів та популяризація відповідальної поведінки в Інтернеті може допомогти окремим особам та організаціям не стати жертвами атак.

Атаки з використанням програм-вимагачів стали сучасною проблемою кібербезпеки, що викликає велике занепокоєння і має глибокі наслідки для окремих осіб, бізнесу та національної безпеки. Тактика кіберзлочинців, що еволюціонує, фінансові стимули та потенційно руйнівні наслідки цих атак підкреслюють нагальність боротьби з цією загрозою. Хоча універсального рішення не існує, поєднання превентивних заходів, співпраці, судових позовів та покращення реагування на інциденти може допомогти пом'якшити наслідки атак зловмисників-здирників і з часом зменшити їх кількість. Боротьба з програмами-вимагачами - це безперервна боротьба, яка вимагає постійної пильності та адаптації до нових загроз у світі кібербезпеки, що постійно змінюється.

Перелік посилань:
1. Ransomware isn’t going away – the problem is only getting worse URL: https://www.bleepingcomputer.com/news/security/ransomware-isnt-going-away-the-problem-is-only-getting-worse/
(дата звернення 25.10.2023)
2. Kaspersky Lab Ransomware Decryptors URL: https://noransom.kaspersky.com/
(дата звернення 12.10.2023)
3. Ransomware Q&A URL: https://www.nomoreransom.org/en/ransomware-qa.html
(дата звернення 16.10.2023)
4. All about ransomware attacks URL: https://www.malwarebytes.com/ransomware
(дата звернення 20.10.2023)

Горун Олена Юріївна
Головний науковий співробітник
Українського науково-дослідного інституту
спеціальної техніки та судових експертиз
Служби безпеки України, Київ, Україна

ЩОДО НЕОБХІДНОСТІ ПОСИЛЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

Кібербезпека є важливою складовою національної безпеки України. Важливим завданням держави залишається посилення стану кібербезпеки в умовах триваючої кібервійни з державою-агресором. Виклики та загрози, які формуються в умовах кібервійни ставлять перед державою та її відповідальними суб’єктами завдання щодо удосконалення національної системи кібербезпеки, приведення її у відповідність до стандартів НАТО та ЄС. Важливим напрямком посилення кібербезпеки є розробка та запровадження механізмів кіберстримування збройної агресії та надання

відсічі агресору у кіберпросторі.

За оцінками світових експертів у сфері кібербезпеки, у переважній більшості країн спостерігається стійка тенденція до значного збільшення кількості та розширення спектру кібератак з метою порушення конфіденційності, цілісності і доступності державних інформаційних ресурсів, зокрема тих, що циркулюють на об'єктах критичної інформаційної інфраструктури. Основними цілями кібератак стають об'єкти стратегічної інфраструктури країн (ядерна, транспортна, хімічна чи будь-яка інша промисловість, системи життєзабезпечення великих мегаполісів, фінансова, продовольча, енергетична національні системи, транспортні мережі, діяльність уряду, правоохоронних органів тощо). Посягання здійснюються через інформаційно-телекомунікаційні системи, особливо автоматизовані системи управління, які необхідні для повсякденного життя людей, функціонування структур економіки, органів державної влади.

Війна рф проти Україні стала каталізатором глобального розвитку кіберзахисту та необхідності посилення кібербезпеки у світі, оскільки кібервійна ведеться як на полі бою, так і в кіберпросторі. Військова збройна агресія рф проти України та цифрова війна у кібердомені вносять свої корективи у світову модель побудови міжнародної безпеки. На цьому фоні дедалі більше держав світу переймаються питаннями посилення стану забезпечення кібербезпеки, що зумовлює уточнення задекларованих стратегічних завдань у цій сфері.

Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури [1].

За таких умов важливими завданнями нашої держави в умовах воєнного стану залишаються: створення та оптимізація ефективної національної системи кібербезпеки, з урахуванням тенденцій динаміки зміни безпекового середовища та імплементації кращих практик у сфері кібербезпеки провідних країн світу; набуття суб'єктами забезпечення кібербезпеки необхідних спроможностей для виконання оперативних завдань у кібердомені за призначенням; створення передумов для опанування сучасних форм та способів підготовки та проведення заходів забезпечення кібербезпеки; нарощування потужностей щодо підготовки та ведення кібербезпеки (у т.ч. кіберзахисту, кібероборони) відповідно до зростання рівня кіберзагроз; вчасне реагування на поточні загрози кібербезпеки шляхом запобігання, завчасного виявлення, випереджувального реагування на них, усунення (мінімізації, ліквідації наслідків) їх впливу; створення ефективних систем управління для забезпечення кібербезпеки; налагодження ефективної співпраці у межах повноважень із суб'єктами забезпечення національної безпеки держави, а також з НАТО, ЄС, державами-партнерами в частині спільного

виконання завдань кібербезпеки.

Тобто в сучасних умовах актуальність проблематики посилення стану забезпечення кібербезпеки не викликає жодних сумнівів. Кібербезпека являє собою стратегічну комплексну проблему будь-якої держави, яка передусім стосується економіки країни, особливо електронної промисловості, сектору безпеки і оборони, питань розвитку інфраструктури електронних комунікацій, технологій кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури, визначення заходів боротьби з кіберзлочинністю та кібертероризмом.

Актуальним питанням є запровадження заходів з метою розробки та запровадження механізмів кіберстримування збройної агресії та надання відсічі агресору у кіберпросторі. За таких умов посилення кібербезпеки передбачає, у першу чергу, оптимізацію діяльності суб`єктів забезпечення кібербезпеки, посилення їхніх спроможностей у рамках функціональності, удосконалення систем захисту об`єктів критичної інфраструктури від кібератак та інших посягань.

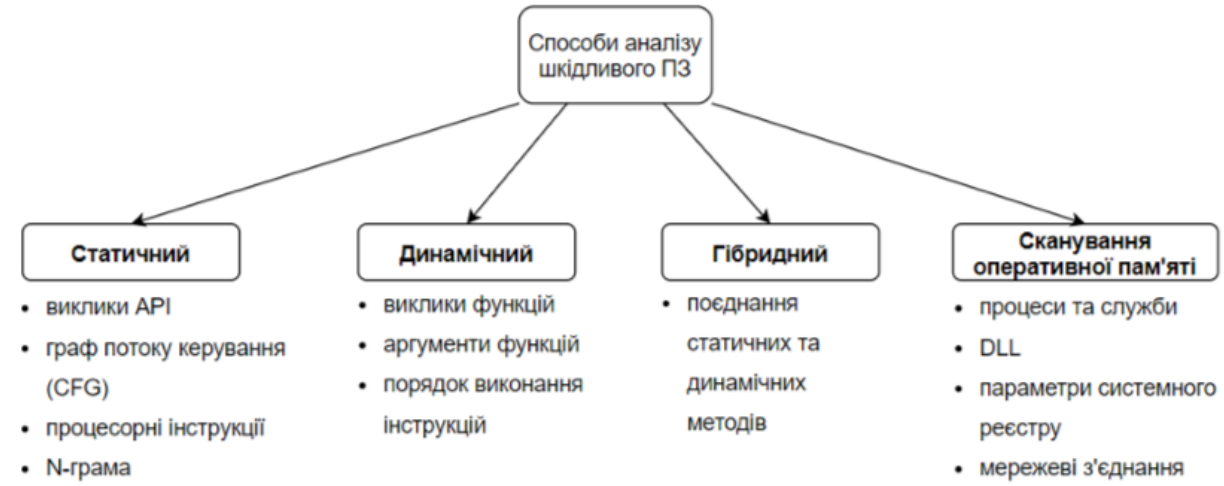
Перелік посилань:

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

Горобець Едуард Володимирович,
Студент групи УБД-32, ННІЗІ ДУІКТ

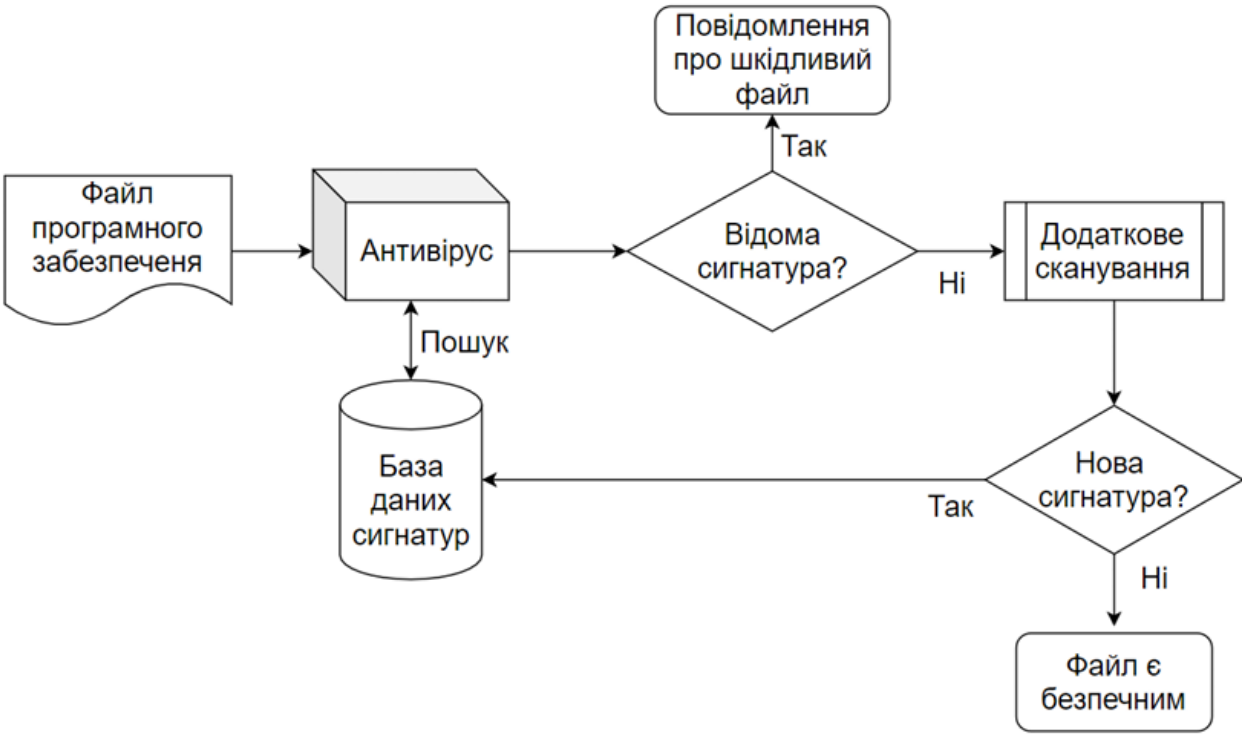
АНАЛІЗ ТА ОЦІНКА ЕФЕКТИВНОСТІ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У МЕРЕЖІ ПІДПРИЄМСТВА АТ«КРЕДІ АГРИКОЛЬ БАНК»

Сьогодні зі зростанням впливу та ролі комп'ютерів у сферах, що пов'язані з наукою, економікою, військовими справами, культурним життям соціуму та звичайного побуту, загроза кіберпорушень з наступним отриманням збитку різного розміру через надходження зловмисного програмного забезпечення (ПЗ) дедалі росте.



пристроїв.

Не кажучи про те, що цей збиток може бути руйнівним для, наприклад, цілого підприємства. Кіберпорушники навчилися не тільки перехоплювати дані, красти майно інтелектуальної власності, блокувати доступ до важливої пам'яті комп'ютера, або ж до окремих її частин, ставати на заваді нормального фукнціонування комп’ютера, або перетворювати його на недієздатне залізо, але і красти обчислювальні потужності, використовуючи їх для своїх цілей.



Шкідливе ПЗ утворюється з зростаючою швидкістю та складністю. Їх все важче детектувати. Зростає ймовірність помилитися, при пошуку шкідливого ПЗ, видалити корисний "чистий" файл, нашкодити самому собі. Деякі спеціалісти пропонують користуватись ліцензованим ПЗ для виявлення вірусного ПЗ, проте варто пам'ятати, що і вони не універсальні, адже ґрунтуються на базах сигнатур, які додаються з часом і не можуть бути довільними, оскільки між появою вірусу з новою сігнатурою та додаванням її в

базу даних, повинен пройти час, за який спеціалісти досліджують це сімейство вірусів, іноді навіть помилково приймають рішення про невіднесення його сигнатури. Все це накладає свої складності на проблему пошуку загроз. Ще одним ускладнюючим фактором стає здатність вірусів до зміни власного коду в процесі виконання, і не тільки. Проте, відомо, що портативні виконувані файли є найбільш поширеним джерелом загроз вірусного зараження. Люди часто завантажують ПЗ з ненадійних сайтів, або стають жертвами обману. Після чого вже не можуть згадати, коли саме вірус міг потрапити на комп'ютер. Тому рекомендується завжди перевіряти, що саме було завантажено. В процесі виконання роботи були розглянуті основні типи вірусів та методи їх детектування, принципи роботи аналізаторів та класифікаторів, це дозволило обрати найбільш ефективні інструменти аналізу та організувати роботу комплексу з метою виявлення шкідливого ПЗ. Актуальність роботи зумовлена стрімкою зміною подій у світі та необхідністю підприємств адаптуватись та розвиватись в цих умовах. Правильна оцінка ризиків може допомогти підприємству прийняти вчасне та якісне управлінське рішення та мінімізувати або нейтралізувати можливі втрати компанії.

Мета вбезпечити конфіденційну інформацію клієнтів та прорахувати всі можливі варіанти витіку інформації, та знаходитись в абсолютній готовності до критичної ситуації, та в підготовці компанії до кризових явищ, до ризиків. Підготовлена нормативна та практична база може пришвидшити реалізацію плану з усунення недоліків системи та скоротити термін його впровадження.

В роботі аведені загальні відомості про АТ «КРЕДІ АГРИКОЛЬ», основні етапи історії розвитку компанії, його цілі та обмеження. Зокрема, можна зробити висновок про клієнт орієнтованість та соціальну відповідальність компанії: основними компонентами місії банку та банківської групи є допомога у вирішенні екологічних та соціальних проблем.

Проаналізована організаційна структура та структура власності. За результатами аналізу, виявлено, що підприємство має лінійну організаційну структуру, що надає йому певну кількість переваг та розгалужену функціональність окремих управлінь компанії.

Структура безпеки компанії дає впевненість у її майбутньому та системній стійкості.

Індивідуальним завданням була оцінка ефективності виявлення шкідливого програмного забезпечення. Було зібрано та систематизовано теоретико-методологічні відомості про оцінку та шкідливе програмне забезпечення. На основі отриманих даних, проведено оцінку ризиків.

Перелік посилань:

1. Jinrong Bai, Junfeng Wang, Guozhong Zou. A Malware Detection Scheme Based on Mining Format Information / Jinrong Bai – The Scientific World Journal. 2014, Vol. 2014.

2. Eureka: A Framework for Enabling Static Malware Analysis, Sharif M. [et al.]. Recent Advances in Intrusion Detection, Lecture Notes in Computer Science., 2008, Vol. 5283, P. 481-500.

3. Microsoft Corporation, PE Format specification. [Електронний ресурс] Режим доступу: https://msdn.microsoft.com/library/windows/desktop/ms680547(v=vs.85).aspx ?id=19509 - 13.12.2020 - Загл. с экрана.

4. Касперски К. Путь воина – внедрение в pe/coff-файлы, 2004, [Електронний ресурс] Режим доступу: http://samag.ru/archive/article/297 13.12.2020 - Загл. с экрана.

5. Microsoft Corporation. What is a DLL. 2007, [Електронний ресурс] Режим доступу: https://support.microsoft.com/kb/815065/EN-US - 13.12.2020 - Загл. с экрана.
6. Manjunath. Malware images: Visualization and automatic classification, Nataraj L. [et al.], In Proceedings of the 8th International Symposium on Visualization for Cyber Security, Pp. 41-47, ACM, 2011.
7. Novel Feature Extraction, Selection and Fusion for Effective Malware Family lassification, Ahmadi M. [et al.], In Proceedings of the 6 ACM Conference on Data and Application Security and Privacy, Pp. 183-194, ACM, 2016.
8. File Signatures [Електронний ресурс] Режим доступу: https://filesignatures.net - 13.12.2020 - Загл. с экрана.
9. Алексей Пустыгин. Построение универсального представления графа потока управления для статического анализа исходного кода - Томск: Издательство ТУСУР, 2012. - 142 с. – С. 61-63.
10. Основи кібербезпеки в банківській системі URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity?SilentAuth=1 та https://finclub.net/ua/priama-mova/yak-bankam-vstoiaty-u-vypadku-kiberataky.html
11. Систематика банкінгу в Україні URL: https://credit-agricole.ua/ru/o-banke/pres-centr/novini/kredi-agrikol-pidklyuchivsya-do-sistemi-bankid-1259
12. Минфин. Банки. URL: http://www minfin.com.ua.
13. Народний рейтинг банків України. URL: http://finance.ua.
14. Герасимович А.М. Аналіз банківської діяльності: підручник. К.: КНЕУ, 2012. 580-599 с.
15. Рейтинг жизнеспособности украинских банков. URL: http://forbes.net.ua/business/1421401-rejting- zhiznesposobnosti-ukrainskih-bankov-2016.

Даниленко Іван Іванович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

ІНТЕРНЕТ РЕЧЕЙ (IOT) І БЕЗПЕКА ПРИСТРОЇВ

У світі сучасних технологій пристрої IoT стають все більш поширеними та необхідними в нашому повсякденному житті. Однак ця швидка експансія IoT вносить нові виклики у галузі кібербезпеки. Зростаюча кількість підключених до Інтернету пристроїв створює додаткові точки входу для потенційних атак і порушень приватності. Теза вказує на необхідність посилення заходів безпеки для захисту пристроїв IoT та важливість підвищення рівня свідомості користувачів щодо безпеки цих пристроїв.

Збільшення поширення та використання пристроїв Інтернету речей (IoT) створює серйозні виклики для кібербезпеки, вимагаючи посилення заходів безпеки та збільшеної свідомості користувачів

Перелік посилань:
1. CompTIA Security+ All-in-One Exam Guide, Sixth Edition (Exam SY0-601).
2. What Is IoT Cybersecurity?: https://www.comptia.org/content/articles/what-is-iot-cybersecurity (дата звернення: 25.10.2023).
3. IoT Cyber Security: Trends, Challenges and Solutions: https://www.knowledgehut.com/blog/security/Iot-cyber-security (дата звернення: 25.10.2023).

Двірний Дмитро Юрійович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

ВИКЛИКИ ТА РИЗИКИ КІБЕРБЕЗПЕКИ

Цей текст розглядає актуальні загрози у сфері кібербезпеки, зокрема розвідувальну та підривну діяльність у кіберпросторі проти України. Обговорюються висока технологічна залежність України від іноземних виробників ІКТ, відсутність національних стандартів безпеки та недоліки в кіберзахисті державних інформаційних ресурсів. Текст також надає інформацію про вплив цих чинників на безпеку та розвиток країни та закликає до усвідомлення важливості вдосконалення заходів з кібербезпеки для

захисту національних інтересів в цифровому віці.

Сучасне Українське суспільство стикається з низкою кібербезпекових викликів, які мають потенційно серйозні наслідки для країни. Однією з найактуальніших загроз є розвідувально-підривна діяльність у кіберпросторі, спрямована проти України.

Ця діяльність в основному виконується іноземними спецслужбами, особливо Російською Федерацією, і включає в себе кібершпигунство, спрямоване на здобуття конфіденційної інформації, а також підривні акції, спрямовані на дезорганізацію нормального функціонування важливих об'єктів інфраструктури, таких як системи управління державою, елементи життєзабезпечення, електроенергетика, транспорт, ядерна та хімічна промисловість, а також банківський сектор.

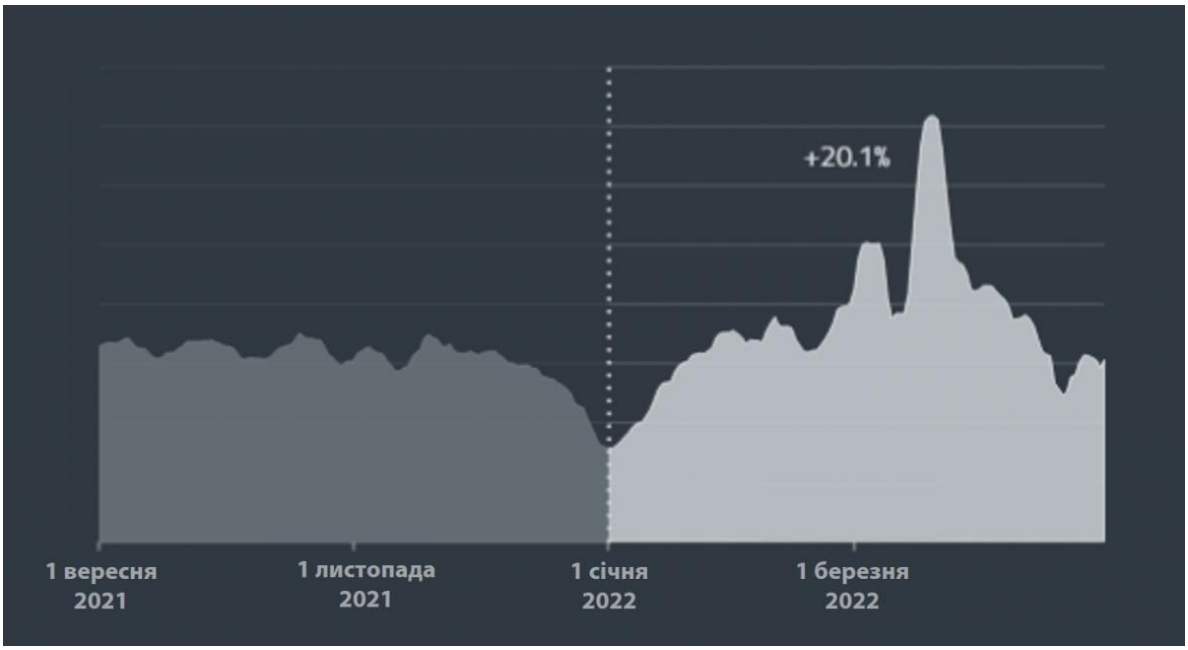


Рис.1. Динаміка росту кіберзагроз в Україні

Паралельно з цим, висока технологічна залежність України від іноземних виробників інформаційно-комунікаційних технологій та програмного забезпечення створює додаткові ризики для національної кібербезпеки. Відсутність сучасних національних стандартів щодо вимог з безпеки у ланцюжку поставок такого обладнання та розробки програмного забезпечення робить країну більш вразливою перед кіберзагрозами.

Недостатній кіберзахист інформаційних систем органів влади та підприємств, які опрацьовують значну кількість конфіденційної інформації, призводить до порушень прав користувачів цифрових послуг та може завдати шкоди процесам цифрової трансформації в країні. В цілому, кібербезпека стає однією з найважливіших завдань, з якими Україна повинна впоратися для забезпечення стійкості та захисту національних інтересів в кіберпросторі.

Важливо враховувати, що в Україні існує велика залежність в галузі

інформаційно-комунікаційних технологій та програмного забезпечення від іноземних виробників, що створює додаткові загрози для національної кібербезпеки.

Рис.2. Динаміка росту кіберзагроз в Україні в категорії «Шкідливий програмний код»

Потреба у сучасних національних стандартах для забезпечення безпеки в ланцюжку поставок інформаційно-комунікаційного обладнання та розробки програмного забезпечення стає надзвичайно важливою, оскільки вона зменшить ризики, пов'язані з кіберзагрозами.

Недостатній рівень кіберзахисту інформаційних систем органів влади та підприємств, що опрацьовують значну кількість конфіденційної інформації, може призвести до порушень прав користувачів цифрових послуг та суттєво ускладнити процеси цифрової трансформації в країні. Загалом, забезпечення кібербезпеки стає однією з найважливіших завдань для України з метою забезпечення стабільності та захисту національних інтересів в кіберпросторі.

Перелік посилань:

1. Стратегія кібербезпеки України (2021 – 2025 роки) URL: proekt strategii_kyberbezpeki_Ukr.pdf (rnbo.gov.ua) (дата звернення: 17.09.2023).
2. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки URL: https://scpc.gov.ua/api/docs/19b0a96e-8c31-44bf-863e-cd3e0b651f20/19b0a96e-8c31-44bf-863e-cd3e0b651f20.pdf (дата звернення: 12.10.2023).

Денисенко Дімітрій Борисович
студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ ВІД ІНСАЙДЕРСЬКИХ АТАК

Захист від інсайдерських загроз стає надзвичайно актуальним у сучасному світі, де конфіденційні дані та комерційна інформація є найціннішими активами організацій. Статистика показує зростання випадків внутрішніх загроз та витоків даних, що наносить серйозну шкоду бізнесу та репутації компаній. Ризики внутрішніх загроз включають в себе витоки конфіденційних даних, фінансові втрати, втрату довіри клієнтів та навіть юридичні наслідки. Більшість інсайдерських загроз виникають з-за людського фактору: надмірного зловживання довірою або недбалості співробітників. Тому, необхідно постійно вдосконалювати методи захисту від інсайдерських загроз.

Загальні положення

Інсайдер — це будь-яка особа, яка має або мала авторизований доступ або знання ресурсів організації, включаючи персонал, приміщення, інформацію, обладнання, мережі та системи. Інсайдерська загроза — це можливість для інсайдера використовувати свій авторизований доступ або розуміння організації, щоб завдати їй шкоди. Ця шкода може включати навмисні чи ненавмисні дії, які негативно впливають на цілісність, конфіденційність і доступність організації, її даних, персоналу чи засобів.

Приклади інсайдера можуть включати [1]:

1. Особа, якій організація довіряє, включаючи співробітників, членів організації та тих, кому організація надала конфіденційну інформацію, таку як фінансові дані, бізнес-стратегія, сильні та слабкі сторони організації. У контексті функцій уряду це також може включати секретну інформацію. Ця особа також може мати як фізичний, так і цифровий доступ до конфіденційних просторів.
2. Особа, якій надано смарт карту або пристрій доступу, який ідентифікує її як особу з регулярним або постійним доступом (наприклад, працівник або член організації, підрядник, постачальник, зберігач або ремонтник).
3. Особа, якій організація надала комп’ютер та/або доступ до мережі.
4. Особа, яка має глибокі знання та, можливо, допомагає розвивати продукти та послуги організації; до цієї групи входять ті, хто знає секрети продуктів, які забезпечують цінність організації.

Інциденти внутрішньої загрози можливі в будь-якому секторі чи організації.

Аналізуючи звіти провідних компаній виділимо основні методи захисту від інсайдерських атак.

Методи захисту [2]:

1. Моніторинг діяльності користувачів: Ведення журналу подій та аналіз поведінки співробітників для виявлення незвичайних або підозрілих дій.
2. Обмеження прав доступу: Реалізація принципу "не більше, ніж потрібно" - надання користувачам доступу тільки до тих ресурсів, які необхідні для виконання їх робочих обов'язків.
3. Використання технологій DLP: Реалізація систем контролю за витоком

даних (Data Loss Prevention), які виявляють та запобігають незаконному витоку конфіденційної інформації.

4. Сегментація мережі: Розділення мережі на сегменти з різними рівнями доступу до даних, що обмежує можливості внутрішніх загроз.

5. Забезпечення свідомості та навчання персоналу: Надання працівникам освіти щодо основ безпеки, ризиків інсайдерських загроз та правил користування корпоративними ресурсами.

6. Аудит та перевірка систем безпеки: Періодична оцінка ефективності впроваджених заходів та виявлення можливих слабких місць у захисті [2].

Ці методи у поєднанні з правильною стратегією та технологічними рішеннями можуть допомогти ефективно захистити інформаційну систему від інсайдерських загроз.

Щоб протистояти цим ризикам, необхідно розглядати впровадження ефективних методів захисту. Це включає в себе впровадження технологій UEBA (User and Entity Behavior Analytics), які аналізують поведінку користувачів та сутностей, виявляючи незвичайні патерни. UEBA є потужним інструментом для виявлення та захисту від інсайдерських загроз у системах інформаційної безпеки [3]. Ця технологія використовує аналіз поведінки користувачів та сутностей, що включають пристрої та додатки, для виявлення аномалій, які вказують на потенційні загрози.

Основні переваги використання UEBA для захисту від інсайдерських атак включають:

1. Виявлення аномалій: UEBA аналізує звичайну поведінку користувачів та сутностей, ідентифікуючи незвичайні патерни, які можуть свідчити про загрозу.

2. Контекстне розуміння: UEBA враховує контекстну інформацію, включаючи час, місцезнаходження та тип пристрою, щоб визначити, чи є певна активність нормальною чи підозрілою.

3. Ідентифікація привілейованих акаунтів: UEBA допомагає виявити випадки надмірного використання привілейованих акаунтів, що свідчить про недобросовісну діяльність.

4. Забезпечення відповідності: UEBA допомагає виконати вимоги щодо контролю та аудиту діяльності користувачів, що є важливим для багатьох регуляторних стандартів.

5. Аналіз протягом часу: UEBA виявляє зміни у поведінці протягом тривалого періоду, сприяючи виявленню погіршення ситуації в часі.

6. Інтеграція з іншими системами безпеки: UEBA легко інтегрується з іншими інструментами безпеки, щоб створити комплексний захист [3].

Застосування UEBA є надзвичайно важливим аспектом, оскільки інсайдерські атаки завдають значної шкоди організації. Ця технологія дозволяє виявляти аномалії, що допомагає вчасно реагувати на потенційні загрози та забезпечити високий рівень захисту інформаційної системи.

Перелік посилань:

1. Insider Threat Mitigation | Cybersecurity and Infrastructure Security Agency CISA. *Home Page | CISA*.

URL: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation#:~:text=The%20key%20steps%20to%20mitigate,organization%20or%20insider%20threat%20team. (date of access: 18.10.2023).

2. Looking Within | Strategies for Detecting and Mitigating Insider Threats. *SentinelOne*. URL: https://www.sentinelone.com/blog/looking-within-strategies-for-detecting-and-mitigating-insider-threats/?utm_source=google-paid&utm_medium=paid-search&utm_campaign=nl-bau-dsa&utm_term=&campaign_id=20488859444&ad_id=671100420918&gclid=CjwKCAjw1t2pBhAFEiwA_-A-NL1tbd71TnjyAvdASNo5OL0KkjB0LmG3RgfRtyNmPDsuz6OF0G5_AhoCEowQAvD_BwE (date of access: 18.10.2023).

3. What is User Entity and Behavior Analytics (UEBA)? | Fortinet. *Fortinet*. URL: https://www.fortinet.com/resources/cyberglossary/what-is-ueba#:~:text=UEBA%20Definition,and%20endpoints%20in%20that%20network. (date of access: 18.10.2023).

Детченя Дмитро Юрійович, БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА АНОМАЛЬНУ МЕРЕЖЕВУ АКТИВНІСТЬ НА ПРИКЛАДІ FORTINDR

Визначено мету і основні завдання щодо виявлення та реагування на аномальну мережеву активність в організації. Розглянуто зміст технології виявлення та реагування на аномальну мережеву активність на прикладі FortiNDR.

Мережі поширюються на хмару та постійно зростають як у розмірі, так і в складності. Це призвело до безпрецедентного обсягу даних, що проходять через розподілену мережу, і створило ідеальне середовище, у якому могли сховатися зловмисники. Рішення виявлення та реагування мережі вирішують цю проблему шляхом збору телеметрії з мережевих пристроїв і застосування аналітичних методів, таких як машинне навчання, для виявлення загроз, які пропускають інші інструменти.

Рішення для виявлення та реагування мережі (NDR) використовують комбінацію передових аналітичних методів, які не ґрунтуються на сигнатурах, як-от машинне навчання, щоб виявити підозрілу мережеву активність. Це дозволяє командам реагувати на аномальний або зловмисний трафік і загрози, які пропускають інші інструменти безпеки.

Рішення NDR постійно відстежують і аналізують необроблений корпоративний мережевий трафік, щоб створити базову лінію нормальної поведінки мережі. Коли виявляються підозрілі шаблони мережевого трафіку, які відхиляються від цього базового рівня, інструменти NDR сповіщають групи безпеки про потенційну присутність загроз у їхньому середовищі.

FortiNDR забезпечує захист, виявлення та реагування на повний життєвий цикл мережі. Він використовує штучний інтелект, машинне навчання, поведінковий аналіз і аналіз людини для аналізу мережевого трафіку, щоб команди безпеки могли виявити поведінку зловмисників і усунути загрозу. FortiNDR забезпечує аналіз мережевого трафіку та файлів, ідентифікацію першопричини, обсяг інцидентів та інструменти для швидкого усунення інцидентів [1].

Щоб протистояти складності сучасних кіберзагроз і обсягу мережевої активності, де можуть сховатися зловмисники, Fortinet використовує штучний інтелект, щоб скоротити трудомісткі завдання, які потрібно виконувати аналітику SOC. Модель машинного навчання (ML) працює, щоб зрозуміти нормальну мережеву діяльність і визначити відхилення. Він класифікує код, пов’язаний із ненормальним трафіком, і виконує пошук спалаху для виявлення потенційних інцидентів. При інтеграції з іншими інструментами Fortinet Security Fabric FortiNDR може ініціювати автоматичні відповіді для підвищення ефективності SOC [1].

Рішення FortiNDR і FortiNDR Cloud представляють технології захисту від загроз на основі штучного інтелекту, розроблені для нечисленних команд операційних центрів безпеки (SOC) для захисту від різних загроз, включаючи сучасні постійні загрози, за допомогою навченого Virtual Security Analyst і "керованого SaaS", який допомагає виявляти, класифікувати і реагувати на загрози, в тому числі добре замасковані. Використання метаданих для виявлення загроз має важливе значення в сучасних SOC. Контрольоване і неконтрольоване машинне навчання (ML) можна застосовувати до метаданих, особливо в даних зі сходу на захід в центрах обробки даних для виявлення загроз. FortiNDR значно скорочує час на виявлення мережевих аномалій і шкідливого контенту в мережі та їх усунення за допомогою Fortinet Security Fabric і інтеграції зі сторонніми розробниками [2].

Основні можливості рішення FortiNDR [2]:

виявлення мережевих аномалій там, де традиційні рішення для захисту не спрацьовують;

дослідження загрози за допомогою історичних трендів і даних за 365 днів;

полювання на зловмисників за допомогою керованих сценаріїв;

автоматизація та реагування вручну для карантину та контролю;

імітація досвідченого аналітика безпеки для виявлення спалахів, аномалій та шкідливого програмного забезпечення, обробка великих обсягів мережевих даних;

скорочення часу виявлення та розслідування зловмисного програмного забезпечення з хвилин до секунд;

забезпечення навчання на місці, щоб зменшити кількість помилкових спрацьовувань, аналізуючи специфічний для організації трафік і адаптуючись до нових замаскованих загроз;

інтеграція в Security Fabric від Fortinet шляхом об'єднання з FortiGates та іншими рішеннями для автоматичного виявлення карантинних атак;

аналіз трафіка нульового дня.

FortiNDR підходить для клієнтів з локальним SOC, а також для розгортання з логічним розв’язкою або з високими вимогами до відповідності, де всі дані залишаються локальними. Використовуючи інтеграцію з Security Fabric, FortiNDR може автоматично виявляти і класифікувати кожен пристрій, що взаємодіє з мережею, включаючи трафік зі сходу і заходу в центрі обробки даних. FortiNDR також підтримує високопродуктивне сканування шкідливих

програм за допомогою ANN і підтримує різні інтеграції з Fabric. На рисунку 1 показано еталонну схему архітектури з FortiNDR.

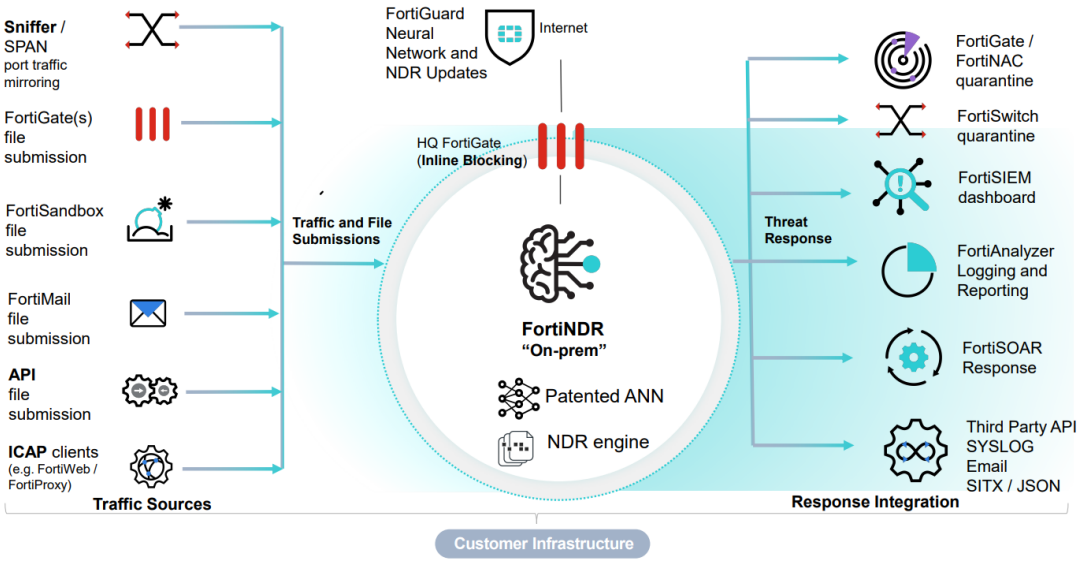


Рис. 1. Схема архітектури з рішенням FortiNDR [2]

Отже, рішення FortiNDR виступає в якості віртуального аналітика безпеки, який може ідентифікувати зловмисну мережеву активність і файли, що дозволяє в режимі реального часу ідентифікувати складні загрози, включаючи атаки нульового дня. FortiNDR Cloud поєднує ML/AI з людським аналізом і досвідом, щоб покращити безпеку та зменшити помилкові спрацьовування.

Перелік посилань:

1. Network Detection and Response. Fortinet. URL: https://www.fortinet.com/products/network-detection-and-response. (дата звернення: 29.09.2023).

2. FortiNDR and FortiNDR Cloud. Data Sheet. URL: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortindr.pdf. (дата звернення: 29.09.2023).

Дигас Максим Віталійович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ УПРАВЛІННЯ КІНЦЕВИМИ ТОЧКАМИ ОРГАНІЗАЦІЇ ТА ЇХ ЗАХИСТУ НА ПРИКЛАДІ MICROSOFT INTUNE

Ця теза розглядає сучасні технології управління кінцевими точками (Endpoint Management) і їх важливість для забезпечення безпеки та ефективності в сучасних організаціях. Особлива увага приділяється аналізу рішення Microsoft Intune, яке є однією з передових платформ в цій галузі.

Упровадження сучасних технологій управління кінцевими точками стає ключовим завданням для організацій у сучасному цифровому світі. В цій тезі ми розглянемо роль і важливість технології управління кінцевими точками на прикладі рішення Microsoft Intune, що дозволяє забезпечити безпеку та ефективність організаційних процесів.

Технологія управління кінцевими точками - це стратегічний підхід до керування пристроями, які використовуються в організації, такими як

комп'ютери, смартфони, планшети, сервери та інші. Основна мета полягає в тому, щоб забезпечити централізоване управління цими пристроями, забезпечити їх ефективність та захистити від кіберзагроз.

Основні функції технології управління кінцевими точками Microsoft Intune включають:

- Централізоване керування пристроями: Можливість дистанційного керування всіма пристроями в організації з одного місця, включаючи їх конфігурацію, оновлення та надання дозволів.
- Розгортання програмного забезпечення: Автоматизований процес розгортання та оновлення програмного забезпечення на всіх пристроях.
- Моніторинг та звітність: Збір даних про стан пристроїв та їхню продуктивність для забезпечення ефективного управління та прийняття рішень на основі даних.
- Захист інформації: Забезпечення безпеки пристроїв та даних на них від кіберзагроз, таких як віруси, зловмисний код та несанкціонований доступ.

Сучасні організації стикаються з безпрецедентними викликами та загрозами, пов'язаними з кінцевими точками. До них включаються:

- Кіберзагрози: Зловмисники активно використовують кінцеві точки як вектори для атак, включаючи розповсюдження вірусів та рейдерських атак.
- Розподілене робоче середовище: Багато організацій перейшли до роботи віддалено або використовують гібридні моделі, що ускладнює управління кінцевими точками.
- Диверсифікація пристроїв: Різноманітність пристроїв, включаючи робочі та особисті смартфони та планшети, ускладнює управління.

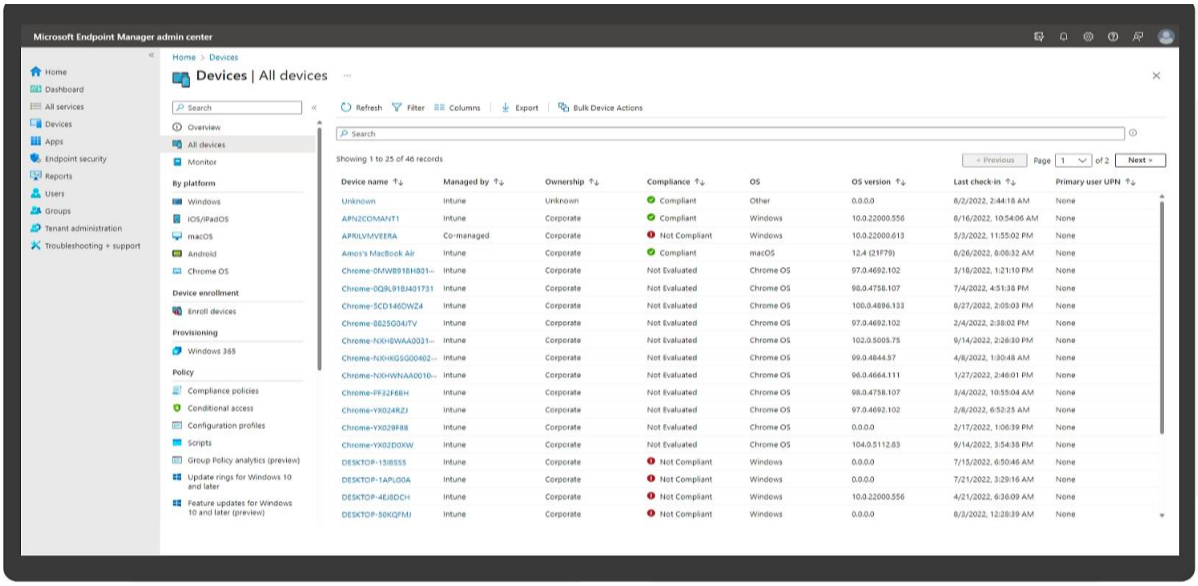


Рис.1. Кросплатформне керування кінцевими точками

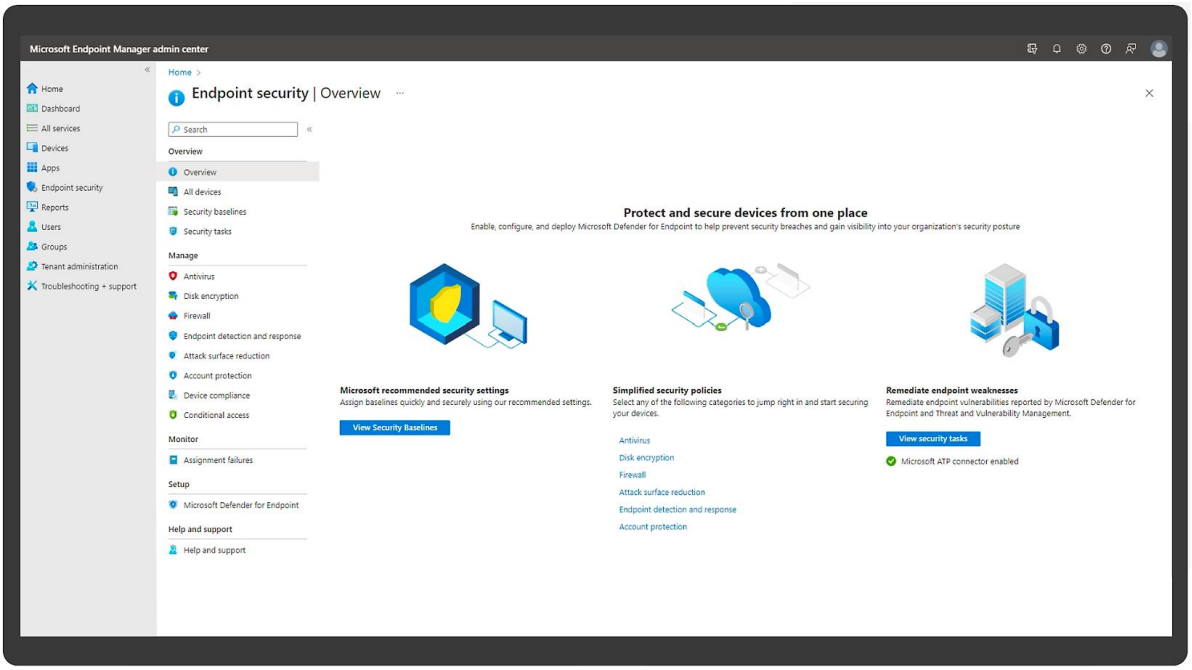


Рис.2. Вбудований захист кінцевих точок

Перелік посилань:

1. Основні можливості Microsoft Intune: https://www.microsoft.com/uk-ua/security/business/endpoint-management/microsoft-intune#tabx9b99045c129647bca286083132981345 (дата звернення: 22.10.2023).

2. Manage endpoint security in Microsoft Intune: https://learn.microsoft.com/uk-UA/mem/intune/protect/endpoint-security (дата звернення: 25.10.2023).

Діденко Данило Юрійович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

КІБЕРАТАКИ НА ПРИСТРОЇ IoT В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Інтернет речей, або IoT (Internet of Things) наразі є однією з найбільш універсальних та широко розповсюджених технологій, які існують сьогодні. Поширення мережі Інтернет, все більш зростаюча пропускна здатність та різноманітність корисних та зручних розумних пристроїв зумовлюють аномально швидкий ріст популярності IoT у всьому світі. Очікується, що у 2023 році темпи росту популярності IoT будуть й далі збільшуватись. А до 2025 року загальна кількість встановлених розумних пристроїв досягне відмітки 19,08 мільярда [1].

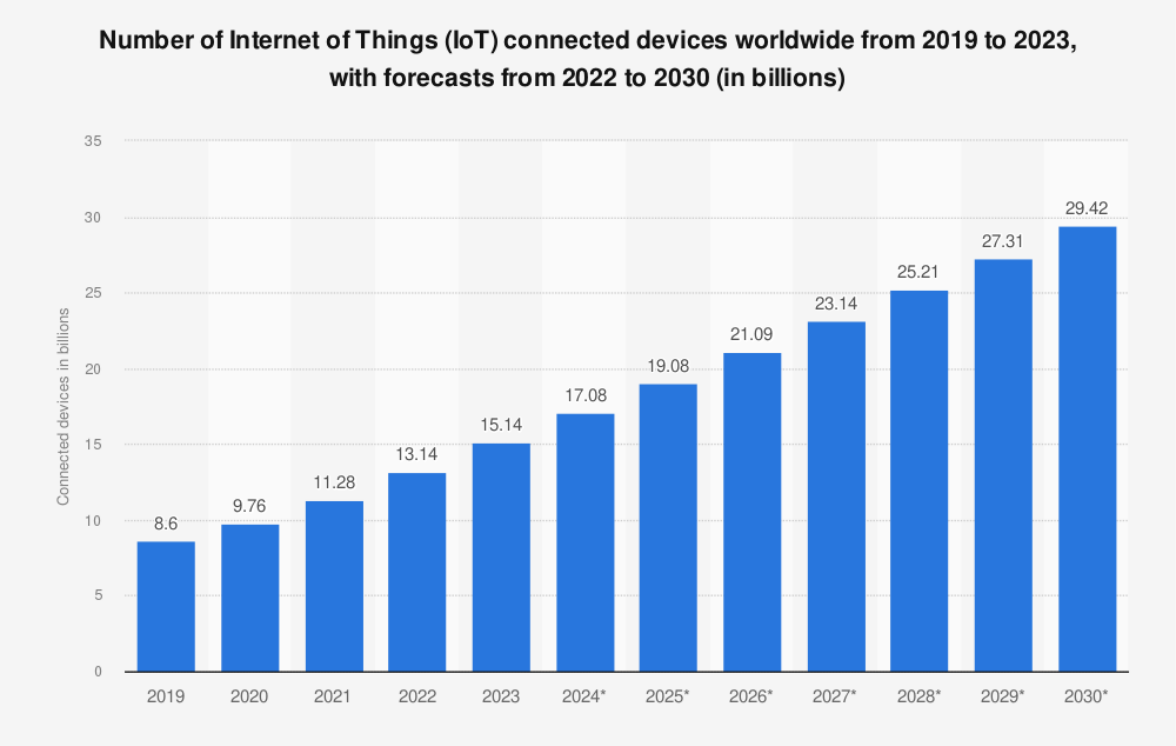


Рис.1. Графік зростання кількості пристроїв IoT у світі

Пропоную для початку визначити, що таке IoT в загальному розумінні. Ось як характеризує цей термін компанія **Gartner** [2]:

«Інтернет речей – це мережа фізичних об'єктів, які мають вбудовані технології, що дозволяють здійснювати взаємодію з зовнішнім середовищем, передавати відомості про свій стан і приймати дані ззовні».

Тобто, по суті, це екосистема пристроїв і технологій, підключених через Інтернет, які постійно збирають і передають дані. Часто до назви таких пристроїв додають приставку «смарт» або «розумний».

На перший погляд, визначення виглядає як звичайна мережа. Однак, її специфіка полягає в тому, що в такій мережі немає користувачів, сервісів та баз даних.

Основні недоліки пристроїв IoT полягають у великій кількості кібервразливостей та відсутності стандартизації.

Кожен пристрій IoT є потенційно вразливою точкою входу в мережу та бізнес-процеси. Тому такі мережі можуть стати (і стають) першим етапом компрометацій, особливо якщо атака націлена саме на конкретну організацію. З розвитком технологій, кібербезпека пристроїв стає все більш критичним питанням. Особливо це стає зрозуміло в контексті Інтернету речей, оскільки, кількість пристроїв, які можуть отримувати та надсилати конфіденційну інформацію щоденно росте. Тож впровадження й оновлення заходів безпеки пристроїв має стати пріоритетом на найближчі роки для технології IoT.

Поширені атаки на IoT

Щоб запобігти атакам на пристрої IoT, перш за все треба знати які

поширені види атак можуть використовувати кіберзлочинці для досягнення своїх цілей:

- **DDoS-атака**: відбувається коли ботнет – заражена мережа комп'ютерів – неперервно надсилає величезну кількість запитів до системи. Аномально висока активність може призвести до створення значних затримок у роботі системи або взагалі до її зупинки. Більш того, заражені пристрої IoT також можуть стати частиною ботнету та допомагати зловмисникам проводити ще більш руйнівні атаки зсередини локальної мережі.
- **Експлойт програмного забезпечення**: багато кіберзлочинців використовують вже відомі вразливості в програмній частині пристрою для проведення атаки. Розробники зазвичай закривають знайдені «діри» безпеки в оновленнях. Однак, далеко не завжди свіжі версії ПЗ вчасно завантажуються на пристрої. Саме це робить їх вразливими до атак з використанням експлойтів.
- **MITM-атака (атака посередині)**: хакери можуть перехопити мережевий трафік (вставши посередині каналу передачі між пристроєм відправником і пристроєм отримувачем) і отримати облікові дані або конфіденційну інформацію, яку пристрої IoT передають через корпоративні мережі.
- **Фізичне втручання:** простого підключення кіберзлочинцем USB флешки зі шкідливим кодом, до зовнішнього пристрою IoT може бути достатньо, щоб розповсюдити зловмисне програмне забезпечення через мережу та шпигувати за комунікаціями що в ній проходять.
- **Брутфорс атаки**: той факт, що в компаніях зазвичай не приділяється достатньо уваги парольній безпеці пристроїв IoT, робить їх вразливими до потенційних атак грубою силою або «Брутфорс». Часто паролі пристроїв IoT залишаються незмінними після встановлення просто використовуючи базовий пароль, що дозволяє зловмисникам дуже просто їх підбирати.
- **Викрадення прошивки**: якщо оновлення мікропрограми пристрою не було криптографічно підписано або прошивка передається по не захищеному каналу зв'язку – це дає смогу зловмисникам перехопити її та завантажувати шкідливе ПЗ на пристрої під виглядом оновленнь. Також за допомогою викраденої прошивки у кіберзлочинців з'являється можливість отримати облікові дані пристрою.

Захист пристроїв IoT

З вищезазначених векторів атак на IoT можна зробити висновок, що основні компоненти систем Інтернету речей є досить вразливими до атак зловмисників. Незалежно від масштабу та типу середовища, у яке вбудовується система IoT, безпека повинна розглядатися ще на етапі проєктування мережі, щоб покращити її інтегрування.

Ось декілька основних рекомендацій, щоб запобігти кібератакам на пристрої та загалом зменшити ризики безпеки компанії:

1.Проводити інвентаризацію та моніторинг усіх пристроїв;

2. Використовувати практику сегментації мережі;

3. Встановлювати криптостійкі паролі для IoT;

4. Забезпечити захист всіх пристроїв IoT на фізичному рівні;

5. Своєчасно оновлювати прошивки пристроїв;

6. Шифрувати пристрої IoT.

Висновок

Пристрої IoT це чудова технологія без якої важко уявити наше майбутнє. Проте ідеальних технологій, на жаль, просто не існує. Основний недолік технології IoT є те, що при нехтуванні правилами кібербезпеки, вона створює додаткові ризики для організацій. За допомогою наведених вище рекомендацій ці ризики можна суттєво зменшити та використовувати повну користь від технології IoT.

Перелік посилань:

1. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030 URL: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
2. Gartner Glossary URL: https://www.gartner.com/en/information-technology/glossary/internet-of-things#:~:text=The%20Internet%20of%20Things%20(IoT,states%20or%20the%20external%20environment
3. Common Cyber-Attacks in the IoT URL: https://www.globalsign.com/en/blog/common-cyber-attacks-in-the-iot

Дімогло Олексій Георгійович
Студент групи БСДМ-61, ННІЗІ, ДУІКТ, Київ, Україна

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ ЗА ДОПОМОГОЮ AD

Основним фактором, який робить безпеку Active Directory або безпеку AD винятково важливою для загальної системи безпеки бізнесу, є те, що Active Directory організації контролює весь доступ до системи. Ефективне керування Active Directory допомагає захистити облікові дані, програми та конфіденційні інформаційної системи організації від несанкціонованого доступу. Важливо мати надійний захист, щоб зловмисники не могли отримати доступ до мережі та завдати шкоди.

Атаки на обчислювальну інфраструктуру зросли за останнє десятиліття в усіх частинах світу. У результаті організаціям будь-якого розміру в усьому світі

доводиться стикатися з витоками інформації, крадіжкою інтелектуальної власності (IP), атаками типу «відмова в обслуговуванні» (DDoS) або навіть зруйнованою інфраструктурою.

Однак, оскільки ландшафт загроз змінювався протягом багатьох років, ландшафт безпеки також адаптувався для протидії цим загрозам. Хоча жодна організація з інфраструктурою інформаційних технологій (IT) ніколи не має абсолютного імунітету до атак, кінцевою метою безпеки є не повне запобігання спробам атак, а захист IT-інфраструктури від атак. За допомогою правильних політик, процесів і елементів керування можна захистити ключові частини IT-інфраструктури від компрометації.

Розглянемо найпоширеніші вразливості безпеки.

Початкові об’єкти злому або точки входу – це області, де зловмисникам найпростіше проникнути у IT-інфраструктуру. Точками входу зазвичай є прогалини в безпеці або оновлення, якими зловмисники можуть скористатися, щоб отримати доступ до системи організації. Зловмисники зазвичай починають з однієї або двох систем одночасно, а потім посилюють свою атаку, поширюючи свій вплив на більшу кількість систем непомітно.

Найпоширенішими вразливими місцями є:

- Прогалини в розгортанні антивірусів і зловмисного програмного забезпечення
- Застарілі програми та операційні системи
- Неправильна конфігурація
- Відсутність безпечних практик розробки програм

Атаки з крадіжки облікових даних — це випадки, коли зловмисник отримує привілейований доступ до комп’ютера в мережі за допомогою інструментів для вилучення облікових даних із сеансів облікових записів, у які наразі ввійшли. Зловмисники часто використовують певні облікові записи, які вже мають підвищені привілеї. Зловмисник викрадає облікові дані цього облікового запису, щоб імітувати його особу та отримати доступ до системи.

Зменшити область атаки за допомогою Active Directory

Можна запобігти атакам, зменшивши область для атак за допомогою розгортання Active Directory.

Active Directory (AD) — це база даних і набір служб, які з’єднують користувачів із мережевими ресурсами, необхідними для виконання роботи.

База даних (або каталог) містить критично важливу інформацію про середовище, включно з тим, які користувачі та комп’ютери існують і кому дозволено робити що. Наприклад, база даних може містити 100 облікових записів користувачів із такими деталями, як посада, номер телефону та пароль кожної особи. Він також запише їхні дозволи.

Служби контролюють велику частину діяльності, яка відбувається у вашому IT-середовищі. Зокрема, вони переконуються, що кожна особа є тим, за кого себе видає (автентифікація), як правило, шляхом перевірки ідентифікатора користувача та пароля, які вони вводять, і дозволяють їм отримати доступ лише до тих даних, які їм дозволено використовувати (авторизація).

Active Directory спрощує життя адміністраторів і кінцевих користувачів, одночасно підвищуючи безпеку для організацій. Адміністратори користуються централізованим керуванням користувачами та правами, а також централізованим контролем конфігурацій комп'ютера та користувачів за допомогою функції групової політики AD. Користувачі можуть пройти автентифікацію один раз, а потім безперешкодно отримати доступ до будь-яких ресурсів у домені, для якого вони авторизовані (єдиний вхід). Крім того, файли зберігаються в центральному сховищі, де ними можна ділитися з іншими користувачами, щоб спростити співпрацю, а IT-команди створюють належні резервні копії для забезпечення безперервності бізнесу.

Забезпечення безпеки організації на базі AD

1. Мінімізація дозволів користувачів

Можливо, найфундаментальнішою основою найкращої практики IT-безпеки є принцип найменших привілеїв. Надайте кожному користувачеві саме той доступ, який йому потрібен для виконання роботи, ні більше, ні менше. AD дозволяє помістити користувачів зі схожими ролями (наприклад, усіх адміністраторів служби підтримки або весь персонал відділу кадрів) у групу безпеки AD і керувати ними разом. Користувачі можуть бути — і зазвичай є — членами кількох груп AD, наприклад груп на основі проектів.

Використання груп безпеки AD — це не просто зручність для адміністраторів; він покращує безпеку, зменшуючи помилки під час надання та деініціалізації, а також мінімізуючи складність структури дозволів, щоб легше з упевненістю сказати, хто до чого має доступ.

2. Керування дозволами користувачів і груп

Як зазначалося раніше, принцип найменших привілеїв є найосновнішою передовою практикою безпеки IT. Якби довелося вручну призначати дозволи кожному користувачу для кожного ресурсу окремо — і підтримувати ці дозволи в актуальному стані, оскільки користувачі приходять і йдуть і змінюють ролі в організації — адміністратори були б перевантажені, і організація була б піддана високому ризику порушень і невідповідності .

Можливість створювати групи безпеки AD і спільно керувати дозволами для схожих користувачів зменшує навантаження. Користувачі можуть — і зазвичай є — членами кількох груп AD, наприклад груп на основі проектів. Наприклад, новому менеджеру з продажу можна надати доступ до всіх потрібних ресурсів, просто додавши його до групи безпеки Sales і групи безпеки Sales Manager. Подібним чином, якщо є нова папка або спільний файл, до якого потрібен доступ усім продавцям, можна надати доступ групі продажів замість того, щоб додавати їх до окремих облікових записів користувачів по одному. І навпаки, якщо користувач переходить із ролі Sales на іншу посаду, можна скасувати його доступ до всіх ресурсів Sales, видаливши його з групи Sales замість того, щоб ретельно переглядати кожен ресурс, до якого він має дозволи, і визначати, чи доступ усе ще залишається. законним.

3. Застосування параметрів групової політики для запобігання порушенням безпеки

Використовуючи параметри групової політики, можна обмежити доступ користувачів до певних ресурсів, виконувати сценарії та виконувати прості операції. Ці операції включають примусове відкриття певної домашньої сторінки для кожного користувача в мережі, зміну робочого столу та контроль над доступом до інструментів адміністрування та панелі керування. При правильному застосуванні групову політику можна використовувати для запобігання встановлення небажаного програмного забезпечення та налаштування операційної системи до неприйнятного рівня.

4. Багатофакторна автентифікація

Віддалених користувачів можна легко зламати, часто навіть не усвідомлюючи цього. Багатофакторна автентифікація (MFA) пропонує один із найкращих способів захистити віддалені пристрої від онлайн-атак. Рішення MFA вимагає, щоб користувач успішно надав два або більше доказів, перш ніж отримати доступ до системи. Якщо хакери отримають облікові дані користувача Active Directory, процес MFA не дозволить їм підвищити привілеї в системі.

5. Стандарти моніторингу та аудиту

Послідовний моніторинг Active Directory у реальному часі може виявитися безцінним ресурсом для компаній, які прагнуть захистити свої мережі. Розроблення процесу, який дозволить уповноваженому персоналу контролювати та перевіряти всю систему на предмет будь-якої несанкціонованої чи небезпечної діяльності, яка може поставити мережу під загрозу. Впровадження рішення, яке оцінює зміни користувача та поведінку мережі, може допомогти виявити незвичайне залучення системи якомога швидше, щоб обійти потенційну кібератаку.

Перелік посилань:

1. Best Practices for Securing Active Directory [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

2. What is Active Directory Security? [Електронний ресурс] – Режим доступу: https://www.proofpoint.com/us/blog/identity-threat-defense/active-directory-security-best-practices

3. Active Directory Best Practices to Minimize Cybersecurity Risk [Електронний ресурс] – Режим доступу: https://www.tenable.com/blog/8-active-directory-best-practices-to-minimize-cybersecurity-risk

Дорохін Орест Олександрович
студент групи АІКБ-125, ННІЗІ ДУІКТ, Київ, Україна,
Борсуковський Юрій Володимирович
Доцент кафедри Інформаційної та кібернетичної безпеки, ННІЗІ ДУІКТ, Київ, Україна

МЕТОД ВИЯВЛЕННЯ АТАК КОРПОРАТИВНИХ ВЕБ-ДОДАТКІВ НА ОСНОВІ ГРАДІЄНТНОГО БУСТІНГУ

Веб-застосунки стали невід'ємною частиною нашого повсякденного життя, що робить їх пріоритетною ціллю для кібератак. Один із найбільш серйозних загроз – міжсайтинговий скриптинг (XSS). XGBXSS, як новий веб-орієнтований фреймворк для виявлення атак XSS, що базується на техніці ансамблю з використанням алгоритму Extreme Gradient Boosting (XGboost) з підходом

екстремальної оптимізації параметрів є можливим рішенням проблеми. Запропонований новий гібридний підхід для вибору ознак, що включає в себе об'єднання інформаційної вигоди (Information Gain, IG) з послідовним зворотнім відбором (Sequential Backward Selection, SBS) для вибору оптимального піднабору, що зменшує обчислювальні витрати і одночасно забезпечує високу ефективність виявлення. Запропонований фреймворк успішно пройшов кілька тестів на тестовому наборі даних і отримав передові результати з точністю, вибірковою здатністю, імовірністю виявлення, F-коефіцієнтом, числом хибно-позитивних та хибно-негативних спрацювань і оцінкою AUC-ROC відповідно 99,59%, 99,53%, 99,01%, 99,27%, 0,18%, 0,98% і 99,41%. Він має потенціал бути впровадженим як самостійна система, яка є достатньо ефективною для запобігання атакам, включаючи XSS-атаки нульового дня.

Уразливості міжсайтового скриптингу (XSS) є однією з поширених високоризикових кібератак веб-додатків, які піддають високому ризику як користувачів, веб-додатки, так і корпоративну інфраструктуру, наприклад через подальше застосування lateral movement. XSS може бути використаний для заподіяння шкоди, наприклад, повна зміна зовнішнього вигляду або поведінки веб-сайту організації, крадіжка конфіденційної інформації підприємства або конфіденційної інформації користувача, дії від імені справжнього користувача та багато іншого. Були запропоновані різні схеми запобігання та пом'якшення наслідків для протидії атакам на основі XSS як на стороні клієнта, так і на стороні сервера або на стороні пари, використовуючи різні методи аналізу, такі як статичний, динамічний або гібридний. Однак запропоновані рішення з використанням існуючих традиційних методів виявлення таких атак стали недостатніми через складні та зростаючі форми корисних навантажень (payload) XSS. Крім того, більшість з них не масштабуються в часі і мають високий відсоток помилкових спрацьовувань [1]. Згідно з дослідженням PreciseSecurity, майже 40% усіх атак, зафіксованих експертами з безпеки, є XSS-атаками. Вони зазначили, що майже 75 % престижних компаній у Північній Америці та Європі були атаковані XSS станом на 2019 рік [2]. Крім того, загальна кількість нових XSS-вразливостей у 2019 році (2023) зросла на 30,2% порівняно з 2018 роком (1554) та на 79,2% порівняно з 2017 роком (1129) за даними National Vulnerabilities Database (NVD) [3].

Методи штучного інтелекту (ШІ) стають мейнстрімом, а розробка ефективного та надійного механізму кіберзахисту з новітніми схемами штучного інтелекту, які мають потенціал для точного та точного виявлення цих складних атак на основі XSS, викликає великий інтерес у дослідників та веб-спільнот.

Дослідники намагаються використовувати ШІ для підвищення ймовірності виявлення, що видно зі значного використання методів машинного навчання (ML) під час виявлення кібератак. Системи захисту навчаються за допомогою набору даних про раніше відому поведінку, і кожна група поведінки розпізнається як злоякісна або доброякісна. Незважаючи на те, що штучний інтелект додає значну цінність у вирішенні таких проблем, згідно з оглядом літератури, XSS-детектори на основі машинного навчання (ML) і глибокого навчання (DL) все ще страждають від значного фундаментального дефіциту, який полягає в значній кількості відсутніх випадків (це збільшує частоту хибно-

негативних результатів (FN)). FN викликають більш серйозне занепокоєння, ніж хибно-позитивні спрацьовування (FP), оскільки це в кінцевому підсумку призводить до реальних загроз і компрометації системи безпеки. Насправді, ця проблема пов'язана з неглибоким рівнем виявлення в цих системах (тобто показники виявлення атак все ще далекі від 100%). Крім того, більшість із цих запропонованих моделей також все ще мають принаймні одну з суттєвих проблем, яка або забирає багато часу для обробки величезної кількості даних та/або має високу частоту FP. Таким чином, питання про те, чи можна використовувати передові підходи машинного навчання для підвищення можливостей виявлення XSS-атак, є важливим для можливого посилення захисту від такого роду кібератак.

У цьому аналізі пропонується огляд нової підходу до виявлення атаки, а саме XGBXSS, для подолання розглянутих вище недоліків. Запропонована структура складається з трьох основних принципів, включаючи: покращений процес вилучення ознак, шляхом підвищення здатності моделі масштабувати пошук ознак за допомогою функції пошуку за словником, об'єднання збору інформації (Information Gain, IG) з послідовним зворотним відбором (Sequential Backward Selection, SBS) для виконання нового гібридного підходу до вибору ознак для вибору оптимальної підмножини при збереженні високої продуктивності у всіх вимірюваннях, і прийняття ансамблевого навчання з використанням алгоритму на основі XGBoost з екстремальним підходом до оптимізації.

Запропонована структура досягла авангардних результатів на нещодавно використаному наборі даних тестування з точністю, точністю, ймовірністю виявлення, частотою FP, FN та показниками ROC (AUC) 99,59%, 99,50%, 99,02%, 0,20%, 0,98% та 99,41% відповідно. Основні внески дослідження [4] можна підсумувати наступним чином:

• Було створено новий фреймворк XGBoost разом із оптимізацією екстремальних параметрів на реалістичному та актуальному наборі даних XSS, який охоплює 160 функцій для завдання виявлення, щоб забезпечити вищу точність і вищу швидкість виявлення.

• Запроваджено підхід об'єднаного збору інформації (IG) з послідовним зворотним відбором (SBS) для вибору найбільш оптимальних характеристик з набору даних, спрямованих на зниження обчислювальних вимог з одночасним підвищенням продуктивності.

• Виведено найкращу підмножину ознак, що складається з 30 ознак, здатних ефективно характеризувати сценарії XSS.

XGBXSS, порівняно з усіма детекторами, демонструє більшу ефективність і переваги в різних аспектах, де він досяг великої оптимальної продуктивності з усіма вимірюваннями. Запропонована структура виявлення є ефективною та надійною, що стає очевидним, спостерігаючи за помітною досконалістю та

кращими показниками продуктивності різних експериментів, що розглядають обидва класи. Там, де він одночасно забезпечував дуже високу точність запам'ятовування, це також видно за допомогою F-показника. F-показник є важливим показником, який широко використовується для передачі вимірювань в один цілісний показник. Крім того, дуже низькі показники FP і FN близькі до нуля.

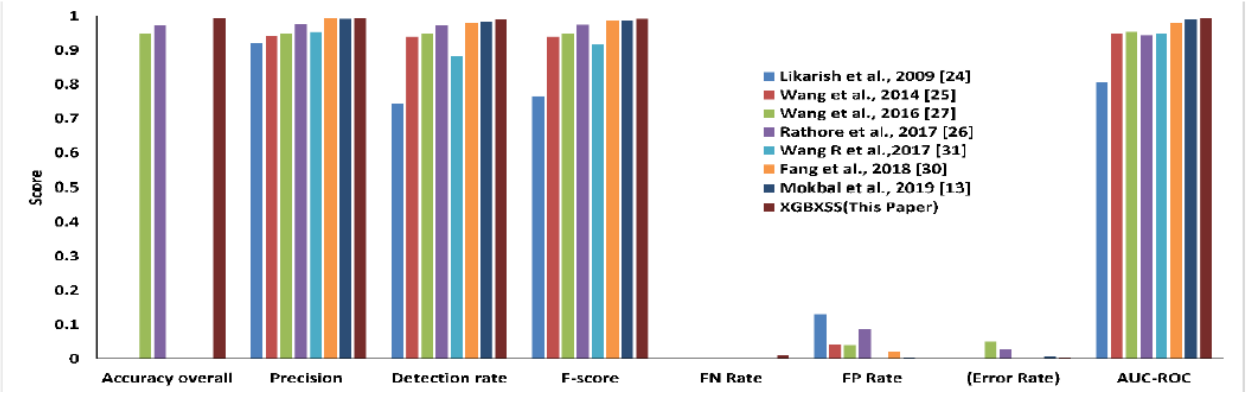


Рис.1. Порівняння результатів XGBXSS з іншими детекторами

Слід зазначити, що показники всіх алгоритмів, які застосовувались для порівняння не є критично гіршими (Рис. 1). Показники виявлення XSS все ще далекі від того, щоб наблизитися до одиниці, де результати є 100% або ближчими до неї; однак абсолютного ідеалізму (тобто 100%) може бути складно досягти, але не неможливо за допомогою методів штучного інтелекту.

XGBXSS довів свою ефективність, здатну досягати надзвичайної точності та швидкості виявлення з мінімальними показниками хибно-позитивних та хибно-негативних результатів, тобто майже еквівалентними нулю. Фреймворк виявлення прийняв великий набір даних для перспективи навчання та тестування із запропонованою технікою вилучення та відбору ознак, а також техніку ансамблевого навчання для завдання виявлення. Було проведено численні аналізи для перевірки запропонованої структури на різних етапах. Результати експериментів встановлюють ефективність фреймворку XGBXSS при багаторазових вимірюваннях обох класів порівняно з п'ятьма добре відомими алгоритмами машинного навчання. Запропонована структура виявлення може зменшити розміри набору даних до 30 об'єктів, зберігаючи при цьому високопродуктивні показники.

Крім того, однією з особливостей запропонованого фреймворку, є те, що його можна доволі легко розгорнути як цілісну систему.

Перелік посилань:

1. Rodríguez GE, Torres JG, Flores P, Benavides DE. Cross-site scripting (XSS) attacks and mitigation: A survey. Comput Networks 2019;166. URL: https://doi.org/10.1016/j.comnet.2019.106960 (дата звернення 29.10.2023).-

2. Cross-Site Scripting (XSS) Makes Nearly 40% of All Cyber Attacks in 2019 - PreciseSecurity.com n.d. https://www.precisesecurity.com/articles/cross-site-scripting-xss-makes-nearly-40-of-all-cyber-attacks-in-2019 (дата звернення 29.10.2023).
3. NIST.gov. National Vulnerability Database (NVD), Vulnerabilities n.d.URL: https://nvd.nist.gov/vuln. (дата звернення 29.10.2023).
4. Fawaz M. M. Mokbal: XGBXSS: An Extreme Gradient Boosting Detection Framework for Cross-Site Scripting Attacks Based on Hybrid Feature Selection Approach and Parameters Optimization. URL: https://www.researchgate.net/publication/350239315_XGBXSS_An_Extreme_Gradient_Boosting_Detection_Framework_for_Cross-Site_Scripting_Attacks_Based_on_Hybrid_Feature_Selection_Approach_and_Parameters_Optimization (дата звернення 29.10.2023).

Дорош Сергій Валерійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ЕФЕКТИВНЕ ВПРОВАДЖЕННЯ РІШЕННЯ MDM (MOBILE DEVICE MANAGEMENT) У ВЕЛИКИХ КОРПОРАЦІЯХ: ВИКЛИКИ, ПЕРЕВАГИ ТА КЛЮЧОВІ АСПЕКТИ УСПІХУ

Звідкіля й куди: Зрозуміти важливість та мету впровадження рішень MDM у великих корпораціях.

1. Визначення MDM та його роль:
- MDM (Mobile Device Management) – це стратегія та набір технологій, спрямованих на керування та забезпечення безпеки мобільних пристроїв та даних у великих організаціях.

2. Виклики впровадження MDM в великих корпораціях:
- Різноманітність пристроїв та операційних систем.
- Питання приватності та дотримання регуляторних вимог.
- Запровадження нових процесів та політик безпеки.

3. Переваги впровадження MDM:
- Забезпечення безпеки даних та захист від загроз кібербезпеки.
- Спрощення керування мобільними пристроями та програмами.
- Зменшення ризику втрати конфіденційної інформації.

4. Ключові аспекти успішного впровадження MDM:
- Стратегія та планування: Визначення мети та обсягу проекту, встановлення метрик успіху.
- Вибір правильного MDM рішення: Врахування потреб корпорації та можливостей рішення.
- Дотримання законодавства та нормативних вимог: Забезпечення відповідності з регуляторними вимогами та політиками безпеки.
- Навчання та підтримка співробітників: Забезпечення, що користувачі розуміють та дотримуються правил безпеки.

5. Впровадження MDM у великих корпораціях є ключовим етапом у забезпеченні безпеки та ефективності мобільних робочих процесів. Відповідне планування, вибір та імплементація MDM рішення допоможуть знизити ризики та підвищити продуктивність в організації

Перелік посилань:

1. Впровадження рішення по управлінню мобільними пристроями (MDM): https://www.intrasystems.ua/projects/intrasystems-realizuvala-proekt-vprovadzhennya-rishennya-po-upravlinnyu-mobilnimi-pristroyami-mdm-dlya-kompaniyi-pat-ukrtelekom

Дрось Данило Анатолійович
студент групи бсдм-62, ННІЗІ ДУІКТ, Київ, Україна

РОЛЬ ТЕХНОЛОГІЙ У ВДОСКОНАЛЕННІ ЗАХОДІВ ПРОТИДІЇ СОЦІАЛЬНОМУ ІНЖЕНЕРЕНГУ В ОРГАНІЗАЦІЯХ НА ПРИКЛАДІ СУЧАСНИХ МЕТОДІВ ТА ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Сучасна епоха визначається не тільки швидким розвитком технологій, але й зростанням загроз кібербезпеці. Організації повинні відповідати на ці загрози та розвивати методи та стратегії протидії соціальному інженеренгу. Однак технології можуть бути великою допомогою в цьому процесі. Наша теза досліджує роль технологій у вдосконаленні заходів протидії соціальному інженеренгу в організаціях на прикладі сучасних методів та підходів до забезпечення кібербезпеки.

Розділ 1: Поняття соціального інженеренгу та його загрози

Соціальний інженеренг - це процес отримання конфіденційної інформації або навіть доступу до системи шляхом маніпулювання людьми. Цей метод атаки стає все більш небезпечним, оскільки атакуючі використовують психологічні методи, щоб отримати доступ до цінних ресурсів.

Розділ 2: Роль технологій у захисті від соціального інженеренгу

2.1. Аналітика та моніторинг поведінки користувачів

Сучасні технології аналізу поведінки користувачів, такі як машинне навчання та штучний інтелект, можуть допомогти виявляти незвичайні патерни та поведінку, що можуть бути пов'язані з атаками соціального інженеренгу.

2.2. Системи ідентифікації та автентифікації

Вдосконалені системи ідентифікації та автентифікації, такі як біометричні дані та двофакторна аутентифікація, зменшують ризик надмірної довіри та сприяють захисту від атак соціального інженеренгу.

2.3. Захист інформації про співробітників та клієнтів

Застосування криптографії та інших технологій для зберігання та передачі конфіденційної інформації може значно ускладнити завдання атакуючим у використанні соціального інженеренгу.

Розділ 3: Перспективи та виклики

Технології мають великий потенціал у покращенні заходів протидії соціальному інженеренгу. Однак разом з цим існують виклики, такі як приватність та етичні питання використання даних користувачів. Організації повинні бути обережними та балансувати між захистом та правами користувачів.

Висновок:

Технології грають важливу роль у протидії соціальному інженеренгу в організаціях, забезпечуючи більшу надійність та захист від атак. Однак успішність заходів залежить від правильної інтеграції технологій та збалансованості між безпекою та приватністю. Дана теза має на меті обговорити цей аспект та підкреслити важливість використання сучасних технологій для підвищення рівня кібербезпеки в організаціях у світі, де загрози соціального інженеренгу стають все більш актуальними.

Євтушенко Борис Олександрович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

АКУТАЛЬНІ ПРОБЛЕМИ ЗАХИСТУ ВІДДАЛЕНИХ КОРИСТУВАЧІВ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

В сучасному світі віддалена робота стала необхідною складовою для багатьох організацій та їхніх співробітників. За останні роки зростання технологій та глобальні зміни в способі роботи призвели до посилення використання віддалених мереж та інформаційних технологій. Проте, разом із цим зросла загроза кібербезпеці для віддалених користувачів корпоративної мережі організації.

Актуальні проблеми кібербезпеки віддаленим користувачам корпоративної мережі організації включають в себе різні аспекти, оскільки робота з віддаленими працівниками стала більш розповсюдженою та складною завдяки зростанню технологій та змінам в способі роботи. Це вимагає комплексного підходу та постійного оновлення стратегій та технологій, оскільки загрози постійно змінюються. Ось деякі з цих проблем та їх рішення:

1)Захист кінцевих пристроїв (End-Point Security): Віддалені користувачі підключаються до корпоративної мережі з різних пристроїв, включаючи особисті комп'ютери і мобільні пристрої. Забезпечення безпеки цих пристроїв, зокрема антивірусними програмами, брандмауерами та оновленнями, є важливим завданням.

2)Віддалений доступ до мережі (Remote Network Access): Щоб віддалені співробітники могли працювати з корпоративними ресурсами, організації використовують VPN та інші технології. Важливо забезпечити безпеку цього віддаленого доступу, включаючи аутентифікацію та шифрування.

3)Багатофакторна аутентифікація (Multi-Factor Authentication, MFA): Використання MFA стає обов'язковим для забезпечення додаткового рівня безпеки. Це може включати в себе використання паролів, пін-кодів та фізичних пристроїв для аутентифікації.

4)Захист від фішингу і соціальної інженерії: Віддалені працівники можуть бути більш вразливими до атак фішингу та соціальної інженерії через електронну пошту та інші комунікаційні канали. Інструктаж та навчання щодо виявлення підозрілих повідомлень дуже важливі.

5)Захист даних на віддалених пристроях: Важливо забезпечити

шифрування даних, які зберігаються на віддалених пристроях, та віддалений стирання в разі втрати або крадіжки пристрою.

6)Моніторинг та аналіз поведінки (Behavioral Monitoring): За допомогою інструментів моніторингу та аналізу поведінки можна виявити аномальні дії в мережі, що можуть свідчити про можливі кібератаки.

7)Автоматизовані системи виявлення загроз (IDS/IPS): Використання систем виявлення та запобігання інцидентів є важливим для оперативного реагування на потенційні загрози.

8)Забезпечення сталої зв'язності з віддаленими користувачами: Організації повинні забезпечити, щоб віддалені користувачі завжди мали доступ до необхідних ресурсів і не були вразливі до перерв в мережі.

9)Захист від DDoS-атак: Віддалені користувачі можуть стати мішенями для розподілених атак на відмову в обслуговуванні (DDoS). Важливо мати захисні заходи, щоб відновити доступ у разі таких атак.

Перелік посилань:

1. Небезпека віддаленого режиму роботи: як захистити корпоративну мережу URL: https://www.eset.com/ua/about/newsroom/blog/business-security/opasnost-udalennogo-rezhima-raboty-kak-zashchitit-korporativnuyu-set/ (дата звернення: 24.10.2023).
2. 7 Best Practices For Securing Remote Access for Employees: https://phoenixnap.com/blog/secure-remote-access-best-practices (дата звернення: 25.10.2023).

Єкімов Іван Вікторович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

У наш цифровий вік, що швидко розвивається, важливість управління кібербезпекою неможливо переоцінити. Постійне зростання технологій і взаємопов’язаність нашого світу створюють незліченні можливості, але вони також створюють нові та складні проблеми, пов’язані із захистом конфіденційної інформації та систем від кіберзагроз. У цьому есе досліджуватимуться ключові елементи ефективного управління кібербезпекою, виклики, з якими воно стикається, і стратегії забезпечення безпеки та стійкості цифрового середовища.

Розуміння складності управління кібербезпекою

Управління кібербезпекою полягає не лише у впровадженні технічних заходів захисту; він охоплює комплексний підхід до захисту цифрових активів від різних загроз. Він передбачає запобігання, виявлення, реагування та відновлення після порушень безпеки. Одним із фундаментальних викликів в управлінні кібербезпекою є динамічний характер кіберзагроз. Зловмисники постійно вдосконалюють свою тактику, що вимагає постійної адаптації заходів безпеки.

Ключові компоненти ефективного управління кібербезпекою

Оцінка ризиків. Першим кроком до ефективного управління кібербезпекою є розуміння потенційних ризиків. Це передбачає виявлення цінних цифрових активів, оцінку потенційних загроз і оцінку вразливостей. Оцінка ризиків допомагає визначати пріоритети заходів безпеки та ефективно розподіляти ресурси.

Профілактичні заходи: Профілактика часто є найбільш економічно ефективним підходом. Він включає такі практики, як використання надійних паролів, шифрування даних, підтримка програмного забезпечення в актуальному стані та навчання користувачів найкращим практикам безпеки. Ці заходи можуть допомогти запобігти багатьом поширеним кіберзагрозам.

Обізнаність про безпеку: людські помилки є суттєвим фактором порушень кібербезпеки. Програми навчання та підвищення обізнаності з кібербезпеки є життєво важливими для навчання співробітників і користувачів потенційним ризикам, таким як спроби фішингу або важливість надійної автентифікації.

Постійний моніторинг: впровадження заходів безпеки – це лише початок. Регулярний моніторинг систем і мереж на наявність незвичних дій або вразливостей може допомогти виявити загрози на ранніх стадіях і запобігти порушенням безпеки.

Реагування на інциденти. Наявність чітко визначеного плану реагування на інциденти має вирішальне значення для пом’якшення впливу порушення безпеки. План повинен окреслювати кроки, які необхідно вжити у випадку виявлення порушення, включаючи зв’язок, стримування та відновлення.

Виклики в управлінні кібербезпекою

Ландшафт загроз, що розвивається: кіберзагрози постійно розвиваються, стають все складнішими та їх важче виявити. Це вимагає постійного навчання та адаптації, щоб випереджати зловмисників.

Обмеження ресурсів: адекватні ресурси, як з точки зору бюджету, так і кваліфікованого персоналу, часто є проблемою для організацій. Управління кібербезпекою може потребувати ресурсів, і багатьом організаціям важко виділити достатньо коштів і талантів.

Баланс між безпекою та зручністю використання. Ефективна кібербезпека часто передбачає впровадження суворих заходів безпеки, що іноді може призвести до незручностей або ускладнень для користувачів. Встановлення правильного балансу між безпекою та зручністю використання є проблемою.

Стратегії ефективного управління кібербезпекою

Співпраця. Ефективне управління кібербезпекою часто вимагає співпраці між різними зацікавленими сторонами, зокрема IT-командами, керівництвом і співробітниками. Спільна робота та обмін знаннями можуть допомогти досягти вищого рівня безпеки.

Регулярні оновлення. Необхідно постійно оновлювати програмне забезпечення, програми та заходи безпеки. Уразливості в застарілих системах можуть бути використані кіберзлочинцями.

Структури кібербезпеки: багато організацій вважають корисним прийняти визнані рамки кібербезпеки, такі як NIST або ISO 27001, щоб керувати своїми зусиллями з кібербезпеки.

Інтелектуальна інформація про загрози: бути в курсі останніх кіберзагроз і тенденцій є надзвичайно важливим. Служби аналізу загроз можуть надати цінну інформацію про нові ризики.

Тип загрози	Опис
Шкідливе програмне забезпечення	Шкідливе програмне забезпечення, включаючи віруси, хробаки та програми-вимагачі.
Фішинг	Оманливі електронні листи або повідомлення, призначені для того, щоб оманою змусити користувачів розкрити конфіденційну інформацію.
DDoS-атаки	Розподілені атаки на відмову в обслуговуванні переповнюють мережі або веб-сайти, щоб порушити обслуговування.
Внутрішні загрози	Ризики безпеки зсередини організації, часто залучаючи працівників або підрядників.

Таблиця 1: Поширені загрози в кібербезпеці

Підсумовуючи, ефективне управління кібербезпекою має важливе значення в нашу цифрову еру для захисту конфіденційних даних, систем і цифрового середовища. Це вимагає проактивного підходу, постійного навчання та рішучості адаптуватися до нових загроз. Розуміючи складність управління кібербезпекою, вирішуючи виклики та використовуючи ефективні стратегії, організації та окремі особи можуть підвищити свою стійкість проти кіберзагроз і зробити свій внесок у безпечніший цифровий світ.

Перелік посиланнь:

1. Навчальний посібник. Дніпро 2020. А.М. Гребенюк, Л.В. Рибальченко. Дніпроп. держ. ун-т внутріш. справ. ОСНОВИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ [ст.76] https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1I%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3I%D0%91%20.pdf
2. Стаття про 10 поширених загроз кібербезпеці для малих бізнесів та способи їх запобігання, написаний співробітниками 'ITEЗ'. https://itez.com.ua/10-cybersecurity-threats-small-businesses-prevention.html

Єльчанінов Данило Олексійович
Студент групи УБД-41

АНАЛІЗ ТА ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДІВ ТА ІНСТРУМЕНТІВ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У цій тезі я надав оцінку ефективності сучасних методів та інструментів аудиту інформаційної безпеки, а також підкреслив важливість інтеграції технологій з процесами та практиками безпеки в організації. Також, я написав загальний висновок про те, як ці методи та інструменти впливають на ефективність аудиту інформаційної безпеки і важливість ролі експертів у цьому процесі.

Аудит інформаційної безпеки є важливою частиною управління інформаційною безпекою в сучасних організаціях. Сучасні методи та інструменти аудиту інформаційної безпеки можуть виявляти порушення безпеки, оцінювати ризики , розробляти стратегії запобігання , грати важливу роль у забезпеченні безпеки даних та інфраструктури організації. Однак, важливо розуміти, що аудит безпеки - це не просто застосування інструментів, але і системний підхід до управління ризиками та безпекою, що включає в себе

інтеграцію технологій з процесами та практиками безпеки в організації. Ефективність аудиту інформаційної безпеки полягає в поєднанні високоякісних технологій та методів, забезпечення співпраці та комунікації в організації, а також в усвідомленні важливості безпеки для керівництва та співробітників.

Серед багатьох методів аудиту ІБ є такі що дозволяють зменшити участь людини у процесах забезпечення ІБ. Такі інструменти роблять сканування вашої інфраструктури, автоматично аналізуючи журнали подій і виявляючи вразливості. Поведінковий аналіз дозволяє оперативно реагувати на загрози, які можуть бути невідомі традиційному антивірусному програмному забезпеченню. Це робить перевірки швидшими та точнішими.

Існуючі підходи можуть надавати детальну інформацію про стан системи та ризики, що допомагає приймати обґрунтовані рішення тим сами підвищуючи точність інформації.

Централізований моніторинг і управління дозволяють поєднувати дані з різних джерел і відстежувати їх в єдиному інтерфейсі. Це полегшує керування та аналіз інформаційної безпеки. У той же час штучний інтелект використовується для аналізу великих обсягів даних і виявлення найменших загроз. Це особливо корисно для реагування на нові, раніше невідомі загрози. Деякі інструменти, такі як, забезпечення відповідності спеціально розроблені для відповідності законодавству та стандартам безпеки, допомагаючи організаціям виконувати нормативні вимоги .

Хоча інструменти важливі, ефективність аудиту інформаційної безпеки також залежить від кваліфікації та досвіду експертів, які аналізують зібрані дані та розробляють план безпеки.

Загалом, аудит інформаційної безпеки є важливим і незамінним інструментом для забезпечення захисту даних та інформаційної інфраструктури організації. Використання нових підходів та інструментів сприяє підвищенню ефективності цього процесу і забезпеченню безпеки організації в умовах зростаючих загроз у сфері інформаційної безпеки.

Перелік посилань:
1)*АУДИТ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ*
Навчальний посібник. Автор: КАЧИНСЬКИЙ А.Б.
2) АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
https://kr-labs.com.ua/service/cybersecurity/audyt-informatsijnoyi-bezpeky/
3) КАБІНЕТ МІНІСТРІВ УКРАЇНИ ПОСТАНОВА
від 24 березня 2023 р. N 257
«Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури»

Єрьоменко Микита Олексійович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ НА РІЗНИХ РІВНЯХ: ІНДИВІДУАЛЬНИЙ, КОРПОРАТИВНИЙ, ДЕРЖАВНИЙ

В сучасному цифровому світі забезпечення кібербезпеки на різних рівнях стає все більш важливим завданням. Інформаційна безпека є дуже важливою і стосується кожної сфери нашого життя, від особистого використання смартфонів до захисту національної кіберінфраструктури. Тому знання та розуміння загальних ризики та викликів, які ставлять під загрозу безпеку даних та інформаційних систем на всіх рівнях суспільства, є дуже важливим та необхідним вмінням в реаліях сьогодення.

На сьогоднішній день є декілька рівнів або груп кібербезпеки. Вони поділяють охоплення безпеки інформаційної системи за кількістю людей залучених в цю систему.

Найменшим та неподільним є рівень «індивідуальний», який описує безпеку індивідуума в сфері інформаційних технологій.

Наступний по охоплюваності є рівень «корпаративний». В цю категорію входять всі інформаційні системи від малих бізнесів, які складаються з декількох комп'ютерів об'єднаних в систему, і закінчуючи великими корпораціями, які мають розгалужену мережу обчислювальних ресурсів та складний інформаційний стек.

Найбільшим рівнем по охопленню є «державний». На державному рівні інформаційні системи становлять важливу складову для забезпечення національної безпеки і функціонування державних органів. Цей рівень включає в себе інформаційні системи, які використовуються державними органами, агентствами та установами для вирішення різних завдань, таких як: захист національної безпеки, адміністрування публічних послуг, військові операції, зберігання та обробка конфіденційної інформації та багато інших.

Важливість забезпечення кібербезпеки на різних рівнях:

Захист особистої інформації на індивідуальному рівні є дуже вадливим, так як на якості кібербезпечності індивідів будується кібербезпека вищих рівнів. Окрім цього, в інтернет-світі, де особиста інформація може бути використана для багатьох цілей, контроль несанкціонованого доступу до систем та пристроїв є дуже важливим.

Важливість зберігання конфіденційності на корпоративному та державному рівні є очевидною, бо отримання несанкціонованого доступу до інформації про користувачів та клієнтів компанії, або отримання доступу до критичної інфраструктури країни може призвести до значних збитків як для компанії, так і для країни.

Для уникнення можливих ризиків безпеки та підвищення загальної цілісності та стабільності кібербезпеки в сфері інформаційних технологій на всіх рівнях треба проводити наступні заходи:

1. Використовувати сильні паролі та багаторівневу автентифікацію.

На індивідуальному рівні це означає - не використовувати прості та однотипні паролі в повсякденних сервісах, а також використовувати менеджери зберігання паролів для легкого та надійного керування ними.

кількість символів	містить тільки цифри	малі літери	великі і малі літери	цифри, великі і малі літери	цифри, великі і малі літери, символи
4	Миттєво	Миттєво	Миттєво	Миттєво	Миттєво
5	Миттєво	Миттєво	Миттєво	Миттєво	Миттєво
6	Миттєво	Миттєво	Миттєво	1 сек	5 сек
7	Миттєво	Миттєво	25 сек	1 хвилина	6 хвилин
8	Миттєво	5 сек	22 хвилини	1 година	8 годин
9	Миттєво	2 хвилини	19 годин	3 дні	3 тижні
10	Миттєво	58 хвилин	1 місяць	7 місяців	5 років
11	2 сек	1 день	5 років	41 рік	400 років
12	25 сек	3 тижні	300 років	2т років	34к років
13	4 хвилини	1 рік	16к років	100к років	2млн років
14	41 хвилина	51 рік	800к років	9млн років	200млн років
15	6 годин	1к років	43млн років	600млн років	15млрд років
16	2 дні	34к років	2млрд років	37млрд років	1трлн років
17	4 тижні	800к років	100млрд років	2трлн років	93трлн років
18	9 місяців	23млн років	6трлн років	100трлн років	7квадрильйонів

Рис.1. Залежність паролю від кількості та різноманітності використаних символів

На корпоративному та державному рівні рівні це також включає в себе створення політик використання паролів, які будуть описувати основні характеристики яким має відповідати пароль, щоб бути достатньо надіним.(1) А також, не мало важливим є перевірка та впевненість виконання та цих політик робітниками.

2. Регулярно оновлюйте програмне забезпечення.

Одним з найважливіших для всіх рівнів є оновлення програмного забезпечення яке використовується індивідом, компанією, органами державної влади, так як в застарілих версіях можуть бути уразливості, які будуть використані зловмисниками. (2)

3. Навчіться виявляти фішинг та інші загрози.

Прийнято вважати, що найуразливішою ланкою в інформаційній мережі є людина. Тому дуже важливо, як для індивіда, так і для компаній, бути обізнаним про різні методи соціальної інженерії, які можуть бути використані зловмисниками. (3)

Для корпоративного та державного рівня це означає проведення навчальних та лекційних заходів, направлених на підвищення пильності та обізнаності працівників про можливі методи фішингі та соціальної інженерії.

Підводячи підсумок, треба сказати що забезпечення кібербезпеки на індивідуальному, корпоративному та державному рівнях є критично важливим завданням на сьогоднішній день. Такі прості заходи як сильні паролі, оновлення програмного забезпечення та навчання виявленню кіберзагроз, допомагають підвищити загальний рівень інформаційної безпеки на всіх рівнях.

Перелік посилань:

1. CYBERSECURITY INSIGHTS a NIST blog URL: https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-awareness-month-2022-using-strong-passwords-and-password (дата звернення 10.10.2023)

2. Cybersecurity Best Practices URL: https://www.cisa.gov/topics/cybersecurity-best-practices (дата звернення 13.10.2023)

3. How to Recognize and Avoid Phishing Scams URL: https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (дата звернення 16.10.2023)

Журавель Антон Васильович
Студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ УПРАВЛІННЯ БЕЗПЕКОЮ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ ФАЕРВОЛУ PALO ALTO

В сучасному інформаційному світі, де комп'ютерні мережі є життєво важливою складовою бізнес-інфраструктури, захист корпоративної мережі від загроз стає критично важливим завданням. Технологія управління безпекою на основі файерволу Palo Alto виявляється потужним інструментом для забезпечення безпеки корпоративних мереж. Ця технологія надає підприємствам можливість побудувати надійний оборонний бар'єр, що блокує потенційно шкідливий трафік та забезпечує високий рівень безпеки.

Важливою особливістю технології файерволу Palo Alto є її здатність розпізнавати та блокувати різноманітні загрози, включаючи віруси, вразливості, фішинг та інші види атак. Ця платформа використовує високорівневий аналіз мережевого трафіку та поєднує різноманітні методи безпеки для забезпечення високого рівня захисту. Це дозволяє компаніям створити непроникний бар'єр перед потенційними атаками і вірусами, навіть перед тими, як вони стануть загрозою.

Файервол Palo Alto надає можливість компаніям налаштовувати правила доступу та контролювати мережевий трафік. За допомогою цієї технології можна встановлювати обмеження доступу до конкретних ресурсів та додатків, встановлювати політики безпеки та здійснювати детальний контроль над мережею. Це допомагає підвищити продуктивність і забезпечити безпеку мережі.

Технологія файерволу Palo Alto надає можливість моніторингу та аналізу безпеки мережі в режимі реального часу. Ця можливість дозволяє виявляти та реагувати на потенційні загрози миттєво. Компанії можуть вести детальний журнал подій, аналізувати мережевий трафік та виявляти аномалії, що допомагає вчасно реагувати на інциденти та розробляти стратегії безпеки.

Застосування моделі контролю дозволяє підприємствам зменшити ризик атак, дозволяючи лише необхідні програми та блокуючи все інше. Відомі експлойти вразливостей, віруси, програми-вимагачі, шпигунські програми, ботнети та інше небажане програмне забезпечення блокуються в автоматичному режимі, а також невідомі загрози, наприклад, розширені постійні загрози, піддаються контролю.

Фаерволи Palo Alto дозволяють сегментувати дані та програми для захисту

центрів обробки даних, включаючи віртуалізовані центри обробки даних. Застосовуючи принцип нульової довіри, організації можуть створити безпеку, яка залишається непохитною. Технологія фаерволу Palo Alto дозволяє застосовувати узгоджену безпеку як в локальних мережах, так і в хмарних середовищах, забезпечуючи безпеку даних та даних користувачів незалежно від їх місцезнаходження.

Однією з ключових переваг є централізована видимість, що дозволяє оптимізувати мережеву безпеку. Дані стають активними, що дозволяє запобігати успішним кібератакам.

Фаерволи Palo Alto дозволяють ефективно виявляти та запобігати спробам викрадення облікових даних, блокуючи передачу корпоративних облікових даних на незаконні веб-сайти. Також нейтралізується можливість зловмисників використовувати викрадені облікові дані для незаконного доступу та компрометації мережі завдяки політикам автентифікації на мережевому рівні.

Перелік посилань:

- PAN-OS Web Interface Reference URL: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/web-interface-basics/firewall-overview (дата звернення: 26.09.2023)
- Next Generation Firewall URL: https://www.paloaltonetworks.com/network-security/next-generation-firewall (дата звернення: 02.10.2023)
- Palo Alto Networks overview URL: https://techexpert.ua/it-products/palo-alto/ (дата звернення: 10.10.2023)

Загиней Антон Юрійович
аспірант, ННІЗІ, ДУІКТ, Київ, Україна

ПОРІВНЯННЯ АРХІТЕКТУР «КЛІЄНТ-СЕРВЕР» ТА «ПУБЛІКАЦІЯ-ПІДПИСКА» В ПИТАННІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ У СИСТЕМАХ З ТЕХНОЛОГІЄЮ ТУМАННИХ ОБЧИСЛЕНЬ

Для створення інформаційно-комунікаційних систем за технологією туманних обчислень можуть використовуватися різноманітні пристрої з власними операційними системами, програмним забезпеченням, тощо. Об'єднання їх в одну систему потребує використання спільних засобів зв'язку, які б були прийнятними для усіх елементів. У даній роботі розглянуті основні архітектури обміну інформацією, протоколи, використання яких забезпечує стабільну та надійну передачу інформації між різноманітними пристроями. Основний акцент порівнянні двох архітектур для подальшої їх оцінки щодо надійності функціонування та забезпечення безпеки систем.

Стрімкий розвиток інформаційних технологій збільшує використання активних пристроїв які генерують, оброблять та зберігають величезну кількість інформації. Це у свою чергу забезпечує постійний розвиток інтернет речей (IoT), які тим чи іншим чином підвищують ефективність людської праці. Натомість, різноманітність IoT у своїй природі, створює виклики для архітекторів інформаційних систем, програмістів, з питань об'єднання їх та використання як

єдиної системи. Обмін інформацією між IoT забезпечується використанням різних протоколів та технологій, що у свою чергу потребує належного захисту цих засобів зв'язку.

Загалом для обміну інформацією між різними пристроями в інформаційно-комунікаційних системах, які побудовані з використанням технології туманних обчислень використовуються архітектури «клієнт-сервер» та «публікація-підписка». «Клієнт-серверна» архітектура реалізується шляхом надсилання запитів від клієнта до сервера, його обробка на стороні сервера, та відправка відповіді клієнту назад. У випадку направлення декількох запитів одночасно, вони вибудовуються у чергу та виконуються послідовно. У разі надання одному запиту вищої пріоритетності з поміж інших, він виконується позачергово. У архітектурі «публікація-підписка» не здійснюється прямого направлення запиту від клієнта до сервера, натомість сервер розділяє та «публікує» інформацію в залежності від класу, а клієнти виявляють зацікавленість конкретному класу та отримують лише дані які підпадають під цю категорію. Відповідно протоколи обміну інформацією між різними системами реалізують одну з цих архітектур.

Для детальнішого розгляду архітектури «клієнт-сервер» розглянемо протокол HTTP (Hypertext Transfer Protocol) – це версія протоколу, яка є і довгий час залишається найпопулярнішим засобом передачі інформації між різними пристроями, службами, сервісами, тощо. Їх використання в IoT є дещо складнішим з ряду причин. Під час обміну інформацією між IoT у більшості випадків ми взаємодіємо не з великими обсягами даних, що сповільнює швидкість передачі використовуючи HTTP/1.1 у зв'язку з постійним відкриттям та закриттям TCP-з'єднань, натомість HTTP/2.0 надає нам змогу забезпечити багато одночасних передач через одне з'єднання за рахунок швидкої та економічної техніки стиснення пам'яті. Ця властивість особливо приваблива для IoT, оскільки вони значно зменшують розмір пакета, роблячи його більш прийнятною альтернативою.

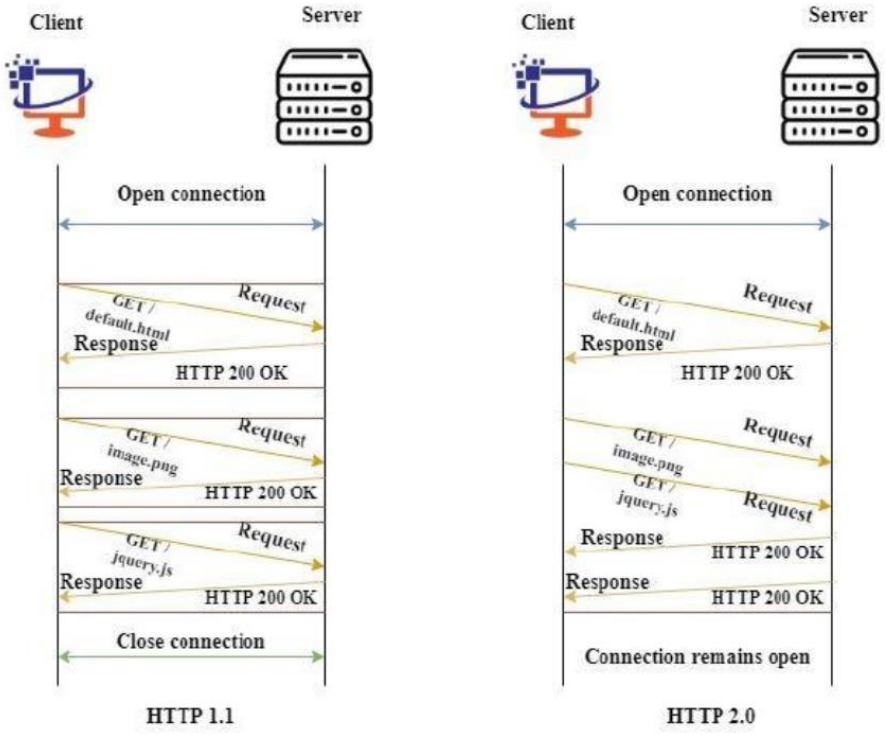


Рис. 2. Різні версії HTTP

Конфіденційність обміну у протоколі можлива з використанням TLS. Рукостискання TLS є першим етапом захисту передачі даних клієнт-сервер. Після цього клієнти та сервер передають облікові дані, які використовують узгоджений механізм обміну ключами шифрування. Надійність протоколу HTTP забезпечується за рахунок використання транспортного протоколу TCP, який особливо зручний для передачі великих обсягів даних, що у випадку з IoT буває не дуже часто.

Для огляду архітектури «публікація-підписка» розглянемо протокол MQTT. MQTT – це протокол, який працює на прикладному рівні, розроблений для зв'язку M2M (машина-машина) для пристроїв які мають обмежені ресурси та мережі з низькою пропускною здатністю. Це яскравий представник парадигми «публікація-підписка» з трьома компонентами: два типи клієнтів (видавник та підписник) та один сервер – брокер. Видавці передають повідомлення які розподілені за класами, а підписники отримують ці повідомлення якщо вони підписані на цей клас через брокера. Особливістю є те, що видавнику не потрібні адреси підписників для надсилання інформації. Також необхідно зазначити що MQTT має можливість зберігати певні дані для нових клієнтів за допомогою спеціальних позначок у широкомовному повідомленні. Якщо нікого не цікавить клас певного повідомлення, оновлення якого публікує видавник, брокер видалить опубліковані повідомлення. Додавання спеціальних позначок спрямовує брокера зберігати завантажене повідомлення, щоб потенційні клієнти могли його отримати.

Захист інформації яка передається протоколом MQTT по аналогії з HTTP можливий з використанням шифрування TLS. Також TLS може забезпечити автентифікацію пристроїв використовуючи сертифікати. Що стосується

забезпечення доступності, то MQTT підтримує три рівні QoS, зокрема 2 рівень може забезпечити гарантовану доставку навіть у випадку втрати з'єднання.

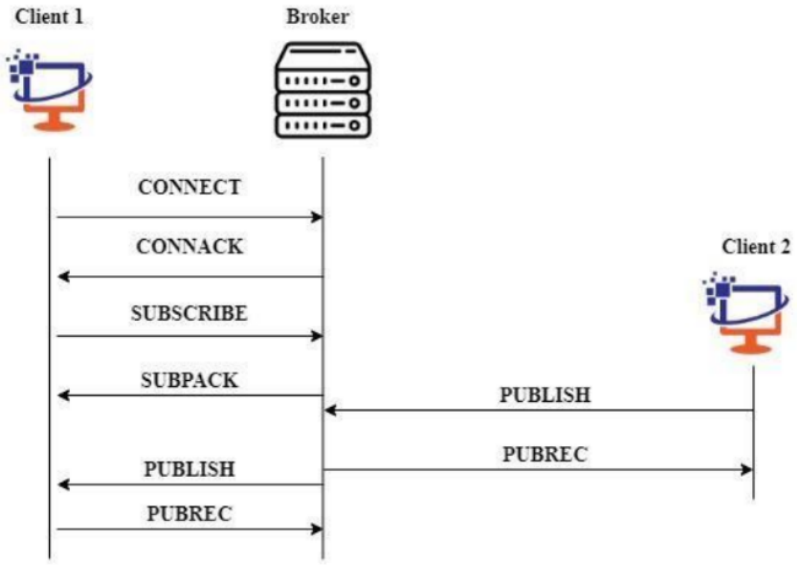


Рис. 2. Потік повідомлень у MQTT

Обидві архітектури можуть бути надійними у системах з туманними технологіями, проте вибір залежить від конкретних вимог та потреб системи. «Клієнт-серверна» архітектура забезпечує централізований контроль, простоту реалізації та управління, натомість висуває високі вимоги до пропускної здатності та має одну точку відмови (Single Point of Failure), що в цілому надає змогу забезпечити безпеку даних які передаються. Натомість архітектура «публікація-підписка» забезпечує асинхронність та розподіленість, що дозволяє краще забезпечити доступність системи, однак явним недоліком є складність управління та забезпечення конфіденційності оброблюваної інформації. Дане дослідження можна використати для більш глибокого вивчення надійності архітектур та розробки їх практичних реалізацій у системах з використанням туманних обчислень.

Перелік посилань:

1. Kadhim, O. N., Ketab, A. S., Obaid, A. J., Albermany, S. A., Raheem, A. R., & Hussien, N. A. (2023). Simulation Secure MQTT Protocol Based on TLS in IoT-Fog Computing Environment. У Proceedings of Fourth Doctoral Symposium on Computational Intelligence (с. 13–21). Springer Nature Singapore. https://doi.org/10.1007/978-981-99-3716-5_2
2. Katal, A., & Sethi, V. (2022). Communication Protocols in Fog Computing: A Survey and Challenges. У Fog Computing (с. 153–170). Chapman and Hall/CRC. https://doi.org/10.1201/9781003188230-11
3. MILOŠEVIĆ, M., MLADENOVIĆ, V., & PEŠOVIĆ, U. (2021). Evaluation of HTTP/3 Protocol for Internet of Things and Fog Computing Scenarios. Studies in Informatics and Control, 30(3), 75–84. https://doi.org/10.24846/v30i3y202107

Катков Юрій Ігорович
доктор технічних наук, професор кафедри комп'ютерних наук, ННІТ, ДУІКТ, Київ, Україна
Березовська Юлія Володимирівна
доктор філософії, доцент кафедри комп'ютерних наук, ННІТ, ДУІКТ, Київ, Україна
Заднепрянець Олександр Юрійович
студент групи КНДМ-62, ННІТ, ДУІКТ, Київ, Україна

ДОСЛІДЖЕННЯ СПОСОБІВ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МОНІТОРИНГУ ІТ-ІНФРАСТРУКТУРИ

Застосування штучного інтелекту (ШІ) для моніторингу ІТ-інфраструктури у сучасних організаціях стало необхідністю для забезпечення надійності та продуктивності комп'ютерних систем і мереж. ШІ дозволяє автоматизувати і покращити процеси моніторингу, аналізу даних і реагування на події, що відбуваються в ІТ-середовищі. Одним зі способів застосування штучного інтелекту (ШІ) для моніторингу ІТ-інфраструктури є виявлення аномалій і відхилень.

Ключові слова: кібербезпека, моніторинг ІТ-інфраструктури, виявлення вразливостей і кіберзагроз, штучний інтелект.

1. Моніторинг метрик.

Один з ключових способів застосування ШІ у моніторингу ІТ-інфраструктури полягає в аналізі метрик. ІТ-системи та мережі генерують величезну кількість метрик, таких як використання центрального процесора, величина пам'яті, мережевий трафік, завантаження диска і багато інших. ШІ може автоматично аналізувати ці метрики в реальному часі та визначати аномалії. Наприклад, система може виявити, що використання центрального процесора на сервері раптово зросло до максимуму, що може свідчити про проблеми з програмними додатками або несправність обладнання. ШІ може автоматично сповістити адміністраторів про цю аномалію та надати додаткову інформацію для розслідування.

Такий підхід дозволяє оперативно реагувати на потенційні проблеми та зменшує час, необхідний для їх вирішення. Окрім того, ШІ може виявити навіть найменш помітні аномалії, які важко виявити вручну.

Прикладами систем моніторингу метрик є такі:

Dynatrace пропонує автоматизовану систему моніторингу, яка використовує штучний інтелект для аналізу метрик та виявлення аномалій у реальному часі [2];

New Relic надає засоби для моніторингу продуктивності та метрик додатків у хмарному середовищі, а також для виявлення аномалій [7].

2. Аналіз логів.

Лог-файли є ще одним важливим джерелом інформації для моніторингу. Вони містять журнали подій, помилок та інших важливих даних, які дозволяють виявляти аномалії та відхилення в роботі системи. ШІ може аналізувати ці логи автоматично і виявляти несправності або незвичайну активність. Наприклад, велика кількість підрядкових помилок в логах може бути ознакою проблеми в програмному коді або конфігурації системи. ШІ може виявити це і надіслати

сповіщення, дозволяючи операторам швидко реагувати на ситуацію. Крім того, ШІ може аналізувати велику кількість логів, що людині було б досить важко зробити вручну. ШІ виявляє складні взаємозв'язки та патерни, які вказують на проблеми або потенційні загрози безпеці.

Прикладами систем аналізу логів є:

Splunk – це платформа для аналізу даних, включаючи журнали подій та логи [1];

IBM QRadar – це система безпеки та інформаційної безпеки, яка включає в себе засоби для агрегування логів, кореляції подій та виявлення аномалій [3].

3. Виявлення вразливостей і кіберзагроз.

OpenVAS (Open Vulnerability Assessment System) – це відкрита система сканування вразливостей, яка використовує штучний інтелект для аналізу системи на предмет вразливостей. Вона може сканувати мережі, веб-додатки та інші складові інфраструктури для виявлення потенційних проблем безпеки [6].

SIEM (Security Information and Event Management) системи: SIEM системи, такі як Splunk, IBM QRadar, або Elastic SIEM, використовують штучний інтелект для аналізу журналів подій та виявлення незвичайної активності, яка може свідчити про вторгнення або інші кіберзагрози [4]. Вони можуть визначати зв'язки між різними подіями та генерувати попередження.

Деякі антивіруси використовують методи машинного навчання для виявлення нових видів вірусів та кіберзагроз, які можуть бути менш очевидними для традиційних сигнатурних методів виявлення. Наприклад, ESET NOD32 Antivirus використовує машинне навчання для виявлення нуль-денних загроз [5].

Висновок.

За допомогою ШІ можна проводити аналіз системи на предмет вразливостей і потенційних кіберзагроз. Алгоритми машинного навчання можуть аналізувати великі обсяги даних, включаючи дані про патерни атак і несправності у програмному забезпеченні. Наприклад, ШІ може виявити незвичайну активність, яка може бути пов'язана зі спробами вторгнення або атаками, і надати попередження адміністраторам для подальшого реагування.

Це особливо важливо в умовах зростаючої кількості кіберзагроз і необхідності забезпечення безпеки інфраструктури.

Загалом, використання штучного інтелекту для виявлення аномалій і відхилень у моніторингу IT-інфраструктури дозволяє покращити надійність та безпеку системи, автоматизувати процеси аналізу даних і реагування на події, що відбуваються в IT-середовищі, й підвищити продуктивність адміністраторів та інженерів.

Перелік посилань:

1. Центр ресурсів Splunk https://www.splunk.com/en_us/resources.html
2. Центр ресурсів Dynatrace https://www.dynatrace.com/resource-center
3. Центр ресурсів IBM Security® QRadar® SIEM https://www.ibm.com/products/qradar-siem/resources
4. What is SIEM (Security Information and Event Management)? https://www.elastic.co/what-is/siem
5. Енциклопедія Інтернет-загроз https://www.eset.com/ua/support/information/entsiklopediya-ugroz/
6. Форум розробника OpenVAS https://forum.greenbone.net/
7. Центр ресурсів New Relic https://newrelic.com/resources

Залива Віталій Вікторович
старший викладач кафедри ІПЗ, ННІЗІ ДУІКТ, Київ, Україна

ОСНОВНІ ВРАЗЛИВОСТІ ВЕБ-КОМПОНЕНТІВ БЕЗ ВИКОРИСТАННЯ SHADOW ROOTS

Веб-компоненти, які не використовують Shadow roots, можуть бути піддані ряду вразливостей, що стосуються ізоляції стилів, конфліктів імен та непередбачуваної взаємодії з глобальними стилями та скриптами. Ця презентація розглядає ключові вразливості, які можуть виникнути при відсутності Shadow DOM в архітектурі веб-компонентів, а також надає рекомендації щодо їх уникнення та мінімізації потенційних ризиків.

Веб-компоненти, які не використовують Shadow roots, можуть стикатися з численними викликами та вразливостями. Один з основних викликів — це відсутність ізоляції стилів. Без Shadow roots, стилі веб-компонента можуть непередбачувано взаємодіяти з глобальними стилями сторінки. Це може призвести до конфліктів, коли глобальні стилі випадково застосовуються до компонентів, порушуючи їх дизайн та функціональність.

Додатково, відсутність ізольованого простору імен може призвести до конфліктів між ідентифікаторами та класами, що використовуються у веб-компонентах та на головній сторінці. Ці конфлікти можуть зробити код менш стабільним і відтак збільшити ймовірність помилок.

Ще однією проблемою є взаємодія веб-компонентів з глобальними скриптами. Скрипти, які виконуються на головній сторінці, можуть випадково впливати на веб-компоненти, змінюючи їх поведінку або взаємодію.

Безпека також є великим питанням. Відсутність ізольованого контексту може збільшити ризик атак, таких як XSS. Зловмисники можуть спробувати використовувати вразливості веб-компонентів для виконання шкідливого коду на сторінці.

Останнім, але не менш важливим, є питання доступності. Глобальні стилі та скрипти можуть негативно впливати на доступність веб-компонентів, роблячи їх менш доступними для користувачів з особливими потребами.

Для вирішення цих проблем рекомендується використовувати Shadow DOM, якщо це можливо, для ізоляції стилів, скриптів та розмітки. Також важливо використовувати унікальні префікси для класів та ідентифікаторів, регулярно тестувати веб-компоненти на вразливості та забезпечувати навчання розробників щодо потенційних вразливостей та найкращих практик їх уникнення.

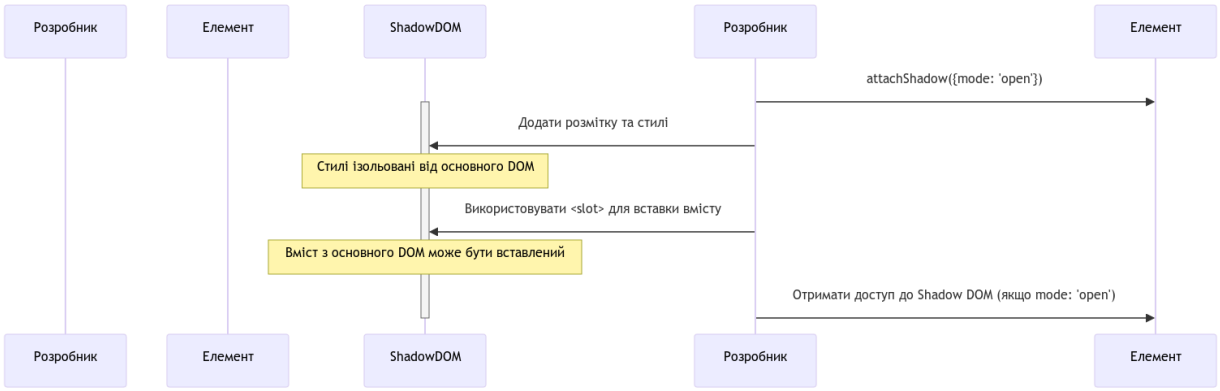


Рис.1. Структура Shadow roots

Для вставки Shadow roots на сторінку, ви можете створити новий Shadow DOM на будь-якому елементі DOM. Ось базовий приклад того, як це можна зробити:

```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <title>Shadow DOM Example</title>
</head>
<body>
   <div id="shadowHost"></div>
   <script>
// Отримуємо елемент, на якому хочемо створити Shadow DOM
const shadowHost = document.getElementById('shadowHost');
// Створюємо Shadow root на цьому елементі
const shadowRoot = shadowHost.attachShadow({ mode: 'open' });
// Додаємо розмітку та стилі в Shadow DOM
shadowRoot.innerHTML = `
   <style>
      p {
         color: blue;
         font-size: 20px;
      }
   </style>
   <p>Цей контент знаходиться у Shadow DOM!</p>
`;
         </script>
</body>
</html>
```

Коли ця сторінка буде відкрита у веб-браузері, то з’явиться текст "Цей контент знаходиться у Shadow DOM!" з синім кольором. Текст і стилі для нього ізольовані в межах Shadow DOM, і вони не впливають на зовнішній DOM.

Веб-компоненти без використання Shadow roots можуть зіткнутися з

численними викликами, зокрема з проблемами ізоляції стилів, що може призвести до непередбачуваних взаємодій з глобальними стилями. Відсутність ізольованого простору імен може викликати конфлікти іменування, а глобальні скрипти можуть неправильно взаємодіяти з такими веб-компонентами. Додатково, відсутність ізольованого контексту може збільшити ризик безпеки, особливо від атак типу XSS. Тому важливість Shadow DOM полягає в його спроможності ізолювати розмітку, стилі та логіку, забезпечуючи стабільність та консистентність веб-компонентів.

Перелік посилань:

1. Eric Bidelman. Shadow DOM v1: Self-Contained Web Components. URL: https: //web.archive.org/web/20191014084634/https://developers.google.com/ web/fundamentals/web-components/shadowdom (дата звернення: 25.10.2023).
2. Manuel Eberl et al. Archive of Formal Proofs. URL: https://www.isa-afp.org (дата звернення: 24.10.2023).

Капелюшна Тетяна Вікторівна, доцент кафедри управління інформаційною та кібернетичною безпекою, ННІЗІ ДУІКТ, Київ, Україна
Іванов Данило Андрійович, студент групи УБДМ_61, ННІЗІ ДУІКТ, Київ, Україна

ВРАХУВАННЯ РЕПУТАЦІЙНИХ РИЗИКІВ ПРИ УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ КОМПАНІЇ

Нинішні умови характеризуються особливою небезпекою у всіх напрямках діяльності компаній, оскільки сформованим загрозам передувала низка подій, таких як: пандемія, прискорення цифровізації, геополітичні конфлікти.

Перехід бізнесу у діджитал-середовище призвів до появи викликів інформаційній безпеці підприємства, посилилася конкурентна боротьба, збільшилася ймовірність виникнення репутаційних ризиків, тому гостро постало питання щодо забезпечення інформаційної безпеки компанії. Джерела появи репутаційних ризиків розширилися із переходом бізнесу у цифровий простір з одночасною простотою розміщення в інформаційному просторі недостовірної, викривленої, упередженої інформації та поширенням кіберзлочинності щодо функціонування підприємств.

Управління репутаційними ризиками має включатися як важливий напрям для пошуку дієвих засобів у забезпеченні інформаційної безпеки компанії.

Репутаційні ризики в процесі їх реалізації знижують прибуток компанії, призводять до скорочення інвестицій, а, відповідно, сповільнюють інноваційний розвиток підприємства, спричиняють скорочення доходів за рахунок відтоку клієнтів.

Ефективне управління репутаційними ризиками компанії вимагає системного підходу, що включає в себе діагностику ймовірних загроз, розробку стратегій стабілізації кризових ситуацій, взаємодію зі стейхолдерами та моніторинг репутаційних індикаторів.

У діджитал просторі функціонування компаній ускладнюється управління репутаційними ризиками через швидкість передачі та поширення інформації, тому варто реагувати на інциденти миттєво: моніторинг події - відповідь в режимі реального часу [1].

Процес управління ризиками загально включає ідентифікацію, контроль та мінімізацію невизначеності, що спричинені впливом факторів та подій, що чинять руйнівний вплив на інформаційні активи компанії. Повний ланцюг процесу управління ризику містить:

— визначення контексту (визначення інформаційного активу, стейкхолдерів);

— оцінка ризиків (визначення рівня ризику, враховуючи важливість активів, ймовірність загрози та наявність вразливостей);

— аналіз ризиків (визначення та оцінка подій, які можуть загрожувати інформаційним активам і розробка запобіжних заходів);

— розгляд ризиків (виявлення властивостей інформаційних активів, які можуть бути використані для реалізації загрози, оцінка ефективності заходів інформаційної безпеки);

— визначення ступеня допустимого ризику (ранжування ризиків за ступенем вразливості з визначенням меж його дії);

— зниження ризику (впровадження контролю для запобігання ризиків, а також реалізація заходів для відновлення в разі їхньої дії);

— інформування про ризики (доведення результатів щодо управління ризиками до всіх, хто працює з інформаційним активом, включаючи зовнішнє оточення);

— моніторинг ризиків та звітність про ризики (постійне відслідковування ризиків та ведення документації щодо отриманої інформації).

Важливо проводити саме кількісний аналіз ризику, при якому визначається функція загроз, вразливостей і можливих збитків. Таким чином, розмір збитків залежить від інформації, яка потребує захисту та ймовірності виникнення загрози [2].

При управлінні ризиками належна увага має приділятися і репутаційним ризикам, оскільки вони формують імідж та бренд компанії, у грошовому виразі можуть підвищити вартість компаній (гудвіл). Тому інвестування у забезпечення інформаційної безпеки дозволить захистити інформаційні активи, тим самим суттєво знизити ймовірність реалізації загрози й нанесення збитків компанії, щоб досягти бажаних результатів та цілей.

Управління репутаційними ризиками потребує системного та комплексного підходу, взаємодії між відділами, стейкхолдерами, які працюють з інформаційним активом, відслідковування всіх змін та факторів, що виникають під дією цифровізації в онлайн середовищі.

Репутаційні ризики та ризики інформаційної безпеки мають враховуватися при забезпеченні безпеки підприємства. Управління репутаційними ризиками в умовах динамічних змін Інтернет середовища та збільшення обсягів передачі інформації в глобальній мережі, потребує розширенням переліку ризиків та їх врахування у ланцюзі процесу управління ними.

Врахування репутаційних ризиків в умовах активної діджиталізації всіх бізнес-процесів дозволить захистити важливий для роботи компаній

інформаційний актив, тому дані ризики мають враховуватися (усіма без виключення компаніями) як складова при управлінні інформаційною безпекою.

Перелік посилань:
1. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ: НІСД, 2022. 456 с.
2. Кириленко А., Бабинюк О. Кібербезпека на захисті бізнесу. URL: https://ir.kneu.edu.ua/bitstream/handle/2018/31417/ZE_2019_118.pdf?sequence=1 (дата звернення: 12.10.2023).

Іванов-Кожевніков Артем Антонович
студент групи БСД-62, ННІЗІ ДУТ, Київ, Україна

ANDROID: ДОВІЛЬНЕ ВИКОНАННЯ КОДУ ЧЕРЕЗ КОНТЕКСТИ СТОРОННІХ ПАКЕТІВ

Існують додатки для Android, які мають можливість додавати додатковий функціонал, використовуючи зовнішні модулі. Деякі завантажують власні бібліотеки або сторонні dex-або app-файли, але в цій статті ми розглянемо модулі, які встановлюються з ринків як сторонні додатки і використовуються основним додатком як набір додаткових функцій: фільтри камери, теми, набори шрифтів і т. д. За статистикою Oversecured, принаймні один із кожних 50 популярних додатків піддається цій вразливості.

Після встановлення модуля основний додаток починає шукати його серед всіх додатків, встановлених на одному пристрої, використовуючи певні шаблони (префікс імені пакету, значення з AndroidManifest.xml). Якщо перевірка є слабкою, додаток зловмисника може бути визнаний законним модулем. На момент завантаження модуля виконується код з нього в контексті основного додатка, що призводить до виконання довільного коду. В результаті зловмисник може отримати можливість викрасти будь-які конфіденційні дані, які користувач вводить в додаток, або які додаток отримує від сервера, а також замінити ці дані, розкрити фінансові деталі та відстежувати користувача.

Суть вразливості

Такі додатки можуть сканувати пристрій наступним чином:

```
java
public static void searchModules(Context context) {
    for (PackageInfo info :
context.getPackageManager().getInstalledPackages(0)) {
        String packageName = info.packageName;
        if (packageName.startsWith("com.victim.module.")) {
            processModule(context, packageName);
        }
        //...
```

і потім працювати, взагалі небезпечно, з цими сторонніми додатками:

```
java
public static void processModule(Context context, String packageName) {
   Context appContext = context.createPackageContext(packageName,
CONTEXT_INCLUDE_CODE | CONTEXT_IGNORE_SECURITY);
   ClassLoader classLoader = appContext.getClassLoader();
   try {
      Object interface = classLoader.loadClass("com.victim.MainInterface")
            .getMethod("getInterface")
            .invoke(null);
      //...
```

У цьому прикладі вразливий додаток отримує ClassLoader будь-якого додатку, ім'я пакету якого починається із com.victim.module., намагається знайти com.victim.MainInterface і викликати його метод getInterface. Небезпека полягає в тому, що зловмисник може створити свій власний додаток із іменем пакету, яке починається із відповідного префіксу, створити вказаний клас із цим методом і включити в цей метод код, який потім виконуватиметься в контексті додатка-жертви.

```
java
package com.victim;

public class MainInterface {
   public static Object getInterface() {
      try {
         Runtime.getRuntime().exec("...команда, керована
зловмисником...").waitFor();
      } catch (Throwable th) {
      }
      return null;
   }
}
```

Фактично, додатки можуть не лише викликати методи за допомогою Java Reflection API: вони також можуть створювати екземпляри класів, отримувати значення полів тощо, що також призводить до виконання довільного коду.

Рекомендації

Доброю захистом в цьому випадку буде перевірка підпису поточного додатка і модуля. Метод може бути переписаний наступним чином:

```
java
public static void searchModules(Context context) {
   PackageManager packageManager = context.getPackageManager();
   for (PackageInfo info : packageManager.getInstalledPackages(0)) {
      String packageName = info.packageName;
      if (packageName.startsWith("com.victim.module.")
            && packageManager.checkSignatures(packageName,
context.getPackageName()) == PackageManager.SIGNATURE_MATCH) {

         processModule(context, packageName);
      }
      //...
```

Зловмиснику не вдасться підписати свій додаток тим самим сертифікатом, яким було підписано атакований додаток, що запобігає завантаженню незаконного модуля.

1. MobSF. "Mobile Security Framework". [Посилання на репозиторій] https://github.com/MobSF/Mobile-Security-Framework-MobSF
2. OWASP. "OWASP Mobile Application Security Testing Guide (MASTG)". [Посилання на репозиторій] https://github.com/OWASP/owasp-mastg
3. Oversecured Blog. [Посилання на блог] https://blog.oversecured.com/

Івахненко Кирило Володимирович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ОСНОВНІ РИЗИКИ БЕЗПЕКИ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

Анотація. Те, що література чи фільми розглядалися як можливість протягом десятиліть, сьогодні стало відчутною реальністю. Штучний інтелект вже є частиною нашого життя. Це стало однією з важливих проблем цієї епохи в розпалі машинного навчання або генеративного штучного інтелекту настільки, що штучний інтелект змінить нашу продуктивну структуру та спосіб життя. Розвиток штучного інтелекту потребує прискореної уваги до цих проблем для забезпечення безпеки та ефективного використання технології із захистом від будь-яких потенційних загроз, пов'язаних зі ШІ.

Останніми роками, особливо у 2023 році, різні організації розширили виробництво методологій і посібників, щоб зосередити увагу на ризиках безпеки штучного інтелекту та допомогти компаніям успішно їх запобігати, але зі зростанням актуальності систем штучного інтелекту та їх потенціалу для компаній і громадян, ризики безпеки ШІ стали серйозною проблемою з точки зору кібербезпеки. [1]

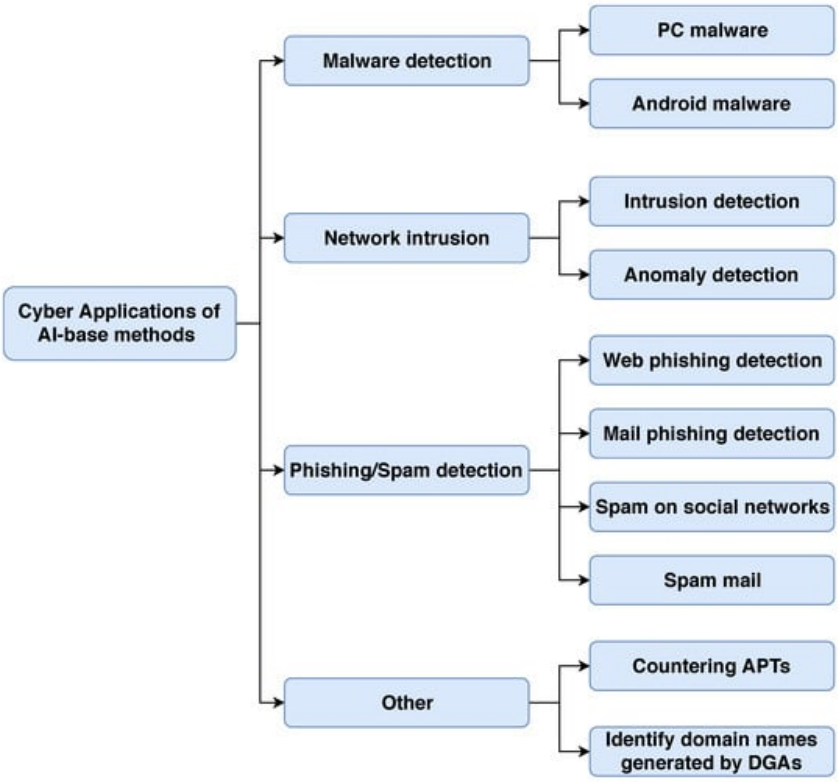


Рис. 1 - Галузі додатків кібербезпеки, які використовують методи ШІ. [1, ст. 1]

Новими та найскладнішими викликами кібербезпеці є:

- Дані, які використовуються для побудови системи штучного інтелекту, можуть невірно відображати контекст або передбачуване використання системи, а якість даних може вплинути на надійність штучного інтелекту з негативними наслідками.
- Залежність систем ШІ від даних, які використовуються для навчання.
- Зміни на етапі навчання, навмисні чи ненавмисні, можуть змінити продуктивність системи ШІ.
- Набори даних, які використовуються під час навчання ШІ, можуть застаріти після розгортання системи, що вплине на продуктивність ШІ.
- Існуюча невідповідність між масштабом і складністю систем штучного інтелекту та звичайних програмних додатків, які їх розміщують.
- Попередньо підготовлені моделі мають вирішальне значення для сприяння дослідженню штучного інтелекту та розробці високопродуктивних систем за менший час і з меншими витратами. Однак вони також можуть збільшити рівень статистичної невизначеності та спричинити зміщення та проблеми з відтворюваністю.
- Численні ризики для конфіденційності як наслідок величезної здатності систем штучного інтелекту агрегувати дані.
- Виконувати тестування безпеки програмного забезпечення на основі штучного інтелекту складніше, оскільки розробка коду штучного інтелекту

відрізняється від традиційної розробки коду, і можуть виникнути запитання щодо того, що і як тестувати. [1]

Безпека ШІ є важливою проблемою в цю епоху.

Впровадження штучного інтелекту в різні виробничі сектори та демократизація доступу до ШІ з інструментами, доступними для малих і середніх підприємств, а не лише для великих компаній, є новою віхою в технологічній революції, яку ми пережили в останні десятиліття.

Таким чином, ризики безпеки штучного інтелекту повинні бути центральними для публічних дебатів і серцевиною бізнес-стратегій .

Успішні атаки на системи ШІ можуть мати катастрофічні наслідки для компаній, які їх розробляють, а також для компаній, які їх використовують, і громадськості: викрадання приватних даних, дезінформація, втрата репутації, правові наслідки…

Тому важливо займатися безпекою штучного інтелекту протягом усього його життєвого циклу, запроваджуючи адекватні засоби контролю безпеки та проводячи постійні оцінки безпеки. [1]

Перелік посилань:

1. Які ризики безпеки AI? URL: https://www.tarlogic.com/blog/ai-security-risks/ (дата звернення: 20.10.2023)
2. Штучний інтелект у кіберсфері: напад і захист URL: https://www.mdpi.com/2073-8994/12/3/410 (дата звернення: 23.10.2023)

Іллюша Олександр Олександрович
студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ В КОРПОРАТИВНІЙ МЕРЕЖІ НА БАЗІ TREND MICRO DEEP DISCOVERY

Вимоги до мережевої безпеки

Мережа повинна лежати в основі стратегії кібербезпеки, оскільки вона охоплює усі аспекти бізнесу. Незважаючи на те, що все більше людей працюють вдома чи поза офісом, вони все одно підключаються до мережі, що є основним вектором атаки для хакерів. Переважна більшість атак, які починаються з кінцевої точки, є лише першим кроком у спробі отримати доступ до мережі через вкрадені та/або розширені облікові дані.

Сильна мережева безпека, орієнтована на периметр, необхідна для будь-якої успішної стратегії безпеки. Зупинка вторгнення або шкідливого ПЗ на кордоні мережі має вирішальне значення. Це нікого не повинно дивувати, проте багато організацій зупиняються на цьому і не беруть до уваги те, що захист, орієнтований на периметр, не здатний зупинити сучасні цільові атаки і сучасні загрози. Сучасні зловмисники дуже досвідчені і розуміють, які засоби безпеки ви використовуєте для захисту своєї мережі. Вони використовують тактику ухилення, щоб обійти навіть найкращі засоби захисту периметра.

Пейзаж загроз еволюціонує

В рамках цифрової трансформації організації переживають фундаментальні зміни у своїй діяльності.

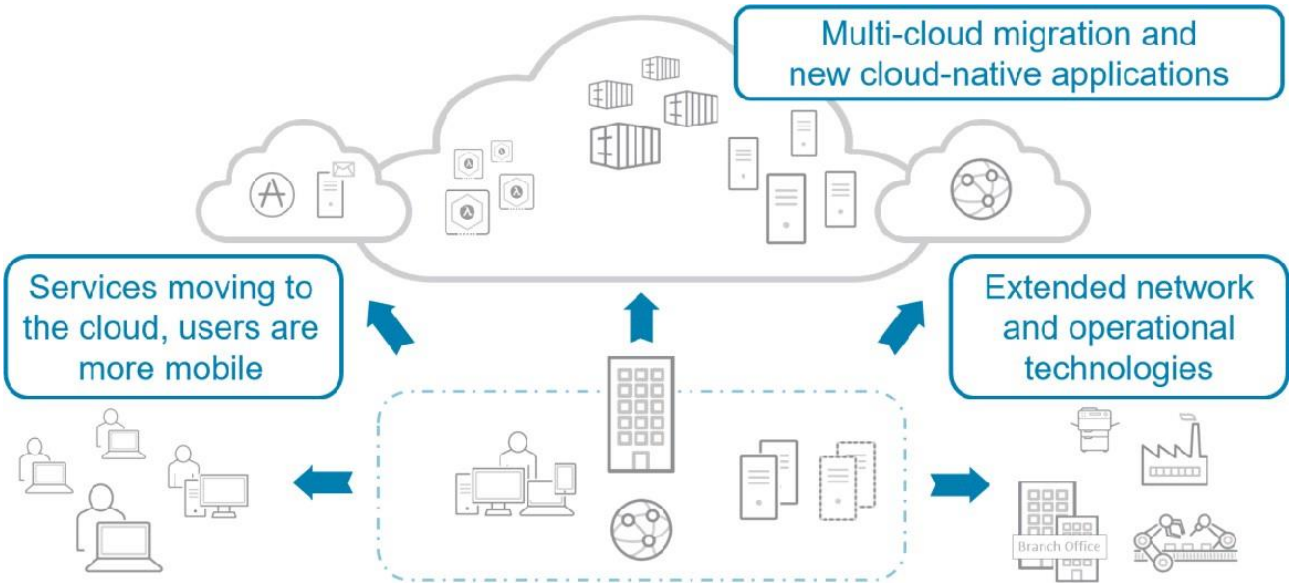


Рис.1 – Приклад фундаментальних змін (перенесення інфраструктури в хмару)

Вони переносять інфраструктуру в хмарні (і мультихмарні) розгортання, а також створюють нові, "хмарні" додатки.

Послуги, орієнтовані на користувачів (як-от електронна пошта, зберігання даних та інші), переходять у хмару, в той час як користувачі продовжують бути ще більш мобільними, ніж будь-коли.

Розширена мережа продовжує розширюватися, тепер вона охоплює хмару, а також охоплює операційні технології (IoT, IIoT), такі як розумні фабрики та багато іншого.

Це різноманітне середовище створює нові можливості для атак і ризик виникнення незакритих вразливостей.

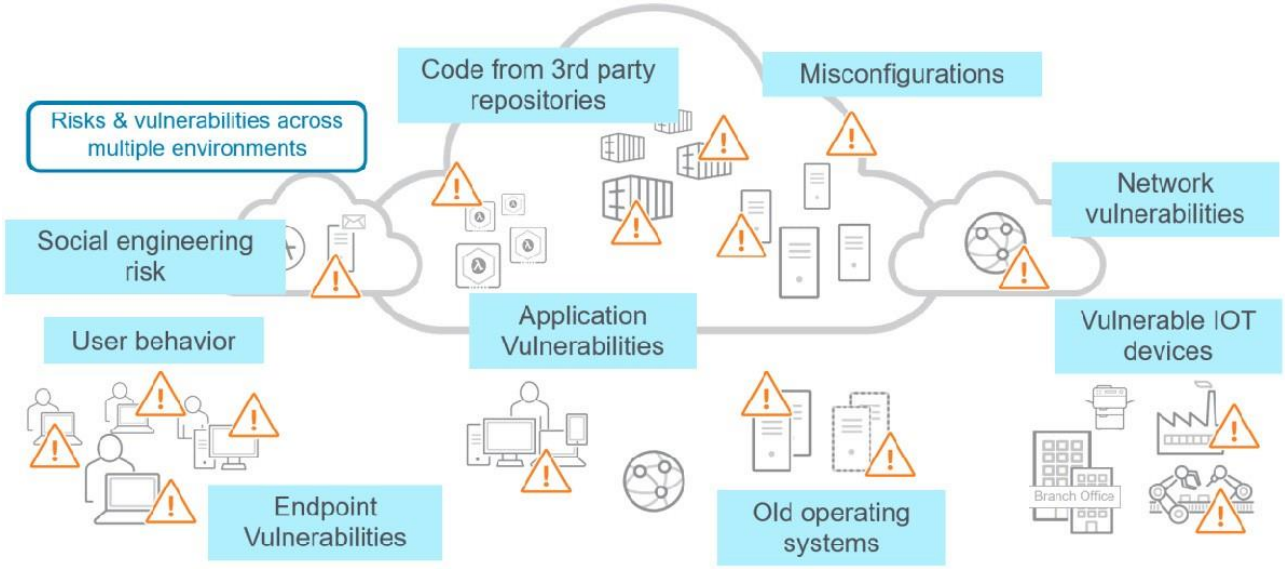


Рис. 2 – Приклад ризиків безпеки в сучасних корпоративних мережах

Потрапивши в мережу, система безпеки, орієнтована на периметр, не має

можливості спостерігати за атакою і не помічає її існування. Загроза може вільно переміщатися в бічному напрямку мережею з мінімальними шансами бути виявленою. В такому випадку необхідно провести контрзаходи для забезпечення безпеки від шкідливої активності, що поширюється мережею із заражених машин, була виявлена і відповідним чином усунена.

Виявлення та реагування на загрози в мережі (NDR) - це галузева категорія, що дедалі більше цінується та набуває більшого значення серед спеціалістів з кібербезпеки та аналітиків. Виявлення та реагування на загрози в мережі дає змогу організаціям відстежувати вхідний, вихідний і бічний мережевий трафік на предмет шкідливої активності та підозрілої поведінки. Після виявлення загрози на неї можна реагувати на мережевому рівні та за межами корпоративної мережі. Заходи реагування можуть бути автоматичними або ручними для пошуку загроз або посилення контролю.

Trend Micro Deep Discovery

Моніторинг бічного переміщення за такими протоколами, як SMB, RDP, SNMP, IRC, дуже важливий. Якщо у вас немає інструменту, який відстежує ці протоколи, ви можете бути сліпі до наявної атаки. У середньому, загроза залишається непоміченою протягом декількох місяців через стратегію безпеки, орієнтовану на периметр. Щойно загроза проникає всередину мережі, цей трафік не відстежується через припущення, що засоби захисту периметра блокують усі атаки.

Trend Micro Deep Discovery розроблений для розміщення на порту SPAN або TAP, тому він може контролювати не тільки вхідний і вихідний трафік, а й трафік, що переміщується мережею, відстежуючи понад 100 протоколів і всі порти. Такий широкий огляд допоможе запобігти вільному переміщенню невиявлених шкідливих програм мережею. Deep Discovery може ділитися своїми результатами виявлення з іншими рішеннями безпеки, такими як IPS або ж засобами захисту кінцевих точок, щоб у режимі реального часу забезпечити впровадження та усунення наслідків.

Trend Micro Deep Discovery захищає від спрямованих атак, сучасних загроз і програм-вимагачів, надаючи вам можливості для виявлення, аналізу та реагування на сучасні приховані атаки в режимі реального часу.

Перелік посилань:

1. Trend Micro Research, News, and Perspectives URL: https://www.trendmicro.com/en_us/research.html (дата звернення: 25.10.2023)

Капелюшна Тетяна Вікторівна, доцент кафедри управління інформаційною та кібернетичною безпекою, ННІЗІ ДУІКТ, Київ, Україна
Чернявський Ігор Романович, студент групи УБДМ_61, ННІЗІ ДУІКТ, Київ, Україна

ПРОБЛЕМА БЕЗПЕКИ ДАНИХ ПРИ ВИКОРИСТАННІ ХМАРНИХ СЕРВІСІВ

Бізнес-середовище нині характеризується високим ступенем діджиталізації та переходу роботи в режимі віддаленого доступу, що посилюється невизначеними умовами функціонування підприємств. Компанії збільшують ланцюги постачання послуг, так як намагаються якнайшвидше передавати інформацію та використовувати її з максимальною можливою швидкістю. Організації активно використовують хмари та хмарні сервіси для вирішення наступних завдань: відкривають інтернет-магазини, бази даних, системи управління підприємством, поштові сервери. Хмара слугує віртуальною IT-інфраструктурою, в якій можна розгорнути будь-які системи та програми компанії. З їх популярністю зростають загрози цілісності даних та з'являється потреба у додаткових засобах їх захисту.

Останніми роками по всьому світу спостерігається зростання кібератак на підприємства, а особливо урядові організації, підприємства критичної інфраструктури. Пояснення у зростанні попиту на використання хмарних сервісів, як новітнього виду мережевих послуг. Хмара дозволяє власне інформаційними засобами віртуального середовища розширити програмні та технічні ресурси пристрою користувача, які реалізуються за умов динамічного масштабного доступу до розподілених зовнішніх мережевих ресурсів.

Хмарні сервіси мають низку переваг [1]:

- користувач може задіяти віртуальний комп'ютер майже будь-якої конфігурації для виконання ресурсоємних завдань;
- може працювати в будь-якому місці за умов використання комп'ютерного пристрою, що має підключення до інтернету;
- користувач застрахований від збоїв у роботі пристрою і може за потреби ділитися результатами роботи з іншими користувачами;
- на відміну від інсталяції платних програм на окремому комп'ютері, хмарні серевси можуть використовуватися на безоплатній основі;
- зниження витрат за рахунок переведення їх на провайдера.

Однак, з активізацією використання хмарних технологій та сервісів виникає серйозна проблема, дані стають більш вразливими до загроз, виникають порушення інформаційної безпеки організацій.

В умовах невизначеності, які нині склалися в Україні, доцільно розгорнути віртуальний сервер, орендувати хмарні ресурси (віртуальна хмара (IaaS, Cloud VDS, CVDS), тобто мати виділений фізичний сервер у країнах Європи, приватний віртуальний сервер, розміщення обладнання. При чому надійність дата-центру має визначатися міжнародною класифікацією ANSI/TIA-942. Стандарт ранжує дата-центри за чотирма класами –Tier I, Tier II, Tier III, Tier IV [2] за ступенем відмовостійкості (вищий клас - менше відмов обладнання), що на пряму впливає на стабільну роботу інфраструктури.

Крім того, надважливим залишається питання захисту даних компанії, тобто організовати безпеку на рівні внутрішніх протоколів компанії, у дата-

центрі та на рівні законодавства країни, в якій розміщено хмару. При виборі найкраще керуватися міжнародною сертифікацією (сертифікат ISO/IEC 27001). Даним стандартом регулюється політика безпеки даних.

Тож, в надскладних умовах функціонування, що нині склалися в країні, необхідно приділити особливу увагу безпеці в цілому, а для підприємств та організацій - безпеці інформації та забезпеченню безпеки даних та сервісів при використанні хмарних технологій.

Перелік посилань:

3. Softwareon-demand, Platform as a service, Infrastructure as a service, Google Apps Education Edition. URL:http://www.google.com/a/help/intl/en/edu/index.html (дата звернення: 02.10.2023).

4. Захищені дата-центри у Європі. URL: https://www.sim-networks.com/ukr/company/data-centers (дата звернення: 11.10.2023).

Карпенко Владислав Русланович, БСДМ-61
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ЗЛОВМИСНОЇ АКТИВНОСТІ В ІНФОРМАЦІЙНІЙ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ IBM QRADAR DNS ANALYZER

Визначено мету і основні завдання щодо виявлення зловмисної активності в інформаційній системи організації. Розглянуто методи та засоби виявлення зловмисної активності в інформаційній системи організації. Розроблено рекомендації щодо виявлення зловмисної активності в інформаційній системи організації на базі IBM QRadar DNS Analyzer.

Під зловмисною активністю в інформаційній системі організації розуміються будь-які несанкціоновані або зловмисні дії в системі, які можуть призвести до пошкодження або компрометації інформаційних ресурсів. Виявлення зловмисної активності в інформаційній системі організації має важливе значення з багатьох причин. Так, зловмисники можуть викрасти або скомпрометувати конфіденційні дані, такі як фінансова інформація, персональні дані та комерційна таємниця. Виявляючи зловмисну активність, організації можуть запобігти витоку даних і захистити свої активи.

Використання SIEM-системи може підвищити цінність декількох невеликих за обсягом потоків даних, однак більшість коробкових SIEM мають високу вартість і дороги в обслуговуванні. В результаті, недоцільно розгортати SIEM вартістю в кілька мільйонів доларів і отримувати до 10 000 подій в день (враховуючи, що за допомогою Perl-скриптів і grep можна робити це безкоштовно) [1].

IBM QRadar DNS Analyzer – це рішення для аналізу безпеки, призначене для аналізу DNS-трафіку і виявлення потенційних ризиків безпеки або зловмисної активності. Воно дозволяє організаціям виявляти і розслідувати інциденти безпеки, пов'язані з DNS, а також допомагає їм визначати пріоритети і більш ефективно реагувати на події безпеки [2].

Деякі з ключових можливостей IBM QRadar DNS Analyzer включають [2]:

моніторинг і аналіз DNS-трафіку в режимі реального часу. Додаток може відстежувати DNS-запити і відповіді в режимі реального часу і надавати детальну інформацію про мережеву активність;

виявлення загроз на основі DNS. Додаток може виявляти різні загрози на основі DNS,

такі як DNS-тунелювання, DNS-ексфільтрація та перехоплення DNS;

інтеграція з іншими інструментами безпеки. IBM QRadar DNS Analyzer може інтегруватися з іншими інструментами безпеки, такими як брандмауери, системи виявлення вторгнень і SIEM, щоб забезпечити більш повне уявлення про загрози безпеки;

настроювані інформаційні панелі та звіти. Додаток надає настроювані інформаційні панелі і звіти, які дозволяють командам безпеки швидко виявляти і розслідувати потенційні інциденти безпеки.

В цілому, IBM QRadar DNS Analyzer є потужним інструментом для організацій, які прагнуть поліпшити свою систему безпеки DNS і знизити ризик атак на основі DNS.

Додаток IBM QRadar DNS Analyzer надає інформацію про локальний DNS-трафік організації, виявляючи зловмисну активність і дозволяючи команді фахівців з безпеки виявляти алгоритм генерування доменів (DGA), тунелювання або самовільне захоплення доменів, до яких здійснюється доступ з корпоративної мережі. Використовуючи потоки або журнали QNI з інформацією про домен з інших пристроїв, таких як DNS-сервери (BIND), проксі-сервери, веб-сервери Apache або інші BIND-сумісні пристрої, надається можливість виявляти і відстежувати вихідні запити до зловмисних сайтів. Завдяки інформаційній панелі DNS Analyzer і можливостям деталізації команда фахівців може визначати тенденції DNS і розслідувати такі дії, як спроби самозахоплення. Увімкнувши INDEXING (індексування) в обліковому записі адміністратора, можна також покращити продуктивність додатку.

Додаток QRadar DNS Analyzer призначений для того, щоб допомогти організаціям виявляти і досліджувати потенційні загрози безпеки DNS в їх мережі. Деякі з ключових функцій додатка наступні:

аналіз DNS трафіку в режимі реального часу. QRadar DNS Analyzer безперервно відстежує DNS-трафік в режимі реального часу, що дозволяє йому швидко виявляти і реагувати на потенційні загрози безпеці;

настроювані правила. Додаток поставляється з набором настроюваних правил, які можуть бути використані для виявлення і оповіщення про конкретні події DNS, які свідчать про загрози безпеці;

набори зразків. QRadar DNS Analyzer включає в себе попередньо налаштовані еталонні набори, які можна використовувати для виявлення відомих DNS-загроз і підозрілих доменних імен;

створення порушень. Додаток може автоматично генерувати порушення в QRadar при виявленні загроз безпеці DNS, що дозволяє командам безпеки швидко розслідувати і реагувати на потенційні інциденти;

ієрархія мережі. Додаток можна налаштувати на моніторинг певних сегментів мережі, що дозволяє організаціям зосередити свої зусилля з моніторингу там, де вони найбільш необхідні;

інтеграція з іншими інструментами безпеки. QRadar DNS Analyzer може бути інтегрований з іншими інструментами безпеки, такими як SIEM, щоб забезпечити більш повне уявлення про мережеву безпеку.

Необхідно зазначити, що QRadar DNS Analyzer є потужним інструментом для виявлення і пом'якшення загроз безпеки DNS, а його настроювані правила, набори посилань і можливості виявляти зловмисну активність роблять його цінним доповненням до арсеналу безпеки будь-якої організації.

Отже, технологія виявлення зловмисної активності в інформаційній системи організації на базі QRadar DNS Analyzer надає додаткові можливості щодо виявлення зловмисної активності в інформаційній системі організації. Правильне налаштування параметрів даного додатка забезпечить ефективне виявлення та своєчасне реагування на наявну зловмисну активність в мережі організації.

Перелік посилань:

1. MITRE. Ten Strategies of a World-Class Cybersecurity Operations Center. /Carson Zimmerman –The MITRE

Corporation, 2014. – 346 p.

2. QRadar DNS Analyzer app. Last Updated: 2023-03-21. IBM. Available online: https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-dns-analyzer-app.

Качний Кирило Сергійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ТА ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ І РЕАГУВАННЯ НА ЗАГРОЗИ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ.

В сучасному цифровому світі корпоративні інформаційні системи зазнають зростаючого тиску від кіберзлочинців та загроз, які стають все більш виразними і удосконаленими. Для захисту цих систем і даних в них необхідні вдосконалені методи виявлення та реагування на загрози. У цьому контексті використання машинного навчання та штучного інтелекту стає важливою стратегією для виявлення, прогнозування та нейтралізації кіберзагроз.

Машинне навчання та штучний інтелект надають корпоративним інформаційним системам здатність аналізувати величезний обсяг даних, ідентифікувати аномалії та надзвичайні події, а також прогнозувати можливі загрози з високою точністю. Завдяки навчанню на даних та алгоритмам, інтелектуальні системи можуть навчатися на льоту, адаптуватися до нових видів атак та постійно покращувати ефективність своїх заходів забезпечення безпеки.

Застосування машинного навчання та штучного інтелекту для виявлення і реагування на загрози в корпоративних інформаційних системах має декілька переваг. Вони включають в себе підвищену швидкість реагування на загрози, зниження кількості помилкових спрацювань, автоматизацію виявлення відхилень, і можливість вирішувати завдання з розумінням контексту.

Проте, разом з численними перевагами, використання машинного навчання та штучного інтелекту також стикається з викликами та обмеженнями, такими як необхідність налагодження та підтримки складних моделей, питання конфіденційності та етики, а також можливість зловживання цими технологіями для атак на самі системи.

Отже, використання машинного навчання та штучного інтелекту для виявлення і реагування на загрози в корпоративних інформаційних системах - це важливий крок у покращенні кібербезпеки. Правильно розроблені та налаштовані системи, здатні реагувати на загрози в реальному часі, що сприяє підвищенню загального рівня захищеності корпоративних інформаційних систем в умовах постійно зростаючої загрози кібернападів.

Качний Ілля Сергійович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

НОВІ ТЕНДЕНЦІЇ У СВІТІ ПРОГРАМ-ВИМАГАЧІВ НА ПРИКЛАДІ RANSOMWARE-AS-A-SERVICE

Програми-вимагачі як послуга (RaaS) - це кіберзлочинна бізнес-модель, в якій хакери продають код своїх програм-вимагачів іншим хакерам, які потім використовують його для здійснення власних атак. RaaS знижує вимоги для входження в сферу кіберзлочинності, дозволяючи здійснювати кібератаки навіть зловмисникам з обмеженими технічними навичками. Крім того, RaaS є взаємовигідним: хакери можуть заробляти на вимаганні, не розробляючи власне шкідливе програмне забезпечення, а розробники програм-вимагачів можуть збільшити свої прибутки без необхідності проводити атаки на мережі власноруч.

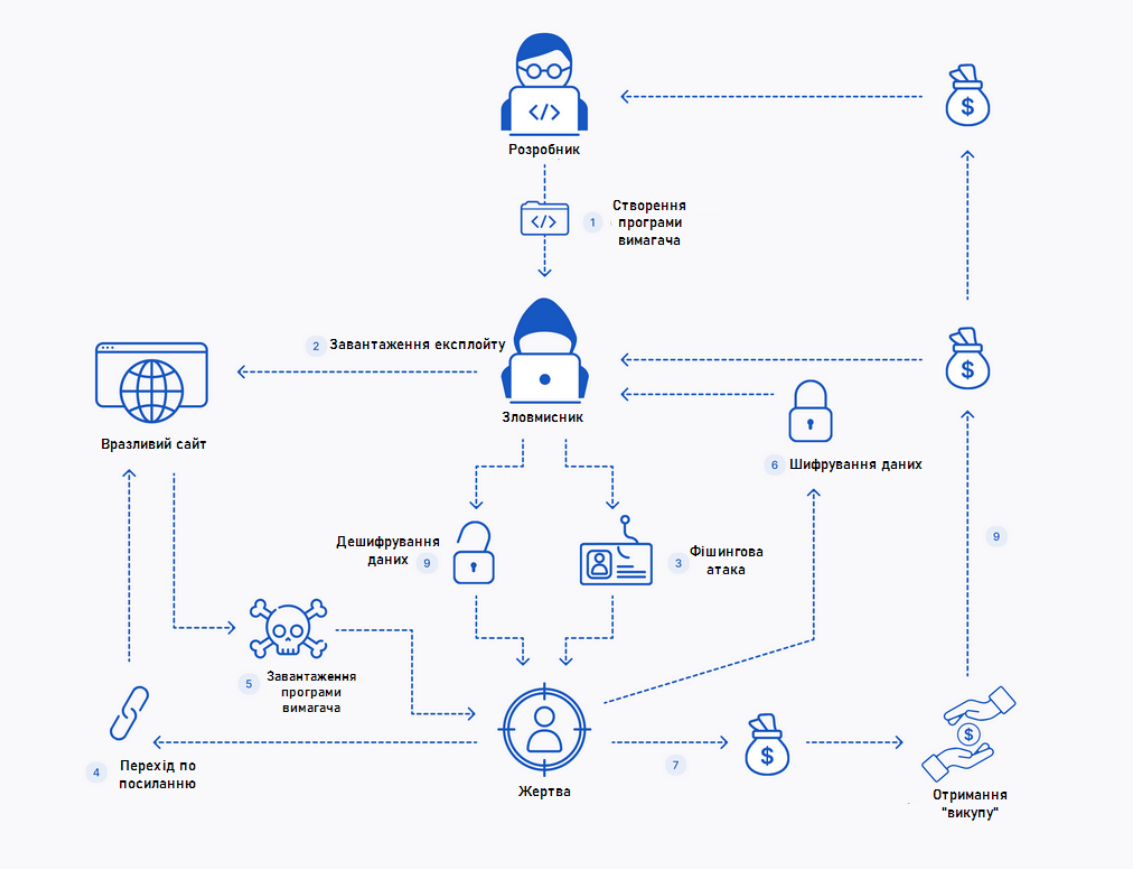


Рис.1. Структура та принцип роботи RaaS

Більшість розробників RaaS використовують одну з наступних моделей доходу для продажу своїх програм:

- Щомісячна підписка: клієнти RaaS сплачують регулярну плату - іноді лише 40 доларів на місяць - за доступ до інструментів для вимагання
- Одноразова плата: клієнтм купляють код програми-вимагача
- Партнерські моделі: клієнти сплачують щомісячну плату і діляться з операторами RaaS невеликим відсотком від отриманих ними викупів

- Розподіл прибутку: Оператори RaaS нічого не беруть заздалегідь, але отримують значну частку від кожного викупу, який отримує клієнт, часто 30-40%.

Найефективніша стратегія протидії атакам вимагачів - це поєднання навчання персоналу, створення засобів захисту та постійний моніторинг вашої екосистеми на наявність вразливостей.

Перелік посилань:

1. What is ransomware-as-a-service? URL: https://www.ibm.com/topics/ransomware-as-a-service (дата звернення: 24.10.2023).

2. The dangerous threat to world security URL: https://www.upguard.com/blog/what-is-ransomware-as-a-service (дата звернення: 24.10.2023).

Кизим Валентин Володимирович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ В КОРПОРАТИВНІЙ МЕРЕЖІ ЯК ЗАСІБ ПРОФІЛАКТИКИ ІНЦИДЕНТІВ БЕЗПЕКИ

Кожного року компанії стикаються з інформаційними загрозами. Значну частину з них складають вразливості. Як відомі, так і ще не розкриті або недосліджені (zero-day). Одним із ефективних способів попередження можливих інцидентів безпеки є регулярне проведення аудитів безпеки в цілому і проведення тестувань на проникнення в якості окремої перевірки або одного з етапів аудиту.

Згідно останніх досліджень, кожна п’ята компанія не проводить тестувань на проникнення своїх продуктів. В той же час лише за 2022 рік було виявлено та опубліковано 25.000 вразливостей [1]. Важко сказати, скільки ще залишилось не виявлено. В 2021 році цей показник становив 20171 виявлена вразливість [2].

Все ж кожним роком кількість виявлених вразливостей зростає. В основному причиною цього є два фактори: збільшення кількості застарілих версій та розширення використання інформаційних технологій в усіх аспектах введення бізнесу. Проте, разом з цим зростання виявлених вразливостей може бути пов’язане із більш активним використанням тестування на проникнення та\або автоматичних засобів виявлення вразливостей.

Успішно проведене тестування дозволяє:

1. Виявити не враховані при розробці помилки.
2. Впевнитись, що налаштування та конфігурації системи зроблені правильно
3. Дозволяє впевнитись, що механізми захисту працюють та можуть виявляти проведені маніпуляції
4. Виявити вразливості в системах\корпоративній мережі та усунути їх.

Разом вищезазначене дозволяє покращити захищеність мережі та підготувати інформаційну мережу компанії до можливих майбутніх атак. Не менш важливо зазначити, що для того, щоб ці міри були ефективними, тестування повинні проводитись на регулярній основі. Найбільш оптимально проводити тестування та\або аудит інформаційної безпеки хоча б раз в рік.

Перелік посилань:
1. Kumar A. Penetration testing statistics, vulnerabilities and trends in 2023 [Електронний ресурс] / Amit Kumar // TheCyphere. – 2023. – Режим доступу до ресурсу: https://thecyphere.com/blog/penetration-testing-statistics/
2. Browse Vulnerabilities By Date [Електронний ресурс] // CVE Details. – 2023. – Режим доступу до ресурсу: https://www.cvedetails.com/browse-by-date.php

Катков Юрій Ігорович
доктор технічних наук, професор кафедри комп'ютерних наук, ННІТ, ДУІКТ, Київ, Україна
Кладько Іван Михайлович
Студент групи КНДМ-63 ННІТ, ДУІКТ, Київ, Україна

УМОВИ ЗАХИСТУ МІКРОСЕРВІСІВ В ХМАРНИХ ОБЧИСЛЕННЯХ В УМОВАХ КОНТЕЙНЕРНОЇ ВІРТУАЛІЗАЦІЇ

Системи управління захисту мікросервісної архітектури у контексті безпеки хмарних обчислень і контейнерної віртуалізації відіграють ключову роль в спрощенні та оптимізації процесів розгортання, масштабування, керування та адміністрування в хмарних обчисленнях. Проблема у тому, що мікросервіси, які становлять будівельні блоки цієї архітектури, мають загрози. Це виникає тому, що вони володіють властивістю незалежного масштабування, що є важливою конкурентною перевагою. Кожен мікросервіс може бути розгорнутий окремо на власних серверах чи контейнерах, надаючи гнучкість та швидкість реакції на зміни у навантаженні. Мікросервісна архітектура передбачає, що програмний продукт складається з множини таких самодостатніх мікросервісів, які працюють разом у гармонії, створюючи надійну та масштабовану інфраструктуру для сучасних хмарних рішень. Порушення цієї гармонії є головною метою зловмисників.

Ключові слова: мікросервіси, моніторинг мікросервісної архітектури, хмарні обчислення, контейнерна віртуалізація, оркестрація контейнерів.

Для розуміння проблеми захисту мікросервісної архітектури у контексті безпеки хмарних обчислень і контейнерної віртуалізації треба розуміти, що таке мікросервіси, що таке моніторинг мікросервісної архітектури, які загрози можуть бути для хмарних обчислень, контейнерної віртуалізації та оркестрації контейнерів.

Мікросервіси - це революційний підхід до архітектури програмного забезпечення, який полягає в розбитті додатку на невеликі, незалежні компоненти, які працюють разом для надання послуги. Кожен мікросервіс представляє собою автономний ізольований модуль, який може бути розроблений, розгорнутий, та масштабований незалежно від інших. Ця архітектура надає можливість швидкого впровадження змін, великої гнучкості та високої доступності додатку. Всі мікросервіси взаємодіють через стандартизовані інтерфейси, що дозволяє забезпечити їх спільну роботу, навіть якщо вони написані різними мовами або розгорнуті на різних серверах. Такий підхід сприяє покращенню масштабованості та підтримки додатку, зменшенню ризиків і полегшенню розробки, що робить мікросервіси важливим елементом для сучасних програмних систем [1]. Тому є проблеми безпеки мікросервісів, а

саме: ізоляція (складна проблема безпеки для мікросервісів через розподіл характеру архітектури); складність гібридної та мультихмарної хмари (оскільки збільшують кількість напрямків атак і ускладнюють управління та захист усієї системи); управління безпекою кількох хмарних провайдерів та локальних середовищ; захист даних, що передаються між службами та зовнішніми джерелами (оскільки кожна служба може мати власне сховище даних та протокол зв'язку, існує ризик витоку, підробки чи перехоплення даних зловмисниками); управління рівнями даних (труднощі забезпечення узгодженої безпеки даних у всіх сервісах); забезпечення мікросервісам відповідний рівень доступу до даних (в архітектурі мікросервісів кожна служба призначена для виконання певних бізнес-можливостей та може вимагати доступу до певних даних). Мікросервіси також можуть створювати проблеми, пов'язані з конфіденційністю та дотриманням вимог. У деяких галузях або регіонах правила конфіденційності даних можуть вимагати додаткового контролю над обробкою та зберіганням даних. Може виявитися непросто забезпечити дотримання вимог конфіденційності та відповідності вимогам всіх рівнях даних в архітектурі мікросервісів.

Моніторинг мікросервісної архітектури - є процесом систематичного та надзвичайно детального нагляду, спрямованого на спостереження, аналіз та управління функціонуванням мікросервісних компонентів та їх взаємозв’язки. Цей комплексний підхід включає в себе постійний аналіз ресурсів, надання послуг, завантаження, ефективність та стабільність мікросервісів. Метою моніторингу є вчасне виявлення аномалій, вдосконалення продуктивності та забезпечення надійності мікросервісної архітектури. Цей процес вимагає використання різноманітних інструментів та метрик, щоб забезпечити оптимальне функціонування всіх компонентів та підтримати надійність послуг, наданих мікросервісами. Звідси однією з основних проблем безпеки в архітектурі мікросервісів є забезпечення безпеки зв'язку між сервісами. У середовищі мікросервісів кілька сервісів взаємодіють один з одним через API, а це означає, що будь-яка вразливість в API потенційно може поставити під загрозу всю систему.

Хмарні обчислення – це революційна парадигма інформаційних технологій, що трансформує спосіб, яким сучасні організації забезпечують доступ до обчислювальних ресурсів і зберігання даних. Вона ґрунтується на концепції віртуалізації, що дозволяє віддалену, миттєву і масштабовану обробку і зберігання інформації. Цей підхід надає користувачам можливість отримувати доступ до великих обчислювальних потужностей, даних і програм через Інтернет, не прив'язуючись до конкретних фізичних серверів або обладнання. Важливою особливістю хмарних обчислень є гнучкість і масштабованість, що дозволяють користувачам змінювати свої ресурси в залежності від потреб, сприяючи зниженню витрат і підвищенню продуктивності. Існує декілька моделей хмарних обчислень: Software as a Service (SaaS) (наприклад ПЗ Salesforce)[3] – програмне забезпечення як послуга, Platform as a Service (PaaS) (наприклад Red Hat OpenShift)[4] – платформа як послуга, Infrastructure as a

Service (IaaS) (Наприклад IBM Cloud Infrastructure)[5] – інфраструктура як послуга. Звідси критичними хмарними загрозами є: інше програмне забезпечення та ризики ланцюжка поставок; хмарні програми-вимагачі; розширені постійні загрози (APT); мультихмарне розростання; тіньові дані; перевищення дозволів у хмарі; а також людські помилки, неправильні конфігурації та неправильне використання даних.

Контейнерна віртуалізація – представляє собою перетворену парадигму обчислення, що забезпечує ізоляцію та ефективне управління віртуальними середовищами, відомими як контейнери. Цей інноваційний підхід дозволяє упаковувати додатки та їх залежності в легкі та портативні контейнери, що можуть бути використані для виконання практично в будь-якому середовищі, яке підтримує контейнеризацію. Кожен контейнер функціонує як самодостатня одиниця, ізольована від інших контейнерів та оптимізована для швидкого розгортання та масштабування. Цей підхід сприяє забезпеченню консистентності та надійності додатків, знижує витрати на інфраструктуру і полегшує управління обчислювальними ресурсами. Контейнерна віртуалізація стала важливою технологією в розробці та розгортанні програмного забезпечення, забезпечуючи швидкість і надійність в процесі роботи з додатками. Найпопулярніші додатки для контейнерної віртуалізації прийнято вважати Docker[6] та Kubernetes [7]. Проте найпоширенішими типами загроз безпеки контейнерів є: контейнерне шкідливе програмне забезпечення; небезпечні привілеї контейнера; контейнери із конфіденційними даними; трубопровід розвитку; контейнери зображення; реєстри контейнерів; середовище виконання контейнера.

Оркестрація контейнерів - є важливою практикою в управлінні контейнерною віртуалізацією, яка включає в себе високорівневий процес планування, розгортання та керування контейнерами у великих масштабах. Ця динамічна стратегія дозволяє автоматизувати управління контейнерами, забезпечуючи автоматичну оркестрацію ресурсів, розподіл навантаження та виявлення несправностей. Оркестрація контейнерів допомагає гармонійно координувати дії між контейнерами та їхнім життєвим циклом, що включає в себе розгортання, масштабування та усунення неполадок. Вона забезпечує надійність, високу доступність та ефективну взаємодію контейнерів у реальному часі, дозволяючи забезпечувати послуги високого рівня, навіть у складних розподілених середовищах. Звідси використання оркестрації контейнерів дозволяє вирішувати такі завдання з безпеки: забезпечення та розгортання; конфігурація та планування; розподіл ресурсів; наявність контейнера; масштабування або видалення контейнерів на основі балансування робочих навантажень у інфраструктурі; балансування навантаження та маршрутизація трафіку; моніторинг стану контейнера.

Висновок.

Системи управління безпекою мікросервісів в хмарних обчисленнях в умовах контейнерної віртуалізації відіграють ключову роль у створенні сучасних, ефективних та масштабованих програмних продуктів. Інтеграція мікросервісної архітектури з контейнерами дозволяє розробникам та операторам

розгортати та керувати додатками з високою гнучкістю та ефективністю. Ці системи забезпечують автоматизоване розгортання, масштабування, управління, а також покращують надійність та безпеку додатків. При цьому, вони сприяють розвитку сучасних хмарних обчислень, де швидкість, портативність та легкість управління стають дійсно важливими факторами у конкурентному світі програмної розробки. Завдяки системам управління мікросервісами в умовах контейнерної віртуалізації, розробники можуть більше уваги приділити розробці функціональності, а не інфраструктурним питанням. Тим часом, з точки зору бізнесу, ця технологія дозволяє покращити швидкість впровадження нових функцій та реагувати на зміни на ринку швидше, що є критичним в сучасному світі інформаційних технологій. У підсумку, системи управління мікросервісами та контейнерною віртуалізацією є потужним інструментарієм, що революціонізує спосіб, яким ми розглядаємо та розробляємо програмне забезпечення.

Перелік посилань:

1. Офіційний веб-сайт "Microservices.io"// [Електронний ресурс] Режим доступу до ресурсу: https://microservices.io/
2. Офіційна специфікація HTTP/1.1 від Консорціуму Всесвітньої павутини (World Wide Web Consortium). // [Електронний ресурс] Режим доступу до ресурсу: https://www.w3.org/Protocols/rfc2616/rfc2616.html
3. Документація для розробників, які планують розробляти SaaS-додатки на платформі Salesforce. // [Електронний ресурс] Режим доступу до ресурсу: https://developer.salesforce.com/docs/atlas.en-us.sasfindev/index.html
4. Офіційний сайт Red Hat OpenShift // [Електронний ресурс] Режим доступу до ресурсу: https://docs.openshift.com/
5. Документація IBM Cloud Infrastructure// [Електронний ресурс] Режим доступу до ресурсу: https://www.ibm.com/cloud/infrastructure
6. Офіційна документація Docker// [Електронний ресурс] Режим доступу до ресурсу: https://docs.docker.com/
7. Офіційна документація Kubernetes// [Електронний ресурс] Режим доступу до ресурсу: *https://kubernetes.io/docs/home/*

Коврижко Артем Олександрович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ПІДВИЩЕННЯ МОЖЛИВОСТЕЙ ВИЯВЛЕННЯ ЗАГРОЗ КОРПОРАТИВНІЙ СИСТЕМІ НА ПРИКЛАДІ QRADAR USE CASE MANAGER

Корпоративні систсеми з кожним роком піддаються все більшій і більшій кількості атак, зловмисники використовують різні вектори, методи, типи атак для проникнення до корпоративної мережі компаній. Часто це ставить під загрозу існування цілий ряд компаній які можуть бути скомпроментовані та в результаті цього понести збитки не сумісні з подальшим існуванням або на довгий час.

Для підвищення можливостей з виявлення загроз можливо використати систему IBM QRadar Use Case Manager.Можливо користуватись керованим порадами у розділі IBM® QRadar Use Case Manager, щоб переконатися, що IBM QRadar оптимально налаштований для точного виявлення загроз у всьому

ланцюжку атак. До складу QRadar Use Case Manager браузер варіантів використання з гнучкими звітами за правилами. Крім того, QRadar Use Case Manager пропонує стандартні відображення в системні правила і допомагає пов'язати ваші власні правила користувача з тактиками і прийомами MITRE ATT&CK.

QRadar Use Case Manager підтримується в Google Chrome та Mozilla Firefox. Є можливість додати додаткові перевірки при включенні та виключенні правил, щоб уникнути включення правила з вимкненими залежностями або вимкнення правила, від якого залежать інші включені правила.

Атрибути правил користувача надають можливість створення розширених правил, які не можна створити за допомогою існуючих атрибутів. Приклади атрибутів користувача: варіант використання, якому належить правило, колектив, який відповідає за створення та обслуговування правила, або користувач, який перевірив правило. Також можна створити будь-який атрибут користувача правила і вказати його значення, присвоїти значення атрибуту користувача правилу і додати атрибут користувача як стовпця в Оглядач варіантів використання.

Для роботи IBM QRadar Use Case Manager треба:

- Створити правила за допомогою візуалізації та створених звітів
- Налаштувати своє середовище на основі вбудованого аналізу
- Візуалізувати покриття загроз у рамках MITER ATT&CK
- Налаштувати та встановитипотрібні IBM Security App Exchange, які доступні для встановлення.

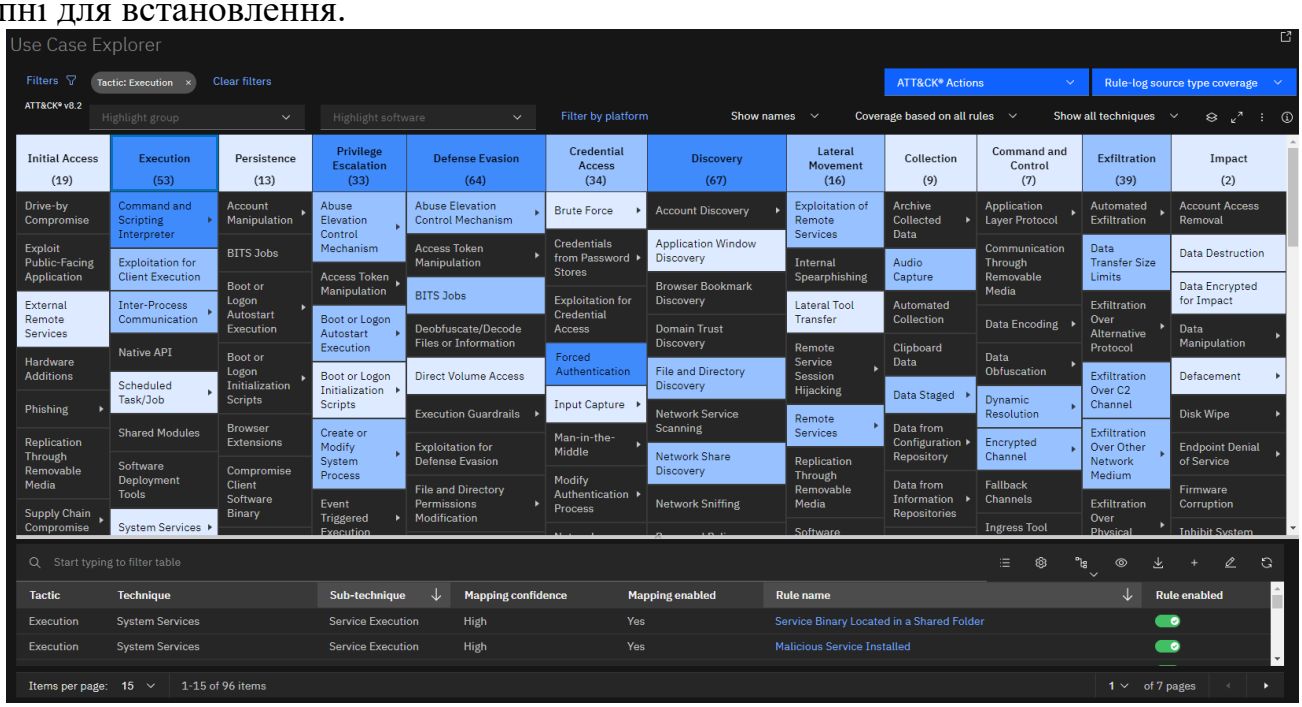


Рис.1. Інтерфейс QRadar Use Case Manager

Перелік посилань:

1. Менеджер варіантів використання QRadar — QRadar 7.3.3 FP6+/7.4.2 FP3+ URL: https://exchange.xforce.ibmcloud.com/hub/extension/511b125b505e515f4da5c553a7504b55 (дата звернення: 13.10.2023).

2. QRadar Use Case Manager IBM Documentation URL: https://www.ibm.com/docs/ru/qradar-common?topic=apps-qradar-use-case-manager-app (дата звернення: 20.10.2023).

Колесник Володимир Дмитрович
студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

АНАЛІЗ АВТОМАТИЗОВАНИХ СКАНЕРІВ ВРАЗЛИВОСТЕЙ ВЕБ-САЙТІВ ТА ВЕБ-ДОДАТКІВ

У сучасних умовах тестування на проникнення є невід'ємною частиною сфери інформаційних технологій. За статистикою, набули популярності автоматизовані інструменти для проведення таких тестувань. Разом з функціональністю та автоматизацією з'явилося зниження точності тестування та "false-positive" вразливості. Однак нові технології з'являються кожен день, тестування застарілих технологій потребує автоматизації з мінімальним ризиком и максимальною ефективністю. Тому, при наявності великої кількості автоматизованих сканерів, необхідно правильно підбирати їх під конкретну задачу.

Загальні положення

DAST Scanners (Dynamic Application Security Testing) — це программа, або програмний комплекс, призначений для виявлення умов, що вказують на вразливість безпеки у додатку у його робочому стані [1]. У сфері інформаційної безпеки такі технології називають просто «сканери». Сканерів сьогодні існує дуже багато, кожен з них має у чомусь перевагу над іншими [4]. Згідно з тестом WAVSEP DAST 2017/2018 Шая Чена, інформація з якого є актуальною навіть сьогодні (згідно з OWASP Web Vulnerabilities Checklist 2022), досить небагато сканерів працюють добре [3].

Статистика наведена за категоріями [3]:

1. Підтримка вектора доставки

Термін «вектор доставки вхідних даних» відноситься до структури вхідних даних, що використовуються в комунікації клієнт-сервер для доставки даних з браузера, мобільного пристрою чи клієнтської програми на веб-сервер. Прикладами можуть бути вбудовані параметри рядка запиту (GET), параметри тіла HTTP (POST), масиви JSON у тілі HTTP тощо.

Оскільки здатність аналізувати та моделювати атаки у векторах доставки вхідних даних є ключовим параметром, сканери DAST можуть виявити вразливості, що мають відношення до певного параметра серед переданих даних. Це найважливіший аспект у процесі вибору будь-якого сканера [1].

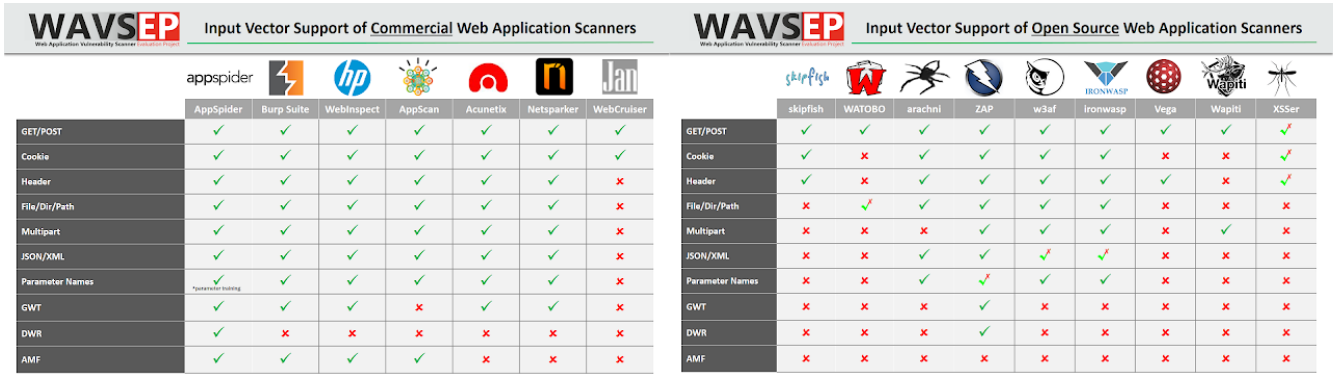


Рис.1 - Порівняння підтримки векторів між комерційними постачальниками DAST (зліва) та між комерційними постачальниками DAST з відкритим кодом

2. Підтримка подолання сучасних бар'єрів сканування

Окрім відсутності підтримки відповідних векторів введення (JSON/XML/etc) або неефективного механізму сканування, існують додаткові «бар'єри», які можуть перешкодити сканеру успішно перевірити ціль.

Підтримка відтворення параметрів/заголовків CSRF (Cross-site Request Forgery), підтримка включення кількох доменів в область одного сканування (критично для архітектури мікросервісів SPA) та подібні ключові елементи необхідні для успішного сканування сучасних програм, особливо в контексті періодичних BDD/TDD оцінки [4].

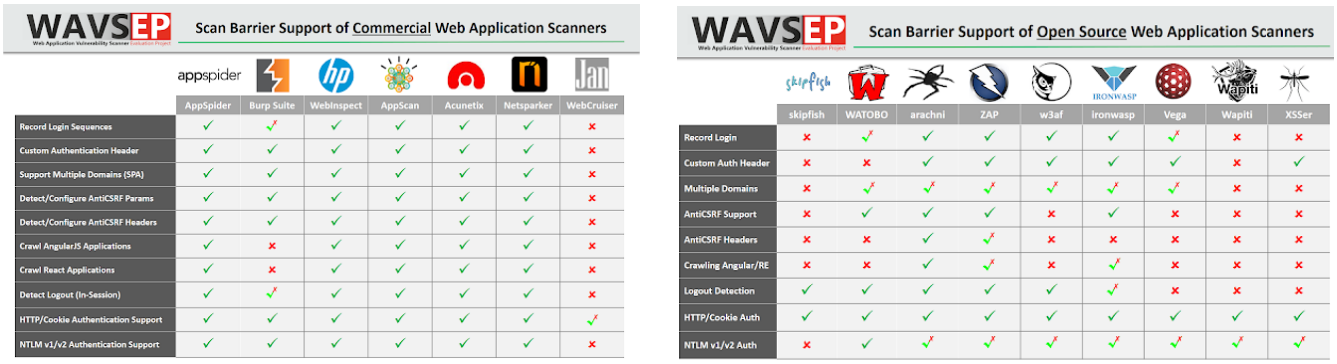


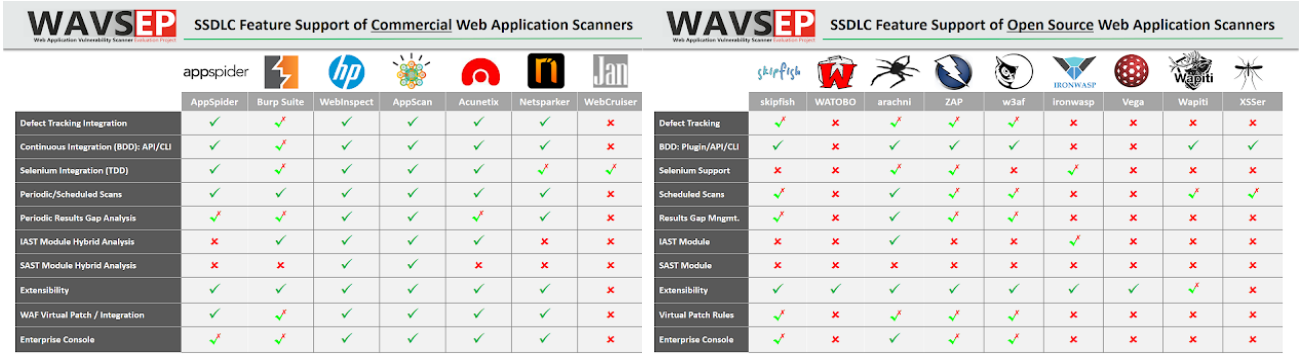
Рис.2 - Порівняння підтримки «обходу» бар'єрів сканування між комерційними сканерами DAST (зліва) та між комерційними постачальниками DAST з відкритим кодом

3. Підтримка важливих функцій інтеграції SSDLC

Щоб мати можливість ефективно використовувати інструменти DAST у SSDLC (Secure Software Development Life Cycle), сканер зазвичай повинен підтримувати кілька ключових функцій:

- Інтеграція відстеження дефектів - підтримка звітування
- Підтримка безперервної інтеграції (BDD/TDD) – підтримка запланованого сканування та імпорту результатів

- Періодичні/заплановані сканування - вбудовані заплановані сканування
- Періодичний аналіз розривів результатів – аналіз результатів, що відрізняються між скануваннями
- WAF Virtual Patch Generation – можливість генерувати правило фільтрації даних для WAF.
- Функції керування корпоративною консоллю - можливість керувати результатами в графічному інтерфейсі користувача



WAVSEP SSDLC Feature Support of Commercial Web Application Scanners

	AppSpider	Burp Suite	WebInspect	AppScan	Acunetix	Netsparker	WebCruiser
Defect Tracking Integration	✓	✓	✓	✓	✓	✓	×
Continuous Integration (BDD): API/CLI	✓	✓	✓	✓	✓	✓	×
Selenium Integration (TDD)	✓	✓	✓	✓	✓	✓	✓
Periodic/Scheduled Scans	✓	✓	✓	✓	✓	✓	×
Periodic Results Gap Analysis	✓	✓	✓	✓	✓	✓	×
IAST Module Hybrid Analysis	×	✓	✓	✓	✓	×	×
SAST Module Hybrid Analysis	×	×	✓	✓	×	×	×
Extensibility	✓	✓	✓	✓	✓	✓	×
WAF Virtual Patch / Integration	✓	✓	✓	✓	✓	✓	×
Enterprise Console	✓	✓	✓	✓	✓	✓	×

WAVSEP SSDLC Feature Support of Open Source Web Application Scanners

	skipfish	WATOBO	arachni	ZAP	w3af	ironwasp	Vega	Wapiti	XSSer
Defect Tracking	✓	×	✓	✓	✓	×	×	×	×
BDD: Plugin/API/CLI	✓	×	✓	✓	✓	×	×	✓	✓
Selenium Support	×	×	✓	✓	×	✓	×	×	×
Scheduled Scans	✓	×	✓	✓	✓	×	×	✓	✓
Results Gap Mngmt.	✓	×	✓	✓	✓	×	×	×	×
IAST Module	×	×	✓	×	×	✓	×	×	×
SAST Module	×	×	×	×	×	×	×	×	×
Extensibility	✓	✓	✓	✓	✓	✓	✓	✓	×
Virtual Patch Rules	✓	×	✓	✓	✓	×	×	×	×
Enterprise Console	✓	×	✓	✓	✓	×	×	×	×

Рис. 3 - Порівняння вбудованої/зовнішньої підтримки помітних функцій SSDLC в комерційних інструментах DAST (зліва) та в в комерційних інструментах DAST з відкритим кодом

Перелік посилань:

1. Nesterenko S. The Secrets of OSINT (Open-source Intelligence) [Електронний ресурс] / Serhii Nesterenko // Udemy. – 2022. – Режим доступу до ресурсу: https://www.udemy.com/course/the-secrets-of-osint-open-source-intelligence/.

2. Wichers D. Open Source Application Security Tools [Електронний ресурс] / Dave Wichers // OWASP. – 2022. – Режим доступу до ресурсу: http://owasp.org/www-community/Free_for_Open_Source_Application_Security_Tools

3. Shay C. Evaluation of Web Application Vulnerability Scanners in Modern Pentest and SSDLC Usage Scenarios [Електронний ресурс] / C. Shay, A. Achiad, T. Blessen // Effective Security. – 2018. – Режим доступу до ресурсу: https://sectooladdict.blogspot.com/.

4. Suto L. Analyzing the accuracy and time costs of web application security scanners [Електронний ресурс] / Larry Suto. – 2010. – Режим доступу до ресурсу: https://www.slideshare.net/lbsuto/accuracy-and-timecostsofwebappscanners .

5. Suto L. Analyzing the Effectivess of Web Application Firewalls [Електронний ресурс] / Larry Suto. – 2011. – Режим доступу до ресурсу: https://www.slideshare.net/lbsuto/analyzing-the-effectivess-of-web-application-firewalls

Коржик Василь Васильович
УБДМ-61, ДУІКТ, Київ, Україна

ЖИТТЄВИЙ ЦИКЛ РОЗГОРТАННЯ КОРПОРАТИВНИХ МОБІЛЬНИХ ПРИСТРОЇВ ВІДПОВІДНО ДО КОНЦЕПЦІЇ NIST

Протидія загрозам корпоративним мобільним пристроям набуває вирішального значення у забезпеченні інформаційної безпеки підприємства. Відповідно до концепції NIST модель розгортання мобільних пристроїв та управління ними протягом усього життєвого циклу експлуатації включає такі етапи: визначення вимог до мобільних пристроїв; оцінювання ризиків; впровадження стратегії корпоративної мобільності; експлуатація і підтримка функціонування; утилізація та/або повторне використання мобільних пристроїв.

З розвитком IT кількість і складність загроз інформаційно-комунікаційним системам організацій постійно зростає. Мобільні пристрої і технології не є винятком. Так, згідно зі звітом про глобальні загрози за 2023 рік від Zimperium, 43% усіх скомпрометованих пристроїв було використано зловмисниками з деструктивною метою, що на 187% більше, ніж у попередньому 2022 році [1]. Отже, організації мають звернути більше уваги на запобігання і протидію загрозам корпоративним мобільним пристроям, які сьогодні широко використовуються для виконання бізнес-завдань.

Оптимальним варіантом є забезпечення безпеки мобільних пристроїв відповідно до їх життєвого циклу як сукупності стадій та етапів, які вони проходять від моменту прийняття рішення про розробку або придбання пристроїв до припинення їх існування або функціонування [2].

Національний інститут стандартів і технологій (NIST) США у 2023 році запропонував модель розгортання мобільних пристроїв та управління ними протягом усього життєвого циклу експлуатації, яка включає такі етапи: визначення вимог до мобільних пристроїв; оцінювання ризиків; впровадження стратегії корпоративної мобільності; експлуатація і підтримка функціонування; утилізація та/або повторне використання мобільних пристроїв (Рис. 1) [3].

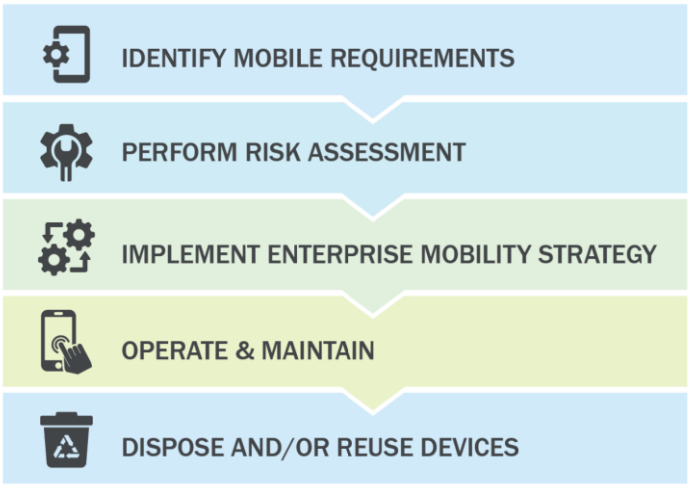


Рис. 1. Життєвий цикл розгортання корпоративних мобільних пристроїв

Розглянемо детальніше кожен із представлених етапів.

Визначення вимог до мобільних пристроїв. На першому етапі життєвого циклу мобільних пристроїв організація визначає потреби й вимоги до мобільних пристроїв для досягнення корпоративних цілей, проводить інвентаризацію мобільних пристроїв, які вже використовуються, і визначає модель розгортання мобільного середовища, яка підходить організації.

Оцінювання ризиків. Процес оцінювання ризиків є основоположним компонентом кібербезпеки і використовується для ідентифікації, оцінки та визначення пріоритетності ризиків корпоративним мобільним пристроям, операціям і активам, які обробляються й передаються в мобільному середовищі організації. Оцінювання ризиків проводять періодично, оскільки ландшафт загроз постійно змінюється, а мобільні системи, які потрібно захистити,

розвиваються.

Впровадження стратегії корпоративної мобільності. Для вирішення завдань управління й забезпечення безпеки мобільного середовища організації використовують рішення з управління корпоративною мобільністю (Enterprise Mobility Management, EMM). EMM є класом програмних засобів, що підтримують можливість використання мобільних пристроїв у корпоративних ділових процесах, яке реалізується за допомогою інтеграції цих апаратних засобів в IT-системи і середовище забезпечення безпеки на всіх етапах управління життєвим циклом IT.

Організації самі обирають варіанти управління корпоративними мобільними пристроями: від повного контролю над усіма засобами (з моменту закупівель до виводу з експлуатації) до санкціонованого використання персоналом власних мобільних пристроїв (можливо, зі схваленого списку) для виконання бізнес-завдань.

Експлуатація і підтримка функціонування. На цьому етапі організація розробляє і впроваджує комплекс заходів для захисту мобільних пристроїв підприємства, а також корпоративних даних і користувачів. Також проводять періодичне оцінювання ефективності таких заходів з метою їх модифікації або додавання нових для покращення захисту мобільних систем у подальшому.

Утилізація й повторне використання мобільних пристроїв. Оскільки мобільні пристрої можуть зберігати конфіденційну інформацію, таку як паролі, дані облікових записів, е-листи, голосові повідомлення, журнали текстових повідомлень або дані, пов’язані з бізнес-діяльністю, ці апаратні засоби потрібно належним чином утилізувати, щоб конфіденційна інформація не потрапила до чужих рук.

Отже, відповідно до концепції NIST модель розгортання мобільних пристроїв та управління ними протягом усього життєвого циклу експлуатації включає такі етапи: визначення вимог до мобільних пристроїв; оцінювання ризиків; впровадження стратегії корпоративної мобільності; експлуатація і підтримка функціонування; утилізація та/або повторне використання мобільних пристроїв.

Перелік посилань:

1. New Research Reveals 187% Increase in Sophisticated Attacks Against Mobile Devices. URL: https://cybersecuritynews.com/mobile-threat-report/

2. Карпова Т. О. Життєвий цикл інформаційної системи та його вплив на розвиток підприємства. Науковий вісник Ужгородського національного університету. 2017. Випуск 15. Ч.1. С. 142-146.

3. Murugiah Souppaya, Karen Scarfone. NIST Special Publication NIST SP 800-124r2. Guidelines for Managing the Security of Mobile Devices in the Enterprise. May 2023. 51 p.

Корнієнко Євгеній Ігорович
студент групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Інформаційна безпека стала важливою складовою сучасного суспільства і глобальної політики. В цій доповіді я досліджував актуальні аспекти інформаційної безпеки, включаючи кіберзагрози, дезінформацію та кібератаки. Вона також наголошує на ролі інформаційної безпеки в системі національної безпеки країни, а також на важливості розвитку кіберзахисту і медіаграмотності громадян. Інформаційна безпека визнається як важливий фактор для забезпечення стабільності та безпеки в умовах сучасного інформаційного суспільства..

У науковій та довідково-енциклопедичній літературі зазначається, що термін «безпека» (від грецького – «володіти ситуацією») почав вживатися з 1190 р. і означав спокійний стан духу людини, яка вважала себе захищеною від будь-якої небезпеки.

Розрізняють політичні небезпеки, економічні, екологічні, харчові, криміногенні небезпеки інформаційні тощо. У свою чергу, можна виділити національне та міжнародно-правове розуміння безпеки. Національне розуміння зазначеного найзагальнішого поняття закріплене у Державному стандарті України 2293-99, який визначає термін «безпека» як стан захищеності особи та суспільства від ризику зазнати шкоди.

Сьогодні я хочу розглянути важливу тему інформаційної безпеки та її роль і проблематику у системі національної безпеки України. Ця тема є дуже актуальною в сучасному світі, оскільки інформація стала важливим ресурсом, який може впливати на політичні, економічні та соціальні процеси.

Інформаційна безпека - це сукупність заходів та стратегій, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації. В контексті національної безпеки, інформаційна безпека грає ключову роль, оскільки забезпечує захист важливих національних інтересів та надійність функціонування державних інституцій. Україна, як і інші країни, стикається з численними викликами у цій сфері:

1) Кіберзагрози та кібератаки: Однією з найбільших проблем є постійна загроза кібератак. Україна була об'єктом численних кіберзагроз, які включають в себе атаки на державні інституції, критичну інфраструктуру та політичні системи. Найбільш відомий приклад - атаки на енергетичну систему України, які відбулися в минулому. Інформаційна безпека повинна бути зосереджена на виявленні, запобіганні та відповіді на кібератаки;

2) Дезінформація та гібридна війна: Україна також стикається з проблемою дезінформації та гібридної війни, в тому числі через розповсюдження фейків та пропаганду. Інформаційна безпека має бути спрямована на виявлення та боротьбу з такою дезінформацією, а також на підвищення медіаграмотності громадян;

3) Недостатній розвиток кіберзахисту: Україна повинна інвестувати в розвиток кіберзахисту та створення сильних команд інформаційної безпеки. Це

включає в себе як залучення кваліфікованих фахівців, так і розвиток відповідних технологій і стратегій;

4) Залежність від іноземних постачальників технологій: Україна стикається з проблемою залежності від іноземних постачальників технологій та програмного забезпечення. Це може створювати ризики для інформаційної безпеки. Розвиток власних технологій та кіберзахисту має велике значення для зменшення цієї залежності;

5) Потреба в координації: Важливо підкреслити потребу в ефективній координації зусиль різних організацій та інституцій, що працюють у сфері інформаційної безпеки. Координація сприяє більш ефективному вирішенню проблем;

6) Захист інфраструктури критичних систем: Інформаційна безпека включає в себе заходи для захисту критичної інфраструктури, такої як енергетика, транспорт та телекомунікації від можливих атак та вторгнень;

7) Забезпечення інформаційної готовності: Важливо мати механізми для швидкого реагування на кризові ситуації та надання інформаційної підтримки важливим рішенням у сферах безпеки та оборони.

Зміцнення інформаційної безпеки України є важливою передумовою

забезпечення національної безпеки в умовах сучасного світу. Це вимагає комплексного підходу, інвестицій та співпраці з партнерами на міжнародному рівні. З метою ефективної захисту національних інтересів, Україна повинна надати пріоритет інформаційній безпеці в своїй стратегії національної безпеки.

Загальні висновки:

1) Актуальність проблем: Проблеми інформаційної безпеки є дуже актуальними в сучасному світі, оскільки Україна стикається з постійними загрозами у сфері кібербезпеки, дезінформації та гібридної війни. Вони мають потенційний вплив на національну безпеку та стабільність країни;

2) Специфіка загроз: Кіберзагрози і дезінформація можуть завдати серйозних збитків, і їхні форми постійно еволюціонують. Розуміння цих загроз та їхніх специфік важливо для ефективного боротьби з ними;

3) Розвиток кіберзахисту: Підвищення рівня кіберзахисту є критичним завданням для України. Це включає в себе розвиток кваліфікованих кадрів, створення сучасних кіберзахисних структур та вдосконалення технологічної інфраструктури;

4) Медіаграмотність громадян: Підвищення медіаграмотності громадян має велике значення для запобігання дезінформації та поширенню фейків. Освіта і інформаційна грамотність громадян є важливими складовими інформаційної безпеки.

Перспективи:

1) Співпраця з міжнародними партнерами: Україна може співпрацювати з іншими країнами та міжнародними організаціями для обміну досвідом та підтримки в сфері інформаційної безпеки;

2) Створення національної стратегії інформаційної безпеки: Розробка і прийняття національної стратегії інформаційної безпеки є важливим кроком для координації зусиль різних інституцій та створення цільових програм;

3) Вдосконалення законодавства: Потрібно вдосконалити законодавство, щоб врахувати сучасні загрози та врегулювати питання кібербезпеки та даних;

4) Розвиток кіберзахисту і кібергігієни: Інвестиції в розвиток кіберзахисту, як у сфері технологій, так і в сфері навчання та обізнаності, допоможуть зміцнити інформаційну безпеку;

5) Громадянська участь та освіта: Залучення громадян до питань інформаційної безпеки та забезпечення доступної освіти є важливими кроками у забезпеченні інформаційної безпеки.

Узагальнюючи, інформаційна безпека в Україні вимагає комплексних заходів, спрямованих на вирішення актуальних проблем. Це має велике значення для забезпечення національної безпеки та стабільності в умовах сучасного інформаційного середовища.

Перелік посилань:

1. Головні визначення – безпека, загроза, небезпека, надзвичайна ситуація, ризик. URL: https://studfiles.net/preview/5704573/page:3/. (дата звернення: 30.09.2023).

2. ДСТУ 2293-99. Охорона праці. Терміни та визначення основних понять. URL: http://online.budstandart.com/ua/catalog/docpage.html?id_doc=21726. (дата звернення: 30.09.2023).

3. Коптєва О. О. Безпека людини як концепція міжнародного права. URL: Nzizvru_2014_6_14.pdf. (дата звернення: 30.09.2023).

4. Про національну безпеку України: Закон України від 08.07.2018 року. URL: https://zakon.rada.gov.ua/laws/show/2469-19. (дата звернення: 02.10.2023).

5. Інформаційна безпека. URL: https://sites.google.com/site/infobezpekaosobu/informacijna-bezpeka. (дата звернення: 05.10.2023).

6. Бондар І. Р. Інформаційна безпека як основа національної безпеки безпеки. (дата звернення: 06.10.2023).

URL: https://core.ac.uk/download/pdf/141443493.pdf (дата звернення: 10.10.2023).

7. Панченко О. Р. Інформаційна складова національної безпеки URL: https://www.rdc.org.ua/download/stati/Informational-warehouse.pdf (дата звернення: 20.10.2023).

Коровайченко Артем Юрійович
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

ТЕХНОЛОГІЇ КОНТРОЛЮ ВІДПОВІДНОСТІ КОНФІГУРАЦІЙ ХМАРНИХ ІНФРАСТРУКТУР СТАНДАРТАМ БЕЗПЕКИ

Управління конфігурацією безпеки хмарного середовища — це процес керування параметрами безпеки хмарних ресурсів для забезпечення їх цілісності. Комплекс дій включає виявлення неправильних конфігурацій, оцінку ризику та усунення вразливостей. Неправильні налаштування можуть призвести до різноманітних ризиків безпеки, зокрема:

- не авторизований доступ до інформації;

- DoS атаки;
- пошкодження даних.

Неправильні конфігурації в хмарних середовищах, наприклад у правилах мережевих екранів, дозволах, механізмах автентифікації або політиках IAM (Identity and Access Management), створюють вразливі місця, якими можуть скористатися хакери. Нехтування політиками захисту даних є однією з найпоширеніших причин їх витоку [1].

Належний менеджмент може зменшити ці ризики, підтримуючи узгоджену безпеку в усіх хмарних сервісах. Правильний підхід та моніторинг відхилень, таких як несподівані зміни параметрів, забезпечують важливу лінію захисту.

Організація може застосувати кілька різних підходів до керування параметрами безпеки хмарного середовища. Деякі обирають ручний процес, а інші використовують автоматизовані інструменти.

Підхід компанії залежить від кількох факторів, таких як розмір і складність хмарного середовища, необхідний рівень безпеки та бюджет. Ось шість кроків, які допоможуть визначити правильний підхід для вашої організації [2]:

1. Визначення стратегії наперед – необхідно визначити стратегічну політику та процедури, які керуватимуть реалізацією. Керівна група або комітет, включаючи відповідне вище керівництво та технічних спеціалістів і спеціалістів із безпеки, погодить і офіційно закріпить їх. Політика може включати вказівки відповідних визнаних організацій, таких як CIS, NIST (США) і NCSC (Великобританія).
2. Створення інвентаризації активів – цей крок передбачає ідентифікацію всіх хмарних ресурсів. Це може бути ручна інвентаризація всіх систем, але такий підхід може призвести до недогляду та людських помилок. Більш ефективним рішенням є інструменти CAASM, які автоматично сканують інфраструктуру, надаючи єдиний перелік усіх ресурсів.
3. Визначення інструментів – наступним кроком є узгодження набору інструментів і платформ. Необхідно визначитись із рішеннями, які забезпечать автоматизований контроль за параметрами безпеки. Це можуть бути IaC утиліти, такі як Terraform, або інструменти керування конфігурацією, такі як Ansible, Salt Stack тощо.
4. Впровадження інструментів – цей крок передбачає впровадження обраних інструментів і виконання тестів, щоб переконатися, що вони працюють правильно.
5. Створення процесу контролю змін – такі процеси гарантують, що запропоновані зміни та їх наслідки для безпеки відстежуються та досліджуються. Однак такі процедури не повинні бути надто вимогливим, оскільки вони можуть перешкоджати інноваціям і гнучкості бізнесу.
6. Забезпечення відповідності – має бути постійний моніторинг для зменшення ймовірності пропуску випадкових неправильних налаштувань та виявлення нових вразливостей.

Керування конфігурацією безпеки необхідне кожній організації.

Ефективні процеси і правильні інструменти захищають від вразливостей і загроз безпеці, одночасно знижуючи ризики, забезпечуючи відповідність і запобігаючи втраті даних.

Перелік посилань:
1. Cloud Security Configuration Management: A Comprehensive Guide. URL: https://www.tufin.com/blog/cloud-security-configuration-management-comprehensive-guide#:~:text=Cloud%20security%20configuration%20management%20is,security%20within%20the%20information%20system.
2. Cloud Security Configuration Management. URL: https://paladincloud.io/caasm/cloud-security-configuration-management/

Короленко Данило Миколайович,
студент 6 курсу, групи СЗДМ-62
Науковий керівник: Котенко Андрій Миколайович,
к.т.н., доцент кафедри Інформаційної та кібернетичної безпеки,
Державний університет інформаційно-комунікаційних технологій, м.Київ

ВИКОРИСТАННЯ ОБФУСКАЦІЙНОГО МЕТОДУ ДЛЯ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Постановка задачі. В умовах зростаючого інтересу до інформаційних технологій та швидкого розвитку цифрового середовища, безпека програмного забезпечення стає критично важливою задачею. Несанкціонований доступ, зловмисні атаки та розповсюдження шкідливого коду стали поширеними явищами. Відомо, що обфускаційний метод може бути використаний для ускладнення аналізу та розуміння програмного коду, але його ефективність та вплив на продуктивність є предметом дослідження. Поставимо за мету дослідити використання обфускаційного методу як інструменту для захисту програмного забезпечення, з'ясувати його переваги та обмеження, і визначити його роль у забезпеченні безпеки інформаційних систем.

Мета дослідження. Основною метою цього дослідження є оцінка ефективності обфускаційного методу у підвищенні рівня захисту програмного забезпечення від несанкціонованого доступу та аналізу, вивчення впливу обфускації на продуктивність програм та систем, аналіз результатів попередніх досліджень щодо обфускації і їх відображення на сучасних вимогах до інформаційної безпеки.

Результати дослідження. Обфускація може вплинути на продуктивність, збільшуючи обчислювальні затрати, але вплив може бути зменшений за допомогою оптимізації. Зараз існує багато програм, які дають можливість шифрувати код за допомогою обфускаційного методу, серед них:

– ProGuard – використовується для оптимізації та обфускації коду Java;

– DashO - інструмент для захисту Android-додатків, що включає обфускацію та інші заходи безпеки;

– Dotfuscator - обфускатор для .NET-програм, який забезпечує захист від реверс-інженірингу;

– Allatori - обфускатор для Java-програм, який підтримує різні рівні захисту;

– SmartAssembly - обфускатор та оптимізатор для .NET-додатків з інструментами захисту;

– Themida - Захищає від кейгенів та кракінгу, обфускує код та додає антидебаг функції;

– ConfuserEx - Обфускатор для .NET, який надає різноманітні функції захисту та обфускації.

Перевагою обфускаційного методу є те що він ускладнює реверс-інжиніринг програм, зменшує ризик витоку конфіденційної інформації, захищає від піратства та незаконного використання програми. Проте в даного методу є і недоліки, серед яких: підвищує складність підтримки та розробки програм, може привести до збільшення обсягу програмного коду, не гарантує 100% захисту.

Дослідження показало, що обфускаційний метод ефективно підвищує рівень захисту програмного забезпечення, роблячи код менш доступним для аналізу та модифікації зловмисниками.

Аналіз результатів попередніх досліджень підкреслив важливість вибору правильного обфускаційного інструменту та стратегії в залежності від конкретного випадку використання.

Висновки та перспективи. Обфускаційний метод є значущим інструментом для підвищення рівня захисту програмного забезпечення від потенційних загроз. Він важливий для забезпечення конфіденційності інформації, недоступності вразливостей та важливий для захисту від атак. Проте важливо враховувати, що обфускація не є універсальним рішенням і має свої обмеження, особливо щодо впливу на продуктивність.

Майбутні дослідження можуть включати: розробку більш ефективних методів обфускації, що мінімізують вплив на продуктивність, дослідження використання обфускації в конкретних галузях, таких як медицина, фінанси та критичні інфраструктури, аналіз потенційних загроз та вдосконалення обфускаційних інструментів для забезпечення високого рівня безпеки в сучасному цифровому світі.

Перелік посилань:

1. Giacobbe, M., Cabitza, A., & Barocas, S. (2019). The future of adversarial thinking. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems // [Електронний ресурс]: https://dl.acm.org/doi/10.1145/3290605.3300733, Дата звернення: 10.10.2023

2. Nagra, J., & Sezer, S. (2010). State-of-the-art in obfuscation techniques for software protection—a survey. ACM Computing Surveys (CSUR), 42(2), 6 // [Електронний ресурс]: https://dl.acm.org/doi/10.1145/1883612.1883617, Дата звернення: 13.10.2023

3. Collberg, C., & Thomborson, C. (2002). Watermarking, tamper-proofing, and obfuscation—tools for software protection. IEEE Transactions on Software Engineering, 28(8), 735-746. // [Електронний ресурс]: https://ieeexplore.ieee.org/document/1025083, Дата звернення: 18.10.2023

4. Raza, S. A., & Rehman, S. U. (2016). An in-depth analysis of code obfuscation. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security // [Електронний ресурс]: https://dl.acm.org/doi/10.1145/2976749.2978300, Дата звернення: 22.10.2023

Корчук Дмитрій Вікторович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ЗАСТОСУВАННЯ ВІДКРИТОЇ ІНФОРМАЦІЇ У СУЧАСНИХ ВІЙНАХ ТА СПОСОБИ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНІ

Сучасний світ наповнений нестримним потоком інформації, що ускладнює її фільтрацію та перевірку. У цьому контексті відкрита інформація (OSINT) стає важливим інструментом як у військовій, так і в цивільній сферах. Проте зі збільшенням доступності інформації зростає ймовірність її ненадійності та використання в інформаційних атаках. У цій роботі ми розглянемо роль відкритих джерел розвідки в сучасних конфліктах та шляхи боротьби з інформаційною війною.

Роль **OSINT** у сучасних війнах.

OSINT – це скорочення від open source intelligence ("розвідка за відкритими джерелами"). Коли джерела інформації розвідника – не таємничі інформатори, а відкриті сайти, реєстри та статистичні дані, такий розвідник називає себе "осінтером". [1]

У сучасних війнах OSINT виступає одним із ключових джерел інформації для аналізу поведінки противника, пошук його слабких сторін та передбачення можливих дій. Відкрита інформація з соціальних мереж, новинних джерел та громадських звітів надає змогу здійснювати аналіз та передбачати ворожі дії, а також виявляти можливі джерела допомоги і підтримки ворога. OSINT допомагає розкривати масштаби воєнних злочинів, що може бути важливим для міжнародних правозахисних організацій.

Виклики та небезпеки **OSINT**.

Збільшення доступності інформації створює великий виклик у плані її перевірки на достовірність та джерело. Фейкові новини та маніпулювання інформацією можуть спричинити серйозні наслідки, включаючи поширення неправдивої інформації, що може вплинути на громадську думку, політичні вибори та міжнародні відносини. Важливо розвивати та вдосконалювати технічні та аналітичні навички для відсіювання дійсної інформації від фейкової.

Інформаційна війна та методи протидії їй.

Інформаційна війна це - форма протиборства між різними суб’єктами (державами, неурядовими, економічними або іншими структурами), яка передбачає проведення комплексу заходів із завдання шкоди інформаційній сфері протилежної сторони та захисту власної безпеки інформаційної. [2].

В ній є три основні мети:

1. Контроль та захист інформаційного простору від ворожих дій;
2. Проведення інформаційних атак на інформаційний простор ворога;
3. Мотивація військового та цивільного населення та демотивація ворога.

Щоб протидіяти інформаційним атакам ворога та захистити свій інформаційний простір можна використовувати наступні речі:

1. Спростувати інформацію ворога напряму;
2. Ліквідувати потенційні канали витіку інформації;
3. Використовувати непряме спростування;

4. Відволікти населення на щось інше.

Враховуючи надзвичайно високу небезпеку, яку несуть агенти інформаційної війни для всіх держав, особливо для їхніх національних органів влади, національні інституту та міжнародні організації повинні розробити відповідну правову базу, яка б враховувала всі можливості сучасної інформаційної війни. Сфокусуватися на виробництві та розвитку інформаційних і телекомунікаційних технологій у сфері державного управління, покращенні здатності національних органів влади та місцевого самоврядування використовувати ефективні методи управління та організації конструктивної взаємодії з громадськістю; акцентувати увагу на недостатній підготовці кадрів у сфері створення та використання інформаційно-комунікаційних технологій, а також сформулював низку заходів щодо вдосконалення професійних стандартів.

Перелік посилань:
1. OSINT в Україні: хто і як допомагає фронту під час війни URL: https://www.pravda.com.ua/columns/2023/01/23/7386112/
2. Інформаційна війна URL: https://vue.gov.ua/iІнформаційна_війна

Костенко Денис Вікторович
Державний університет інформаційно-комунікаційних технологій

ТЕХНОЛОГІЯ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ОБМІНУ ДАННИМИ ВІДДАЛЕНИХ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ VPN

Анотація. Сьогодні, в контексті швидко розвиваючихся інформаційних технологій, питання захисту персональних даних набуває вельми важливого значення, особливо при обміні данними державних установ і організацій, які обробляють і використовують особисту інформацію про фізичних осіб. Відповідно до законодавства України, такого як Закон "Про захист персональних даних" і Закон "Про захист інформації в інформаційно-телекомунікаційних системах", а також ряду підзаконних нормативних актів, такі дані повинні бути надійно захищені від незаконного доступу, зміни та поширення.

У наш час, в умовах стрімкого розвитку інформаційних технологій, комп'ютерні мережі вже не просто важливий атрибут, але невід'ємна частина практично будь-якої сфери діяльності. Вони дозволяють нам виконувати безліч завдань і значно спрощують наші повсякденні дії. Впровадження сучасних інформаційних технологій стало важливою умовою успішного функціонування практично будь-якого бізнесу.

У сучасному світі, інформація є цінним активом та масовим засобом впливу. З цим пов'язане стрімке збільшення кількості кіберзлочинців, які намагаються незаконно здобути доступ до систем підприємств. Засоби масової інформації нерідко повідомляють про кібератаки на різні організації. Для запобігання цьому потрібно докладно розглянути питання модернізації мережі,

особливо в частині кібербезпеки.

Сучасні комп'ютерні мережі - це складні інформаційно-обчислювальні системи з різними архітектурами, які часто взаємодіють з іншими системами. Коли ми використовуємо їх для обробки важливої інформації, такої як збір, зберігання, передача тощо, виникає потреба в спеціалізованих засобах для захисту цієї інформації. Щоб забезпечити найвищий рівень безпеки та відповідати вимогам законодавства щодо захисту інформації, такі засоби повинні бути враховані в архітектурі комп'ютерної інформаційно-обчислювальної системи.

На жаль, на сьогоднішній день не існує універсального рішення для захисту важливої інформації в будь-якій мережі, особливо в корпоративних мережах зі складною архітектурою. Комерційний аспект гри в індустрії кібербезпеки часто веде до пропозицій від розробників, які прагнуть максимізувати свій прибуток, а не завжди враховують реальну потребу і ефективність використання конкретних засобів захисту. В цьому питанні на допомогу може прийти VPN.

На сьогоднішній день існує багато можливостей для реалізації віртуальних приватних мереж (VPN) для різних цілей та сценаріїв використання. Ця різноманітність варіантів виникає з різних вимог та потреб користувачів, які прагнуть забезпечити захист інформації у своїх мережах. Перед користувачами VPN виникає важке завдання вибору належної архітектури VPN, яка б відповідала їх вимогам та забезпечувала необхідний рівень безпеки.

Для правильного вибору архітектури VPN, користувачам важливо розуміти принципи роботи, побудову та відмінності між різними реалізаціями VPN. Особливо актуальним стає використання віртуальних приватних мереж для забезпечення віддаленого доступу до ресурсів, розташованих на різних територіях. Це стає важливим як для організацій, які розпоряджаються різними вузлами та ресурсами, так і для автоматизації процесів у підприємствах.

Комп'ютерні мережі потребують спеціалізованого VPN-сервера для забезпечення можливості користувачам отримувати доступ до приватних мереж через загальнодоступні мережі, такі як Інтернет. Використання VPN-мережі може значно підвищити рівень безпеки передачі даних в мережі та знизити ризик витоку або крадіжки інформації, яка передається через ненадійні зовнішні мережі, такі як Інтернет.

Отже, вибір та належна налаштування VPN-мережі стає дуже важливим аспектом для користувачів, які прагнуть забезпечити захист своїх даних та безпеку мережових з'єднань.

Література

1. Актуальні кіберзагрози: I квартал 2020 року [Електронний ресурс]: Кіберзагрози, інциденти / Positive technologies – 2020. – Режим доступу: World Wide Web. – URL.: https://www.ptsecurity.com/ruru/research/analytics/cybersecurity-threatscape-2020-q1/ - Загол. з екрану (переглянуто 5 жовтня 2020). 2. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О.

Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. — К.: ДУТ, 2015.— 288 с. 3. ТОП 5 найпопулярніших методів соціальної інженерії і методи захисту від них [Електронний ресурс]:

NWU All Rights Reserved – 2020. - Режим доступу: World Wide Web. – URL.:

https://www.nwu.com.ua/ua/novyny-ta-zahody/statti/top-5-najpopuljarnishyh-metodiv-socialnoji-inzheneriji-imetody-zahystu-vid-nyh.html - Загол. з екрану (переглянуто 5 жовтня 2020).

Костровський Денис Володимирович
Студент групи БСДМ-61, ННІЗІ, ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО РЕСУРСІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

Технологія захисту від несанкціонованого доступу до ресурсів інформаційної системи організації обумовлена постійним зростанням загроз для безпеки даних та вимогами до дотримання нормативних актів щодо захисту конфіденційної інформації. Організації повинні розглядати впровадження таких рішень, як Forcepoint DLP, як важливий елемент своєї стратегії інформаційної безпеки для захисту своєї інформації та репутації в цифровому світі.

Використання технології захисту від несанкціонованого доступу до ресурсів інформаційної системи організації на основі рішення Forcepoint DLP має велике значення для організацій, які прагнуть забезпечити конфіденційність інформації та захистити її від несанкціонованого доступу. Ця технологія дозволяє виявляти, моніторити та контролювати рух даних, а також встановлювати ефективні політики захисту. Правильно налаштована і використана Forcepoint DLP може допомогти запобігти витокам даних, а також відповідати вимогам щодо захисту інформації.

Forcepoint DLP захищає організації від втрати даних на основі [6]:

Моніторингу даних під час їх переміщення всередині та за межами організації.

Захист даних під час маніпулювання ними в офісних програмах за допомогою засобів контролю на основі політики, які відповідають бізнес-процесам.

Визначення та ранжування інцидентів високого ризику, щоб допомогти запобігти або виправити втрату та крадіжку даних.

Forcepoint DLP складається з наступних компонентів:

Сервер керування — це машина під керуванням Windows, на якій розміщено Forcepoint Security Manager і програмне забезпечення Forcepoint DLP.

Сервер керування забезпечує основну технологію втрати інформації, фіксуючи відбитки пальців, застосовуючи політики та зберігаючи криміналістику інцидентів. Розгортання може включати кілька серверів Forcepoint DLP для спільного аналізу навантаження, але є лише один сервер керування.

Механізм політики знаходиться на всіх серверах Forcepoint DLP, серверах Web Content Gateway і пристроях Forcepoint Email Security. Механізми політики також інтегровані з Windows і Mac OS X під керуванням Forcepoint DLP Endpoint.

Механізм політики відповідає за аналіз даних і використання аналітики для порівняння їх із правилами в політиках.

Механізм аналітики знаходиться на 64-бітній машині Linux.

Він використовується для ідентифікації потенційно ризикованих інцидентів, їх ранжирування за аналогічною діяльністю та призначення їм оцінки ризику.

База даних політик є сховищем для політик Forcepoint DLP. Для оптимальної продуктивності він зберігається локально на кожному сервері (як база даних відбитків пальців).

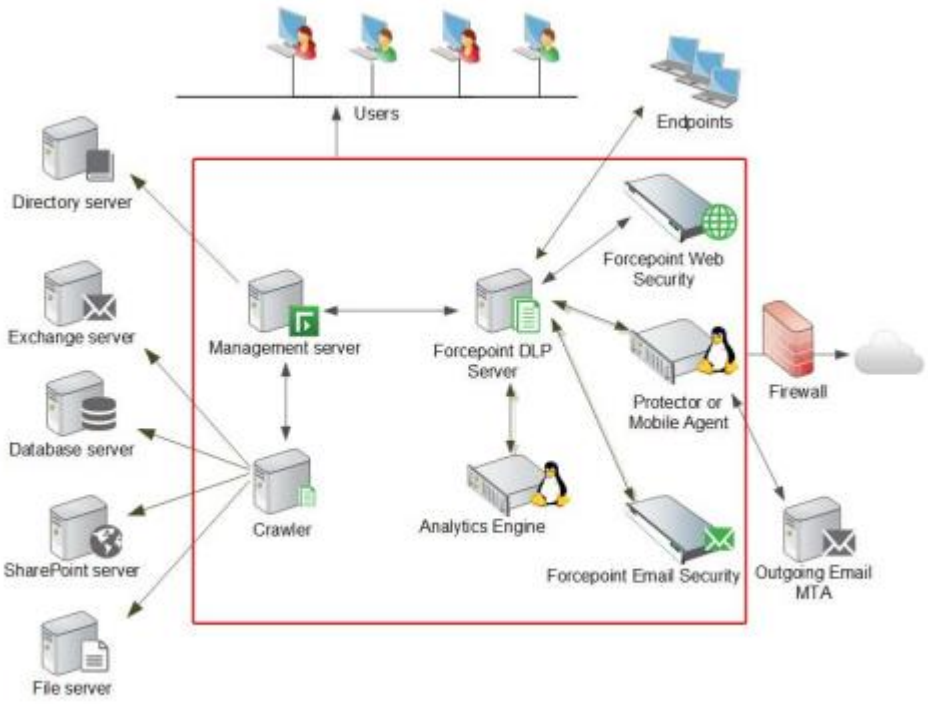


Рис.1. Компоненти Forcepoint DLP [6]

На рис 1. продемонстровано розширені можливості Forcepoint DLP, включені в більш складне мережеве середовище. Воно включає додатковий DLP-сервер Forcepoint і кілька додаткових агентів для підтримки великих обсягів транзакцій і кількості користувачів. Дуже великі розгортання можуть мати кілька серверів і засобів захисту Forcepoint DLP.

Успішне впровадження DLP не може бути досягнуто за допомогою нового технічного дзвоника або свистка, і його не можна поставити на стелажі і скласти в центрі обробки даних. Замість цього, це буде залежати від вашої здатності:

1. Зрозумійте методологію та стратегію реалізації DLP постачальника. Ваша організація отримає вигоду, якщо зрозуміє, як різні постачальники підходять до DLP. Це дозволить вам визначити найбільш перспективні методології постачальників для вашого середовища та технології DLP, які слід

оцінити. Вибір постачальника, який пропонує рішення, що адаптується до ризиків, може додати організації довгострокові переваги, включаючи підвищення ефективності та продуктивності. І не забувайте: застосування методології одного постачальника до технології іншого має негативні довгострокові наслідки.

2. Застосовуйте формулу ризику втрати даних. Після того, як ваша команда безпеки зрозуміє і застосує формулу ризику втрати даних, вона може співпрацювати з власниками даних, щоб визначити і пріоритезувати інформаційні активи. Крім того, кожен діяльність з мінімізації ризиків повинна бути розроблена з єдиною метою - знизити частоту виникнення (ЧВ) даних втрати. RO - це правильний показник для відстеження зниження ризиків і відображення рентабельності інвестицій в засоби контролю DLP. Нагадуємо: будьте особливо уважні, порівнюючи традиційні DLP-рішення з DLP задаптивною до ризиків технологією, щоб переконатися, що ви не порівнюєте хибнопозитивні спрацьовування. до справжнього позитиву.

3. Застосовуйте правило 80/20 для розподілу ресурсів. Зрозумівши, які вектори втрати даних становлять найбільший ризик серйозного витоку даних, ваша організація може використовувати правило 80/20 для розподілу ресурсів і сформулювати ефективні стратегії захисту даних.

4. Дотримуйтесь кроків до успіху DLP. Незалежно від того, чи використовуєте ви традиційний підхід до DLP,чи адаптивний. Дана методологія є формулою для впровадження засобів контролю DLP у спосіб, який є практичним для вашого бізнесу і який забезпечить дієві, вимірювані та адаптовані до ризиків результати.

Перелік посилань

1. Кращі DLP URL: https://ermetic.com/blog/cloud/ibm-cost-of-a-data-breach-2022-highlights-for-cloud-security-professionals/ (дата звернення: 01.10.2023).
2. 11 BEST Data Loss Prevention Software DLP Solutions In 2023URL: https://www.softwaretestinghelp.com/data-loss-prevention-software/ (дата звернення: 02.10.2023).
3. Forcepoint DLP appliances URL: https://help.forcepoint.com/dlp/10/dlphelp/2AA22546-066F-4988-90B5-739055E671DD.html (дата звернення: 15.10.2023).
4. Ultimate Guide to Data Security URL: https://www.forcepoint.com/cyber-edu/data-security (дата звернення: 15.10.2023).

Котецька Вікторія Ігорівна
студентка групи УБД-42, ННІЗІ ДУІКТ, Київ, Україна

АНАЛІЗ ПРОЦЕСІВ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

У даній роботі розглядаються процеси управління ризиками інформаційної безпеки в організації. Докладно аналізуються кроки, включаючи ідентифікацію ризиків, оцінку їх потенційних наслідків і розробку стратегій управління. Обговорено основну мету, яка полягає у зменшенні ризиків, пов'язаних з інформаційною безпекою організації, та наголошено на постійній динаміці цього процесу для забезпечення стійкості інформаційної інфраструктури.

Процеси управління ризиками інформаційної безпеки організації є важливою частиною її діяльності. Вони спрямовані на ідентифікацію, оцінку, мінімізацію та керування ризиками, які можуть впливати на конфіденційність, цілісність та доступність інформації організації.

Основними ключовими аспектами аналізу процесів є:

1. Ідентифікація ризиків: Цей етап включає в себе визначення всіх можливих загроз та вразливостей, які можуть вплинути на інформаційну безпеку організації.
2. Оцінка ризиків: Після ідентифікації ризиків необхідно визначити ймовірність та потенційні наслідки кожного ризику.
3. Управління ризиками: На цьому етапі виробляються стратегії та плани для зменшення або прийняття ризиків.
4. Моніторинг і аудит: Після впровадження стратегій управління ризиками важливо постійно моніторити та аудитувати стан інформаційної безпеки організації.
5. Захист інформації: На практиці, це включає в себе впровадження технологічних рішень, які забезпечують конфіденційність, цілісність та доступність даних.
6. Підготовка персоналу: Важливо навчити персонал організації правилам безпеки, свідомому використанню технологій та виявленню підозрілих дій.
7. Оцінка та перегляд: Регулярна оцінка та перегляд процесів управління ризиками, а також аналіз результатів інцидентів для вдосконалення заходів безпеки. [1]

Ці процеси охоплюють всіх співробітників та структурні підрозділи організації, а також вимагають участі вищих керівників.

Основна мета аналізу полягає в тому, щоб виявити потенційні загрози та ризики для інформаційної безпеки організації та розробити стратегії для їх управління. Головний акцент робиться на зменшення ризиків для організацій включаючи фінансові втрати, репутаційні проблеми, юридичні проблеми, втрату виробничої потужності, зниження якості продукції, втрату ключових співробітників. [2]

Цей аналіз зазвичай виконується спеціалістами в галузі інформаційної безпеки в організації, а іноді може залучати зовнішніх консультантів. Важливо для забезпечення стійкості інформаційної інфраструктури організації та попередження можливих інцидентів і порушень безпеки, що можуть статися через атаки, помилки або природні катастрофи. [3]

Аналіз виконується через використання різних методів, таких як аудит інформації, технічні оцінки, аналіз внутрішніх процесів та дотримання стандартів і законодавства. Цей процес проводиться в офісах та дата-центрах організації і може включати оцінку зовнішніх постачальників і партнерів. Команда, відповідальна за інформаційну безпеку, включає різних спеціалістів, таких як інформаційні аналітики, адміністратори мережі, аудитори інформаційної безпеки і інші фахівці.

Цей процес аналізу ризиків інформаційної безпеки повинен бути постійним і динамічним, оскільки ризики постійно змінюються. Важливо також пам'ятати про важливість усвідомлення всім персоналом організації питань інформаційної безпеки та навчання їх управлінню ризиками в їхніх повсякденних діях.

Перелік посилань:

1. Що таке аналіз ризику: визначення та інструменти | Повний посібник: https://visuresolutions.com/uk/блог/аналіз-ризику/
2. Моделювання процесів аналізу ризиків інформаційної безпеки як спосіб оптимізації витрат: https://doi.org/10.32782/2663-5941/2022.5/13
3. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості системи: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/3663/harasymyurromakavarybiimm.pdf

Кошман Олексій Богданович, БСДМ-61
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ РОЗШИРЕНОГО ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА АТАКИ КОРПОРАТИВНИХ КІНЦЕВИХ ТОЧОК НА БАЗІ FORTIXDR

Визначено мету і основні завдання щодо розширеного виявлення та реагування на атаки корпоративних кінцевих точок. Розглянуто зміст технології розширеного виявлення та реагування на атаки корпоративних кінцевих точок на базі FortiXDR.

Протягом багатьох років організації додавали нові продукти кібербезпеки, щоб протистояти новим загрозам кібербезпеки. Хоча в багатьох випадках вони ефективні окремо, в цілому вони стають непосильними для управління, моніторингу та реагування на них перевантаженими командами безпеки. Як наслідок, організації ризикують пропустити потенційно шкідливі кібератаки, які прослизають крізь щілини, губляться в шумі або не помічаються з інших причин [1].

Сьогодні більшість організацій займаються або планують консолідацію постачальників, сподіваючись підвищити безпеку та операційну ефективність. Однак, щоб успішно реалізувати ці результати, консолідація повинна привести до створення інтегрованого, ефективного і результативного загального рішення для забезпечення безпеки, а не набору незалежних продуктів від одного постачальника. Саме тут може допомогти FortiXDR, заснований на широкому, інтегрованому і автоматизованому рішенні Fortinet Security Fabric з повністю автоматизованим виявленням, розслідуванням і реагуванням на загрози [1]. Це допомагає організаціям підвищити рівень безпеки та операційну ефективність, зменшуючи навантаження на команди безпеки.

Безумовно, важливо виявляти загрози, які в іншому випадку залишаться непоміченими, завдаючи великої шкоди організації. Однак, останнє, що потрібно

більшості команд безпеки - це більше сповіщень. У той час як деякі постачальники використовують підхід, який полягає в тому, щоб зіставити і представити більше інформації про безпеку в одному місці. FortiXDR дозволяє повністю автоматизувати не тільки нормалізацію/кореляцію даних і аналітику виявлення, а й процес розслідування, класифікації та усунення інцидентів. В результаті, це розвантажує, а не створює роботу для команд безпеки, одночасно підвищуючи рівень кібербезпеки [1]. (рис. 1) [2].

Враховуючи зростаючий обсяг, складність та швидкість сучасного ландшафту загроз, перед командами безпеки стоїть більше завдань, ніж будь-коли - в той час, коли персонал та навички з кібербезпеки залишаються в дефіциті. З такою кількістю окремих (часто "найкращих у своєму класі") продуктів безпеки, якими потрібно керувати, інформації про безпеку, яку потрібно аналізувати, і потенційних інцидентів, які потрібно розслідувати, потрібен принципово інший підхід до безпеки підприємства. Ось чому так багато організацій прагнуть до консолідації постачальників і чому нові рішення, такі як XDR, є такими багатообіцяючими. FortiXDR використовує унікальний підхід до повної автоматизації процесу виявлення, розслідування та реагування (рис.1). Це підвищує ймовірність виявлення кібератак, що тривають (до того, як вони перетворяться на витік даних або успішні інциденти з вимогами викупу). Крім того, це зменшує навантаження на команди безпеки, звільняючи їх для більш важливих стратегічних заходів [1].

Як розширення Fortinet Security Fabric, рішення FortiXDR використовує найширший набір телеметричних даних, що надходять від найбільш незалежних сертифікованих засобів управління та охоплюють більшість етапів ланцюжка кіберзагроз, доступних в індустрії. FortiXDR підтримує попередньо налаштоване автоматичне реагування, скоординоване як з продуктами Fortinet, так і з продуктами сторонніх виробників [2].

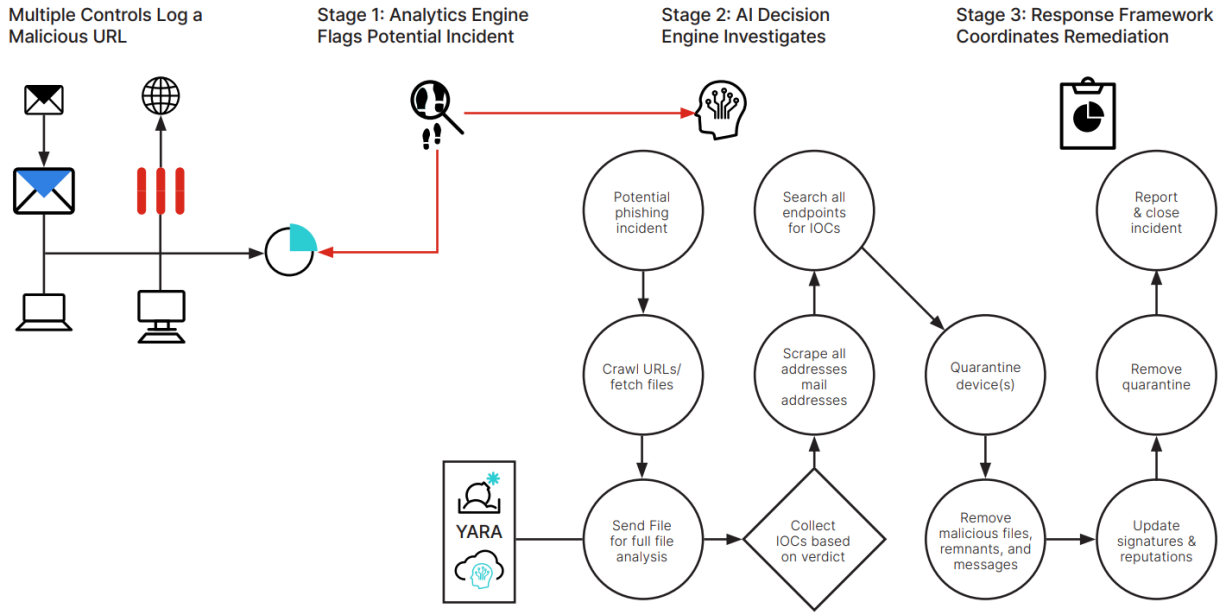


Рис. 1. Зміст технології XDR на прикладі виявлення, розслідування та реагування на фішинг [1]

Найважливіше те, що FortiXDR - це єдине рішення XDR, яке включає в себе штучний інтелект, на який подано заявку на отримання патенту, навчений динамічно проводити розслідування інцидентів, використовуючи мікросервіси, що імітують різні аспекти процесу так само, як це робить експерт-професіонал у сфері безпеки. Побудоване на хмарній платформі FortiEDR, це рішення легко розгортається і постійно підтримується експертами Fortinet [2].

Унікальне виявлення загроз і кореляційна аналітика від FortiGuard Labs постійно відстежують канали безпеки, щоб виявити підозрілу активність. Потім механізм прийняття рішень на основі штучного інтелекту вживає експертних дій для повного розслідування та оцінки будь-якого потенційного інциденту. Нарешті, попередньо встановлені політики виконують дії блокування та виправлення на основі класифікації інцидентів, групи користувачів, рівня ризику та інших критеріїв [2].

Отже, розширене виявлення й реагування (XDR) – це інструмент типу "програмне забезпечення як послуга", який забезпечує комплексний оптимізований захист завдяки інтеграції відповідних продуктів і даних зі спрощеними рішеннями. Оскільки підприємства все частіше стикаються зі складними загрозами й кібератаками, а співробітники працюють у багатохмарних і гібридних середовищах, безпека XDR – це ефективніше рішення для проактивного виявлення інцидентів.

На відміну від таких систем, як протидія загрозам у кінцевих точках (EDR), XDR розширює можливості засобів захисту, а також інтегрує їх у більшу кількість продуктів, зокрема в корпоративні кінцеві точки, сервери, хмарні додатки, електронну пошту тощо. XDR поєднує засоби для запобігання, виявлення, розслідування та реагування, а також забезпечує видимість, аналіз, кореляцію оповіщень про інциденти й автоматичні відповіді, щоб покращити безпеку даних і протидію загрозам.

Перелік посилань:

1. Fully Automate Threat Detection, Investigation, and Response with FortiXDR. SOLUTION BRIEF. Fortinet. URL: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-fully-automate-threat-detection-investigation-response-fortixdr.pdf. (дата звернення: 29.09.2023).
2. Extended Detection and Response. URL: https://www.fortinet.com/products/fortixdr. (дата звернення: 29.09.2023).

Кошовий Єгор Борисович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАХИСТУ ХМАРНОГО СЕРЕДОВИЩА НА БАЗІ CHECK POINT CLOUDGUARD

Хмарне середовище стало важливою складовою багатьох компаній. Від зберігання інформації і баз даних до серверів та мережевого програмного забезпечення – хмара є недорогим і безцінним інструментом. Дослідження [1] показали, що 94% підприємств використовують хмарні сервіси; 67%

корпоративної інфраструктури базується в хмарі.

Не слід забувати про загрози які несе з собою використання хмарних сервісів. Згідно дослідження [2], найрозповсюдженішими загрозами є витік даних(data breach), неправильні налаштування хмарного середовища(cloud misconfigurations), хмарне ШПЗ та ботнети. У травні 2022 року неправильна конфігурація хмари в McDonald's розкрила інформацію про співробітників, зокрема номери соціального страхування та реквізити банківських рахунків, майже 12 000 працівників по всій Північній Америці. У лютому 2022 року неправильна конфігурація Google Cloud Storage призвела до розголошення особистої інформації понад 23 мільйонів клієнтів роздрібного продавця спортивних товарів.

Забезпечення нормальної роботи та необхідного рівня захисту хмарного середовища є важливим пріоритетом для підприємства. На ринку існує багато рішень які тільки частково покривають проблеми пов’язані з безпекою в хмарі. Необхідна єдина платформа яка забезпечує захист та моніторинг хмарних сервісів організації.

Check Point CloudGuard забезпечує автоматизоване запобігання загрозам для захисту хмарних активів і робочих навантажень від найскладніших кібератак. До особливостей та переваг CloudGuard можна віднести: уніфіковану безпеку для багатохмарної інфраструктури, автоматизований DevSecOps та управління засобами безпеки в хмарі.

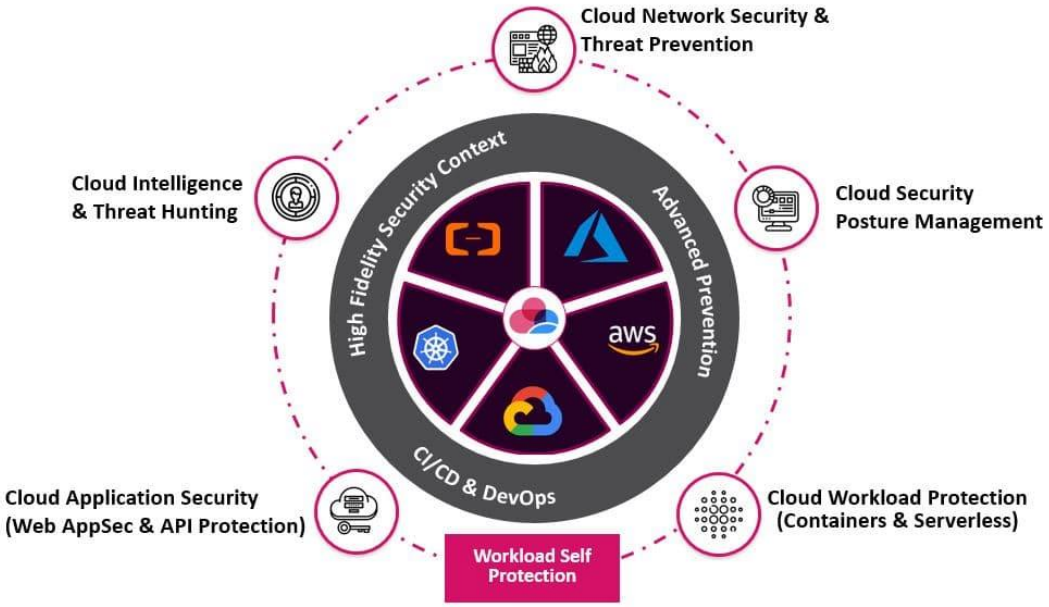


Рис. 1. Можливості Check Point CloudGuard [3]

Cloud Web App & API Protection. CloudGuard наближає безпеку додатків до межі робочого навантаження, надаючи кращий захист в реальному часі, ніж звичайні брандмауери веб-додатків (WAF). CloudGuard надає захист для веб-додатків та прикладних програмних інтерфейсів(API) від найскладніших типів загроз завдяки автоматизованій єдиній платформі безпеки.

Cloud Intelligence and Threat Hunting. CloudGuard надає security forensics за допомогою багатофункціональної візуалізації машинного навчання,

беручи до уваги контекст загроз та аномалій в хмарному середовищі.

Cloud Network Security & Threat Prevention. CloudGuard забезпечує запобігання загрозам і безпеку мережі через віртуальний шлюз безпеки — автоматизований та уніфікований як для хмарного так і для локальних середовищ.

Cloud Security Posture Management (CSPM). CloudGuard запобігає заданню критично неправильних конфігурацій безпеки та забезпечує комплаєнс з більш ніж 50 фреймворками та кращими практиками.

Cloud Workload Protection. CloudGuard виконує оцінку вразливостей і захист під час виконання хмарних робочих навантажень, що включає в себе безсерверні функції та контейнери. Це забезпечує автоматизацію безпеки при мінімальних витратах на хмарне середовище.

Отже, Check Point CloudGuard забезпечує автоматизований захист хмарного середовища організації та надає повну інформацію про стан відповідного середовища та його аномалії в реальному часі. Рішення використовує бази знань про вразливості і використовує штучний інтелект для аналізу поточної ситуації в середовищі для коректної візуалізації. Рішення позиціонує себе як єдина платформа для запобігання загроз та захисту хмарного середовища.

Перелік посилань:

1. 25 Amazing cloud adoption statistics [2023]: cloud migration, computing, and more URL: https://www.zippia.com/advice/cloud-adoption-statistics/ (дата звернення 24.10.2023)
2. Cloud Security Threats to Watch Out for in 2023: Predictions and Mitigation Strategies URL: https://cloudsecurityalliance.org/blog/2023/06/29/cloud-security-threats-to-watch-out-for-in-2023-predictions-and-mitigation-strategies/ (дата звернення 24.10.2023)
3. CloudGuard for Cloud Native Security URL: https://www.checkpoint.com/cloudguard/ (дата звернення 24.10.2023)

Крочак Руслан Петрович
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ЗАГРОЗ ШЛЯХОМ МОНІТОРИНГА МЕРЕЖІ НА ОСНОВІ SOC

Питання кіберзахисту є важливим для України та світу з огляду на світові тенденції та агресивну війну, яку розпочала росії. Війна на кіберфронті України розпочалася у 2014 році, коли росія здійснила масовану DDoS-атаку на Дарницьку ТЕЦ. За цим послідували інші атаки. Через три дні після російського повномасштабного вторгнення в лютому кількість кібератак на український державний та військовий сектор зросла на 196% порівняно з довоєнним рівнем. Рекордсменом стали 275 DDoS-атак на день. Найпотужніші перевищували 100 Гбіт/с.

Процесом виявлення і реагування зазвичай займаються аналітики в центрах моніторингу інформаційної безпеки (SOC). Зазвичай Security Operations Center працює в режимі 24/7 та вирішує питання з кібербезпеки та інформаційної системи організації на технічному та організаційному рівні[1].

Security Operation Center (SOC) є невід'ємною складовою сучасних організацій, забезпечуючи неперервний моніторинг, аналіз та реагування на інциденти інформаційної безпеки. Централізоване управління безпековими заходами, виявлення аномальних активностей та вчасне реагування на загрози забезпечують високий рівень захисту даних, інфраструктури та репутації компанії. Інноваційні технології, такі як штучний інтелект та аналітика великих даних, роблять SOC більш ефективними, забезпечуючи точні та швидкі реакції на сучасні кіберзагрози. Успішна робота SOC відображається не лише на безпеці компанії, але й на її стабільності та довірі клієнтів, що робить його невід'ємною частиною сучасного бізнес-ландшафту. SOC є ключовим компонентом в сучасних стратегіях кібербезпеки, який об'єднує в собі технології, процеси та експертність для надійного виявлення, аналізу та реагування на кіберзагрози. SOC забезпечує захист інформації, зберігаючи довіру клієнтів та гарантуючи незалежність від зростаючих загроз у цифровому світі[2].

Також варто зазначити, SOC не займається розробкою політик та процедур, а скоріше здійснює моніторинг за всіма аспектами мережі корпорації, щоб виявити будь-яку нетипову поведінку, таку як незвичайна активність на серверах, кінцевих точках, базах даних, програмах і всьому іншому апаратному чи програмному забезпеченні.

Таким чином, Security Operations Center відіграє важливу роль у сучасному цифровому світі, забезпечуючи високий рівень захисту для підприємств та їх клієнтів, забезпечуючи спокій та довіру в глобальному цифровому середовищі.

Перелік посилань:

1. What is a Security Operations Center (SOC)? [Електронний ресурс] / Режим доступу до ресурсу: https://www.mcafee.com/enterprise/ru-ru/security-awareness/operations/what-is-soc.html
2. What is a Security Operations Center (SOC)? [Електронний ресурс] / Nate Lord Режим доступу до ресурсу: https://digitalguardian.com/blog/what-security-operations-center-soc

Кузьменко Олександр Тарасович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

АКТУАЛЬНІСТЬ ПРОБЛЕМИ ВИКОРИСТАННЯ ПРОТИПРАВНОГО ЛІНКБІЛДІНГУ

Споживачі інформації в сучасному цифровому світі довіряють пошуковим системам, які надають результати пошуку, які базуються на релевантності та авторитеті веб-сайтів. Це призвело до розвитку тактик оптимізації для пошукових систем, зокрема лінкбілдінгу - процесу створення посилань на веб-сайт для підвищення його рейтингу в пошукових системах. Проте існує важлива різниця між законним і протиправним лінкбілдінгом, і саме останній представляє серйозну загрозу для кібербезпеки.

Протиправний лінкбілдінг охоплює різноманітні недобросовісні та шкідливі практики, що включають створення посилань на веб-сайти з метою підвищення їхнього рейтингу в пошукових системах, нехтуванням законами та етичними нормами. Ця проблема стає особливо актуальною з точки зору кібербезпеки, на це можуть впливати важливі аспекти:

1. Розповсюдження шкідливого вмісту: Протиправний лінкбілдінг може призвести до поширення вірусів, троянських коней, різноманітних шкідливих програм та інших кіберзагроз. Зловмисники можуть вставляти шкідливі посилання або код на веб-сайти, які незахищені, завдаючи шкоди користувачам, які переходять за цим посиланням.
2. Фішинг та обман: Протиправний лінкбілдінг може використовуватися для створення фішингових атак, коли користувачі обманюються та переконуються перейти за посиланнями, що містять обманливий або шахрайський вміст. Це може призвести до витоку конфіденційної інформації та погіршення репутації компаній.
3. Погіршення репутації веб-сайту: Використання недобросовісних методів лінкбілдінгу може призвести до покарань від пошукових систем. В результаті веб-сайт може втратити свою видимість у пошукових результатах або навіть бути видалений з індексу. Це має серйозні наслідки для бізнесів та інтернет-проектів.
4. Спам та збільшення ризику кросс-сайтового скриптінгу (XSS) та кросс-сайтового запиту (CSRF): Протиправний лінкбілдінг може включати в себе вставку шкідливого коду в посилання або анкорний текст. Це створює загрозу кросс-сайтового скриптінгу (XSS) та кросс-сайтового запиту (CSRF), що можуть бути використані для атак на веб-сайти та їхніх користувачів.
5. Недовіра користувачів: Користувачі, які виявляють недобросовісні практики лінкбілдінгу на веб-сайтах, можуть втратити довіру до інтернет-ресурсів. Це може призвести до зниження активності користувачів та втрати репутації веб-сайту.

Протиправний лінкбілдінг створює екосистему загроз для кібербезпеки, і боротьба з цією проблемою є надзвичайно важливою. Існує кілька рекомендацій, які можуть бути прийняті для захисту від протиправного лінкбілдінгу та покращення кібербезпеки:

- Важливо регулярно аналізувати беклінк-профіль веб-сайту та відхиляти недобросовісні або небажані посилання за допомогою інструментів, які надають пошукові системи або сторонні сервіси, такі як Google Disavow Tool.
- Власники веб-сайтів повинні проводити регулярний аудит безпеки свого сайту для виявлення можливих вразливостей та загроз кібербезпеці. Вчасне усунення цих проблем може допомогти запобігти атакам.
- Використання законних та етичних методів лінкбілдінгу допомагає забезпечити безпеку веб-сайту та зберегти його репутацію. Відмова від недобросовісних практик є ключовою для збереження довіри користувачів та пошукових систем.
- Важливо навчати співробітників та користувачів щодо ризиків, пов'язаних із протиправним лінкбілдінгом та загрозами кібербезпеки. Навички та свідомість щодо безпеки важливі для запобігання інцидентам.

Протиправний лінкбілдінг становить серйозну загрозу для кібербезпеки, яка має потенційно серйозні наслідки для веб-сайтів та користувачів. Боротьба з цією проблемою вимагає обачливості, спільних зусиль та свідомості щодо

ризиків, які вона представляє. Захист від протиправного лінкбілдінгу та покращення кібербезпеки є завданням, яке потребує постійної уваги та дій.

Перелік посилань:
1. What is Black Hat SEO? URL https://blog.hubspot.com/marketing/black-hat-seo#:~:text=Black%20hat%20SEO%20goes%20against,and%20a%20good%20user%20experience.
2. Why Outsource Link Building? The Pros and Cons You Need to Know URL: https://editorial.link/outsource-link-building-the-pros-and-cons/#:~:text=Risks%3A%20Low%2Dquality%20links%20from,%2C%20inconsistency%2C%20and%20reputation%20damage.

Лабяк Дар'я Сергіївна
УБДМ-61, ДУІКТ, Київ, Україна

ЗАСАДИ ПРОТИДІЇ ВНУТРІШНІМ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

Протидія внутрішнім загрозам має вирішальне значення у забезпеченні інформаційної безпеки підприємства і має охоплювати комплекс різноманітних заходів для виявлення й ефективного вирішення проблем, пов'язаних з халатною чи деструктивною діяльністю персоналу, використовувати сучасні програмні засоби з метою моніторингу й аналізу діяльності працівників компанії.

Забезпечення інформаційної безпеки в компанії вимагає комплексного підходу та застосування різних методів і технологій для протидії внутрішнім загрозам. Адже, без належного захисту організація втрачатиме як довіру своїх клієнтів, так і свій дохід.

Запобігання і протидія внутрішнім загрозам інформаційній безпеці підприємства - це комплекс заходів і стратегій, які призначені для запобігання, виявлення та ефективного врегулювання загроз, що виникають внаслідок дій або бездіяльності співробітників, партнерів чи інших осіб, які мають доступ до будь-якого виду інформації та ресурсів підприємства. Gartner визначає таке дерево внутрішніх загроз (рис.1) [1]:

Рис.1- Дерево внутрішніх загроз

До внутрішніх загроз відносять:

1. Неналежне керування правами доступу до різних систем. Наприклад, компанія періодично не переглядає, хто з користувачів має доступ і якого типу, чи надаються права адміністратора користувачам без нагальної потреби.

2. Відсутність політик і процедур безпеки. В організації не належним чином впроваджені задокументовані процеси, а працівники не ознайомлені з ними.

3. Внутрішнє шпигунство та крадіжки інтелектуальної власності. Відомим прикладом крадіжки інтелектуальної власності є проникнення в системи німецького партнера BioNTech виробника ліків США Pfizer. Pfizer подав до суду на співробітника, який збирався піти в іншу компанію після того, як викрав безліч конфіденційних документів. Частина викраденої інтелектуальної власності була пов'язана з розробкою компанією вакцини проти COVID-19 [2].

Для своєчасного реагування та зменшення ризиків внутрішніх загроз в підприємству необхідно використовувати засоби моніторингу, аналізатори поведінки користувачів, логувати будь-які дії користувачів при доступі до критичних інформаційних систем [3].

На ринку існує різноманітне програмне забезпечення, яке допомагає компаніям покращити інформаційну безпеку в контексті протидії внутрішнім порушникам. Загалом їхня ідея полягає в тому, щоб стежити за діяльністю співробітників і виявляти потенційні загрози. Залежно від специфіки рішення та бізнес-потреб таке програмне забезпечення може збирати різні дані, зокрема про:

- Інтернет-активність користувача: відвідані веб-сайти, обмін електронними листами, завантаження файлів і програм, онлайн-пошук.
- діяльність на робочому місці: маніпуляції з файлами та даними, запущені програми, підключені USB-пристрої.

Сучасні технології значно вдосконалили рішення для моніторингу діяльності користувачів, і тепер Gartner виділяє дві основні категорії такого програмного забезпечення: інструменти, орієнтовані на внутрішні загрози, і рішення, які забезпечують широку аналітику поведінки користувачів і організацій (UEBA) [1].

Отже, протидія внутрішнім загрозам має вирішальне значення у забезпеченні інформаційної безпеки підприємства, яке має здійснювати комплекс різноманітних заходів для виявлення й ефективного вирішення проблем, пов'язаних з халатною чи деструктивною діяльністю персоналу, використовувати сучасні програмні засоби з метою моніторингу й аналізу діяльності працівників компанії.

Перелік посилань:
1. What Is an Insider Threat? Definition, Types, and Countermeasures.
URL: https://www.ekransystem.com/en/blog/insider-threat-definition
2.Pfizer sues departing employee it says stole COVID-19 vaccine secrets.
URL: https://www.reuters.com/ business/healthcare-pharmaceuticals/pfizer-sues-departing-employee-it-says-stole-covid-19-vaccine-secrets-2021-11-24/

3. 10 ways to prevent computer security threats from insiders.
URL: https://www.techtarget.com/searchsecurity/feature/Ten-ways-to-prevent-insider-security-threats

Легомінова Світлана Володимирівна,д.е.н.,проф.,
Тюленінов Андрій Сергійович,
студент групи УБДМ-61,
ННІЗІ ДУІКТ, Київ, Україна

ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА: СУТНІСТЬ, ОЗНАКИ, ПРОЦЕСИ ОБРОБКИ ІНЦИДЕНТІВ

Засадами забезпечення інформаційної безпеки підприємства є створення реальної дієвої системи інформаційної безпеки підприємства, яка буде здатна до зниження ризиків та нівелювання або запобігання виникненню негативних наслідків від інцидентів інформаційної безпеки. Тому у фокусі роботи кожного підприємства має бути налагодження такої системи, її аналіз, корегування політик безпеки, виявлення причин виникнення інцидентів.

Інцидент інформаційної безпеки (information security incident) – одинична подія або ряд небажаних і непередбачених подій інформаційної безпеки, через які існує ймовірність компрометації бізнес-інформації і загрози інформаційній безпеці.

До інформаційних активів підприємства відносимо:

- інформація: бази даних та файли даних, контракти та угоди, системна документація, дослідницька інформація, настанови для користувачів, навчальний матеріал, процедури функціонування або підтримки, плани безперервності бізнесу, заходи щодо його відновлення, журнали аудиту та архівна інформація;
- програмні активи: прикладне програмне забезпечення, системне програмне забезпечення, засоби розробки та утиліти;
- фізичні активи: комп'ютерне обладнання, телекомунікаційне обладнання, замінювані носії та інше обладнання
- послуги: обчислювальні та телекомунікаційні послуги, комунальні послуги, наприклад, опалення, освітлення, енергопостачання та кондиціювання повітря;
- люди та їх кваліфікація, навички та досвід;
- нематеріальні активи, такі як репутація та імідж організації [4].

Виявлення того ,що інцидент стався має характеризуватись ключовими ознаками, а саме [1]:

1. Повідомлення про інцидент ІБ надходять одночасно з декількох джерел (користувачі, IDS, файли журналів тощо);
2. IDS сигналізують про багаторазове повторення певних подій;
3. Аналіз файлів журналів автоматизованої системи (АС) дає підставу для висновку про можливість настання інциденту.

Для обробки подій та інцидентів інформаційної безпеки необхідно

організувати процес реагування на інциденти. Потім слід розробити необхідні нормативні документи щодо управління інцидентами. Як правило, такі документи повинні описувати [2]:

1. Визначення інциденту ІБ – перелік подій, що є інцидентами (тобто, що саме в цій організації є інцидентом ІБ);

2. Порядок сповіщення відповідальної особи про виникнення інциденту (необхідно визначити формат звіту, а також відобразити контактну інформацію осіб, яких слід оповіщати про інцидент);

3. Порядок усунення наслідків і причин інциденту;

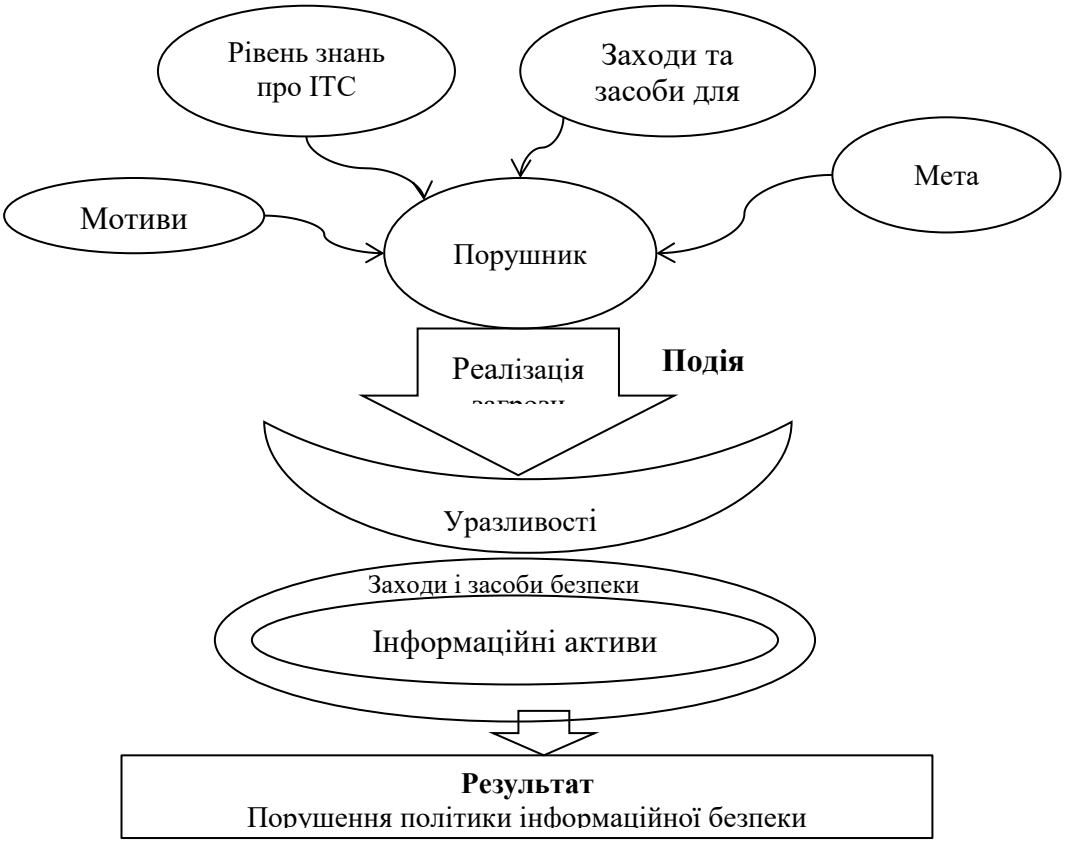
4. Порядок розслідування інциденту (визначення причин інциденту, винних у виникненні інциденту, порядок збору і збереження доказів);

5. Внесення дисциплінарних стягнень;

6. Реалізація корегуючих і превентивних заходів.

Алгоритмом дій щодо розкриття інциденту має слугувати визначення ключових етапів роботи інформаційної системи та її складових. на етапі експлуатації є розслідування інцидентів.

Графічна інтерпретація сутності інциденту інформаційної безпеки наведено на рисунку 1.



Основним елементом даної моделі є інформаційні активи підприємства, оскільки саме проти них спрямовується негативна подія або низка небажаних і непередбачених подій інформаційної безпеки, в результаті їх впливу відбувається порушення політики інформаційної безпеки.

Отже, запобіганню виникнення інцидентів має слугувати чітке розуміння

самого інциденту інформаційної безпеки, що має бути захищеним на підприємстві, основні характерні ознаки інциденту для його виявлення. В основі організації обробки подій та інцидентів інформаційної безпеки мають бути розроблені нормативні документи чітких дій.

Перелік посилань:

1. Звіт «Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ» (КСЗІ АІС НАНУ): Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. 05540149.90000.043.И3-06. Київ.: НАН України 2009. 149 с.

2. Гнатюк С.О., Хохлачова Ю.Є., Охріменко А.О., Гребенькова А.К. Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки. *Захист інформації*. 2012. №1 (54). URL:https://jrnl.nau.edu.ua/index.php/ZI/article/view/2073

3. ISO/IEC 27005:2011(E). URL: http:// www.klubok.net/Downloads-index-reqviewdownloaddetails-lid-421.html.

4. Інформаційні технології. Методи захисту. Звіт правил для управління інформаційною безпекою : ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Київ: Національний банк України. 2010. 163 с. :

Лисенко Петро Олександрович
студента групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ОРГАНІЗАЦІЇ ДОСТУПУ ДО КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ПРОТОКОЛУ RADIUS

У сучасному суспільстві, коли величезна кількість даних та інформації зберігається в цифровому вигляді, забезпечення кібербезпеки є більш важливим, ніж будь-коли. Небажане втручання та атаки на інформаційні системи можуть призвести до витоку секретної інформації або навіть закриття компанії. Одним з найважливіших аспектів забезпечення кібербезпеки є організація доступу до бізнес-мережі, а одним з найефективніших методів для цього є протокол RADIUS.

Протокол RADIUS дозволяє здійснювати аутентифікацію, авторизацію та моніторинг користувачів, які намагаються отримати доступ до мережевих ресурсів. Він був створений для забезпечення безпеки та контролю доступу до мережі, включаючи бездротові мережі Інтернету, внутрішні бізнес-мережі та інші системи. Можливість централізовано керувати аутентифікацією та авторизацією користувачів, а також записувати їхні дії є однією з ключових переваг протоколу RADIUS.

Організація доступу до бізнес-мережі з використанням протоколу RADIUS включає в себе наступні процедури:

1. Автентифікація користувача: При спробі доступу до мережі користувач зазвичай повинен ввести ім'я користувача і пароль. Ця інформація надсилається на сервер RADIUS для перевірки. Сервер перевіряє, чи є користувач у списку дозволених і чи дійсні його дані. Якщо користувач автентифікований, йому надається доступ до мережі.

2. Авторизація користувача: Після успішної автентифікації RADIUS-сервер визначає ресурси користувача та його права доступу. Цей етап дозволяє налаштувати параметри для кожного користувача, регулювати рівні доступу, а також визначити, які сервіси та ресурси доступні.

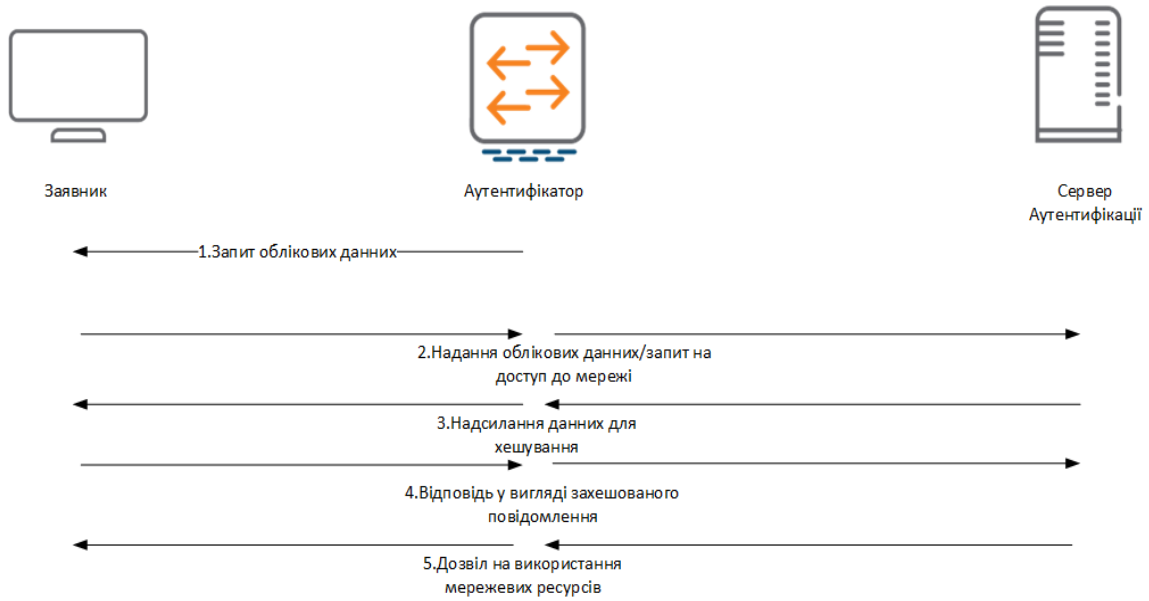


Рис. 1. Процес автентифікації та авторизації користувача

3. Облік користувачів: Протокол RADIUS має можливість реєстрації подій та обліку використання мережевих ресурсів. Це дозволяє контролювати поведінку користувачів, виявляти можливі небезпеки та реагувати на них.

Технологія RADIUS має наступні переваги для контролю доступу:

- Централізоване управління: RADIUS дозволяє керувати всіма елементами доступу до мережі з одного місця. Це спрощує адміністрування і гарантує одноманітність управління користувачами.

- Високий рівень безпеки: Для забезпечення надійності і стійкості до атак протокол RADIUS використовує ряд функцій безпеки, включаючи шифрування паролів і зашифрований зв'язок.

- Проста інтеграція: RADIUS легко інтегрується з існуючими інформаційними системами та каталогами користувачів.

- Масштабованість: Оскільки RADIUS підтримує велику кількість користувачів і пристроїв, його можна використовувати в широкому діапазоні ситуацій.

Використання протоколу RADIUS для організації доступу до бізнес-мережі є ефективним методом забезпечення безпеки і контролю над мережевими ресурсами. Ця система дозволяє централізовано керувати користувачами, а також забезпечити надійний захист і облік користувачів. В умовах зростаючих ризиків кібербезпеки використання RADIUS допомагає знизити ризик виникнення подій і забезпечує стабільне функціонування бізнес-мережі.

Перелік посилань:

1. Droms, R., & Baker, F. (2000). "RFC 2865 - Remote Authentication Dial In User Service (RADIUS)". IETF. Посилання
2. Beadles, M. (1997). "RFC 2058 - A One-Time Password System". IETF. Посилання

Лозовий Олександр Вячеславович

студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ХМАРНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ CSPM WIZ

CSPM (Cloud Security Posture Management) - це системи, які спрямовані на забезпечення безпеки хмарних ресурсів шляхом моніторингу та управління конфігураціями. Їх основна мета - виявлення та виправлення небезпечних конфігурацій і вразливостей у хмарних середовищах. Важливість CSPM для хмарного середовища компанії полягає у наступних аспектах.

1) Неправильні конфігурації можуть викрити чутливі дані або ресурси компанії. CSPM допомагає виявляти та виправляти такі конфігурації, зменшуючи ризик порушення безпеки.
2) Багато галузевих стандартів та регулятивних актів вимагають належного управління хмарними ресурсами. CSPM допомагає компаніям відстежувати та демонструвати дотримання цих вимог.
3) З ростом хмарних ресурсів стає все важче відстежувати їх конфігурацію ручним способом. CSPM автоматизує цей процес, що спрощує управління безпекою.
4) CSPM система забезпечує детальний огляд стану безпеки, що дає можливість командам з безпеки легко визначати проблемні зони та пріоритети.
5) Може інтегруватися з іншими системами (як-от SIEM, системами ідентифікації загроз та ін.) для надання всебічного погляду на безпеку та координованого реагування на інциденти.

Як приклад важливості використання CSPM можна навести недавній епізод з критичною вразливістю у продуктах NetScaler ADC і NetScaler Gateway, яка може призвести до несанкціонованого розкриття чутливої інформації (CVE-2023-4966) [1]. Бюлетень був випущений 10 жовтня 2023 року разом з оновленням безпеки. Вразливість має CVSS-рейтинг 9,4, що вказує на її критичну серйозність. Вона виникає через помилку в коді, яка дозволяє зловмисникам надсилати спеціально сформовані запити, які можуть призвести до виведення на екран інформації, яка не повинна бути доступна. Ця інформація може включати імена користувачів, паролі, ключі шифрування та інші конфіденційні дані.

За допомогою CSPM системи WIZ адміністратор безпеки хмарних середовищ може легко перевірити наявність цієї вразливості в хмарній системі організації і спланувати кроки для її усунення у разі потреби. На приклад такий запит до WIZ, знаходить у хмарних середовищах організації всі екземпляри CVE-2023-4966, що присутні на всіх вразливих віртуальних машинах [2]:

https://app.wiz.io/graph#~(query~(relationships~(~(type~(~(type~'CAUSES))~with~(relationships~(~(type~(~(type~'ALERTED_ON))~with~(as~'scoped_entity~relationships~(~(optional~true~type~(~(reverse~true~type~'CONTAINS))~with~(as~'optional_scoped_group~select~true~type~(~'COMPUTE_INSTANCE_GROUP))))~

select~true~type~(~'VIRTUAL_MACHINE~'CONTAINER_IMAGE~'SERVERLESS))))~select~true~type~(~'SECURITY_TOOL_FINDING))))~type~(~'VULNERABILITY)~where~(name~(EQUALS~(~'CVE-2023-4966)))~select~true)~view~'graph)

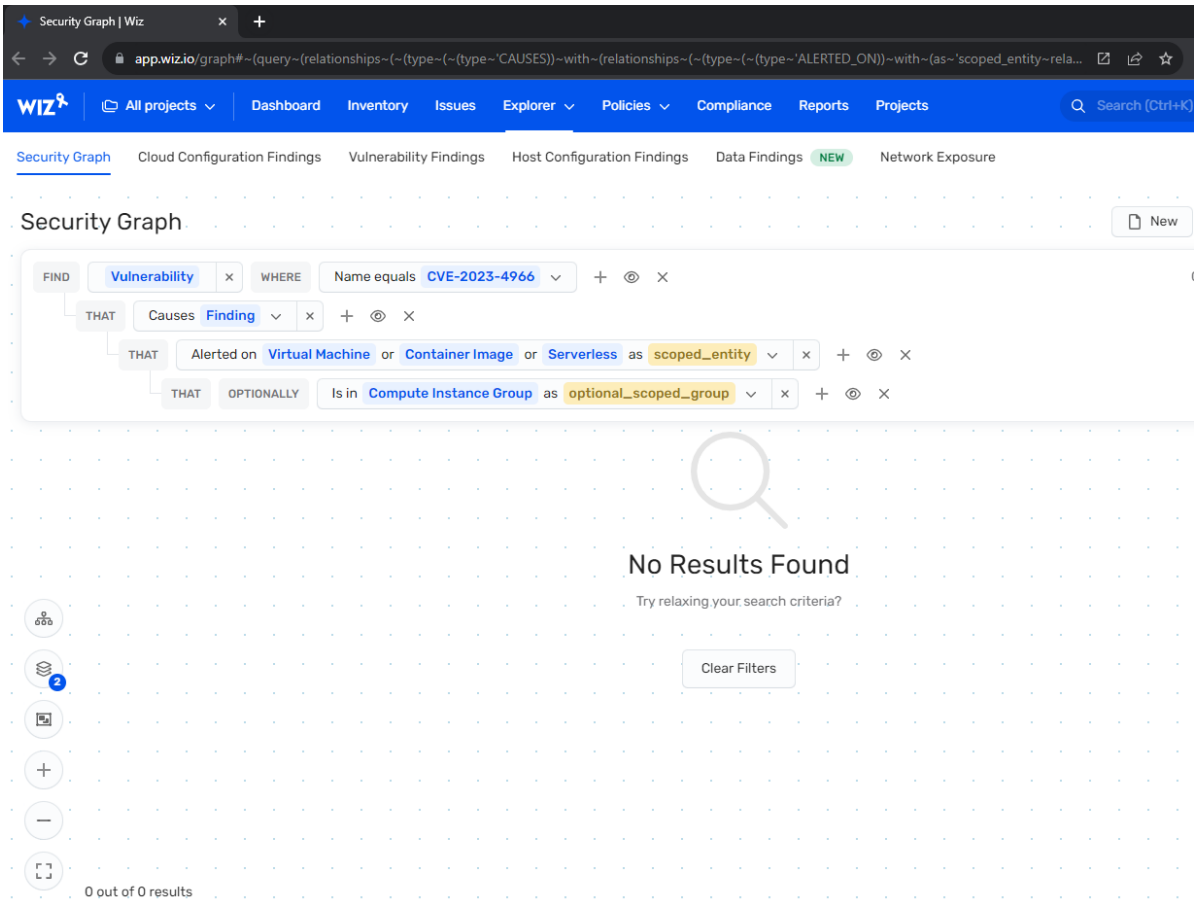


Рис.1. Приклад запита у WIZ для відображення вразливості CVE-2023-4966 у хмарних середовищах організації

На відміну від попереднього цей запит фокусується лише на машинах, що доступні із Інтернет і таким чином дозволяє сфокусуватися на усуненні вразливостей для найбільш ризикових ресурсах:

https://app.wiz.io/graph#~(query~(relationships~(~(type~(~(type~'CAUSES))~with~(relationships~(~(type~(~(type~'ALERTED_ON))~with~(as~'scoped_entity~relationships~(~(optional~true~type~(~(reverse~true~type~'CONTAINS))~with~(as~'optional_scoped_group~select~true~type~(~'COMPUTE_INSTANCE_GROUP)))~(type~(~(type~'SERVES))~with~(type~(~'ENDPOINT)~select~true~where~(portValidationResult~(NOT_EQUALS~(~'Closed))))))~select~true~type~(~'VIRTUAL_MACHINE~'SERVERLESS))))~select~true~type~(~'SECURITY_TOOL_FINDING))))~type~(~'VULNERABILITY)~where~(name~(EQUALS~(~'CVE-2023-4966)))~select~true)~view~'graph)

Перший запит повертає 0 результатів через відсутність вразливих ресурсів. Другий запит повертає підмножину ресурсів порівняно з першим запитом (лише доступні з інтернет) і тому кількість результатів незмінна.

Перелік посилань:
1. NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967 URL: https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967 (дата звернення: 23.10.2023).
2. Critical and high severity flaws in NetScaler exploited in-the-wild https://docs.wiz.io/wiz-docs/docs/wiz-adv-2023-079 (дата звернення: 23.10.2023).

Лозовський Сергій Дмитрович
студентка групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

РОЗРОБКА СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРАТАКАМ У ГАЛУЗІ МОБІЛЬНИХ ДОДАТКІВ ТА ІОТ-ПРИСТРОЇВ

Розробка ефективної системи виявлення та запобігання кібератак у галузі мобільних додатків та IoT-пристроїв є критично важливою для забезпечення безпеки та захисту основних інфраструктур та приватності користувачів в умовах швидкого росту цих технологій. Ця система повинна використовувати передові методи шифрування, а також механізми виявлення аномалій та машинного навчання для постійного моніторингу та реагування на потенційні загрози. Додатково, важливо враховувати специфічні особливості мобільних додатків та IoT-пристроїв, такі як обмежені ресурси та зв'язані з ними виклики. Розробка такої системи сприятиме забезпеченню безпеки в цих областях і допоможе запобігти серйозним наслідкам кібератак.

Системи виявлення та запобігання кібератакам в галузі мобільних додатків та IoT-пристроїв відіграють критичну роль у забезпеченні безпеки і захисту основних інфраструктур та приватності користувачів. Ось як вони допомагають у житті:

1. Захист від даних та приватності: Ці системи допомагають захищати особисті дані користувачів мобільних додатків та IoT-пристроїв від несанкціонованого доступу.

2. Запобігання втраті даних: Вони допомагають уникнути втрати важливих даних через кібератаки, що можуть спричинити серйозні фінансові та репутаційні збитки.

3. Забезпечення безпеки IoT-пристроїв: Ці системи виявляють та блокують спроби зламу IoT-пристроїв, що можуть мати віддалені наслідки, наприклад, злам автоматизованих систем вдома.

4. Захист від зловмисних додатків: Вони виявляють та блокують завантаження та використання зловмисних додатків на мобільних пристроях.

Приклад: Системи виявлення кібератак, такі як файрволи та системи моніторингу мережі, можуть блокувати спроби несанкціонованого доступу до IoT-пристроїв у розумному будинку, щоб запобігти віддаленим керуванням та злому системи безпеки. Це допомагає зберегти безпеку проживання.

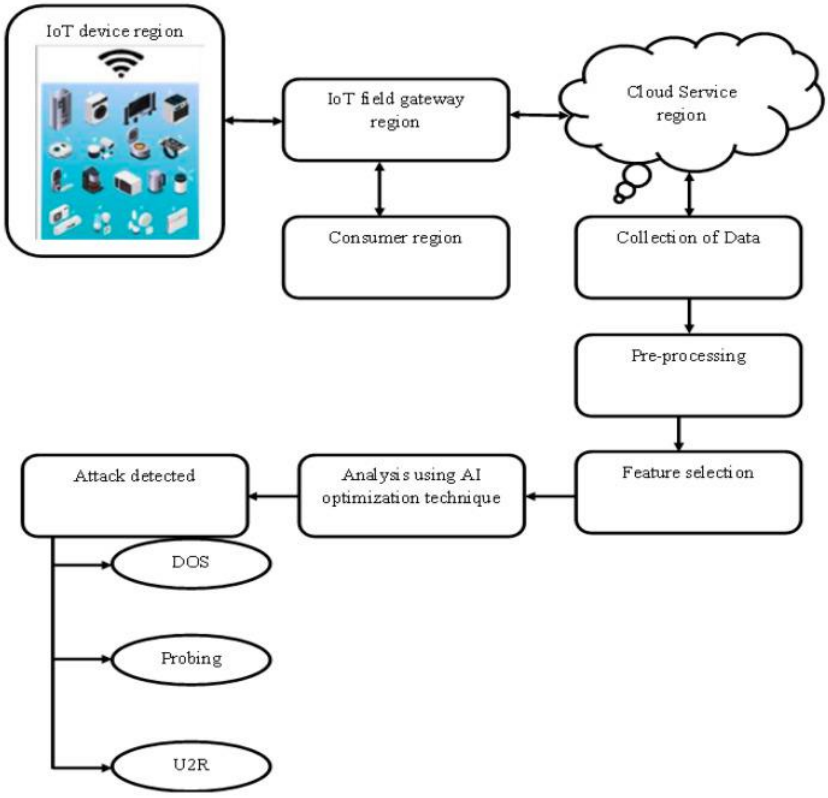


Рис.1. Ілюструється, як системи виявлення кібератак допомагають захищати підключені IoT-пристрої та приватні дані.

Перелік посилань:
1. A Critical Cybersecurity Analysis and Future Research URL: https://www.mdpi.com/1424-8220/23/8/4117
2. Cyber Security in IoT-Based Cloud Computing URL: https://www.mdpi.com/2079-9292/11/1/16
3. Prevention of Cyber Security with the Internet of Things URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9413110/
4. IoT Security: Safeguarding Critical Networks Against Digital Threats URL: https://www.eccouncil.org/cybersecurity-exchange/network-security/guide-to-iot-security-protecting-critical-networks/
5. Artificial intelligence for cybersecurity: Literature review URL: https://www.sciencedirect.com/science/article/pii/S1566253523001136
6. A Comprehensive Survey of Recent Internet Measurement Approaches for Cyber Security URL: https://www.sciencedirect.com/science/article/pii/S0167404823000330

Катков Юрій Ігорович
доктор технічних наук, професор кафедри комп'ютерних наук, ННІТ, ДУІКТ, Київ, Україна
Локойда Андрій Олегович
Студент групи КНДМ-61, ННІТ, ДУІКТ, Київ, Україна

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК І ТЕРОРИСТИЧНИХ ЗАГРОЗ

Захист критичної інфраструктури – пріоритет національної безпеки. Критична інфраструктура, така як енергетичні системи, транспорт, охорона здоров'я та фінанси, є основою сучасного суспільства, та її вразливість до кібератаків та терористичних загроз становить серйозну загрозу національній безпеці. Кібератаки на критичну інфраструктуру стають дедалі складнішими та руйнівними. З появою нових технологій та методів атак, кіберзагрози стають більш загрозливими і можуть спричинити серйозні наслідки, такі як відключення енергосистем, порушення транспортної інфраструктури тощо.

Ключові слова: критична інфраструктура, кібератаки, терористичні загрози.

1. Загроза кібератак та терористичних загроз на критичну інфраструктуру.

Кіберзлочинці можуть атакувати системи критичної інфраструктури, щоб здійснювати різні злочинні дії, такі як: шпигунство, вимагання викупу, саботаж інфраструктури тощо. Наприклад, кібератака на електричну мережу може призвести до відключення електроенергії в містах і регіонах із серйозними наслідками для населення та економіки. Також терористичні групи можуть використовувати кіберзброю для атак на критичну інфраструктуру з метою завдання шкоди, створення паніки або впливу на політичні процеси.

Захист критичної інфраструктури від кібератак вимагає застосування ефективних заходів безпеки, які здатні в першу чергу забезпечити високій рівень кібербезпеки для систем критичної інфраструктури, використовуючи такі заходи, як захист від шкідливих програм, контроль доступу та сегментація мережі. Крім того, необхідно постійно оновлювати та захищати програмне забезпечення.

Прикладами кібератак та терористичних загроз на критичну інфраструктуру є атаки на операційні технології (OT) критичної інфраструктури [1]. Операційні технології - це апаратне та програмне забезпечення, яке детектує або викликає зміни за допомогою прямого спостереження та/або управління промисловим обладнанням, активами, процесами та подіями. Термін введений для демонстрації технологічних та функціональних відмінностей між традиційними IT-системами та промисловими системами управління. За останнє десятиліття системи OT, які колись були ізольованими, стали все більш підключеними до Інтернету, оскільки системи водопостачання та енергетики стають приводом для розумних датчиків IoT, а урядові операції глибоко кореняться в даних.

Кібератаки на критичну інфраструктуру здійснюються за допомогою

комп'ютерних хробаків. Наприклад, *Stuxnet (win32/Stuxnet)*— комп'ютерний хробак, що вражає комп'ютери, які працюють на операційній системі Microsoft Windows. У червні 2010 року він був виявлений не тільки на комп'ютерах рядових користувачів, але і в промислових системах, які керують автоматизованими виробничими процесами. Цей комп'ютерний вірус, який цілився на програмовані логічні контролери (PLC), зруйнував іранську ядерну програму, пошкодивши центрифуги, що використовуються для розділення ядерного матеріалу. Це перший відомий комп'ютерний хробак, що перехоплює і модифікує інформаційний потік між програмованими логічними контролерами марки SIMATIC S7 і робочими станціями SCADA-системи SIMATIC WinCC фірми Siemens. Таким чином, хробак може бути використаний як засіб несанкціонованого збору даних (шпигунства) і диверсій у автоматизованих системах керування промислових підприємств, електростанцій, аеропортів тощо[2].

2. Захист критичної інфраструктури.

Щоб захистити критичну інфраструктуру від кібератак, необхідно регулярно проводити тестування та аудит безпеки мережі, щоб виявити можливі слабкі ланки в системі та вчасно їх усунути. Крім того, необхідно забезпечити своєчасне реагування на кібератаки та розробити плани на випадок надзвичайних ситуацій для швидкого відновлення систем критичної інфраструктури. Прикладами захисту критичної інфраструктури є:

Технології для захисту критичної інфраструктури [3]: Багато прикладів захисту критичної інфраструктури використовують такие технологии, як Deep CDR (Content Disarm and Reconstruction), який розбирає файл на складове частини та усуває будь-які потенційні загрози, а також Proactive DLP (Data Loss Prevention), який захищає чутливу інформацію шляхом видалення метаданих, автоматичного засекречення документів тощо

Ініціативи з кібербезпеки критичної інфраструктури [4]: В 2023 році було започатковано ряд ініціатив для підвищення кіберстійкості критичної інфраструктури.

3. Забезпечення високого рівню кібербезпеки.

Необхідно забезпечити високий рівень кібербезпеки для працівників, відповідальних за критичну інфраструктуру. Цього можна досягти за допомогою регулярних тренінгів із кібербезпеки, що покращить навички працівників і зменшить ризик людської помилки під час використання системи.

Аналіз основних тренінгів із кібербезпеки показує, що поширено застосування *безкоштовні програми навчання*, наприклад, CISA пропонує безкоштовні програми навчання для урядових та приватних партнерів [5]. Специфічне навчання CISA пропонує специфічне навчання для різних секторів, таких як хімічний сектор, комерційні об'єкти, аварійні служби та ядерні реактори, матеріали та відходи. Ці програми навчання включають веб-курси самостійного вивчення, курси з викладачем та пов'язані навчальні матеріали. А

також поширено публікація оглядів літератури, наприклад, один з оглядів літератури зосереджується на аналізі розв'язки та пропозицій для підвищення обізнаносте з критичною інфраструктурою та кібербезпекою, а також досліджує ключові показники ефективності для оцінки цієї розв'язки[6].

Висновок.

Захист критичної інфраструктури від кібератак і терористичних загроз є важливим завданням для забезпечення безпеки суспільства і економіки. Для вирішення цього завдання необхідно вжити комплексу заходів, які дозволять підвищити безпеку систем і мереж, включаючи захист інформаційної безпеки, фізичної безпеки та міжнародне співробітництво, а також готовність до реагування на інциденти і обізнаність про кібербезпеку і тероризм.

Перелік посилань:

1. The Ongoing Cyber Threat to Critical Infrastructure. Провідна організація CSA [Електронний ресурс] / – Режим доступу до ресурсу: https://cloudsecurityalliance.org/blog/2022/09/26/the-ongoing-cyber-threat-to-critical-infrastructure
2. Центр ресурсів Allianz // [Електронний ресурс] / – Режим доступу до ресурсу: https://www.allianzre.com/en_GB.html
3. What Is Critical Infrastructure Protection (CIP)? Навчальний інститут Fortinet //[Електронний ресурс] / – Режим доступу до ресурсу: https://www.fortinet.com/resources/cyberglossary/critical-infrastructure-protection
4. *10 notable critical infrastructure cybersecurity initiatives in 2023. Центр ресурсів CSO* //[Електронний ресурс] / – Режим доступу до ресурсу: https://www.csoonline.com/article/575449/10-notable-critical-infrastructure-cybersecurity-initiatives-in-2023.html
5. *Critical Infrastructure Training* //[Електронний ресурс] / – Режим доступу до ресурсу: https://www.cisa.gov/critical-infrastructure-training
6. *Науково-інформаційна соціальна мережа ResearchGate* //[Електронний ресурс] / – Режим доступу до ресурсу:https://www.researchgate.net/directory/publications

Лягушкін Іван Анатолійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ЗАХОДИ ПОСИЛЕННЯ МУЛЬТИФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

Сьогодні автентифікація відіграє важливу роль у будь-якій системі віддаленого та невіддаленого доступу. Базова автентифікація здійснюється за допомогою логіна і пароля, але вже деякий час багатофакторна автентифікація (MFA) розглядається як стандарт і "must have", оскільки вона забезпечує додатковий захист. MFA може бути реалізована і використана багатьма способами, такими як фізичні токени, біометричні дані, програмні додатки, SMS тощо. Оскільки не всі знають про токени або біометричні дані як засоби для здійснення MFA, методи на основі додатків приймаються як більш безпечний спосіб автентифікації користувачів замість SMS або телефонних дзвінків. Базове функціонування MFA покладається на одноразові паролі (OTP). Такі програми, як Authy або Microsoft Authenticator, впровадили функції криптографічного хешування, такі як Hash-based Message Authentication Code (HMAC) для генерації OTP, які зазвичай складаються з 6-значного числа, обчисленого з міткою часу і

секретним ключем.

Для того, щоб використовувати багатофакторну автентифікацію, необхідно враховувати три чинники:

а) **Те, що ви знаєте.** Цей метод заснований на використанні пароля або парольної фрази, PIN-коду або відповідей на секретні запитання (виклик-відповідь). Це передбачає перевірку того, що надає користувач.

б) **Те, що у вас є.** Це може бути пристрій-токен, смарт-карта, електронна пошта, номер мобільного телефону або смартфон у поєднанні з програмним додатком OTP. Він передбачає перевірку предмета, який має користувач.

в) **Те, чим ви являєтеся**. Наприклад, відбиток пальця, розпізнавання обличчя або голосу, сканування сітківки або райдужної оболонки ока. Цей метод передбачає перевірку властивих особистості властивостей.

Зловмисники продовжують відкривати нові способи скомпрометувати процес автентифікації, тому нижче наведено п’ять заходів зміцнення, які покращують використання корпоративного MFA. Заходи ґрунтуються на поточних найкращих практиках і недавніх формах експлуатації, які застосовуються сьогодні.

1. Вимикання конфігурації за замовчуванням MFA для текстових повідомлень.

SMS як MFA широко використовується, оскільки його легко налаштувати та для отримання OTP потрібен лише номер телефону. Ця позасмугова автентифікація вважається найслабшою формою MFA, тому у нього є деякі недоліки.

Цей тип MFA вразливий до заміни SIM-карти, не покладається на шифрування, може бути перехоплений за допомогою програмно-визначених радіостанцій, стільників FEMTO або служб перехоплення SS7.

2. Вимикання спливаючих сповіщеннь, щоб уникнути атаки MFA Fatigue Attack (MFA Bypass)

«Втома MFA» можна розглядати як другий фактор обходу автентифікації, а спосіб дії суб’єктів загрози стосується перевантаження сповіщень, які користувач отримує протягом дня, щоб виконати вхід або схвалити різні дії. Через величезну кількість сповіщень втомлені користувачі намагаються позбутися будь-яких спливаючих вікон, які їх засмучують, і починають відкидати найкращі практики безпеки.

3. Блокування облікового запису користувача після кількох відмов MFA.

У цьому сенсі нечасто знайти елементи керування безпекою за замовчуванням, щоб обмежити зловживання автентифікацією OTP. За можливості кожен обліковий запис слід налаштувати на блокування або на ініціювання процесу відновлення пароля після певної кількості відмов MFA.

MFA на основі програм вразливий до грубої сили, фішингу та зловмисного програмного забезпечення, запущеного на пристрої жертви.

У цьому контексті налаштування максимальної кількості відмов MFA має бути необхідним правилом.

4. Блокування доступу за місцем розташування.

Нетипове місцезнаходження, не призначене для повсякденної роботи, не повинно використовуватися для автентифікації.

Блокування доступу за місцезнаходженням постійно зменшує кількість дозволених автентифікацій, що, відповідно, зменшує поверхню атаки.

Підсумовуючи, рекомендується вмикати автентифікацію за гео користувача лише для визначених IP. Автентифікації з IP, які компанія не визнає легітимними, повинні бути заблоковані.

5. Налаштування фізичного маркеру або біометричної автентифікації

Фізичні токени та біометрична автентифікація використовують для автентифікації протокол FIDO U2F. Протокол розроблений, щоб діяти як другий фактор для посилення входу на основі імені користувача та пароля. Він використовує шифрування з відкритим ключем, що означає, що для кожної використовуваної служби генерується нова пара ключів і може підтримуватися необмежена кількість служб, зберігаючи повне розділення між ними для збереження конфіденційності.

Протокол U2F можна використовувати трьома способами.

1. Без пароля або без токена: користувачеві достатньо розблокувати пристрій за допомогою біометрії.

2. Для мобільних пристроїв: користувач вводить ім’я користувача та пароль, а потім торкається зареєстрованого фізичного маркера. Зв’язок між токеном і зареєстрованими пристроями здійснюється через NFC або bluetooth.

3. Для USB: користувач вводить ім’я користувача та пароль, вставляє фізичний маркер у комп’ютер і натискає кнопку.

Протокол U2F також гарантує, що вхід користувача прив’язаний до реального сайту. Іншими словами, автентифікація на підробленому сайті буде невдалою, навіть якщо користувач переконаний, що він був справжнім.

Для використання маркера цей тип MFA є вразливим до крадіжки обладнання. Для цього рекомендується мати другий фізичний маркер як резервну копію, збережений у безпечному місці.

Література:

1. https://cipher.com/blog/hardening-measures-for-multi-factor-authentications/ - Hardening Measures for Multi-Factor Authentications

Маєр Дмитро Володимирович
студент групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

КОМПЛЕКСНИЙ ПІДХІД ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ

Ця теза розглядає важливість комплексного підходу до управління інформаційною безпекою на підприємствах. Зростаюча кількість кіберзагроз та інцидентів із порушенням інформаційної безпеки надає актуальності розробці і впровадженню власних стратегій та заходів для захисту корпоративних ресурсів та даних. Ця теза досліджує ключові аспекти комплексного підходу, включаючи технічні заходи, політики безпеки, управління ризиками та навчання персоналу. Робота також надає практичні рекомендації щодо вдосконалення системи управління інформаційною безпекою на підприємстві та підкреслює важливість цього підходу для забезпечення стійкості та надійності корпоративних систем і даних.

- **Технічний аспект:** Комплексний підхід до технічної інформаційної безпеки на підприємстві включає в себе застосування сучасних засобів шифрування, мережевого моніторингу та інтегрованих систем безпеки для захисту корпоративних даних від несанкціонованого доступу та кібератак.
- **Організаційний аспект:** Організаційний аспект комплексного управління інформаційною безпекою включає в себе розробку політик безпеки, створення команди для відповіді на інциденти, проведення регулярних аудитів безпеки та розробку планів відновлення після інцидентів.
- **Кадровий аспект:** Забезпечення інформаційної безпеки вимагає освіченого та навченого персоналу. Кадровий аспект комплексного підходу включає в себе навчання та постійну підвищену кваліфікацію співробітників щодо правил безпеки та вмінь реагувати на інциденти.
- **Управління ризиками:** Комплексний підхід також враховує аналіз та управління ризиками, що допомагає ідентифікувати можливі загрози та приймати заходи для зменшення ймовірності виникнення інцидентів.

Перелік посилань:

- **"CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide"** - автори: James M. Stewart, Mike Chapple, Darril Gibson.
- **"Information Security Management Principles"** - автор: David Alexander, M. E. Kabay, et al.
- **"Cybersecurity – Attack and Defense Strategies"** - автор: Yuri Diogenes, Erdal Ozkaya.
- **"ISO 27001/ISO 27002: A Pocket Guide"** - автор: Alan Calder.

Мазурик А. В.
Студент УІКБ-61

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ

Високий рівень безпеки і відповідність нормативним вимогам є обов'язковими умовами в проектах по розгортанню корпоративних мереж.

Для захисту власних інформаційних ресурсів підприємства впроваджують

в інфраструктуру рішення щодо забезпечення безпеки мережі, що гарантують безпеку мережі і комерційних даних на всіх рівнях:

- міжмережевий екран
- керовані VPN мережі
- пошук і блокування спроб вторгнень в мережу
- захист кінцевих точок обміну трафіком
- корпоративна антивірусна система.

Безпека підключень

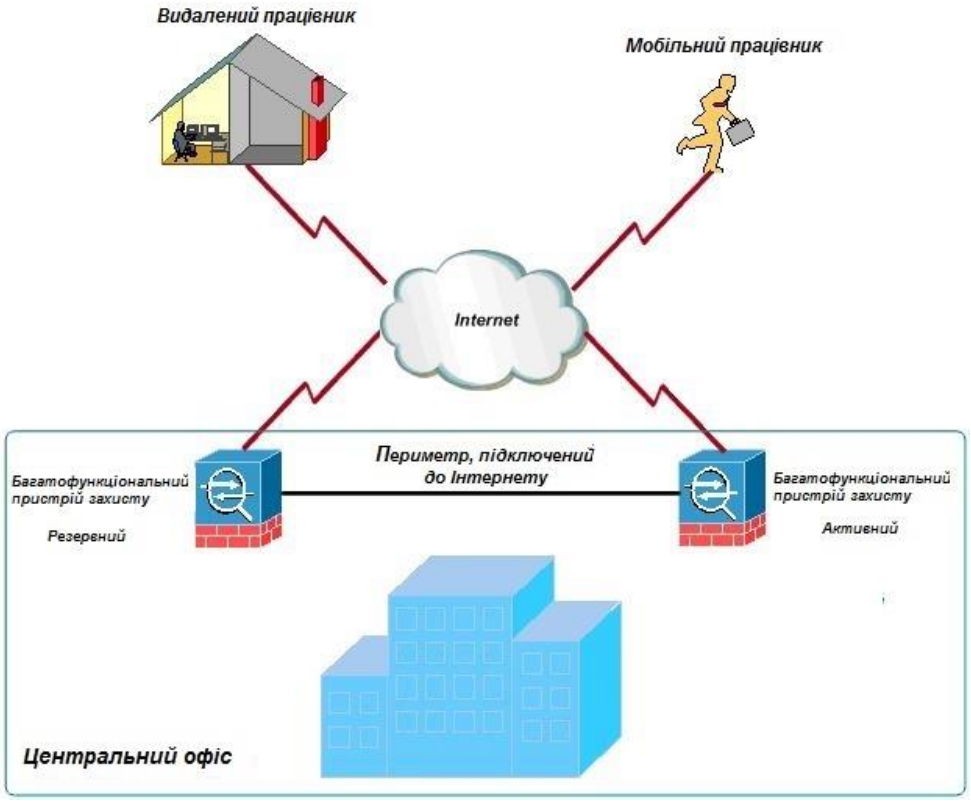
Для співробітників, які перебувають у відрядженнях або працюють з дому, послуга віддаленого доступу до корпоративної мережі стала робочою необхідністю.

Все більше організацій дозволяють партнерам здійснювати віддалений доступ до своїх мереж з метою скорочення витрат на обслуговування систем. Тому захист кінцевих точок обміну трафіком - одна з найважливіших завдань забезпечення безпеки мережі компанії.

Місця, де корпоративна мережа підключається до Інтернету, є периметром безпеки мережі. У цих точках перетинається вхідний і вихідний трафік. Трафік корпоративних користувачів виходить за межі мережі, а інтернет-запити від зовнішніх користувачів для отримання доступу до веб-додатків і додатків електронної пошти входять в мережу компанії.

Через те, що в кінцевих точках виконується постійне підключення до Інтернету, яке зазвичай дозволяє проходження зовнішнього трафіку в корпоративну мережу, вона є основною метою атак зловмисників.

При побудові корпоративної мережі безпеки даних на кордонах мережі в точках виходу в Інтернет встановлюють міжмережеві екрани. Ці пристрої дозволяють запобігти і блокувати зовнішні загрози при проведенні термінації VPN тунелів.



Мал.1 Периметр безпеки корпоративної мережі

Набір інтегрованих рішень для безпечних підключень від Cisco Systems забезпечує конфіденційність інформації. У мережі ведеться експертиза всіх кінцевих точок і методів доступу в усіх мережах компанії: LAN, WAN і бездротової мобільної мережі

Забезпечується повна доступність брандмауера і сервісів VPN. Функції брандмауера забезпечують фільтрацію рівня додатків зі збереженням стану для вхідного і вихідного трафіку, захищений вихідний доступ для користувачів і мережу DMZ для серверів, до яких необхідно здійснювати доступ з Інтернету.

Комплексні рішення по забезпеченню безпеки корпоративної мережі Cisco Systems, Juniper Networks і Huawei Technologies мають ряд переваг, важливих для ефективного бізнесу:

скорочення IT-бюджетів на експлуатацію та обслуговування програмно-апаратного забезпечення

підвищення гнучкості мережі

зниження витрат на впровадження

зниження загальної вартості володіння

посилення контролю за допомогою єдиного управління та запровадження політик безпеки

підвищення прибутку і збільшення показників ефективності підприємства

зниження загроз безпеки для мережі і СГД

застосування ефективних політик безпеки і правил на кінцевих вузлах мережі: ПК, КПК і серверах

скорочення термінів впровадження нових рішень в області безпеки

ефективна профілактика мережі від вторгнень

інтеграція з ПЗ інших розробників в області безпеки і управління.

повномасштабне управління доступом до мережі

Продукти з безпеки Cisco на всіх рівнях мережі

Безпека кінцевих точок: Програма-агент безпеки Cisco Cisco Security Agent захищає комп'ютери і сервери від атак черв'яків.

Вбудовані брандмауери: модулі PIX Security Appliance, Catalyst 6500 Firewall Services Module і набір функцій брандмауера (firewall) захищають мережу всередині і по периметру.

Захист від мережевих вторгнень: Датчики IPS 4200 Series sensors, модулі служб IDS Catalyst 6500 (IDSM-2) або IOS IPS ідентифікують, аналізують і блокують зловмисний небажаний трафік.

Виявлення та усунення атак DDoS: Детектор аномалій трафіку Cisco Traffic Anomaly Detector XT і Guard XT забезпечують нормальну роботу в разі атак, що переривають роботу служби. Модулі служб детектора аномалій трафіку Cisco і Cisco Guard створюють стійкий захист від атак DdoS в комутаторах серії Catalyst 6500 і маршрутизаторах серії 7600.

Безпека контенту: модуль пристрою Access Router Content Engine module захищає бізнес-додатки, що працюють з інтернет, забезпечує доставку веб-контенту без помилок.

нтелектуальні служби адміністрування мережі і систем безпеки: в маршрутизаторах і комутаторах Cisco знаходять і блокують небажаний трафік і додатки.

Менеджмент і моніторинг:

Продукти:

CiscoWorks VPN / Security Management Solution (VMS)

CiscoWorksSecurity Information Management System (SIMS) - система управління інформацією про стан безпеки

Вбудовані менеджери пристроїв: менеджер маршрутизаторів і пристроїв безпеки Cisco (SDM), менеджер пристроїв PIX (PDM), менеджер пристроїв адаптивної безпеки (ASDM) швидко і ефективно здійснюють відстеження, ведуть моніторинг служб безпеки і активності мережі.

Технологія Network Admission Control (NAC) від Cisco

Контроль доступу в мережу (Network Admission Control, NAC) - це набір технологій і рішень, фундаментом яких є загальногалузева ініціатива, реалізована під патронажем Cisco Systems.

NAC використовує інфраструктуру мережі для контролю над дотриманням політики безпеки на всіх пристроях, які прагнуть отримати доступ до ресурсів мережі. Так знижується можливий збиток в мережі від загроз безпеки.

до корпоративної VPN співробітникам і партнерам багатофункціональні пристрої захисту забезпечують за допомогою протоколів SSL і IPsec VPN, вбудованих блокувальних сервісів для попередження та запобігання IPS

вторгнень.

Self-Defending Network - стратегія самозахистом мережі від Cisco

Self-Defending Network є стратегією майбутнього від Cisco яка розвивається. Технологія дозволяє захистити бізнес-процеси підприємства шляхом виявлення та запобігання атак, адаптації до внутрішніх і зовнішніх загроз мережі.

Підприємства можуть ефективніше використовувати інтелектуальні можливості мережевих ресурсів, оптимізувати бізнес-процеси і скоротити витрати.

Пает управління безпекою Cisco

Пакет управління безпекою Cisco представляє собою набір продуктів і технологій, розроблених для масштабованого адміністрування та посилення політик безпеки для мережі Cisco що сама захищається.

Інтегрований продукт Cisco дозволяє автоматизувати завдання управління безпекою за допомогою ключових компонентів: менеджера управління і Cisco Security MARS - системи моніторингу, аналізу та реагування.

Менеджер управління системою безпеки Cisco має простий інтерфейс для налаштування брандмауера, VPN і системи захисту від вторгнень (IPS) на пристроях безпеки, міжмережевих екранах, маршрутизаторах і комутаторах Cisco.

Мазурик А. В.
Студент УІКБ-61

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ

В умовах сучасних реалій кібербезпека – одне з першочергових завдань, які потребують вирішення в Україні. За останні кілька років робилися неодноразові спроби дестабілізувати банківську систему країни та зламати бази даних державних органів. Зловмисники зацікавлені отримати доступ не лише до персональних відомостей українців, а й до їхніх банківських рахунків.

Найпоширенішою причиною зливу особистої інформації стають погано захищені канали фінансових операцій через інтернет. Українські громадяни ризикують купуючи товари в неперевірених інтернет-магазинах або відвідуючи нелегальні онлайн-казино.

Існує кілька надійних способів мінімізувати ризик витоку інформації:

Вибирати для азартних розваг лише ліцензовані онлайн-казино. Одним з перших операторів гемблінг індустрії, котрі пройшли процедуру легалізації, став онлайн-клуб Pin Up. Подібні розважальні заклади дотримуються принципів відповідальної гри та використовують якісний ліцензійний софт. Безпечне дозвілля гарантує вивчення експертних оглядів азартних закладів, наприклад, казино Золотий Кубок.

Підключення смс-повідомлень про здійсненні фінансові транзакції.

Використання складних паролів для персональних кабінетів на веб-сайтах. Не варто застосовувати однакові комбінації логіну та пароля для різних платформ.

Введення відомостей банківської картки лише на надійних сайтах через безпечні шлюзи платіжних систем.

Азартна промисловість – це конкурентна галузь. Нелегальні компанії прагнуть отримати перевагу перед ліцензованими представниками грального бізнесу. Не маючи можливості надати клієнтам високий рівень сервісу та якісний софт тіньові казино купують хакерські послуги.

Отримані персональні дані хакери використовують для зламування електронних поштових скриньок та банківських рахунків користувачів. Інформація може передаватися третім особам або використовуватися зловмисниками для особистої вигоди. Подібні втрати даних супроводжуються значними репутаційними ризиками для гральних компаній. Знижується довіра клієнтів до компанії.

На думку ІТ-фахівців сьогодні ризику хакерської атаки однаково схильний, як малий бізнес, так і великі міжнародні гемблінгові компанії. Представникам українського азартного бізнесу слід посилити заходи, спрямовані на захист від ворожих кібер атак.

Катков Юрій Ігорович
доктор технічних наук, професор кафедри комп'ютерних наук, ННІТ, ДУІКТ, Київ, Україна
Май Максим
Студент групи КНДМ-61, ННІТ, ДУІКТ, Київ, Україна

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

Кібербезпека стала невід'ємною частиною нашого цифрового життя, оскільки сучасний світ все більше стикається із загрозами від кібератак, які можуть нести руйнівні наслідки для організацій та індивідів. У цьому контексті штучний інтелект (ШІ) здобуває все більше значущості, виступаючи як незамінний союзник у сфері кібербезпеки. ШІ виявляється унікальним інструментом, який поєднує в собі інтелект людини та швидкість обробки даних машини, що дозволяє ефективно виявляти, запобігати та реагувати на кіберзагрози [1].

Ключові слова: Кібербезпека, загрози, кібератаки, штучний інтелект, роль, вплив, суспільство.

1. Проактивний аналіз загроз за допомогою ШІ.

Проактивний аналіз загроз в кібербезпеці за допомогою ШІ виконує ключову роль у запобіганні кібератак і забезпеченні безпеки організацій. Ось більше деталей стосовно цього аспекту [2, 3, 4]:

- *Раннє виявлення загроз*: Системи інформаційної безпеки наділені інструментами для неперервного моніторингу мереж і інфраструктури, що

дозволяє виявляти навіть найменші аномалії, які можуть вказувати на потенційні загрози.

- *Аналіз великих обсягів даних*: Використання аналітики даних та штучного інтелекту в ШІ допомагає виділяти легітимну активність від потенційно небезпечної та ідентифікувати незвичайні патерни, які можуть свідчити про загрози.
- *Запобігання перед атакою*: На підставі зібраних даних і виявлених аномалій, системи інформаційної безпеки дозволяють вживати заходи для захисту системи, включаючи блокування зловмисної активності, виявлення та усунення вразливостей, а також ізоляцію загрози для подальшого аналізу.

Таким чином, проактивний аналіз загроз за допомогою ШІ через системи інформаційної безпеки сприяє запобіганню кібератак, зменшенню ризиків та забезпеченню безпеки інформаційної інфраструктури організацій.

2. Захист інформації та даних за допомогою ШІ.

Захист інформації і даних через системи інформаційної безпеки в кібербезпеці за допомогою ШІ – це важлива складова для забезпечення конфіденційності, цілісності і доступності даних в організаціях та системах [3, 4, 5]. Відомо, що ШІ використовує шифрування для захисту інформації у спокійному стані, під час передачі та зберігання. Використання сильних шифрів ускладнює розшифрування даних навіть при незаконному доступі. Вони також допомагають визначати, хто, коли і до якої інформації має доступ, включаючи ідентифікацію користувачів, ролей та прав доступу, забезпечуючи принцип найменшого доступу для запобігання несанкціонованому доступу.

Додатково, ШІ включають системи моніторингу та виявлення загроз для своєчасного реагування на незвичайну активність та атаки, забезпечуючи їхню ізоляцію та виправлення. ШІ також сприяє резервному копіюванню важливих даних, забезпечуючи можливість відновлення в разі втрати даних через кібератаку чи інші інциденти.

3. Реагування на інциденти та відновлення за допомогою ШІ.

Реагування на інциденти та відновлення з використанням систем інформаційної безпеки за допомогою ШІ - це важливий процес для забезпечення стійкості та стабільності інфраструктури та організацій під час кібератак та інших інцидентів. Ось коротке узагальнення цього аспекту [4, 5, 6]:

1. *Виявлення та діагностика інцидентів*: ШІ включає системи моніторингу та детекції, що допомагають реагувати на зловмисну активність та аномалії в реальному часі для швидкого виявлення та класифікації інцидентів.
2. *Ізоляція та контроль інцидентів*: ШІ сприяє ізоляції зловмисної активності та обмеженню її поширення, що запобігає подальшому поширенню інциденту.
3. *Аналіз та відновлення*: Після ізоляції інциденту, ШІ надає інструменти для аналізу та відновлення системи та даних, включаючи

відновлення збитків, виправлення вразливостей та відновлення нормальної роботи.

4. *Документування та вивчення інцидентів*: ШІ допомагає вести документацію про інциденти, їхні причини та наслідки для подальшого вивчення та удосконалення процесів безпеки.

5. *Планування відновлення після кризи*: ШІ допомагає розробляти плани відновлення після кризи, які включають в себе процеси відновлення систем та даних після серйозних інцидентів.

Висновок.

Загалом системи інформаційної безпеки за допомогою ШІ відіграють ключову роль у кібербезпеці, забезпечуючи захист інформації та даних в організаціях. За допомогою ШІ забезпечується проактивний аналіз загроз, захист конфіденційності та цілісності інформації, реагування на кібер інциденти та забезпечення її відновлення. Завдяки ШІ, організації можуть бути більш стійкими до кіберзагроз та забезпечити безпеку своєї інфраструктури та даних в сучасному кіберсередовищі.

Перелік посилань:

1. Спеціалізований портал про освіту в Україні. Education.ua compromised // [Електронний ресурс] Режим доступу до ресурсу: *https://www.education.ua/resources/*
2. Школа майбутнього Robot Dreams compromised https://robotdreams.cc/uk/blog/352-shtuchniy-intelekt-ne-zahistit-yakshcho-ne-vikoristovuvati-intelekt-prirodniy-yak-rozvitok-shi-vplivaye-na-kiberbezpeku
3. Зробіть на крок ближче до майбутнього/ Блог про ШІ та технології майбутнього HashDork // [Електронний ресурс] Режим доступу до ресурсу: *https://hashdork.com/uk/*
4. Провідна компанія, що пропонує рішення Кібербезпеки на основі ШІ Crowdstrike // [Електронний ресурс] Режим доступу до ресурсу: https://www.crowdstrike.com/resources/
5. Провідна компанія, що пропонує рішення Кібербезпеки на основі ШІ Cynet // [Електронний ресурс] Режим доступу до ресурсу: *https://www.cynet.com/resources/*
6. Провідна компанія, що пропонує рішення Кібербезпеки на основі ШІ Darktrace // [Електронний ресурс] Режим доступу до ресурсу:*https://darktrace.com/resources/*

Катков Юрій Ігорович
доктор технічних наук, професор кафедри комп'ютерних наук, ННІТ, ДУІКТ, Київ, Україна
Май Павло
Студент групи КНДМ-61, ННІТ, ДУІКТ, Київ, Україна

ПИТАННЯ ВРАЗЛИВОСТІ WINDOWS SUBSYSTEM FOR LINUX (WSL) В WINDOWS SERVER 2022

Microsoft Windows Server використовується як операційна система для великих і важливих серверних робочих навантажень. В Microsoft Windows Server є технологічна платформа Windows Subsystem for Linux (WSL), яка дозволяє користувачам запускати і виконувати дистрибутиви Linux (такі як Ubuntu, Debian, Fedora та інші) безпосередньо у середовищі Windows без необхідності встановлення і використання віртуальних машин. Але WSL має вразливості. Якщо зловмисник отримає доступ до WSL, він зможе скористуватися цим доступом для атак на сервер або для отримання доступу до конфіденційної інформації. Це може створити потенційну загрозу для безпеки сервера, що є безумовно актуальною

проблемою захисту. Для вирішення цієї проблеми існують підходи, які треба досліджувати.

Ключові слова: кібербезпека, виявлення вразливостей у WSL, загроза безпеки, способи запобігання виникнення вразливостей у WSL.

1. Особливості Windows Subsystem for Linux (WSL) та його версії.

Windows Subsystem for Linux (WSL) - технологічна платформа в операційній системі Microsoft Windows, яка дозволяє користувачам запускати і виконувати дистрибутиви Linux (такі як Ubuntu, Debian, Fedora та інші) безпосередньо у середовищі Windows без необхідності встановлення і використання віртуальних машин. WSL використовує ядро Linux, яке повертається в образ WSL. Це дозволяє користувачам запускати програми Linux, які не були б доступні в Windows [1].

WSL доступний в Windows Server 2022. Він підтримує дві версії: WSL 1 і WSL 2. WSL 1 - це перша версія WSL. Вона використовує гіпервізію для запуску ядра Linux в контейнері. WSL 1 має обмежену продуктивність і не підтримує деякі функції Linux, такі як управління віртуальними машинами і мережею. WSL 2 - це нова версія WSL, яка використовує віртуальну машину для запуску ядра Linux. WSL 2 має значно кращу продуктивність, ніж WSL 1, і підтримує всі функції Linux [2].

2. Приклади вразливості у Windows Subsystem for Linux (WSL) в Windows Server 2022.

Windows Subsystem for Linux (WSL) - це потужний інструмент, який дозволяє користувачам Windows запускати програми Linux безпосередньо в Windows. Однак, як і будь-яка інша комп'ютерна система, WSL також може бути вразливим до атак [3]. Ось деякі приклади вразливості у WSL в Windows Server 2022:

- ***Вразливості в ядрі Linux.*** Ядро Linux є основою для операційної системи Linux, і воно постійно оновлюється для виправлення виявлених вразливостей. Однак існує ймовірність того, що в ядрі Linux можуть залишитися невідкриті вразливості. Якщо зловмисник зможе скористатися такою вразливістю, він зможе отримати контроль над ядром Linux і, отже, над WSL.
- ***Вразливості в WSL.*** Сам WSL також може містити вразливості. Ці вразливості можуть бути викликані помилками в коді WSL або в його взаємодії з іншими компонентами Windows. Якщо зловмисник зможе скористатися такою вразливістю, він зможе отримати контроль над WSL і, отже, над програмами Linux, які запускаються в WSL.
- ***Вразливості в програмах Linux.*** Програми Linux, які запускаються в WSL, також можуть містити вразливості. Ці вразливості можуть бути викликані помилками в коді програми або в її взаємодії з іншими програмами Linux. Якщо зловмисник зможе скористатися такою вразливістю, він зможе отримати контроль над програмою Linux і, отже, над WSL [4].

3. Методи захисту від атак, які використовують вразливості у WSL.

Що запобігти і захистити себе від атак, необхідно дотримуватися наступних рекомендацій [5]:

- ***Встановлюйте останні виправлення для WSL.*** Microsoft регулярно випускає виправлення для виявлених вразливостей у WSL. Встановлення останніх виправлень допоможе захистити ваш сервер від атак, які використовують ці вразливості.
- ***Використовуйте брандмауер для захисту WSL від несанкціонованого доступу.*** Брандмауер може допомогти захистити WSL від атак, які надходять з Інтернету.
- ***Встановіть антивірусне програмне забезпечення для захисту WSL від шкідливих програм.*** Антивірусне програмне забезпечення може допомогти захистити WSL від шкідливих програм, які можуть бути використані для запуску атак.
- ***Не запускайте в WSL програмне забезпечення з невідомих джерел.*** Не запускайте в WSL програмне забезпечення, яке ви не впевнені, що це безпечне. Крім того, можна використовувати віртуальну машину для запуску WSL. Це допоможе захистити основну операційну систему від шкідливих програм, які можуть бути запущені в WSL [6].

Висновок.

Windows Subsystem for Linux (WSL) - це потужний інструмент, який дозволяє користувачам запускати програми Linux на комп'ютерах з Windows. Однак, як і будь-яка інша технологія, WSL має свої вразливості.У цьому документі були розглянуті деякі з найбільш поширених вразливостей WSL, включаючи:

Вразливість ядра Linux: Ця вразливість дозволяє зловмисникам отримати контроль над ядром Linux, а отже, і над усією системою.

Вразливість драйвера WSL: Ця вразливість дозволяє зловмисникам отримати доступ до системних ресурсів, наприклад, до файлів і каталогів.

Вразливість безпеки мережі: Ця вразливість дозволяє зловмисникам отримати доступ до мережі через WSL.

Щоб захиститися від цих вразливостей, користувачі повинні:

*Тримати WSL в актуальному стан*і: Microsoft регулярно випускає оновлення для WSL, які усувають вразливості.

Використовувати надійні паролі: Встановіть надійні паролі для облікових записів WSL.

Блокуйте неавторизований доступ: Використовуйте брандмауер для блокування неавторизованого доступу до WSL.

Використання цих заходів безпеки допоможе захистити комп'ютер від вразливостей WSL.

Перелік посилань:

1. Центр ресурсів Microsoft [Електронний ресурс] / – Режим доступу до ресурсу: Install Linux Subsystem on Windows Server | Microsoft Learn

2. Центр ресурсів Redmondmag [Електронний ресурс] / – Режим доступу до ресурсу: Windows Subsystem for Linux 2 Available for Windows Server 2022 -- Redmondmag.com
3. Центр ресурсів The Register[Електронний ресурс] / – Режим доступу до ресурсу: Now there's malware for Windows Subsystem for Linux • The Register
4. Центр ресурсів BleppingComputer[Електронний ресурс] / – Режим доступу до ресурсу: New malware uses Windows Subsystem for Linux for stealthy attacks (bleepingcomputer.com)
5. Центр ресурсів ZDNET[Електронний ресурс] / – Режим доступу до ресурсу: Windows 10's Subsystem for Linux: Here's how hackers could use it to hide malware | ZDNET
6. Центр ресурсів How-To Geek[Електронний ресурс] / – Режим доступу до ресурсу: "Bring Your Own Vulnerable Driver" Attacks Are Breaking Windows (howtogeek.com)

Матеєнко Назар Володимирович
студент групи УБДМ-51, ДУІКТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ

Забезпечення кібербезпеки на даний час є важливою проблемою на всіх рівнях публічного управління: від місцевих органів влади, що займаються онлайн-транзакціями, до центральних органів влади, що займаються питаннями національної безпеки.

Кібербезпека – це динамічна мета, яка змінюється з такою швидкістю, що дуже важко отримати абсолютно актуальне уявлення про неї. Нові кіберзагрози або варіації старих виникають майже щодня, як і стратегії захисту від них. Однак існують і деякі загальні підходи до забезпечення кібербезпеки, які слід визначати та адаптувати до специфіки конкретних держав і конкретних органів публічної влади [1,с.9].

Існуючі проблеми кібербезпеки в Україні можна поділити на

1. організаційні,
2. технічні (апаратні, інструментальні),
3. правові,
4. інформаційно-технологічні (програмні, алгоритмічні, тощо).

Серед організаційних проблем кібербезпеки слід, насамперед, виділити:

- відсутність системної роботи з підготовки організацій (підприємств,інституцій, державних установ) до кібератак;
- приділення недостатньої уваги організаційним аспектам забезпечення кібербезпеки напротилежність технічним аспектам;
- недостатність процедур по протидії, протистоянню, реагуванню на кібератаки та мінімізації їх наслідків;
- відсутність ефективних механізмів по видаленню порушників кібербезпеки з локальних мереж організацій та глобальних міждержавних (світових) мереж;
- відсутність ефективного інструментарію забезпечення кібербезпеки, який сприяє визначенню наявності кібератаки на мережі конкретної організації та відповідному реагуванню на ці атаки;
- недостатній рівень державної допомоги організаціям, що піддалися чи піддаються атаці, щодо вилучення зловмисників з комп'ютерних мереж тих організацій, які зазнали атак;

- відсутність достатньої державної координації дій щодо управління кібербезпекою як на рівні країни, так і на рівнях окремих підприємств;

- відповідність існуючим світовим стандартам щодо кібербезпеки повинні підтверджувати не державні аудитори, а експерти, що володіють міжнародною сертифікацією по IT-аудиту та кібербезпеці [3,с.4].

В наш час багато проблем кібербезпеки регулюються галузевими регуляторами. Промислові комп'ютерні мережі ставлять унікальні задачі перед фахівцями в області безпеки, бо вони недуже схожі на традиційні комп'ютерні мережі, особливо ті, що були побудовані ще до виникнення таких обсягів кіберзагроз, кібервтручань та кіберзлочинів.

Ці мережі багато років були ізольовані від глобальних мереж. Тому в них не передбачалися заходи щодо забезпечення кібербезпеки. Але в наш час навіть така ізольованність не є запорукою кібербезпеки.

Серед технічних проблем кібербезпеки слід виділити, насамперед:

- відсутність точного реєстру апаратно-технічного обладнання (як підприємств, так і мереж);

- відсутність підтримки технічними засобами механізму управління змінами і реалізації політики безпеки;

- недостатні можливості апаратного моніторингу станів підприємства та мереж;

- недостатнє апаратно-технічне забезпечення запобіганню проникнення до мережі (підприємства, установи, інституції тощо) кіберзлочинців [3,с.7].

Для захисту комп'ютерних мереж, слід спочатку зрозуміти, які IT вони використовують та на яких принципах працюють.

Забезпечення безпеки комп'ютерних мереж вимагає, зокрема,знання ПЗ, яке використовується підприємствами (або окремими користувачами), поточних налаштувань відповідного ПЗ.

Важливою проблемою безпеки комп'ютерних мереж є забезпечення прозорості дій, яка може вплинути на безпеку і надійність критично важливих інформаційних активів. Складність усунення цієї проблеми полягає в тому, що в мережах використовуються кілька різних комунікаційних протоколів.

Ще однією проблемою безпеки комп'ютерних мереж є неможливість забезпечення управління змінами та дотримання політики безпеки. Без системи запобігання неавторизованому доступу чи інформування про нього, можна вільно отримати доступ до активу і змінити його налаштування. Кібербезпека передбачає вирішення багатьох проблем, в тому числі й боротьба з комп'ютерними вірусами.

Кібербезпека стикнулася з тим, що групи кіберзлочинців стають все більш «корпоративними», ставлячи своїми мішенями:

- нові технології все частіше моделюють корпоративну ієрархію (у багатьох організаціях застосовуються так звані «шлюзи», що маскують шкідливу активність; це надає можливість кіберзлочинцям захоплювати кіберпростір та уникати виявлення);

- можливості та ризики хмарних технологій (багато хмарних застосунків,

ініціаторами застосування яких є співробітники компанії з метою підвищення ефективності та пошуку нових бізнес-перспектив, зараховано до категорії підвищеного ризику);

- звичне рекламне ПЗ, що стає джерелом зараження більше половини мереж підприємств. Забезпечення кібербезпеки є актуальним для багатьох сфер діяльності,зокрема, сфер науки, техніки та технологій (особливо ІТ), що охоплюють проблеми, пов'язані із захищеністю кіберпростору країни, окремих об’єктів його інфраструктури тощо [2,с.12].

Перелік посилань:

1. Баранов, О.А.,2014. Про тлумачення та визначення поняття «кібербезпека»,Правова інформатика.

2. Андреев В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є Основи кібербезпеки / За ред. проф. В.О. Хорошка. вид., доп. і перероб. — К. : Вид. ДУІКТ, 2009. —292 с

3. Летичевський О.О. Сучасні наукові проблеми кібербезпеки. Вісник НАН України. 2023. № 2. С. 12—20. https://doi.org/10.15407/visn2023.02.012

Матвієнко Олексій Володимирович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАХИСТУ ПРОМИСЛОВИХ IOT ІЗ ВИКОРИСТАННЯМ CISCO CYBER VISION

У зв’язку з швидким розвитком мереж Інтернету речей та зручністю їх використання люди все частіше надають їм перевагу у виборі при підключенні до мережі Інтернет. Інтернет речей (англ. Internet of Things, IoT) – це способи взаємодії фізичних об'єктів, пристроїв і систем між собою і з навколишнім світом із застосуванням різних технологій зв'язку і стандартів з'єднання. Будь-який пристрій Internet of Things є вразливим. Персональні дані, зібрані IoT-пристроями, завжди мають цінність для хакерів і викрадачів ідентифікаційної інформації. Крім того, кібератака на IoT-пристрої потенційно здатна завдати шкоди фізичним пристроям і об’єктам критичної інфраструктури.

Зі зростанням кількості підключених пристроїв і систем IoT зростає ймовірність кіберзагроз, які можуть серйозно вплинути на виробничі процеси та безпеку. В сучасному світі промислові компанії повинні активно вивчати інноваційні рішення для захисту своїх систем.

Сучасні стандарти безпеки для промислових IoT можуть бути недостатніми, і необхідно постійно вдосконалювати їх для врахування зростаючих загроз. Промислові стандарти та нормативи мають забезпечити міцний захист систем IoT.

Важливо вести постійний моніторинг мереж і систем IoT для виявлення аномальної активності. Використання інструментів аналізу трафіку та машинного навчання допомагає вчасно реагувати на потенційні атаки.

Cisco Cyber Vision - це розробка, яка спеціально призначена для виявлення та захисту промислових IoT систем. Вона використовує передові технології, такі як машинне навчання та аналіз трафіку, щоб відстежувати активність в мережі та ідентифікувати аномалії, які можуть свідчити про можливі кіберзагрози.

Використовуючи Cisco Cyber Vision, компанії можуть впроваджувати постійний моніторинг систем IoT та автоматично виявляти

аномальну активність. Це дозволяє операторам систем вчасно реагувати на потенційні атаки та витік даних.

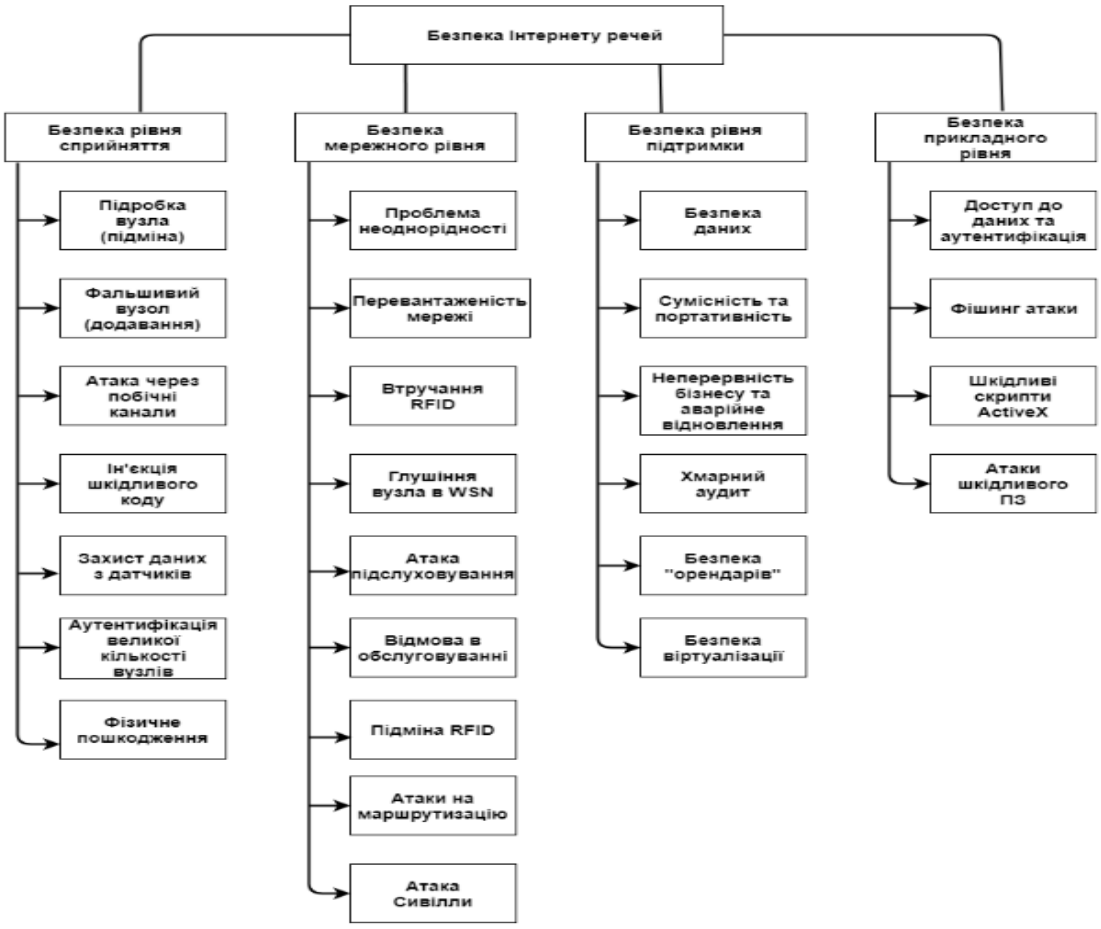


Рис.1. Безпека та атаки на IoT

Перелік посилань:

1. ТЕХНІЧНА СПЕЦИФІКАЦІЯ CISCO CYBER VISION URL: https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/datasheet-c78-743222.html (дата звернення: 15.10.2023).
2. ПРОМИСЛОВИЙ IOT: ЗАГРОЗИ ТА ЗАХОДИ ПРОТИДІЇ URL: https://www.rambus.com/iot/industrial-iot/ (дата звернення: 21.10.2023).

Коваль М. А., к.т.н., Бобровський О. В., к.т.н.,
Гаращенко І. О. к.держ.упр., Никитюк А. П.
ДУІКТ
м. Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ

Забезпечення кібербезпеки на даний час є важливою проблемою на всіх рівнях публічного управління: від місцевих органів влади, що займаються онлайн-транзакціями, до центральних органів влади, що займаються питаннями національної безпеки.

Кібербезпека – це динамічна мета, яка змінюється з такою швидкістю, що дуже важко отримати абсолютно актуальне уявлення про неї. Нові кіберзагрози або варіації старих виникають майже щодня, як і стратегії захисту від них. Однак існують і деякі загальні підходи до забезпечення кібербезпеки, які слід визначати та адаптувати до специфіки конкретних держав і конкретних органів публічної влади.

Існуючі проблеми кібербезпеки в Україні можна поділити на

1. організаційні,
2. технічні (апаратні, інструментальні),
3. правові,
4. інформаційно-технологічні (програмні, алгоритмічні, тощо).

Серед організаційних проблем кібербезпеки слід, насамперед, виділити:

- відсутність системної роботи з підготовки організацій (підприємств,інституцій, державних установ) до кібератак;
- приділення недостатньої уваги організаційним аспектам забезпечення кібербезпеки напротилежність технічним аспектам;
- недостатність процедур по протидії, протистоянню, реагуванню на кібератаки та мінімізації їх наслідків;
- відсутність ефективних механізмів по видаленню порушників кібербезпеки з локальних мереж організацій та глобальних міждержавних (світових) мереж;
- відсутність ефективного інструментарію забезпечення кібербезпеки, який сприяє визначенню наявності кібератаки на мережі конкретної організації та відповідному реагуванню на ці атаки;
- недостатній рівень державної допомоги організаціям, що піддалися чи піддаються атаці, щодо вилучення зловмисників з комп'ютерних мереж тих організацій, які зазнали атак;
- відсутність достатньої державної координації дій щодо управління кібербезпекою як на рівні країни, так і на рівнях окремих підприємств;
- відповідність існуючим світовим стандартам щодо кібербезпеки повинні підтверджувати не державні аудитори, а експерти, що володіють міжнародною сертифікацією по IT-аудиту та кібербезпеці.

В наш час багато проблем кібербезпеки регулюються галузевими регуляторами. Промислові комп’ютерні мережі ставлять унікальні задачі перед фахівцями в області безпеки, бо вони недуже схожі на традиційні комп’ютерні мережі, особливо ті, що були побудовані ще до виникнення таких обсягів кіберзагроз, кібервтручань та кіберзлочинів.

Ці мережі багато років були ізольовані від глобальних мереж. Тому в них не передбачалися заходи щодо забезпечення кібербезпеки. Але в наш час навіть така ізольованність не є запорукою кібербезпеки.

Серед технічних проблем кібербезпеки слід виділити, насамперед:

- відсутність точного реєстру апаратно-технічного обладнання (як підприємств, так і мереж);
- відсутність підтримки технічними засобами механізму управління

змінами і реалізації політики безпеки;

- недостатні можливості апаратного моніторингу станів підприємства та мереж;

- недостатнє апаратно-технічне забезпечення запобіганню проникнення до мережі (підприємства, установи, інституції тощо) кіберзлочинців.

Для захисту комп'ютерних мереж, слід спочатку зрозуміти, які ІТ вони використовують та на яких принципах працюють.

Забезпечення безпеки комп'ютерних мереж вимагає, зокрема,знання ПЗ, яке використовується підприємствами (або окремими користувачами), поточних налаштувань відповідного ПЗ.

Важливою проблемою безпеки комп'ютерних мереж є забезпечення прозорості дій, яка може вплинути на безпеку і надійність критично важливих інформаційних активів. Складність усунення цієї проблеми полягає в тому, що в мережах використовуються кілька різних комунікаційних протоколів.

Ще однією проблемою безпеки комп'ютерних мереж є неможливість забезпечення управління змінами та дотримання політики безпеки. Без системи запобігання неавторизованому доступу чи інформування про нього, можна вільно отримати доступ до активу і змінити його налаштування. Кібербезпека передбачає вирішення багатьох проблем, в тому числі й боротьба з комп'ютерними вірусами.

Кібербезпека стикнулася з тим, що групи кіберзлочинців стають все більш «корпоративними», ставлячи своїми мішенями:

- нові технології все частіше моделюють корпоративну ієрархію (у багатьох організаціях застосовуються так звані «шлюзи», що маскують шкідливу активність; це надає можливість кіберзлочинцям захоплювати кіберпростір та уникати виявлення);

- можливості та ризики хмарних технологій (багато хмарних застосунків, ініціаторами застосування яких є співробітники компанії з метою підвищення ефективності та пошуку нових бізнес-перспектив, зараховано до категорії підвищеного ризику);

- звичне рекламне ПЗ, що стає джерелом зараження більше половини мереж підприємств. Забезпечення кібербезпеки є актуальним для багатьох сфер діяльності,зокрема, сфер науки, техніки та технологій (особливо ІТ), що охоплюють проблеми, пов'язані із захищеністю кіберпростору країни, окремих об'єктів його інфраструктури тощо.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Баранов, О.А.,2014. Про тлумачення та визначення поняття «кібербезпека»,Правова інформатика.

2. Андреев В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є Основи кібербезпеки / За ред. проф. В.О. Хорошка. вид., доп. і перероб. — К. : Вид. ДУІКТ, 2009. —292 с

3. Летичевський О.О. Сучасні наукові проблеми кібербезпеки. Вісник НАН України. 2023. № 2. С. 12—20. https://doi.org/10.15407/visn2023.02.012

Мельник Ілля Андрійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ОСНОВНІ РИЗИКИ СПАМУ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

Спам у інформаційній системі організації може призвести до порушення конфіденційності даних, завантаження шкідливого ПЗ, перевантаження ресурсів системи та витрат часу співробітників на обробку небажаної пошти. Для захисту від цих ризиків організації повинні впроваджувати високоякісні фільтри для електронної пошти, навчати своїх співробітників розпізнавати та уникати шкідливого контенту, а також регулярно оновлювати своє програмне забезпечення та системи безпеки.

Основні ризики спаму в інформаційній системі організації

Спам є одним з найпоширеніших і найвідоміших видів кіберзагроз, з якими стикається більшість організацій у світі. Ці повідомлення можуть здаватися незначущими або просто дратівливими, але вони несуть великі ризики для інформаційних систем організації.[1]

1. Завантаження шкідливого ПЗ: Часто спам-листи маскуються під легітимні повідомлення від відомих організацій. Але їх справжньою метою є змусити користувача відкрити вкладені файли або натиснути на посилання, яке може завантажити шкідливе ПЗ на комп'ютер. Таке ПЗ може вкрасти особисту інформацію, зламати систему або навіть зашифрувати дані, вимагаючи викуп.
2. Фішингові атаки: Фішинг є спробою шахрайства, коли зловмисники намагаються отримати доступ до конфіденційних даних, таких як логіни, паролі та номери банківських карток, шляхом введення в оману. Спамові листи з фішинговими атаками можуть імітувати повідомлення від банків, соціальних мереж або служб підтримки.
3. Перевантаження ресурсів: Кожен спам-лист, який надходить на сервер організації, використовує ресурси: місце для зберігання, потужність обробки та мережевий трафік. У великих обсягах спам може серйозно уповільнити роботу системи.
4. Втрата важливої інформації: Фільтри, які блокують спам, можуть іноді помилково класифікувати важливі листи як спам. Це може призвести до втрати критичної інформації або пропущених можливостей для організації.
5. Витрати часу: Для співробітників організації необхідно витрачати час на перевірку папки "Спам" на наявність важливих повідомлень, що може поглибити ризики втрати часу та продуктивності.
6. Порушення конфіденційності: В деяких спамових повідомленнях можуть бути вкладені відстежувачі, які збирають інформацію про користувача, його поведінку та звички, що може призвести до порушення приватності.

Дотримуючись рішень та рекомендацій, організація зможе знизити ризики, пов'язані зі спамом, та забезпечити безпеку своєї інформаційної системи:

- Встановлення антивірусних програм з регулярними оновленнями.
- Заборона автоматичного відкриття вкладень в електронних листах.

- Проведення регулярних навчань для співробітників щодо безпеки в інтернеті та ризиків, пов'язаних з шкідливими вкладеннями.
- Використання фільтрів електронної пошти для виявлення підозрілих листів.
- Навчання персоналу розпізнавати фішингові атаки та відповідно реагувати.
- Встановлення двофакторної аутентифікації для всіх систем.
- Впровадження ефективних спам-фільтрів.
- Збільшення мережевої пропускної здатності та ресурсів сервера.
- Використання хмарних рішень для зберігання пошти з можливістю масштабування.
- Перевірка налаштувань спам-фільтрів, щоб уникнути помилкового видалення легітимних повідомлень.
- Регулярне резервне копіювання електронної пошти.
- Введення системи внутрішнього відстеження комунікацій.
- Автоматизація процесу сортування та видалення спаму.
- Навчання співробітників користуватися інструментами електронної пошти ефективніше.
- Введення системи швидкого повідомлення про спам для підтвердження його наявності.
- Встановлення захисних мережевих брандмауерів та інших інструментів захисту.
- Навчання персоналу основам кібербезпеки та методам розпізнавання шпигунського ПЗ.
- Регулярний аудит інформаційних систем на предмет можливих витоків даних.

Перелік посилань:

3. Spam Impact on Information Security URL:https://shubbakom.files.wordpress.com/2014/10/spam-impact-on-information-security-shubbakom.pdf
4. SPAM. How to recognize it and better protect yourself URL: https://www.wdsinvest.com/PDFs/Spam-ProtectYourself-ConsumerAffairs.pdf

Мельников Антон Анатолійович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

КІБЕРБЕЗПЕКА У КОРПОРАТИВНИХ СОЦІАЛЬНИХ МЕРЕЖАХ

Корпоративні соціальні мережі (Enterprise Social Network, ESN) є важливим інструментом для підвищення комунікації та обміну інформацією всередині організацій. Забезпечення кібербезпеки у ESN є вирішальним завданням, оскільки вони містять чутливу інформацію. Загрози витку даних, атак та соціальної інженерії тощо, можуть призвести до серйозних наслідків. Комплексний підхід до кібербезпеки, що включає розробку політики захисту, навчання співробітників та дотримання

законодавства, є необхідним для успішного захисту корпоративних соціальних мереж і функціювання компанії.

Корпоративні соціальні мережі (Enterprise Social Network, ESN) є віртуальними середовищами або онлайн-платформами, що розроблені для внутрішнього використання організацією або підприємством. ESN створені з метою покращення комунікації та обміну інформацією між співробітниками та іншими зацікавленими сторонами й надають співробітникам інструменти для спілкування, спільної роботи над проектами, обміну інформацією та знанням. ESN відрізняються від загальнодоступних соціальних мереж, таких як Facebook або X (Twitter), тим, що призначені для обмеженої аудиторії та орієнтовані на задоволення конкретних корпоративних потреб [1].

Кібербезпека корпоративних соціальних мереж має критичне значення, оскільки це засоби для обміну конфіденційною інформацією та даними всередині організації. Порушення безпеки ESN може призвести до витоку чутливих даних, шахрайства, атак на внутрішні ресурси та потенційно серйозних фінансових збитків, а також пошкодити репутацію компанії. Гарантія захисту корпоративних соціальних мереж є обов'язковою для забезпечення надійної комунікації та співробітництва в організації.

Загрози та ризики у ESN пов'язані з можливістю порушення безпеки даних та інформації всередині організації. Вони зазвичай включають можливість витоку конфіденційної інформації, шахрайство, вірусні атаки, а також соціальну інженерію, яка може призвести до компрометації облікових даних співробітників та порушення безпеки. Внутрішні загрози також можуть становити ризик, оскільки співробітники можуть несвідомо чи навмисно порушувати правила безпеки у корпоративних соціальних мережах, створюючи потенційні вразливості для організації. Ці загрози можуть мати серйозні наслідки як для безпеки, так і репутації організації. Ефективне управління та моніторинг безпеки в ESN є невід'ємною частиною захисту корпоративних ресурсів та даних.

Для корпоративних соціальних мереж існують різні загрози і ризики, включаючи наступні [2, 3]:

1. Соціальна інженерія. Зловмисники можуть використовувати маніпуляцію співробітниками, щоб отримати доступ до конфіденційної інформації або інтегрувати у мережу шкідливе програмне забезпечення.

2. Шахрайство і фішинг. Зловмисні шкідливі активності можуть включати фішингові атаки, які представляються як довірені джерела ESN, з метою обдурити співробітників і отримати доступ до облікових даних.

3. Витік конфіденційної інформації. Ненадійна система безпеки ESN може призвести до небажаного витоку корпоративної інформації та даних, включаючи інтелектуальну власність та персональні дані.

4. Шкідливі програми та віруси. В ESN можуть бути розміщені шкідливі посилання або файли, які можуть стати причиною зараження робочої мережі або пристроїв співробітників.

5. Внутрішні загрози. Співробітники можуть ненавмисно або навмисно становити загрозу безпеці, публікуючи конфіденційні дані або розкриваючи чутливу інформацію.

6. Недоліки безпеки застосунків і платформ. Недоліки у безпеці застосунків, сервісів і платформ, у тому числі вбудованих та інтегрованих, ESN можуть стати вразливими місцями та використані зловмисниками.

7. Атаки на структуру мережі. Зломи та атаки на інфраструктуру ESN можуть призвести до простоїв у роботі, втрати доступу до даних та втрати самих даних.

8. Порушення законодавства про дані. Недотримання законів про захист, збереження і обробку даних та конфіденційності в ESN може призвести до юридичних і репутаційних наслідків та штрафів.

Корпоративні соціальні мережі включають три ключові компоненти: людський, програмний та інфраструктурний. Ризики безпеки пов'язані з кожним із цих компонентів. Розробка та дотримання стратегій безпеки, які охоплюють всі три аспекти, необхідна для запобігання загрозам та мінімізації ризиків у ESN.

Основні принципи кібербезпеки у корпоративних соціальних мережах [3]:

1. Навчання співробітників. Регулярне навчання працівників з питань безпеки, включаючи виявлення фішингу та соціальної інженерії, допомагає зміцнити людський фактор безпеки.

2. Керування доступом. Обмеження доступу до даних та функцій лише на необхідному рівні для виконання робочих обов'язків скорочує ризики несанкціонованого доступу.

3. Шифрування даних. Захист конфіденційної інформації шляхом шифрування даних при збереженні та передачі забезпечує додатковий рівень безпеки.

4. Моніторинг та виявлення інцидентів. Безперервний моніторинг активності в мережі дозволяє швидко виявляти та реагувати на потенційні загрози та інциденти.

5. Регулярне оновлення та патчі. Оновлення програмних систем, застосунків та платформ вчасно, а також встановлення патчів для усунення відомих вразливостей допомагає запобігати атакам.

У контексті корпоративних соціальних мереж, правові аспекти та дотримання законодавства стають невід'ємною частиною діяльності організації. Захист персональних даних є одним із ключових аспектів, оскільки мережі можуть містити чутливу інформацію про співробітників та клієнтів. Дотримання нормативів, таких як Загальний регламент захисту даних (GDPR) та інших нормативних актів, необхідне для запобігання порушенням та штрафам, пов'язаним з неприпустимою обробкою персональних даних. Ризик порушення законів порушує питання не лише юридичної відповідальності, а й заподіяння шкоди репутації компанії, що робить дотримання законодавства вкрай важливим аспектом в управлінні ESN та вимагає від компанії розробки суворих політик та заходів безпеки.

Для забезпечення та підвищення безпеки у корпоративних соціальних мережах компанії повинні приділяти особливу увагу навчанню співробітників, що націлене на розпізнавання та запобігання кіберзагрозам і сприяє підвищенню обізнаності та зниженню ризиків соціальної інженерії та фішингу. Реалізація сучасних стандартів та найкращих практик у галузі кібербезпеки, включаючи заходи контролю доступу, усунення програмних вразливостей, шифрування даних та управління ідентифікацією є необхідною складовою ESN. Створення, впровадження та дотримання довгострокової стратегії, що включає оцінку загроз, розробку планів моніторингу, реагування на інциденти, розслідування аномалій сценаріїв використання, а також регулярні аудити безпеки (кодової бази та інфраструктури), допоможе компанії більш ефективно управляти ризиками та реагувати на потенційні атаки [3].

Кібербезпека у корпоративних соціальних мережах є важливим і необхідним завданням для сучасних організацій. Відсутність адекватних заходів безпеки може призвести до витоку конфіденційної інформації, фінансових втрат та загроз для репутації компанії. Дотримання законодавства, навчання співробітників, дотримання кращих практик та розробка стратегії кібербезпеки – ключові елементи успішного забезпечення безпеки в корпоративних соціальних мережах.

Перелік посилань:

1. Butler C. Enterprise Social Networking and Collaboration / Chester Butler. – Martin Butler Research, 2010. – 25 с.
2. Cybersecurity for Social Networking Sites Issues, Challenges, and Solutions | by Priya Reddy | Lotus Fruit | Medium URL: https://medium.com/lotus-fruit/cyber-security-for-social-networking-sites-issues-challenges-and-solutions-1be871211a9 (дата звернення: 18.10.2023).
3. Cerra A. The Cybersecurity Playbook: How Every Leader and Employee Can Contribute to a Culture of Security (1st Edition) / Allison Cerra. – Wiley, 2019. – 224 с. – (1st Edition).

Мельникова Єлизавета Дмитрівна
студентка групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

УПРАВЛІННЯ ПОЛІТИКОЮ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Взв'язку з науково-технологічним прогрессом останні десятиліття широко поставлене питання інформаційної безпеки. Багато важливих інтересів підприємства в сучаності значною мірою визначається станом навколишнього інформаційного середовища. Тому інформаційна безпека в теперешніх умовах є однією з необхідних установ нормального функціонування підприємства. В найбільш загальному вигляді інформаційна безпека може бути визначена як неможливість нанесення шкоди властивостям об'єкту безпеки, що можно зазначити інформацією та інформаційною інфраструктурою. К об'єктам інформаційної безпеки в організації відносять: інформаційні ресурси, які містять відомості, що відносяться до комерційної таємниці та конфіденційну інформацію, яка представлена у вигляді інформаційних масивів та баз даних; засоби та системи інформатизації; засоби комп'ютерної та організаційної техніки; мережі та системи; загальне системне та прикладне програмне забезпечення; автоматизовані системи управління в організаціях; системи зв'язку та передачі даних; технічні засоби збору; реєстрації, передачі, обробки та відображення інформації.[1]

Політика інформаційної безпеки – це набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності підприємств і спрямовані на досягнення та підтримку інформаційної безпеки організацій.

Головною причиною запровадження політики безпеки зазвичай є вимога наявності такого документа від регулятора — організації, що визначає правила роботи підприємств даної галузі. У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності. Крім того, певні вимоги (рекомендації) пред'являють галузеві або загальні, місцеві чи міжнародні стандарти. Зазвичай це виражається у вигляді зауважень зовнішніх аудиторів, які проводять перевірки діяльності підприємства. Відсутність політики викликає негативну оцінку, яка в свою чергу впливає на публічні показники підприємства — позиції в рейтингу, рівень надійності і тому подібне.

Метою політики інформаційної безпеки має бути впровадження та ефективне управління системою забезпечення інформаційної безпеки, спрямованої на:

- захист інформаційних активів організації,
- забезпечення стабільної діяльності організації,
- мінімізації ризиків інформаційної безпеки,
- створення позитивних для організації інф. відносин з партнерами, клієнтами та всередині організації.

Система управління інформаційною безпекою – це частина загальної системи управління, яка ґрунтується на підході, що враховує ризики інформаційної безпеки, як бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Для процесів системи управління інформаційною безпекою застосована модель ПВПД (плануй-виконуй-перевіряй-дій; англ. ***Plan-Do-Check-Act, PDCA***)

Рис. 1. Модель ПВДП(PDCA)

Методологія PDCA(ще називають Цикл Демінга) є найпростішим алгоритмом дій керівника по управлінню процесом і досягнення його цілей. Цикл управління починається з планування.

1. Планування: встановлення цілей і процесів, необхідних для досягнення цілей, планування робіт по досягненню цілей процесу і задоволення споживача, планування виділення і розподілу необхідних ресурсів.
2. Виконання: виконання запланованих робіт.
3. Перевірка: збір інформації та контроль результату на основі ключових показників ефективності, що вийшло в ході виконання процесу, виявлення та аналіз відхилень, встановлення причин відхилень.
4. Вплив (управління, коректування): вжиття заходів щодо усунення причин відхилень від запланованого результату, зміни в плануванні та розподілі ресурсів.

Реалізація розглянутих 4-х функцій складає зміст процесу управління якістю в рамках підприємства, коли здійснюється вплив системи якості на виробничий процес. Заявлений у стандартах ISO 9000:2000 процесний підхід до управління якістю організовує процес управління саме відповідно до названих в циклі Демінга функцій, будуючи їх у логічній послідовності.[2]

Для ефективного забезпечення інформаційної безпеки важливим є достатність різноманітних моделей та методів оцінки ризиків в системах управління інформаційною безпекою. Будь-яка оцінка ризиків інформаційної

безпеки починається з обстеження інформаційної системи, ідентифікації інформаційних ресурсів та опису технологій обробки інформації.

При побудові систем управління інформаційною безпекою важливе місце займають процедури та процеси обробки ризиків на основі актуальних глобальних стандартів. Головним завданням стандартів безпеки є створення основи для взаємодії між виробниками, споживачами та експертами з кваліфікації продуктів інформаційних технологій.

У сучасного бізнесу основною потребою є ідентифікування ризиків і управління ними. Технічні можливості постійно збільшуються, технічні засоби ускладнюються, вимоги стрімко ростуть. Саме тому одним з найважливіших аспектів роботи підприємства є управління політикою захисту інформаційної безпеки, на основі чіткого дотримання систем захисту інформації.

Перелік джерел :

1. Лобода О.М. Захист інформації в корпоративних мережах. Публічне управління та адміністрування у процесах економічних реформ: матеріали IV Всеукр. наук.-практ.конф., м.Херсон, 11 лист. 2020р. ХДАЕУ, 2020. С.61-63.
2. Управління якістю [Текст]: підручник / П. П. Воробієнко, І. В. Станкевич, Є. М. Стрельчук, Глухова, О. І. – Одеса: ОНАЗ ім. О. С. Попова, 2014. – 376 с

Мельниченко Нікіта Миколайович
Студент групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

АУДИТ ЗАХОДІВ З ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

У даній тезі я надав рекомендації що до аудиту заходів з забезпечення безперервності бізнесу, пояснив чому він є важливим елементом стратегії управління ризиками та забезпечує готовність організації до різноманітних негативних сценаріїв, зберігаючи стабільність та надійність свого бізнесу. BCM – (англ. Business Continuity Management) керування безперервністю бізнесу. BCP – (англ. Business Continuity Planning) план забезпечення безперервності бізнесу.

Система безперервністю бізнесу може бути основана на міжнародном стандарті ISO2230, яка буде служити для мінімізації ризику збою через серйозні події, які можуть загрожувати існуванню вашої організації. На відміну від звичайного управління ризиками, BCM зосереджується на критичних ключових процесах, щоб забезпечити безперервне існування вашої організації в разі надзвичайних ситуацій.

Аудит безперервності бізнесу - це систематичний процес призначений для виявлення та усунення можливих ризиків, оцінки, а тако ж перевірки аспектів, пов’язаних з процусом забезпечення безперервності бізнесу. Цей процес, може вплинути на компанію у разі виникнення непередбачених умов та обставин.

На сам перед треба виявити основні BCP цілі аудиту заходів з забезпечення безперервності бізнесу. Перший етап аудиту - «Оцінка ризиків». Другий – «Перевірка старих процудур захисту». Третій етап аудиту - «Виявлення слабких місць». Четвертий етап аудиту - «Готовність компанії до непередбачених ситуацій». П’ятий етап аудиту - «Удосконалення процесів». Цей

план є базовим та може буди вдосконалений за потребою клієнта.

Оцінка ризиків включає в себе перевірку всієї компанії та допомагає виявити потенційні загрози та можливі вразливі місця, які можуть вплинути на діяльність організації,а також через деякий час визначити їх серйозність.

Перегляд процедур які були впровадженні до проведення аудиту потрібно проаналізувати існуючі плани безперервності бізнесу (включаючи процедури евакуації, відновлення системи, комунікації та інші аспекти), щоб переконатися в їх працездатності та відповідності.

Виявлення слабких місць допомагає виявити слабкі місця, якщо такі є, а також визначення проблеми в існуючих планах забезпечення безперервності, якщо такі є то й забезпечення їх усунення.

Готовність до надзвичайних ситуацій допомагає забезпечити готовність організації до непередбачених подій, такі як стихійні лиха, технологічні збої чи навіть кібератаки. Забезпечення впроваджень стандартів та дотримання стандартів законодавства. Аудити гарантують, що організація дотримується правових вимог і внутрішніх стандартів безперервності бізнесу.

Удосконалення процесів робиться на основі BCP результатів аудиту та документування цих результатів. На основі цього можна покращити плани та процедури безперервності бізнесу, щоб забезпечити більшу надійність та ефективність.

Загалом кажучи «Аудити заходів забезпечення безперервності бізнесу» є ключовим інструментом для забезпечення стабільності та надійності операцій організації в умовах непередбачуваних обставин. Це допомагає виявити, оцінити та усунути потенційні ризики, забезпечити безперервність бізнесу та захистити активи компанії

Перелік посилань:

Сертифікація стандарту ISO22301 - https://www.dqsglobal.com/uk-ua/sertifikujte/iso-22301.

Аудит принципу безпреривної діяльності ГРИНЧШИН Я.М.- http://bses.in.ua/journals/2020/57_2020/25.pdf.

Забезпечення безперервності бізнесу - https://www.servicedesk.site/uk/2019/01/05/забезпечення-безперервності-бізнесу/.

Управління безперервністю бізнесу – система менеджменту - https://www.dqsglobal.com/uk-ua/navchajtesya/blog/upravlinnya-bezperervnistyu-biznesu-–-sistema-menedzhmentu-stijkistyu

РОЗГЛЯД-АУДИТОРОМ-БЕЗПЕРЕРВ.ДІЯЛЬНОСТІ-ПІД-ЧАС-АУДИТУ - https://www.apu.com.ua/wp-content/uploads/2022/05/2_Інф.лист-РАПУ_РОЗГЛЯД-АУДИТОРОМ-БЕЗПЕРЕРВ.ДІЯЛЬНОСТІ-ПІД-ЧАС-АУДИТУ-ФЗ-5.pdf.

Миколаєнко Олексій Сергійович
студент групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

АНАЛІЗ ТА ОЦІНКА ВРАЗЛИВОСТЕЙ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ (IOT) ТА РОЗРОБКА МЕТОДІВ ЇХ ЗАХИСТУ.

Дана робота присвячена проблемі аналізу та оцінювання вразливостей у мережах Інтернету речей (IoT), наголошено наважливості розроблення методів їхнього захисту, розглядаються технічні та організаційні аспекти безпеки IoT і необхідність постійного

моніторингу та оновлення заходів безпеки для запобігання потенційним загрозам. У статті також розглядається необхідність.

Інтернет-речей (IoT)- це мережі, що складаються із сукупності фізичних об'єктів (речей) або пристроїв, які мають вбудовані сенсори, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даних між об‘єктами і комп'ютерними системами.

Протягом останнього десятиліття Інтернет речей плавно увійшов в наше життя завдяки появі систем бездротового зв'язку, таких як RFID, Wi-Fi, 5G, IEEE 802.15.x, які найчастіше використовуються в основі додатків моніторингу та контролю. Сьогодні системи Інтернету речей використовують не тільки для приватних мереж, а й на виробництвах, фабриках, заводах, підприємствах та навіть в державних установах. Основна проблема використання мереж IoT полягає в тому, що вони не мають захисту від впливів зі сторони зловмисника. Це може призвести, в ліпшому випадку, до заподіяння шкоди майну користувача, а в гіршому – його здоров‘ю та життю. Наприклад, пристрої контролю та управління електричною мережею можуть бути захоплені зловмисником за допомогою будь-якого девайсу, що має доступ до мережі Інтернет, та відповідного програмного забезпечення. Отримавши повний чи частковий контроль над пристроєм зловмисник може спричинити вимкнення або псування електричних приладів, в тому числі критично-необхідних приладів (систем життєзабезпечення в лікарнях, систем моніторингу на виробництві, охоронних систем, тощо), створити коротке замикання в мережі та навіть спричинити пожежу або аварію, якщо мова йде про виробництво. Саме тому постає актуальна проблема дослідження безпеки Інтернету речей та, зокрема, безпеки користувача, його майна та особистої інформації, що передається, обробляється та зберігається в мережах IoT. Предметом дослідження є загальна оцінка небезпек для Інтернету речей на основних структурних рівнях, проблеми захисту персональних даних людини та забезпечення конфіденційності її інформації, основні ризики, пов‘язані з інтеграцією Інтернету речей в життя людини, вплив незахищеності Інтернету речей на життєдіяльність людини. Аналіз публікацій. Високий рівень неоднорідності в поєднанні з широкою гамою систем Інтернету речей, як очікується, підвищить існуючий рівень загроз безпеки в глобальній мережі, яка все частіше використовується для взаємодії людей, машин і роботів. Зокрема, традиційні заходи дотримання конфіденційності і протидії загрозам не можуть бути безпосередньо застосовані до технологій IoT через їх обмежені обчислювальні потужності. [1].

Тому були виділені такі слабкі місця IoT:

- перехід на IPv6;
- живлення датчиків;
- стандартизація архітектури та протоколів, сертифікація пристроїв;
- інформаційна безпека;
- стандартні облікові записи від виробника, слабка аутентифікація;
- надання підтримки з боку виробника для усунення вразливостей;

- важко або неможливо оновити ПЗ і ОС;
- використання текстових протоколів і непотрібних відкритих портів;
- використовуючи слабкість одного гаджета, хакера легко потрапити в усю мережу;
- використання незахищених мобільних технологій;
- використання незахищеної хмарної інфраструктури;
- використання небезпечного ПЗ.

У питаннях залишається гостро, компанії-розробники техніки, засобів комунікації, мережевих пристроїв, програмного забезпечення, кіберзахисні компанії переймаються пошуками засобів захисту пристроїв IoT. Однією з провідних компаній у розробці засобів безпеки в IoT є Cisco Systems, яка успішно виконувала провідну роль у розробці моделі IoT на Всесвітньому форумі IoT (IWF), розробила фреймворк безпеки IoT, що став корисним доповненням до еталонної моделі. На малюнку 1 продемонстровано середовище безпеки, пов'язане з логічною структурою IoT.

Модель Cisco IoT є спрощеною версією моделі Всесвітнього форуму IoT. Вона складалася з наступних рівнів:

1. «Розумні» об'єкти та вбудовані системи;
2. Туманна, периферійна мережа;
3. Ядро мережі;
4. Центр даних та хмарних сервісів;

За допомогою цієї чотирьохрівневої моделі архітектури Cisco шукає чотири загальні можливості безпеки, які охоплюють кілька рівнів:

1. Безпека на основі ролей: системи управління доступом на основі ролей призначають права доступу до ролей, а не окремим користувачам. Користувачам, у свій час, зіставляються різні ролі, або статично, або динамічно, відповідно до обов'язків.

2. Захист від втручання і виявлення втручань: ця функція особливо важлива на рівнях пристроїв і туманної мережі, але розширюється також і на рівні ядра мережі. Усі ці рівні можуть використовувати компоненти, які фізично знаходяться на території вільного доступу до них будь-ким.

3. Захист даних і конфіденційність: ці функції охоплюють усі рівні архітектури.

4. Захист протоколів Інтернету: захист від прослуховування і перехоплення важливих для всіх рівнів.

У документах Cisco також пропонується концепція безпеки IoT, що визначає компоненти функції безпеки для IoT, яка охоплює всі рівні:

1. Аутентифікація: цей компонент охоплює елементи, які ініціюють доступ, і в першу чергу ідентифікує пристрій IoT. На відміну від типових корпоративних мережевих пристроїв, кінцеві пристрої IoT повинні оснащуватися такими методами аутентифікації, які не вимагають втручання людини. Таким методам належать радіочастотні мітки, сертифікати x.509 або MAC-адреси кінцевих пристроїв.

2. Авторизація: авторизація керує доступом до пристрою через структуру

мережі. Цей елемент включає в себе контроль доступу. Разом з рівнем аутентифікації він виробляє додаткові параметри для того, щоб дозволити обмін повідомленнями між пристроями та між пристроями та відповідними платформами, тим самим забезпечуючи роботу IoT-служб.

3. Мережева політика: цей компонент охоплює всі елементи, які визначають маршрутизацію та транспортування трафіку з кінцевих пристроїв інфраструктури, будь то контроль, управління або власне трафік даних.

4. Аналітика безпеки: цей компонент включає в себе всі функції, необхідні для централізованого управління пристроями IoT. На основі видимості можна спроможність здійснювати контроль, включаючи конфігурацію, патчі та оновлення, а також контрзаходи для припинення загроз[2].

Висновок Аналіз і оцінка вразливостей мереж Інтернету речей (IoT) є одним із ключових елементів сучасної кібербезпеки. Виявлені вразливості можуть призвести до серйозних кібератак порушення конфіденційності. Розроблення методівзахисту необхідне для забезпечення безпеки під'єднаних пристроїв і призначених для користувачів даних, заходи безпеки постійно контролюються, оновлюються для захисту мережі IoT, виробники, оператори споживання технологій IoT працюють спільно. Тільки так можна забезпечити сталий розвиток майбутнього Інтернету речей.

Перелік посилань

1.Кисиленко В.К. Аналіз безпеки інтернет речей.
Сайт

2. Глухенький О.С., Лобанчикова Н.М. Analysis of attacks on components of IoT systems and cybersecurity technologies.
Сайт.

Моісєєв Артемій Миколайович, БСДМ-62
Державний університет телекомунікацій Навчально-науковий інститут захисту інформації
М. Київ

ТИПОВИЙ СЦЕНАРІЙ РЕАГУВАННЯ НА ІНЦИДЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Security Operations Center (SOC) дослівно оперативний центр безпеки, в практичній діяльності отримав назву центр моніторингу та реагування на інциденти інформаційної безпеки. Основною метою його діяльності є виявлення і реагування на інциденти інформаційної безпеки. Розглянемо, типовий сценарій реагування на інцидент інформаційної безпеки.

Security Operations Center (SOC) - дослівно - центр оперативний центр безпек, на практиці його називають центром моніторингу та реагування на інциденти інформаційної безпеки. Його основне призначення - виявлення та реагування на інциденти інформаційної безпеки. Розглянемо типовий сценарій реагування на інцидент інформаційної безпеки.

Процес реагування на інцидент складається з декількох етапів. Перший, початковий етап передбачає створення та навчання команди реагування на

інциденти, а також отримання необхідних інструментів та ресурсів. Під час цієї підготовки організація також намагається обмежити кількість інцидентів, які можуть статися, обираючи та впроваджуючи набір функцій контролю та запобігання на основі результатів оцінки ризиків. Однак завжди існує залишковий ризик, який неминуче залишиться після впровадження засобів контролю. Таким чином, своєчасне виявлення та повідомлення про будь-які порушення безпеки є невід'ємною частиною процесу реагування. Зрештою, залежно від серйозності інциденту, організація може пом'якшити його наслідки, усунувши порушення і, зрештою, відновивши систему. На цьому етапі роботи часто повертаються до фази виявлення та аналізу - наприклад, щоб з'ясувати, чи не були заражені додаткові хости під час ліквідації інциденту зі шкідливим програмним забезпеченням.

Коли ви отримуєте оповіщення або повідомлення про події інформаційної безпеки від користувачів і систем, вам необхідно їх зареєструвати. Згодом необхідно визначити, чи є ця подія інцидентом інформаційної безпеки. За наявності ознак належності події до інциденту ІБ проводиться попередній аналіз, збір та уточнення інформації про подію, визначається класифікація інцидентів за рівнем критичності, до якого належить подія. Останнім етапом реагування є фіксація результатів реагування на інциденти ІБ, їх закриття в системі реагування та інформування ініціаторів про закриття інциденту повідомленнями про закриття інциденту. Після повного опрацювання інциденту організація видає звіт, в якому детально описується причина інциденту, вартість збитків, завданих інцидентом, і кроки, які організація повинна вжити для запобігання майбутнім інцидентам. Таким чином, основними завданнями етапу розслідування інциденту інформаційної безпеки є

- Точна діагностика інциденту;
- локалізація та мінімізація наслідків і втрат;
- виявлення основних причин інциденту;
- збір доказів інциденту;
- відновлення порушених інформаційних систем;
- вдосконалення систем безпеки;
- впровадження заходів захисту для запобігання подібних інцидентів у майбутньому;

Перелік посилань:

1. Реагування на інциденти: що вам повинен SOC [Електронний ресурс] – Режим доступу: https://www.anti-malware.ru/analytics/Technology_Analysis/Correct-SOC-Incident-Response

2. Analyst's Notebook data. IBM Knowledge Center [Електронний ресурс] – Режим доступу: https://www.ibm.com/support/knowledgecenter/SSXVXZ_2.3.1/com.ibm.i2.landing.doc/eia_welcome.htm

Мурзін Ігор Васильович
студент групи БСДм-61, ННІЗІ ДУІКТ, Київ, Україна

РОЛЬ SURICATA В ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ МЕРЕЖІ ТА ВИЯВЛЕННІ ЗАГРОЗ

У сучасному цифровому світі, де кібер загрози стають все більш складними та розповсюдженими, важливість ефективних систем виявлення вторгнень стає критичною для забезпечення безпеки мережі. Suricata, як система відкритого джерела, виявляється ключовим інструментом у боротьбі з цими загрозами, завдяки своїм передовим можливостям та гнучкості.

Загальні поняття та принципи роботи Suricata

Suricata є системою відкритого джерела, яка базується на мережевому механізмі виявлення вторгнень (IDS) та системі запобігання вторгнень (IPS). Вона працює на основі обробки пакетів мережі і використовує набір правил та сигнатур для виявлення потенційних загроз у мережі. Suricata може аналізувати різні протоколи, включаючи TCP, UDP, та ICMP, та виявляти аномалії в пакетах для ідентифікації можливих атак.[1]

Suricata відіграє ключову роль у забезпеченні безпеки мережі завдяки своїм передовим можливостям виявлення вторгнень та запобіганню кібер загроз. Його гнучкість та швидкодія роблять його необхідним інструментом у сучасному цифровому середовищі. У цій статті буде детально розглянуто технологічні аспекти функціонування Suricata, його переваги порівняно з іншими системами виявлення вторгнень та важливість його застосування для забезпечення безпеки мережі в умовах постійно зростаючих кібер загроз.

Тенденції у розвитку Suricata

Suricata продовжує активно розвиватися, щоб відповідати зростаючим вимогам сучасного цифрового світу. Однією з ключових тенденцій є покращення алгоритмів машинного навчання для підвищення точності виявлення нових та невідомих загроз. Впровадження технологій штучного інтелекту дозволяє Suricata більш ефективно аналізувати та реагувати на нові типи атак, що робить його ще більш потужним інструментом для захисту мережі.

еякі з найважливіших тенденцій у розвитку Suricata включають:

- Підтримка нових протоколів та технологій: Suricata активно вдосконалюється для підтримки нових мережевих протоколів та технологій, таких як IPv6, TLS 1.3, та інші, що дозволяє ефективніше виявляти загрози в нових середовищах.

- Вдосконалення аналізу поведінки: Розробники постійно працюють над вдосконаленням алгоритмів аналізу поведінки мережі для виявлення аномальних патернів та надійнішого виявлення нових типів атак.
- Інтеграція з іншими системами безпеки: Suricata активно інтегрується з іншими системами безпеки, такими як системи керування подіями та інцидентами (SIEM), що дозволяє операторам мережі отримувати комплексний огляд ситуації та швидко реагувати на загрози.

- Застосування машинного навчання та штучного інтелекту: У майбутньому очікується збільшення застосування методів машинного навчання та штучного інтелекту для покращення точності виявлення загроз та зниження кількості помилкових спрацювань.

Ці тенденції демонструють постійне вдосконалення Suricata для забезпечення більш ефективного виявлення загроз у сучасних мережевих середовищах.[2]

Обґрунтування ефективності Suricata порівняно з іншими системами виявлення вторгнень

Suricata виділяється серед інших систем виявлення вторгнень своєю здатністю працювати в реальному часі при великому обсязі мережевого трафіку. Вона має високу швидкодію обробки пакетів і здатність виявляти навіть складні типи атак, такі як атаки відмови в обслуговуванні (DDoS) та атаки на мережеві протоколи.

У порівнянні з іншими популярними системами, Suricata надає більш гнучкі налаштування та можливості інтеграції з іншими інструментами мережевої безпеки. Її відкрита архітектура дозволяє розробникам створювати власні правила та сигнатури для виявлення нових загроз, що робить її більш адаптованою до змінюючихся умов мережевої безпеки.

Незважаючи на свої переваги, Suricata також має свої обмеження, такі як вимоги до обчислювальних ресурсів, які можуть бути значними при обробці великого обсягу даних. Проте, завдяки своїй високій ефективності та широким можливостям налаштування, Suricata залишається важливим інструментом для забезпечення безпеки мережі в умовах постійно зростаючих кібер загроз.

Висновок

Suricata є потужним інструментом для виявлення загроз у мережі, який відзначається високою ефективністю та гнучкістю налаштування. Його здатність працювати в реальному часі та виявляти навіть складні типи атак робить його невід'ємною частиною комплексної стратегії мережевої безпеки в сучасному цифровому середовищі.

Перелік посилань:
1. What is Suricata? URL: https://docs.suricata.io/en/latest/what-is-suricata.html
2. Suricata DESCRIPTION URL: https://docs.suricata.io/en/latest/manpages/suricata.html

Мухомора Іван Валерійович
студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

МЕРЕЖЕВА РОЗВІДКА ЯК ЗАГРОЗА РОЗКРИТТЯ ПЕРСОНАЛЬНИХ ДАНИХ

Загроза розкриття персональних даних набрала обертів у сучасному світі. У зв'язку з війнами, більшість країн світу почали не тільки озброювати армії, а й збирати дані про осіб у інших країнах

Загроза полягає в тому, що ці дані можуть використовуватися не тільки для аналізу громадської думки або оцінки ситуації у деякій країні, а й для зловживання, шпигунства чи втручання в особисте життя громадян. Це може мати наслідком порушення приватності та безпеки особистих даних.. Один з способів збору персональних даних є OSINT та Recon. Тому важливість збереження особистих даних є важливою ціллю для кіберзахисту. Удосконалення методів приховування від мережевих розвідок та освіченості суспільства має важливу роль для кіберзахисту.

Open-SourceIntelligence (OSINT) - це процес збору, аналізу та використання відкритої інформації для забезпечення безпеки та розуміння ситуації. Це включає в себе збір інформації з відкритих джерел, таких як мас-медіа, соціальні мережі, публічно доступні бази даних, веб-сайти та інші громадські джерела. Інформація з джерел OSINT може бути використана для аналізу загроз, прогнозування тенденцій, здійснення досліджень та забезпечення інформаційної переваги. Збір інформації з відкритих джерел може включати моніторинг новин, аналіз соціальних медіа, дослідження відгуків споживачів, перегляд відкритих документів та публікацій, які доступні для громадськості. Методи збору можуть варіюватися від ручного пошуку до використання автоматизованих інструментів та технологій, що аналізують великі обсяги даних для виявлення корисної інформації. Інформація, зібрана з відкритих джерел, може бути використана в багатьох сферах, включаючи розвідку, кібербезпеку, бізнес-аналітику, дипломатію та дослідження ринків. За допомогою правильного аналізу даних з відкритих джерел, можна отримати цінні інсайти, які допомагають в прийнятті обґрунтованих рішень та стратегій [1].

Recon у сфері кібербезпеки відноситься до процесу збору інформації про цільову систему або мережу для подальшого аналізу та використання цієї інформації для планування атаки. Цей процес включає в себе пошук вразливостей, збір інформації про мережеву інфраструктуру, сканування портів, виявлення послаблення безпеки та ідентифікацію можливих точок входу.

Recon може бути виконаний шляхом різноманітних технік, включаючи сканування мережі для виявлення активних хостів, збір інформації про сервери, домени, IP-адреси та системи, визначення версій програмного забезпечення та операційних систем, а також аналіз конфігурацій мережі та систем.

Мета Recon полягає в тому, щоб зрозуміти уразливості системи та знайти можливі точки входу для подальших атак. Це дозволяє кіберзлочинцям чи етичним хакерам виявити слабкі місця та знайти способи проникнення у систему з метою внесення змін, викрадання даних або здійснення інших злочинних дій.

Приклади OSINT та Recon [2]:

1. Пошук відкритої інформації на веб-сайтах: Це може включати використання пошукових систем, таких як Google, Bing або спеціалізовані пошукові інструменти, для знаходження публічно доступної інформації, такої як інформація про компанії, особи, події тощо.
2. Моніторинг соціальних мереж: Відслідковування активності на соціальних мережах для отримання інформації про вподобання, думки, звички або розташування користувачів.

3. Аналіз публічних документів: Дослідження публічних документів, таких як документи компаній, правові документи, звіти про фінансову діяльність тощо, для отримання інформації про діяльність та стан організацій.

4. Сканування портів та виявлення вразливостей: Використання спеціальних програм для виявлення вразливостей у мережевій інфраструктурі та програмах, які можуть бути використані для забезпечення доступу до системи.

5. Збір інформації про домени та IP-адреси: Вивчення інформації про домени та IP-адреси для визначення власників, місцезнаходження, стану безпеки та інших параметрів, що допомагають у виявленні потенційних загроз.

Методи захисту [3]:

1. Моніторинг онлайн-профілю: Ретельно контролюйте свій онлайн-профіль, обмежуючи публічні деталі та переглядаючи доступну інформацію, яка може бути використана для збору даних.

2. Зміцнення приватності в соціальних мережах: Налаштуйте налаштування конфіденційності в соціальних мережах, щоб обмежити доступ до особистої інформації.

3. Контроль доступу до особистої інформації: Обережно ставтеся до того, кому ви надаєте свою особисту інформацію, і обмежуйте доступ до конфіденційних даних.

4. Використання безпечних паролів: Використовуйте складні паролі для всіх ваших онлайн-акаунтів і активуйте двофакторну аутентифікацію там, де це можливо.

5. Використання VPN: Використовуйте віртуальні приватні мережі (VPN) для шифрування і захисту вашого інтернет-з'єднання, особливо при роботі з відкритими мережами Wi-Fi.

6. Шифрування даних: Застосовуйте шифрування для захисту конфіденційних даних на вашому комп'ютері, смартфоні та в інших цифрових пристроях.

7. Оновлення програмного забезпечення: Підтримуйте всі програми та операційні системи оновленими, щоб уникнути використання вразливостей, які можуть бути використані для збору даних.

8. Етичний хакінг: Здійснюйте етичний хакінг та тестування на проникнення, щоб виявити можливі уразливості в вашій системі та вжити заходів для їх виправлення.

Перелік посилань:

1. OSINT курс від Molfar. *OSINT-Molfar*. URL: https://molfar.com/services/osint-course (дата звернення: 20.10.2023).

2. Як працює OSINT-розвідка та чому небезпечно публікувати інформацію в інтернеті. *ФАКТИ ICTV*. URL: https://fakty.com.ua/ua/ukraine/suspilstvo/20220429-yak-praczyuye-osint-rozvidka-ta-chomu-nebezpechno-publikuvaty-informacziyu-v-internet/ (дата звернення: 20.10.2023).

3. The Art of Intrusion. The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers. Kevin D. Mitnick. Скачать в формате fb2, epub, doc, txt. Hotlib. HOTLIB.NET. *Электронная библиотека. Книги на любой вкус.Hotlib. HOTLIB.NET*. URL: https://hotlib.net/htbk263183_the_art_of_intrusion_the_real_stories_behind_the_exploits_of_hackers_intruders_and_deceivers.html (дата звернення: 10.10.2023).

М’ясников Микита Сергійович
студент групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

ДОСЛІДЖЕННЯ ТА ПОРІВНЯННЯ МЕТОДІВ АВТЕНТИФІКАЦІЇ БІОМЕТРИЧНИМИ ДАНИМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Ця дослідницька робота присвячена дослідженню і порівнянню різних методів автентифікації, які використовують біометричні дані для забезпечення інформаційної безпеки. У сучасному світі, де даними можна легко маніпулювати та викрасти, інформаційна безпека стає надзвичайно важливою для користувачів і організацій. Біометричні дані, такі як відбитки пальців, розпізнавання обличчя, голосу та інші, надають можливість унікально ідентифікувати особу на основі її фізіологічних або поведінкових рис.

Впровадження біометричних систем в життя суспільства є незаперечним фактом. Світові аналітики прогнозують підвищення попиту на біометрії в усіх галузях і розширення сфери її застосування. Актуальність розвитку біометричних технологій ідентифікації особи обумовлена збільшенням числа об’єктів і потоків інформації, які необхідно захищати від несанкціонованого доступу, а саме: криміналістика; системи контролю доступу; системи ідентифікації особи; інформаційна безпека; облік робочого часу та реєстрація відвідувачів; системи голосування, проведення електронних платежів; автентифікація на Web-ресурсах; різні соціальні проекти, де потрібна ідентифікація людей; проекти цивільної ідентифікації (перетин державних кордонів, видача віз на відвідування країни). Ідентифікація на основі біометричні данні – це засіб автоматичного розпізнавання особистості на базі унікальних фізичних або поведінкових параметрів. Ідентифікація виконується за допомогою порівняння отриманих біометричних характеристик і шаблонів, що зберігаються у базі даних. Для користувачів, які застосовують системи біометричної ідентифікації і автентифікації, дуже важливим є зручність застосування цих засобів (це не тільки швидкість і простота проведення процедури, але і можливість використання звичного обладнання). На сьогодні оптимальним співвідношенням між надійністю автентифікації, ціною і зручністю використання має визначення особистості по обличчю, чим і пояснюється високий темп розвитку і поширення таких технологій. [1]

Перший метод автентифікації, який розглянуто в дослідженні, - розпізнавання обличчя. Це найбільш древній і поширений спосіб ідентифікації, заснований на тому, що риси обличчя і форма черепа кожної людини індивідуальні. Комп'ютер лише автоматизує процедуру, виконуючи аналогічну процедуру, з тією різницею, що замість фото застосовуються біометричні дані, записані в еталонному образі. Так як використовуються фізіологічні характеристики людини, цей метод відноситься до статичних методів біометрії. Це самий інтуїтивно зрозумілий метод ідентифікації, найбільш близький до того, як люди ідентифікують один одного. Розпізнавання обличчя стало широко

використовуваним, особливо на мобільних пристроях та в системах відеоспостереження. Його перевагами є зручність використання і відсутність необхідності в додатковому обладнанні. Проте він вразливий до атак, які використовують фотографії чи образи обличчя, і вимагає великого обсягу ресурсів для обробки і порівняння обличь.[2]

Другий метод - аналіз голосу. Він базується на унікальних особливостях голосу кожної особи, таких як тембр, інтонація та акцент. Аналіз голосу може використовувати як текстові команди, так і голосові команди для автентифікації. *«Hey Google»* або *«Hey Siri»* — це приклади команд, які можна використовувати для взаємодії з голосовим помічником телефона. Саме вони і представляють системи розпізнавання голосу, які реагують лише на конкретні голосові команди. Під час налаштування телефона потрібно лише вимовити кілька речень вголос, щоб дозволити алгоритму вивчати ваші голосові особливості. Чим більше ви розмовляєте з віртуальним помічником, таким як Google або Siri, тим краще він розпізнає ваш голос. Такий спосіб автентифікації має високий рівень надійності, проте може бути уразливим до атак, які використовують записи голосу. [3]

Третій метод - сканування відбитків пальців. Він використовує унікальні патерни відбитків пальців для ідентифікації особи. Цей метод є одним з найбільш надійних і широко використовується в банківських установах та сфері медицини. Він є менш вразливим до атак порівняно з попередніми методами, проте вимагає спеціального обладнання для сканування. Також ця технологія має певні обмеження: надмірно волога чи суха шкіра може погіршити продуктивність системи, або коли відбитки пальців пошкодженні або мають шрами. [4]

Результати дослідження показують, що вибір методу автентифікації біометричними даними повинен бути здійснений з урахуванням конкретних потреб і вимог користувачів та організацій. Кожен з розглянутих методів має свої переваги та недоліки, і важливо враховувати їх при впровадженні системи автентифікації.

Перелік посилань:

1. Бугаєнко Х.А. “Аналіз трьох біометричних методів автентифікації особи” : http://nbuv.gov.ua/UJRN/Prre_2012_11_2_27

2. Нечипоренко О. В. “Біометрична ідентифікація і автентифікація особи за геометрією обличчя” : http://nbuv.gov.ua/UJRN/Vchnu_tekh_2016_4_26

3. “Найпоширеніші типи біометричної автентифікації” : https://www.eset.com/ua/about/newsroom/blog/data-protection/mogut-li-khakery-pokhitit-vash-otpechatok-paltsa-nedostatki-biometricheskoy-autentifikatsii/

4. К.В. Колесніков, Б.П. Ободовський ”Види біометричної автентифікації та методи їх оцінки” : http://dspace.nbuv.gov.ua/bitstream/handle/123456789/162340/07-Kolesnikov.pdf

Негода Вадим Андрійович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ЗЛОВМИСНИКІВ В КОРПОРАТИВНІЙ МЕРЕЖІ ПІДПРИЄМСТВА НА ОСНОВІ FIDELIS DECEPTION

Інформаційні технології все швидше розвиваються з кожним роком, а разом з ними загрози, в мережі організацій, стають дедалі складнішими. В кібербезпеці існує такий вислів «Зловмисники завжди на шаг попереду», тому підприємства постійно шукають інноваційні способи виявлення зловмисників та способи посилити свої заходи кібербезпеки. Однією з таких технологій, яка стала потужним інструментом у боротьбі з кіберзлочинцями, є Fidelis Deception.

Корпоративні мережі є джерелом життєвої сили сучасних підприємств, спрощуючи спілкування, зберігання даних і важливі бізнес-процеси. Однак вони також є основними цілями для кіберзлочинців, які прагнуть отримати несанкціонований доступ до конфіденційної інформації, фінансових даних або інтелектуальної власності.

Хоча традиційні рішення інформаційної безпеки, такі як брандмауери та антивірусне програмне забезпечення або EDR рішення, важливі, їх часто недостатньо для захисту від тактики кібер-зловмисників, що постійно змінюється. Ці зловмисники мають високі навички уникнення виявлення та використання вразливостей. Ось тут і вступає в дію технологія обману, така як Fidelis Deception.

Fidelis Deception — це рішення інформаційної безпеки, яке використовує проактивний підхід до виявлення загроз[1, с.258]. Принцип роботи цього рішення пов’язаний з обманом зловмисника та подальшим його виявленням, методом створення оманливих елементів в корпоративній мережі, таких як сервери-приманки, підроблені облікові дані та сфабриковані дані(breadcrumbs). Ці елементи створені для імітації справжніх активів і даних, що робить їх привабливими цілями для зловмисників.

Як працює Fidelis Deception[1, с.260]:

1. Заманювання зловмисників: за допомогою Fidelis Deception розгортаються пастки та breadcrumbs(оманливі елементи) в мережі, кожен з яких виглядає як реальний актив. Кібер-зловмисники, які знаходяться всередині мережі, приваблюють пастки, несвідомо починають з ними комунікувати.
2. Сповіщення в режимі реального часу: коли зловмисники взаємодіють із приманками, Fidelis Deception спостерігає за їх поведінкою, аналізуючи кожен їхній рух. Будь-які дії викликають попередження в реальному часі, визначаючи тактику зловмисника, що дозволяє командам безпеки швидко реагувати на потенційну загрозу.
3. Детальні криміналістичні дані: Fidelis збирає детальну інформацію про тактику, прийоми та процедури зловмисника (TTP). Ці дані є безцінними для розуміння природи загрози та вдосконалення стратегій кібербезпеки.

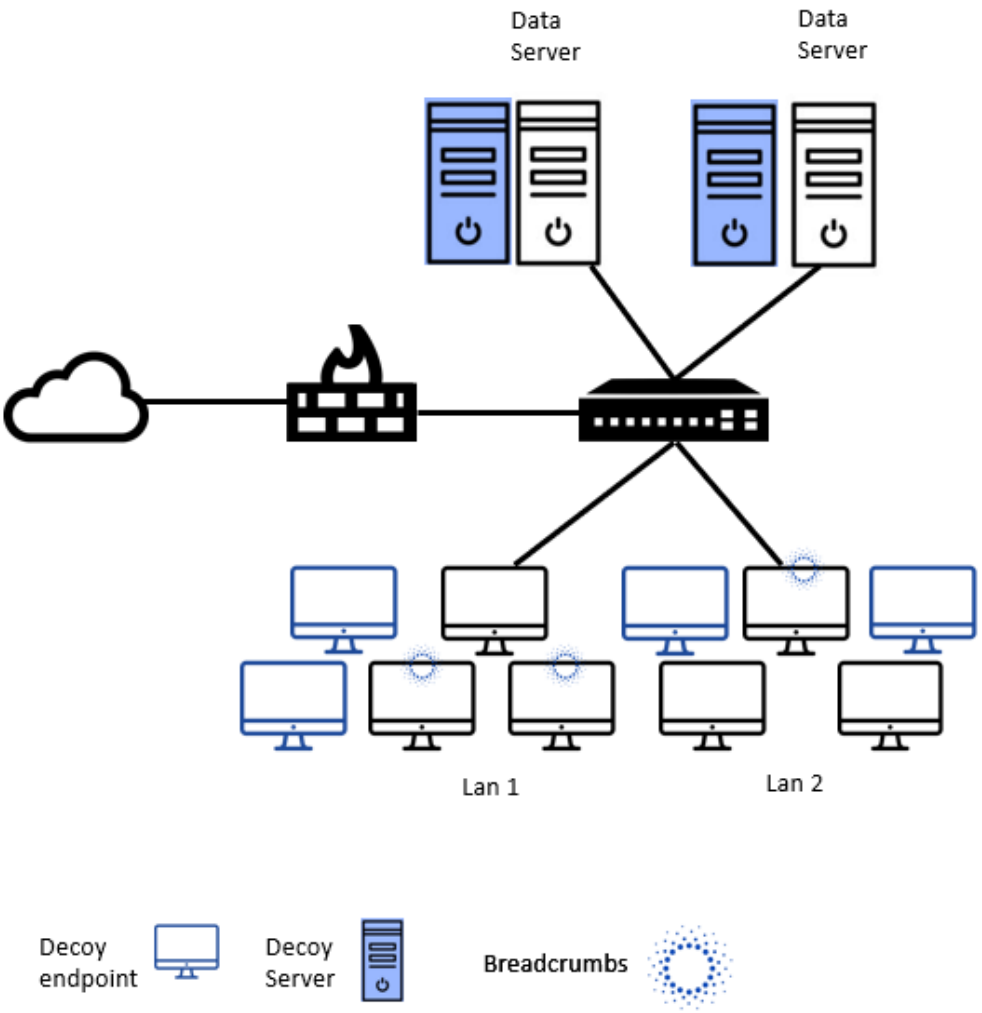


Рис.1 – Схема роботи Deception технології

Переваги Fidelis Deception:

1. Раннє виявлення загроз: технологія обману має проактивний характер і призначена для виявлення загроз на ранніх стадіях. Залучаючи зловмисників до взаємодії з оманливими елементами, він визначає підозрілу активність до того, як буде завдано будь-якої фактичної шкоди. Це раннє виявлення має вирішальне значення для запобігання витоку даних і мінімізації збитків.

2. Зменшення помилкових спрацьовувань: Deception технологія дуже точно розрізняє реальні загрози та помилкові спрацювання. Це пояснюється тим, що технологія створює оманливі елементи, які точно імітують реальні активи, ускладнюючи зловмисникам розрізнення між справжніми та підробленими ресурсами, тому будь-яка комунікація з пасткою потребує розслідування. У результаті організації стикаються з меншою кількістю помилкових спрацьовувань, що зменшує навантаження на команди безпеки.[2]

3. Threat Intelligence: Fidelis Deception надає цінну інформацію про загрози, відстежуючи тактики, прийоми та процедури зловмисника(TTP), що дозволяє організаціям зміцнити свій захист.

4. Активний захист: на відміну від багатьох традиційних рішень безпеки, які покладаються на пасивний моніторинг і попередження, Deception технологія використовує активний підхід до кібербезпеки. Він взаємодіє зі зловмисниками, відволікаючи їхню увагу від справжніх активів на приманки. Це не тільки визначає загрози, але також може збити з пантелику зловмисників.

Підсумовуючи, технологія Fidelis Deception стала могутнім союзником у боротьбі з кіберзагрозами в корпоративних мережах. Вводячи в оману та швидко виявляючи зловмисників, він дає змогу організаціям бути на крок попереду тих, хто прагне скомпрометувати їхні дані. Оскільки кіберзагрози продовжують розвиватися, такі рішення, як Fidelis Deception, є незамінними для захисту цілісності та безпеки корпоративних даних і бізнес-процесів.

Перелік посилань:

3. Fidelis Deception Documentation URL: https://support.fidelissecurity.com/hc/en-us/articles/15357225648275-9-6-x-Deception-Documentation
4. What is Deception Technology URL: https://www.zscaler.com/resources/security-terms-glossary/what-is-deception-technology

Новик Леонід Анатолійович,
студент групи УБДМ-51, ННІЗІ ДУІКТ, Київ, Україна

БЕЗПЕКА ХМАРНИХ ТЕХНОЛОГІЙ ТА ОСНОВНІ ІНФОРМАЦІЙНІ ЗАГРОЗИ

Хмарними рішеннями зараз цікавляться майже всі компанії. Якщо у бізнесі присутні будь-які IT-процеси, включаючи електронні документи, бази даних, бухгалтерія, – вам знадобляться віртуальні сервери. В останні роки представники різних сфер та бізнеси всіх масштабів починають активніше використовувати хмарні рішення. Постає питання відповідальності за виконання умов, стандартів згідно з законодавством.

Підключенням хмарної інфраструктури компанії намагаються забезпечити збереження даних та реалізувати вимоги інформаційної безпеки.

Як обрати правильне хмарне рішення

При виборі будь-якої хмарної інфраструктури для початку варто зрозуміти, які бізнес-завдання мають бути вирішені. Вартість і час, які потрібні на перехід у хмару, залежать від задач, що стоять перед бізнесом, і від обсягу необхідної інфраструктури для переносу інформації.

Загалом існує три типи хмарних рішень: публічні, приватні та гібридні. Всі вони побудовані на базі серверів, які програмно об'єднані в один кластер.

Якщо попит на обробку даних починає перевищувати можливості локального центру, компаніям краще використовувати хмари для миттєвого масштабування продуктивності та задоволення зростаючих потреб. Це також дозволить їм відмовитися від придбання, встановлення та обслуговування нових серверів, які можуть використовуватися епізодично.

Обчислювальні ресурси публічного варіанту хмарного сховища програмно діляться між замовниками, що, відповідно, впливає на потужності, які може

отримати кожен клієнт.

Приватна хмара надає ресурси виключно для одного замовника. Вона є ізольованою, і на фізичному, і на програмному рівнях. Такий варіант найкраще підходить великим корпораціям.

Для галузей, які працюють із конфіденційними даними, наприклад, банки, державний сектор, сфера охорони здоров'я, гібридна хмара буде оптимальним варіантом. Наприклад, іноді потрібно, щоб певні типи даних зберігалися в локальному середовищі, а менш конфіденційні – у хмарі.

З такою гібридною хмарною архітектурою організації отримують переваги додаткової гнучкості загальнодоступного сховища для виконання менш регламентованих обчислювальних задач, виконуючи в той же час усі галузеві вимоги.

Хто несе відповідальність за безпеку даних

Відповідальність за виконання вимог закону або стандарту лежить саме на замовниках. Для цього потрібно укласти спеціальну угоду з сертифікованим хмарним провайдером.

Вендори хмарних рішень мають забезпечувати виконання вимог із безпеки на рівні інфраструктури і доступу власних адміністраторів. Вони повинні прийняти вимоги про захист і офіційно підтвердити свою відповідність.

Водночас замовник має створити детальне технічне завдання, в якому буде вказано перелік бажаних хмарних послуг. Зокрема, які стандарти і вимоги необхідно забезпечити з інформаційної безпеки. Також потрібна деталізація ступеня залучення хмарного провайдера для гарантування безпеки, необхідності захисту каналів зв'язку з системами або користувачами, що знаходяться поза межами хмарної інфраструктури.

При цьому, якщо провайдер надає якісь засоби захисту, то клієнт повинен самостійно перевірити, на що саме поширюються ці засоби захисту і чи достатньо їх для задоволення вимог, закріплених у його власних документах.

Перехід до хмарних рішень є ключовим етапом на шляху цифрового розвитку компаній. Однак потрібно пам'ятати, що міграція даних у хмару не знімає відповідальність за регулярний пошук і застосування передових методів управління даними. Застосування cloud-технологій будь-якої з моделей не позбавляє від необхідності оцінювати й ухвалювати рішення з мінімізації ризиків, які притаманні класичній IT-інфраструктурі.

Малі та середні підприємства, як і глобальні компанії, все більше покладаються на послуги безпеки хмарних обчислень для підтримки повсякденних бізнес-функцій, розробки програмного забезпечення і навіть для забезпечення технологічної інфраструктури, необхідної для роботи.

Нижче наведено основні хмарні загрози:

Витік даних або несанкціонований доступ до даних

Все більше підприємств малого та середнього бізнесу розміщують у хмарі велику кількість даних, включаючи конфіденційні дані, які несуть інформацію, яка стосується транзакцій клієнтів. На відміну від даних, що зберігаються локально в корпоративних центрах обробки даних, дані у хмарі знаходяться за

межами захисту брандмауера та вразливі до будь-яких загроз, з якими може зіткнутися постачальник хмарних послуг.

Несанкціонований доступ до даних через недостатній контроль доступу або неправильне використання облікових даних співробітників може зробити важливі бізнес-дані відкритими для хакерів та інших зловмисників.

У нещодавньому звіті про основні загрози хмарних обчислень некомерційної організації Cloud Security Alliance (CSA), що займається просуванням передових методів забезпечення безпеки у хмарних обчисленнях та навчання використанню хмарних обчислень для забезпечення безпеки всіх інших форм обчислень.

На думку CSA, негативні наслідки витоку даних можуть включати вплив на репутацію і довіру клієнтів або партнерів, нормативні наслідки, які можуть призвести до грошових збитків, і вплив на бренд, який може викликати зниження ринкової вартості.

Неправильна конфігурація хмари

Ще однією поширеною проблемою, пов’язаною з хмарою, є неправильна конфігурація, яка впливає на безпеку. На базовому рівні це відбувається, коли адміністратор або користувач неправильно застосовує параметри безпеки для хмарної платформи. Це може містити такі проблеми, як неправильне обмеження доступу, неактивне шифрування даних, паролі за замовчуванням, неправильне керування дозволами.

Деякі неправильні налаштування можуть бути результатом внутрішніх загроз, включаючи ненавмисні помилки, недбалість або відсутність проінформованості користувачів про безпеку. Випадкові зміни налаштувань також можуть спричинити неправильну конфігурацію

Спеціалісти CSA повідомили, що неправильна конфігурація хмарних ресурсів є однією з основних причин витоку даних і може призвести до видалення або зміни ресурсів та переривання обслуговування.

“Відсутність ефективного контролю змін є найпоширенішою причиною неправильної конфігурації у хмарному середовищі”, – заявили в CSA. “Хмарні середовища та методології безпеки хмарних обчислень відрізняються від традиційних IT, тим, що зміни складніше контролювати”.

SMB можуть вирішити проблему неправильної конфігурації хмари, дізнавшись більше про всі використовувані хмарні сервіси, включаючи налаштування та дозволи; змінюючи облікові дані та дозволи при необхідності; і розгортаючи багатофакторну автентифікацію зниження ризику несанкціонованого доступу.

DDoS атаки

DDoS – ще одна поширена загроза, з якою стикаються організації під час використання хмарних послуг. У ході таких атак кіберзлочинець прагне зробити систему або мережевий ресурс недоступним для користувачів, порушуючи роботу вузла, підключеного до мережі.

Відмова в обслуговуванні зазвичай досягається шляхом заповнення машини або іншого ресурсу запитами у спробі перевантажити системи та

завадити виконанню реальних запитів. При DDoS-атаках вхідний трафік, що викликає переповнення, надходить із кількох джерел.

Враховуючи, що малі та середні підприємства дедалі більше ведуть бізнес в Інтернеті, такі атаки можуть спричинити серйозні проблеми та призвести до втрати бізнесу.

Одним із способів боротьби з DDoS-атаками у хмарі є забезпечення надмірної пропускної спроможності інтернет-з'єднання. Це допоможе мінімізувати вплив потоку запитів. Компанії також можуть розгорнути такі інструменти, як сканери додатків для пошуку вразливостей у мережах та системах, які можуть бути використані зловмисниками, та брандмауери веб-додатків для моніторингу та фільтрації певного трафіку.

Злом акаунтів

Використовуючи злом облікових записів, зловмисники можуть отримати доступ до облікових записів користувачів хмарних сервісів. За даними CSA, найбільшим ризиком є облікові записи хмарних сервісів або підписки.

"Фішингові атаки, експлуатація хмарних систем або крадіжка облікових даних можуть скомпрометувати ці акаунти", – йдеться у звіті організації. "Ці загрози – унікальні та потенційно потужні – можуть спричинити значні порушення у роботі хмарного середовища, такі як втрата даних та ресурсів, а також скомпрометовані операції". За сл'овами представників організації, наслідки таких атак іноді бувають дуже серйозними, а в недавніх випадках злому мали місце значні збої в операційній діяльності та бізнесі.

Серед способів, якими зловмисники можуть захопити облікові записи, – фішинг, коли користувачі викрадають інформацію під час відвідування незахищених веб-сайтів; кейлоггінг, коли програма записує натискання клавіш користувача та надсилає інформацію зловмисникам; і переповнення буфера, коли зловмисники перезаписують дані пам'яті іншими даними, що дає їм несанкціонований доступ.

SMB повинні підвищувати проінформованість працівників про ці типи загроз. Для цього необхідно навчити людей розпізнавати можливі атаки фішинга і що робити, якщо вони з ними зіткнулися. Інші ефективні методи включають розгортання технології багатофакторної аутентифікації (MFA) та створення надійних паролів з їх регулярною зміною.

Незахищені програмні інтерфейси програм (API)

API можуть бути надзвичайно корисними для інтеграції різних хмарних платформ та інструментів, однак вони несуть у собі можливі ризики безпеки. Якщо API не захищені, зловмисники можуть використовувати вразливість та отримати доступ до конфіденційних даних.

Дослідницька компанія Gartner прогнозує, що до 2022 року атаки на API стануть найчастішим вектором атак, що призводить до витоку даних із корпоративних веб-додатків. За даними компанії, багато широко розрекламованих вразливостей у безпеці API вже торкнулися цілої низки організацій.

CSA, яка віднесла незахищені інтерфейси і API до основних хмарних

загроз, зазначає, що постачальники хмарних послуг надають набір інтерфейсів і API, які дозволяють клієнтам керувати хмарними послугами і взаємодіяти з ними. За даними CSA, безпека та доступність загальних хмарних сервісів залежить від безпеки цих API, а погано продумані API можуть призвести до зловживань або витоку даних.

Для усунення цього ризику, на думку CSA, компаніям слід дотримуватись належної гігієни API, включаючи ретельний нагляд за такими елементами, як інвентаризація, тестування, аудит та захист від аномальної активності. Вони також повинні забезпечити належний захист ключів API, уникаючи повторного використання, та розглянути можливість використання стандартних та відкритих API-фреймворків.

Перелік посилань:

1. Безпека хмарних технологій: міф чи реальністью URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/bezopasnost-informatsionnykh-sistem/informatsionnaya-bezopasnost-avtomatizirovannykh-sistem-asu/
2. Топ хмарних загроз, з якими необхідно боротися малим та середнім підприємствам. URL: https://softico.ua/uk/news/top-hmarnih-zagroz-z-yakimi-neobhidno-borotisya-malim-ta-serednim-pidpriyemstvam/

Одноочко Денис Володимирович
студент групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

ЗАСТОСУВАННЯ DLP-СИСТЕМ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Дана дослідницька робота присвячена аналізу застосування DLP-систем як одного із ключових інструментів забезпечення інформаційної безпеки. На теперішній час конфіденційна інформація у цифровому середовищі є основним активом для більшості організацій, несанкціоноване поширення якої може призвести до непоправних наслідків. Саме тому вивчення та використання DLP-систем надзвичайно важливе, адже вони розроблені для виявлення та запобігання витокам даних.

Останні роки характеризуються збільшенням кількості витоків інформації та масштабних кібератак на інформаційні системи компаній усіх форм власності. Однією з причин посилення тенденції витоку інформації є зростання частки державних та приватних організацій, які не приділяють достатньої уваги інформаційній безпеці. Найчастіше джерелом витоку конфіденційних даних є інсайдери, послугами яких часто користуються як спецслужби, так і різні зловмисники. Саме витоки інформації із державних організацій можуть становити загрозу національній безпеці.

Розробка та впровадження окремих систем для контролю за обігом конфіденційної інформації та запобігання її витоку – одне із важливих завдань кожного підприємства. Ці системи відрізняються своїми можливостями та функціональністю, але всі вони узагальнюються абревіатурою DLP (Data Leak Prevention), яка запропонована агентством Forrester в 2005 році. Якщо брати національну термінологію, то це «системи запобігання витоку інформації» [1].

Головним аспектом вибору і впровадження DLP-системи є її сумісність з

принципами й вимогами роботи всієї організації. Всю інформацію, наявну в мережі можна розділити на кілька типів [2]:

- не класифікована;
- загальнодоступна інформація;
- конфіденційна, але не критична;
- строго конфіденційна інформація.

Вибір DLP-системи залежить від завдань, які потрібно вирішити конкретній компанії. У найзагальнішому вигляді завдання поділяються на кілька груп, включаючи контроль руху конфіденційної інформації, нагляд за активністю співробітників протягом дня, моніторинг мережевий (аналіз шлюзів) та комплексний (мережі та кінцеві робочі станції). Для цілей більшості компаній оптимальним буде вибір комплексного рішення DLP. Для малих та середніх підприємств підійдуть хостові системи. Плюси хостових DLP – задовільна функціональність та невисока вартість. Серед мінусів – низькі продуктивність, масштабованість та відмовостійкість.

У мережевих DLP таких недоліків немає. Вони легко інтегруються та взаємодіють з рішеннями інших вендорів. Це важливий аспект, оскільки DLP-система має злагоджено працювати в тандемі з продуктами, які вже встановлені в корпоративній мережі. Не менш важлива і сумісність DLP з базами даних та програмним забезпеченням.

DLP-системи засновані на аналізі потоків даних, що перетинають периметр захищеності інформаційної системи. При виявленні в цьому потоці конфіденційної інформації спрацьовує активна компонента системи, і передача повідомлення (пакета, потоку, сесії) блокується.

Як окремий програмний продукт DLP-система характеризується наявністю наступного функціонала: DLP-системи аналізують витікаючий трафік, DLP-системи проводять аналіз інформаційних потоків за декількома технологіями [3, с. 24]. Принцип роботи DLP-системи показано на рис. 1.

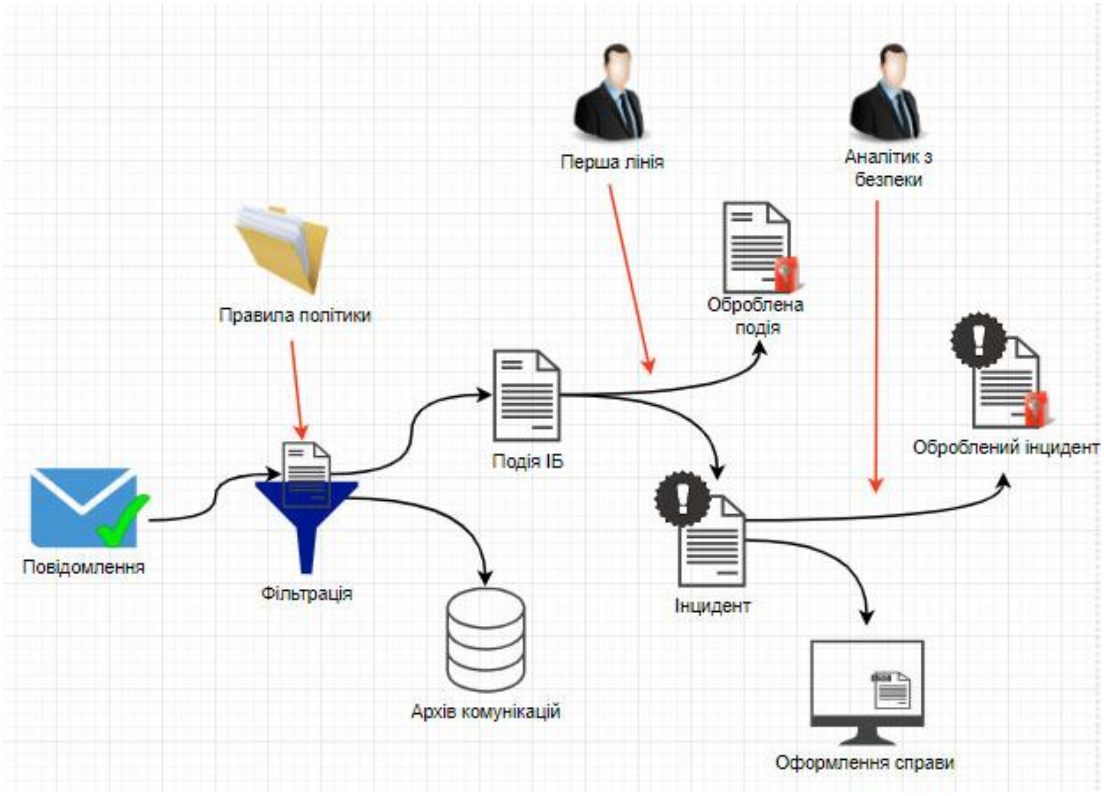


Рис. 1 – Принцип роботи DLP-системи

При виборі DLP враховуються канали передачі даних, які використовуються в компанії. Канали передачі даних - це різноманітні методи, якими інформація може переміщуватися внутрішньо та зовні компанії. Оцінка цих каналів допомагає компанії визначити потенційні точки витоку даних і вжити заходи для їх захисту. Приклад каналів передачі даних, які контролюються DLP-системою показано на рис. 2.

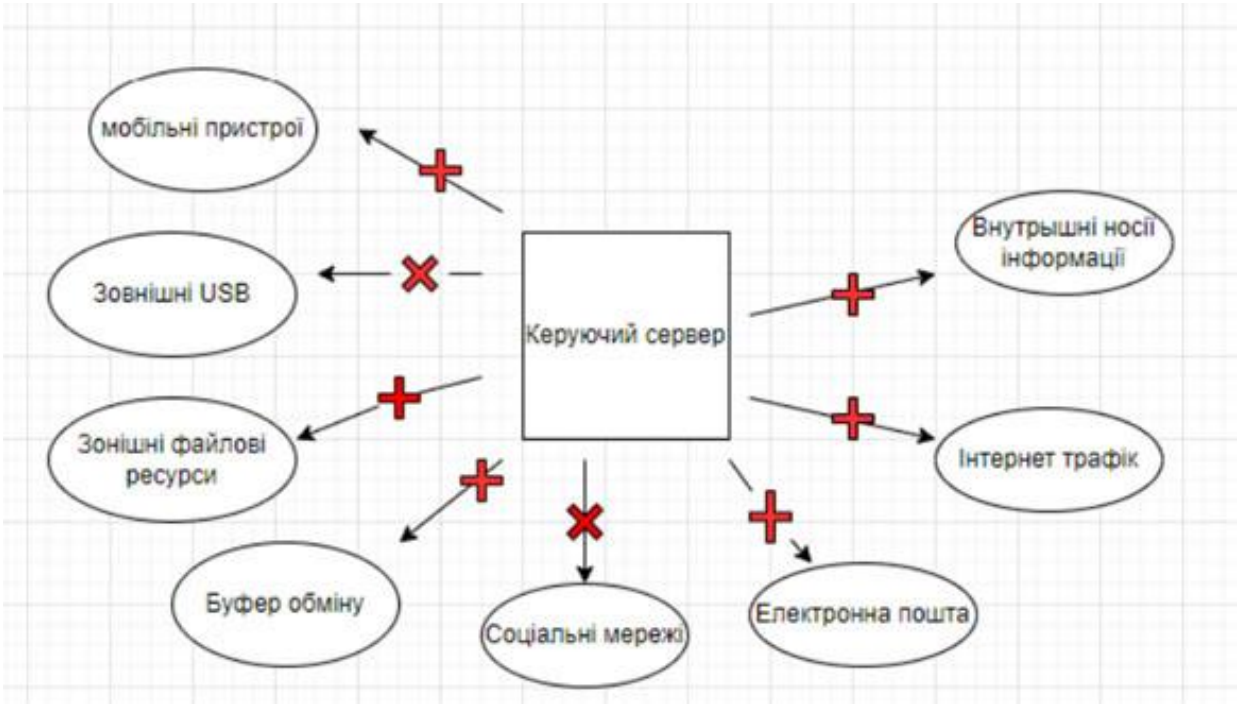


Рис. 2 – Канали передачі даних контрольовані DLP-системою

Як висновок, застосування DLP-систем є важливим кроком для забезпечення інформаційної безпеки в організаціях. За допомогою цих систем можна контролювати, моніторити та захищати конфіденційну інформацію від зовнішніх та внутрішніх загроз. Зі зростанням кількості кіберзлочинів та витоків даних, DLP-системи стають необхідним інструментом для будь-якої організації, яка цінує свою інформаційну безпеку.

Перелік посилань:
1. АРХІТЕКТУРА DLP-СИСТЕМ В УМОВАХ ПОЛІТИКИ BYOD URL: https://ela.kpi.ua/bitstream/123456789/50872/1/%28151-154%29_Vovchanovskyi.pdf (дата звернення: 23.10.2023).
2. DLP – рішення для запобігання витоку даних в організаціях URL: http://dspace.oneu.edu.ua/jspui/handle/123456789/7124?locale=ru (дата звернення: 24.10.2023).
3. Методи та моделі забезпечення інформаційної безпеки інформаційнотелекомунікаційних систем на основі DLP технології URL: https://ir.nmu.org.ua/bitstream/handle/123456789/151307/%D0%A1%D1%83%D0%B4%D0%B0%D1%80%D0%B8%D0%BA%D0%BE%D0%B2.pdf?sequence=3&isAllowed=y (дата звернення: 24.10.2023).

Оладько Ярослав Олександрович
студент групи БСДМ-62, ІКБ ДУТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ ЗА БАЗІ SAFETICA ONE

Інформаційна безпека є невід'ємною частиною сучасного бізнесу та державного управління. Обсяг даних, що обробляються організаціями, зростає з кожним днем, так само як і загрози

конфіденційності, цілісності та доступності цих даних. Зловмисники та кіберзлочинці постійно вдосконалюють свої методи проникнення в інформаційні системи та завдання їм шкоди. Тому важливо мати надійні технології та стратегії захисту конфіденційних даних.

Саме тому ми приділяємо особливу увагу технологіям захисту конфіденційних даних в інформаційних системах організації та розглядаємо в цьому контексті рішення Safetica ONE. Інформаційна безпека - один із найважливіших чинників успішного функціонування сучасної організації, особливо тієї, яка спирається на обробку великих обсягів даних.

Safetica ONE - це комплексне рішення для захисту конфіденційних даних в інформаційних системах організації, що ґрунтується на технології Data Loss Prevention (DLP), яка дає змогу ідентифікувати, класифікувати, контролювати та захищати конфіденційні дані в режимі реального часу. Основні функції включають:

Моніторинг активності Safetica ONE відстежує активність користувачів в інформаційних системах. Вона аналізує, які файли користувачі відкривають, копіюють, відправляють або намагаються передати несанкціонованими каналами.

Класифікація даних: автоматично класифікує дані за рівнем чутливості, полегшуючи виявлення та управління найбільш чутливими даними.

Запобігання витоку даних Safetica ONE виявляє спроби несанкціонованого вилучення даних і негайно реагує на ці загрози. Передача файлів може бути припинена, а користувачам можуть бути виведені настроювані попередження.

Шифрування даних, щоб зловмисники не змогли отримати доступ до конфіденційної інформації в разі втрати фізичного доступу.

Компанія Safetica Technologies має багаторічний досвід і знання в галузі інформаційної безпеки та кіберзахисту. Компанія спеціалізується на розробці рішень для виявлення, управління та захисту конфіденційної інформації, а також запобігання доступу до неї неавторизованих користувачів. Контроль продуктивності Safetica Technologies надає інструменти для моніторингу активності користувачів і оптимізації робочих процесів, допомагаючи збалансувати безпеку і продуктивність. Інноваційні рішення: ми постійно впроваджуємо нові технології та розробляємо інноваційні підходи до забезпечення інформаційної безпеки та кіберзахисту. Safetica Technologies активно співпрацює із замовниками, розробляючи рішення та адаптуючи їх до специфічних потреб організації. На основі накопиченого досвіду і досліджень компанія Safetica Technologies розробила систему Safetica ONE, яка забезпечує надійний захист даних і відповідність стандартам інформаційної безпеки.

Safetica ONE захищає всі пристрої, підключені до локальної мережі організації. Це робочі станції, сервери та інші пристрої, що використовуються для обробки і зберігання даних. Також дозволяє визначати і контролювати доступ до даних на цих пристроях. Оскільки багато організацій використовують хмарні сервіси для зберігання та обміну даними, Safetica ONE забезпечує захист і на цьому рівні. Моніторинг і контроль доступу до даних у хмарних сервісах дає змогу запобігти можливим витокам інформації. У зв'язку зі зростанням кількості мобільних пристроїв, використовуваних співробітниками, Safetica ONE також забезпечує захист на рівні мобільних платформ. Доступ до даних на мобільних

телефонах і планшетах можна контролювати і захищати. Така універсальність дозволяє компаніям захищати дані як усередині, так і поза корпоративною мережею. Вона забезпечує централізований і комплексний підхід до безпеки та є потужним інструментом захисту конфіденційної інформації в сучасному інформаційному середовищі. Safetica ONE визначається ефективністю захисту даних з використанням новітніх технологій і методів. До числа поширених алгоритмів шифрування, доступних для Safetica ONE, належать:

AES (Advanced Encryption Standard): цей алгоритм шифрування є одним із найпоширеніших і найсильніших, з різними режимами, включно з ECB, CBC і GCM.

RSA (Rivest-Shamir-Adleman): алгоритм, що використовується для асиметричного шифрування, наприклад, шифрування ключів. Забезпечує безпеку під час обміну ключами та захист від несанкціонованого доступу.

SHA (Secure Hash Algorithm): хеш-алгоритми, такі як SHA-256, використовуються для перевірки цілісності даних. Він генерує унікальний хеш-код для набору даних і слугує цифровим підписом, що дає змогу ідентифікувати зміни в даних.

PKI (Public Key Infrastructure): для створення та управління ключами шифрування і підпису в Safetica ONE використовується інфраструктура відкритих ключів. Це забезпечує безпеку обміну ключами та шифрування даних.

Safetica ONE - це новітня і найбільш ефективна технологія захисту конфіденційних даних в інформаційних системах організації. Вона забезпечує комплексний захист даних на всіх рівнях і може бути легко інтегрована в існуючі інформаційні системи. Safetica ONE також дозволяє оцінити ефективність захисту даних за допомогою звітів та аналітичних матеріалів. Майбутні напрямки досліджень за цією темою охоплюють порівняльний аналіз Safetica ONE з іншими продуктами захисту інформації, представленими на ринку, і розробку методів підвищення інформаційної безпеки організацій, що використовують Safetica ONE. Safetica ONE відкриває нові можливості для забезпечення безпеки.

Література:

1. Dulaney, E., & Easttom, C. (2020). "CompTIA Security+ Study Guide: Exam SY0-601
2. Whitman, M., & Mattord, H. (2018). "Management of Information Security."
3. Safetica Technologies (2023). Safetica ONE [Електронний ресурс] – Режим доступу: https://www.safetica.com/ua
4. Safetica ONE 11.0 (2023).[Електронний ресурс] – Режим доступу: https://www.eset.com/ua-ru/about/newsroom/press-releases/products/safetica-one-11-0-novyy-uroven-zashchity-ot-utechki-dannyh
5. Safetica ONE Enterprise-ready DLP and Insider Threat Protection (2023). Електронний ресурс] – Режим доступу: https://www.safetica.com/products-safetica-one
6. Tipton, H., & Krause, M. (2017). "Information Security Management Handbook, Sixth Edition..
7. Yaraghi, N., & Du, A. Y. (2016). The impact of information security breaches on financial performance of firms: An empirical investigation. Journal of Management Information Systems,.
8. Anderson, R. (2008). "Security Engineering: A Guide to Building Dependable Distributed Systems.

9. Andress, J., & Winterfeld, S. (2014). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Syngress.

Осадчий Богдан Ігорович
студент групи УБДМ-61, ННІЗІ ДУІКТ, Київ, Україна

НЕДОЛІКИ ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Встановлено, що біометрична ідентифікація є найстарішим методом ідентифікації особи, оскільки широко використовується в криміналістиці ще з XIX століття, а з іншого - найновішим у сфері інформаційних технологій. Біометрія - це ідентифікація особи за унікальними біологічними характеристиками, притаманними лише їй. Завдяки цьому використання біометричних технологій у забезпеченні інформаційної безпеки є цілком логічним. Однак, поряд із багатьма перевагами біометричні методи мають низку недоліків, серед яких є висока вартість впровадження, вразливість до підробки, складність зберігання даних користувачів та час, який необхідно витрачати під час ідентифікації та обробки даних.

Використання біометричних технологій для ідентифікації осіб стає все більш популярним і розповсюдженим в різних галузях. Однак разом із зростанням цієї популярності з'являються недоліки, пов'язані з використанням біометричних технологій у сфері інформаційної безпеки. Які складнощі та ризики виникають при використанні біометричних технологій?

До недоліків можна віднести, по-перше, те, що впровадження системи біометричної ідентифікації вимагає відносно великих фінансових вкладень; по-друге, те, що деякі біометричні ідентифікатори можуть бути підроблені, наприклад, відбитки пальців, підпис або голос.

Одним із головних недоліків використання біометричних технологій є питання приватності та конфіденційності даних користувачів. Збереження біометричних даних вимагає високого рівня захисту, і в разі порушення безпеки даних можуть виникнути серйозні наслідки.

Важливою умовою зберігання та обробки персональних даних, які використовуються для біометричної ідентифікації, є знеособлення даних. Знеособлення - це процес, який полягає в видаленні або приховуванні індивідуальних ідентифікаторів, що дозволяють ідентифікувати конкретну особу, іншими словами, видаляючи будь-яку можливість зв'язку між біометричними даними та конкретною особою.

На сьогодні існує близько 20-ти біометричних ідентифікаторів, які можна використовувати, в залежності від обраного методу біометричної ідентифікації, зустрічаються різні недоліки.

Ідентифікація за особливостями очей (сітківка і райдужна оболонка) вважаються найнадійнішими серед біометричних. Однак недоліків у систем, що працюють з сітківкою ока більш ніж достатньо. По-перше, це висока вартість сканерів та їхні великі розміри. По-друге, аналіз зображення займає багато часу (не менше хвилини). Третій недолік - неприємність самої процедури сканування.

Справа в тому, що користувач повинен дивитися в певну точку під час цього процесу. Крім того, сканування здійснюється за допомогою інфрачервоного променя, що викликає больові відчуття. І останній недолік використання сітківки ока в біометрії - значне погіршення якості зображення при певних захворюваннях, наприклад, катаракті. Це означає, що люди з ослабленим зором не зможуть скористатися цією технологією. Недоліки ідентифікації за сітківкою призвели до того, що ця технологія погано підходить для використання в системах інформаційної безпеки. Тому вона найчастіше використовується в системах доступу на секретні наукові та військові об'єкти.

Порушення приватності, можливість обману систем, проблеми збереження даних та необхідність збалансованого підходу між безпекою і приватністю є серйозними питаннями, які вимагають уваги та дослідження. Для забезпечення інформаційної безпеки слід ретельно вивчати та вдосконалювати біометричні системи, звертаючи увагу на ці недоліки.

Отже, основними недоліками використання біометричних технологій є висока вартість впровадження, вразливість до підробки, складність зберігання даних користувачів та час, який необхідно витрачати під час ідентифікації та обробки даних.

Перелік посилань:

1. Царьов Р.Ю., Лемеха Т.М. Біометричні технології: навч. посіб. [для вищих навчальних закладів]. Одеса: ОНАЗ ім. О.С. Попова, 2016. 140 с.

2. Недоліки біометричної автентифікації. URL: https://www.eset.com/ua/about/newsroom/blog/data-protection/mogut-li-khakery-pokhitit-vash-otpechatok-paltsa-nedostatki-biometricheskoy-autentifikatsii/ (дата звернення: 25.10.2023).

3. Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. 2-ге вид., доп. Львів: ЛьвДУВС, 2015. 492 с.

Павлюк Артем Вікторович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ Україна

УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ КІНЦЕВИХ ТОЧОК ІНФОРМАЦІЇНОЇ СИСТЕМИ ПІДПРИЄМСТВА

Вразливості кінцевих точок інформаційної системи підприємства — це слабкі місця в комп'ютерних системах, які можуть бути використані зловмисниками. Вони включають в себе слабкі паролі, застаріле програмне забезпечення та недостатню фізичну безпеку. Виявлення та усунення цих вразливостей є важливими для забезпечення безпеки інформаційних систем. Для цього використовуються інструменти, такі як Nessus, а також регулярні сканування, оновлення та навчання персоналу щодо безпеки даних.

Для управління вразливостями кінцевих точок перше що потрібно, це мати інформацію про ці вразливості, де вони знаходяться та який вплив мають на всю систему. З цим нам може допомогти сканер вразливостей такий як Nessus який розроблений і підтримується компанією Tenable. Після проведення сканування ми отримаємо детальний звіт.

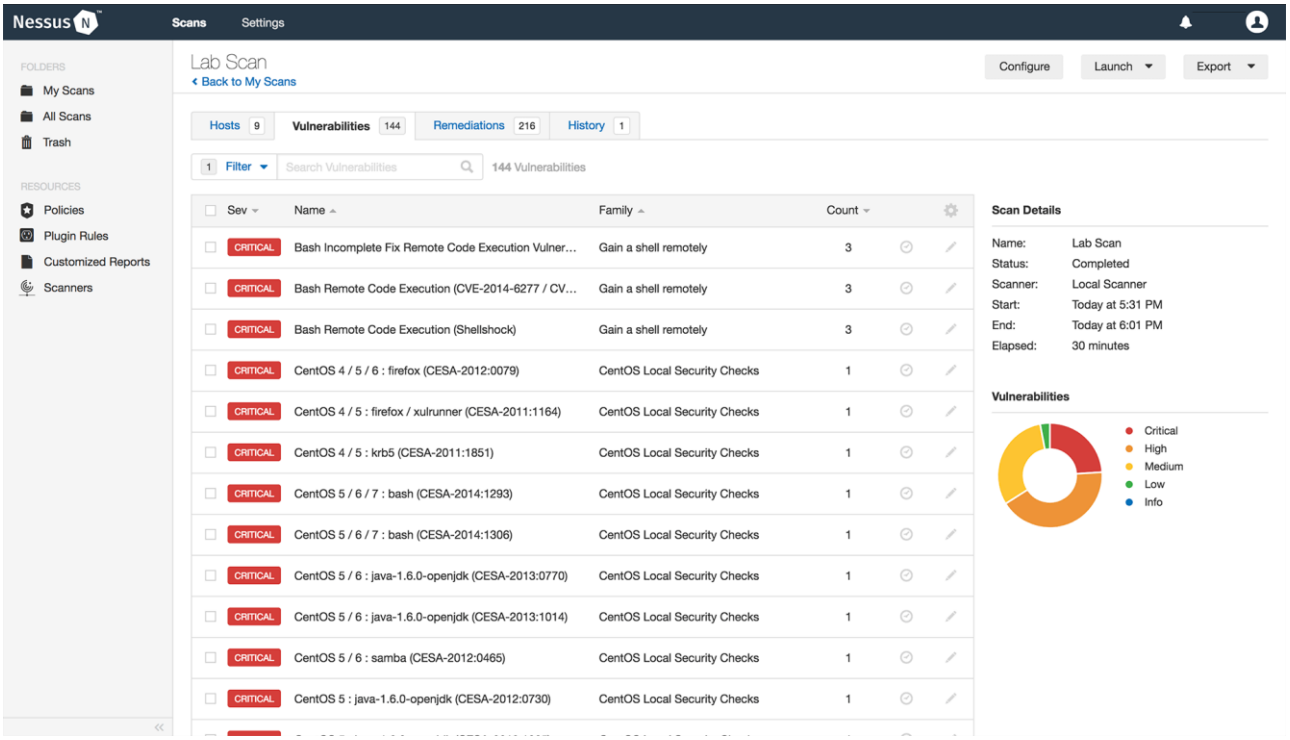


Рис. 1. Звіт сканування вразливостей за допомоги Nessus

Після такого сканування стає зрозуміло які вразливості становлять найбільшу загрозу для нашої інформаційної системи, а також тепер легше створити план подальших дій для вирішення цих загроз. Також за допомогою таких даних створюється чітке уявлення про те які інструменти краще використовувати для вирішення конкретних загроз.

Перелік посилань:

1. Endpoint Protection – багаторівневий підхід до захисту від сучасних загроз URL: https://itbiz.ua/statti-ta-obzori/endpoint-protection-bagatorivnevij-pidxid-do-zaxistu-vid-suchasnix-zagroz/
2. Tenable Nessus URL: https://www.tenable.com/products/nessus/nessus-essentials

Паламарчук Ілля Вікторович
студент групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

СОЦІАЛЬНА ІНЖЕНЕРІЯ В ЦИФРОВОМУ СЕРЕДОВИЩІ: АНАЛІЗ НОВИХ МЕТОДІВ ТА ЇХ ВПЛИВУ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ОРГАНІЗАЦІЇ

Сучасне суспільство стрімко переходить до онлайн-середовища для соціальної взаємодії. Інтернет та соціальні мережі вже стали необхідністю для більшості. Майже кожна людина, пов’язана з комп’ютером, зареєстрована хоча б в одній соціальній мережі, що значно спрощує роботу так званим соціальним інженерам.

У майбутньому, головною загрозою для інформаційної безпеки організацій стануть методи соціальної інженерії, які використовуються для обходу засобів захисту та здійснення інших видів шахрайства. Ця загроза обумовлена тим, що використання соціальної інженерії не вимагає великих фінансових витрат та глибоких знань в галузі інформаційних технологій.

Соціальна інженерія – це метод несанкціонованого доступу до інформації або систем зберігання інформації, який не базується на використанні технічних засобів, а використовує вразливості людського фактору. Наукові дослідження показують, що існують певні психологічні та поведінкові риси, які можуть бути використані соціальними інженерами для маніпулювання людьми. Важливо зазначити, що більшість вторгнень не відбуваються через технічний врив, а саме завдяки використанню методів соціальної інженерії.

Перший етап будь-якої атаки - дослідження. Соціальний інженер повинен дізнатися хто з працівників організації має доступ до інформації, що його цікавить, хто в якому підрозділі працює, де розташовані підрозділи, яке програмне забезпечення встановлено на корпоративних комп'ютерах і т.д.

Найпоширенішими методами атак є:

- отримання, передача або зміна паролів;
- запуск шкідливого ПЗ;
- отримання інформації про способи віддаленого доступу до корпоративної інформаційної мережі;
- створення облікових записів(з правами користувача або адміністратора);
- передача або поширення конфіденційної інформації.
- несанкціоноване надання додаткових прав і можливостей зареєстрованим користувачам системи;

Схема дії соціальної інженерії:

- визначення мети впливу на об'єкт;
- збір інформації про об'єкт;
- виявлення найбільш зручної мішені впливу;
- створення необхідних умов для впливу;
- примус до виконання потрібної дії;
- досягнення потрібного результату.

Найпоширеніші методи соціальної інженерії:

- віртуальні методи(зловмисники використовують електрону пошту, спливаючі вікна, телефоні технології);
- фізичні методи(встановлення особистого контакту з жертвою).

Фізичні методи, як правило, більш ризиковані, але вони надають свої переваги. Віртуальні - простіші, вимагають менше ресурсів, але водночас і менш ефективні. На руку віртуальним методам грає поширення віддаленого типу роботи, у зв'язку з Covid-19 та російсько-українською війною, тому що поширення мобільних технологій, які дають змогу користувачам підключатися до робочої інформаційної мережі вдома або в дорозі, є серйозною загрозою для компанії.

Класичні види шахрайства, основою яких є соціальна інженерія

Фішинг - процес відправки електронних листів, які начебто надходять від достовірного джерела, з метою отримання конфіденційної інформації адресата.

Фармінг - встановлення на комп'ютери користувачів шкідливих програм, які після запуску збирають конфіденційну інформацію.

Вішинг(від слів фішинг та voice(голос)**)** - процес отримання інформації за допомогою телефону. Зловмисники використовують *phone spoofin*g, тобто підміну телефонного номера.

Уособлення - вид шахрайства, у якому соціальний хакер виступає в ролі іншої людини.

Зворотна соціальна інженерія - вид шахрайства, коли соціоінженер своїми діями змушує жертву звернутися до нього за “допомогою”.

Еволюція шахрайства, основою яких є соціальна інженерія

2022 рік став роком приходу штучного інтелекту в побут звичайного користувача інтернет-технологіями. 2023 рік тільки зберіг цю тенденцію і тепер ми використовуємо потужності нейромереж та штучного інтелекту для багатьох завдань: генерація текстів, зображень, відео, програмного коду і т.д. Еволюція технологій не пройшла повз і зловмисників. Буде не правильно сказати, що технічний процес приніс щось нове в кібератаки, проте штучний інтелект дозволяє прискорювати, масштабувати та економити ресурси, в тому числі й людські.

Використання штучного інтелекту для шахрайств, основою яких є соціальна інженерія

Підробка/клонування голосу. Такий вид шахрайства був і раніше, проте вимагав чималих ресурсів та зусиль. Як мінімум, вам потрібні були кілька годин запису голосу певної людини для навчання голосової моделі. Нові моделі штучного інтелекту дозволяють клонувати голос людини в реальному часі, маючи лише 5 секунд промови.

Deepfake(підробка відео). Використання штучного інтелекту для створення Deepfake-відео може слугувати дуже потужним методом шахрайства. Таким чином можна створити відео, у якому будь-яка людина органічно говорить те, що потрібно зловмиснику, в тому числі й може наказувати своїм підлеглим розказати конфіденційну інформацію, або надати доступ до системи.

Автоматизовані боти для соціальної інженерії на основі штучного інтелекту. Чат-бот - це заснована на правилах комп'ютерна програма, яка імітує людську взаємодію з кінцевими користувачами через інтерфейс чату. Іншими словами, чат-бот може розмовляти з вами як жива людина, ставити запитання та відповідати на них відповідно до заздалегідь визначених правил і логіки. Кіберзлочинці використовують шкідливих ботів, щоб отримати контроль над одним комп'ютером і з'єднати його з іншим, щоб створити мережу до іншого, щоб створити мережу "комп'ютерів-зомбі", відому як ботнети, які потім можуть запускати масштабні кібератаки, що призводять до повного відключення користувачів від Інтернету.

Вплив нових методів шахрайства на інформаційну безпеку організації

Використання штучного інтелекту для шахрайства на основі соціальної інженерії значно спрощує та прискорює отримання зловмисниками конфіденційної інформації або грошових ресурсів. Вже є успішні кейси проведення кібер-атак з використанням штучного інтелекту та отримання значних сум грошей. На жаль, не існує абсолютно надійних методів захисту,

інформаційна безпека стає надзвичайно важливою, і організаціям необхідно бути постійно пильними та вдосконалювати свої заходи зі збереження інформаційної цілісності та захисту від кіберзагроз.

Висновок

Отже, соціальна інженерія та її розвиток в сучасному суспільстві створюють серйозні виклики для інформаційної безпеки організацій.

З використанням штучного інтелекту, зловмисники отримують нові можливості для шахрайства, які ще спрощують та прискорюють процес злому.

У такому контексті організаціям необхідно постійно вдосконалювати свої заходи зі збереження інформаційної цілісності та захисту від кіберзагроз. Це включає в себе навчання та підвищення свідомості персоналу, впровадження новітніх технологій захисту, та регулярне оновлення політик безпеки. Тільки завдяки цим заходам можна впоратися з різноманітними видами атак та зберегти інформаційну безпеку організації на високому рівні.

Перелік посилань:

1. Діденко К.О - Соціальна інженерія в системі інформаційної безпеки [с.2-3] Режим доступу: https://rmv.nmu.org.ua/ua/arkhiv-zbirok-konferentsiy/molod-nauka-ta-innovatsii-2017/%D0%A2%D0%BE%D0%BC%2012.PDF
2. AI: a boon for social engineering URL: https://incyber.org/en/ai-a-boon-for-social-engineering/
3. Sowjanya Manyam - AI'S IMPACT ON SOCIAL ENGINEERING ATTACKS [с.14-21] Режим доступу: https://opus.govst.edu/cgi/viewcontent.cgi?article=1521&context=capstones

Панарін Валерій Ігорович
студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СФЕРІ КІБЕРБЕЗПЕКИ ТА ВИКЛИКИ ПОВ'ЯЗАНІ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ ЗЛОВМИСНИКАМИ

В сучасному світі використання штучного інтелекту (ШІ) та машинного навчання стає розповсюдженою практикою у всіх сферах, починаючи зі сфери кібербезпеки і закінчуючи медіа та соціальними мережами. ШІ дозволяє вирішувати задачі, які було би важко вирішити з використанням інших наявних в наш час підходів. В тому числі ШІ почав активно застосовуватися зловмисниками. Нижче розглянуто основні задачі в сфері кібербезпеки, що вирішуються за допомогою ШІ, їх недоліки та вразливості, а також основні способи використання ШІ зловмисниками.

Штучний інтелект і машинне навчання внесли значний вклад у підвищення рівня кібербезпеки, допомагаючи спеціалістам з кібербезпеки виявляти справжні кіберзагрози серед величезної кількості даних про підозрілі дії, оскільки традиційне програмне забезпечення не справляється із швидким зростанням кількості зловмисного ПЗ. Системи на основі ШІ здатні аналізувати поведінку і виявляти шкідливі програми і вимагачі на ранніх етапах. Вони використовують складні алгоритми для прогнозування та виявлення аномалій, кібератак і стратегій запобігання, оскільки кіберзлочинці постійно оновлюють свої методи атаки.Для атак зловмисники використовують фішинг та методи

соціальної інженерії, які змушують співробітників натискати на заражені посилання. Їх надсилають електронною поштою або у повідомленнях месенджерів.

ШІ допомагає кібербезпековим системам отримувати актуальні знання про загрози для прийняття обґрунтованих рішень із захисту систем. ШІ допомагає у створенні точного і детального переліку ІТ-активів, включаючи пристрої, користувачів і програми з різними доступами. Враховуючи цю інвентаризацію та потенційні загрози, системи на базі ШІ можуть прогнозувати потенційні місця порушень безпеки, допомагаючи планувати і виділяти ресурси ефективніше.

Також ШІ широко використовується у боротьбі з ботами, оскільки вони становлять значну частку інтернет-трафіку і можуть викликати різні загрози, від крадіжки облікових даних чи реєстрації фальшивих акаунтів до шахрайства з даними. ШІ аналізує великі обсяги даних, розрізняючи різні типи ботів та адаптуючи стратегії кібербезпеки. Це дозволяє компаніям визначити типи трафіку на їхніх веб-сайтах і випереджати зловмисних ботів.

Але завдяки широкій доступності хмарних обчислень для швидкого розгортання та використання потужних моделей ШІ зловмисники також адаптувалися до нових технологій і використовують ШІ та машинне навчання для розробки більш складних та ефективних методів атаки.

Один з найпростіших способів використання ШІ зловмисниками - це моделювання інфраструктури для тестування свого програмного забезпечення для кібератак, вивчаючи, які події і шаблони поведінки шукають системи безпеки. Вони можуть використовувати своє забезпечення для створення профілю атаки, який можна виявити за допомогою моделей машинного навчання. Зловмисники активно намагаються відтворити існуючі моделі штучного інтелекту, які використовуються провайдерами кібербезпеки та операційними групами, щоб вивчити те, як саме системи безпеки на основі ШІ виявляють атаки. Завдяки цьому зловмисники постійно змінюють свої методи, залишаючись на крок попереду відносно інструментів, які покладаються на ШІ.

Також ще однією великою вразливістю інструментів на основі ШІ є сам процес навчання моделі. Оскільки системи штучного інтелекту та машинного навчання вимагають великих обсягів складних даних, існує багато способів пошкодити модель ще на етапі її навчання. Отримавши доступ до даних, на яких навчається модель зловмисники можуть впливати на неї, вводячи безпечні файли, схожі на зловмисне програмне забезпечення, або створюючи шаблони поведінки, які виявляються помилковими. Таким чином можливо змусити моделі ШІ повірити, що поведінка атак не є зловмисною. Це дозволяє хакерам повністю уникнути відомих моделей, делікатно змінюючи дані, щоб уникнути виявлення на основі розпізнаних шаблонів.

Більш важливою проблемою є те, атака на моделі, що навчаються, може нести пряму безпеку життю людей. Серед найбільш вразливих сфер на поточний момент можна назвати військову сферу, промисловість, що використовує роботів, а також автомобілебудування. Атака на ці сфери можуть бути більш комплексними і включати фізичну взаємодію з елементами реального світу та

розробку методів обману ШІ. Як приклад можна привести той факт, що наклейки, розміщені на дорожніх знаках змусили Tesla Model S розпізнати знак «Stop» як знак «Added Lane», а знаки обмеження швидкості “35” сприймати як “85“. Подібний вплив на моделі ШІ може призводити до небезпечних для життя ситуацій під час руху автомобілів.

Окрім реального світу у більшості випадків алгоритми машинного навчання можна змусити працювати не правильно, маніпулюючи базовими пікселями зображення. Ці зміни непомітні для людини, але вони збивають алгоритм. На рисунку 1 показано, як ці методи можуть змусити ШІ побачити гелікоптер на фотографії з чотирма автоматами.

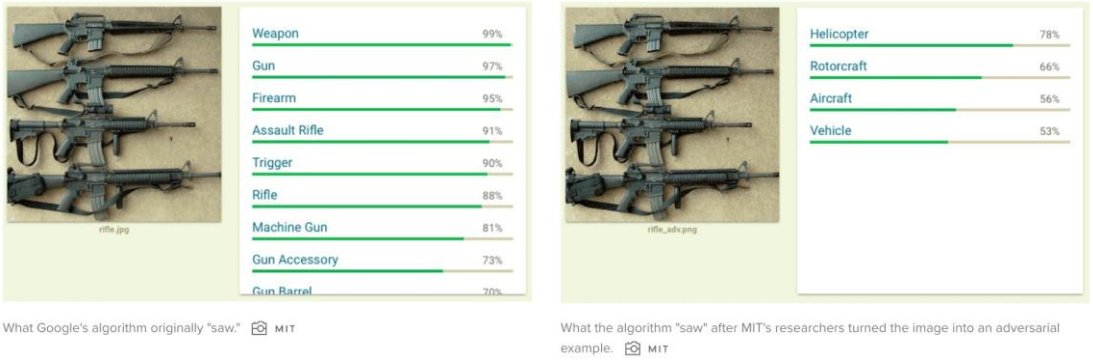


Рис.1. Результати розпізнавання ШІ зображення до та після маніпуляцій з базовими пікселями зображення.

На поточний момент немає однозначно надійних способів захисту від як атак на власний ШІ, так і від атак з використанням ШІ зловмисників. Тому зараз активно розвиваються підходи до захисту від подібного роду атак. Серед прикладів можна навести навести “TrojAI Software Framework”, що являє з себе набір інструментів для генерування “отруєних” що є на меті створення системи класифікації таких даних.

Компанії, які застосовують машинне навчання в своїх продуктах, потребують рішення для захисту як великих даних, так і моделей даних, щоб захистити свої проекти ШІ. І платформи, такі як CloudFlare вже покращують свої рішення для покращення ізоляції даних у хмарі, надають інструменти для захисту від шкідливих ботів тощо.

Перелік посилань:

1. How hackers use AI and machine learning to target enterprises: https://www.techtarget.com/searchsecurity/tip/How-hackers-use-AI-and-machine-learning-to-target-enterprises(дата звернення: 23.10.2023).

2. The Use of Artificial Intelligence in Cybersecurity: A Review: https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity

3. How to Hack AI? Machine Learning Vulnerabilities That Nobody Talks About: https://broutonlab.com/blog/how-to-hack-ai-machine-learning-vulnerabilities

4. A Strong Baseline for Natural Language Attack on Text Classification and Entailment: https://arxiv.org/pdf/1907.11932.pdf

5. Protecting data from AI, pros and cons of AI-enhanced development https://www.cloudflare.com/en-gb/the-net/data-protection-ai

Парфенюк Тетяна Миколаївна
студентка групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ОСНОВНІ ПРИКЛАДИ ВИКОРИСТАННЯ СИСТЕМ DLP ДЛЯ ЗАХИСТУ ДАНИХ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Системи запобігання втраті даних (DLP) - це набір інструментів і процесів, які використовуються для того, щоб запобігти втраті, неправильному використанню або доступу до конфіденційних даних несанкціонованими користувачами.

DLP (Data Loss Prevention) системи створені для запобігання витоку чутливої інформації за межі корпоративних мереж.

Існує декілька причин, через які організації віддають перевагу впровадженню DLP систем:

Захист чутливої інформації: Багато компаній зберігають конфіденційну інформацію, таку як дані про клієнтів, фінансові дані, інтелектуальну власність тощо. Втрата або несанкціонований доступ до такої інформації може призвести до фінансових втрат, штрафів або правових проблем.

Відповідність законодавству: Багато країн вимагають захист особистої інформації громадян. Наприклад, GDPR в Європейському Союзі встановлює строгі вимоги до обробки та захисту особистих даних.

Захист бренду та репутації: Витік інформації може пошкодити репутацію компанії, втратити довіру клієнтів і партнерів.

Внутрішні загрози: Не завжди витоки даних відбуваються через зовнішні атаки. Іноді витоки можуть відбутися через недбалість або навмисне використання даних співробітниками.

Підтримка бізнес-процесів: DLP системи можуть також допомогти у визначенні та контролі того, як ділова інформація використовується в межах організації, допомагаючи оптимізувати бізнес-процеси.

Віддалена робота: З ростом популярності віддаленої роботи і використанням особистих пристроїв для службових цілей (BYOD), зростає ризик витоку даних. DLP системи допомагають контролювати передачу даних на таких пристроїв.

Інтеграція з іншими безпековими рішеннями: DLP може працювати в поєднанні з іншими системами безпеки для забезпечення голістичного підходу до захисту інформації.

Нижче наведено три основні приклади використання DLP систем:

Захист особистих даних: Запобігання розсиланню чутливої особистої інформації, такої як номери соціального страхування, банківські реквізити або медична інформація.

Інтелектуальна власність: Виявлення та блокування спроб передачі конфіденційних документів, проектів, патентів або іншої інтелектуальної власності.

Керування електронною поштою: Моніторинг та контроль електронних повідомлень, що містять чутливу інформацію, та запобігання її передачі.

Безпека веб-трафіку: Аналіз та блокування спроб передачі чутливої інформації через веб-сайти або інші веб-сервіси.

Управління пристроями зберігання: Обмеження або блокування передачі даних на зовнішні пристрої, такі як USB-накопичувачі.

Захист від внутрішніх загроз: Виявлення аномальних дій співробітників, які можуть вказувати на витік чутливої інформації.

Шифрування: Автоматичне шифрування чутливої інформації при спробах її передачі або зберігання поза безпечним середовищем.

Ідентифікація та класифікація даних: Автоматичне виявлення та міткування документів на основі їх вмісту, щоб визначити, які з них містять чутливу інформацію.

Запобігання загрозам інсайдерів: Виявлення спроб співробітників передати чутливу інформацію третім особам або конкуруючим компаніям.

Дотримання стандартів та регуляторів: Перевірка відповідності ділових процесів вимогам законодавства, стандартів або галузевих регулятив.

Перелік посилань:

1. What is Data Loss Prevention (DLP)? Definition, Types & Tips URL: https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/
2. Data Loss Prevention (DLP) URL: https://www.digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

Пашалик Яна Юріївна, БСДМ-61
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ АНАЛІТИЧНИМИ ДАНИМИ ЩОДО НОВІТНІХ ЗАГРОЗ НА БАЗІ IBM QRADAR THREAT INTELLIGENCE

Визначено мету і основні завдання із забезпечення аналітичними даними щодо новітніх загроз. Розглянуто технологію щодо забезпечення аналітичними даними щодо новітніх загроз на базі IBM QRadar Threat Intelligence.

За даними групи IBM X-Force [1] після вторгнення росії в Україну російські державні кібератаки не призвели до широкомасштабних і потужних атак, яких спочатку побоювалися західні урядові структури. Однак росія розгорнула безпрецедентну кількість засобів для знищення об'єктів в Україні, що свідчить про її постійні інвестиції у створення деструктивного шкідливого програмного забезпечення.

Аналітичні дані щодо новітніх загроз відіграють важливу роль у забезпеченні кібербезпеки інформаційних систем організацій. Забезпечення аналітичними даними щодо новітніх загроз (Threat Intelligence) передбачає збір,

аналіз та інтерпретацію інформації про потенційні та реальні загрози для інформаційних систем організації. Аналітичні дані щодо новітніх загроз можуть бути використані для проактивного виявлення та пом'якшення загроз до того, як вони зможуть завдати шкоди.

Забезпечення аналітичними даними щодо новітніх загроз необхідне на таких етапах діяльності фахівців з кібербезпеки:

виявлення потенційних і реальних загроз інформаційним системам організації;

реагування на потенційні та реальні загрози інформаційним системам організації. Знання аналітичних даних щодо новітніх загроз допомагає виявляти і локалізувати загрози, а також пом'якшити наслідки будь-яких успішних атак;

запобігання потенційним загрозам інформаційним системам організації. Знання аналітичних даних щодо новітніх загроз допомагає організаціям впровадити проактивні заходи для зменшення ймовірності успішних атак, такі як виправлення вразливостей і поліпшення контролю доступу.

У [3] зазначається, що виявлення зловмисних дій та інших слідів зловмисників є надзвичайно складним завданням у сучасному складному середовищі, особливо зважаючи на те, що зловмисник може легко виглядати як легітимний користувач.

Забезпечення аналітичними даними щодо новітніх загроз (розвідка кіберзагроз) – це цінний спосіб розширити можливості SOC ідентифікувати зловмисників і відрізняти їхні дії від дій авторизованих користувачів. Це переносить SOC від підходу, орієнтованого на окремі інциденти, до парадигми, орієнтованої на противника.

У [2] зазначається, що забезпечення аналітичними даними щодо новітніх загроз фахівців організації (Threat Intelligence) ґрунтується на аналітичних методах, відточених протягом кількох десятиліть урядовими та військовими відомствами.

Традиційна розвідка фокусується на шести окремих фазах, які складають так званий "розвідувальний цикл" (рис. 1) [2]: Спрямування; Збір; Обробка; Аналіз; Поширення; Зворотний зв'язок.

Інструменти необхідні для автоматизації етапів збору, обробки та поширення розвідувальної інформації, а також для підтримки і прискорення аналізу. Без належних інструментів аналітики витрачатимуть весь свій час на механічні аспекти цих завдань і ніколи не матимуть часу на справжній аналіз.

Більшість зрілих груп з розвідки загроз використовують два типи інструментів [4]:

рішення для розвідки загроз, призначені для збору, обробки та аналізу всіх типів даних про загрози з внутрішніх, технічних і людських джерел;

існуючі інструменти безпеки, такі як SIEM та інструменти аналітики безпеки, які збирають і корелюють події безпеки та дані журналів.

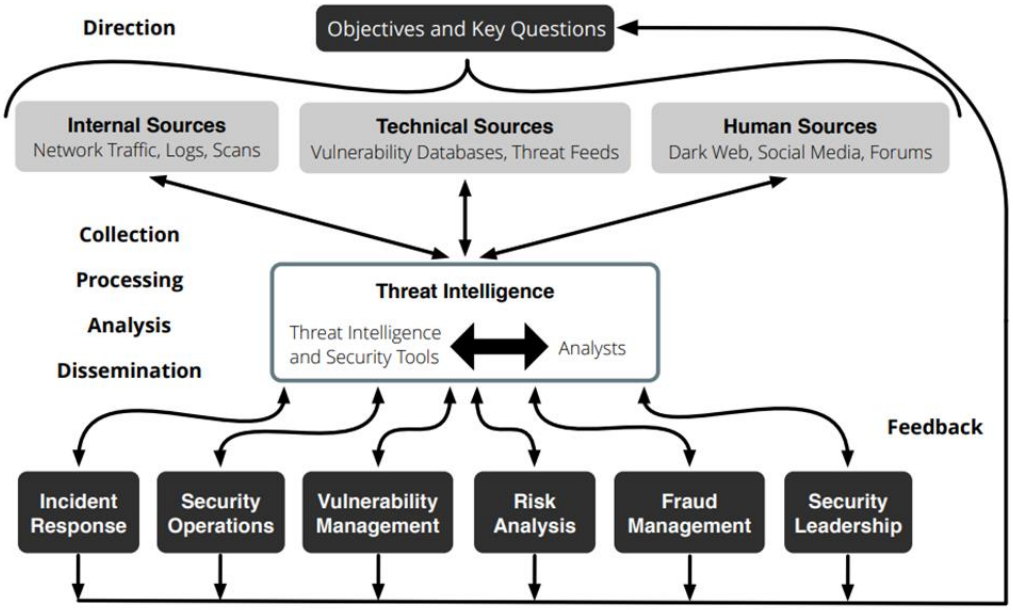


Рис. 1. Схема процесів Threat Intelligence [2]

Щоб захистити себе найбільш ефективно, організаціям потрібен доступ до набагато ширшого спектру даних про загрози, ніж будь-коли раніше. Додавання X-Force Threat Intelligence до платформи QRadar Security Intelligence Platform може забезпечити додаткову інформацію, необхідну для боротьби з цими сучасними загрозами [4].

X-Force Threat Intelligence – це набагато більше, ніж просто компіляція даних про загрози. За цим стоїть потужність команди дослідників і розробників IBM X-Force – однієї з найвідоміших комерційних дослідницьких груп у сфері безпеки в світі. Ця команда експертів з безпеки забезпечує основу для превентивного підходу IBM до безпеки в Інтернеті, зосереджуючи свою увагу на дослідженні та оцінці вразливостей і проблем безпеки, розробці оцінок і технологій протидії для продуктів IBM, а також навчанні користувачів про нові загрози і тенденції в Інтернеті.

Використання X-Force Threat Intelligence з QRadar надає цінні можливості, що виходять за рамки стандартного каналу розвідданих QRadar (рис. 2), такі як часті оновлення, внутрішня аналітика, рейтинг довіри і всебічне покриття.

Дані про репутацію X-Force IP постійно оновлюються і підтримуються, а контент в цих стрічках отримує відносну оцінку загрози. Це дозволяє користувачам QRadar визначати пріоритетність інцидентів і правопорушень, спричинених цим контентом. Дані з цих джерел розвідки автоматично включаються в функції кореляції і аналізу QRadar і служать для значного збагачення його можливостей виявлення загроз найсвіжішими даними про загрози в Інтернеті. Будь-яка подія безпеки або дані про мережеву активність, пов'язані з цими адресами, автоматично позначаються, додаючи цінний контекст до аналізу та розслідування інцидентів безпеки.

Користувачі також можуть включити в інформаційну панель QRadar останні повідомлення про загрози безпеки X-Force і інформаційні оновлення. Ця

інформаційна панель включає поточний рівень X-Force AlertCon, який надає користувачам швидкий і стислий індикатор поточного стану загроз в Інтернеті. Використання X-Force Threat Intelligence з QRadar Security Intelligence Platform є простим і швидким – як тільки користувачі додадуть ці дані про загрози, вони відразу ж почнуть отримувати розширені дані про загрози автоматично і безперебійно.

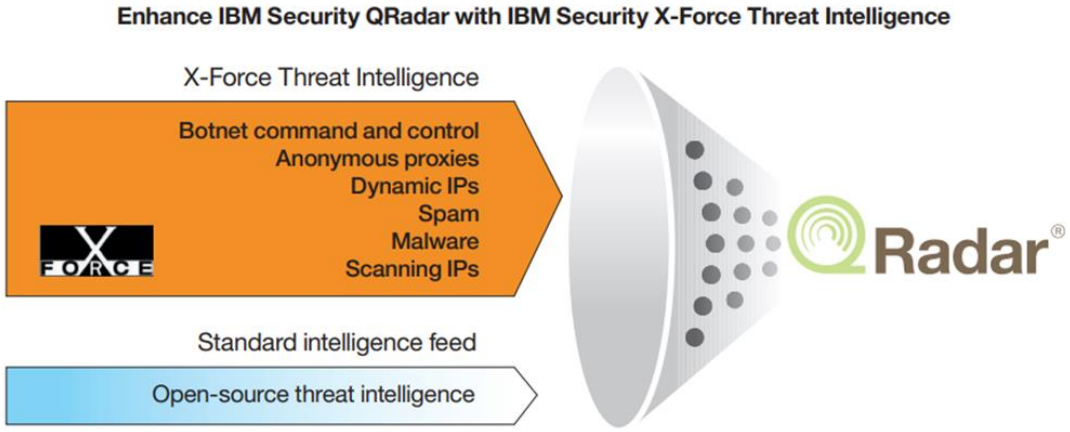


Рис. 2. Вдосконалення IBM QRadar за допомогою IBM X-Force Threat Intelligence [4]

Додавши динамічну інформацію з X-Force Threat Intelligence до аналітичних можливостей QRadar Security Intelligence Platform, користувачі можуть отримати більш інтелектуальне і точне забезпечення безпеки. Ця додаткова інформація від X-Force Threat Intelligence дозволяє користувачам QRadar застосовувати ці цінні дані в режимі реального часу для більш ретельного моніторингу і надійного захисту свого середовища.

IBM QRadar Threat Intelligence залучає канали аналізу загроз за допомогою відкритих стандартних форматів STIX і TAXII і розгортає дані для створення спеціальних правил для кореляції, пошуку та звітування. Наприклад, можна використовувати додаток, щоб імпортувати загальнодоступні колекції небезпечних IP-адрес із IBM X-Force Exchange і створити правило для збільшення масштабів будь-якого порушення, яке включає IP-адреси з цього списку спостереження [5].

Отже, забезпечення аналітичними даними щодо новітніх загроз є важливим компонентом стратегії кібербезпеки будь-якої організації. Це надає критично важливу інформацію про потенційні та реальні загрози, що дозволяє організаціям виявляти, реагувати та запобігати атакам на власні інформаційні системи.

Перелік посилань:

1. X-Force Threat Intelligence Index 2023. IBM Security. [online], https://www.ibm.com/downloads/cas/DB4GL8YM (Accessed September 29, 2023)

2. The Threat Intelligence Handbook. A Practical Guide for Security Teams to Unlocking the Power of Intelligence. Edited by Chris Pace. 2018, CyberEdge Group, LLC. – 108 p.

)

3. Kathryn Knerler, Ingrid Parker, Carson Zimmerman. 11 Strategies of a World-Class Cybersecurity

Operations Center. The MITRE Corporation, 2022. – 452 p. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjwnKK97fv9AhXPvIsKHbVlB6AQFnoECAoQAQ&url=https%3A%2F%2Fwww.mitre.org%2Fsites%2Fdefault%2Ffiles%2F2022-04%2F11-strategies-of-a-world-class-cybersecurity-operations-center.pdf&usg=AOvVaw14oA34nNabWa6aN-Yq-xsx

4. IBM Security X-Force Threat Intelligence. Use dynamic IBM X-Force data with IBM Security QRadar to detect the latest Internet threats. Available online: https://www.infopoint-security.de/medien/wgd03025usen.pdf

5. QRadar Threat Intelligence app. Last Updated: 2023-03-14. Available online: https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-threat-intelligence-app

Петрівний Дмитро Олександрович
Дежавний університет інформаційно-комунікаційних технологій

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Анотація

Актуальні проблеми кібербезпеки визначають сучасні кіберзагрози та викликають необхідність постійного вдосконалення заходів захисту в цифровому просторі.

Розгалуження технологій та стрімкий розвиток цифрового середовища вносять нові завдання в галузь кібербезпеки. Динамічний образ загроз вимагає постійного оновлення технічних та стратегічних підходів до захисту інформації. Важливою проблемою є нестабільність кіберзагроз та швидкість їх еволюції, що вимагає адаптивності та оперативності у впровадженні заходів безпеки.

Збільшення кількості пристроїв Інтернету речей (IoT) та їх взаємодія висуває нові завдання в області кібербезпеки. Вразливості IoT можуть служити вхідними точками для атак на системи та мережі, вимагаючи розробки надійних методів захисту для забезпечення цілісності та безпеки даних.

Слід підкреслити необхідність уваги до комплексності та багатоплановості вирішення проблем кібербезпеки у сучасному світі, а також важливість постійного вдосконалення стратегій та технічних рішень для забезпечення безпеки в цифровому середовищі.

Актуальні проблеми кібербезпеки в Україні

Результати війни в кіберпросторі є визначальними для загального розвитку бойових дій у сучасних протистояннях. Кібернапад та кібервторгнення можуть завдати величезних збитків або спричинити значні руйнування критичної інформаційної інфраструктури на будь-якому рівні. Це стосується насамперед кібератак на об’єкти енергетичної, транспортної та військової інфраструктури, під час яких виводяться з ладу об’єкти управління постачанням, керування логістикою тощо.

Спостерігалися також атаки на сайти державних установ та органів центральної влади, в результаті чого зловмисники розміщували на них провокаційні оголошення або виводили їх з ладу за допомогою так званих DDoS-атак.

Основні засоби кібернападу пов’язані з використанням шкідливого коду та спробами вторгнення за допомогою вразливостей систем. Шкідливий код найчастіше потрапляє в систему внаслідок порушення користувачами кібергігієни — перехід на небезпечні сайти, відкриття вкладень у підозрілих листах з електронної пошти, а тому ступінь успішності вторгнення визначається якістю системи захисту.

Також слід відзначити такі методи кібернападу як:

Ransomware-атаки: Зловмисники використовують розшифровку даних як засіб вимагання викупу. Ці атаки можуть впливати на різні сфери, включаючи бізнес, організації та державні структури.

Атаки на постачальницький ланцюг: Зловмисники намагаються компрометувати системи через слабкість в постачальному ланцюзі. Це може призвести до серйозних проблем у безпеці інформації та виробничому процесі.

Zero-Day Вразливості: Зловмисники активно використовують невідомі вразливості в програмному забезпеченні, відомі як "zero-day" для виконання атак до того, як виробник випускає виправлення.

Загрози Інтернету речей (IoT): Збільшення кількості підключених пристроїв вносить нові можливості для кіберзлочинців. Недостатня безпека в інтернеті речей може призвести до атак на особисті дані та використання пристроїв для великомасштабних атак.

Важливо відзначити, що кіберзагрози постійно змінюються, і нові виклики можуть з'являтися з часом. Організації та кібербезпекові експерти повинні залишатися високоактивними та готовими адаптуватися до нових трендів у кібербезпеці.

Сучасні системи виявлення вторгнень

Сучасні системи виявлення вторгнень забезпечують істотне поліпшення функцій захисту порівняно з попередніми засобами кібербезпеки, такими як мережевий екран, віртуальна приватна мережа та шифрування сповіщень. Такі системи виконують дві головних функції. По-перше, система виявляє небажану поведінку у вигляді аномалії, навіть якщо це може не бути справжнім вторгненням (хибне виявлення). По-друге, система збирає дані, аналізує дії в мережевих протоколах та порівнює їх з так званими сигнатурами, що містять дані про можливі атаки.

Сигнатури відомих атак існують у базі даних системи виявлення в різних специфікаціях, наприклад у формі правил над параметрами протоколу у вигляді if-then-else. Якщо правило, яке міститься в базі даних сигнатур і кваліфікується як певний вид вторгнення, виконується для параметрів протоколу, то спрацьовує сигнал тривоги.

Є певні труднощі з виявленням вторгнень, що проявляються впродовж деякого проміжку часу і містять ознаки вторгнення в різних пакетах трафіку протоколу. Для подолання цих ускладнень деякі системи використовують представлення сигнатур скінченних автоматів.

Вважається, що порівняння з сигнатурами для таких систем виявлення вторгнень є досить дієвим методом, який дає непогані результати у виявленні вже відомих атак, але в разі атак нульового дня, тобто невідомих раніше, вони безсилі.

Системи на основі виявлення аномалій можуть зафіксувати такі невідомі раніше вторгнення, як відхилення від нормальної поведінки мережевої активності. Серед цих систем виділяють кілька різновидів.

Системи виявлення на основі статистики створюють модель розподілу

подій для нормальної поведінки, потім виявляють події з низькою ймовірністю та позначають їх як потенційні вторгнення.

Системи, засновані на знаннях, використовують факти про нормальну діяльність мережевого протоколу і будь-яке відхилення класифікують як вторгнення. Недоліком цього методу є те, що зібрати всі факти про нормальну роботу системи дуже складно, навіть з використанням формалізації роботи протоколу за допомогою формальних конструкцій.

Більш сучасні системи на основі виявлення аномалій найчастіше використовують машинне навчання. Вони демонструють кращу точність як на відомих атаках, так і на вторгненнях нульового дня. Крім того, такі системи в разі тренування їх на правильних даних можуть класифікувати відомі атаки, хоча при цьому виникають інші проблеми.

Машинне навчання — це процес отримання знань з великої кількості даних з метою розпізнавання чи прогнозування поведінки. Знання формуються у вигляді моделі класифікації, що забезпечується певним алгоритмом генерації. Для побудови моделей класифікації поведінки мережі використовують алгоритми кластеризації, генерації нейронних мереж, генетичні алгоритми, дерева рішень та метод k-найближчих сусідів. На сьогодні нейронні мережі є основною моделлю в системах виявлення вторгнень.

Висновок

Використання методів штучного інтелекту, таких як машинне навчання та алгебраїчні дедуктивні методи, є більш ефективним у вирішенні проблем кібербезпеки, ніж інженерні рішення, які ґрунтуються на вірусних і конкретних поведінкових сигнатурах та карантинних «пісочницях».

Джерела:
1. doi: https://doi.org/10.15407/visn2023.02.012

Петрова Олександра Сергіївна
Студентка групи БСД-12, ННІЗІ, Київ, Україна

DEEPFAKE TECHNOLOGY IN CYBERSECURITY

In recent years, the emergence of Deepfake technology has presented a paradigm shift in the landscape of digital manipulation. Deepfakes, powered by advanced machine learning algorithms, have the capability to generate highly convincing synthetic media, blurring the lines between reality and fiction. This technology, initially developed for entertainment purposes, has found its way into more sinister applications, raising significant concerns within the realm of cybersecurity.

1. **DeepFake technology poses a threat to trust and authenticity in the digital world.** The ability to create realistic video and audio manipulations can lead to situations where it's challenging to determine the veracity of information.

2. **The application of DeepFake can have serious implications for political and societal processes.** Manipulating images and videos can influence elections, public opinion, and civic engagement.

3. **Cybercriminals may use DeepFake for fraud and extortion.** This can include demanding ransom, forging electronic identities for access to confidential data, and more.

4. **Companies and organizations must pay special attention to detecting and preventing DeepFake.** Developing and implementing algorithms for detecting fake videos and audio is a crucial step in ensuring cybersecurity.

5. **The ethical considerations related to the use of DeepFake require careful consideration.** This encompasses questions of privacy, responsibility, and the morality of using the technology to create falsified materials.

6. **Potential Exploitation of DeepFake Technology in the Ukraine-Russia Conflic**t. Introduction of Advanced Disinformation Tactics.The Ukraine-Russia conflict could witness the introduction of DeepFake technology as a means to disseminate highly convincing and manipulated visual and audio content. This has the potential to exacerbate existing disinformation campaigns and further complicate efforts to discern factual information from fabricated content.

7. **Implications of DeepFake Utilization in the Ukraine-Russia Conflict.** Eroding Trust and Escalating Tensions. The application of DeepFake in the Ukraine-Russia conflict has the potential to erode trust between involved parties and escalate existing tensions. DeepFake-generated content may be used to manipulate public opinion, sway international narratives, and provoke reactions, thereby intensifying the complexity of the conflict and hindering diplomatic resolution efforts.

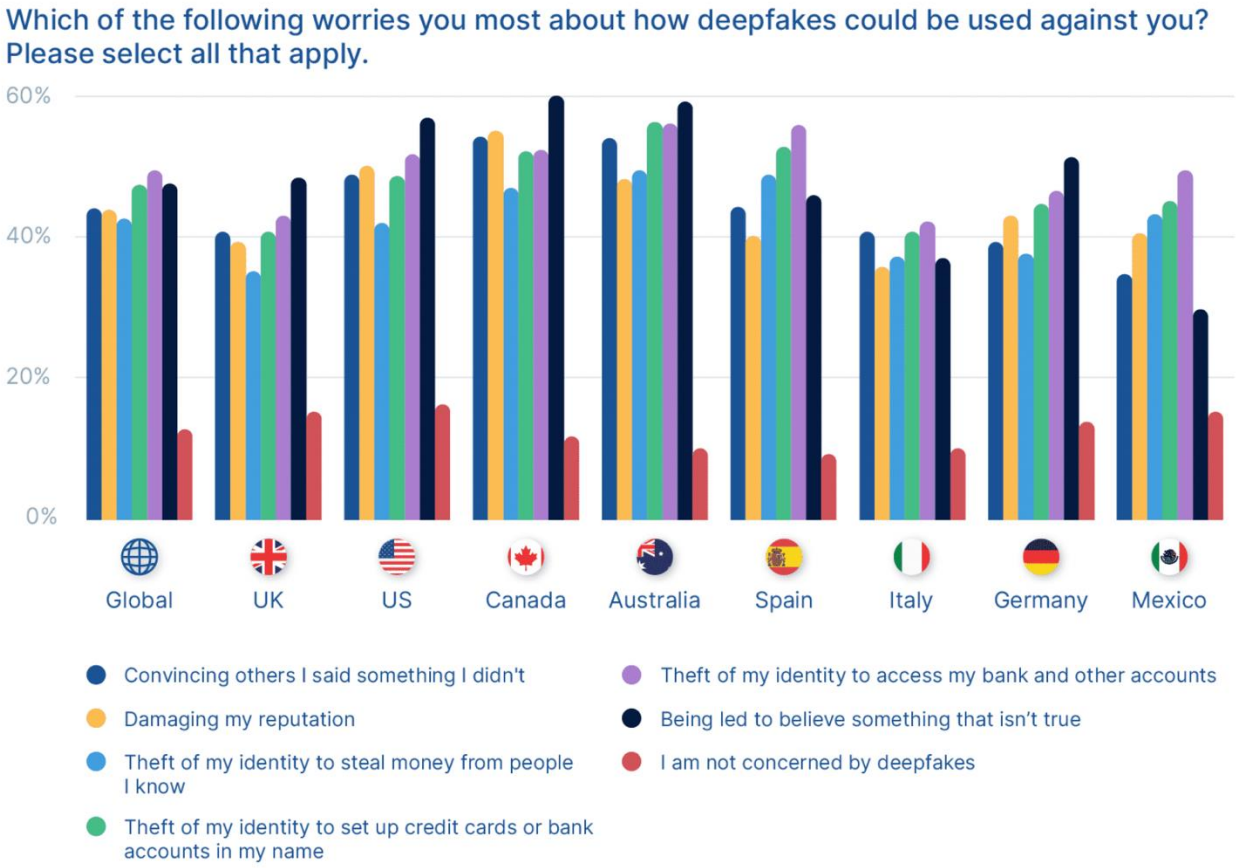


Diagram 1. The respondents' concern about the damage that deepfake technologies can bring

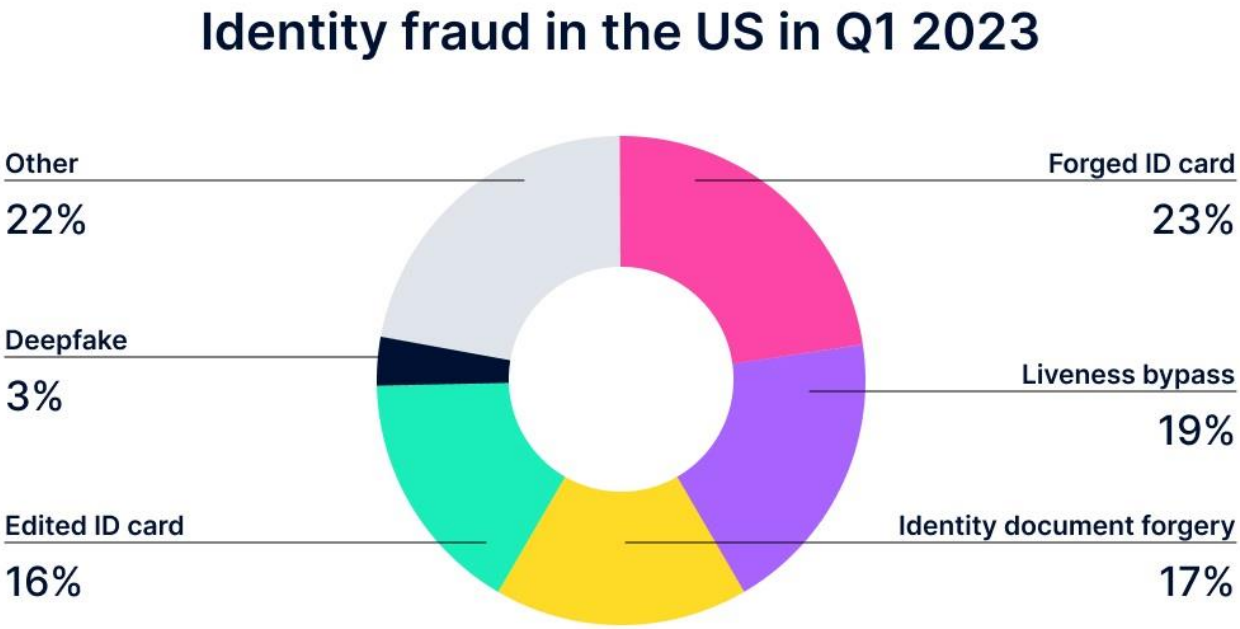


Diagram 2.Fraud in the US in 2023

References:
1.Deepfake Technology: The Risks, Benefits and Detection Methods
URL: https://www.linkedin.com/pulse/Deepfake-technology-risks-benefits-detection-methods-sahota-%E8%90%A8%E5%86%A0%E5%86%9B-?utm_source=share&utm_medium=guest_desktop&utm_campaign=copy

2. Journal of Computer and Communications Abdulqader(2021) M. Almars Deepfakes Detection Techniques Using Deep Learning: a survey/ College of Computer Science and Engineering, Taibah University, Yanbu, Saudi Arabia. URL: https://www.scirp.org/pdf/jcc_2021051813373227.pdf
3.Deepfake Detection Software: Types and Practical Application. URL: https://antispoofing.org/Deepfake-detection-software-types-and-practical-application/

Поліщук Артем Сергійович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В СУЧАСНОМУ СВІТІ: РОЛЬ ТЕХНІЧНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Специфікація проблеми

Сучасне суспільство живе в інформаційній епохі, де велика частина цінних активів і конфіденційної інформації зберігається та обробляється в електронному форматі. Однак цей цифровий перехід призводить до загроз кібербезпеці, які є більш серйозними і руйнівними, ніж будь-коли раніше. Кіберзлочинці, хакери та кібертерористи використовують різноманітні методи та атаки, спрямовані на здобуття несанкціонованого доступу до важливої інформації та інфраструктури. Це не тільки підірвує довіру в інтернет, але й ставить під загрозу фінансову стабільність, національну безпеку та приватність громадян.

Таким чином, забезпечення кібербезпеки стає завданням першочергового значення. Технічні системи захисту інформації відіграють важливу роль у цьому контексті, надаючи інструменти та технології для виявлення, запобігання та реагування на кібератаки. Забезпечуючи конфіденційність, цілісність та доступність даних, вони визначають, наскільки ефективним та стійким є інформаційний простір у сучасному світі.

Роль технічних систем захисту інформації

Технічні системи захисту інформації - це сукупність апаратних та програмних засобів, які призначені для забезпечення конфіденційності, цілісності та доступності даних. Вони включають в себе різноманітні рішення, такі як брандмауери, антивірусні програми, системи виявлення вторгнень, шифрування даних, та інші технічні засоби. Ці системи допомагають захищати інформацію від несанкціонованого доступу та зберігають функціональність систем навіть у випадку кібератак.

Технічні засоби захисту інформації

1. Засоби захисту інформації комплексів технічного захисту (КТЗІ)
Генератори шуму
Електромережні фільтри

Розділові трансформатори
Засоби віброакустичного захисту
2. Засоби захисту інформації від несанкціонованого доступу (НСД)
Засоби мережевого захисту
Засоби захисту кінцевих мережевих вузлів
Засоби моніторингу та аудиту
Засоби автентифікації користувачів
Засоби захисту каналів передачі даних
3. Вимірювальні комплекси в галузі ТЗІ
Для проведення пошукових робіт
Для оцінки захищеності ОІД (мовна інформація)
Для проведення оцінки захищеності обєктів ЕОТ (ПЕМВН)
4. Інженерні системи та комплекси
Засоби відеонагляду
Охоронна та протипожежна сигналізація

Актуальні проблеми

Проте сучасна кіберзагроза постійно змінюється, і тому технічні системи захисту інформації повинні бути постійно оновлюваними та адаптованими до нових загроз. Саме ця динаміка створює кілька актуальних проблем у галузі кібербезпеки:

Брак кваліфікованих кадрів: Недостатній обсяг кваліфікованих фахівців у галузі кібербезпеки є серйозною проблемою. Відсутність спеціалістів може призвести до недоліків у розробці, впровадженні та підтримці технічних систем захисту інформації.

Нові види загроз: Кіберзлочинці постійно вдосконалюють свої методи та винаходять нові атаки. Потрібно постійно оновлювати технічні системи захисту для виявлення та запобігання новим загрозам.

Постійні оновлення: Технічні системи захисту інформації повинні бути постійно оновлюваними, щоб залишатися ефективними в змінному кіберсередовищі. Порядок і час оновлень мають бути ретельно сплановані, щоб забезпечити найвищий рівень захисту.

Збільшення витрат: Забезпечення кібербезпеки вимагає фінансових інвестицій у технічні засоби та інфраструктуру. Зростаюча комплексність атак та вимоги до захисту призводять до збільшення витрат на кібербезпеку.

Висновок

Технічні системи захисту інформації відіграють важливу роль у

забезпеченні кібербезпеки у сучасному світі. Проте, їхнє ефективне функціонування вимагає рішучості та інвестицій. Важливо продовжувати дослідження та розвиток в цій галузі, а також залучати більше фахівців до сфери кібербезпеки. Тільки так можна забезпечити надійний захист інформації в мережі та зберегти безпеку в цифровому світі.

Перелік посилань:

1. Обладнання - ТЗІ URL https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjhxJf97YeCAxWu_7sIHQFWBAcQFnoECCAQAQ&url=https%3A%2F%2Ftzi.com.ua%2Fobladnannya.html&usg=AOvVaw3JfSEV59gP-OppoktXOzIN&opi=89978449 (дата звернення: 14.10.2023).

Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом URL: https://data.gov.ua/dataset/eab73672-181f-4b20-8819-56d47723ff11 (дата звернення: 10.10.2023)

Пономаренко Микита Олексійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАХИСТУ ВІД ВЕБ ЗАГРОЗ ХМАРНОЇ ІНФРАСТРУКТУРИ НА БАЗІ AWS

Хмарні технології, такі як Amazon Web Services (AWS), надають компаніям можливість розгортати і керувати інфраструктурою в Інтернеті. Однак ця інфраструктура вимагає надійного захисту від різних веб-загроз, таких як DDoS-атаки, SQL-ін'єкції, кросс-сайтові атаки та інші.

Відповідальність за безпеку та відповідність вимогам спільно несуть AWS та клієнт. Така модель загальної відповідальності допомагає знизити операційне навантаження на клієнта, оскільки AWS перебирає питання експлуатації, контролю та управління компонентами від рівня віртуалізації та операційної системи вузла до рівня фізичної безпеки об'єктів, де працює сервіс. Клієнт бере на себе відповідальність за гостьову операційну систему та керування нею (включаючи оновлення та виправлення безпеки) та іншим прикладним програмним забезпеченням, а також налаштування брандмауера групи безпеки, що надається платформою AWS. Клієнти повинні ретельно оцінювати послуги, які вони обирають, оскільки їх обов'язки змінюються в залежності від використовуваних послуг, їх інтеграції у власні IT-середовища та застосовних законів і нормативних актів. Система такої загальної відповідальності також забезпечує гнучкість та контроль клієнта за виконанням розгортань. [1]

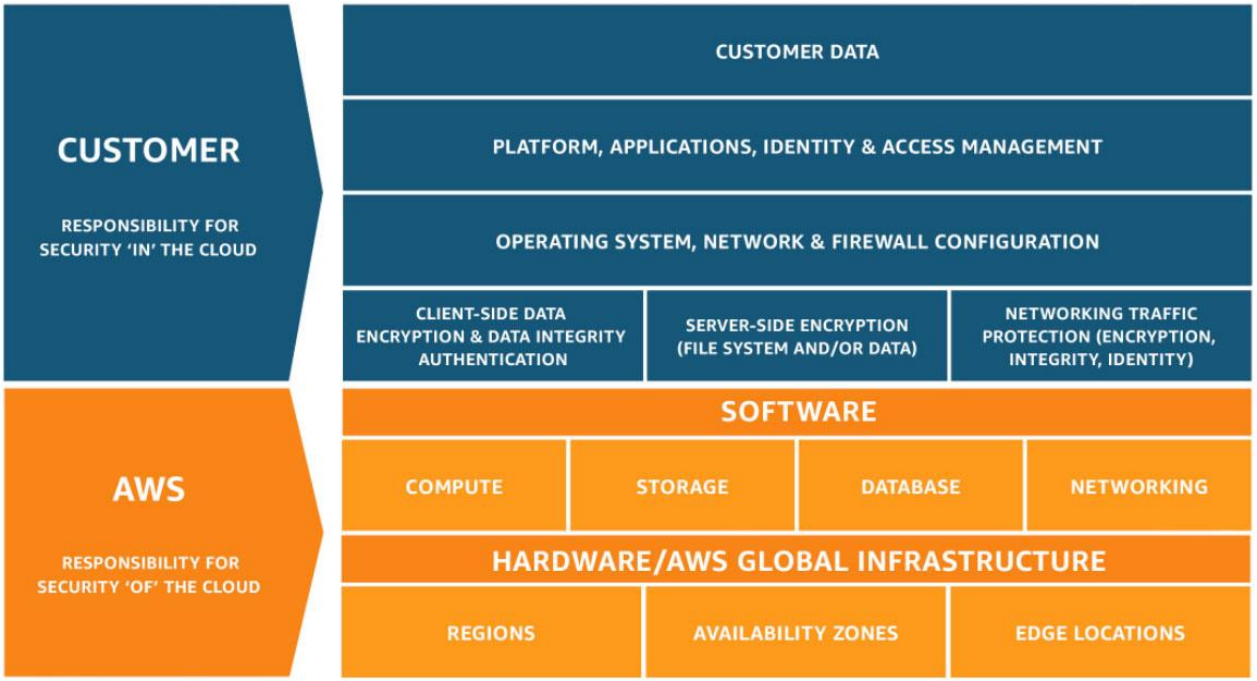


Рис. 1. - Схема розподілення обов'язків

Як показанано на рисунку вище, AWS чітко розрізняє відповідальність клієнта і провайдера. В залежності від типу сервіса, використаного користувачем, схема може змінюватися. Так, якщо використовується сервіс типу SaaS, то клієнт відповідає лише за додаток, який там розміщено.

Однією з основних технологій захисту є використання AWS Security Groups і Network Access Control Lists (NACL). Security Groups дозволяють керувати трафіком до та з різних ресурсів в AWS. Використовуючи NACL, можна налаштовувати більш докладний контроль над трафіком на рівні підмереж та IP-адрес. Ці інструменти допомагають встановити бар'єри перед зловмисниками.

Для запобігання несанкціонованому доступу використовується AWS Identity and Access Management (IAM). Ця система дозволяє точно налаштовувати права доступу до AWS-ресурсів і встановлювати принцип найменших привілеїв, щоб зменшити ризик надмірних дозволів. [2]

AWS пропонує рішення для моніторингу і журналювання подій в інфраструктурі. Amazon CloudTrail дозволяє відстежувати всі дії користувачів та API-виклики. CloudWatch надає можливість моніторити ресурси і виявляти аномальні активності, що допомагає реагувати на можливі загрози.

AWS Key Management Service (KMS) дозволяє керувати ключами шифрування, а це важливо для захисту даних. Дані слід шифрувати в покою та під час переміщення, щоб запобігти їх доступності для несанкціонованих осіб.

Для захисту від Distributed Denial of Service (DDoS) атак можна використовувати AWS Shield, який надає захист на рівні мережі і захищає від великих інтернет-атак. Крім того, AWS WAF дозволяє фільтрувати трафік під час DDoS-атак і відсікати потенційно шкідливі запити.

AWS WAF допомагає виявляти та блокувати веб-загрози, такі як SQL-

ін'єкції і кросс-сайтові атаки. Використання AWS Lambda для автоматичного реагування на загрози може значно підвищити ефективність захисту. [3]

Резервне копіювання даних і відновлення важливі для забезпечення надійності інфраструктури. AWS пропонує різні рішення для автоматичного резервного копіювання даних та відновлення, щоб забезпечити швидке відновлення в разі вироку даних.

AWS Config допомагає відстежувати зміни в конфігураціях ресурсів і виявляти потенційні проблеми безпеки. Це важливо для забезпечення цілісності інфраструктури.

Навчання користувачів та розробників щодо основних принципів безпеки в AWS є важливою частиною захисту. Свідомість і навички користувачів можуть запобігти багатьом загрозам.

AWS VPC надає можливість створити ізольовані мережі та сегменти для даних і додатків, що допомагає захистити дані в покою.

Захист від веб-загроз у хмарній інфраструктурі на базі AWS - це важливий аспект безпеки, який вимагає комплексного підходу та постійного оновлення стратегій і інструментів. AWS надає різноманітні технології та ресурси для забезпечення безпеки, і важливо їх належним чином використовувати для захисту власної інфраструктури.

Перелік посилань:

1. Модель загальної відповідальності URL: https://aws.amazon.com/ru/compliance/shared-responsibility-model/ (дата звернення 24.10.2023)
2. Керування ідентифікацією та доступом AWS URL: https://aws.amazon.com/ru/iam/ (дата звернення 24.10.2023)
3. The Top 10 Security Tools for Your AWS Environment URL: https://www.missioncloud.com/blog/the-top-10-security-tools-for-your-aws-environment (дата звернення 24.10.2023)

Посвященна Алла В'ячеславівна
Студентка групи УБДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Кіберзлочинність - це проблема, з якою зіштовхнулась планета у 21 столітті, явища новітньої, цифрової доби. З розвитком новітніх технологій розвиваються й нові злочинні можливості спрямовані на заволодіння інформацією з баз даних, перехоплення інформації, знищення інформації за допомогою розповсюдження програм-вірусів, фішингових програм, злому з корисливих, політичних чи особистих мотивів.

Інтернет, комп'ютери, мобільні телефони та інші цифрові технології здійснили революцію у всіх сферах людського життя за останні декілька десятиліть, тобто повністю змінили наше життя, включаючи те, як ми спілкуємося, здійснюємо банківські операції, робимо покупки, дізнаємося новини, розважаємося тощо [1].

Існування кіберзлочинності становить досить серйозну проблему в умовах глобального процвітання інноваційно-технологічних ресурсів. Це впливає абсолютно на всіх, як на окремих фізичних та юридичних осіб, так і на об'єкти

критичної інформаційної інфраструктури й державні органи. Окрім, відповідної прямої шкоди, кіберзлочинність є величезною перешкодою для цифрової довіри, значною мірою підриваючи переваги кіберпростору.

Україна останніми роками дедалі більше відчуває на собі масштаби кібернетичних атак та їх негативні наслідки. Кількість кримінальних правопорушень у сфері інформаційних технологій постійно зростає.

Передумовами та чинниками, які формують загрози у сфері кібербезпеки України, є [2, 4]:

– військова агресія російської федерації проти України;

– гіперпопит на різні види інформаційних послуг;

– процеси глобалізації світової економіки, розвиток сучасних інформаційних технологій, особливо інтернет-ресурсів, що забезпечують майже неконтрольований процес формування спокус.

– недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації;

– повільна імплементація положень європейського права в Українське законодавство;

– недостатня урегульованість цифрової складової частини розслідування злочинів, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері;

– відсутність у значної частини міністерств і відомств відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом;

– фінансування робіт із кіберзахисту здійснюється за залишковим принципом з технологічними помилками;

– невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі.

Проведений аналіз дав змогу окреслити основні першочергові напрями у протидії цьому суспільно небезпечному явищу, з-поміж них[3]:

– необхідність активізувати діяльність правоохоронних структур в Україні у протидії кібезлочинності;

– посилення взаємодії з правоохоронними структурами інших держав;

– створення нових і доповнення чинних нормативно правових актів для протидії кіберзагрозам зокрема на основі міжнародного досвіду та міжнародних стандартів;

– удосконалення програмно-технічного забезпечення роботи інформаційних та телекомунікаційних систем;

– поліпшення інформування суспільства про систему забезпечення кібернетичної безпеки тощо;

– підготовка та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту.

Лише комплексний підхід до вирішення питання забезпечення кібернетичної безпеки в державі сприятиме зниженню кількість злочинів у цій сфері, а також дасть змогу підвищити ефективність заходів щодо їх розкриття.

З вище викладеного випливає, що кіберзлочинність в Україні розвивається досить швидко, але й Держава не стоїть на місці та з кожним днем демонструє високі показники боротьби з кіберзлочинністю [2].

Тому, лише завдяки належному рівню кібербезпеки можливе нормальне функціонування мереж та систем, які з кожним днем все більше інтегруються в життя нашого суспільства.

Перелік посилань:

1. Ю.П. Лісовська, «Кібербезпека: ризики та заходи»: Навчальний посібник. Ст.119-206;
2. Боротьба з кіберзлочинністю в умовах воєнного стану. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v- umovakh-d-vonnogo-stanu-zakon-2149-ix;
3. «Стратегія кібербезпеки України (2021-2025 роки) безпечний кіберпростір - запорука успішного розвитку країни», затверджена указом Президента України від 26 серпня 2021 року № 447/2021, URL: https://www.rnbo.gov.ua/ua/Ukazy/4974.html?PRINT;
4. Правове забезпечення кібербезпеки України. URL: http://pgp-journal.kiev.ua/archive/2019/9/18.pdf

Приблудюк Юрій Олександрович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ОСНОВНІ РИЗИКИ БЕЗПЕКИ В ХМАРНИХ СЕРВІСАХ ОРГАНІЗАЦІЇ

Хмарні сервіси пропонують організаціям гнучкість, масштабованість та оптимізацію витрат, однак з ними пов'язані ключові ризики безпеки, до яких відносяться: несанкціонований доступ до даних, недостатня ізоляція користувачів, вразливості API, ризики втрати даних та недостатнє управління ідентичністю та доступом. Для забезпечення безпечного використання хмарних технологій організаціям необхідно активно співпрацювати з постачальниками хмарних сервісів та впроваджувати комплексні стратегії безпеки.

Хмарні сервіси: новий етап цифрової еволюції

Хмарні технології вже не є новизною в сучасному світі. Вони змінили спосіб, яким організації зберігають та обробляють дані, надаючи гнучкість, масштабованість та економічні переваги. Проте, як і будь-яка інша технологія, вони мають свої ризики, особливо у сфері безпеки [1]:

1. Несанкціонований доступ до даних: інформація, збережена в хмарі, може стати легкою здобиччю для зловмисників, якщо захисні механізми не належним чином реалізовані. Зловмисники можуть використовувати вразливості в програмному забезпеченні, слабкі паролі користувачів або інші техніки для отримання доступу до цінної інформації.
2. Недостатнє управління ідентичністю та доступом: організації часто мають багато користувачів з різними рівнями доступу до хмарних сервісів.

Відсутність строгого контролю ідентичності може призвести до витоку даних або зловживань.

3. Вразливості API: інтерфейси програмування додатків (API), які використовуються для взаємодії з хмарними сервісами, можуть мати свої вразливості. Ці вразливості можуть бути використані для атак на систему.

4. Ризики втрати даних: хмарні сервіси залежать від своєї інфраструктури, і будь-які збої в цій інфраструктурі можуть призвести до втрати даних. Це може бути результатом атаки, технічного збою або людської помилки.

5. Недостатній фізичний захист: хоча постачальники хмарних сервісів зазвичай вкладають значні ресурси в фізичний захист своїх центрів обробки даних, існує можливість фізичного злому або інших загроз.

6. Міжмісцевість даних: через розподілену природу хмар, дані можуть бути розташовані в різних юрисдикціях, що може призвести до проблем з дотриманням законодавства.

Ці ризики можуть мати критичний вплив на функціонування організацій, якщо їх не виявляти та не вирішувати вчасно. Але, як говориться, кожна проблема - це можливість для зростання. Тому замість того, щоб уникати використання хмарних технологій через страх перед потенційними загрозами, краще зосередитися на знаходженні відповідних рішень для кожного із цих ризиків [2]:

- Впровадження двоетапної автентифікації: це додатковий рівень захисту, який вимагає від користувача надання двох форм ідентифікації.
- Регулярні перевірки безпеки: це допоможе ідентифікувати та усунути вразливості в системі.
- Інтеграція систем управління ідентичністю та доступом (IAM): забезпечте централізований контроль над доступом користувачів до ресурсів.
- Мінімізація прав доступу: надавайте користувачам лише ті права, які вони дійсно потребують.
- Шифрування трафіку: використовуйте SSL/TLS для захисту даних, які передаються між клієнтами та API.
- Регулярне тестування безпеки API: інструменти, такі як сканування вразливостей та тестування на проникнення, можуть виявити потенційні проблеми.
- Резервне копіювання: створюйте регулярні резервні копії даних та зберігайте їх у безпечному місці.
- Впровадження шифрування: шифруйте дані на стороні клієнта перед завантаженням їх у хмару.
- Вибір надійних постачальників: обирайте хмарних провайдерів, які мають високі стандарти фізичної безпеки для своїх центрів обробки даних.
- Розподілена архітектура: розміщуйте критичні компоненти системи в різних місцях для зменшення ризиків.

- Політика управління даними: визначте, в яких регіонах дозволено зберігати дані та слідкуйте за тим, щоб ваш постачальник хмарних послуг дотримувався цієї політики.
- Шифрування: захистіть дані, які можуть бути піддані юрисдикційним ризикам, використовуючи сильні методи шифрування.

Для ефективного вирішення ризиків, організації мають підійти до питання безпеки в хмарних сервісах комплексно. Це включає в себе вибір надійних постачальників хмарних послуг, регулярну перевірку політик безпеки та впровадження найкращих практик з кібербезпеки.

Перелік посилань:

1. Top Threats to Cloud Computing: Pandemic 11 Deep Dive [Електронний ресурс] – Режим доступу: https://s3.amazonaws.com/content-production.cloudsecurityalliance/a5rszg1baumen37lyouk2nvzpghv?response-content-disposition=inline%3B%20filename%3D%22Top-Threats-to-Cloud-Computing-Pandemic%2011-Deep-Dive-20231016.pdf%22%3B%20filename%2A%3DUTF-8%27%27Top-Threats-to-Cloud-Computing-Pandemic%252011-Deep-Dive-20231016.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAS6XDIRHKHO4F5SU4%2F20231024%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20231024T204918Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-Signature=33364b1b042b1f5004048ad1e0da6e49dc1aff18a677970997331251b9f292f3
2. Cloud Native Application Protection Platform (CNAPP) Survey Report [Електронний ресурс] – Режим доступу: https://s3.amazonaws.com/content-production.cloudsecurityalliance/y4hbyz7438gh0bu8oc2yhvgjwx7e?response-content-disposition=inline%3B%20filename%3D%22CNAPP%20Survey%20-%20Sponsored%20by%20Microsoft%20082223.pdf%22%3B%20filename%2A%3DUTF-8%27%27CNAPP%2520Survey%2520-%2520Sponsored%2520by%2520Microsoft%2520082223.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAS6XDIRHKHO4F5SU4%2F20231024%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20231024T205407Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-Signature=cebf35e28dc8cd1bff71a70d99714cac438d52ff4d6fd65776a8cd74714b602a

Примаченко Діана Володимирівна
студентка групи УБДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ВПРОВАДЖЕННЯ ЕФЕКТИВНОГО МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНІЗАЦІЯХ: СТРАТЕГІЧНІ ВИКЛИКИ І МОЖЛИВОСТІ

Розглянуто важливість впровадження ефективного менеджменту інформаційної безпеки в організаціях і висвітлено стратегічні виклики та можливості, які пов'язані із цим процесом. У контексті зростаючих загроз інформаційній безпеці, проаналізовано сучасні стратегії та підходи до захисту даних та інформаційних ресурсів організацій. Досліджено, як ефективний менеджмент інформаційної безпеки може вплинути на стратегічну діяльність організації, забезпечуючи захист від потенційних загроз і забезпечуючи довгострокову стійкість.

У світі, який вивчає нові можливості та технологічні досягнення, забезпечення інформаційної безпеки стає дедалі більш важливим завданням для організацій будь-якого масштабу та галузі. Особливу актуальність ця тема набуває в контексті цифрового віку, коли дані та інформація стали найціннішими

активами. Впровадження ефективного менеджменту інформаційної безпеки в організаціях породжує численні стратегічні виклики та можливості, які варто розглянути. [1]

Серйозною загрозою для сучасних організацій є кібератаки. Зловмисники постійно вдосконалюють свої методи, і впровадження заходів інформаційної безпеки стає необхідністю. Організації повинні розробити стратегії захисту від кіберзагроз, виявлення і ліквідації вразливостей та постійно моніторити обставини для вчасного реагування на можливі загрози.

Зміна законодавства та регулюючих вимог також має велике значення. У багатьох країнах діють стандарти і вимоги щодо захисту інформації, і їх недотримання може призвести до серйозних наслідків. Організаціям варто постійно оновлювати свої практики та процедури відповідно до законодавства.

Внутрішні загрози, такі як інсайдерські атаки, не менш небезпечні. Впровадження культури інформаційної безпеки в організацію може допомогти запобігти таким загрозам. Навчання співробітників та розвиток систем виявлення та реагування можуть значно покращити безпеку.

Зростання обсягів даних створює ще один виклик. Організаціям потрібно ефективно управляти даними, забезпечувати їх безпеку та дотримуватися різних стандартів їх обробки. Використання сучасних технологій, таких як штучний інтелект і машинне навчання, може полегшити цей процес і допомогти виявляти загрози. [2]

Стратегічне управління інформаційною безпекою вимагає розробки планів і стратегій, які відповідають бізнес-цілям організації. Це повинно бути вбудовано в загальну стратегію компанії і підтримувати її розвиток.

Співпраця і партнерство з іншими організаціями та спеціалізованими компаніями можуть допомогти зменшити загрози та підвищити рівень інформаційної безпеки. [3]

Таким чином, впровадження ефективного менеджменту інформаційної безпеки в організаціях вимагає систематичного підходу, інвестицій у технології та освіту співробітників, а також гнучкості для адаптації до загроз, що постійно змінюються. Інформаційна безпека повинна бути не лише завданням відділу IT, але і частиною загальної стратегії організації, яка сприяє її стабільності та конкурентоспроможності.

Перелік посилань:

1. Tipton H. F., Krause M. Information Security Management Handbook. Taylor & Francis Group, 2004.

2. Шемчук В. Принципи забезпечення інформаційної безпеки. Наукові записки Інституту законодавства Верховної Ради України. 2018. № 4. с. 50–56.

3. Поддубний В. О., Сєвєрінов О. В. Менеджмент вразливостей як складова частина системи управління інформаційної безпеки. 2020. URL: http://openarchive.nure.ua/handle/document/14290

Раков Микита Євгенович
Державний університет інформаційно-комунікаційних технологій

ДОСЛІДЖЕННЯ І УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ТА ПРОТОКОЛІВ АУТЕНТИФІКАЦІЇ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ

Анотація

Актуальність та значення цифрової безпеки у сучасному світі не можна переоцінити, оскільки інформація та комунікації є необхідними складовими сучасного суспільства. Однак ця залежність також робить нас більш уразливими перед кіберзлочинцями та загрозами. Електронні цифрові підписи (ЕЦП) грають ключову роль у забезпеченні безпеки цифрових комунікацій та транзакцій. Ця робота спрямована на дослідження та удосконалення механізмів та протоколів аутентифікації електронних цифрових підписів, зокрема їх виклики та алгоритми.

Актуальні виклики кібербезпеки

Сучасний цифровий світ стикається з безпрецедентними викликами в галузі кібербезпеки. Зростаюча кількість кібератак та загроз для конфіденційності та цілісності даних вимагає постійного вдосконалення та адаптації засобів захисту. Ці виклики стосуються не лише державних органів та великих корпорацій, але й звичайних громадян, оскільки кожен з нас використовує цифрові технології у повсякденному житті.

Електронні цифрові підписи в контексті викликів кібербезпеки

Електронні цифрові підписи є однією з ключових технологій, яка допомагає вирішувати виклики кібербезпеки. Вони гарантують аутентичність та недоторканість цифрових документів та повідомлень, забезпечуючи можливість відслідковувати автора та забезпечити конфіденційність даних. Проте існують виклики, пов'язані з ефективністю та безпекою самого механізму ЕЦП, які потребують удосконалення.

Атаки на електронні цифрові підписи (ЕЦП) є серйозною загрозою для цифрової безпеки і можуть призвести до підробки підписів та порушення автентичності даних. Деякі з відомих методів атаки на ЕЦП включають:

1. Перехоплення та відтворення підпису (Replay Attack): У цій атакі зловмисник перехоплює легітимний ЕЦП і використовує його знову для підписування інших повідомлень. Ця атака може бути успішною, якщо не вжито заходів для захисту від відтворення підпису.
2. Атака на вибір хеш-функції (Hash Collision Attack): Ця атака використовує колізії в хеш-функціях для створення двох різних повідомлень, які мають однаковий хеш-значення. Це може призвести до підробки ЕЦП на одному повідомленні та його застосування на іншому.

3. Атака на приватний ключ (Private Key Attack): Якщо зловмиснику вдається отримати доступ до приватного ключа, він може створити власні

підписи від імені легітимного користувача. Захист від цієї атаки полягає в надійному зберіганні приватного ключа та використанні безпечних протоколів.

4. Атака на важкодоступний ключ (Key Search Attack): У цій атакі зловмисник намагається "вгадати" важкодоступний ключ, який використовується для створення ЕЦП. Ця атака вимагає великої обчислювальної потужності і може бути надійно захищена за допомогою використання ключів великої довжини.

5. Соціальна інженерія (Social Engineering): Зловмисники можуть намагатися обманути користувача або особу, яка має доступ до приватного ключа, щоб отримати доступ до ключа або підпису. Це може включати в себе соціальну маніпуляцію та шахрайство.

6. Сторонні атаки (Man-in-the-Middle Attacks): У таких атаках зловмисники впроваджуються між комунікуючими сторонами і можуть перехоплювати та змінювати повідомлення та ЕЦП. Ця атака може бути успішною, якщо зловмисник отримав доступ до ключів або вміє імітувати легітимний обмін ключами.

7. Атака "відомий-текст" (Known-plaintext Attack): Якщо зловмиснику відомі пари повідомлення і відповідні ЕЦП, він може намагатися знайти відповідність між конкретним текстом і підписом. Ця атака може виявити слабкість алгоритму підписування.

Аутентифікація на основі ЕЦП

Аутентифікація на основі ЕЦП - це процес перевірки особи, яка видається власником цифрового підпису. Цей процес грає важливу роль у забезпеченні безпеки комунікацій та транзакцій.

У своїй роботі Гольдвассер, Мікалі та Рівест описують такі моделі атак, які актуальні і в даний час:

- Атака із використанням відкритого ключа. Криптоаналітик має лише відкритий ключ.
- Атака з урахуванням відомих повідомлень. Противник має допустимі підписи набору електронних документів, відомих йому, але не вибираються ним.
- Адаптивна атака на основі вибраних повідомлень. Криптоаналітик може отримати підписи електронних документів, які він сам обирає.

Також у роботі описано класифікацію можливих результатів атак:

- Повний злам цифровий підпис. Отримання закритого ключа, що означає повний зламування алгоритму.
- Універсальна підробка цифрового підпису. Знаходження алгоритму, аналогічного алгоритму підпису, що дозволяє підробляти підписи будь-якого електронного документа.
- Вибіркова підробка цифрового підпису. Можливість підробляти підписи для документів, вибраних криптоаналітиком.

- Екзистенційне підроблення цифрового підпису. Можливість отримання допустимого підпису для якогось документа, що не обирається криптоаналітиком.

Ясно, що «небезпечною» атакою є адаптивна атака на основі обраних повідомлень, і при аналізі алгоритмів ЕП на криптостійкість потрібно розглядати саме її (якщо немає яких-небудь особливих умов).

При безпомилковій реалізації сучасних алгоритмів ЕП отримання закритого ключа алгоритму є практично неможливим завданням через обчислювальну складність завдань, на яких ЕП побудовано. Набагато ймовірнішим є пошук криптоаналітиком колізій першого і другого пологів. Колізія першого роду еквівалентна екзистенційному підробленню, а колізія другого роду - вибірковій. З урахуванням застосування хеш-функцій, знаходження колізій для алгоритму підпису еквівалентне знаходження колізій для самих хеш-функцій.

Алгоритми ЕЦП

Алгоритми ЕЦП є ключовою складовою технології цифрових підписів. Дослідження алгоритмів ЕЦП дозволить зрозуміти їхню ефективність та безпеку. Зазвичай це включає вивчення різних типів алгоритмів, таких як RSA, DSA, та ECDSA, а також їхню відповідність сучасним стандартам кібербезпеки.

Висновок

Дослідження та удосконалення механізмів та протоколів аутентифікації електронних цифрових підписів є надзвичайно важливим завданням у контексті зростаючих викликів кібербезпеки. ЕЦП відіграють ключову роль у забезпеченні цифрової безпеки, та їх дослідження, удосконалення та застосування дозволить забезпечити безпеку комунікацій та транзакцій у цифровому світі. Результати даної роботи сприятимуть розвитку більш надійних та безпечних механізмів аутентифікації та захисту даних в онлайн середовищі.

Перелік посилань:

1. Мао В. Сучасна криптографія: Теорія та практика - М.: Вільямс, 2005. - 768 с. - ISBN 5-8459-0847-7

Рибаченко Вадим Ярославович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ЗАХИСТ WEB-ДОДАТКІВ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Розвиток веб-технологій у поєднанні зі зміною бізнес-середовища означає, що сьогодні веб-додатки стають все більш поширеними в корпоративних і державних службах. Хоча веб-додатки можуть забезпечити зручність і ефективність, існує також ряд нових загроз безпеці, які потенційно можуть становити значні ризики для інфраструктури інформаційних технологій організації, якщо з ними не поводитися належним чином.

Сьогодні традиційних заходів і технологій мережевої безпеки може бути недостатньо для

захисту веб-програм від нових загроз, оскільки атаки зараз спрямовані спеціально на недоліки безпеки веб-програм.

Безпека веб-додатків (також відома як Web AppSec) — це ідея створення веб-сайтів, які функціонуватимуть належним чином, навіть коли вони зазнають атаки. Концепція передбачає набір елементів керування безпекою, розроблених у веб-програмі для захисту її активів від потенційно зловмисних агентів. Веб-програми, як і будь-яке програмне забезпечення, неминуче містять дефекти. Деякі з цих дефектів є фактичними вразливими місцями, якими можна скористатися, створюючи ризики для організацій. Безпека веб-додатків захищає від таких дефектів. Це передбачає використання методів безпечної розробки та впровадження заходів безпеки протягом усього життєвого циклу розробки програмного забезпечення, гарантуючи усунення недоліків на рівні дизайну та помилок на рівні реалізації.

Тестування веб-безпеки має на меті виявити вразливі місця у веб-додатках та їх конфігурації. Основною метою є прикладний рівень (тобто те, що працює за протоколом HTTP). Перевірка безпеки веб-додатку часто передбачає надсилання різних типів вхідних даних, щоб спровокувати помилки та змусити систему поводитись несподіваним чином. Ці так звані «негативні тести» перевіряють, чи робить система щось, для чого вона не призначена.

Важливо також розуміти, що тестування веб-безпеки стосується не тільки тестування функцій безпеки (наприклад, автентифікації та авторизації), які можуть бути реалізовані в програмі. Не менш важливо перевірити, чи безпечно реалізовані інші функції (наприклад, бізнес-логіка та використання належної перевірки вхідних даних і вихідного кодування). Мета полягає в тому, щоб гарантувати безпеку функцій, відкритих у веб-додатку.

Типи тестів безпеки:

- Динамічний тест безпеки додатків (DAST). Цей автоматизований тест безпеки додатків найкраще підходить для внутрішніх додатків із низьким рівнем ризику, які мають відповідати нормативним оцінкам безпеки. Для додатків із середнім рівнем ризику та критичних додатків, які зазнають незначних змін, найкращим рішенням є поєднання DAST із ручним тестуванням веб-безпеки на загальні вразливості.
- Статичний тест безпеки додатків (SAST). Цей підхід до безпеки програми пропонує автоматизовані та ручні методи тестування. Це найкраще для виявлення помилок без необхідності виконання програм у робочому середовищі. Це також дозволяє розробникам сканувати вихідний код і систематично знаходити та усувати вразливості безпеки програмного забезпечення.
- Тест на проникнення. Цей ручний тест безпеки програми найкраще підходить для критичних програм, особливо тих, які зазнають серйозних змін. Оцінка включає в себе бізнес-логіку та тестування на основі супротивника, щоб виявити передові сценарії атак.

- Самозахист програми під час виконання (RASP). Цей підхід до безпеки додатків, що розвивається, охоплює низку технологічних прийомів для інструментування програми, щоб можна було відстежувати атаки під час їх виконання та, в ідеалі, блокувати їх у режимі реального часу.

Як тестування безпеки програми знижує ризик для організації?

Веб-додаток у сучасному середовищі може зазнавати широкого кола проблем. Знання різних атак, які роблять програму вразливою, на додаток до потенційних наслідків атаки, дозволить завчасно усунути вразливості та точно перевірити їх.

Визначивши основну причину вразливості, на ранніх стадіях SDLC можна запровадити засоби пом'якшення, щоб запобігти будь-яким проблемам. Крім того, знання про те, як працюють ці атаки, можна використовувати для націлювання на відомі об'єкти інтересу під час перевірки безпеки веб-додатків.

Визнання впливу атаки також є ключовим для управління ризиками організації, оскільки наслідки успішної атаки можна використовувати для оцінки загальної серйозності вразливості. Якщо під час перевірки безпеки виявлено проблеми, визначення їх серйозності дозволить ефективно визначати пріоритети заходів з усунення. Краще почати із критичних проблем і працювати над проблемами меншого впливу, щоб мінімізувати ризик.

Перш ніж виявити проблему, оцінка потенційного впливу на кожну програму в бібліотеці програм може полегшити визначення пріоритетів тестування безпеки програми. Завдяки встановленому списку високопрофільних додатків можна запланувати тестування безпеки, щоб спершу націлити на критичні додатки з більш цілеспрямованим тестуванням, щоб знизити ризик для бізнесу.

Які функції слід перевірити під час перевірки безпеки веб-додатків?

Неналежне впровадження кожної з них може призвести до вразливостей, створюючи серйозний ризик для організації.

- Конфігурація програми та сервера. Потенційні дефекти пов'язані з конфігураціями шифрування/криптографії, конфігураціями веб-сервера тощо;
- Перевірка введених даних і обробка помилок. Впровадження SQL, міжсайтовий скриптинг (XSS) та інші поширені вразливості є результатом поганої обробки введення та виведення;
- Аутентифікація та керування сеансами. Уразливості, які потенційно можуть призвести до видавання користувача за іншу особу. Слід також враховувати надійність і захист облікових даних;
- Авторизація. Тестування здатності програми захищати від вертикального та горизонтального підвищення привілеїв;

- Бізнес-логіка. Це важливо для більшості програм, які забезпечують бізнес-функціональність.

Перелік посилань:

1. Web Application Security URL: https://www.synopsys.com/glossary/what-is-web-application-security.html#:~:text=Definition,assets%20from%20potentially%20malicious%20agents.
2. Securing Web Application URL: https://www.infosec.gov.hk/en/best-practices/business/securing-web-application.

Розгон Денис Анатоілйович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ОСНОВНІ РИЗИКИ БЕЗПЕКИ ДЛЯ КОРИСТУВАЧА В ІГРАХ

Ігри стали невід'ємною частиною сучасного життя, займаючи центральне місце в розвагах та розвитку. Вони не лише надають можливість насолоджуватися вільним часом, але й впливають на наше мислення, вчать навичкам та розвивають творчість. Проте, разом із піднесеним інтересом до гри виникають і серйозні виклики, пов'язані із забезпеченням безпеки користувачів. Сучасні ігри, особливо онлайн-ігри, надають можливість спілкування та взаємодії з іншими гравцями з усього світу, що вносить аспекти соціальної динаміки в ігровий процес. Однак цей світ також приховує численні ризики, з якими користувачі можуть зіткнутися, включаючи кібербулінг, крадіжку особистої інформації, шахрайства та залучення до небезпечних ситуацій.

Основними загрозами для користувача в іграх:

- Шкідливі програми;
- Крадіжка даних
- Сватінг та доксинг
- Витік даних

Тепер трішки детальніше про кожен з видів загроз. Коли користувач завантажує неліцензійні версії ігор (так само, як і інших програм) він може заразити свій комп'ютер вірусами та шкідливими програмами. Цей ризик присутній також при використанні гравцями додаткового програмного забезпечення. Але важливо також відмітити, що завантажуючи гру з легального сайту все одно можна наразитись на небезпеку через уразливості в системі безпеки, тому розробникам це потрібно враховувати.

Кіберзлочинці можуть збирати особисту інформацію гравців для проведення подальших дій, таких як соціальна інженерія, або сватінг та доксинг. Найбільшою небезпекою в цьому плані є онлайн ігри з чатом. Тут потрібно бути обережним щодо обміну інформацією під час гри і не довіряти незнайомцям. Зі сторони розробників важливим є створення такого середовища, що мінімізує загрозу, а саме розробка нагадувань для користувача, що убезпечать його від крадіжки даних, а також впровадження систем, що для прикладу можуть приховувати пароль користувача, якщо він напише його в чат.

Отримавши персональні дані користувача, зловмисники можуть опублікувати персональні дані гравця, або використати їх для помсти, цькування,

переслідування або для розваги. Така поведінка називається доксингом. Сватінг та доксинг часто використовується в онлайн іграх як засіб помсти та знущання над іншими гравцями.

Кіберзлочинці можуть атакувати безпосередньо розробників ігор. Отримавши доступ до систем розробників вони можуть викрасти величезні обсяги інформації починаючи від персональних даних гравців і до вихідного коду проєкту. Після витоку зловмисники можуть використати цю інформацію для своїх цілей.

Щоб користувачі могли безпечно грати в онлайн ігри потрібно дотримуватись певних правил:

- Встановлюйте лише офіційні версії ігор, та уникайте сторонніх програм.
- Використовуйте надійне антивірусне програмне забезпечення.
- Захищайте свої акаунти надійними та унікальними паролями. Також ні в якому разі не розголошуйте свій логін та пароль.
- Проявляйте обережність в спілкуванні з незнайомцями в онлайн іграх. Не повідомляйте їм свої персональні данні, адресу, телефон і таке інше.

На основі цих порад корисувачу розробники ігор можуть сформувати свої правила, які допоможуть зробити гру безпечною для гравця.

Перелік посилань:
1. Cybersecurity threats from online gaming URL: https://www.orfonline.org/expert-speak/cybersecurity-threats-from-online-gaming/ (дата звернення: 20.10.2023).
2. Security and privacy in massively multiplayer online games and social and corporate virtual worlds URL: https://www.academia.edu/33374392/Security_and_privacy_in_massively_multiplayer_online_games_and_social_and_corporate_virtual_worlds (дата звернення: 20.10.2023).

Романенко Дмитро Павлович
студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ У МЕРЕЖАХ БАНКІВСЬКИХ СТРУКТУР НА ОСНОВІ BANKID

Це метод, який використовується банками та фінансовими установами для перевірки і підтвердження особистої ідентичності клієнтів у цифровому середовищі. Основні особливості цієї технології включають наступне:

1. Електронний ідентифікатор: BankID - це електронний ідентифікатор, який видається спеціальними сертифікованими постачальниками послуг. Він зазвичай пов'язаний з особистими даними користувача, такими як номери паспорта, коди податкового обліку і т.д.
2. Одноразові паролі: Для входу в банківський обліковий запис за допомогою BankID, користувач отримує одноразовий пароль або використовує біометричні дані, такі як відбитки пальців або скан обличчя для автентифікації.

3. Безпека: Ця технологія забезпечує високий рівень безпеки завдяки шифруванню та ідентифікації користувача на основі унікальних даних. Вона допомагає запобігти шахрайству та незаконному доступу до банківських рахунків.

4. Зручність: Користувачі можуть зручно користуватися BankID для здійснення фінансових операцій онлайн без необхідності відвідувати банк особисто.

5. Регулювання: Використання BankID регулюється відповідними законами та стандартами безпеки, що забезпечують відповідність фінансових установ вимогам щодо ідентифікації та збереження даних клієнтів.

Технологія ідентифікації користувачів на основі BankID сприяє зручності та безпеці фінансових операцій в онлайн-середовищі та допомагає знизити ризик шахрайства та шахрайських дій в банківському секторі.

Руднік Анатолій Андрійович
студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

НЕБЕЗПЕЧНЕ ЗБЕРІГАННЯ API КЛЮЧІВ У ВЕБ ТА МОБІЛЬНИХ ЗАСТОСУНКАХ

Сучасні веб та мобільні застосунки все частіше використовують API для інтеграції з різноманітними сервісами. Для аутентифікації та авторизації користувачів API використовують API ключі, які зазвичай являють собою строку що складається з набору пседовипадкових символів. Доволі часто розробники не дбають про безпеку API ключів та зберігають їх у самому коді, це дозволяє зловмиснкам вкрадати їх, що призводить до нелегального використання API зловмисниками і тягне за собою втрату конфіденційної інформації та фінансові збитки для компаній.

Як зловмисники крадуть API ключі.

Для кражі API ключів зловмисники застосовують засоби зворотньої розробки програмного забезпечення такі як статичний аналіз, динамічне інструментування та перехоплення трафіку застосунку.

Також частою причиною кражі ключів є відкриті репозиторії з кодом, в якому збережений API ключ. Зловмисники сканують репоизторії за допомогою утиліти для автоматичного пошуку секретів як trufflehog, що допомогає їм знаходити API ключі.

Перелік посилань:

1. https://mas.owasp.org/MASTG/techniques/#generic-techniques (дата звернення 08.10.2023)
2. https://www.zdnet.com/article/over-100000-github-repos-have-leaked-api-or-cryptographic-keys/ (дата звернення 10.10.2023)
3. https://github.com/trufflesecurity/trufflehog (дата звернення 11.10.2023)

Саєнко Андрій Святославович, БСДМ-61
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ УПРАВЛІННЯ ЖУРНАЛАМИ БЕЗПЕКИ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА БАЗІ IBM QRADAR SIEM ТА WINCOLLECT

Визначено мету і основні завдання щодо управління журналами безпеки кінцевих точок організації. Розглянуто зміст технології управління журналами безпеки кінцевих точок організації.

Управління журналами – це процес збору, аналізу та зберігання даних журналів, що генеруються інформаційними системами з метою виявлення порушень безпеки, визначення проблем з продуктивністю та відстеження активності системи. Журнали створюються різними системами, додатками та пристроями і можуть містити інформацію про дії користувачів, системні події та мережевий трафік. Загальний огляд сценарію управління журналами представлено на рисунку 1 [1].

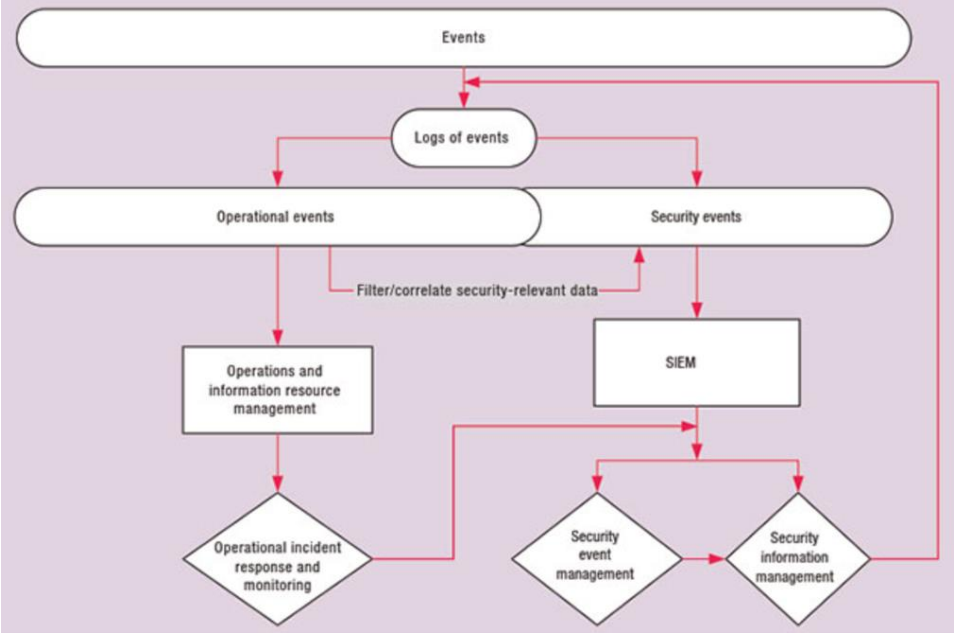


Рис. 1. Алгоритм управління журналами безпеки кінцевих точок організації з використанням SIEM [1]

Управління журналами відіграє важливу роль у кібербезпеці. Журнали забезпечують запис системної активності, який може бути використаний для ідентифікації подій безпеки та відстеження дій користувачів і зловмисників. Аналізуючи журнали, організації можуть виявити потенційні порушення безпеки, такі як несанкціонований доступ, зараження шкідливим програмним забезпеченням або витік даних, і вжити відповідних заходів для пом'якшення наслідків цих подій.

Основною проблемою в управлінні журналами є балансування між обмеженою кількістю ресурсів для управління журналами та безперервним постачанням даних журналів. Створення та зберігання логів ускладнюється, головним чином, великою кількістю джерел логів, неузгодженістю форматів логів між джерелами та великим обсягом даних логів на щоденній основі. Управління журналами також передбачає захист журналів від порушень їхньої конфіденційності та цілісності, а також підтримку їхньої доступності. Ще однією проблемою в управлінні журналами є те, що адміністратори повинні виконувати регулярний, ефективний та результативний аналіз даних журналів.

Системи SIEM відрізняються за своїми можливостями, але зазвичай усі вони пропонують наведені нижче основні функції [2]:

керування журналами. Системи SIEM збирають великий обсяг даних в одному місці, упорядковують їх, а потім визначають, чи є ознаки загрози, атаки або порушення безпеки;

кореляція подій. Потім дані сортуються для визначення зв'язків і закономірностей між ними, що дає змогу швидко виявляти потенційні загрози й реагувати на них;

моніторинг інцидентів і реагування на них. Технологія SIEM відстежує інциденти безпеки в корпоративній мережі, а також створює оповіщення й перевіряє всі дії, пов'язані з інцидентом.

Системи SIEM допомагають зменшувати ризики для кібербезпеки за допомогою низки сценаріїв використання, які активуються під час виявлення підозрілих дій користувачів, моніторингу поведінки користувачів, обмеження спроб доступу й створення звітів про відповідність.

WinCollect – це засіб пересилання подій Syslog, який адміністратори можуть використовувати для пересилання подій із журналів Windows до QRadar. WinCollect може збирати події з систем локально або бути налаштованим на віддалене опитування подій в інших системах Windows. WinCollect є одним з багатьох рішень для збирання подій Windows. WinCollect використовує API журналу подій Windows для збору подій, а потім WinCollect надсилає події до QRadar. Приклад керованого розгортання WinCollect показано на рисунку 2 [3].

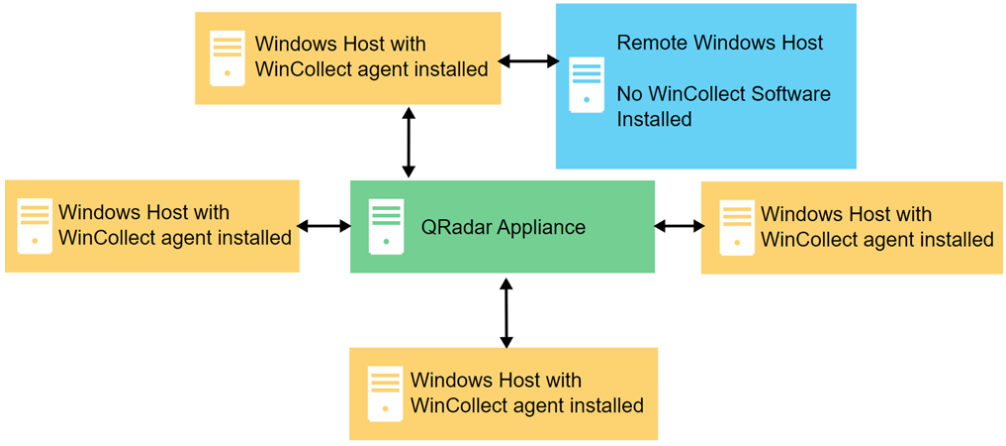


Рис. 2. Приклад керованого розгортання WinCollect для QRadar [3]

Отже, у сучасному складному цифровому середовищі, що швидко

розвивається, ефективне управління системними журналами стає все більш важливим аспектом управління IT-операціями та безпекою. Журнали є безцінним джерелом інформації про продуктивність системи, активність користувачів і події безпеки, надаючи організаціям інформацію, необхідну для усунення несправностей, моніторингу дотримання нормативних вимог, а також виявлення і реагування на загрози безпеці.

Перелік посилань:

1. Vasant Raval. The Practical Aspect: Challenges of Security Log Management. ISACA Journal. URL: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/the-practical-aspect-challenges-of-security-log-management. (дата звернення: 15.10.2023).

2. The Complete Guide to Log and Event Management. Dr. Anton Chuvakin, sponsored by NetIQ. URL: https://www.netiq.com/en-au/docrep/documents/m47h82fbmy/the_complete_guide_to_log_and_event_management_wp_ap.pdf. (дата звернення: 15.10.2023).

3. IBM QRadar Security Intelligence Platform 7.5. WinCollect 10 URL: https://www.ibm.com/docs/en/qsip/7.5?topic=configuring-wincollect-10. (дата звернення: 15.10.2023).

Саєнко Андрій Святославович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

АКТУАЛЬНІСТЬ ПРОТИДІЇ ПОШТОВОМУ СПАМУ

Будь-хто, хто користується Інтернетом і електронною поштою, знає про спам – ці небажані та дратівливі повідомлення у скриньці, які намагаються спонукати купити щось, надіслати гроші чи особисту інформацію, або натиснути посилання чи вкладення. Дещо з того, що люди вважають спамом, є законною, хоча й етично сумнівною рекламою, але спам також може бути інструментом для шахрайства та шкідливого програмного забезпечення, яке використовують хакери.

Сьогодні спам – це термін, який охоплює широкий спектр загроз кібербезпеці та небажаних повідомлень електронною поштою на пристроях. Технологічна фірма Cisco зазначає, що спам-лист може спричинити різноманітні проблеми, від незначних роздратувань до серйозної шкоди, включаючи крадіжку особистих даних.

Оцінки поширеності електронної пошти зі спамом відрізняються, частково через те, що люди по-різному сприймають це. Деякі опитування вказують на відсоток спаму в електронній пошті від 45% до 50%, тоді як інші говорять, що до 85% усього електронного трафіку сьогодні є спамом.

Більшість сьогоднішніх служб електронної пошти фільтрують спам, але фахівці з безпеки кажуть, що все одно важливо стежити за тим, що відкриває користувач, які посилання та вкладення натискає. Кіберзлочинці постійно вдосконалюють свої методи, щоб обійти фільтри та спробувати заманити людей. Наприклад, вони можуть спробувати вселити страх щодо (неіснуючої) помилки безпеки на пристрої або припустити, що користувач виграв приз або розіграш.

Хоча деякі зі спаму, який отримується, можуть стосуватися законних продуктів або послуг від реальних компаній, клацання спаму може відкрити скриньку ризиків Пандори. До них входить розміщення шкідливого програмного забезпечення на пристрої, яке може викрасти облікові дані пароля або створити

«бекдор» у пристрої для завдання шкоди.

Як зупинити спам

Ніхто не може повністю зупинити спам. Однак є кроки, які можна вжити, щоб обмежити ризик спаму для пристроїв і особистих даних і уникнути того, щоб стати жертвою онлайн-шахраїв.

- Використовувати спам-фільтри

Фільтри спаму входять до складу більшості служб електронної пошти у формі папки спаму, але можна налаштувати параметри фільтра, щоб вони були більш або менш агресивними. Також можна створити власні фільтри для папки «Вхідні» на основі певних критеріїв і визначити авторизованих відправників, яких не буде заблоковано.

- Зберігати свою електронну адресу приватною

Фахівці з безпеки радять не публікувати адресу особистої електронної пошти на форумах, веб-сторінках або в соціальних мережах, де вони можуть бути «зібрані» спамерами.

- Використовувати окремі облікові записи електронної пошти

Ще один спосіб приборкати спам — створити окремі особисті облікові записи електронної пошти або навіть тимчасову «викидну» електронну пошту для деяких типів онлайн-транзакцій. Навіть якщо цей тимчасовий обліковий запис зламано, можна створити інший.

- Ретельно вивчати повідомлення

Деякі спамові електронні листи видаються самі собою. Електронний лист може виглядати так, ніби він надійшов, наприклад, від PayPal, але якщо навести курсор миші на ім’я відправника, можна отримати адресу веб-сайту, яка не є PayPal. Також варто звертати увагу на орфографічні та граматичні помилки, які можуть бути спробою уникнути спам-фільтрів.

- Не відповідати на спам

Важливо не відповідати на спам. Відповідь дозволяє зловмисникам знати, що обліковий запис активний, потенційно відкриваючи двері для більшої кількості небажаних електронних листів.

Перелік посилань:
1. What Spam Email Is and How To Stop It URL: https://www.usnews.com/360-reviews/privacy/what-spam-email-is
2. Effective Anti-Spam Strategies in Companies: An International Study URL: https://www.researchgate.net/publication/4216229_Effective_Anti-Spam_Strategies_in_Companies_An_International_Study

Сайчук Вадим Дмитрович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ

Комп’ютерні мережі – сучасний вид зв’язку, без якого не можлива наша комунікація з зовнішнім світом. За допомогою мереж кожну секунду передаються сотні Гігабіт даних та інформації. Відбувається спілкування людей між собою на великих відстанях та у різних країнах. За допомогою мереж ми маємо доступ до усієї інформації, яка нам необхідна для роботи та життя. В той же час кіберзлочинці постійно намагаються отримати доступ до корпоративних мереж для того, щоб заволодіти конфіденційною інформацією великих компаній та особистою інформацією користувача, для подальшого її використання у незаконних цілях.

Для захисту мереж від кіберзлочинців, найчастіше користуються технічними системами та засобами захисту інформації в корпоративних мережах. Як основний засіб захисту від атак через мережу Інтернет на локальну мережу - використовують Брандмауер (firewall). Ці пристрої використовуються, як для захисту мережі в цілому, так і для захисту окремих комп’ютерів у даній мережі.

У локальних мережах брандмауер може бути на основі як програмного так і апаратного забезпечення, який забезпечує зв’язок між локальними (безпечними) та небезпечними (Інтернет) мережами.

Головна задача брандмауера – це перевірка трафіку, який проходить по усім каналам зв’язку, як захищених (SSH, SSL, TLS та ін.) так і незахищених (Telnet, http, SMTP на ін.). За допомогою відстеження мережевого трафіку він виявляє шкідливі програми (віруси, шпигунські програми і так далі) та блокує їх ще на вході у мережу.

Для захисту комп’ютера у мережі за часту використовуються антивірусні програми, які безпосередньо встановлюються на комп’ютер клієнта. Вони захищають інформації людини від неправомірного доступу до неї з мережі.

В даний час все частіше зустрічаються приклади використання цілих комплексів захисту інформації в мережі. Вони об’єднують як брандмауери, антивіруси так і постійний моніторинг трафіку в середині мережі та сповіщення про підозрілий контент.

З вище сказаного, можна зробити висновок, що технічні системи захисту інформації в корпоративних мережах є необхідною мірою захисту в сучасному цифровому світі. Вони повинні постійно розвиватись та удосконалюватись, тому що кіберзлочинці все частіше знаходять нові і нові методи доступу до даних в мережі, з метою подальшого їх заволодіння.

Перелік посилань:

1) Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013ю — 256 с.
2) Буров Є. В. Комп'ютерні мережі: підручник / Євген Вікторович Буров. — Львів: «Магнолія 2006», 2010. — 262 с.
3) Комп'ютерні мережі та телекомунікації : навч. посібник / В. А. Ткаченко, О. В. Касілов, В. А. Рябик. – Харків: НТУ "ХПІ", 2011. – 224 с.

Самаренко Віталій Владиславович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА ДЛЯ ВІДДАЛЕНИХ КОРИСТУВАЧІВ НА БАЗІ VPN.

Інформаційні системи підприємств зіштовхуються зі збільшенням віддалених користувачів, що підкреслює важливість технології VPN для забезпечення безпечного віддаленого доступу. У цій тезі аналізуються різні аспекти використання VPN-рішень з метою забезпечення захисту даних та забезпечення цілісності інформаційних систем. Розглядається два протоколи VPN, їх переваги та недоліки, а також методи забезпечення безпеки. Стаття несе ціль більше розкрити тему, щодо вибору та налаштування VPN-рішень для забезпечення безпеки та ефективності віддаленого доступу.

Існують різні типи VPN-рішень, включаючи віддалений доступ через L2TP/IPSec та мережі, які використовують протокол OpenVPN.

IPsec VPN: IPsec (Internet Protocol Security) – це протокол, який забезпечує шифрування та автентифікацію даних, надаючи високий рівень безпеки. IPsec VPN-рішення зазвичай використовуються для створення безпечних з'єднань між окремими пристроями або між мережами. Вони підходять для широкого спектру додатків та надають сильний захист даних.

L2TP/IPsec VPN: Це комбіноване рішення, яке використовує L2TP (Layer 2 Tunneling Protocol) для створення тунелю між клієнтом та сервером, а потім IPsec для шифрування даних. Воно надає високий рівень безпеки та підходить для різних сценаріїв, включаючи віддалений доступ.

OpenVPN: Це VPN протокол з відкритим кодом. Кожен може переглянути код або перевірити наявність уразливостей. Це дуже безпечна система тунелювання, яка працює як на протоколах безпеки TCP, так і на UDP, а також на SSL/TLS для обміну ключами. Зазвичай OpenVPN вважається достатньо компетентним в обході більшості брандмауерів. Однак одна з проблем OpenVPN полягає в тому, що це найскладніший протокол VPN для налаштування.[1]

Переваги та недоліки обох протоколів:

L2TP/IPsec:

Переваги:

1. Безпека: IPsec забезпечує високий рівень безпеки із шифруванням даних на рівні мережевого стека. Це робить L2TP/IPsec надійним протоколом захисту даних.
2. Сумісність: L2TP/IPsec широко підтримується на різних операційних системах та пристроях, включаючи Windows, MacOS, iOS та Android.

3. Двофакторна аутентифікація: L2TP/IPsec підтримує двофакторну аутентифікацію, що підвищує безпеку.
4. Підтримка мобільних пристроїв: Він добре працює на мобільних пристроях, що робить його придатним для співробітників, які використовують смартфони та планшети.

Недоліки:

1. Швидкість: IPsec може додавати невелике навантаження на мережу через шифрування, що може знижувати швидкість передачі даних.
2. Блокування портів: Деякі громадські Wi-Fi та корпоративні мережі можуть блокувати порти, що використовуються L2TP/IPsec, що може спричинити проблеми з підключенням.

OpenVPN:

Переваги:

1. Гнучкість: OpenVPN є відкритим та гнучким протоколом, який може працювати на різних портах та протоколах (TCP та UDP).
2. Висока продуктивність OpenVPN часто забезпечує хорошу продуктивність і може бути налаштований для оптимізації.
3. Підтримка IPv6: OpenVPN підтримує IPv6, що є важливим для сучасних мереж.
4. Безліч платформ: Він підтримує безліч операційних систем та платформ, включаючи Linux, Windows, macOS та інші.

Недоліки:

1. Налаштування може бути складним: Налаштування OpenVPN може вимагати більше часу та знань, ніж L2TP/IPsec.
2. Сумісність на мобільних пристроях: Налаштування OpenVPN на мобільних пристроях може вимагати встановлення додаткових програм.
3. Блокування портів: Як і L2TP/IPsec, OpenVPN може бути заблокований на деяких мережах, якщо використовуються нестандартні порти.

У підсумку обидва протоколи мають свої сильні сторони і вибір залежить від конкретних потреб підприємства, його розмірів і зважаючи на його бюджет. Якщо підприємство середнього типу, але важлива висока безпека та сумісність із різними пристроями, L2TP/IPsec може бути гарним вибором. Якщо підприємство великого розміру та має можливість мати власний IT відділ та потрібна гнучкість та висока продуктивність, OpenVPN може підійти краще.

Перелік посилань:

1. Different Types of VPN Protocols (Tunnels) & VPN Types Explained URL: https://crm.org/news/types-of-vpn (дата звернення: 22.10.2023).
2. Eric F. Crist, Jan Just Keijser, book, "Mastering OpenVPN", Packt Publishing, 2015

Самойленко Владислав Олексійович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

РОЛЬ ЛЮДСЬКОГО ФАКТОРУ У КІБЕРБЕЗПЕЦІ КОРПОРАТИВНИХ СИСТЕМ

В сучасному світі, де кіберзлочинці постійно шукають нові способи доступу до конфіденційної інформації, корпоративні системи є особливо уразливими. Однак, необхідно враховувати, що більшість атак на ці системи здійснюється через помилки, недбалість або недосвід користувачів, тобто через людський фактор. Користувачі, використовуючи незахищені канали зв'язку, нерідко передають бізнес-інформацію через власні слабозахищені пристрої зв'язку. Співробітники, використовуючи переглядають поштові скриньки організації та особисті, що створює можливість для кіберзлочинців вчиняти онлайн-шахрайства. Зловмисники можуть отримати віддалений доступ до пристроїв, дізнавшись особисту і корпоративну інформацію, використовуючи фішинг та методи соціальної інженерії через заражені посилання у повідомленнях та електронній пошті.

Розуміння ролі людського фактору в кібербезпеці та пошук шляхів мінімізації ризиків, є надзвичайно важливими завданнями. Шляхи мінімізації цих ризиків включають у себе посилення освіти користувачів про фішинг та соціальну інженерію, впровадження міцних аутентифікаційних методів та надійних криптографічних засобів зв'язку, а також створення суворих політик безпеки щодо використання пристроїв в корпоративних інформаційних системах.

Недостатньо освічені користувачі часто стають легкою мішенню для кіберзлочинців. Вони можуть приймати неправильні рішення, не дотримуватися правил безпеки та не розпізнавати шкідливі посилання чи відкриті файли. Тому одним зі способів мінімізації ризиків є підвищення культури кібербезпеки серед співробітників. Для досягнення цієї мети можна проводити навчання та тренінги з питань кібербезпеки, розробляти політику безпеки організації, встановлювати системи контролю та моніторингу, а також створювати свідомість серед співробітників щодо важливості дотримання правил безпеки.

Крім того, впровадження технологій, які допомагають запобігти помилкам або зловмисним діям, також є важливим елементом захисту від ризиків, пов'язаних з людським фактором. Такі технології можуть включати системи автоматичного виявлення витоку даних, програми забезпечення безпеки електронної пошти та захисні фаєрволи.

Політики безпеки також важливі для забезпечення захисту корпоративних систем. Вони встановлюють стандарти та процедури, які допомагають забезпечити безпеку інформаційних систем.

Отже, важливо зрозуміти, що людський фактор може бути знижений через правильне навчання та освіту. Тренінги з кібербезпеки для персоналу, що включають навчання з розпізнавання фішингових атак, використання сильних паролів та основ безпечного використання Інтернету, можуть бути корисними

для захисту корпоративних систем. Ці рекомендації можуть допомогти організаціям знизити ризики, пов'язані з людським фактором, та забезпечити вищий рівень безпеки їх інформаційних систем.

Перелік посилань:
1. Людський фактор у кібербезпеці: розуміння поведінки користувачів URL: https://shorturl.at/huNUX (дата звернення: 24.10.2023).
2. Захист даних бізнесу: основне про кібербезпеку URL: https://ua.gbc-time.com/article/zahist-danih-biznesu-osnovne-pro-kiberbezpeku66163.html (дата звернення: 24.10.2023).
3. Як компанії вирішують кібервиклики вже сьогодні URL: https://rubryka.com/blog/cyber-challenges/ (дата звернення: 24.10.2023).
4. Секрети кібербезпеки: 5 ключових правил безпеки в Інтернеті URL: https://eba.com.ua/sekrety-kiberbezpeky-5-klyuchovyh-pravyl-bezpeky-v-interneti/ (дата звернення: 24.10.2023).

Сарапіна Аліна Костянтинівна, студентка
Навчально-науковий інститут захисту інформації, ДУІКТ
Київ, Україна

ЗАПОБІГАННЯ ЗАГРОЗ ПОВ'ЯЗАНИХ З IAM В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Концепція кібербезпеки в корпоративному секторі охоплює низку стратегій, політик і практик, які захищають корпоративну інформацію, інфраструктуру та ресурси від кіберзагроз. В умовах постійного зростання і зміни загроз інформаційна безпека є найважливішим аспектом для всіх організацій, незалежно від їхнього розміру. Варто підкреслити важливість ресурсів керування доступом (IAM) для забезпечення безпеки інформаційних систем підприємства та розглядати різноманітні інструменти та практики IAM, які допомагають захистити ресурси підприємства від несанкціонованого доступу та кібератак. А саме, якісне управління правами, моніторингу та ідентифікації користувачів для забезпечення високого рівня безпеки інформаційних систем компаній.

Для запобігання загрозам в корпоративних інформаційних системах значну увагу приділяють до:

- управління ідентичністю і доступом (IAM)
- захист даних і конфіденційності
- моніторинг і виявлення інцидентів розробки та впровадження політик безпеки та планів відновлення після інцидентів (IRP)
- захист від зловмисних програм та зломів
- дотримання нормативних вимог і стандартів.

Використовуючи ці методи й аспекти кібербезпеки, організації можуть забезпечити захист своєї інформації, дотримуватися правових норм або захистити корпоративні системи та дані. Управління кібербезпекою вимагає постійного вдосконалення й адаптації до загроз і технологій, що виникають. Система керування доступом (IAM) може зіткнутися з багатьма різними проблемами, які впливають на її ефективність і безпеку. Наразі, найактуальніші з них це:

- слабка аутентифікація
- недостатні права і доступи

- недостатня безпека привілеїв
- недостатня відновлення після інцидентів (IRP)
- відсутність плану відновлення після інциденту може ускладнити реагування на кіберінциденти і відновлення нормальної роботи
- недостатня автоматизація процесів
- соціальна інженерія і інсайдерські загрози
- недостатній моніторинг та аудит
- системні помилки і вразливості
- недостатня комплексність інтеграції.

Надмірний доступ і обмеження можуть негативно вплинути на продуктивність працівників, обмежуючи їхні здібності. Також необхідно враховувати інші аспекти, які можуть стати проблемою для організації. Наприклад, неадекватна інтеграція системи IAM з іншими системами в організації може призвести до проблем з керуванням доступом і автентифікацією. Якщо система IAM не працює ефективно з іншими компонентами інфраструктури, може знадобитися ручне втручання та ускладнити процеси. Якщо належний аудит і моніторинг привілеїв не забезпечено, це може створити можливості для зловживань і несанкціонованого доступу до ресурсів. Відсутність плану відновлення мережевих інцидентів може ускладнити реагування на інциденти та відновлення нормальної роботи. Автоматизація контролю доступу може підвищити продуктивність і знизити витрати, але без належного контролю та моніторингу вона також може призвести до серйозних проблем. Виявлення системних помилок і вразливостей безпеки в IAM може стати відправною точкою для кібератак і порушень безпеки. Загалом, щоб забезпечити ефективне та безпечне керування доступом, важливо враховувати всі ці проблеми та вживати відповідних заходів для їх запобігання та подолання.

1. Що таке керування ідентифікацією? | Enterprise Identity Management Solutions: https://hideez.com/uk-ua/blogs/news/identity-and-access-management

Святська Надія Андріївна
студентка групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ФОРМУВАННЯ ОБІЗНАНОСТІ Й НАВЧАННЯ ПЕРСОНАЛУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В роботі розглянуті важливість формування обізнаності та навчання персоналу з інформаційної безпеки та онлайн-ресурси, які можуть полегшити IT-компаніям навчання персоналу.

Формування обізнаності та навчання персоналу з інформаційної безпеки є невід’ємним завданням для будь-якої організації, оскільки кількість загроз та їх негативні наслідки постійно зростають. Інформаційна безпека стає все більшим пріоритетом, оскільки порушення безпеки можуть призвести до серйозних

фінансових, репутаційних та юридичних наслідків для організації.

Ефективні програми навчання та освіти з інформаційної безпеки допомагають співробітникам розуміти ризики, виявляти потенційні загрози та приймати заходи для їх запобігання. Організації також повинні постійно оновлювати свої підходи до навчання, оскільки загрози розвиваються разом із технологіями та тактиками злочинців. Усі ці зусилля спрямовані на забезпечення максимального рівня безпеки і довіри в інформаційних системах організації. [1]

Фішинг-шахрайство, слабкі паролі та скомпрометовані акаунти сьогодні є поширеними причинами витоку даних та фінансових втрат для підприємств. Навчальні платформи з підвищення обізнаності про безпеку надають користувачам доступ до навчальних матеріалів з таких питань, як кібербезпека. Платформи для підвищення обізнаності з питань безпеки також дозволяють адміністраторам створювати навчальні кампанії з інтерактивними вікторинами та тестами, щоб переконатися, що користувачі навчаються і взаємодіють з матеріалами.

Формування обізнаності рекомендується систематизувати та проводити згідно плану, який розроблений як окремо для кожного працівника компанії, так і для всього персоналу разом. Для найкращого результату рекомендується спочатку провести ретельну оцінку загроз та слабких місць у організації. Навчання працівників повинно бути направлене на прогалини в їх навичках або на вже існуючі загрози. [2]

Враховуючи особливості сприйняття матеріалу різними поколіннями, зараз навчання буде більш спрямоване на онлайн-ресурси, використання штучного інтелекту та засвоєння матеріалу через геймінг або симуляції. Наразі є чимало ресурсів, що дозволяють компаніям обирати кращу для їх персоналу базу матеріалів та досягати поставленої мети у обізнаності персоналу.

TryHackMe - це одна з найпопулярніших онлайн-платформ, яка призначена для навчання та розвитку навичок в галузі кібербезпеки та інформаційної безпеки. Ця платформа використовує гейміфікацію для створення навчальних завдань, головоломок та ігор, які роблять процес навчання більш захоплюючим та мотивуючим. TryHackMe постійно оновлюється, враховуючи нові загрози та тенденції в кібербезпеці, а персонал розвиває свої навички на основі практичного досвіду, що отримує з цієї платформи.

Hack The Box (HTB) - це онлайн-платформа, що дозволяє перевірити свої навички тестування на проникнення та обмінятися ідеями та методологіями з іншими учасниками зі схожими інтересами. Вона містить багато завдань, які постійно оновлюються. Деякі з них імітують реальні сценарії, а деякі більше наближені до CTF.

Ще однією онлайн-платформою що орієнтована на навчання людей через вирішення симульованих завдань з кібербезпеки. Змагання "Capture the Flag", або просто CTF, популярні серед спільноти. Перед учасниками ставлять ряд завдань, які перевіряють їхню креативність, технічні навички та вміння вирішувати проблеми.

Важливо, щоб хороша навчальна платформа з підвищення обізнаності

щодо безпеки надавала IT-командам дані та аналітику, які показують, які користувачі в організації мають найбільший ризик спричинити витік даних, а також надавала адміністраторам інструменти для допомоги користувачам, які її найбільше потребують. [3]

Навчання для підвищення обізнаності про безпеку має бути важливим компонентом надійної стратегії кібербезпеки для компаній будь-якого розміру. Компанії повинні прагнути навчити персонал крокам, які вони можуть зробити, щоб захистити себе і мережу компанії, коли вони стикаються з низкою реальних викликів кібербезпеки, навчаючи їх мислити незалежно і критично.

Перелік посилань:

1. Security Awareness Training URL: https://manufacturerstores.techdata.com/docs/default-source/carbonite/webroot_security_awareness_training_smb.pdf?sfvrsn=2
2. The Top 10 Security Awareness Training Solutions For Business URL: https://expertinsights.com/insights/the-top-security-awareness-training-platforms-for-businesses/
3. The Importance of Cyber Security Awareness Training for Employees URL: https://www.elev8me.com/insights/the-importance-of-cyber-security-awareness-training-for-employees

Селіванов Іван Сергійович
студент групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

ОЦІНКА ЕФЕКТИВНОСТІ ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ В ОРГАНІЗАЦІЯХ

Зараз на данний час компанії мають більш уважно стежити за безпекою передачі інформації в середині них. З переходом у еру масової цифровізації складно стало конролювати потік інформації в структурі копманії. Тому їм потрібно ефективно запобігати витокам інформації в середині системи та використовувати ефективні заходи для подолання цієї проблеми ,щоб у майбутньому у результаті витоку інформації компанія збанкротувала .

Захист інформації – це сукупність організаційних, технічних та правових заходів, спрямованих на запобігання нанесенню збитків інтересам власника інформації.

Розглянемо об`єкти які мають захищати компанії ,які хочуть запобігти витоку інформації у себе на підприємстві .

Основними об'єктами захисту інформації є [1 – 3]:

1.Інформація з обмеженим доступом (ІзОД), тобто інформаційні ресурси, зокрема, ті, що містять відомості, які належать або до таємної, або до конфіденційної інформації;

2. Технічні засоби приймання, обробки, зберігання та передання інформації, а саме:

а) системи та засоби інформатизації (обчислювальна техніка, інформаційно-обчислювальні комплекси, мережі та системи);

б) програмні засоби (операційні системи, системи керування базами даних та інше загально системне і прикладне програмне забезпечення);

в) автоматизовані системи керування; системи зв'язку; технічні засоби отримання, передання та обробки ІзОД (звукозапис, звукопідсилення, звуко

супроводження, переговорні та телевізійні пристрої;

г) засоби тиражування і виготовлення документів та інші технічні засоби обробки графічної, алфавітно-цифрової та текстової інформації), їх інформативні фізичні поля;

3. Допоміжні технічні засоби і системи (ДТЗС), тобто технічні засоби і системи, які не належать до ТЗПІ, але розташовані в приміщеннях, де обробляється ІзОД, до них відносять технічні засоби відкритого телефонного або гучномовного зв'язку, системи пожежної та охоронної сигналізації, система енергопостачання, радіотрансляційна мережа, система часофікації, енергопобутові прилади тощо, а також самі приміщення, де циркулює ІзОД.

Поговоримо про захист інформації від витоку, вони забезпечуються технічними каналами, проектно-архітектурними рішеннями та проведенням організаційних і технічних заходів, а також виявленням портативних закладних пристроїв [4].

Далі розглянемо методи й засоби блокування каналів витоку інформації –

1. Організаційні заходи – це спрямовані на захист інформації заходи, проведення яких не потребує спеціально розроблених технічних засобів. До основних організаційних заходів відносять:

а) залучення до робіт для захисту інформації організацій, що мають ліцензії відповідних органів на діяльність в області технічного захисту інформації (ТЗІ);

б) категорування й атестацію об'єктів ТЗПІ та приміщень, виділених для проведення секретних заходів (виділених приміщень) щодо відповідності вимогам забезпечення захисту інформації під час проведення робіт з відомостями відповідного ступеня секретності;

в) використання на об'єкті сертифікованих ТЗПІ та ДТЗС;

г) встановлення КЗ навколо об'єкта;

д) залучення до робіт із монтування апаратури, будування чи реконструкції об'єктів ТЗПІ організацій з відповідними ліцензіями;

2. Технічні заходи - це спрямовані на захист інформації заходи, проведення яких передбачає використання спеціальних технічних засобів, а також реалізацію технічних рішень.

Технічні заходи слугують для закриття каналів витоку інформації за рахунок ослаблення рівня інформаційних сигналів або зменшення відношення сигнал /завада у місцях можливого розміщення ТЗР або їх датчиків до рівнів, що унеможливлюють виділення інформаційних сигналів засобами розвідки. Під час проведення таких заходів використовують активні та пасивні методи

Таким чином, безпека досягається комплексним застосуванням апаратних, програмних і криптографічних методів, і засобів захисту, а також організаційних заходів.

Висновок

Швидкий, але поступовий розвиток сучасних технологій і технічних засобів сприяє постійному розширенню спектра можливих каналів витоку інформації, тому дослідження каналів витоку стає все більше актуальним, і

складним завданням.

На ефективність систем безпеки істотно впливають характеристики каналів витоку інформації, тому створення систем ефективного захисту має відбуватися з урахуванням особливостей реальних каналів.

Перелік посилань:

1.Лаврентьев А. В. Организация в офисах защиты информации от утечки по техническим каналам. – Безопасность информации. – 1996. - № 3. – С. 62 – 66.

2.Лаврентьев А. В. Анализ технических каналов утечки информации и классификация технических средств разведки. - Безопасность информации. 2000. - №4. – С. 32 – 38.

3.Архипов О. Є, Луценко В. М., Худяков В. О. Захист інформації телекомунікаційних мережах та системах зв'язку: Учеб. пособие. - К.: Політехніка, 2003 – 38 с.

4.Куренков Е. В., Лысов А. В., Остапенко А. Н. Рекомендации по оценке защищенности конфиденциальной информации от ее утечки за сет ПЭМИ.

Сергеєв Сергій Олегович, БСДМ-63
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ В AMAZON WEB SERVICES З ВИКОРИСТАННЯМ FORTIGATE CNF

Визначено мету і основні завдання щодо захисту корпоративних інформаційних ресурсів в Amazon Web Services з використанням FortiGate CNF. Розглянуто зміст технології захисту корпоративних інформаційних ресурсів в Amazon Web Services з використанням FortiGate CNF.

У сучасному світі з високим рівнем взаємозв'язку вихідний трафік з хмарних мереж став основною проблемою безпеки для бізнесу. Зростаюча залежність від хмарних технологій призвела до збільшення потенційних загроз, таких як витік даних, розповсюдження шкідливого програмного забезпечення, створення бот-мереж і надмірно великі обсяги вихідного трафіку. Щоб протистояти цим ризикам, організаціям потрібне рішення, яке може ефективно убезпечити хмарні мережі та забезпечити захист конфіденційних даних. FortiGate CNF - це комплексне рішення для захисту хмарних мереж, що дозволяє знизити ці ризики. Рішення забезпечує узгоджену політику безпеки для декількох хмарних облікових записів і мереж, тим самим знижуючи ймовірність інцидентів, пов'язаних з безпекою. Завдяки своїм надійним функціям безпеки FortiGate CNF забезпечує захист від витоку даних, допомагає запобігти поширенню шкідливого програмного забезпечення, зупиняє утворення бот-мереж і контролює надмірні обсяги вихідного трафіку [1].

FortiGate Cloud-Native Firewall (CNF) - це сервіс брандмауера наступного покоління, що надається як SaaS, яка спрощує безпеку хмарних мереж, одночасно забезпечуючи доступність і масштабованість. FortiGate CNF зменшує робоче навантаження на мережеву безпеку, усуваючи необхідність в

конфігуруванні, забезпеченні та підтримці будь-якої програмної інфраструктури брандмауера, дозволяючи командам безпеки зосередитися на управлінні політикою безпеки [1].

Рішення FortiGate CNF - це керований сервіс безпеки хмарної мережі, призначена для надання клієнтам можливостей брандмауера нового покоління (NGFW) у спрощеному та легкому у використанні вигляді. Сервіс є доступним для віртуальних приватних хмар Amazon Web Services (AWS). Щоб скористатися CNF, клієнтам просто потрібно вибрати хмарні мережі, які вони хочуть захистити, приєднати їх до ініційованого ними екземпляру CNF і визначити політику безпеки, яку вони хочуть застосувати. CNF подбає про все інше, включаючи управління інфраструктурою, масштабування та виправлення вразливостей коду.

Клієнти можуть визначати свої політики безпеки за допомогою простої та інтуїтивно зрозумілої мови політик, які CNF впроваджує на мережевому рівні. Політики можуть бути налаштовані відповідно до конкретних потреб, включаючи блокування шкідливих IP-адрес, створення географічних огорож навколо хмарних робочих навантажень і забезпечення безпеки хмарної мережі зі сходу на захід за допомогою динамічних об'єктів, що усуває необхідність змінювати політики щоразу, коли робоче навантаження переміщується.

CNF - це регіональний сервіс, кожен екземпляр якого працює в одному регіоні AWS. Таке розгортання забезпечує високу доступність і масштабованість, дозволяючи клієнтам розгортати тестові CNF в одному регіоні, а робочі CNF - в інших регіонах, або розгортати сезонні CNF у певних регіонах за потреби. Послуга особливо підходить для клієнтів з дуже мінливими і непередбачуваними моделями використання і трафіку, оскільки дозволяє їм зосередитися на управлінні політиками безпеки, а не на інфраструктурі та обслуговуванні рішення для забезпечення мережевої безпеки.

В цілому, CNF надає клієнтам спрощене і просте у використанні рішення мережевої безпеки, яке дозволяє їм визначати, застосовувати і ефективно управляти своїми політиками безпеки, усуваючи при цьому необхідність інвестувати інженерні ресурси в створення власного рішення.

FortiGate CNF призначений для задоволення потреб двох типів клієнтів. До першого типу відносяться існуючі клієнти Fortinet, які використовують FortiManager для управління своїм парком FortiGate в локальних і хмарних середовищах. FortiGate CNF є ідеальним рішенням для цих клієнтів, оскільки він надає просте у впровадженні рішення FortiOS NGFW, яке вирішує проблеми безпеки хмарних мереж, які складніше вирішити за допомогою існуючих віртуальних машин FortiGate, наприклад, вихідний трафік. Крім того, цим клієнтам може знадобитися послуга, яка керує доступністю, масштабованістю та оновленням програмного забезпечення для забезпечення мережевої безпеки для конкретних хмарних робочих навантажень. Другий тип клієнтів, на яких орієнтується CNF, - це ті, кому потрібне хмарне рішення мережевої безпеки SaaS, яке постійно розвивається за двома основними сценаріями використання. По-перше, безпека вихідного трафіку, що включає блокування шкідливих IP-адрес і

створення географічних огорож навколо хмарних робочих навантажень, враховуючи, що більша частина їх трафіку зашифрована, що робить IPS менш важливим. По-друге, безпека хмарної мережі зі сходу на захід, яка використовує динамічні об'єкти, усуваючи таким чином необхідність змінювати політики щоразу, коли робоче навантаження переміщується. Крім того, ці клієнти також розуміють, що IPS менш критична, оскільки більша частина їх трафіку зашифрована [1].

FortiGate CNF забезпечує надійну безпеку будь-якого масштабу для середовищ AWS. Fortinet керує інфраструктурою надання послуг, спрощуючи операції безпеки мережі та знижуючи витрати. FortiGate CNF поєднує в собі такі можливості брандмауера наступного покоління (NGFW), як система запобігання вторгненням (IPS), веб-фільтрація, безпека системи доменних імен (DNS) тощо з явними перевагами хмари (рис. 1) [2].

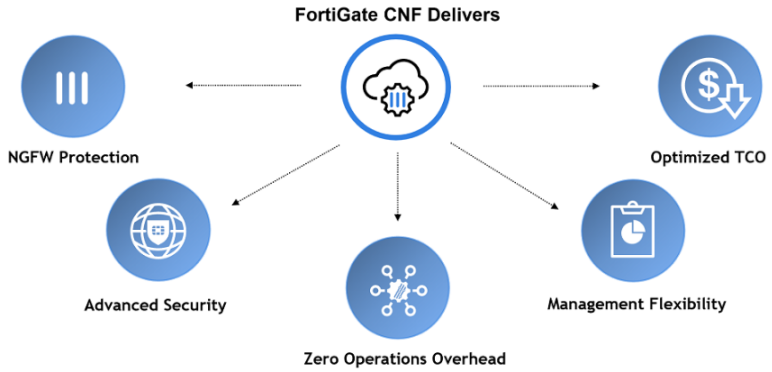


Рис. 1. Зміст технології FortiGate CNF [2]

Отже, сервіс керованого брандмауера FortiGate CNF дозволяє розвантажити обслуговування інфраструктури безпеки, отримати глибоку видимість, застосувати надійні елементи керування та оптимізувати витрати на безпеку хмари. Хмарна безпека тепер є імперативом для бізнесу. Організаціям потрібне рішення безпеки мережі в хмарі, яке пропонує розширений захист, гнучкість і передбачувані витрати. FortiGate CNF базується на FortiOS, розробленій для стабільної роботи в будь-якому середовищі. Цей унікальний підхід забезпечує загальну безпеку мережі в хмарі AWS і локальних середовищах.

Перелік посилань:

1. FortiGate CNF CloudNative Firewall Service. Data Sheet. Fortinet. URL: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-cnf.pdf. (дата звернення: 29.09.2023).
2. Extended Detection and Response. URL: https://www.fortinet.com/products/fortixdr. (дата звернення: 29.09.2023).

Середа Артем Олександрович
студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ АНОМАЛІЙ В МЕРЕЖЕВОМУ ТРАФІКУ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ CISCO SECURE NETWORK ANALYTICS

Своєчасне виявлення загроз та аномалій у мережевому трафіку є досить важливим аспектом у кібербезпеці. Швидке виявлення та усунення незвичних шаблонів поведінки може запобігти витоку даних, кібератакам та враженню системи. Раннє виявлення аномалій у мережі дозволяє негайно реагувати та запобігати інцидентам, зменшуючи потенційну шкоду та мінімізуючи час простою. Своєчасне виявлення аномалій підвищує загальну безпеку мережі і збільшує здатність організації захищати конфіденційну інформацію та підтримувати повну працездатність мережі без зупинок.

Cisco Secure Network Analytics (CSNA) - це інноваційна платформа для аналізу та моніторингу мережевого трафіку, яка допомагає організаціям зберігати безпеку своєї мережі та даних у цифровому середовищі. Інтегруючи передові технології машинного навчання та біхевіористики. CSNA надає засоби виявлення загроз та аномалій у мережевому трафіку, сприяючи вчасному реагуванню на потенційні загрози та захисту мережевої інфраструктури. Ця платформа є необхідною для організацій, які прагнуть підвищити рівень безпеки та мережевого управління.

CSNA використовує ряд передових технологій для ефективного виявлення загроз у мережевому трафіку. Ці технології включають:

- **Flow Data Analysis**: збирає та аналізує дані потоку, такі як записи NetFlow, sFlow та IPFIX, які надають детальну інформацію про потоки мережевого трафіку. Він відстежує схеми зв'язку між пристроями, включаючи IP-адреси джерела та призначення, порти, протоколи тощо, щоб виявити незвичні схеми трафіку та аномалії.

- **Behavioral Analytics**: Машинне навчання та і поведінкова аналітика використовуються для встановлення базових показників мережевої активності, створюючи профілі нормальної поведінки для мережевих об'єктів (пристроїв, користувачів, додатків). Відхилення від цих базових показників викликають сповіщення про потенційні загрози або аномалії.

- **Anomaly Detection**: використовує техніки виявлення аномалій для ідентифікації відхилень від встановлених норм мережевого трафіку. Цей підхід є важливим для ідентифікації загроз "нульового дня" та нових загроз в сфері

- **Threat Intelligence Integration**: може інтегруватися із зовнішніми каналами та базами даних для розширення можливостей виявлення загроз. Зіставляючи мережеву активність з відомими індикаторами загроз, CSNA може

ще ефективніше ідентифікувати та пріоритетизувати можливі загрози безпеці.

- User and Entity Behavior Analytics (UEBA): використовує аналітику поведінки користувачів і об'єктів для відстеження поведінки користувачів та об'єктів мережі, що допомагає виявляти загрози внутрішніх користувачів і незвичні дії, які можуть вказувати на несанкціонований доступ або витік даних.

- Integration with Other Security Solutions: може інтегруватися з іншими продуктами та технологіями забезпечення безпеки Cisco, такими як Cisco Firepower, Cisco Identity Services Engine (ISE) та Cisco Threat Grid, для створення всебічної екосистеми безпеки і покращення можливостей виявлення аномалій.

- Machine Learning Models: використовує різні моделі машинного навчання для різних аспектів виявлення загроз, включаючи аналіз поведінки користувачів та об'єктів (UEBA) для ідентифікації загроз внутрішніх та мережевих аномалій.

Ці технології і підходи роблять Cisco Security Network Analytics одним з найкращих рішень для виявлення аномалій та загроз у мережевому трафіку. Він безперервно відстежує мережеву активність, аналізує дані в реальному часі та надає командам з безпеки необхідну інформацію для швидкого реагування на можливі загрози організації.

Перелік посилань:
1. Cisco Secure Network Analytics (Stealthwatch) - Cisco URL: https://www.cisco.com/c/en_hk/products/security/stealthwatch/index.html
2. Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet URL: https://www.niap-ccevs.org/MMO/Product/st_vid11313-agd7.pdf

Сизоненко Артем Олександрович, БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ДОСТУПУ ГІБРИДНИХ ПРАЦІВНИКІВ ДО КОРПОРАТИВНИХ ДОДАТКІВ НА БАЗІ FORTINET UNIVERSAL ZTNA

Визначено мету і основні завдання щодо забезпечення безпечного доступу гібридних працівників до корпоративних додатків. Розглянуто зміст технології забезпечення безпечного доступу гібридних працівників до корпоративних додатків на базі Fortinet Universal ZTNA.

Сьогодні зростає увага до забезпечення роботи кінцевих користувачів

організацій у відповідності до стратегій нульової довіри та хмарних технологій, а також прагнення забезпечити більш безпечне та адаптивне підключення для гібридних робочих груп, викликає інтерес до ринку доступу до мережі з нульовою довірою (zero-trust network access, ZTNA). Організації в першу чергу розглядають рішення ZTNA як заміну VPN, причому їх основною мотивацією є зменшення ризиків, а не зниження витрат [1].

ZTNA на основі агентів все частіше впроваджується як частина ширшої архітектури послуг безпечного доступу (secure access service edge, SASE) або з хмарною службою безпеки (security service edge, SSE), щоб замінити традиційні постійно увімкнені VPN, які зазвичай пропонують комплексний стек мережевої безпеки для віддалених керованих пристроїв. Тим часом, безклієнтська ZTNA продовжує підтримувати сторонні рішення і рішення на основі стратегії BYOD [1].

Оскільки гібридна робоча сила стає новою нормою, співробітники повинні мати безпечний доступ до всіх своїх робочих програм із різних місць. Fortinet Universal ZTNA забезпечує безпечний доступ до додатків, розміщених де завгодно, незалежно від того, чи працюють користувачі віддалено чи в офісі [2].

Рішення Fortinet Universal ZTNA є частиною всієї операційної системи організації: воно є унікальним масштабованим та гнучким як для розгортання в хмарі, так і для локальних розгортань, охоплюючи користувачів незалежно від того, перебувають вони в офісі чи віддалено. Fortinet Universal ZTNA забезпечує мережу контрольних точок, організовану FortiClient EMS, яка створює архітектуру з низькою затримкою, де ми можемо застосовувати перевірки безпеки поверх елементів керування ZTNA (рис. 1) [2].

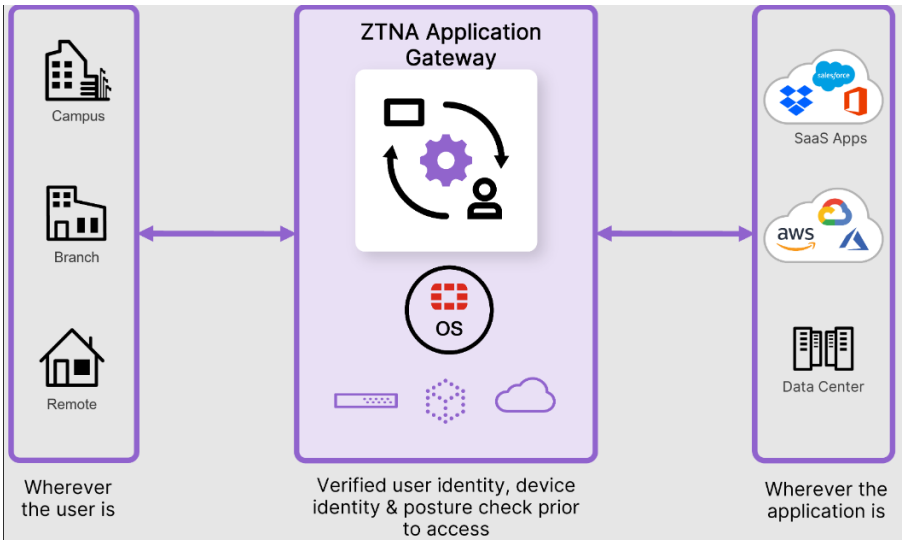


Рис. 1. Місце Fortinet Universal ZTNA в операційній системі організації [2]

Для того, щоб впровадити технологію забезпечення безпечного доступу гібридних працівників до корпоративних додатків на базі Fortinet Universal ZTNA керівники з безпеки та управління ризиками, відповідальні за безпеку

інфраструктури , повинні реалізувати стратегію нульової довіри високого рівня. Спершу необхідно визначити можливості для зменшення ризиків і переконатися, що технології та процеси керування ідентифікацією та доступом в організації добре зрозумілі та зрілі, перш ніж вибрати та запровадити рішення ZTNA.

Розгортання технології ZTNA має бути поетапним проектом, який потребує керівництва зацікавленими сторонами для зменшення операційного негараздів. Необхідно визначити або високочутливі додатки для захисту, щоб максимізувати рентабельність інвестицій зі зниження ризику, або додатки з низьким рівнем ризику та технічно підготовлених пілотних користувачів, щоб мінімізувати будь-який потенційний вплив на роботу. Згодом необхідно запровадити технологію ZTNA для більшої кількості додатків і користувачів [1].

При застосуванні цільових BYOD (bring-your-own-device) і у випадках використання розширеної робочої сили необхідно заміняти VPN віддаленого доступу безклієнтським ZTNA. Необхідно консолідувати ZTNA на основі агентів як частину ширшої архітектури SASE, щоб розширити повний стек мережевої безпеки, який може замінити постійно активні реалізації VPN.

Також необхідно надавати перевагу постачальникам, які відповідають широким вимогам безпеки для керованих пристроїв, максимізують зменшення поверхні атак і забезпечують шлях до уніфікації високодинамічних, адаптивних політик контролю доступу для підтримки прийняття організацією принципів нульової довіри. Необхідно уникати зосередження на постачальниках, які підходять лише для заміни VPN віддаленого доступу на вузькій основі.

Отже, завдяки рішенню Fortinet Universal ZTNA стає можливим запровадити принципи нульової довіри у всій корпоративній мережі, особливо якщо інформаційна система організації включає в себе поєднання приватних і публічних хмар і рішень SaaS. З іншого боку, рішення Fortinet Universal ZTNA дозволяє користувачам безпечно підключатися незалежно від того, де вони знаходяться.

Перелік посилань:

1. Market Guide for Zero Trust Network Access. Gartner. Published 14 August 2023 - ID G00766936. By Aaron McQuaid, Neil MacDonald, John Watts, Rajpreet Kaur. URL: https://www.gartner.com/doc/reprints?id=1-2EZXPKWN&ct=230914&st=sb. (дата звернення: 29.09.2023).

2. What is Universal ZTNA? Zero trust Network Access Defined. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/universal-ztna. (дата звернення: 29.09.2023).

Сироватський Владислав Олегович, БСДМ-62
Державний університет телекомунікацій, м. Київ

ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ ВІДДАЛЕНИХ КОРИСТУВАЧІВ НА БАЗІ VPN

Розглянуто технології віртуальних приватних мереж (VPN) як ефективний засіб захисту інформаційної системи організації віддалених користувачів. Визначено мету і основні завдання, щодо основний аспектів використання VPN, включаючи типи VPN-протоколів, переваги та недоліки, а

також практичні приклади впровадження. Розроблено рекомендації, щодо дослідження, яке базується на аналізі сучасних джерел інформації та практичних дослідів в галузі захисту інформаційних систем.

Сучасна інформаційна епоха вимагає надійних засобів захисту конфіденційності та цілісності даних в організаціях, особливо коли мова йде про доступ до інформаційних систем віддалених користувачів. Віртуальні приватні мережі (VPN) стали невід'ємною частиною технологій захисту інформаційних систем, надаючи можливість створити безпечне і зашифроване з'єднання між віддаленими користувачами і корпоративною мережею. Проте, необхідно враховувати недоліки, такі як можливе перевантаження мережі та витрати на побудову і підтримку VPN [1].

Віртуальна приватна мережа (VPN) - це технологія, яка дозволяє побудувати безпечне з'єднання між віддаленими користувачами та корпоративною мережею через публічну інфраструктуру, таку як Інтернет. Однією з основних переваг використання VPN є шифрування даних, що передаються по мережі, що робить їх недоступними для сторонніх осіб. Це забезпечує конфіденційність інформації та запобігає несанкціонованому доступу.

Захист інформаційної системи на базі VPN включає в себе декілька ключових аспектів. Перш за все, це аутентифікація і авторизація користувачів. Організації повинні перевіряти ідентифікацію користувачів і надавати їм доступ лише до необхідних ресурсів. Другим важливим аспектом є шифрування даних, передаваних через VPN. Шифрування забезпечує конфіденційність інформації, унеможливлюючи її читання незаконними особами під час транспортування через віртуальний канал [2].

Для захисту інформаційної системи організації віддалених користувачів на базі VPN, слід виконати наступні кроки:

1. Вибір типу VPN: Існує кілька типів VPN, таких як PPTP, L2TP, IPSec, SSL/TLS і інші. Обирайте той, який найкраще відповідає потребам вашої організації та забезпечує найвищий рівень безпеки.

2. Конфігурація сервера VPN: Налаштуйте сервер VPN в корпоративній мережі, визначте параметри підключення та ресурси, до яких можуть мати доступ віддалені користувачі.

3. Аутентифікація та авторизація: Встановіть сильні методи аутентифікації, такі як паролі, двофакторну аутентифікацію або сертифікати, для перевірки ідентифікації користувачів. Надайте відповідні права доступу лише авторизованим особам.

4. Шифрування даних: Використовуйте сучасні криптографічні протоколи для шифрування даних, що передаються по VPN. Забезпечте високий рівень безпеки для конфіденційної інформації.

5. Моніторинг та управління: Ведіть моніторинг активності користувачів і серверів VPN, а також вчасно оновлюйте конфігурацію для запобігання потенційним загрозам [3].

Недоліки використання технології VPN в контексті захисту інформаційної

системи організації від віддалених користувачів можуть бути значущими і варто враховувати їх при розробці та впровадженні цієї технології. Ось стислий огляд недоліків:

1. Витрати на обладнання та підтримку:

Встановлення та налагодження VPN-серверів та зв'язаного обладнання може вимагати значних фінансових витрат. Організація повинна інвестувати в закупівлю, налаштування, підтримку та оновлення цього обладнання.

2. Зниження швидкості з'єднання:

Використання шифрування та інших заходів безпеки призводить до збільшення обробки даних на стороні VPN-сервера і клієнтів, що може сповільнити швидкість з'єднання. Це особливо важливо для організацій, де важлива висока швидкість передачі даних, наприклад, в галузі онлайн-ігор або фінансових послуг.

3. Складність налаштування та управління:

Налаштування VPN вимагає високо кваліфікованих спеціалістів. Це може бути складно для менших організацій, які не мають великих IT-відділів. До цього може додати складність управління користувачами, доступами та оновленнями.

Завдяки використанню технології VPN, організації можуть забезпечити надійний захист інформаційних ресурсів віддалених користувачів та знизити ризик несанкціонованого доступу і витоку даних. VPN стає невід'ємною частиною сучасних інформаційних систем і є важливим інструментом для забезпечення безпеки та конфіденційності в інтернет-середовищі [4].

У підсумку, використання VPN технології дозволяє організаціям забезпечити захист інформаційної системи віддалених користувачів, забезпечуючи конфіденційність та безпеку даних. Вибір правильного типу VPN та правильна конфігурація грають важливу роль у забезпеченні безпеки інформації в організації.

Перелік посилань:

1. Anderson, R., & Schneier, B. (2000). Security Engineering: A Guide to Building Dependable Distributed Systems.
2. Hamon, M., & Rivest, R. L. (2004). The Secure Sockets Layer (SSL) Protocol Version 3.0.
3. Ferguson, P., & Huston, G. (1998). A Method for the Construction of Keyed Hash Functions.
4. Kaufman, C., Perlman, R., & Speciner, M. (2002). Network Security: Private Communication in a Public World.

Скибун Олександр Жоржович
студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

ВИКОРИСТАННЯ МОБІЛЬНИХ ПРИСТРОЇВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ КОМПАНІЇ

Сучасне функціонування корпоративних інформаційних систем компаній визначається зростанням рівня використання працівниками власних мобільних пристроїв (далі – МП) для виробничих процесів (входження до корпоративної мережі та робота в інформаційній системі). Вказана тенденція несе в собі як і позитивізм і переваги, так і певні недоліки, адже МП певним чином нівелюють чіткі кордони присутності працівників на робочому місці (онлайн та/або офлайн) разом із виконанням ними посадових обов'язків. Вказане потребує певного переналагодження усіх процесів функціонування компанії для адаптації під нові реалії. Оскільки широке використання МП додатково впливає на рівень інформаційної безпеки компанії та потребує додаткових заходів. Таким чином забезпечення функціонування МП в корпоративних мережах, а також їх керування та захист здійснюється за допомогою відповідного програмного забезпечення – «керування мобільними пристроями» (далі – MDM). Наявність MDM дає можливість «IT-службам та службам безпеки компанії керувати усіма пристроями компанії, незалежно від їх типу та ОС», адже «хороше програмне забезпечення MDM забезпечує безпеку особистих мобільних пристроїв, що підвищує ефективність роботи працівників компанії як у офісі, так і дома (віддалено)» [2]. Такий стан речей досить позитивно впливає на ефективність роботи компанії в цілому та дає можливість забезпечувати відповідний рівень інформаційної безпеки, зважаючи на те, що «ринок Endpoint Management-рішень» в рамках якого відбувається використання відповідного програмного забезпечення (MDM, MAM, MIM, MxM) для створення сприятливих умов інформаційної безпеки усіх суб'єктів [3]. Застосування вказаного програмного забезпечення робиться для того щоб «підготувати пристрій для безпечного ремоуту», коли ми «захищатимемо або самі пристрої (контроль рівня ОС – Mobile Device Management або MDM), або встановлені на них застосунки – Mobile Application Management або MAM) [3].

При цьому необхідно зважати на те, що з точки зору організації менеджменту інформаційної безпеки, зазначені особи, які впливають на інформаційну безпеку компанії, можуть розглядатися як внутрішні стейкхолдери [1]. Так, до категорії внутрішніх стейкхолдерів, можуть бути віднесені: керівники організацій, особи топ-менеджменту, фахівці IT-департаменту (адміністратори корпоративної мережі), працівники служби інформаційної безпеки. Окрім цього, у деяких випадках, у якості внутрішніх стейкхолдерів, слід розглядати і зовнішніх осіб, таких як: акціонерів компаній, зовнішніх аудиторів та технічних експертів, клієнтів тощо. В свою чергу вимогами міжнародного стандарту ISO/IEC 27001:2013 встановлюється необхідність не тільки визначення зазначених стейкхолдерів (пункт 4.2

стандарту), але й забезпечення безпеки інформації при використанні ними МП (пункт А.6.2, А.9.1, А.9.2 та інш.) [4].

Використання компаніями у корпоративних мережах основних сценаріїв використання пристроїв умовно поділяють на: власний пристрій (CYOD); персональні пристрої, що належать компанії (COPE); пристрої, що належать лише компанії (COBO) [3]. Що дає змогу більш ефективно вирішувати питання зниження витрат компанії на корпоративну IT-інфраструктуру. Разом з тим необхідно враховувати, що використання МП може привести до погіршення стану інформаційної безпеки інформаційних систем компанії через: втрату, крадіжку, пошкодження МП; низьку компетенцію стейкхолдерів в функціях МП; зміну поколінь, технологій та програм МП; витік інформації через шкідливе програмне забезпечення, програми-шпигуни; відстеження поведінки користувача) [3]. Ось чому для зменшення рівня уразливості інформаційної системи компанії, де є потреба у використанні МП, застосовується «використання МП з апріорі встановленою платформою віртуалізації (по типу гіпервізора) поверх якої встановлюється операційна система стейкхолдера з його базою даних і налаштуваннями, та, так званою, корпоративною операційною системою, управління якою повністю покладається на IT-департамент (адміністраторів корпоративної мережі) компанії та підрозділів з інформаційної безпеки» [5]. Що тим самим забезпечує розумний компроміс між забезпеченням високого рівня інформаційної безпеки інформаційних систем компанії та інтересів стейкхолдерів.

Таким чином слід відзначити, що на сьогодні все більше компаній різних форм власності та розмірів дозволяють своїм працівникам використовувати МП під час виконання виробничих процесів в таких режимах роботи як: офлайн, онлайн, змішаний. При цьому вказані МП широко інтегруються в корпоративні інформаційні системи, взаємодіють всередині корпоративних мереж з іншими МП, мають доступ до чутливої інформації та використовують IT-ресурс компанії. У зв’язку з чим постає проблема ефективного адміністрування та забезпечення достатнього рівня кібербезпеки функціонування інформаційних систем компаній. Рівень поширення вказаних тенденцій визначає потребу у подальших розвідках питань використання особистих мобільних пристроїв в інформаційних системах компаній, як на рівні працівника, так і на рівні споживача.

Перелік посилань.

1. Добринін К.І. Підходи щодо захисту інформації організацій при використанні внутрішніми стейкхолдерами мобільних пристроїв. *Матеріали Міжнародної науково-практичної конференції «Інформаційна безпека та інформаційні технології»*: *тези доповідей, 24 – 25 квітня 2019 р.* Харків : ХНЕУ імені Семена Кузнеця, 2019. 68 с, С.6.

2. Що таке MDM: визначення та що вам слід знати. [Електронний ресурс] – Режим доступу: https://businessyield.com/uk/management/what-is-mdm/.

3. Як зробити особисті пристрої співробітників безпечними для даних компанії. [Електронний ресурс] – Режим доступу: https://dou.ua/forums/topic/39686/.

4. ISO/IEC 27001:2013 Information technology. Security techniques, Information security management systems. [Електронний ресурс] – Режим доступу: https://www.iso.org/ru/standard/54534.html.

5. Lankoski L., Stmith N., and Van Wassenhove L. Stakeholder Judgments of Value: Advancing Stakeholder, Theory through Prospect Theory, INSEAD. [Online]. [Електронний ресурс] – Режим доступу: http://www.hbs.edu/faculty /conferences/2013-sustainability-andcorporation/Documents/Stakeholder judgments of value 0513FV.pdf.

Скрипка Олександр Володимирович
студент групи УБД-31, ННІЗІ ДУІКТ, Київ, Україна

ОСНОВНІ ЗАГРОЗИ БЕЗПЕКИ ACTIVE DIRECTORY В КОРПОРАТИВНИХ МЕРЕЖАХ

Кібербезпека стає все більш важливою в сучасному цифровому світі, де корпоративні мережі є основним ресурсом для захисту у багатьох організацій. Однією з ключових складових цих систем є Active Directory, яка забезпечує управління ідентифікацією та доступом до ресурсів. У зв'язку з цим варто розглянути основні загрози безпеці для Active Directory та найкращі методи їх усунення.

Active Directory (AD) являє собою службу каталогів операційної системи Microsoft Windows, яка дозволяє IT-адміністраторам керувати корпоративною мережою та її компонентами. Зокрема це дані користувачів, інформаційні та комп'ютерні системи, конфіденційні дані, програмне забезпечення (ПЗ) тощо, захист яких є найвищим пріоритетом для компанії, оскільки він є головною ціллю для кібератак. AD є основою багатьох важливих функцій, включаючи автентифікацію користувачів, авторизацію та доступ до мережі.

Одним із прикладів наслідків компрометації AD є атака на медичну платформу healthcare.gov у 2018 році [1]. Зловмисники викрали облікові дані користувачів та використали їх, щоб отримати доступ до бази даних, при цьому залишившись непоміченими. Це призвело до розкриття понад 75 000 файлів, що містять особисту інформацію про пацієнтів. Цей інцидент підкреслює важливість захисту AD і можливі наслідки успішної атаки.

Нижче наведено поширені та основні загрози безпеці AD та їх можливе усунення [2, 3]:

1. Велика кількість адміністраторів.

Коли в організації більшість користувачів мають адміністративні права, це означає, що занадто багато осіб мають доступ із високими рівнями привілеїв, включаючи тих, хто не потребує такого рівня доступу для своєї роботи. Це створює ризик, що будь-який з них може зловживати цим доступом або навіть навмисно поширювати конфіденційну інформацію. Тому важливо обмежувати адміністративний доступ тільки для тих користувачів, які дійсно потребують його для виконання своєї роботи і вживати заходів для контролю цього доступу (PAM).

2. Слабка парольна політика.

Парольна політика визначає правила та вимоги щодо паролів користувачів. Паролі, які мають низький рівень складності або є надто простими, стають вразливими до атак перебору паролів, що може дозволити зловмисникам отримати несанкціонований доступ до системи. Встановлення надійної

парольної політики є ключовим аспектом в забезпеченні безпеки системи AD. Ця політика вимагає від користувачів використовувати складні та унікальні паролі, а також регулярно їх змінювати, що зменшує ризик зламу паролю.

3. Неактивні користувачі в мережі.

Коли співробітник покидає організацію, його обліковий запис може бути не видалено адміністраторами корпоративної мережі. Зловмисники можуть скомпрометувати його та отримати доступ до системи. Неактивні облікові записи можуть залишитися непоміченими і не включені в регулярну перевірку безпеки. Для усунення цієї загрози необхідно регулярно проводити аудит та моніторинг облікових записів користувачів та їх дій у мережі з метою виявлення підозрілої активності, відключення неактивних користувачів та їх видалення з системи.

4. Відсутність оновлень безпеки та використання застарілого програмного забезпечення.

На більшості систем встановлено велику кількість ПЗ, яке постійно оновлюється та вдосконалюється. Однак, в більшості випадків, організації не звертають увагу на появу оновлень для їхніх програм, які також містять і патчі безпеки. Несвоєчасне оновлення або його відсутність спричиняє появу застарілого ПЗ, яке в свою чергу може містити вразливості з відповідними ідентифікаторами CVE та дозволити зловмисникам їх експлуатацію. Регулярне оновлення програмного забезпечення дозволить запобігти непередбачуваним атакам та покращить загальний стан безпеки систем.

Розуміння загроз AD та впровадження відповідних заходів безпеки є необхідним для забезпечення цілісності, доступності та конфіденційності даних організації. Це включає аудит та моніторинг безпеки, розмежування та контроль доступу, впровадження надійної парольної політики та регулярні оновлення ПЗ.

Перелік посилань:

1. Healthcare.gov FFE Breach Compromises 75K Users' Data. URL: https://www.darkreading.com/vulnerabilities-threats/healthcare-gov-ffe-breach-compromises-75k-users-data
2. Glossary Active Directory Security. URL: https://www.beyondtrust.com/resources/glossary/active-directory-security
3. Top 10 Risks to Active Directory Security. URL: https://www.lepide.com/blog/top-10-risks-to-active-directory-security/

Слободська Лада Олегівна
студентка групи УБД-42, ННІЗІ ДУІКТ, Київ, Україна

АНАЛІЗ ТА ВДОСКОНАЛЕННЯ МЕТОДІВ ТЕСТУВАННЯ ЗАХИЩЕНОСТІ МОБІЛЬНИХ ДОДАТКІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРИСТУВАЧІВ

Тестування на проникнення мобільних додатків - це процес перевірки мобільних додатків для виявлення та ідентифікації уразливостей або порушень

безпеки до того, як вони будуть використані для злочинних цілей, з метою аналізу ступеня загрози, яку вони становлять для додатка, через ручне чи автоматизоване тестування на проникнення. Мобільні додатки є частиною великого мобільного екосистеми, що взаємодіє з усім, від мобільного пристрою та мережевої інфраструктури до серверів та центрів обробки даних. Поверхня атаки додатково розширюється зі зростанням використання мобільних пристроїв з передовими можливостями. Зі зростанням складності кібератак та запропонованих мільйонних винагород за виявлення помилок у мобільних додатках, організації почали інвестувати у тестування на проникнення мобільних додатків.

Основні складові, що підлягають аналізу під час тестування на проникнення мобільних додатків, охоплюють такі аспекти:

8. **Архітектура, дизайн та моделювання загроз:** Під час тестування на проникнення важливо розуміти архітектуру мобільного додатка. Ручні тести мають включати перевірку наявності небезпечного дизайну та архітектури.
9. **Мережеве спілкування:** Безпечність передачі даних через публічні мережі є критичним питанням, оскільки зловмисники можуть використовувати цей канал для крадіжки чутливої інформації користувачів. Тестування на проникнення мобільних додатків має фокусуватися на перевірці безпеки мережевого спілкування.
10. **Зберігання даних та конфіденційність:** Зберігання чутливих даних у відкритому вигляді може відкривати доступ до цих даних для зловмисників. Багато додатків зберігають таку інформацію у файлі Strings.xml, що створює загрозу безпеки.
11. **Аутентифікація та управління сесіями:** Тестування мобільних додатків повинно включати перевірку проблем, пов'язаних з управлінням сесіями, таких як некоректне завершення сесії при зміні пароля чи проблеми з багатофакторною аутентифікацією.
12. **Помилки неправильної конфігурації у коді або налаштуваннях збірки:** Деякі розробники мобільних додатків можуть не приділяти належної уваги повідомленням про помилки. Під час тестування слід перевіряти, чи не видаються додатком непотрібні внутрішні дані через повідомлення про помилки.

У відповідності до постійного розвитку мобільних технологій та поширення використання мобільних додатків у сучасному світі, забезпечення безпеки цих додатків стає першочерговим завданням для бізнесу та користувачів. Одним із ключових методів оцінки та підтвердження надійності мобільних додатків є проведення мобільного пентесту, який дозволяє виявити вразливості та ризики їхньої експлуатації. Далі детально будуть розглянуті та проаналізовані ключові методології та підходи, що застосовуються при проведенні мобільного пентесту, з орієнтацією на розуміння потенційних загроз та шляхів їхнього запобігання. Тестування мобільних додатків на проникнення виконується за 4 кроки, зазначені нижче:

1. **Збір інформації:** Цей етап включає збір необхідної інформації для визначення слабких місць у системі. Під час цієї фази важливо ретельно

досліджувати дизайн та архітектуру мобільного додатка, а також аналізувати потік даних на рівні мережі. Крім того, використання відкритих джерел для збору додаткової інформації може допомогти отримати більше уявлення про потенційні вразливості та ризики, пов'язані з додатком.

2. **Аналіз та оцінка:** На цьому етапі додаток спостерігається до та після його встановлення на пристрій. Деякі з технік оцінки, що застосовуються на цьому етапі, включають статичний та динамічний аналіз, аналіз архітектури, зворотний розбір, аналіз файлової системи та взаємодії між додатками.

3. **Експлуатація:** Фаза експлуатації включає тестування додатка за допомогою симульованих атак у реальному світі, щоб зрозуміти, як він буде поводитися при здійсненні атаки. Цільові мобільні додатки перевіряються на наявність шкідливих навантажень, наприклад, зворотного шелу або рут-експлойту. Команда намагається використати всі вразливості, виявлені тестувальниками на проникнення, за допомогою створених самостійно та загальнодоступних експлойтів.

4. **Звітність:** Після завершення фази експлуатації команда готує детальний звіт про проведені атаки. Інформація зазвичай містить дані про тестирування кінцевих точок, завдану шкоду, аналіз ризиків, а також виявлені вразливості з відповідними кроками їхньої експлуатації та усунення.

У сфері тестування на проникнення важливим аспектом є розуміння та використання різноманітних аналітичних методів для виявлення вразливостей. Серед ключових інструментів у цьому контексті є статичний та динамічний аналіз. В даній частині доповіді детально буде розглянута різниця між цими підходами, їх переваги та обмеження, а також те, як їх можна оптимально використовувати для ефективного виявлення потенційних загроз у мобільних додатках.

Статичний аналіз	Динамічний аналіз
Виконується без запуску мобільного додатку.	Виконується, коли мобільний додаток працює на пристрої.
Виконується на декомпільованому вихідному коді та наданих файлах.	Виконується на локальній файловій системі, зв’язку між програмами та сервером.
Включає перевірку якості коду, повідомлень про налагодження та помилки та проблем бізнес-логіки.	Включає тестування комунікацій на рівні мережі, криміналістику та слабку криптографію тощо.

Рис. 1. Різниця між статичним та динамічним аналізом мобільних додатків

В результаті дослідження процесу тестування на проникнення мобільних додатків, стає очевидним, що зростання використання мобільних пристроїв та широкий спектр їх функціональних можливостей призвели до збільшення загроз безпеці. У зв'язку з цим, організації стали вкладати значні ресурси в тестування на проникнення, для того щоб виявити й усунути можливі уразливості в мобільних додатках до того, як вони можуть бути використані для зловмисних дій. Ретельний аналіз компонентів, що підлягають перевірці під час процесу

тестування на проникнення, свідчить про важливість розуміння архітектури додатків, безпечного мережевого спілкування, адекватного зберігання даних, ефективної аутентифікації та управління сесіями, а також правильної конфігурації у коді та налаштуваннях збірки. Крім цього, процес тестування на проникнення мобільних додатків розглядається у чотирьох етапах, які включають збір інформації, аналіз та оцінку, експлуатацію та підготовку детального звіту. Цей цикл дозволяє виявити можливі загрози та уразливості, що можуть бути використані для запобігання можливих атак.

У високотехнологічному світі, де мобільні додатки стають все більш важливими для підтримки різноманітних аспектів життя, забезпечення їх безпеки стає критично важливим завданням. Тому ретельне тестування на проникнення мобільних додатків є необхідним для гарантування захищеності даних і забезпечення безпечного користування.

Перелік посилань:

1. Посібник з тестування безпеки мобільних додатків від OWASP: https://mobile-security.gitbook.io/mobile-security-testing-guide/
2. Vijay Kumar Velu, Mobile Application Penetration Testing (Березень 2016)
3. Тестування мобільних додатків на проникнення: https://redteamsecurity.com/penetration-testing/mobile-application-penetration-testing

Соколянський Костянтин Анатолійович
Студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ВИКОРИСТАННЯ IBM QRADAR SOAR ДЛЯ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ SECURITY OPERATIONS CENTER (SOC)

Сьогоднішній цифровий світ став свідком стрімкого росту кіберзагроз та інцидентів, що вимагають швидкого та ефективного реагування. Організації повинні вдосконалювати свої підходи до кібербезпеки та надавати пріоритет захисту своєї інфраструктури та конфіденційних даних. У цьому контексті, використання системи IBM QRadar SOAR (Security Orchestration, Automation, and Response) стає важливим елементом стратегії забезпечення кібербезпеки організації.

IBM QRadar SOAR - це інтегрована платформа, яка об'єднує в собі низку інструментів для автоматизації та управління процесами SOC. Однією з ключових функцій є можливість інтеграції з іншими системами безпеки, такими як SIEM (Security Information and Event Management), IDS/IPS (Intrusion Detection System/Intrusion Prevention System), антивіруси та інші. Ця інтеграція дозволяє збирати дані з різних джерел і проводити комплексний аналіз для виявлення потенційних загроз.

Однією з основних переваг IBM QRadar SOAR є можливість автоматизації рутинних завдань та процесів у SOC. Наприклад, платформа може автоматично виконувати стандартні завдання, такі як аналіз журналів подій, виявлення патернів атак, та ідентифікація загроз. Це дозволяє розгортувати ресурси аналітиків на більш складні та стратегічні завдання.

Для прикладу, при виявленні підозрілих дій на мережі, IBM QRadar

SOAR може автоматично розпочати розслідування, ініціювати процедури відкриття інциденту, а також приймати заходи щодо ізоляції інфікованих систем. Це робиться швидше, ніж будь-коли раніше та допомагає запобігти поширенню загроз у мережі.

Для більшого розуміння, розглянемо приклад впровадження IBM QRadar SOAR в університетському SOC. Університетський SOC виявив проблему із збільшенням кількості фішинг-атак, які спрямовувалися на студентів та співробітників. Завдяки IBM QRadar SOAR, SOC може налаштувати автоматизовані процеси для виявлення та блокування фішингових спроб. Крім того, платформа здатна аналізувати електронну пошту, ідентифікувати схожість з відомими шаблонами фішингу та автоматично вжити заходів щодо блокування атак.

Використання IBM QRadar SOAR для автоматизації процесів SOC може суттєво покращити захист від кіберзагроз та зменшити вплив інцидентів. Ця платформа дозволяє реагувати швидше та ефективніше, зменшує навантаження на аналітиків та допомагає виявляти та виправляти загрози на ранніх стадіях.

Завдяки конкретним можливостям і прикладам використання, ми бачимо, що IBM QRadar SOAR стає ключовим інструментом для підвищення безпеки в цифровому світі. Ця платформа допомагає SOC бути готовим до найсучасніших кіберзагроз та діяти швидко та ефективно для захисту активів та даних.

Перелік посилань:

1. What is SOAR? Security orchestration, automation and response: https://www.ibm.com/topics/security-orchestration-automation-response (дата звернення: 22.10.2023).

Соколянський Костянтин Анатолійович
Студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОБОТИ СИСТЕМИ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ЗАГРОЗИ (SOC) ЗА ДОПОМОГОЮ MITRE ATT&CK

Системи моніторингу та реагування на загрози (SOC) стали ключовими компонентами для забезпечення кібербезпеки сучасних організацій. Однак з появою все більш складних та витончених кіберзагроз, необхідні нові підходи до їх виявлення та протидії. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) - це цінний інструмент для підвищення ефективності SOC та оптимізації захисту інформації.

Першим кроком в роботі з MITRE ATT&CK є ретельне ознайомлення з фреймворком. Це допоможе вам зрозуміти його призначення та структуру. MITRE ATT&CK включає в себе матрицю, методики, тактики та суб-техніки. Відвідайте веб-сайт ATT&CK (https://attack.mitre.org/) та детально огляньте матрицю, методики та суб-техніки.

Для ефективного використання MITRE ATT&CK, важливо ідентифікувати техніки та тактики, які відповідають інфраструктурі, додаткам та даним вашої організації. Відобразіть MITRE ATT&CK техніки на існуючі заходи забезпечення безпеки, такі як брандмауери, системи виявлення вторгнень та засоби захисту кінцевих точок.

Після відображення технік MITRE ATT&CK на ваші заходи безпеки, розробіть правила виявлення та використовуйте їх для виявлення підозрілих дій. Використовуйте вашу систему управління інформацією та подіями безпеки (SIEM) або платформи для обробки інформації про загрози для створення правил, які спрацьовуватимуть при виявленні підозрілих дій, пов'язаних з конкретними техніками MITRE ATT&CK.

MITRE ATT&CK може бути використаний як основа для проведення активних пошукових вправ. Шукайте індикатори компрометації (IOCs), пов'язані з відомими техніками MITRE ATT&CK, та використовуйте їх для ідентифікації потенційних загроз у вашому середовищі.

MITRE ATT&CK може також бути використаний для підвищення ефективності процедур реагування на інциденти. Розробіть плани реагування та протоколи, які відповідають конкретним технікам та тактикам MITRE ATT&CK для ефективного управління та ліквідації загроз.

Варто не забувати про важливість співпраці з зовнішніми джерелами загроз та загрозовим інтелектом. Слідкуйте за останніми звітами загрозового інтелекту, які посилаються на техніки та тактики MITRE ATT&CK.

Запровадження MITRE ATT&CK в SOC вимагає систематичного та докладного підходу. Ось деякі додаткові кроки та фактори, які слід враховувати для оптимізації впровадження:

- Оцінка покриття: Ретельно оцініть, наскільки багато та які саме техніки MITRE ATT&CK ви вже включили в свої заходи безпеки. Якщо ви виявите прогалини, подумайте про те, як ви можете покращити це покриття.
- Оновлення та моніторинг: MITRE ATT&CK постійно оновлюється, оскільки кіберзагрози розвиваються. Періодично переглядайте матрицю та ресурси MITRE для забезпечення актуальності ваших заходів безпеки.
- Навчання та сертифікація: Розгляньте можливість навчання вашого персоналу з використання MITRE ATT&CK. Деякі організації надають сертифікати або навчальні програми, які допоможуть вашій команді розуміти та ефективно використовувати цей фреймворк.

- Співпраця зі спільнотою: MITRE ATT&CK користується підтримкою широкої кібербезпечної спільноти. Зв'яжіться з іншими фахівцями в цій галузі, обмінюйтеся досвідом та відкритими джерелами інформації.

Використання MITRE ATT&CK в SOC допомагає збільшити ефективність оборони від кіберзагроз та оптимізувати заходи з реагування на інциденти. Основними перевагами цього підходу є усвідомленість, оскільки за допомогою MITRE ATT&CK, ви можете бути краще підготовлені до того, як атаки можуть відбутися та які ризики можуть виникнути; зниження часу реагування: правила виявлення на основі MITRE ATT&CK дозволяють виявляти загрози на ранніх стадіях, зменшуючи час реагування на інциденти; краща проактивність: MITRE ATT&CK стимулює проактивну пошукову діяльність, яка дозволяє виявляти загрози, навіть коли немає очевидних індикаторів компрометації.

MITRE ATT&CK - це потужний інструмент для підвищення ефективності роботи SOC та захисту від сучасних кіберзагроз. Правильне використання цього фреймворку може підвищити рівень захисту та зробити SOC більш відповідальним на виклики кібербезпеки.

Перелік посилань:
1. MITRE ATT&CK Navigator: https://mitre-attack.github.io/attack-navigator/ (дата звернення: 22.10.2023).
2. MITRE ATT&CK матриця: https://attack.mitre.org/ (дата звернення: 22.10.2023).
3. MITRE ATT&CK Джерела Даних: https://attack.mitre.org/versions/v13/datasources/ (дата звернення: 22.10.2023).

Степанов Михайло Григорович
Студент групи БСДМ-63, ННІЗІ ДУТ, Київ, Україна

HOW TO PROTECT CORPORATE WIRELESS ACCESS POINTS

The protection of corporate wireless access points is of paramount importance in today's digital landscape. As organizations increasingly rely on wireless networks for their day-to-day operations, securing these access points becomes a critical task. This article delves into a crucial aspect of wireless network security—the four-way handshake, which is a message exchange between an access point and client device, generating encryption keys for secure communication.

The four-way handshake is a message exchange between an access point and the client device. The devices exchange 4 messages that generate the encryption keys.

Here’s how a handshake based authentication work in depth:

- PTK (Pairwise Transient Key) – a key that encrypts traffic between the access point and client device. If you’re friends with mathematical formulas, here’s one for PTK:PTK = PRF (PMK + ANonce + SNonce + Mac (AA)+ Mac (SA))PRF is a pseudo-random function that sums up all the formula components.
- PMK (Pairwise Master Key) – an encryption key generated from MSK (Master Session Key).

- ANonce – a random number generated by an access point.
- SNonce – a random number generated by a client device.
- MAC (AA) – MAC address of the access point.
- MAC (SA) MAC address of the client device.
- GTK (Group Temporal Key) – an encryption code unique to each access point. It encrypts all traffic between one access point and multiple client devices.
- RSN – a set of network security features that prevent exploiting WEP weaknesses.
- MIC (Message Integrity Check) – a network security feature that prevents bit-flip attacks. It's an improvement to the previous ICV (Integrity Check Value).

The handshake algorithm happens in 4 steps:

1. The access point sends ANonce to the client device.
2. The client generates PTK and then it sends SNonce, RSN, and MIC back to the access point.
3. The access point sends ANonce, RSN, MIC, and GTK to the client.
4. The client sends a message with MIC to notify the access point if the temporal keys have been installed successfully.

By default, the network card listens only for the packets addressed to itself. The monitor mode enables the network card to listen to every packet in the air. Listening to all the packets can help the card capture the 4-way handshakes.

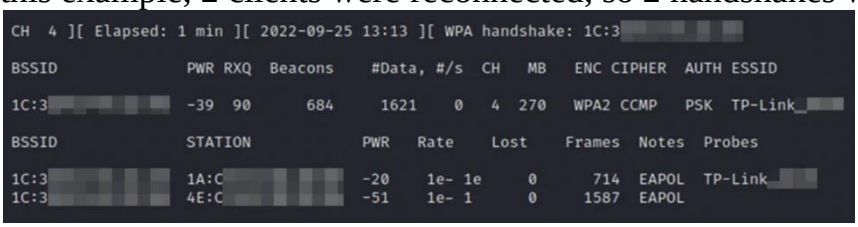
Not all network cards support the monitor mode. For the purpose of example, the AWUS1900 is used. It supports both 2.4GHz and 5GHz frequencies while also having a long-range distance.

Vulnerability Tutorial: Handshake Capture

- Install the latest drivers on your adapter
- Kill all the adapter processes to run without restriction. Go to the terminal and execute this command:airmon-ng check kil
- Switch down wlan0 interface with:ifconfig wlan0 down
- Turn on the monitor mode with:iwconfig wlan0 mode monitor
- Switch on wlan0 interface with:ifconfig wlan0 up

Capture the handshake with running airodump-ng –channel {channel id} –bssid {BSSID} –essid {ESSID} -w {output directory of the captured file} wlan0

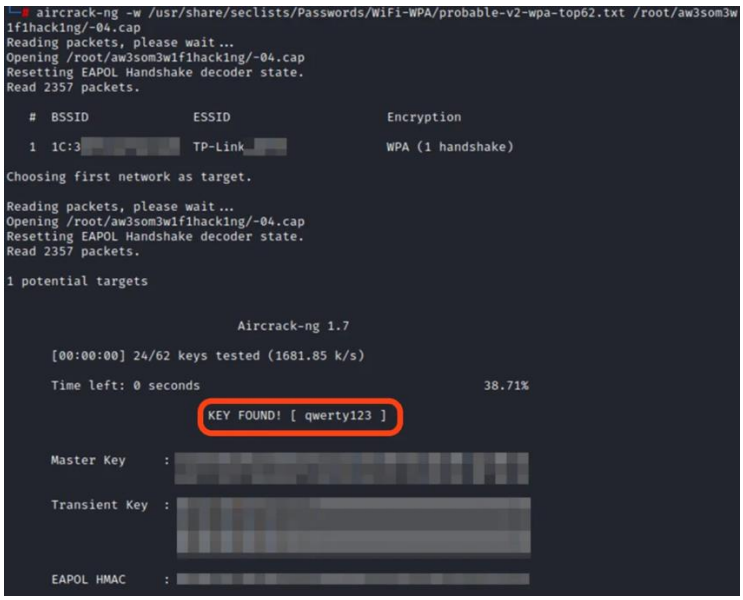
Deauthenticate clients from target access point with aireplay-ng -0 0 -e {ESSID} -a bssid wlan0 –ig. After the deauthentication attack completed the captured handshakes can be viewed. In this example, 2 clients were reconnected, so 2 handshakes were made.



Pic.1 – Connected clients

At this point, handshakes are the encrypted password for the network. Now, the right password needs to be guessed by the computer using your list of possible passwords.

It will now take time for computer to process all the words from wordlist. Once the password is found, the “KEY FOUND” text will be displayed.



Pic.2 – Discovered password

If a password is too hard, the wordlist may not even contain it. That’s why there are paid services that take your handshakes and decrypt them on their end. They usually have more wordlists and processing power.

How to protect your Wi-Fi network

The best solution is to configure the WI-FI router to use WPA3 where the four-way handshake is replaced with a much stronger authentication algorithm.

Keep in mind that not all your devices may support it, so use at least WPA2 combined with a strong unpredictable password. We recommend you generate a password with a minimum of 10 symbols in length, lower- and upper-case letters, numbers, and special symbols.

Савченко Віталій Анатолійович
Степанченко Богдан Сергійович
аспірант групи АІКБ-125, ДУІКТ, Київ, Україна

МЕТОДИКА ПРОГНОЗУВАННЯ ЧАСУ ПОЧАТКУ DDOS АТАКИ НА ОСНОВІ ДОСЛІДЖЕННЯ ДИНАМІКИ ПОВЕДІНКИ ЕВОЛЮЦІЙНИХ РІВНЯНЬ

Атаки розподіленої відмови в обслуговуванні (DDoS) є поширеною загрозою у кібербезпеці, коли зловмисники використовують кілька комп'ютерів, щоб перевантажити мережу та ресурси цілі з метою створення завад. Ці атаки перешкоджають законному доступу, погіршують продуктивність мережі і використовуються, як інструменти інформаційної війни. Виявлення DDoS атак складне завдання, оскільки використання зловмисниками законних мережевих протоколів ускладнює розпізнавання атаки хакерів від роботи звичайного користувача. Для задачі виявлення та розрізнення DDoS атак, методи машинного навчання, виявилися найбільш ефективними. Деякі з найбільш використовуваних моделей машинного навчання включають: Штучні нейронні мережі (ANN), Баєсова мережа (BN), Градієнтний спуск (GD), Дерева рішень (DT), Ансамбль навчання (EL), Випадковий ліс (RF), Логістичну регресію (LR) та Опорновекторні машини (SVM).

Уже є наявний фреймворк виявлення DDoS атак під назвою FAMS, який складається з чотирьох етапів: підготовка даних, вибір ознак, вибір моделі та оптимізація. Підготовка даних включає операції, такі як видобування ознак, кодування, обробка відсутніх значень, видалення викидів, балансування даних, видалення дублікатів та нормалізація. Методи вибору ознак розділені на: фільтр, обгортку та вбудовані методи. FAMS поєднує їх, щоб створити оптимізований алгоритм вибору ознак. Вибір моделі визначає найбільш підходящий алгоритм машинного навчання зі списку: GD, SVM, LR, RF та інші алгоритми голосування. На етапі вибору, моделі RF перевершують інші з точки зору точності, запам'ятовування, оцінки F1, середнього значення та часу прогнозування. Таким чином, RF вибирається для подальшої оптимізації в фазі оптимізації RF.

Дослідження перевірятиме FAMS на різних наборах даних і синтетичних даних, демонструючи його ефективність у виявленні DDoS атак, з результатами порівняння з іншими моделями. Буде розглянуто пов'язана робота в цій галузі, різні підходи до машинного навчання та їх ефективність. На один із головних планів виноситься важливість вибору функцій і правильного вибору алгоритмів машинного навчання для точного й ефективного виявлення атак.

Крім того, існує нова загроза DDoS-атак у контексті Інтернету речей (IoT)

і пов’язаних технологій, таких як Інтернет дронів (IoD). Ці технології, які часто підключаються до незахищених мереж, створюють нові можливості для кібератак, включаючи перешкоди, введення команд і підробку GPS. Виявлення та пом’якшення DDoS-атак у цих контекстах є надзвичайно важливими. Також важливим є момент зі зростаючою актуальністю додатків Інтернету речей, мереж з низьким енергоспоживанням і втратами, а також необхідністю ефективного виявлення DDoS атак.

Також, є наявним поглиблений аналіз категорій і архітектур DDoS атак, зосереджуючись на ролі зловмисників, ботнетів і цільових мереж або серверів. Він розрізняє централізовані та децентралізовані архітектури атак, відзначаючи переваги безпеки першої. Розглядається виснаження ресурсів при DDoS-атаках, аналізується ймовірність виснаження пропускної здатності. Крім того, представляється нова архітектура для DDoS атак, яка спрощує керування ботнетом, зменшує витрати та підвищує надійність.

На завершення пропонується розширена структура виявлення DDoS-атак, розглядається відповідна робота в цій галузі та досліджуються наслідки DDoS-атак для IoT і пов’язаних технологій. Надається цінна інформація про методи виявлення атак, наголошуючи на важливості вибору функцій і правильного вибору алгоритму машинного навчання, а також запропоновано структурований аналіз категорій і архітектур DDoS атак.

Перелік посилань:

1. DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges URL: https://www.mdpi.com/2224-2708/12/4/51
2. A DDoS Attack Detection Method Based on Natural Selection of Features and Models URL: https://www.mdpi.com/2079-9292/12/4/1059

Стріканов Даніїл Олегович
студент групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

ОЦІНКА ЗАГРОЗ ЦІЛІСНОСТІ ІНФОРМАЦІЇ НА ПІДПРИЕМСТВАХ

В цій роботі розглянута проблема загроз цілісності інформації на підприємствах та їх оцінка. Інформація стала однією з найцінніших активів сучасних організацій, і її цілісність є важливою складовою інформаційної безпеки. Отже, вивчення та оцінка загроз цілісності інформації стають надзвичайно актуальними завданнями.

На сьогоднішній день своєчасна та об’єктивна інформація є важливим елементом виробництва та вважається одним із головних ресурсів суспільного розвитку. Сучасні інформаційні системи і технології є засобом підвищення продуктивності та ефективності праці. Проте глобальна комп’ютеризація

багатьох сфер управління та виробництва тягне за собою появу принципово нових загроз інтересам окремих людей, підприємств, суспільств і націй.

Концепція цілісності означає, що інформація є точною, повною та не містить неавторизованих змін у межах очікувань користувача. Звернемо увагу, що інформація не є на 100% безпомилковою, але якість інформації відповідає очікуванням користувачів.

Цілісність означає, що інформація захищена від необережного поводження чи навмисних неавторизованих змін, не обробляється за допомогою ненадійних процедур і дані контролюються на всіх етапах обробки [2].

Для оцінки інформаційної безпеки часто використовують методи рентабельності витрат на здійснення заходів щодо захисту інформації, методи оцінки шкоди від загрози хакерських атак.

Значного поширення отримав метод нечітких множин. При цьому експертним шляхом оцінюють ймовірність подолання системи захисту інформації, імовірність доставки одиниці інформації до споживача, час доставки й апаратурну складність. Інколи використовують показники частки працівників інформаційних відділів у загальній кількості працівників, частки витрат на забезпечення інформаційної безпеки в загальній величині витрат.[3]

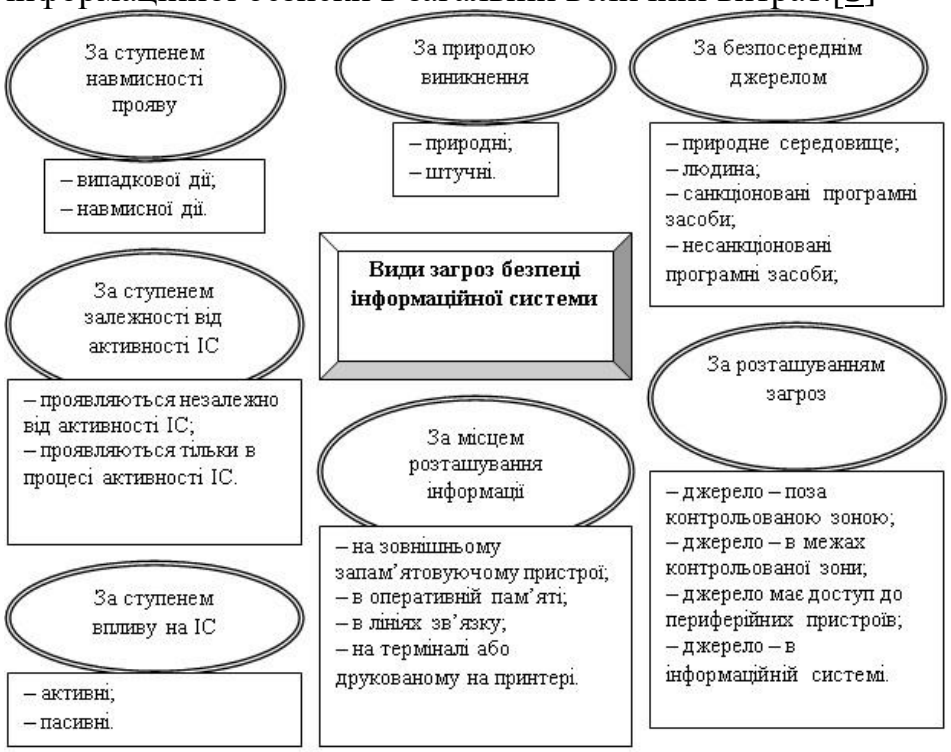


Рис.1. Види загроз безпеці інформаційної системи [1].

Крім того, деякі науковці аналізують такі показники:
– продуктивність інформації;
– коефіцієнт інформаційної озброєності;
– коефіцієнт захищеності інформації .

Перелік параметрів оцінювання рівня захисту інформації та ступінь їх конкретизації визначають такою методичною умовою: кількість оцінюваних параметрів повинна бути достатньо обмеженою з метою забезпечення оперативності управлінських рішень, які приймають. Формування та групування параметрів спирається на аналіз широкого комплексу проблем економічного і соціального характеру, тому множина вхідних чинників повинна задовольняти умови повноти, дієвості та мінімальності. [3].

Перелік посилань:

1. ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНОГО ПІДПРИЄМСТВА [Електронний ресурс] – Режим доступу: http://sophus.at.ua/publ/2014_04_17_18_kampodilsk/sekcija_4_2014_04_17_18/osoblivosti_organizaciji_informacijnoji_bezpeki_suchasnogo_pidpriemstva/54-1-0-931 (дата звернення: 23.10.2023).
2. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ [Електронний ресурс] – Режим доступу: http://dspace.onua.edu.ua/bitstream/handle/11300/11111/ОІБ%20конспект%20лекцій.pdf?sequence=1&isAllowed=y (дата звернення: 24.10.2023).
3. МЕТОДИЧНИЙ ПІДХІД ДО ОЦІНЮВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВАХ [Електронний ресурс] – Режим доступу: https://praci.vntu.edu.ua/index.php/praci/article/download/6/6/11 (дата звернення: 24.10.2023).

Ступін Денис Володимирович
студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

АНАЛІЗ АКТУАЛЬНИХ ЗАГРОЗ КІБЕРБПЕЗПЕЦІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ТА РОЛЬ ОПЕРАЦІЙНОГО ЦЕНТРУ БЕЗПЕКИ У ЇХ ВИЯВЛЕННІ ТА РЕАГУВАННІ

З розвитком кіберзагроз надійні операційні можливості для забезпечення безпеки мають вирішальне значення для корпоративного захисту. Операційний центр безпеки (SOC) слугує сполучною ланкою для виявлення та реагування на складні атаки на бізнес-системи та дані. Основні можливості SOC включають агрегування даних про події безпеки в гібридних середовищах, використання аналітики та розвідки загроз для виявлення аномалій, координацію робочих процесів реагування на інциденти. Продвинуті SOC забезпечують швидке виявлення, локалізацію та усунення загроз для протидії ризикам, пов'язаним з програмами-вимагачами, атаками на ланцюжки поставок, крадіжкою облікових даних тощо. Потужні SOC є основою стійкої кібербезпеки.

Корпоративні інформаційні системи стикаються з постійно зростаючими високотехнологічними кібератаками як з боку звичайних груп хакерів, так і з боку хакерів, що спонсоруються державами. Оскільки атаки стають все більш складними, організації мають впровадити надійні методи забезпечення безпеки шляхом виявлення, розслідування та реагування на кіберінциденти. Належно обладнаний операційний центр безпеки (SOC) з компетентною командою забезпечує організацію необхідними технологіями для протидії сучасним загрозам [1].

Однією з найактуальніших загроз сьогодення є Ransomware as a

Service(RaaS) – вимагач-шифрувальники як сервіс. Фактично, це бізнес-модель, в якій група хакерів продає свій код вимагачів-шифрувальників іншим хакерам, які потім використовують його для здійснення власних атак. Прикладом успішної атаки за допомогою Ransomware є атака на американську нафтову компанію Colonial Pipeline у 2021 році. Завдяки знаходженню вразливості у VPN компанії, хакери змогли увійти в мережу і розгорнути шкідливе програмне забезпечення. В результаті трубопровідна система була зупинена більше ніж на тиждень, а компанія була вимушена виплатити 9 мільйонів доларів вимагачам за розшифрування даних [1].

Крім цього, популярним є використання безфайлового програмного шкідливого забезпечення (fileless malware). У цьому випадку код працює безпосередньо в пам'яті комп'ютера, а не на жорсткому диску. У 2020 така атака на компанію SolarWinds призвела до витоку персональних даних більше сотні тисяч клієнтів[1].

Атаки на ланцюжки постачання (supply chain attack), також є актуальною загрозою. Атака на ланцюжок поставок — це кібератака, яка має на меті завдати шкоди організації, націлюючись на менш безпечні елементи в ланцюзі постачання. Атака на ланцюжок постачання може відбуватися на апаратному або програмному рівні. У 2017 році популярне програмне забезпечення для очищення системи CCleaner зазнало масштабної атаки, під час якої хакери скомпрометували сервери компанії та замінили оригінальну версію програмного забезпечення на шкідливу. Атака зловмисного програмного забезпечення заразила понад 2,3 мільйона користувачів, які завантажили або оновили свій додаток CCleaner у період із серпня по вересень 2017 року з офіційного веб-сайту за допомогою бекдорної версії програмного забезпечення [1].

Згідно зі «Звітом Microsoft про цифровий захист» у 2023, фішинг залишається найпопулярнішим методом для зловмисників, які прагнуть закріпитися в мережі компанії. В одному конкретному випадку, що був розслідуваний Microsoft Detection and Response Team (DART), велика виробнича організація була атакована, використовуючи фішингову атаку. Фішинговий електронний лист був надісланий кільком працівникам компанії. В середині було посилання, що перенаправляло на підроблену веб-сторінку, в якій необхідно було ввести логін та пароль від домену організації. За допомогою постійного моніторингу IT-інфраструктури та використовуючи рішення Microsoft Sentinel, атаку вдалося попередити [1].

Хоча такі засоби як брандмауери, залишаються важливими у забезпеченні безпеки корпоративних інформаційних систем, сучасні загрози підкреслюють потребу в глибокій видимості внутрішніх систем, користувачів і даних. Операційний центр безпеки служить центром для цього, приймаючи та співвідносячи дані з різних гібридних середовищ. Використовуючи такі рішення як IBM QRadar або Microsoft Sentinel, члени SOC повинні вміти аналізувати отриману інформацію, щоб виявити ознаки компрометації [2].

Ефективний SOC має спиратись на технології, а також на кваліфікований персонал. Аналітики безпеки сортують сповіщення, виявляють загрози та

контролюють процес реагування на інциденти. Аналітики аналізу загроз відстежують ризики, характерні для організації та галузі. Менеджери SOC координують команди, інструменти та процеси для безперебійного робочого процесу [2].

У міру еволюції загроз, можливості SOC мають розвиватися за рахунок автоматизації, інтеграції хмарних сервісів, штучного інтелекту та спеціалізованого персоналу. Гнучкий та стійкий SOC повинен поєднувати в собі технології, управління та інституційну підтримку для покращення можливостей виявлення та реагування [3].

Таким чином, сучасні SOC відіграють незамінну роль у захисті корпоративних систем від кіберзагроз, спрямованих на порушення роботи, крадіжку власності або нанесення шкоди репутації бренду. Виконуючи функцію об'єднаного центру для забезпечення критично важливої видимості, своєчасної розвідки загроз, скоординованого реагування та постійного вдосконалення, SOC дозволяє підприємствам ефективно протистояти кіберризикам.

Перелік посилань:

1. Звіт про цифровий захист Microsoft 2023. https://www.microsoft.com/uk-ua/security/security-insider/microsoft-digital-defense-report-2023
2. Microsoft Sentinel. Planning and implementing Microsoft’s cloud-native SIEM solution. https://www.microsoftpressstore.com/store/microsoft-sentinel-planning-and-implementing-microsofts-9780137901029.
3. Richard Diver. Microsoft Sentinel in Action. Packt, 2022. 126 p.

Катков Юрій Ігорович
доктор технічних наук, професор кафедри комп’ютерних наук, ННІТ, ДУІКТ, Київ, Україна
Супчук Дмитро Едуардович
Студент групи КНДМ-62, ННІТ, ДУІКТ, Київ, Україна

АНАЛІЗ СЕРЙОЗНИХ ВРАЗЛИВОСТЕЙ БЕЗПЕКИ REACT І ЯК ЇХ УНИКНУТИ

Розглядається питання вразливості безпеки React. Надзвичайно важливо бути добре обізнаним про головні вразливості безпеки React, щоб уникнути їх заздалегідь. React — це дуже затребувана інтерфейсна структура для створення ефективних веб-додатків, для щоденного використання, включаючи Netflix, Facebook, Instagram, Airbnb і Dropbox. Незважаючи на те, що React пропонує численні переваги, він також може виявити вразливість системи безпеки, якщо з нею поводитися належним чином. Як і з будь-якою іншою технологією, дуже важливо знати про ці потенційні вразливості та усунути їх. Тому важливо розуміти й усунути ці потенційні ризики, дотримуючись найкращих практик безпеки React.

Уразливості системи безпеки React можна запобігти шляхом впровадження найкращих практик безпеки, таких як перевірка даних, багатофакторна автентифікація, шифрування та регулярне сканування програми на наявність потенційних уразливостей. Регулярні оновлення програмного забезпечення та навчання розробників щодо ризиків безпеки також можуть допомогти уникнути вразливості безпеки React. Роблячи це, можна забезпечити захист свого веб-додатку від потенційних загроз, з’ясувати, як знайти витік пам’яті React, або зменшити вразливості create-react-app і підвищити його загальну безпеку.

1. Актуальність.

React — це легка бібліотека Javascript із філософією «навчись один раз, пиши будь-де» для створення ефективних веб-додатків, як односторінкових (single-page applications - SPA), так і багатосторінкових (multi-page applications - MPA). Це веб-фреймворк, створений для спрощення розробки інтерактивних веб-додатків. Головна мета React — допомогти розробникам створити більше інтерактивності. Його основною метою є написання веб-компонентів, які можна використовувати в багатьох різних контекстах [1].

Все більше і більше сайтів стають веб-додатками, які працюють через браузери замість статичних програм. Ці програми дозволяють більше взаємодіяти з відвідувачами сайту, і це означає, що розробники, які використовують базові компоненти React, знають, що вони можуть додавати додаткові елементи зверху, щоб адаптувати їх до різних середовищ. Наприклад, під час написання веб-програми з використанням компонентів React розробник може використовувати React Native для створення нативної мобільної програми з тих самих компонентів. Це дає змогу створювати 100% нативну програму для iOS або Android із власними компонентами інтерфейсу користувача, а не лише компонентами типу веб-інтерфейсу.

Ще одна основна і цікава функція React — це внутрішній стан, пов’язаний з кожним компонентом. Компоненти, створені за допомогою React, можуть відстежувати або значення поля, або певні інші дані, які розробник може пов’язати з ними, і їх можна використовувати від сторінки до сторінки, знову й далі, щоб розробник був задоволений. Ця функція зазвичай використовується для зв’язування внутрішніх сповіщень і змінення значень полів форми з інтерфейсом. Якщо користувач має п’ять сповіщень, які він вирішив переглянути, кожне оновлення буде виділено, коли натиснути на нього, а число на значку сповіщень зменшуватиметься, коли кожне буде відкрито – усі ці дії контролюються React.

Але незважаючи на те, що React пропонує численні переваги, він також може виявити вразливість системи безпеки, якщо з нею поводитися належним чином. Як і з будь-якою іншою технологією, дуже важливо знати про ці потенційні вразливості та усунути їх. Тому розгляд загальних викликів безпеки, з якими стикаються програми React і найкращі методи як їх уникнути є актуальнім і своєчасним.

2. Види вразливості безпеки React

Уразливості системи безпеки React — це слабкі місця в коді веб-програми React, якими можуть скористатися зловмисники, щоб порушити конфіденційну інформацію або зашкодити функціональності програми. Вразливості безпеки React настільки серйозні, що можуть зламати програму. Якщо не усунути вразливості безпеки React, вони можуть завдати серйозної шкоди даним користувача та репутації компанії. Хакери можуть використовувати ці недоліки, щоб викрасти конфіденційну інформацію, маніпулювати даними користувачів і навіть закрити всю програму. Найбільш поширені наступні вразливості безпеки

React включають: міжсайтовий сценарій скриптингу (XSS), ін’єкцію SQL, підробку міжсайтового запиту (CSRF), вразливість у пакетах і залежностях, порушену автентифікацію та неавторизований доступ, блискавка та зовнішні сутності [2, 3].

Запобігти вразливості системи безпеки React можна шляхом впровадження найкращих практик безпеки, таких як перевірка даних, багатофакторна автентифікація, шифрування та регулярне сканування програми на наявність потенційних уразливостей. Регулярні оновлення програмного забезпечення та навчання розробників щодо ризиків безпеки також можуть допомогти уникнути вразливості безпеки React.

3.Характеристика вразливості та способи їх усунення

- **Міжсайтовий сценарій скриптингу (XSS).** XSS є однією з найпоширеніших уразливостей безпеки React, з якою може зіткнутися ваша веб-програма. XSS-атаки відбуваються, коли на веб-сторінки впроваджуються зловмисні сценарії на стороні клієнта, які користувачі можуть клацати або приймати, що призводить до: злому засобів контролю доступу; викрадення сеансів або файли cookie; несанкціоноване підключення до камер або портів комп’ютера. Існує два типи атак XSS, з якими може зіткнутися веб-програма: відображення або збереження міжсайтового сценарію. Для запобігання міжсайтовому сценарію застосовують: вимкнення розмітки з інструкціями щодо виконання коду, наприклад, <object>, <script>, <link> і <embed>; використання {} для зв’язування даних за замовчуванням, що автоматично екранує значення, коли ви це зробите, але він працює лише з textContent, а не з атрибутами HTML; впровадження WAF (брандмауера веб-додатків), що може допомогти захистити від атак XSS за допомогою фільтрації на основі сигнатур; аналіз форматовано тексту HTML на розмітку HTML від уразливостей XSS. OWASP пропонує такі бібліотеки, як OWASP Java HTML Sanitizer і HtmlSanitizer для цієї мети; аналіз URL-адрес і перевірка білого/чорного списків також можуть бути корисними для уникнення XSS-атак на програму React.

- **SQL ін'єкція.** Впровадження SQL (SQLi) — поширена вразливість безпеки, яка може порушити цілісність даних у програмах React. Хакери можуть вводити шкідливий код SQL у вашу базу даних, дозволяючи їм отримувати, редагувати або видаляти дані, не обмежуючись дозволами користувача. Цей тип атаки на безпеку може завдати значної шкоди системам організації, оскільки хакери можуть змінити або знищити конфіденційні дані. SQL-ін’єкція може відбуватися з різних причин, зокрема: неправильне кодування; слабкий контроль безпеки; відсутність перевірки введених користувачем даних.

Щоб запобігти ін’єкції SQL у додатках React, потрібно прийняти наведені нижче найкращі методи безпеки React:

- Фільтрування всіх користувацьких даних через строгий білий список для захисту від SQLi, оскільки це гарантує ретельну перевірку всіх введених даних перед обробкою.
- Дотримуючись принципу найменших привілеїв, призначаючи лише

необхідні привілеї різним обліковим записам. Наприклад, якщо веб-сайту потрібно отримати вміст за допомогою операторів SELECT, він повинен мати лише ці привілеї, а не доступ до таких привілеїв, як UPDATE, INSERT або DELETE.

- Використання сканерів уразливостей, таких як Acunetix, для періодичного сканування ваших програм React може допомогти виявити та усунути будь-які слабкі місця безпеки, перш ніж ними скористаються зловмисники.
- Перевірка всіх функцій API щодо їхніх схем API, особливо для уникнення SQLi на основі часу.

Крім того, організації повинні надавати пріоритет запровадженню практик безпечного кодування, наприклад дотриманнябезпечна розробка продуктужиттєвого циклу та виконання регулярних сканувань безпеки, тестування та перевірки коду. Дотримуючись цих передових практик, програми React можна захистити від небезпек впровадження SQL та інших уразливостей безпеки.

Підробка міжсайтового запиту (CSRF) — це вразливість безпеки, яка впливає на багато веб-сайтів і веб-додатків, у тому числі створених за допомогою React. CSRF атаки: використовуйте довіру веб-сайту до веб-переглядача користувача; оманою змушує користувача робити небажані запити на сервер. Ці запити можуть варіюватися від простих запитів GET до небезпечних запитів POST, які можуть змінювати або видаляти дані.

Щоб запобігти підробці міжсайтових запитів у React треба використовувати методи безпеки React, які можуть допомогти запобігти таким атакам, а саме:

- Реалізація механізму захисту на стороні сервера шляхом генерації унікального токена для кожного сеансу користувача та включення його в заголовок усіх запитів. Тоді сервер може перевірити маркер перед обробкою запиту, гарантуючи, що приймаються лише запити, що надходять із вашої програми.
- Використання атрибута cookie "same-site", який повідомляє веб-переглядачу надсилати файли cookie лише із запитами, зробленими до того самого домену, що й файл cookie. Установивши цей атрибут, ви можете заборонити браузеру надсилати ваші файли cookie на веб-сайт зловмисника, навіть якщо користувача обманом змусили натиснути посилання.

Крім того, React пропонує кілька бібліотек і пакетів, які можуть допомогти вам захистити вашу програму від атак CSRF. Однією з таких бібліотек є бібліотека csurf для Express, яка надає просте у використанні проміжне програмне забезпечення для захисту вашої програми від атак CSRF.

Також важливо постійно оновлювати пакети React і npm, оскільки регулярно виявляються та виправляються нові вразливості безпеки. Будьте в курсі вразливостей системи React і підписайтеся на списки розсилки з питань безпеки, які допоможуть вам бути в курсі будь-яких нових загроз.

Вразливість у пакетах і залежностях. Уразливості в пакетах і

залежностях стосуються слабких місць безпеки або дірок у коді цих програмних компонентів, якими можуть скористатися зловмисники, щоб отримати несанкціонований доступ або завдати шкоди системам. Ці вразливості можуть виникати через низку причин, а саме: застарілі програмні компоненти; помилки кодування; недостатнє тестування; відсутність належного контролю безпеки. У багатьох випадках ці вразливості залишаються непоміченими протягом тривалого періоду, що дозволяє зловмисникам використовувати їх і скомпрометувати безпеку систем, які покладаються на уражені пакети або залежності.

Щоб уникнути вразливостей у пакетах і залежностях, важливо прийняти проактивний підхід, який передбачає регулярне сканування безпеки, тестування та моніторинг. Ось кілька найкращих практик безпеки React, які допоможуть у цьому:

- Оновлюйте компоненти програмного забезпечення, щоб забезпечити оперативне усунення будь-яких відомих вразливостей. Крім того, організації повинні запровадити засоби контролю безпеки, такі як контроль доступу, брандмауери та шифрування, щоб зменшити ризик використання.
- Регулярно переглядайте код пакетів і залежностей, щоб виявити й усунути будь-які потенційні недоліки безпеки. Також рекомендується використовувати перевірені та надійні джерела для завантаження й оновлення пакетів і залежностей, а також ретельно перевіряти код перед його використанням.
- Прийняття анадійна розробка програмного забезпеченняжиттєвий цикл (SDLC), який включає безпеку як критичний аспект і передбачає регулярне тестування безпеки та перегляд коду.

Порушена автентифікації та неавторизований доступ - є значною вразливістю безпеки, яка може вплинути на всі веб-програми, включно з програмами React. Погано реалізовані функції керування сеансом і процеси автентифікації можуть бути легко використані хакерами, щоб обійти або скомпрометувати рішення автентифікації, розміщені в додатку.

Порушена автентифікація - ця вразливість може призвести до маніпулювання інформацією про обліковий запис користувача, паролями, маркерами сеансу тощо. Основною причиною порушення автентифікації часто є неправильне впровадження засобів контролю доступу та ідентифікації. Деякі поширені фактори ризику безпеки в React, пов’язані з несправною автентифікацією, включають: передбачувані або легко вгадані облікові дані для входу; незахищені облікові дані користувача; ідентифікатори сеансу, які розкриваються в URL-адресі; уразливі ідентифікатори сеансу, чутливі до атак із фіксацією сеансу; значення сеансу, які не закінчуються або стають недійсними після виходу; ідентифікатори сеансу, які не змінюються після успішного входу; облікові дані, такі як паролі, ідентифікатори сеансу та інші, які надсилаються через незашифровані з’єднання.

Щоб уникнути порушення автентифікації, важливо дотримуватися цих найкращих практик безпеки React: застосування багатофакторної автентифікації,

де це можливо; примусова перевірка пароля на надійність; використання Рекомендації NIST 800-63 B для довжини та складності пароля; використання узгоджених повідомлень для всіх результатів, пов'язаних з автентифікацією; використання захищеного менеджера сеансів на стороні сервера для створення нового ідентифікатора сеансу кожного разу, коли користувач входить в систему. Крім того, надзвичайно важливо надійно зберігати ідентифікатори сеансу та робити їх недійсними після завершення сеансу, щоб забезпечити безпеку програми.

Блискавка. Zip slip — це вразливість у додатках React, яка дозволяє користувачам надсилати файли zip. Веб-розробники вмикають цю функцію, щоб зменшити розміри файлів під час їх завантаження. Потім програма розпаковує ці файли, щоб отримати оригінальні файли в zip. Zip slip — це в основному обхід каталогу, який хакери можуть використовувати для вилучення файлів, найчастіше з архіву. Застібка на блискавці – це коли іноді кілька частин файлової системи можуть залишатися за межами призначеної папки. Зловмисник може: отримайте доступ до цих частин файлу; замініть їх; викликати ці файли віддалено або змусити систему викликати їх. Таким чином їм вдається досягти віддаленого виконання команд на пристрої користувача, що може призвести до перезапису конфіденційних ресурсів, таких як файли конфігурації не лише на стороні клієнта, а й на стороні сервера.

Щоб уникнути прослизання в React є єдиний спосіб уникнути цієї пастки безпеки — переконатися, що в програму не потрапить шкідливий файл. Нижче наведено найкращі методи безпеки React для запобігання ковзанню zip у React: переконайтеся, що файли мають стандартні імена; заборона використання спеціальних символів у назвах файлів; завжди порівнюйте та зіставляйте імена з регулярними стандартними виразами; перейменування всіх завантажених файлів у архіві zip і створення нових імен для кожного з них перед тим, як програма їх використає або збереже.

Зовнішні сутності XML (XXE). У деяких випадках атаки XXE також вважаються типом ін'єкційних атак. Синтаксичні аналізатори XML, які є застарілими у вашій веб-програмі React, стають найбільш вразливими до зловживань через ін'єкційні атаки, що призводять до атак DoS. У таких нападах: зловмисник намагається зібрати конфіденційні дані з сервера; у деяких випадках атаки XXE підпадають під категорію ін'єкційних атак; застарілі XML-парсери у вашому веб-додатку React є найбільш вразливими до ін'єкційних атак, які призводять до DoS-атак; зловмисник прагне зібрати конфіденційні дані з сервера додатків.

Щоб уникнути атак безпеки XXE у програмах React треба використовувати найкращі методи безпеки React, а саме:

- Відсутність серіалізації конфіденційних даних, тобто треба використовувати складні формати JSON, щоб уникнути серіалізації. Деякі інструменти SAST можуть виявитися корисними для виявлення шкідливого XXE у вашому коді. Ви можете використовувати їх для захисту свого додатка React.
- Регулярно оновлюйте процесори XML, оскільки ця пастка безпеки

виникає через застарілі процесори XML.

Висновки.

Уразливості системи безпеки React можна запобігти шляхом впровадження найкращих практик безпеки, таких як перевірка даних, багатофакторна автентифікація, шифрування та регулярне сканування програми на наявність потенційних уразливостей. Регулярні оновлення програмного забезпечення та навчання розробників щодо ризиків безпеки також можуть допомогти уникнути вразливості безпеки React. Роблячи це, можна забезпечити захист свого веб-додатку від потенційних загроз, з'ясувати, як знайти витік пам'яті React, або зменшити вразливості create-react-app і підвищити його загальну безпеку.

Перелік посилань:

1. What is React.js and how can that technology be used to build a custom web application? // [Електронний ресурс] Режим доступу до ресурсу: https://crustlab.com/blog/what-is-react-js-and-how-can-that-technology-be-used-to-build-a-custom-web-application/
2. 7 Serious React Security Vulnerabilities and How To Avoid Them // [Електронний ресурс] Режим доступу до ресурсу: https://www.thirdrocktechkno.com/blog/react-security-vulnerabilities/
3. Lifecycle of Components// [Електронний ресурс] Режим доступу до ресурсу: https://www.w3schools.com/react/react_lifecycle.asp

Терепа Іван Романович
Студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ АВТОРИЗАЦІЇ ТА АВТЕНТИФІКАЦІЇ ВЕБ-ДОДАТКІВ НА БАЗІ ПРОТОКОЛУ OAuth 2.0

Зростання використання веб-додатків та інтернет-сервісів вимагає надійних методів забезпечення безпеки та конфіденційності користувачів. Отже, дослідження цієї технології стає надзвичайно актуальним. Протокол OAuth 2.0 надає додаткам можливість отримувати обмежений доступ до ресурсів користувачів, не розголошуючи їхні облікові дані. Ця технологія пропонує важливі переваги у забезпеченні безпеки веб-додатків та зручності користувачів при роботі з особистими даними. Дослідження та розвиток OAuth 2.0 відкривають нові можливості для захисту конфіденційності користувачів у світі сучасних веб-додатків і платформ.

Протокол OAuth 2.0 включає в себе декілька важливих кроків у процесі авторизації:

1. Запит на авторизацію: Додаток, який бажає отримати доступ до певних ресурсів користувача, починає запитувати дозвіл на доступ. Це ініціює запит на авторизацію.
2. Перенаправлення на сервер авторизації: Користувач перенаправляється на сервер авторизації, де він надає свій дозвіл на доступ до певних ресурсів.
3. Отримання авторизаційного коду: Після надання дозволу сервер авторизації видаватиме авторизаційний код.

4. Обмін коду на токен доступу: Додаток обмінює цей авторизаційний код на токен доступу, який надалі використовується для доступу до ресурсів користувача без введення його облікових даних.

5. Забезпечення безпеки та конфіденційності

Один із головних аспектів OAuth 2.0 — забезпечення безпеки та конфіденційності. Протокол використовує механізми, які дозволяють зменшити ризики витоку інформації, фішингу та незаконного використання доступу. Використання токенів доступу та оновлення їх строку дії є важливими складовими для захисту даних користувачів.

Багато веб-додатків і платформ вже успішно використовують OAuth 2.0 для забезпечення доступу та авторизації. Популярні соціальні мережі, електронні поштові сервіси та хмарні послуги використовують цей протокол для надання користувачам можливості взаємодіяти зі сторонніми додатками без ризику викладення своїх облікових даних.

OAuth 2.0 відкриває нові можливості для забезпечення безпеки та зручності веб-додатків та послуг. Використання цього стандарту спрощує процес авторизації для користувачів та надає їм більший контроль над своєю особистою інформацією. Майбутнє OAuth 2.0 обіцяє подальший розвиток та вдосконалення методів авторизації, зокрема у вигляді нових версій та додаткових розширень.

Загальна концепція протоколу OAuth 2.0 полягає в тому, щоб додатки могли спілкуватися між собою та з користувачами, забезпечуючи безпеку та конфіденційність. Ця технологія стає невід'ємною частиною сучасного цифрового світу, де збереження даних та доступ до них стають ключовими завданнями.

Перелік посилань:

- OAuth 2.0 URL: https://oauth.net/2/ (дата звернення: 26.09.2023)
- What is OAuth 2.0? URL: https://auth0.com/intro-to-iam/what-is-oauth-2 (дата звернення: 02.10.2023)

Терно Ярослав Анатолійович
студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ

В сучасному світі інформаційна безпека стає все більш важливою темою.

Кіберзлочинність залишається все більш прибутковою для шахраїв. За даними Statista, глобальні збитки від кібератак оцінюють у 7-7,1 трильйона доларів у 2022 році проти 1,2 трильйона доларів у 2019 році.

Протягом п'яти років кіберзлочинність більш модернізувалася та набирає

все більше популярності заради наживи.

У 2017 році витоки даних і фішинг всього становило 28%, тоді як крадіжки особистих даних, шахрайство з кредитними картками та інші види кібератак становлять невелику частку від загальної кількості зареєстрованих злочинів.

Рис.1. Топ 5 найпоширеніших форм Кіберзлоченів 2017

Протягом п'ять років фішинг став найпоширенішим видом кіберзагроз в інтернеті. Минулого року більше половини злочинної діяльності в Інтернеті було пов’язано з нею. Хоча фішинг електронної пошти існує з самого початку Інтернету, злочинці вдосконалють постійно цю техніку та створють спеціалізовані версії фішингу для різних каналів. Фішинг націлений на певну групу людей у компанії, часто використовуючи складнішу мову та жаргон, щоб обдурити потенційних жертв. Також існує вид шахрайства як смішинг — це SMS-шахрайство, тобто ще один вид обману за допомогою сервісів зв’язку. Метою злочинної схеми є змусити користувача перейти за шкідливим посиланням з SMS-повідомлення [2].

Рис.2. Топ 5 найпоширеніших форм Кіберзлоченів 2023

Короті правила користування інтернетом.

1. Не вказувати власні персональні дані на неперевірених сайтах.
2. Нікому не повідомляти термін дії банківської карти та CVV-код.
3. Перевіряти гіперпосилання та наповнення сайту на відповідність офіційним даним компаній.
4. У разі отримання спірних листів чи повідомлень не здійснювати ніяких оплат до встановлення обставин ситуації, що виникла.
5. Не робити передоплат у неперевірених інтернет-магазинах.
6. Не користуватися неперевіреними оголошеннями щодо роботи, яка обіцяє швидкий заробіток за внесення завдатку.

Короті правила перевірки особи яка телефонує до вас.

Месенджери

Осіб, які телефонували з певного номера, можна спробувати знайти в месенджерах, встановлених на смартфон. Найбільш поширені — Viber, Whatsapp і Telegram. Це найпопулярніший спосіб уточнення деталей абонента. Хоча інформація обмежена фото та коротким описом профілю. Якщо пощастить — є шанс дізнатися ім'я, прізвище та компанію, яку представляємо можливий менеджер.

Getcontact

Це служба обміну повідомленнями з більш ніж 250 мільйонами користувачів. Після інсталяції програми можна швидко дізнатися ідентифікатор абонента. Працює навіть якщо дані не збережені у книзі контактів. Основна функція додатка — фільтрація вхідних дзвінків та спам фільтр [4].

Спостерігаючи за цими даними, можна зрозуміти "Актуальні проблеми кібербезпеки" зростає з кожним днем. Тому що більша половина населення землі не може розпізнати злодія завчасно та довір'я свої особисті дані.

Перелік посилань:
1. Дані Statista URL: https://www.statista.com/ (дата звернення: 07.10.2023).
2. Смішинг – SMS-шахрайства URL: https://charivne.info/news/politsiya-poperedzhae-pro-smishinh---sms-shakhraystvo (дата звернення: 07.10.2023).
3. Як не стати жертвою шахраїв в інтернеті та що робити, якщо ви потрапили у пастку URL: https://minjust.gov.ua/m/yak-ne-stati-jertvoyu-shahraiv-v-interneti-ta-scho-robiti-yakscho-vi-potrapili-u-pastku (дата звернення: 07.10.2023).
4. Як дізнатися, хто телефонував з невідомого номера - 4 додатки URL: https://www.moyo.ua/ua/news/kak_uznat_kto_zvonil_s_neizvestnogo_nomera_3_prilozheniya_i_4_alternativy.html (дата звернення: 07.10.2023).

Тищенко Віталій Сергійович,
асистент кафедри УІКБ, , ННІЗІ ДУІКТ, Київ, Україна
Мужанова Тетяна Михайлівна,
к.держ.упр., доц., доц. каф. УІКБ, ННІЗІ ДУІКТ, Київ, Україна

ШТУЧНИЙ ІНТЕЛЕКТ У КІБЕРБЕЗПЕЦІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

У цифрову епоху кібербезпека є одним із найважливіших викликів для бізнесу та суспільства. Зростання кількості кібератак, які можуть призвести до серйозних фінансових втрат, втрати довіри клієнтів та шкоди репутації, вимагає нових підходів до захисту від цих загроз. Штучний інтелект (ШІ) може відігравати важливу роль у зміцненні кібербезпеки, дозволяючи ефективно виявляти та реагувати на загрози в режимі реального часу. Використання ШІ у кібербезпеці може допомогти організаціям запобігти серйозним фінансовим втратам, шкоді репутації та порушенням конфіденційності. Однак для ефективного використання ШІ в кібербезпеці необхідно вирішити ряд проблем, таких як забезпечення надійності та безпеки ШІ-систем, а також розробка методів навчання ШІ на великих обсягах даних про кібератаки.

Штучний інтелект (ШІ) може відігравати важливу роль у зміцненні кібербезпеки, дозволяючи ефективно виявляти та реагувати на загрози в режимі реального часу. ШІ можна використовувати для:

Моніторингу мереж та систем на наявність ознак кібератак, таких як незвичайна активність, аномалії в трафіку або зміни в конфігурації. ШІ-системи можуть аналізувати великі обсяги даних про мережеву активність, щоб виявити ознаки кібератак, які можуть бути непомітними для людини.

Автоматизації завдань із реагування на інциденти, таких як виявлення та ізоляція заражених систем, відновлення даних та повідомлення користувачів про загрози. ШІ-системи можуть автоматизувати завдання із реагування на інциденти, що дозволяє кібербезпековим командам швидше реагувати на загрози та мінімізувати їхній вплив [1].

Розробки нових методів захисту від кібератак, таких як використання машинного навчання для виявлення нових видів зловмисного програмного

забезпечення або створення штучних інтелектів, які можуть протистояти зловмисникам у кібервійнах. ШІ може бути використаний для розробки нових методів захисту від кібератак, які є більш ефективними та стійкими до нових загроз.

Штучний інтелект (ШІ) має значний потенціал для поліпшення кібербезпеки корпоративних інформаційних систем, але його використання також супроводжується рядом проблем та обмежень, які важливо враховувати [2]:

1. Недостатня кількість даних для навчання ШІ-моделей: Однією з ключових проблем використання ШІ в кібербезпеці є необхідність великої кількості даних для навчання моделей. ШІ-системи, такі як нейронні мережі, вимагають значного обсягу інформації для ефективного функціонування. У сфері кібербезпеки може бути складно надати достатньо данних, особливо коли розглядаються нові атаки та загрози.

2. Труднощі інтерпретації результатів: Результати, отримані внаслідок застосування ШІ-моделей, може бути важко інтерпретувати людиною. Це може створити труднощі для фахівців у розумінні та прийнятті обгрунтованих рішень на основі цих результатів. Наприклад, нейронні мережі можуть визначити аномалії в поведінці системи, але інтерпретація цих аномалій може бути складною.

3. Ризик витоку конфіденційної інформації: Для навчання ШІ-моделей, часто використовуються дані, які можуть бути конфіденційними. Це створює ризик витоку цієї конфіденційної інформації. Якщо навчальні дані потраплять в руки атакуючого, це може призвести до серйозних наслідків для безпеки даних.

Ці проблеми та обмеження не повинні заважати розвитку та впровадженню ШІ в кібербезпеку, але вони вимагають ретельного вивчення та розробки стратегій для їх подолання. Важливо розробляти методи захисту конфіденційності даних та створювати інтерпретаційні інструменти, які дозволять зрозуміти рішення, прийняті ШІ-системами.

Незважаючи на ці проблеми, ШІ має потенціал для того, щоб стати потужним інструментом у боротьбі з кібератаками. Організації, які впроваджують ШІ у свої кібербезпекові стратегії, можуть отримати значні переваги у вигляді підвищення ефективності захисту, зниження витрат і зменшення ризику кібератак.

Для ефективного використання штучного інтелекту (ШІ) в галузі кібербезпеки важливо дотримуватись наступних рекомендацій:

- Використовувати ШІ-моделі, навчені на великих обсягах даних: Однією з основних передумов успішного впровадження ШІ в кібербезпеку є наявність великої кількості даних для навчання моделей. Збирайте і зберігайте дані про кібератаки, загрози та аномалії для покращення якості моделей.
- Впроваджувати механізми забезпечення конфіденційності даних: Конфіденційність інформації є критично важливою, особливо в контексті кібербезпеки. Розробляйте та впроваджуйте механізми захисту конфіденційних

даних, використовуваних для навчання ШІ-моделей. Це включає шифрування даних та засоби анонімізації.

- Розробляти інтерпретаційні інструменти для ШІ-моделей: Однією зі складнощей використання ШІ-моделей є інтерпретація результатів. Розробка інтерпретаційних інструментів та платформ для зрозуміння рішень, прийнятих ШІ-системами, допоможе ефективніше реагувати на загрози та вчасно виявляти аномалії.

ШІ може підвищити ефективність кібербезпеки, допомагаючи виявляти та запобігати кіберзагрозам, автоматизуючи завдання та розробляючи нові методи захисту. Для успішного впровадження ШІ в кібербезпеку важливо дотримуватися рекомендацій та розвивати нові підходи до цієї технології.

Перелік посилань:

1. Artificial intelligence-based cyber security in the context of industry 4.0–A survey / A. J. G. de Azambuja et al. Electronics. 2023. Vol. 12, no. 8. P. 1920. URL: https://doi.org/10.3390/electronics12081920
2. Interpretable machine learning / V. Chen et al. Communications of the ACM. 2022. Vol. 65, no. 8. P. 43–50. URL: https://doi.org/10.1145/3546036

Торкін Дмитро Станіславович
Державний університет інформаційно-комунікаційних технологій

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ТА СИСТЕМА МОНІТОРИНГУ ZABBIX

Анотація

У сучасному світі кібербезпека стала однією з найважливіших та актуальних галузей інформаційної безпеки. Цей звіт розглядає актуальні виклики, з якими стикаються компанії та організації в сфері кібербезпеки, і визначає, як система моніторингу Zabbix може вирішити ці проблеми.

Надається аналіз викликів, пов'язаних з атаками на застарілі протоколи, штучний інтелект, мережі IoT, мережі 5G та шифрування трафіку.

За допомогою системи моніторингу Zabbix, автор звіту аргументує, що компанії можуть ефективно виявляти, аналізувати та реагувати на ці загрози. Zabbix надає централізований моніторинг та аналіз даних, автоматизовану реакцію на інциденти, моніторинг безпеки облікових записів та інші інструменти, що сприяють захисту інфраструктури та цифрових активів.

Зазначена система стає необхідною для компаній та організацій, які бажають захистити свою інформацію та мережі від зростаючих кіберзагроз у сучасному світі.

Актуальні виклики кібербезпеки

Атаки на застарілі протоколи та системи: Сучасні атаки націлені на вразливості старих протоколів та систем, що використовуються в компаніях та організаціях. Важливо поновлювати та моніторити застарілі програмні рішення та використовувати системи моніторингу для виявлення потенційних вразливостей.

Атаки на штучний інтелект і машинне навчання: Зловмисники використовують технології штучного інтелекту для вдосконалення своїх атак і

обходу захисту. Компанії повинні вдосконалювати свої системи моніторингу, щоб виявляти незвичайні алгоритми та поведінку, що можуть вказувати на зловмисну діяльність.

Атаки на Інтернет речей (IoT): З підключенням все більшої кількості пристроїв до Інтернету зростає загроза атак на мережу IoT. Використання систем моніторингу для нагляду за активністю IoT-пристроїв може допомогти виявляти та запобігати можливим атакам.

Атаки на мережі 5G та розширені мережі: Розгортання мереж 5G створює нові можливості для атак та шпигунства. Застосування систем моніторингу для постійного аналізу мережі 5G допомагає виявляти та реагувати на загрози.

Атаки на шифрування трафіку: Зловмисники розвивають методи обходу шифрування, щоб доступатися до конфіденційних даних. Системи моніторингу повинні бути здатні розпізнавати аномальну активність, яка може вказувати на такі атаки.

Ці виклики показують, що кібербезпека стає все складнішою і вимагає вдосконалення інструментів моніторингу та захисту для ефективного протистояння сучасним загрозам.

Система моніторингу Zabbix і боротьба з актуальними викликами кібербезпеки

Атаки на застарілі протоколи та системи: Zabbix надає можливість встановлювати моніторинг параметрів і стану системи, включаючи застарілі програмні рішення. Ця система може вчасно виявляти вразливості та проблеми в застарілих компонентах, що дозволяє адміністраторам негайно реагувати на потенційні загрози.

Атаки на штучний інтелект і машинне навчання: Zabbix включає можливості для моніторингу та аналізу системи. Вона може надавати дані для навчання моделей штучного інтелекту, щоб виявляти аномалії та незвичайні алгоритми. Інтеграція системи Zabbix з іншими рішеннями для детектування загроз може зробити цей процес більш ефективним.

Атаки на Інтернет речей (IoT): Завдяки своїй розширюваності, Zabbix може бути використана для моніторингу великої кількості IoT-пристроїв. Вона може виявляти аномальну активність цих пристроїв та автоматично сповіщати про можливі загрози.

Атаки на мережі 5G та розширені мережі: Zabbix може інтегруватися з розширеними мережами, включаючи мережі 5G. Вона здатна виявляти незвичайні патерни активності та швидко сповіщати про проблеми, пов'язані з мережами високої швидкості.

Атаки на шифрування трафіку: За допомогою аналізу мережевого трафіку та даних, Zabbix може виявляти аномальну активність, яка може вказувати на спроби обходу шифрування. Вона може висвітлювати такі активності та надсилати сповіщення адміністраторам для негайного реагування.

Забезпечуючи потужні засоби моніторингу та інтеграції з іншими системами кібербезпеки, Zabbix стає важливим інструментом у боротьбі з

актуальними викликами кібербезпеки. Вона допомагає вчасно виявляти та реагувати на загрози, що забезпечує надійний захист цифрових активів та мереж.

Забезпечення централізованого моніторингу та аналізу даних

Забезпечуючи централізований моніторинг і збір метрик з різних джерел, система Zabbix дозволяє адміністраторам та кібербезпецістам отримувати повний інсайт у стан системи та мережі. Це особливо важливо в умовах зростаючої складності кіберзагроз. Поєднуючи дані з багатьох джерел, включаючи сервери, мережеві пристрої, сервіси та додатки, Zabbix створює повну картину активності, що спрощує виявлення аномалій та загроз.

Автоматизація реакції на загрози

Zabbix не лише виявляє потенційні загрози, але й надає можливість налаштування автоматизованих реакцій на події та аномалії. Це включає в себе автоматичну відключення атакувальних IP-адрес, збільшення рівня моніторингу для ресурсів, що стають цільовими, а також автоматичне повідомлення кібербезпецістів.

Моніторинг безпеки облікових записів та доступу

Zabbix може вести моніторинг активності облікових записів, що дозволяє виявляти незвичайну активність та спроби несанкціонованого доступу. Використовуючи систему моніторингу Zabbix, компанії можуть забезпечити, що доступ до цінних даних обмежується лише необхідним співробітникам.

Аналіз та відстеження інцидентів

Zabbix також може слугувати як інструмент для аналізу та відстеження кіберінцидентів. Збір і збереження історичних даних дозволяє проводити ретроспективний аналіз подій та встановлення причин атак. Це значно полегшує подальший вдосконалення стратегії кібербезпеки.

Висновок

Завдяки своїм потужним засобам моніторингу, інтеграції з іншими системами безпеки, та здатності до автоматизованої реакції на загрози, система моніторингу Zabbix стає незамінним інструментом у боротьбі з актуальними викликами кібербезпеки. Вона не лише допомагає виявляти потенційні загрози, але і допомагає вирішувати їх ефективно та надійно, забезпечуючи захист цифрових активів та інфраструктури.

Перелік посилань:
1. https://www.zabbix.com/ru

Марценюк Олександр Вячеславочич,
студент групи УБДМ-61, ННІЗІ ДУІКТ, Київ, Україна

SIEM СИСТЕМИ (SECURITY INFORMATION AND EVENT MANAGEMENT) – ЩО ЦЕ І НАВІЩО ПОТРІБНО?

Що таке SIEM і навіщо вона потрібна? По суті SIEM - це система, що накопичує в собі всі дані (журнали роботи або, як кажуть фахівці, логи) від інших засобів захисту, що вміє розуміти багато

«формати» логів з різних джерел - засобів захисту, швидко шукати потрібну інформацію в цих логах, тривалий час їх зберігати. Крім цього, SIEM-система повинна вміти виконувати низку додаткових дій: здійснювати таксономію (розподіляти дані, що надходять за типами та категоріями) і кореляцію (тобто пов'язувати здавалося б розрізнені події між собою), надсилати повідомлення відповідальним особам про виявлені підозрілі події в журналах , надавати додаткову інформацію щодо кожного з подій та пристроїв у мережі.

Як працюють SIEM системи? Що робить SIEM-система, у чому користь від її застосування, які функції виконує SIEM? Відповімо по порядку. Перше завдання SIEM – отримати дані від джерела. Це може бути як «активне» джерело, яке вміє передавати дані в SIEM і йому достатньо вказати мережеву адресу приймача, так і «пасивний», до якого SIEM-система повинна звернутися сама. Отримавши джерела дані, SIEM-система перетворює в одноманітний, придатний для подальшого використання формат - це називається нормалізацією. Порівняємо це з великою компанією людей з різних країн: усі говорять своїми мовами, а SIEM-система всіх слухає та нормалізує, тобто. перекладає все англійською, щоб потім можна було переглянути всю розмову єдиною, зрозумілою мовою.

Далі SIEM-система виконує таксономію, тобто. класифікує вже нормалізовані повідомлення в залежності від їх змісту: яке подія говорить про успішну мережеву комунікацію, яке - про вхід користувача на ПК, а яке - про спрацювання антивірусу. Таким чином, ми отримуємо вже не просто набір записів, а послідовність подій з певним змістом та часом настання. Отже, ми можемо зрозуміти, як і послідовності йшли події і який може бути зв'язок між ними. Тут гру входить основний механізм SIEM-систем: кореляція. Кореляція в SIEM - це співвідношення між собою подій, які відповідають тим чи іншим умовам (правилам кореляції). Приклад правила кореляції: якщо на двох і більше ПК протягом 5-ти хвилин спрацював антивірус, це може свідчити про вірусну атаку на компанію. Більш складне правило: якщо протягом 24 годин були зафіксовані чиїсь спроби віддалено зайти на сервер, які зрештою увінчалися успіхом, а потім з цього сервера почалося копіювання даних на зовнішній файлообмінник, це може свідчити про те, що зловмисники підібрали пароль до облікового запису, зайшли всередину сервера та крадуть важливі дані. За підсумками спрацьовування правил кореляції в SIEM-системі формується інцидент інформаційної безпеки (у деяких системах, наприклад в SIEM IBM QRadar інцидент називається Offense). При цьому фахівець з ІБ при роботі з SIEM повинен мати можливість швидкого пошуку по попереднім інцидентам і подіям, що зберігаються в SIEM-системі, на випадок, якщо йому знадобиться будь-які додаткові технічні подробиці для розслідування атаки.

Отже, основні завдання SIEM-систем такі:

1. Отримання журналів із різноманітних засобів захисту
2. Нормалізація отриманих даних
3. Таксономія нормалізованих даних
4. Кореляція класифікованих подій

5. Створення інциденту, надання інструментів щодо розслідування

6. Зберігання інформації про події та інциденти протягом тривалого часу (від 6 місяців)

7. Швидкий пошук за даними, що зберігаються в SIEM

Крім зазначеного функціоналу, SIEM-системи можуть також оснащуватися додатковими функціями, такими як управління ризиками та вразливістю, інвентаризація IT-активів, побудова звітів та діаграм тощо. Автоматизоване реагування на інцидент також можна налаштувати, для цього використовують системи IRP (Incident Response Platform, платформи реагування на інциденти інформаційної безпеки), які можуть без участі людини, наприклад, заблокувати зламаний обліковий запис або відключити інфікований ПК від мережі.

Користь від впровадження та застосування SIEM-системи полягає в тому, що вона значно прискорює процес обробки інцидентів ІБ та отримання необхідної інформації про події ІБ: аналітику не потрібно підключатися до кожного засобу захисту інформації, він бачить усі дані в єдиному консолідованому вигляді в одному зручному інтерфейс. Якщо у компанії відповідно до законодавства є вимоги до зберігання всіх журналів аудиту (тобто логів) засобів захисту за певний часовий період, наприклад, не менше ніж за рік, то використання SIEM-систем дозволяє виконати цю вимогу. Якщо ж компанія серйозно стурбована оперативним реагуванням на інциденти інформаційної безпеки, то можна замислитись про організацію свого Центру SOC, ядром якого стане SIEM-система. Зрозуміло, при впровадженні та налаштуванні SIEM-систем існують очевидні труднощі як організаційного, так і технічного характеру: крім покупки самої SIEM-системи доведеться ще налаштувати всі джерела даних на відправку даних у SIEM, створювати правила кореляції, усувати причини хибно-позитивних спрацьовувань, підтримувати SIEM-систему в актуальному стані, оперативно розслідувати інциденти інформаційної безпеки, що згенеровані SIEM. Але ця гра коштує свічок, оскільки на кону стоїть безпека даних, а значить - найціннішого, що часом є у компанії.

Перелік посилань:

3. SIEM системы (Security Information and Event Management) - что это и зачем нужно? https://www.securityvision.ru/blog/siem-chto-eto-i-zachem-nuzhno/

4. Information Security Journal: A Global Perspective, Vol. 2, (2017). URL: https://www.tandfonline.com/toc/uiss20/current

Федієнко Олександр Павлович,
здобувач,
Київ, Україна

ЩОДО УДОСКОНАЛЕННЯ ЗАКОНОДАВЧОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ВІЙНИ

В сучасних умовах мають бути уточнені законодавчі основи забезпечення кібербезпеки, особливо під час війни. Вирішення цих стратегічних завдань є першочерговою сферою відповідальності нашого політикуму на державному рівні. Важливим залишається деталізація та визначення основних засад й пріоритетів державної кібербезпекової політики. Узагальнено, що мають бути регламентовані та окреслені перспективи удосконалення законодавчого забезпечення кібербезпеки з урахуванням кращих практик та моделей сучасного європейського досвіду. Розглянуто закон ЄС про кібербезпеку та на його підставі деталізовано відповідний понятійний апарат. Висвітлено досвід Молдови у сфері гармонізації національного законодавства відповідно до нормативних вимог ЄС. Оскільки кіберзагрози постійно і динамічно змінюються, необхідним є перегляд основ законодавчої платформи у сфері забезпечення кібербезпеки, у першу чергу, профільного закону про кібербезпеку в умовах тотальної війни у кібердомені.

В сучасних умовах кібербезпека та її складові регулюються Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163 [1]. Цей законодавчий акт набув чинності у травні 2018 році та є декларативним і формалізованим, й по суті оперує лише базовими поняттями у вказаній сфері. Проте тезаурус та понятійно–категоріальний апарат у вказаному законодавчому акті потребують уточнення та деталізації, оскільки не узгоджується із європейськими стандартами та регламентами у сфері кібербезпеки, особливо в умовах євроінтеграційних процесів, які анонсувала наша держава, глобальних викликів, російської військової агресії та війни у кібердомені.

На наш погляд, у вказаному законодавчому акті порушена логіко–структурна модель викладення норм законодавства, оскільки, наприклад, у цьому акті відсутнє поняття «забезпечення кібербезпеки», «кібердомен», не розкрито особливості забезпечення кібербезпеки в умовах кібервійни, яку веде проти України держава–агресор. Основні напрямки розбудови державної політики у сфері забезпечення кібербезпеки ретельно не окреслені. Це є свідченням необхідності корегування та уточнення норм законодавства, присвячених кібербезпековій тематиці на законодавчому рівні, особливо в умовах правового режиму воєнного стану. Наприклад, у законі «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163 відсутні чітко визначені організаційно–правові та техніко–економічні засади забезпечення кібербезпеки саме в умовах воєнного стану, завдання та функції уповноважених та відповідальних суб'єктів, розмежування сфер відповідальності на рівні сектору безпеки і оборони із зазначених питань. На жаль, поза увагою законодавця у цьому акті залишилися питання інституційного та прогресивного розвитку кібербезпеки, механізмів та гарантій її забезпечення, посилення відповідальності за скоєння кримінальних правопорушень у цій сфері в умовах кібервійни.

Положення закону не враховують такий момент, що кібербезпека не є річчю в собі, замкнутої тільки на комп'ютерних системах або телекомунікаційних мережах. Із системних позицій заходи щодо забезпечення кібербезпеки насамперед спрямовані на збереження якості функціонування соціальних і соціотехнічних систем, до складу яких входять відповідні комп'ютерні системи та телекомунікаційні мережі. Тому основними критеріями ефективності заходів щодо забезпечення кібербезпеки повинні бути класифікатори, що базуються на оцінці якості функціонування соціальних і соціотехнічних систем. Наприклад, якщо реалізація кіберзагроз навіть і призводить до порушення роботи комп'ютерних систем, але це майже не позначається на якості функціонування відповідної соціальної або соціотехнічної системи, у зв'язку з чим гострота проблеми забезпечення кібербезпеки різко падає. Отже, проблема оцінки стану кібербезпеки повинна передусім розглядатися в нерозривному зв'язку з оцінкою можливих чи завданих збитків соціальним або соціотехнічним системам як системам більш високого порядку. При цьому, забезпечення кібербезпеки включає, поряд з іншими, і заходи правоохоронного, військового, розвідувального, контррозвідувального, оперативно-розшукового, а також політичного, інформаційного, організаційно-правового, технологічного, соціального, освітянського, наукового характеру та заходи щодо організації дієвого кіберзахисту та кібероборони з метою мінімізації та недопущення кібератак, настання кіберінцидентів, боротьби з транснаціональною кіберзлочинністю та кібертероризмом тощо.

Заслуговує на увагу той факт, що в аспекті діючих нормативно-правових актів за рахунок внесення змін у ключові терміни можливий перегляд їх мети та сфери поширення. Вбачається доцільним, наприклад законодавчо закріпити таке розгорнуте визначення: кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

Сучасний етап формування вітчизняного законодавства у сфері кібербезпеки є надзвичайно динамічним. Становлення національного правового інституту та понятійно-категоріального апарату кібербезпеки, напряму пов'язується з розвитком міжнародного права у цій площині і, перш за все, європейського, яке слугувало певним стандартом у сфері глобальної інформаційної та телекомунікаційної захищеності суспільства. Зокрема, у 2019 році набув чинності новий Регламент ЄС 2019/ 881, який ще вважають Законом ЄС про кібербезпеку «Cybersecurity Act» [2]. В цьому законі кібербезпека означає діяльність, необхідну для захисту мережевих та інформаційних систем, користувачів таких систем та інших осіб, постраждалих від кіберзагроз. Це визначення відрізняється від того, яке було запропоноване в Стратегії

кібербезпеки ЄС ще у 2013 році в тому контексті, що діяльність щодо захисту від кіберзагроз спрямована не тільки на саму інформаційну систему, але й на користувачів таких систем. Так, впроваджуючи європейські стандарти у вітчизняне законодавство, Молдова у травні 2023 року, використовуючи кращі практики ЄС у сфері кібербезпеки прийняла національний закон про кібербезпеку [3], який набуває чинності з 1 січня 2025 року. Поняття кібербезпеки у цьому законодавчому акті повністю трансформовано із Закону ЄС про кібербезпеку, що є свідченням імплементації законодавства Молдови відповідно до європейських нормативних вимог у сфері забезпечення кібербезпеки.

Тобто загальноприйнята світова практика заснована на необхідності уточнення базових понять та термінології у сфері забезпечення кібербезпеки у рамках глобального, регіонального та національного рівнів, виходячи із сучасних загроз та викликів. В умовах воєнного стану, який триває у нашій державі понад 600 днів, актуалізуються питання визначення у абсолютно новій редакції поняття, змісту та особливостей забезпечення кібербезпеки, особливо в умовах кібервійни. На жаль, діючим законом не визначено основного суб'єкта забезпечення кібербезпеки, що досить все ще значно ускладнює парадигму та ієрархічну систему побудови комунікацій і вертикалі підпорядкування суб'єктів забезпечення кібербезпеки. Цитований закон позбавлений практичної складової реалізації державної політики у сфері забезпечення кібербезпеки. Положення цього закону не узгоджується із отриманими здобутками та напрацюваннями у сфері кібербезпеки, а набутий досвід впровадження норм закону та його загальнотеоретичниxx засад у практичну площину продемонстрував хибний підхід та є доволі проблематичним.

Таким чином, закон «Про основні засади забезпечення кібербезпеки України» є виключно декларативним та таким, що не відповідає сучасним реаліям, є досить застарілим, оскільки він теоретично відірваний від існуючої практики використання та застосування його норм, сучасних методологічних процесів забезпечення кібербезпеки в умовах кібервійни. Цей акт вітчизняного законодавства не відповідає сучасним засадам розбудови вітчизняної системи кібербезпеки в умовах воєнного стану з урахуванням кращих практик та стандартів європейського досвіду, що вимагає рішучих дій у напрямку негайної розробки нового та сучасного проекту законодавчого акту в окресленій площині. Це надасть змогу значно покращити та удосконалити законодавчі основи державної кібербезпекової політики в умовах правового режиму воєнного стану.

Перелік посилань:

1. Про основні засади забезпечення кібербезпеки: Закон України від 5 жовтня 2017 року №2163 URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Cybersecurity Act URL: Regulation (EU) 2019/881 of the European Parliament and of the Council URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

3. Moldova adopted the EU-backed Cybersecurity Law URL: https://www.eeas.europa.eu/delegations/moldova/moldova-adopted-eu-backed-cybersecurity-law_en?s=223

Філатов Герман Андрійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

WHAT IS BLOCKCHAIN SECURITY?

Basic blockchain security

Blockchain technology produces a structure of data with inherent security qualities. It's based on principles of cryptography, decentralization and consensus, which ensure trust in transactions. In most blockchains or distributed ledger technologies (DLT), the data is structured into blocks and each block contains a transaction or bundle of transactions. Each new block connects to all the blocks before it in a cryptographic chain in such a way that it's nearly impossible to tamper with. All transactions within the blocks are validated and agreed upon by a consensus mechanism, ensuring that each transaction is true and correct.

Blockchain technology enables decentralization through the participation of members across a distributed network. There is no single point of failure and a single user cannot change the record of transactions. However, blockchain technologies differ in some critical security aspects.

Blockchain security tips and best practices

When establishing a private blockchain, ensure that it's deployed in a secure, resilient infrastructure. Poor underlying technology choices for business needs and processes can lead to data security risks through their vulnerabilities.

Consider business and governance risks. Business risks include financial implications, reputational factors and compliance risks. Governance risks emanate primarily from blockchain solutions' decentralized nature, and they require strong controls on decision criteria, governing policies, identity and access management.

Blockchain security is about understanding blockchain network risks and managing them. The plan to implement security to these controls makes up a blockchain security model. Create a blockchain security model to ensure that all measures are in place to adequately secure your blockchain solutions.

Перелік посилань:

1. What is blockchain security? URL: https://www.ibm.com/topics/blockchain-security (дата звернення: 25.10.2023).

Філатов Герман Андрійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENHANCING CORPORATE INFORMATION SYSTEM CYBERSECURITY: OPPORTUNITIES AND CHALLENGES.

Opportunities of AI in Cybersecurity

AI has the potential to revolutionize the cybersecurity landscape by automating and enhancing various security processes. Some of the key opportunities of AI in cybersecurity include:

Threat detection and prevention: AI algorithms can analyze vast amounts of data and detect patterns that may indicate a cyber threat. By automating threat detection and prevention, organizations can enhance their security posture and respond more quickly to threats.

Incident response: AI can also be used to automate incident response processes, such as identifying the source of an attack and containing it. This can reduce the time it takes to respond to a cyber incident and minimize its impact.

Vulnerability management: AI can analyze vulnerabilities and prioritize them based on their severity, enabling organizations to allocate their resources more efficiently.

Fraud detection: AI can be used to detect fraudulent activity, such as phishing attempts and social engineering attacks, by analyzing user behavior and identifying anomalies.

Challenges of AI in Cybersecurity

While AI offers many opportunities in cybersecurity, it also presents some challenges. Some of the key challenges of AI in cybersecurity include:

Bias: AI algorithms may be biased if they are trained on a limited dataset or if the data used to train them contains inherent biases.

Complexity: AI algorithms can be complex and difficult to understand, making it challenging to troubleshoot and debug them.

Cyber attacks: AI algorithms can also be vulnerable to cyber attacks, such as adversarial attacks that manipulate the data used to train them.

Legal and ethical concerns: The use of AI in cybersecurity raises legal and ethical concerns, such as privacy and data protection issues.

Перелік посилань:

1. Смартфони та корпоративна інформація: основні ризики та як їм запобігти URL: https://www.cyberneticsearch.com/blog/the-role-of-ai-in-cybersecurity--opportunities-and-challenges(дата звернення: 25.10.2023).

Хон Герман Вячеславович
студент групи УБД-42, ННІЗІ ДУІКТ, Київ, Україна

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ З ПОСТІЙНО ЗРОСТАЮЧИМИ ЗАГРОЗАМИ ТА РИЗИКАМИ В ЦИФРОВОМУ СВІТІ

У сучасному світі спостерігається експоненційний ріст кількості кіберзлочинів, що ставлять під загрозу конфіденційність, цілісність та доступність корпоративних даних[1]. Ці напади можуть призвести до фінансових втрат та пошкоджень репутації підприємств. Сучасні корпоративні інформаційні системи стають все більш складними та взаємопов'язаними, що ускладнює завдання забезпечення кібербезпеки. Багато аспектів бізнесу, від фінансів до операцій, залежать від надійності цих систем. Уряди та регулятори вводять все більше обмежень і вимог щодо кібербезпеки. Невиконання цих вимог може призвести до великих штрафів та правових наслідків для компаній. Підприємства стають все більше залежними від цифрових технологій для виробництва, управління та збереження даних. В разі кібератаки, може виникнути серйозний збій у бізнес-процесах. Багато користувачів та співробітників компаній не мають належної освіти та усвідомленості щодо кібербезпеки, що робить їхніх роботодавців більш вразливими перед кіберзлочинцями. Багато вчених та експертів в галузі інформаційної безпеки провели дослідження з проблеми кібербезпеки корпоративних інформаційних систем. До них відносяться такі авторитети як Б. Шнаєр, К. Митник, та багато інших. Їхні дослідження та рекомендації мають велике значення для розробки стратегій забезпечення кібербезпеки.

Проблема кібербезпеки корпоративних інформаційних систем полягає в забезпеченні конфіденційності, цілісності та доступності даних, а також у захисті від кіберзлочинців і загроз, які можуть завдати збитків бізнесу. Ця проблема включає в себе багато аспектів, такі як [2]:

1. Кібератаки: Це включає в себе вторгнення в комп'ютерні системи, злам паролів, використання шкідливих програм і багато іншого. Кібератаки можуть призвести до крадіжок даних, втрати фінансових активів і порушення конфіденційності клієнтів.
2. Внутрішні загрози: Не завжди загрози приходять ззовні. Інсайдери, які мають доступ до систем, можуть завдати серйозних збитків, якщо їх дії не контролюються належним чином.

3. Відсутність належної культури кібербезпеки: Багато компаній не надають належної уваги навчанню та усвідомленості в галузі кібербезпеки серед своїх співробітників, що робить їх вразливими перед соціальними інженерами та іншими загрозами.

4. Захист даних: Важливо забезпечити ефективний захист даних, використовуючи шифрування, бекапи та строгий контроль доступу до інформації.

5. Навчання та усвідомленість: Співробітників повинно навчати та підвищувати їхню усвідомленість щодо кібербезпеки. Це може включати в себе регулярні тренінги та інструкції.

6. Використання сучасних технологій: Використання сучасних інструментів для виявлення, відгуку та захисту від кібератак може значно підвищити рівень безпеки.

7. Постійне оновлення політик і процедур: Компанії повинні постійно переглядати та оновлювати свої політики та процедури з кібербезпеки для врахування нових загроз.

8. Співпраця з експертами з кібербезпеки: Залучення професіоналів у галузі кібербезпеки для аудиту та консультацій може допомогти виявити та усунути слабкі місця в системах безпеки.

Таким чином, підсумовуючи вищезазначене, можна дійти висновку, що забезпечення кібербезпеки корпоративних інформаційних систем - це постійний інвестиційний процес, який вимагає уваги та зусиль, але це необхідно для забезпечення стійкості інформаційних активів підприємства в цифровому світі.

Перелік посилань:

1. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с. (дата звернення 24.10.2023)

2. Кібергігієна. Кібербезпека. Безпека держави: матеріали наукових семінарів (Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. – Київ : Київ. нац. торг.-екон. ун-т, 2020. – с. 81–83 (дата звернення 24.10.2023)

Хотько Олексій Петрович, БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ АНОМАЛЬНОГО ТРАФІКУ У КОРПОРАТИВНІЙ МЕРЕЖІ НА БАЗІ QRADAR NETWORK THREAT ANALYTICS

Визначено мету і основні завдання щодо виявлення аномального трафіку у корпоративній мережі. Розглянуто методи та засоби аномального трафіку у корпоративній мережі. Розроблено рекомендації щодо виявлення аномального трафіку у корпоративній мережі на базі QRadar Network Threat Analytics.

Вартість кібератак зловмисників неухильно зростає і очікується, що до 2023 року збитки від них перевищать 30 мільярдів доларів у всьому світі [1]. Виявлення аномального трафіку в корпоративній мережі є критично важливим завданням для забезпечення мережевої безпеки. Проблема виникає через те, що в мережі важко відрізнити нормальний трафік від аномального, особливо зі зростанням складності та обсягу мережевого трафіку. Аномальний трафік може надходити з різних джерел, таких як мережеві атаки, інсайдерські загрози і ненавмисні помилки конфігурації, і може мати серйозні наслідки, такі як крадіжка даних, компрометація системи і порушення бізнес-операцій. Тому проблема виявлення аномального трафіку в корпоративній мережі є критично важливою і потребує постійної уваги та вдосконалення.

Існують різні типи шкідливих процесів, які можуть бути виявлені в трафіку корпоративної мережі, в тому числі:

функціонування шкідливого програмного забезпечення;

функціонування ботнету. Ботнети можуть використовуватися для здійснення різних типів атак, включаючи DDoS-атаки, спам-кампанії та крадіжку даних;

застосування фішингу з метою обманом змусити жертву розкрити конфіденційну інформацію, наприклад, дані для входу в систему, видаючи себе за легітимну організацію;

витік даних передбачає несанкціоновану передачу даних з мережі в зовнішнє середовище. Це може бути здійснено за допомогою різних методів, таких як протоколи передачі файлів, електронна пошта та соціальні мережі;

трафік управління та контролю (C&C). Цей трафік управління утворюється між зараженим пристроєм і віддаленим сервером управління. Він є ключовим індикатором скомпрометованості системи;

робота інсайдерів, які використовують свій авторизований доступ до мережі для здійснення зловмисних дій, таких як крадіжка конфіденційних даних або порушення мережевих операцій.

Необхідно підкреслити, що більшість ІТ напрямків широко застосовують моніторинг мережевого трафіку для отримання видимості та ситуаційної обізнаності. Належний моніторинг інфраструктури та мережевого трафіку, а також виявлення аномалій і реагування на них мають вирішальне значення для підтримки безперервності та постійного вдосконалення ІТ-середовищ сучасних організацій [1].

Сучасні ІТ-середовища є високорозподіленими та динамічними, з додатками, розгорнутими в приватних центрах обробки даних, численних публічних хмарах та периферійних локаціях. Гібридна робота та Інтернет речей вимагають, щоб співробітники та пристрої були підключені з домашніх офісів або інших віддалених місць. Це нове середовище вимагає від організацій забезпечення безпечного зв'язку між усіма додатками, працівниками та пристроями Інтернету речей [2].

Проблеми в корпоративних мережах виявляються як викликані ними

аномалії трафіку. Загалом, аномалія – це те, що суперечить очікуванням. Наприклад, пошкоджений комутатор може створити неочікуваний трафік в іншій частині мережі або нові коди помилок починають з'являтися, коли служба не працює. Усунення несправностей мережі ґрунтується на аномаліях мережі [3].

Загалом, виявлення аномалії можна розділити на кілька основних компонентів, які показано на рисунку нижче. Вони мають такі функції (рис.1):

параметризація – дані, що контролюються, відокремлюються від вхідних даних у формі, придатній для подальшої обробки;

навчання – коли вибрано цей режим, модель мережі (статус навчання) оновлюється. Це оновлення можна виконати як автоматично, так і вручну;

виявлення – створена (навчена) модель потім використовується для порівняння даних з контрольованої мережі. Якщо він відповідає певним критеріям, створюється звіт про виявлення аномалії.

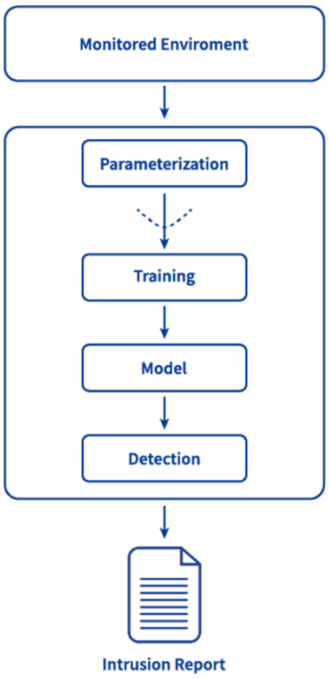


Рис. 1. Складові виявлення аномалії [3]

Виявлення аномалій застосовується для [3]:

виявлення програм-вимагачів – виявлення здійснюється за допомогою пошуку сигнатури виконуваного файлу;

виявлення DDoS-атаки – шляхом порівняння обсягу поточного трафіку з очікуваним обсягом атака може бути виявлена;

відстеження активності ботнету – за допомогою списку відомих командних і контрольних серверів ботнету можна виявити підключення до цих серверів;

виявлення атак за словником – шляхом підрахунку кількості спроб входу та порівняння числа з пороговими значеннями можна виявити спроби злому облікового запису;

виявлення збою з'єднання – це можна визначити, виявивши збільшену кількість з'єднань на резервному з'єднанні;

виявлення неправильної конфігурації додатка – це можна виявити за збільшенням кількості кодів помилок у підключеннях додатка;

виявлення перевантаження сервера – виявляючи зниження якості досвіду, можна виявити перевантаження служб або серверів;

виявлення підозрілої поведінки пристрою – створюючи профілі поведінки та перевіряючи, чи поводиться якийсь пристрій поза створеними профілями, можна виявити підозрілу активність.

У [4] зазначається, що сьогодні у виявленні зловмисної активності в інформаційній системі організації відіграє система управління інформацією та подіями безпеки (SIEM).

Додаток IBM QRadar Network Threat Analytics призначений для постійного відстеження записів потоків у корпоративній мережі, щоб виявляти аномальний трафік. Інформаційна панель додатка забезпечує візуалізацію, щоб показати, які записи потоку найбільше відрізняються від інших записів потоку, які зазвичай спостерігаються у корпоративній мережі. Візуалізації можуть допомогти фахівцям швидко визначити, які потоки можуть вказувати на підозрілу поведінку у корпоративній мережі, і визначити пріоритетність подальших розслідувань [5].

IBM QRadar збирає інформацію про те, як пристрої у корпоративній мережі спілкуються один з одним, і створює запис потоку для збору інформації про зв’язок. Потоки, які спостерігає QRadar, відображаються на вкладці Мережева активність. Більшість потоків представляють нормальний зв’язок між пристроями та не становлять загрози для корпоративного середовища, але деякі потоки можуть бути індикаторами підозрілої активності у корпоративній мережі.

QRadar Network Threat Analytics аналізує записи потоків у корпоративній системі, щоб визначити нормальні шаблони трафіку, а потім порівнює всі вхідні потоки з останнім базовим рівнем мережі, створеним додатком. Кожному потоку присвоюється викидний бал на основі значень атрибутів потоку та того, як часто цей тип зв’язку спостерігається в мережі. Чим вищий показник викиду, тим більш аномальний потік порівняно з набором базових даних.

Отже, дотримуючись цих загальних рекомендацій щодо застосування методів та засобів виявлення аномального трафіку у корпоративній мережі, організації зможуть краще виявляти та реагувати на аномальний мережевий трафік і захищати свої мережі від кіберзагроз.

Перелік посилань:

1. The Cybersecurity Outlook for 2023. Report. Progress Software Corporation. [online], https://d34smkdb128qfi.cloudfront.net/docs/flowmonlibraries/resources/cybersecurity_outlook_2023.pdf?sfvrsn=67ba901a_1 (Accessed September 28, 2023).

2. Bob Laliberte. Choosing the Right Network Observability Platform forHighly Distributed Environments. WHITE PAPER. Enterprise Strategy Group. December 2022. [online], https://d34smkdb128qfi.cloudfront.net/docs/flowmonlibraries/resources/esg-progress-software-network-observability-platform.pdf?sfvrsn=390d558a_7 (Accessed September 28, 2023).

3. Petr Pecha. Science of Network Anomalies. Posted on May 14, 2021. [online], https://www.flowmon.com/en/blog/science-of-network-anomalies (Accessed September 28, 2023).

4. Kathryn Knerler, Ingrid Parker, Carson Zimmerman. 11 Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation, 2022. – 452 p. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjwnKK97fv9AhXPvIsKHbVlB6AQFnoECAoQAQ&url=https%3A%2F%2Fwww.mitre.org%2Fsites%2Fdefault%2Ffiles%2F20

22-04%2F11-strategies-of-a-world-class-cybersecurity-operations-center.pdf&usg=AOvVaw14oA34nNabWa6aN-Yq-xsx.

5. QRadar Network Threat Analytics app. Last Updated: 2023-04-06. Available online: https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-network-threat-analytics-app.

Хуторний Владислав Ігорович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЇ ЗАХИСТУ ХОЛОДНИХ ГАМАНЕЦЬ ВІД ХАКЕРЬСЬКИХ АТАК

Холодний гаманець — це сховище ключів доступу до криптовалютних активів, яке не потребує постійного підключення до інтернету. Сховищем можуть стати флешка і навіть звичайний аркуш паперу, якщо записати на нього ключі. Паперовий гаманець — це «дешево та сердито». Він повністю безкоштовний — сформуйте ключі за допомогою сайту-інтегратора, наприклад, BitAddress, роздрукуйте їх та сховайте аркуш у надійне місце. Щодо флешки, то на ній просто потрібно зберегти відповідні файли. Однак такі гаманці майже ніяк не захищені, а паперовий ще й дуже чутливий до води та сонячних променів. Сучасні криптотрейдери віддають перевагу спеціальним гаджетам — апаратним криптогаманцям. Це пристрої, що зовні схожі на флешку, автомобільний дармовис, невеликий пульт управління або телефон. Вони забезпечують найвищий рівень безпеки коштом захисного чіпа, а також додаткових механізмів та процедур. Основна функція апаратних гаманців — зберігання ключів доступу.

Основні загрози криптогаманців.

1. Шкідливі програми, які замінюють вміст буфера обміну

Цей тип шкідливого програмного забезпечення кіберзлочинці використовують, щоб приховано замінити вміст буфера обміну, скориставшись поширеною дією копіювання та вставки. Вперше таку загрозу було виявлено у магазині Google Play у вигляді додатку MetaMask. Шкідлива програма замінювала адреси гаманців Bitcoin та Ethereum, скопійовані в буфер обміну, на адреси, що належать зловмисникам.

2. Підроблені сторінки для входу.

Кіберзлочинці часто поширюють фальшиві версії популярних криптогаманців для мобільних пристроїв або для відомих бірж криптовалют. Ідея подібних шкідливих кампаній полягає в тому, щоб заповнити нішу, яку залишили відомі торгові марки, та охопити більше потенційних жертв. Після завантаження одного з підроблених гаманців криптовалют користувачі переходять на сторінку для входу в систему. Часто такі сторінки є фішинговими та використовуються для викрадення закритих ключів користувача, які потрібні для отримання контролю над гаманцем.

3. Шкідливі посилання.

Поширеними серед кіберзлочинців стали гомографічні атаки, які передбачають створення доменів, схожих на відомі сайти. Насправді ж більшість таких посилань є фішинговими. За даними телеметрії ESET, за другий квартал 2020 року найбільш популярними доменами серед зловмисників стали blockchain.com та binance.com.

Іншим способом здійснення фішингу є надсилання спам-повідомлень зі шкідливими посиланнями, натискання на які часто призводить до завантаження банківських троянів, таких як Mekotio. Деякі варіанти цієї шкідливої програми можуть викрадати Bitcoin, замінюючи адресу вашого гаманця в буфері обміну. В інших випадках зловмисники використовують програми для зчитування натиснень клавіатури. Використання торрент-сайтів для завантаження програмного забезпечення та ігор також може бути небезпечним. Саме на таких сайтах зловмисники часто поширюють шкідливе програмне забезпечення, як у випадку з загрозою KryptoCibule. Ця шкідлива програма дозволяла кіберзлочинцям перехоплювати транзакції користувача, замінюючи адреси гаманців в буфері обміну, а також викрадати будь-які файли, пов'язані з криптовалютою, на пристрої жертви.

4. Шахрайство.

Деякі користувачі для зменшення ризиків викрадення чи інфікування криптогаманців використовують гаманець без доступу в Інтернет, наприклад Ledger. У таких випадках користувачі часто незадоволені зручністю використання додатків. З метою покращити використання криптогаманців кіберзлочинці пропонують завантажити розширення Google Chrome чи Firefox, які інтегрують гаманець Ledger з браузером. Дізнавшись фразу відновлення, зловмисники можуть швидко клонувати апаратний гаманець та отримати доступ до коштів його власника.

Перелік посилань:
1. https://www.liga.net/crypto/ua/wallets/hardware-wallets
2. https://www.eset.com/ua/about/newsroom/blog/data-protection/bezopasnost-virtualnykh-deneg-populyarnyye-ugrozy-i-sposoby-zashchity-kriptokoshelkov/

Цигикал Богдан Олександрович
Студент групи БСДМ-61, ННІЗІ, ДУІКТ, Київ, Україна

ВИЗНАЧЕННЯ ГОЛОВНИХ КРОКІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ДОСТУПУ ДО МЕРЕЖІ

Технологія контролю доступу до мережі - це сучасний підхід до забезпечення безпеки та управління доступом в корпоративних мережах. Розглянуто основні кроки для забезпечення кібербезпеки для визначення технології, яка може бути використана для створення інтегрованих систем контролю доступу до корпоративних мереж.

Актуальність контролю доступу до корпоративних мереж зумовлено наступними чинниками:

– Зростання кількості кіберзагроз;
– Зростання обсягів даних;
– Вимоги до дотримання стандартів і регуляцій;

В сучасному світі кіберзагрози постійно зростають, і контроль доступу до мережі стає все важливішим аспектом забезпечення безпеки даних та

інфраструктури.

Обсяги корпоративних даних постійно збільшуються, і важливо мати контроль над тим, хто має доступ до цих даних та як вони використовуються.

Епоха цифрових технологій справила революцію у способах роботи підприємств, а Інтернет та технології відіграють центральну роль практично у всіх аспектах сучасного бізнесу. Однак з цим досягненням зростає ризик кібератак і витоків даних, що наражає на ризик компанії та їх клієнтів. Оскільки кіберзагрози продовжують розвиватися і ставати все більш витонченими, дуже важливо, щоб підприємства вживали надійних заходів кібербезпеки для захисту від атак.

1. Кількість зловмисних атак зростає

Зловмисники завжди становили серйозну загрозу для бізнесу. Але зі швидким розвитком технологій в останні роки кібератаки стають більш частими та витонченими, ніж будь-коли раніше. За останніми даними, кожні 39 секунд відбувається атака. Це один із показників кібербезпеки, який напевно не дасть спати ночами будь-якому підприємцю.

2. Державний сектор, технології та роздрібна торгівля страждають найбільше

Хоча кожна галузь схильна до ризику кібератаки, деякі з них більш вразливі, ніж інші. Зокрема, останніми роками ціллю кібератак стали державні установи, технологічні компанії та підприємства роздрібної торгівлі. За оцінками, у 2016 році 95% усіх зламаних записів припадало на ці три сектори. Багато в чому це пов’язано з великим обсягом даних, що зберігаються в цих організаціях, а також конфіденційним характером такої інформації.

3. Витоки даних обходяться дуже дорого

Усі типи витоку даних обходяться підприємствам дуже дорого в контексті часу, ресурсів та втрати прибутку. Фактично, до 2025 року кібератаки коштуватимуть компаніям 10,5 трлн доларів на рік. Ці гроші можна використовувати для стимулювання інновацій, розширення операцій та побудови безпечнішого майбутнього як для бізнесу, так і для клієнтів.

4. Малий бізнес особливо вразливий

Враховуючи, що у малого бізнесу менше ресурсів для забезпечення кібербезпеки, не дивно, що вони більш вразливі для кібератак. Фактично 43% усіх кібератак спрямовані на малий бізнес. Для всіх, хто займається малим бізнесом, дуже важливо серйозно ставитися до захисту даних та інвестувати в надійні заходи кібербезпеки, які можуть забезпечити безпеку організації.

5. Сектор охорони здоров’я стає головною ціллю

Останніми роками сектор охорони здоров’я перетворився на основну мету для зловмисників. У період пандемії особливо різко побільшало атак саме на цей сектор. У міру того, як все більше пацієнтів зверталися за медичною допомогою, зловмисники побачили можливість вкрасти конфіденційну інформацію.

Загалом починаючи з 2020 року зловмисники щороку викрадають 29 мільйонів записів. Це тривожний сигнал для організацій у сфері охорони здоров’я: вони повинні вжити заходів, які допомагають зупинити атаки перед

тим, як вони відбудуться.

6. Covid-19 призвів до збільшення кількості атак

Пандемія справила руйнівний вплив, економічні та соціальні наслідки відчувалися у всьому світі. Оскільки підприємства сподівалися витримати бурю, було реалізовано політики віддаленої роботи. Однак це зрушення надало кіберзлочинцям чудову можливість отримати вигоду з підприємств, які прагнуть підтримувати операційну діяльність за мінімальних витрат. Насправді відразу після початку поширення Covid-19 кількість атак збільшилась на 300%.

7. Фішингові атаки становлять серйозну загрозу

Кіберзлочинці мають нескінченний арсенал методів проникнення в системи компанії. Однак однією з улюблених тактик є фішинг. Це включає відправлення електронного листа, який виглядає як законне джерело, але призначене для того, щоб обманом змусити людей розкрити конфіденційну інформацію, таку як паролі або дані банківського рахунку.

Фактично до 90% витоків даних відбуваються в результаті фішингових атак. Якщо організація хоче залишатися захищеною, дуже важливо виявляти пильність щодо спроб фішингу та вживати заходів, щоб звести до мінімуму ризики.

8. Людський фактор є причиною більшості порушень безпеки

У більшості організацій за безпеку переважно відповідають співробітники. Однак це також може призвести до порушень, коли вони роблять помилки — випадково чи зі злим наміром. Фактично, 95% всіх витоків даних відбуваються внаслідок людської помилки. Ці помилки варіюються від переходу через небезпечні посилання до шахрайства з електронною поштою.

9. Навчання з питань кібербезпеки є важливими

Якщо людський фактор є основною причиною витоків даних, то з цього випливає, що навчання з питань безпеки є одним з найефективніших інструментів боротьби з кібератаками. Згідно з недавнім дослідженням, 97% респондентів заявили, що за останній рік вони проводили навчання з кібербезпеки. Коли співробітники знають, як виявляти та уникати фішингу, шкідливого програмного забезпечення та інших атак, вони можуть допомогти забезпечити безпеку організації.

10. Витрати на IT-безпеку зростають

Зловмисники постійно відточують свої навички та вигадують нові способи проникнення в системи. Це виклик для бізнесу, оскільки необхідність інвестувати в передовий кіберзахист є очевидною як ніколи. Насправді витрати на IT-безпеку досягли рекордно високого рівня. За оцінками аналітиків, до кінця 2022 року загальні витрати на кібербезпеку перевищать 172 мільярди доларів.

11. Використання пристроїв IoT значно зросло

Однією з найсерйозніших загроз кібербезпеці, з якими сьогодні стикається бізнес, є використання пристроїв IoT, кількість яких постійно зростає. Якщо вони не захищені належним чином, зловмисники можуть легко використовувати їх для отримання доступу до мережі компанії. Проте очікується, що до 2025 року використовуватиметься понад 75 мільярдів пристроїв IoT, тому організаціям

дуже важливо вжити заходів для забезпечення максимальної безпеки цих пристроїв.

12. Нестача кадрів у сфері IT-безпеки зростає

Персонал IT-безпеки є величезним ресурсом у боротьбі з кібератаками. І зі зростанням потреби у цих фахівцях збільшується розрив між попитом та пропозицією. За оцінками, 2021 року в усьому світі було незаповнено близько 3,5 мільйонів вакансій. Найближчими роками цей розрив лише збільшуватиметься.

13. Більшість організацій не мають плану реагування на інциденти IT-безпеки

Попри високий рівень кібератак, багато підприємств досі не мають ефективного плану реагування на інциденти у сфері IT-безпеки. За оцінками, 77% організацій у всьому світі не мають такого плану. Якщо бізнес постраждав від витоку даних і не має надійної стратегії щодо усунення наслідків, наслідки можуть бути катастрофічними.

14. Більшість малих підприємств опиняються на грані закриття після злому

Небагато витоків даних залишають бізнес неушкодженим. Особливо сильно тут страждає саме малий бізнес. Близько 60% цих фірм зачиняють свої двері протягом шести місяців після кібератаки. Більшість цієї шкоди є результатом фінансових збитків. Але слід враховувати та вплив на репутацію. Як тільки про злом стає відомо всім, відновити довіру клієнтів та інших зацікавлених сторін може бути надзвичайно складно. Судові позови та штрафи також можуть призвести до того, що малий бізнес боротиметься за існування.

15. Більшість компаній потребують занадто багато часу, щоб виявити порушення

Коли організація потребує багато часу, щоб ідентифікувати атаку, наслідки можуть бути дуже поганими. На жаль, саме це відбувається сьогодні. Більшості потрібно понад 6 місяців, щоб зрозуміти, що їх зламали.

За цей час зловмисники можуть завдати великих збитків. Вони можуть вкрасти конфіденційну інформацію та завдати шкоди мережі. Ось чому системи аудиту та моніторингу такі важливі. У разі наявності будь-яких вразливостей чи злому, компанії хочуть дізнатися про це якнайшвидше, щоб зробити необхідні кроки для мінімізації збитків та захисту бізнесу.

Багато галузей, таких як фінанси та охорона здоров'я, піддаються обов'язковим стандартам щодо безпеки даних. Технологія контролю доступу допомагає відповідати цим вимогам.

Перелік посилань:

1. 15 тривожних фактів та статистики про кібербезпеку URL: https://corewin.ua/blog/cybersecurity-facts-and-statistics/ (дата звернення: 22.10.2023).
2. Важливі перші кроки до підвищення кібербезпеки URL: https://www.kingston.com/ua/blog/data-security/cybersecurity-threats-endpoint-security-challenges-2022 (дата звернення: 23.10.2023).

Чаплієва Анастасія Олександрівна
студентка групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ЯК ПОТРАПИТИ В ПАСТКУ БЕЗ КЛІКУ: РОЗУМІННЯ ЕКСПЛОЙТІВ З НУЛЬОВИМ НАТИСКАННЯМ ТА ЇХНЬОГО ВПЛИВУ

Експлойти з нульовим натисканням часто використовуються для розгортання шпигунського програмного забезпечення, що дозволяє здійснювати таємне спостереження та збирати дані про осіб, яких уряди чи інші організації вважають важливими. Саму ідею згадував Едвард Сноуден ще в 2010-х роках, оскільки він наголосив, що смартфони можна зламати за допомогою лише одного текстового повідомлення, а потім використовувати для шпигування за їхніми власниками. Ця ситуація схожа на нещодавню вразливість, оприлюднену у вересні 2022 року WhatsApp (CVE-2022-36934) [1, с.3]. Зловмиснику потрібно було лише надіслати спеціально створений відеодзвінок, щоб використати вразливість, згодом отримавши можливість виконати код, зв'язавши його з іншою вразливістю.

Експлойт з нульовим натисканням (zero-click exploit) — це складний тип кібератаки, який діє без необхідності прямої взаємодії з цільовим користувачем. На відміну від традиційних експлойтів, коли користувача можна обманом змусити натиснути зловмисне посилання або завантажити підозрілий файл, експлойти з нульовим натисканням призначені для автономного виконання шкідливого коду. Незалежно від того, чи йдеться про серію мережевих пакетів, запитів на автентифікацію, текстових повідомлень, MMS, голосової пошти, сеансів відеоконференцій, телефонних дзвінків або повідомлень через такі платформи, як Skype, Telegram або WhatsApp, основна мета залишається незмінною: використати вразливість у коді програми, яка відповідає за обробку даних.

Наприклад, коли смартфон отримує SMS або електронний лист, він часто відображає сповіщення на основі вмісту повідомлення, навіть до того, як користувач відкриє його. Якщо в коді обробки даних цих програм існує вразливість, добре створене зловмисне повідомлення може використати її, що призведе до неавторизованого виконання коду. Потім зловмисний код може встановлювати зловмисне програмне забезпечення, стерти його сліди та навіть блокувати появу сповіщення, залишаючи користувача без відома про порушення. В контексті зростаючої поширеності штучного інтелекту в робочих процесах, зростає також і ризик стати жертвами експлойтів без натискання.

Сучасним прикладом можливостей шпигунського програмного забезпечення можна привести **«Pegasus»**. Компанією розробником є ізраїльська фірма NSO Group, що була причетна до розповсюдження експлойтів, націлених на широко використовувані програми обміну повідомленнями, включаючи WhatsApp. Коротку ілюстрацію можливостей шпигунського ПЗ Pegasus можна побачити на рисунку 1 нижче.

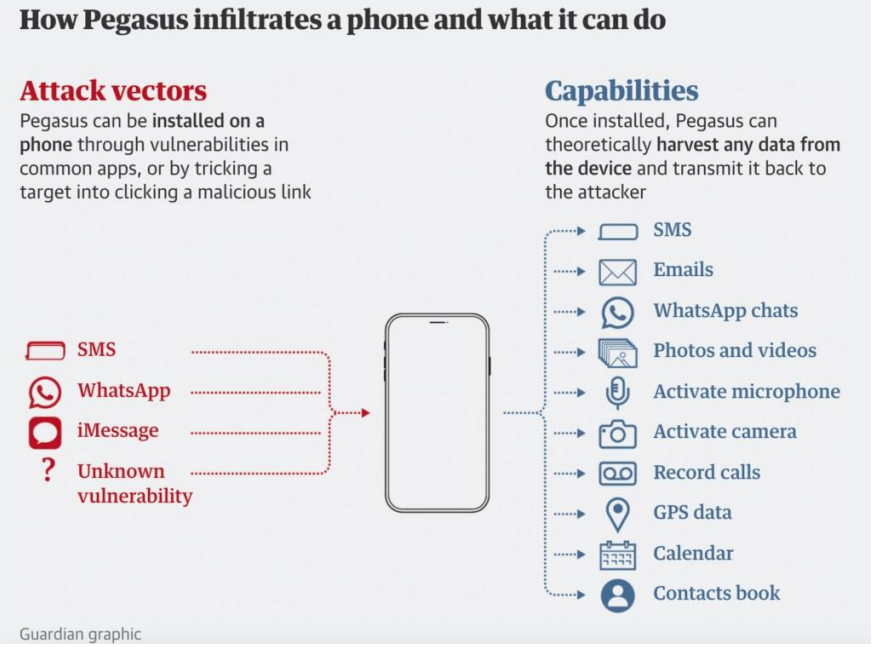


Рис.1. Можливості шпигунського ПЗ Pegasus

Як можна пом’якшити ризики отримання експлойту без натискання:

- **Періодично перезавантажуйте iPhone** . Для користувачів iPhone простим, але ефективним заходом є періодичне перезавантаження пристрою. Перезапуск має перевагу зупинки будь-якого непостійного коду. Однак потенційним недоліком є те, що ця дія може стерти сліди зараження, через що при розслідуванні буде складно визначити, чи був пристрій мішенню атаки без натискання.
- **Уникати пристроїв для джейлбрейку.** Джейлбрейк (Jailbreak) – операція, за допомогою якої здійснюють відкриття повного доступу до файлової системи iOS-пристроїв. Джейлбрейк видаляє певні вбудовані засоби безпеки з мікропрограми пристрою. Більше того, на зламаних пристроях може встановлюватися неперевірене програмне забезпечення, що робить їх сприйнятливими до вразливого коду, який може бути використаний під час атак без натискання.
- **Окремі дані для високопоставлених цілей:** особам із підвищеним ризиком слід розглянути можливість використання спеціального окремого пристрою виключно для конфіденційних комунікацій. На своїх телефонах бажано зберігати мінімум інформації та використовувати функцію зникнення повідомлень з часом. Крім того, для максимальної конфіденційності рекомендується тримати телефони подалі від кімнати під час важливих бесід віч-на-віч.
- **Зверніть увагу на попередження технічних компаній:** і Apple, і WhatsApp неодноразово попереджали користувачів, які могли бути жертвами атак без натискання. Якщо ви отримали таке повідомлення, необхідно негайно вжити заходів.

У сучасному цифровому середовищі, що швидко розвивається, експлойти з нульовим натисканням стали одним із найприхованіших і найпотужніших інструментів кібершпигунства. Ці складні атаки, які **не вимагають взаємодії з користувачем** , спрямовані на вразливі місця в широко використовуваних програмах, особливо на смартфонах. Гучні інциденти, такі як експлойт WhatsApp у 2019 році, підкреслюють реальні наслідки та прихований характер цих зломів.

Хоча такі компанії, як NSO Group, відіграли важливу роль у розробці та розповсюдженні цих експлойтів, їхні дії викликали значні етичні проблеми та проблеми безпеки. Зменшити ризики, пов’язані з експлойтами з нульовим натисканням, складно, але застосування найкращих практик, інформування та пильність можуть підвищити рівень захисту від цих прихованих кіберзагроз.

Перелік посилань:
1. Опис критичної вразливості WhatsApp CVE-2022-36934 URL: https://socradar.io/critical-whatsapp-vulnerabilities-allow-attackers-remote-device-hacking/ (дата звернення: 20.10.2023).
2. Більш детальний огляд атак без натискання: https://socradar.io/beyond-the-click-understanding-zero-click-exploits-and-their-impact/ (дата звернення: 23.10.2023).
3. Що таке Zero Click Attack по версії Check Point https://www.checkpoint.com/cyber-hub/cyber-security/what-is-a-zero-click-attack/ (дата звернення: 23.10.2023).
4. Атаки з нульовим натисканням та чому вони такі небезпечні по версії CSO онлайн https://www.csoonline.com/article/572727/zero-click-attacks-explained-and-why-they-are-so-dangerous.html (дата звернення: 23.10.2023).

Часовський Сергій Анатолійович
студент групи БСДМ-52, ДУІКТ, Київ, Україна

TOP CLOUD CYBERSECURITY CHALLENGES

The advent of cloud computing has transformed the way organizations and individuals store, access, and manage data. The cloud offers numerous benefits, such as scalability, cost-efficiency and flexibility. However, it also introduces a unique set of cybersecurity challenges that need to be addressed to ensure data confidentiality, integrity, and availability.

This thesis delves into the top 5 cloud cybersecurity challenges that organizations face in 2023, emphasizing the importance of robust security measures to protect cloud-based assets.

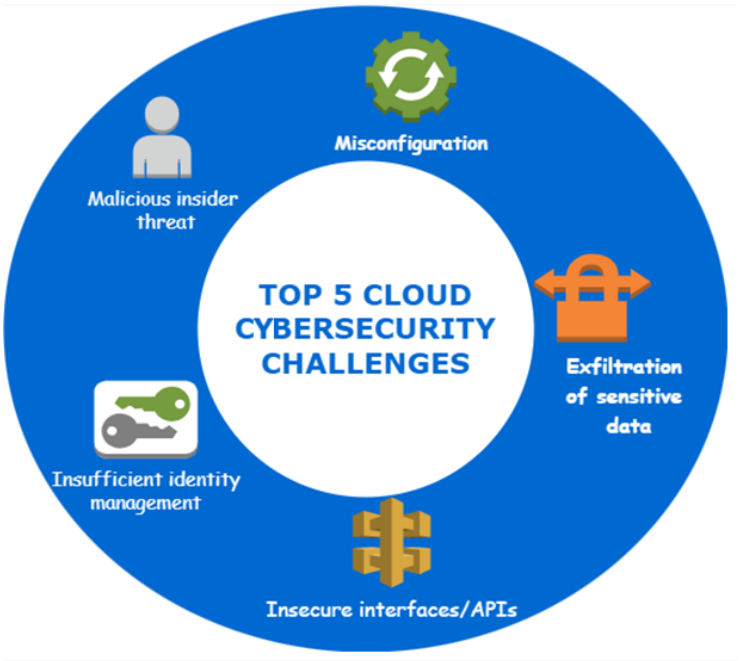


Рис 1. Top 5 cloud cybersecurity challenges

1. Misconfiguration

Misconfigurations pose a significant security threat in the realm of public cloud computing, as reported by 59% of cloud users. Furthermore, among those cloud users who encountered security incidents over the past year, a noteworthy 19% of such incidents were attributable to misconfigured resources or accounts. Here are some key aspects of cloud misconfiguration security challenges:

- **Data Exposure**: misconfigurations can lead to the unintentional exposure of sensitive data. For instance, leaving a cloud storage bucket open to the public or failing to properly secure database access can result in unauthorized access to confidential information, such as customer records, intellectual property, or financial data
- **Identity and Access Management (IAM)**: misconfigurations in IAM settings can lead to unauthorized access to cloud resources. Poorly managed user privileges and roles may result in excessive access rights, making it easier for malicious actors to compromise cloud resources
- **Inadequate Encryption**: failing to enable encryption for data in transit and at rest is a significant misconfiguration. Without encryption, data is vulnerable to interception or theft, especially in multi-tenant cloud environments
- **Network Security**: misconfigurations in network security settings can result in improperly configured firewall rules, open ports, or inadequate segmentation. This can lead to unintended exposure of services and make it easier for attackers to pivot within the network

- **Lack of Logging and Monitoring**: without proper logging and monitoring organizations may not be aware of suspicious activities or unauthorized access until it's too late
- **Compliance and Regulatory Issues**: misconfigurations can lead to non-compliance with industry-specific regulations and standards, which can result in legal and financial consequences for the organization
- **Human Error**: human error is a common factor in misconfigurations. Cloud environments often involve multiple teams working together, and a single mistake in configuration can lead to significant security vulnerabilities.

Mitigating cloud misconfiguration security challenges requires proactive measures like:

- Follow best practices and guidelines provided by cloud service providers.
- Regularly audit and assess configurations for potential vulnerabilities.
- Implement automation tools and practices to detect and rectify misconfigurations.
- Provide security training and awareness programs for personnel.
- Establish clear roles and responsibilities within the organization to ensure accountability for security.

2. Exfiltration of Sensitive Data

As businesses continue their migration to cloud environments, the amount of sensitive data has grown substantially. A significant 51% of organizations identify data exfiltration as a substantial security concern in public clouds, and about 13% of cloud-related incidents involved the improper sharing of files or data by a user over the past year.

Cloud environments often contain vast volumes of sensitive information, including customer data, intellectual property, financial records, and more. Data exfiltration poses a significant risk to the confidentiality, integrity, and availability of this information.

What are motives for exfiltration?

Data exfiltration can occur for various reasons, such as cybercriminal activities, insider threats, industrial espionage, or even accidental exposure. Malicious actors may aim to steal valuable information for financial gain, reputational damage, or competitive advantage.

What are the methods of exfiltration?

Exfiltration methods are diverse and can include unauthorized access to cloud resources, exploiting misconfigurations, or utilizing malware and phishing attacks. Malicious actors may also use legitimate user accounts with elevated privileges to access and exfiltrate data.

What are the detection challenges?

Identifying data exfiltration is often a complex task. Attackers may employ stealthy techniques to bypass traditional security controls. Organizations must implement advanced threat detection and monitoring systems to recognize suspicious behavior patterns indicative of exfiltration.

What is the impact on reputation?

A data breach can corrupt an organization's reputation and lead to a loss of customer trust. Data exfiltration incidents can have far-reaching consequences, including customer attrition and reduced market confidence.

What are the preventative measures?

To address the challenge of data exfiltration, organizations should employ a multi-layered approach to security. This includes:

- robust access controls,
- encryption of data at rest and in transit,
- continuous monitoring,
- intrusion detection,
- user training to recognize and respond to potential threats.

3. Insecure Interfaces/APIs

APIs have become increasingly prevalent in the cloud environment, particularly with the rising popularity of microservices and containerized applications. Nonetheless, they also bring significant security concerns, as highlighted by the 51% of respondents identifying insecure interfaces/APIs as a primary security challenge in public cloud environments.

APIs are fundamental to modern cloud ecosystems. They serve as the bridges that allow different services, applications and components to communicate and interact seamlessly. As a result, APIs are pervasive throughout cloud environments. Here, we will delve into the specifics of this challenge:

The security risks

Insecure interfaces and APIs create substantial security risks. These vulnerabilities can lead to unauthorized access, data breaches, and exploitation by malicious actors. Such security lapses can result in the compromise of sensitive data, service disruption, and reputational damage.

Insecure APIs can suffer from a variety of vulnerabilities, including weak authentication, inadequate authorization controls, data exposure, and insufficient data validation. These vulnerabilities are often exploited by attackers to gain unauthorized access or manipulate the system.

Misconfigured APIs

Misconfigurations in APIs, such as failing to restrict access or improperly configuring permissions, can lead to unauthorized users gaining access to sensitive resources. Misconfigurations are often the result of human error or lack of understanding of API security best practices.

Shadow APIs

Shadow APIs, also known as undocumented or unsanctioned APIs, are a particular concern. These are APIs that exist within an organization's environment but are not officially documented or monitored. They can be created by individuals or teams to fulfill specific requirements without proper oversight or security considerations.

Third-Party APIs

Many cloud environments rely on third-party APIs, which can introduce additional security challenges. Organizations must trust that these APIs are secure, and any vulnerabilities in third-party APIs can potentially impact the security of the entire system.

Overexposure of Data

Some APIs may provide excessive or unnecessary data in response to user requests, creating a risk of data leakage. Overexposing data can occur when APIs do not follow the principle of least privilege and provide more information than is required for a particular task.

Mitigation Strategies

Organizations can mitigate the risks associated with insecure interfaces and APIs by implementing robust security practices, including:

- proper authentication and authorization mechanisms,
- regular security testing,
- encryption,
- user awareness and training,
- continuous monitoring for unusual or suspicious activities.

4. Insufficient Identity Management

The "Insufficient Identity Management" security challenge in a cloud environment relates to deficiencies in how users and entities are identified, authenticated, and managed within the cloud infrastructure.

Identity management is a fundamental aspect of cloud security, ensuring that access to resources and data is granted to the right individuals or systems while denying access to unauthorized parties. Here, we'll explore the specific aspects of this challenge:

Weak authentication

Weak or easily guessable passwords, lack of multi-factor authentication (MFA), and outdated authentication methods can lead to compromised user accounts. Cloud environments must employ robust authentication mechanisms to verify the identity of users and entities securely.

Inadequate authorization

Inadequate authorization controls can lead to excessive permissions, allowing users to access resources and data they shouldn't. Insufficient authorization can also result in unauthorized data manipulation or service disruptions.

User provisioning and deprovisioning

Managing user accounts efficiently during onboarding and offboarding processes is vital. Insufficient identity management can lead to errors in user provisioning or deprovisioning, which can leave former employees with access to sensitive data or result in the denial of access to new employees, hampering productivity.

Role-based access control

Role-based access control (RBAC) is a fundamental part of identity management. Organizations that lack well-defined roles and responsibilities may grant excessive access rights to users, making it easier for malicious actors to compromise cloud resources.

Shadow IT and shadow users

Shadow IT and shadow users are unauthorized or unmanaged instances and accounts within a cloud environment. These are often introduced by employees or departments without IT oversight, making them potential security vulnerabilities.

Identity federation

Identity federation allows users to access multiple cloud services using a single set of credentials. Insufficient federation controls can lead to security issues when users' credentials are compromised.

Third-party integration

The integration of third-party services and APIs into cloud environments can introduce challenges in identity management. Ensuring that these external entities align with the organization's identity management and security standards is crucial.

To address the insufficient identity management security challenge in a cloud environment, organizations should:

- implement robust IAM practices that include strong authentication, authorization controls, and RBAC
- regularly audit and review user access rights to ensure compliance and security.
- develop comprehensive policies and procedures for user provisioning and deprovisioning
- educate users and employees about security best practices and the importance of strong identity management
- leverage advanced security tools and technologies to monitor user activities, detect anomalies, and respond to potential threats.

5. Malicious Insider Threat

The "Malicious Insider Threat" is a significant security challenge in cloud environments. This threat refers to individuals or entities within an organization who have legitimate access to the cloud infrastructure and data but use their access for nefarious purposes, intentionally causing harm to the organization's security, data, or

operations. Here, we'll explore the specific aspects of this security challenge:

Legitimate access

Malicious insiders typically have legitimate access to cloud resources and data as part of their job roles. This makes it challenging to distinguish their actions from ordinary activities.

Motives

Insiders may have various motives for engaging in malicious activities within the cloud environment. These motives can range from financial gain and revenge to sabotage, espionage, or competitive advantage. Understanding the underlying motivations is critical for detecting and preventing insider threats.

Data theft and exfiltration

Malicious insiders can exploit their access to steal sensitive data, intellectual property, customer information, or other valuable assets. They may then attempt to exfiltrate this data for personal gain or to harm the organization.

Data manipulation

Insiders may alter, delete, or manipulate data, leading to data integrity and availability issues. These actions can disrupt operations, damage reputation, or lead to financial losses.

Bypassing security measures

Since insiders often have knowledge of an organization's security controls, they can work to bypass or subvert these measures, making their activities harder to detect.

Evasion techniques

Insiders may employ evasion techniques, such as masking their activities as legitimate actions or attempting to cover their tracks. This can complicate the detection of their actions.

Mitigation strategies

To address the malicious insider threat, organizations should implement a range of security measures, including

- strict access controls,
- auditing and monitoring of user activities,
- the principle of least privilege,
- regular security training,
- reporting mechanisms for suspicious activities,
- some organizations employ psychological profiling techniques to identify potential insider threats based on behavior, attitude, or other indicators,
- encouraging employees to report suspicious behavior through whistleblower programs can also help in early detection

Conclusion

The adoption of cloud computing has revolutionized the way we handle data and conduct business. However, this transformation has also brought forth a new set of cybersecurity challenges that require constant vigilance and adaptation. Addressing these challenges is imperative to ensure the safety and integrity of data in the cloud.

By implementing robust security measures, adhering to best practices, and fostering a security-conscious culture, organizations can safeguard their cloud assets and maintain trust in an increasingly digital world. Cloud cybersecurity is an ongoing journey that requires collaboration between organizations and cloud providers to build a secure digital frontier for the future.

Перелік посилань:

1. https://www.linkedin.com/pulse/top-cloud-security-challenges-how-cloudlytics-addresses-them
2. Cloud Computing Security: Foundations and Challenges by John R. Vacca
3. Fortinet. Cloud Security Report 2022 (https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-cloud-security.pdf)

Чернега Станіслав Олександрович
студент групи БСДМ-63, ДУІКТ, Київ, Україна

РИЗИКИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ WEB-РЕСУРСІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ

Забезпечення безпеки веб-ресурсів в інформаційній системі організації пов'язано з численними ризиками та загрозами.

Здійснення цілеспрямованих заходів для захисту веб-ресурсів від цих ризиків є важливим завданням для організації та включає в себе використання технологій безпеки, навчання персоналу та встановлення ефективної політики безпеки.

Підходи до технології забезпечення безпеки та захисту Web-ресурсів

Захист веб-ресурсів в інформаційній системі організації стає все більш важливим завданням у світі, де цифрова технологія грає ключову роль у бізнесі та комунікаціях. Зловмисники, кіберзлочинці та інші загрози існують на кожному кроці, готові використовувати вразливості веб-систем для власних користей. У цьому контексті теза стверджує, що ефективна технологія забезпечення безпеки та захисту веб-ресурсів в інформаційній системі організації є ключовим чинником для збереження конфіденційності, цілісності та доступності даних та ресурсів. В даній статті буде розглянуто інтегрований підхід до цієї технології, включаючи технологічні, організаційні та освітні аспекти.

Однією з ключових складових технології забезпечення безпеки є використання сучасних інструментів та рішень. Це включає в себе встановлення брандмауерів, систем інтрузійного виявлення, антивірусного програмного забезпечення та систем контролю доступу. Використання технологій шифрування також відіграє важливу роль у захисті конфіденційної інформації в передачі та зберіганні. Багатофакторна аутентифікація, яка базується на чомусь, що користувач знає, має та є, стає стандартом для забезпечення безпеки доступу до веб-ресурсів.

Однак технологічні заходи самі по собі не є достатніми. Важливо постійно

оновлювати і патчувати програмне забезпечення та обладнання для виправлення вразливостей безпеки. Також потрібно використовувати системи моніторингу та журналювання для виявлення аномальної активності та аналізу подій[1].

Організаційний аспект технології забезпечення безпеки включає в себе розробку і впровадження політики безпеки, створення планів відновлення після інциденту та планів безпеки. Політика безпеки визначає правила та процедури, які повинні дотримуватися всіма співробітниками, а також визначає відповідальність за безпеку даних та ресурсів. План відновлення після інциденту (DRP) та план безпеки (BCP) визначають процедури для відновлення роботи системи після інциденту та забезпечення неперервності бізнес-процесів.

Освіта співробітників і користувачів є важливою складовою технології забезпечення безпеки. Персонал організації повинен бути навчений правилам безпеки та розпізнавати загрози. Це включає в себе інформування про соціальний інженерінг, фішинг та інші види атак. Освічені користувачі можуть бути першою лінією захисту проти загроз.

Ефективна технологія забезпечення безпеки та захисту веб-ресурсів в інформаційній системі організації є критично важливою для збереження конфіденційності, цілісності та доступності даних та ресурсів. Цей процес вимагає інтегрованого підходу, що включає в себе технологічні, організаційні та освітні заходи. Забезпечення безпеки веб-ресурсів має бути постійним процесом, оскільки загрози постійно еволюціонують. Розуміння та впровадження цих аспектів технології забезпечення безпеки є важливим завданням для будь-якої організації, яка прагне захистити свої ресурси та довіру своїх клієнтів.

Ефективний захист веб-ресурсів потребує інтегрованого підходу, який включає в себе технологічні, організаційні та освітні заходи.

Технологічні заходи: Використання брандмауерів, систем виявлення і запобігання вторгнень, систем шифрування та інших технічних рішень для забезпечення безпеки мережі та даних. Регулярне оновлення та патчі для усунення вразливостей в програмному забезпеченні. Використання багатофакторної аутентифікації та аудиту безпеки.

Організаційні заходи: Розробка та впровадження політик безпеки, контроль доступу, управління ризиками, резервне копіювання даних та плани відновлення після інцидентів. Створення команди безпеки, відповідальної за моніторинг та реагування на інциденти.

Освітні заходи: Навчання персоналу щодо кібербезпеки та прийомів запобігання соціальному інженерінгу. Забезпечення свідомості про загрози та відповідальності кожного співробітника щодо безпеки в інформаційній системі.

Перелік посилань:

1. Web Application Security Statistics [Електронний ресурс] – Режим доступу до ресурсу: http://projects.webappsec.org/f/wasc-wafec-v1.0.pdf

2. Web Server and its Types of Attacks [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: https://www.greycampus.com/opencampus/ethical- hacking/webserver-and-its-types-of-attacks

Чмига Роман Михайлович, БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО КРИТИЧНОЇ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ НА ПРИКЛАДІ FORTINET IAM

Визначено мету і основні завдання щодо управління ідентифікацією та доступом користувачів до критичної корпоративної інформації. Розглянуто зміст технології забезпечення управління ідентифікацією та доступом користувачів на базі Fortinet IAM.

Ефективне керування ідентифікацією та доступом (IAM) має вирішальне значення, оскільки скомпрометовані облікові дані є однією з найпоширеніших причин порушень безпеки. Рішення Fortinet IAM допомагає фахівцям безпечно керувати політикою автентифікації та авторизації для доступу до всіх ресурсів компанії. Fortinet IAM дозволяє використовувати найменші привілеї для зменшення ризиків, пов’язаних із загрозами безпеці на основі облікових записів. Впроваджуючи принципи нульової довіри, такі як автентифікація без пароля, є можливість перевірки та авторизації запитів на доступ на основі контекстної інформації про користувача [1].

Управління ідентифікацією та доступом - це структура політик, процесів і технологій, які дозволяють організаціям керувати цифровими ідентифікаторами та контролювати доступ користувачів до критичної корпоративної інформації. Призначаючи користувачам певні ролі та забезпечуючи їм належний рівень доступу до корпоративних ресурсів і мереж, IAM покращує безпеку та взаємодію з користувачами, забезпечує кращі бізнес-результати та підвищує життєздатність мобільної та віддаленої роботи та адаптації хмари. Основна мета платформи IAM - призначити одну цифрову ідентифікацію кожній людині чи пристрою. Звідти рішення підтримує, змінює та контролює рівні доступу та привілеї протягом життєвого циклу доступу кожного користувача.

Завдяки рішенням Fortinet IAM ускладняється доступ хакерів до захищеної інформації за допомогою додаткових облікових даних, таких як одноразовий пароль (one-time passcode, OTP). OTP є одним із компонентів багатофакторної автентифікації (multi-factor authentication, MFA). MFA є ключовою функцією безпеки рішення Fortinet IAM, оскільки вона вимагає перевірки кількох облікових даних. Навіть якщо кіберзлочинець має ім’я користувача та пароль, він не може отримати доступ до системи без іншої інформації [1].

Fortinet пропонує просте розгортання єдиного входу (single sign-on, SSO) із централізованим керуванням ідентифікацією (рис. 1). Він автентифікує користувачів як за допомогою традиційних, так і сучасних протоколів автентифікації в Інтернеті та хмарі. Організації отримують повний контроль за доступом. Користувачі безпечно підключаються до ресурсів компанії в хмарі або локально, покращуючи свій досвід [1].

Розглянемо складові частини технології IAM.

FortiAuthenticator надає послуги керування ідентифікацією та доступом (IAM), щоб запобігти порушенням внаслідок отримання неавторизованими користувачами доступу до мережі або невідповідних рівнів доступу, наданих дійсним користувачам. FortiAuthenticator гарантує, що лише правильна особа може отримати доступ до ваших конфіденційних ресурсів і даних у потрібний час [2].

FortiPAM забезпечує керування привілейованим доступом, контроль і моніторинг привілейованих облікових записів, процесів і критичних систем у всьому IT-середовищі. FortiPAM є частиною Fortinet Security Fabric, яка інтегрується з такими продуктами, як FortiClient, FortiAuthenticator і FortiToken. Критичні активи мають бути захищені найвищим рівнем безпеки. FortiPAM забезпечує підвищену безпеку, включаючи контроль доступу до мережі без довіри (ZTNA) , коли користувачі намагаються отримати доступ до критичних ресурсів [3].

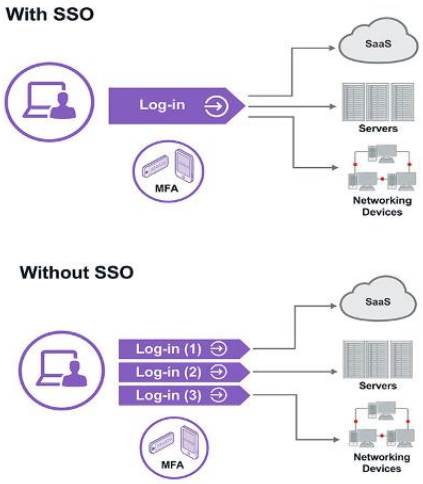


Рис. 1. Схема розгортання єдиного входу із централізованим керуванням ідентифікацією [2]

FortiToken допомагає запобігти зламам, які виникають через скомпрометовані облікові записи та паролі користувачів, підвищуючи надійність ідентичності користувачів, які намагаються отримати доступ до ресурсів. Для досягнення багатофакторної автентифікації (MFA) FortiToken інтегрується з FortiAuthenticator і FortiGate Firewall наступного покоління та є частиною рішення Fortinet Identity and Access Management (IAM).

FortiTrust Identity (FTI) базується на хмарі та вбудовано в Fortinet Security Fabric, щоб забезпечити багатий набір елементів керування безпекою та централізоване керування автентифікацією користувачів, включаючи багатофакторну автентифікацію. FTI дає змогу реалізувати нульову довіру з надійною перевіркою користувача та надійною автентифікацією, а також простотою використання для кінцевого користувача. Адаптивна, багатофакторна автентифікація або автентифікація без пароля та об’єднання ідентифікаторів для

SSO у корпоративному гібридному середовищі включено через ліцензування на основі користувачів.

Таким чином, нульова довіра починається з ідентифікації користувачів. Fortinet IAM дозволяє реалізувати наскрізне рішення для надання мінімального доступу до ресурсів компанії за допомогою MFA корпоративного рівня. Крім того, покращується взаємодія з користувачем за допомогою SSO.

Перелік посилань:

1. Identity and Access Management. Fortinet. URL: https://www.fortinet.com/solutions/enterprise-midsize-business/identity-access-management. (дата звернення: 29.09.2023).

2. FortiAuthenticator. Fortinet. URL: https://www.fortinet.com/products/identity-access-management/fortiauthenticator. (дата звернення: 29.09.2023).

3. Privileged Access Management. Fortinet. URL: https://www.fortinet.com/products/fortipam. (дата звернення: 29.09.2023).

Шайкова Анастасія Олегівна
Студентка групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ ЗА ДОПОМОГОЮ ELASTIC STACK

Загрози кібербезпеці постійно зростають у всьому світі. Організації повинні вдосконалювати свої процеси виявлення та протидії кібер-ризикам, якщо вони хочуть захистити інформацію, інфраструктуру та конфіденційність даних. Платформа для зберігання, пошуку та аналізу даних Elastic Stack є одним з ефективних рішень для досягнення цих цілей.

Elastic Stack є платформою для керування журналами [1].

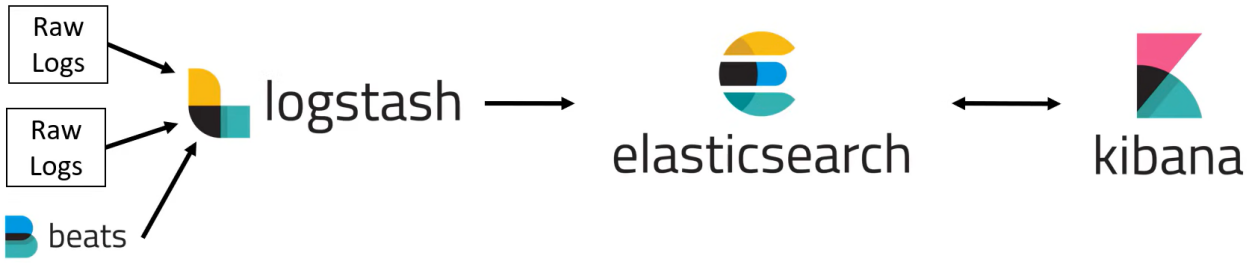


Рис. 1 – Рагальний вигляд Elastic Stack

Перший компонент – Logstash. З його допомогою відстежуються логи, журнали та події, що передаються до Elasticsearch.

Elasticsearch – це система пошуку та аналітики, яка підтримує Elastic Stack. Це просто обробка json-запитів. Будучи центром Elastic Stack, він централізовано зберігає дані для пошуку, точно налаштованої релевантності та потужної аналітики.

Kibana – це веб-інтерфейс. З його допомогою відбуватиметься взаємодія з великою кількістю даних, які Elasticsearch готує та індексує, щоб була можливість їх використовувати та створити інформаційні панелі.

Сервери, мережеві пристрої, програми та системи безпеки – це лише кілька прикладів джерел, з яких Elasticsearch можна налаштувати для отримання, аналізу та зберігання журналів, логів і подій. Інтеграція з різними системами SIEM (Security information and event management) є частиною цього процесу [1].

Потужні можливості індексації та пошуку Elasticsearch забезпечують швидкий пошук і доступ до даних. Це дозволяє дослідникам кібербезпеки швидко отримувати доступ до інформації про інциденти та загрози.

Можна налаштувати правила, які автоматично сповіщатимуть про можливі небезпеки, коли їх буде знайдено.

Elasticsearch зберігає дані у вигляді історії, що дозволяє вивчати попередні інциденти і створювати плани на випадок подібних обставин у майбутньому.

За допомогою Kibana можна створювати графіки та діаграми, які відображають кількість подій, їх розподіл у часі та іншу важливу інформацію. Аналітикам тепер легше виявляти закономірності та аномалії. Є можливість створювати інтерактивні дашборди, які можна налаштувати відповідно до певних вимог. Ці дашборди можуть відображати дані про загальну кількість інцидентів, реальні загрози, часову статистику та інше. Аналітики можуть взаємодіяти з візуалізаціями, фільтрувати дані та виконувати пошук в реальному часі для швидкого виявлення загроз та аномалій.

Використовуючи Elastic Stack у сфері кібербезпеки, організації можуть створити потужну інфраструктуру для моніторингу, оцінки та реагування на кіберзагрози в режимі реального часу, що піднімає планку безпеки та захисту інформації.

Перелік посилань:

1. Security solution unifying SIEM, endpoint & cloud. Elastic [Електронний ресурс] – Режим доступу: https://www.elastic.co/security.

Шапоренко Роман Сергійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна
Шкроб Олександр Олександрович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ФІШИНГОВИХ АТАК В КОРПОРАТИВНІЙ ЕЛЕКТРОННІЙ ПОШТІ

Виявлення фішингових атак в корпоративній електронній пошті є критично важливим завданням для забезпечення безпеки інформації та даних організацій. Фішингові атаки спрямовані на отримання конфіденційної інформації шляхом обману співробітників через відправку листів, які видавалися б за легітимні повідомлення.

За допомогою Cloudflare Area 1 можна комплексно захистити електронну пошту від складних загроз, зупиняючи фішинг на самих ранніх стадіях циклу атаки.

Cloudflare Area 1 надає захист Zero Trust від широкого спектру загроз:

компрометація бізнес-електронної пошти без зловмисного програмного забезпечення, багатоканальний фішинг, збір облікових даних та інший цільовий фішинг. І все це в хмарній службі, яку можна розгорнути за лічені хвилини, щоб захистити своїх користувачів Microsoft 365 і Gmail.

Рис 1. Cloudflare Area 1 – захист електронної пошти

Під час надсилання шкідливих електронних листів зловмисники часто намагаються видати себе за керівників організації. Функція компрометації бізнес-електронної пошти (BEC) захищає від цих атак.

Area 1 Email Security для захисту електронної пошти пропонує дві основні архітектури налаштування: Inline та API.

Завдяки розгортанню Inline Area 1 оцінює повідомлення електронної пошти, перш ніж вони потраплять до папки "Вхідні" користувача. Коли ви обираєте розгортання API, повідомлення електронної пошти потрапляють до зони 1 лише після того, як вони вже досягли папки "Вхідні" користувача.

Завдяки вбудованого розгортання Inline для налаштувань Area 1, Area 1 оцінює повідомлення електронної пошти, перш ніж вони потраплять до папки "Вхідні" користувача (рис 2).

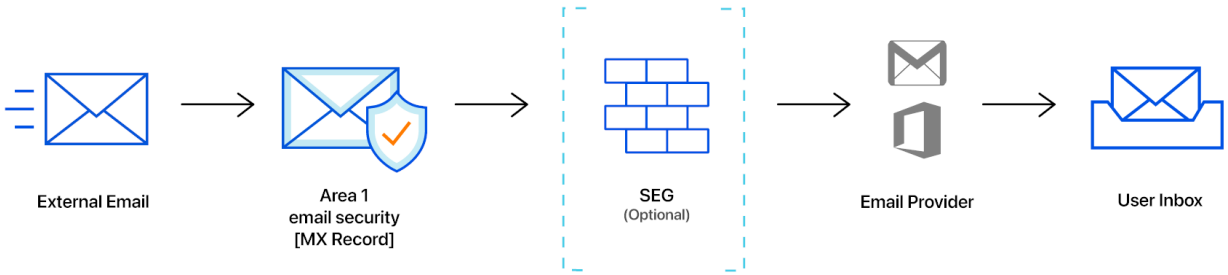


Рис.2. Вбудоване розгортання Inline

Технічно Зона 1 стає переходом у ланцюжку обробки SMTP і фізично взаємодіє з вхідними повідомленнями електронної пошти. Відповідно до вашої політики різні повідомлення блокуються до того, як потраплять до папки "Вхідні".

Завдяки вбудованому розгортанню повідомлення проходять через фільтр

електронної пошти Area 1, перш ніж досягти користувачів організації.

Переваги

Вибираючи вбудоване розгортання, ви отримуєте такі переваги:

Повідомлення обробляються та фізично блокуються перед доставкою в поштову скриньку користувача.

Ваше розгортання простіше, тому що будь-яка складна обробка може відбуватися нижче за потоком і без змін.

Зона 1 може змінювати доставлені повідомлення , додаючи розмітку до теми чи основного тексту.

Зона 1 може запропонувати високу доступність і адаптивне об’єднання повідомлень.

Ви можете налаштувати розширену обробку низхідних повідомлень для некарантинних повідомлень із доданими X-заголовками .

Обмеження

Вбудовані розгортання не позбавлені недоліків. Якщо ви розгортаєте Область 1 як свій запис MX, вам доведеться внести зміни у свій DNS. Якщо ні — і ви розгортаєте Область 1 після свого запису MX — у вас буде складніша архітектура SMTP.

Крім того, це налаштування може вимагати дублювання політики для кількох рішень і агента передачі пошти.

Перелік посилань

1. Безпека електронної пошти UR: https://www.cloudflare.com/en-gb/zero-trust/products/email-security/ (дата звернення 23.10.2023).

2. Вбудоване розгортання URL https://developers.cloudflare.com/email-security/deployment/ дата звернення 24.10.2023).

Шаталов Дмитро Дмтриович, БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА БАЗІ FORTIEDR

Визначено мету і основні завдання щодо забезпечення захисту кінцевих точок організації. Розглянуто зміст технології захисту кінцевих точок організації на базі FortiEDR.

Захист кінцевих точок організації має вирішальне значення, оскільки кінцеві точки часто є точками входу для кібератак і відіграють центральну роль у забезпеченні загальної кібербезпеки. Кінцеві точки, включаючи настільні комп'ютери, ноутбуки, сервери та мобільні пристрої, вразливі до широкого спектру кіберзагроз, таких як шкідливе програмне забезпечення, програми-вимагачі, фішинг та сучасні постійні загрози. Захист кінцевих точок є фундаментальним рівнем захисту від цих загроз.

На кінцевих точках часто зберігаються або отримується доступ до конфіденційних даних, включаючи інформацію про клієнтів, фінансові дані, інтелектуальну власність та записи про співробітників. Порушення або компрометації кінцевих точок можуть призвести до витоку даних, регуляторних санкцій та шкоди репутації.

Зростання обсягів віддаленої роботи та використання мобільних пристроїв означає, що кінцеві точки більше не обмежуються приміщеннями організації. Захист кінцевих точок необхідний для захисту віддалених робочих середовищ і мобільних пристроїв, які отримують доступ до корпоративних мереж і даних. Кінцеві точки часто підключені до корпоративної мережі. Скомпрометовані кінцеві точки можуть бути використані зловмисниками як плацдарм для подальшого переміщення в мережі, що потенційно може призвести до отримання доступу до більш важливих систем і даних.

FortiEDR забезпечує автоматизований захист кінцевих точок в режимі реального часу з організованим реагуванням на інциденти на будь-якому захищеному пристрої. Цей захист охоплює робочі станції, сервери та хмарні робочі навантаження з поточними та застарілими операційними системами, а також виробничі та OT-системи [1]. Побудоване на основі власної хмарної інфраструктури, рішення FortiEDR може бути розгорнуто у хмарі, локально або як гібридне розгортання (рис. 1) [2].

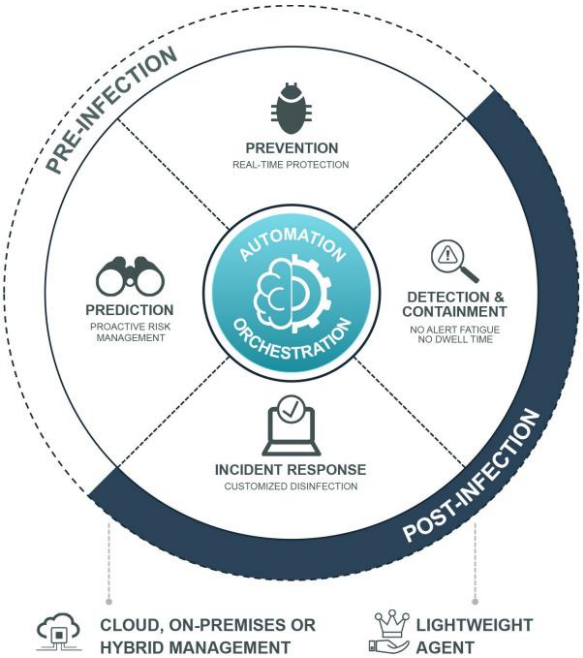


Рис. 1. Зміст технології EDR [2]

FortiEDR забезпечує найсучасніший автоматизований контроль політики поверхні атаки з оцінкою вразливостей, що дозволяє командам безпеки виявляти та контролювати несанкціоновані пристрої (наприклад, незахищені або некеровані пристрої) та пристрої IoT, відстежувати додатки, виявляти і зменшувати використання вразливостей системи і додатків за допомогою виправленням та проактивним політикам на основі ризиків [2].

FortiEDR використовує механізм машинного навчання для захисту від

шкідливих програм, щоб зупиняти атаки ще до їх виконання. Ця функція NGAV для різних операційних систем налаштовується і вбудована в єдиний легкий агент, що дозволяє користувачам призначати захист від шкідливого програмного забезпечення для будь-якої групи кінцевих точок без необхідності додаткового встановлення.

FortiEDR виявляє та знешкоджує безфайлове шкідливе програмне забезпечення та інші сучасні атаки в режимі реального часу, щоб захистити дані та запобігти витокам. Як тільки FortiEDR виявляє підозрілі потоки процесів і поведінку, FortiEDR негайно знешкоджує потенційні загрози, блокуючи вихідний зв'язок і доступ до файлової системи та доступ до файлової системи з боку цих процесів, якщо і коли це буде запитано. Ці кроки запобігають витоку даних, командно-контрольним комунікаціям (C2), фальсифікації файлів і шифрування програм-вимагачів. У той же час Fortinet Cloud Services (FCS), серверна частина FortiEDR, продовжує збирати додаткові докази, збагачувати дані про події та класифікувати інциденти для потенційної політики автоматизованого реагування на інциденти для активації [2].

FortiEDR дозволяє організовувати операції з реагування на інциденти, використовуючи індивідуальні сценарії з крос-середовищними інсайтами. FortiEDR автоматично збагачує дані детальною інформацією про шкідливе програмне забезпечення як до, так і після зараження, щоб проводити криміналістичні дослідження заражених кінцевих точок. Його унікальний інтерфейс надає корисні рекомендації, найкращі практики та пропонує наступні логічні кроки для аналітиків безпеки.

Отже, захист кінцевих точок організації має важливе значення для захисту даних, дотримання нормативних вимог, забезпечення безперервності бізнесу та захисту від широкого спектру кіберзагроз. Це важливий компонент комплексної стратегії кібербезпеки.

Перелік посилань:

1. Endpoint Detection and Response. Fortinet. URL: https://www.fortinet.com/products/endpoint-security/fortiedr. (дата звернення: 29.09.2023).
2. FortiEDR. Data Sheet. URL: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf. (дата звернення: 29.09.2023).

Шило Тетяна Ігорівна
студентка групи УБД-41,ННІЗІ ДУІКТ, Київ, Україна

РОЛЬ ЗАСОБІВ ПОВЕДІНКОВОЇ АНАЛІТИКИ У ПРОТИДІЇ ВНУТРІШНІМ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ОРГАНІЗАЦІЇ

Ця тема досліджує важливість та ефективність використання засобів поведінкової аналітики в контексті забезпечення інформаційної безпеки в організаціях. Внутрішні загрози можуть бути серйозними проблемами для безпеки даних та інформаційних ресурсів підприємства. Ця робота досліджує, як засоби поведінкової аналітики допомагають виявляти незвичайну або аномальну активність співробітників, що може бути індикатором потенційної загрози для інформаційної

безпеки. Аналізуються методи та техніки цього виду аналітики, а також її роль у виявленні, моніторингу та запобіганні внутрішнім загрозам для забезпечення стійкості організаційної інформаційної безпеки.

Ключовою проблемою інформаційної безпеки організації є виявлення компрометованих облікових записів користувачів та інсайдерів всередині компанії, які можуть мати зловмисні наміри (несанкціоновані користувачі). Різноманітність сценаріїв, в яких це може відбуватися, і величезна варіативність характеристик мережевих середовищ в різних компаніях роблять цю проблему дуже складною. Однак припущення про те, що дії скомпрометованого користувача за своєю суттю відрізняються від його повсякденних посадових обов'язків, дещо спрощує вирішення цієї проблеми. Якщо діяльність кожного користувача відстежується з часом і узгоджується з діяльністю інших подібних користувачів, можна скласти базовий профіль поведінки користувача, і будь-які відхилення від цієї поведінки можуть бути позначені як потенційні аномалії, які потребують подальшого розслідування.

Поведінкова аналітика у протидії внутрішнім загрозам інформаційній безпеці організації і виявлення аномалій - це дуже широкі термін. Хоча деякі методи поведінкової аналітики у протидії внутрішнім загрозам інформаційній безпеці організації вже досить давно використовуються в цілях бізнес-аналітики, вони в першу чергу орієнтовані на купівельні звички груп людей. У контексті інформаційної безпеки поведінковий аналіз може бути використаний для ретельної та зрозумілої розробки моделей, які підтримають здатність організації проводити оцінку ризиків ресурсів, таких як користувачі та комп'ютери в корпоративній мережі, для попередження окремих об'єктів, які можуть становити потенційну загрозу.

Приклади атак, які можна виявити за допомогою поведінкової аналітики у протидії внутрішнім загрозам інформаційній безпеці організації, можуть включати кіберзлочинця, який отримав доступ до законних облікових даних працівника, інсайдера, поведінка якого загрожує добробуту компанії, або зламаний сервер в мережі організації, який таємне надсилає корпоративні дані на сервер управління (C&C) у відкритому Інтернеті.

На перший погляд, поведінковий аналіз у протидії внутрішнім загрозам інформаційній безпеці організації може виглядати подібним до методів бізнес-аналітики, таких як когортна аналітика. Останній бере дані, зібрані в результаті використання продуктів або послуг, таких як платформа електронної комерції або онлайн-ігор, і розбиває їх на пов'язані групи для аналізу. Ці споріднені групи або когорти зазвичай мають спільні характеристики протягом певного періоду часу.

Правильно фіксуючи різні характеристики груп (наприклад, структуру покупок з часом), компанія може адаптувати свої послуги для конкретних груп (наприклад, пропонуючи спеціальні стимули на критичних етапах). Таким чином, когортний аналіз корисний для того, щоб зробити масовий маркетинг більш розумним та ефективним. Однак успіх або провал когортного маркетингу менш критичний для добробуту компанії, ніж поведінковий аналіз

інформаційної безпеки організації, де своєчасне виявлення атаки на коштовності компанії може врятувати компанію від втрати бізнесу.

На базовому рівні поведінковий аналіз у протидії внутрішнім загрозам інформаційній безпеці організації спирається на виявлення аномалій - здатність аналізувати великі обсяги даних і виявляти закономірності, які не відповідають статистичним очікуванням. З точки зору інформаційної безпеки такі аномалії можуть являти собою різні загрози: вторгнення в мережі зловмисника, необґрунтоване підвищення привілеїв, передача конфіденційної корпоративної інформації по незаконним каналам і т. д.

Розглянемо приклад аутентифікації користувача за допомогою поведінкової аналітики у протидії внутрішнім загрозам інформаційній безпеці організації. Традиційні методи в основному спиралися на схеми на основі паролів або біометричні методи для аутентифікації особи, яка отримує доступ до системи. Використовуючи підхід поведінкової аналітики, пристрій введення може відстежувати профіль взаємодії користувача, наприклад, швидкість клацання або геометричні закономірності руху миші, і відрізняти несанкціонованих від законних користувачів на основі змін у їх моделях взаємодії.

При розгортанні поведінкової аналітики у протидії внутрішнім загрозам інформаційній безпеці організації майже завжди потрібен етап налаштування для адаптації рішення до конкретного середовища, в якому воно знаходиться. Більше того, оскільки виявлення аномалій базується на статистичних методах, необхідно встановити базовий рівень нормальної поведінки системи. Жодна система не може бути повністю адаптована до особливих потреб організації. У деяких системах поодинокий невдалий вхід є причиною тривоги, тоді як в інших це може бути нормою, а перевірка вимагає виявлення іншого вектору атаки, такого як сканування портів. Щоб ефективно розставляти пріоритети та діяти виключно щодо справжніх порушень безпеки, організації необхідно мати ресурси для розслідування цих проблем. Для цієї мети неоціненно використовувати високоякісний інструмент криміналістики.

При розробці надійної стратегії безпеки підприємства поведінковий аналіз у протидії внутрішнім загрозам інформаційній безпеці організації забезпечує просунутий рівень захисту, але він не може замінити більш базові методи і, по суті, повинен ґрунтуватися на них. Наприклад, припустимо, що антивірусний інструмент стверджує, що успішно видалив шкідливе програмне забезпечення, але інші показники виявляють поведінку цього вірусу після злому. В цьому випадку поведінкова аналітика у протидії внутрішнім загрозам інформаційній безпеці організації може зіставити основні показники і допомогти прийти до правильного висновку.

Перелік посилань :

1.Загрози інформаційної безпеки організації https://csecurity.kubg.edu.ua/index.php/journal/article/view/281

Катков Юрій Ігорович
доктор технічних наук, професор кафедри комп'ютерних наук, ННІТ, ДУІКТ, Київ, Україна
Шлінчак Павло Ігорович
Студент групи КНДМ-62, ННІТ, ДУІКТ, Київ, Україна

ДОСЛІДЖЕННЯ СПОСОБІВ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ СИСТЕМНОГО АДМІНІСТРУВАННЯ МЕРЕЖЕВИХ ПРОЦЕСІВ

Впровадження штучного інтелекту (ШІ) в сфері кібербезпеки мережі стає необхідністю в епоху, коли кіберзагрози стають більш складними і вишуканими. Мережі є найважливішим елементом сучасного бізнесу та суспільства в цілому. Вони забезпечують комунікацію, обмін даними і функціонування місійно-критичних систем. З іншого боку, мережі стають об'єктом постійного вимірювання і атак з боку зловмисників, які намагаються використовувати всілякі методи для злому безпеки та доступу до цінної інформації. В цьому контексті роль ШІ стає ключовою. Штучний інтелект може стати могутнім союзником у боротьбі з кіберзагрозами, спрощуючи виявлення аномалій, виявлення інцидентів безпеки та навіть попередження їх виникнення.

Ключові слова: Штучний інтелект, системне адміністрування, мережеві процеси, аналіз трафіку, кібербезпека.

Методи та алгоритми штучного інтелекту для аналізу трафіку мережі.

Аналіз трафіку мережі стає необхідним завданням в умовах зростаючої комплексності мереж і збільшення кількості кіберзагроз. Для системних адміністраторів і фахівців з кібербезпеки важливо ретельно слідкувати за діяльністю в мережі для виявлення аномалій, виявлення потенційних загроз (викликів) та недопущення виникнення інцидентів. Саме в цьому контексті штучний інтелект (ШІ) виявляється як потужний інструмент для аналізу мережевого трафіку.

Використання ШІ для аналізу трафіку дозволяє автоматизувати процес виявлення аномалій та загроз (викликів), що раніше вимагав б значних зусиль і ресурсів. Це робить можливим ефективну і швидку реакцію на потенційні кіберзагрози та забезпечує високий рівень безпеки мережі (Рис.1).

Рисунок 1 – Класифікація загроз безпеки.

Ось декілька прикладів методів та алгоритмів штучного інтелекту для аналізу мережевого трафіку:

A. Виявлення аномалій в мережевому трафіку за допомогою машинного навчання: Методи машинного навчання, такі як алгоритми класифікації і кластеризації, можуть бути використані для виявлення аномалій в мережевому трафіку. Наприклад, алгоритми навчання з учителем можуть бути натреновані на нормальному трафіку для визначення звичайних патернів. Потім вони можуть виявляти аномалії, які суттєво відрізняються від цих звичайних патернів, що може свідчити про можливі загрози або інциденти безпеки. Прикладом такого застосування методу є технологія Vectra AI Network Detection [1].

B. Використання нейронних мереж для ідентифікації кіберзагроз: Нейронні мережі, зокрема глибокі нейронні мережі, можуть бути використані для аналізу мережевого трафіку на вищому рівні складності. Вони можуть розпізнавати складні патерни та відносини в даних, що може бути корисним при виявленні нових, раніше невідомих загроз. Прикладом такого застосування методу є технологія Darktrace [2] чи IBM Security QRadar [4].

C. Виявлення зловмисних атак на основі збору та аналізу журналів: Аналіз журналів та лог-файлів мережевих пристроїв за допомогою методів ШІ може допомогти виявити зловмисні атаки. Методи обробки природної мови та аналізу тексту можуть бути використані для ідентифікації підозрілих активностей в логах. Прикладом такого застосування методу є технологія Splunk [3].

Висновок

Оптимізація відгуку на кіберзагрози за допомогою штучного інтелекту є важливим напрямком розвитку в сфері кібербезпеки. ШІ дозволяє підвищити ефективність та точність виявлення кіберзагроз, а також знизити час реакції на потенційні інциденти. Організації, які впроваджують оптимізовані стратегії відгуку на кіберзагрози на основі ШІ, отримують важливий конкурентний перевагу в умовах надзвичайно складного та швидкозмінного кібербезпечного середовища. Звідси ШІ використовується для аналізу великих обсягів даних, виявлення аномалій, ідентифікації шкідливого програмного забезпечення та навіть автоматичного запуску заходів щодо запобігання або ліквідації кібератак. Це допомагає знизити ризик втрат та збитків, які можуть виникнути в результаті кіберзагроз. Однак важливо пам'ятати, що штучний інтелігентний аналіз не є панацеєю та має свої обмеження. Він потребує постійного нагляду та підтримки фахівців з кібербезпеки. Також важливо забезпечувати конфіденційність та захист даних під час аналізу, оскільки навіть самі алгоритми ШІ можуть стати об'єктом атак. Тому усе більше організацій розглядають оптимізацію відгуку на кіберзагрози як необхідну складову своєї стратегії кібербезпеки, і разом із штучним інтелектом вони готові забезпечити вищий рівень захисту та швидкості

реакції на кіберзагрози в надзвичайно змінному і вимогливому цифровому середовищі.

Перелік посилань:

1. Центр ресурсів Vectra Know when your network is compromised // [Електронний ресурс] Режим доступу до ресурсу: https://www.vectra.ai/products/ndr
2. Центр ресурсів Darktrace Darktrace Cyber AI Research Centre // [Електронний ресурс] Режим доступу до ресурсу: https://darktrace.com/research
3. Центр ресурсів Splunk Explore our collection of e-books, white papers, analyst reports, briefs and more — all here. // [Електронний ресурс] Режим доступу до ресурсу: https://www.splunk.com/en_us/resources.html
4. Центр ресурсів IBM-QRadar IBM Security QRadar Suite.// [Електронний ресурс] Режим доступу до ресурсу: https://www.ibm.com/qradar

Гайдур Галина Іванівна,
д. т. н., професор
Шулімов Денис Олександрович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ВИЯВЛЕННЯ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКУ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Виявлення аномалій у комунікаційних мережах забезпечує основу для виявлення нових атак, неправильних конфігурацій і мережевих збоїв. Обмеження ресурсів для зберігання, передачі та обробки даних роблять вигідним обмеження вхідних даних функціями, які мають велике значення для завдання виявлення та легко виводяться з мережевих спостережень без дорогих операцій. Видалення сильно корельованих, надлишкових і нерелевантних функцій також покращує якість виявлення для багатьох алгоритмів, які базуються на методах навчання.

Сучасні комунікаційні мережі швидко розвиваються. Те саме стосується мережевих атак. Щодня з’являються нові вразливості, які швидко використовуються в атаках нульового дня. У той час як виявлення на основі сигнатур не може виявити раніше невідомі атаки, методи виявлення аномалій можуть виявити відхилення від нормальних шаблонів трафіку і, отже, є важливим інструментом для підвищення безпеки мережі в сучасних мережах зв’язку.

Хоча існує значна кількість технічної та наукової літератури про методи виявлення аномалій для мережевого трафіку, цінний етап вибору функцій часто недостатньо представлений і розглядається в літературі неуважно. Джерела вказують на три часто дефектні аспекти в дослідженні виявлення аномалій: використані набори даних, характеристики проведених експериментів і методи, що використовуються для оцінки ефективності. У характеристиках експериментів автори підкреслюють попередню обробку даних як одну з фаз, які зазвичай пропускають у відповідних статтях, вказуючи на те, що вибір ознак зазвичай здійснюється вільно без належного обґрунтування. Це досить прикро, оскільки видалення тривіальних і надлишкових функцій не тільки зменшує споживання ресурсів для обробки, зберігання та передачі даних, воно також покращує моделювання явищ, що аналізуються, і, отже, є визначальним кроком у виявленні мережевих аномалій.

Організаціям потрібна динамічна технологія, яка знає, як відрізнити ненормальну поведінку від нормальної поведінки в тому, як хости та сервери взаємодіють із мережею. Тут можуть стати в нагоді статистичні методи, такі як виявлення аномалій на основі машинного навчання. Коротше кажучи, виявлення мережевих аномалій базується на класифікації даних шляхом розрізнення незвичної поведінки програм або пристроїв у порівнянні з тим, що адміністратор мережі організації вважає нормальним. Такі методи, як статистична теорія та теорія інформації, переважно використовувалися мережевими адміністраторами.

Машинне навчання було прийнято в різних сферах для розв'язання складних проблем, і його використання для виявлення аномалій мережевого трафіку в реальному часі є не менш потужним. Замість того, щоб зіставляти наявні сигнатури, машинне навчання адаптується до розпізнавання складних шаблонів трафіку та аналізує поведінку, пов'язану з певними атаками, які є невидимими та можуть завдати шкоди, забезпечуючи розумні рішення на основі цих даних. Таким чином, незалежно від того, чи це відома чи невідома атака, адміністратори не будуть захоплені зненацька.

Використовуючи виявлення аномалій, мережеві адміністратори можуть позначати поведінку як «хорошу», «нормальну», а також «підозрілу» та отримувати сповіщення про конкретну активність, яка відрізняється від звичайного трафіку. Виявлення на основі аномалій може бути корисним для пошуку атак, які не відповідають базовій поведінці, наприклад, коли користувач входить у неробочий час, підключені пристрої додаються до мережі або коли потоки запитів встановлюють з'єднання з мережею. Таким чином, багато вторгнень нульового дня можна відразу виявити та повідомити про них, щоб захистити безпеку мережі.

- Забезпечує цілісне уявлення про весь мережевий трафік;
- Виявляє аномальний трафік для фізичних і віртуальних платформ;
- Відстежує весь потік і атрибути, такі як IP-адреси джерела та призначення, а також порти та протоколи для створення базових показників поведінки;
- Допомагає командам розробників підвищити надійність і продуктивність своїх програм.

Перелік посилань:

1. Analysis of network traffic features for anomaly detection URL: https://link.springer.com/article/10.1007/s10994-014-5473-9
2. Network traffic anomaly detection: A fail-proof traffic monitoring technique URL: https://www.manageengine.com/products/netflow/network-traffic-anomaly-detection.html

Шулімова Дар'я Денисівна
студентка групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Керівники компаній та IT-відділи перебувають під посиленим регуляторним та організаційним тиском щодо захисту доступу до корпоративних ресурсів. Як результат, вони більше не можуть покладатися на ручні та схильні до помилок процеси для призначення та відстеження привілеїв користувачів. IAM автоматизує ці завдання та забезпечує детальний контроль доступу та аудит усіх корпоративних активів.

Управління ідентифікацією та доступом (IAM) – це структура бізнес-процесів, політик і технологій, яка полегшує керування електронною або цифровою ідентифікацією. Завдяки системі IAM керівники інформаційних технологій можуть контролювати доступ користувачів до критично важливої інформації у своїх організаціях. Системи, що використовуються для IAM, включають системи єдиного входу, двофакторну автентифікацію, багатофакторну автентифікацію та керування привілейованим доступом. Ці технології також забезпечують можливість безпечного зберігання ідентифікаційних даних і даних профілів, а також функції керування даними, щоб забезпечити спільний доступ лише до необхідних і актуальних даних.

Системи IAM можуть бути розгорнуті на місці, надані стороннім постачальником через хмарну модель підписки або розгорнуті в гібридній моделі.

На фундаментальному рівні IAM включає такі компоненти:

- як люди ідентифікуються в системі;
- як ідентифікуються ролі в системі та як вони призначаються окремим особам;
- додавання, видалення та оновлення осіб та їхніх ролей у системі;
- призначення рівнів доступу особам або групам осіб;
- захист конфіденційних даних у системі та безпека самої системи.

IAM, який має постійно зростаючий перелік функцій, включаючи біометрію, аналітику поведінки та штучний інтелект, добре підходить для суворих умов нового середовища безпеки. Наприклад, жорсткий контроль IAM доступу до ресурсів у сильно розподілених і динамічних середовищах узгоджується з переходом галузі від брандмауерів до моделей нульової довіри та з вимогами безпеки IoT.

Основні компоненти IAM

Інфраструктура IAM дозволяє IT контролювати доступ користувачів до важливої інформації в їхніх організаціях. Продукти IAM пропонують контроль

доступу на основі ролей, який дозволяє системним адміністраторам регулювати доступ до систем або мереж на основі ролей окремих користувачів на підприємстві.

Переваги IAM

Технології IAM можна використовувати для ініціювання, захоплення, запису та керування ідентифікаційними даними користувачів і пов'язаними з ними дозволами доступу в автоматизований спосіб. Організація отримує такі переваги IAM:

- Права доступу надаються відповідно до політики, і всі особи та служби належним чином автентифіковані, авторизовані та перевірені.
- Компанії, які належним чином керують ідентифікацією, мають більший контроль над доступом користувачів, що зменшує ризик внутрішніх і зовнішніх порушень даних.
- Автоматизація систем IAM дозволяє підприємствам працювати ефективніше за рахунок зменшення зусиль, часу та грошей, які потрібні для ручного керування доступом до їхніх мереж.
- З точки зору безпеки, використання фреймворку IAM може спростити застосування політик щодо автентифікації користувачів, підтвердження та привілеїв.
- Системи IAM допомагають компаніям краще дотримуватися державних постанов, дозволяючи їм демонструвати, що корпоративна інформація не використовується зловживанням. Компанії також можуть продемонструвати, що будь-які дані, необхідні для аудиту, можуть бути доступні на вимогу.

Технології IAM дозволяють компанії надавати користувачам за межами організації – таким як клієнти, партнери, підрядники та постачальники – доступ до своєї мережі через мобільні програми, локальні програми та SaaS без шкоди для безпеки. Це забезпечує кращу співпрацю, підвищення продуктивності, підвищення ефективності та зниження експлуатаційних витрат.

Перелік посилань:

3. What is Identity and Access Management (IAM)? URL: https://www.oracle.com/il-en/security/identity-management/what-is iam/#:~:text=Identity%20and%20access%20management%20(IAM)%20manages%20the%20end%2Dto,to%20systems%2C%20networks%20and%20data.

4. What is identity and access management? Guide to IAM URL: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system

Катков Юрій Ігорович
доктор технічних наук, професор кафедри комп'ютерних наук, ННІТ, ДУІКТ, Київ, Україна
Шуляк Андрій Олегович
Студент групи КНДМ-62 ННІТ, ДУІКТ, Київ, Україна

МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ КОРИСТУВАЧА У ЛОГІСТИЧНОЇ КОМПАНІЇ

Розглядається взаємопов’язаність двох проблем: забезпечення безпеки та конфіденційності даних користувача у логістичної компанії. Проблема забезпечення безпеки даних (захист даних) вживає відповідні заходи, щоб запобігти доступу до будь-яких даних компанії несанкціонованих третіх осіб. Проблема конфіденційності даних базується на властивості конфіденційності, що означає не підлесливість розголосові; довірливість, секретність, суто приватність. Тому конфіденційність даних стосується захисту даних від несанкціонованого доступу та розголошення, включаючи засоби захисту особистої конфіденційності та конфіденційної інформації. У логістичних компаніях захист даних і конфіденційність зазвичай застосовуються до особистої інформації про бізнес процеси і персональну інформацію користувачів послугами (товарами) цієї компанії. Тому забезпечення безпеки та конфіденційності даних користувача відіграє життєва важливу роль у бізнес-операціях, розвитку та фінансах. Захищаючи дані, компанії можуть запобігти витоку даних, що може завдати шкоди репутації та краще відповідати нормативним вимогам. Звідси відповідно до бізнес завдань у логістичної компанії ці дві проблеми взаємопов’язані алгоритмами обробки інформації про процеси переміщення товарів (продукції, послуг) для конкретних користувачів.

Ключові слова: забезпечення безпеки даних, конфіденційність даних, кібербезпека.

1. Актуальність.

Терміни захист даних і конфіденційність даних часто використовуються як синоніми, але між ними є важлива різниця. Незважаючи на те, що захист даних і конфіденційність є важливими і вони часто поєднуються, ці терміни не означають одне й те саме.

Захист даних – це набір стратегій і процесів, які можна використовувати для забезпечення конфіденційності, доступності та цілісності даних. Іноді це також називають безпекою даних.

Конфіденційність даних - визначає, хто має доступ до даних, тоді як захист даних надає інструменти та політики для фактичного обмеження доступу до даних. Правила відповідності допомагають гарантувати, що запити користувачів щодо конфіденційності виконуються компаніями, і компанії відповідають за вживання заходів для захисту особистих даних користувачів. Конфіденційність даних допомагає гарантувати, що конфіденційні дані будуть доступні лише для схвалених сторін. Це запобігає зловмисному використанню даних злочинцями та допомагає гарантувати, що організації відповідають нормативним вимогам.

Таким чином, захист даних стосується механізмів реалізації даних, конфіденційність даних — політику застосування інструментів та процесів захисту даних. Тому рішення щодо захисту даних є актуальним і покладаються на такі сучасні технології, як запобігання втраті даних (Data loss prevention defined - DLP), сховище з вбудованим захистом даних, брандмауери, шифрування та захист кінцевих точок (EPP - endpoint protection platform).

2. Методи забезпечення безпеки та конфіденційності даних користувача у логістичної компанії

Запобігання втраті даних — це рішення безпеки, яке визначає та допомагає запобігти небезпечному чи неналежному обміну, передачі або використанню конфіденційних даних. Це може допомогти компанії контролювати та захищати

конфіденційну інформацію в локальних системах, хмарних розташуваннях і кінцевих пристроях.

Сховище з вбудованим захистом даних – це системи зберігання даних, які часто включають детальний контроль доступу, що дозволяє обмежити, хто може отримати доступ до ваших даних і за яких обставин. Це може допомогти запобігти несанкціонованому доступу та зберегти конфіденційність вашої інформації.

Брандмауер — це пристрій безпеки мережі, який відстежує та фільтрує вхідний і вихідний мережевий трафік на основі попередньо встановлених політик безпеки організації . За своєю суттю брандмауер — це, по суті, бар'єр, який стоїть між приватною внутрішньою мережею та загальнодоступним Інтернетом.

Шифрування – це процес захисту інформації або даних за допомогою математичних моделей для їх кодування таким чином, щоб доступ до них мали лише ті сторони, які мають ключ для їх декодування.

Платформа захисту кінцевих точок— це рішення, яке розгортається на кінцевих пристроях для запобігання атакам зловмисного програмного забезпечення на основі файлів, виявлення зловмисної активності та забезпечення можливостей розслідування та виправлення, необхідних для реагування на динамічні інциденти безпеки та попередження.

Для застосування цих сучасних технології розроблені наступні методи:

Метод визначення стратегії захисту даних – його застосування життєве важливо для будь-якої організації, яка збирає, обробляє або зберігає конфіденційні дані. Успішна стратегія може допомогти запобігти втраті даних, крадіжці або пошкодженню, а також може допомогти мінімізувати шкоду, заподіяну в разі порушення чи катастрофи. Метод стратегії захисту даних базується на принципах захисту даних, які допомагають захистити дані та зробити їх доступними за будь-яких обставин. Це охоплює оперативне резервне копіювання даних і безперервність роботи/аварійне відновлення, а також включає впровадження аспектів керування даними та доступності даних. Ось ключові аспекти керування даними, що пов'язані із захистом даних:

Доступність даних — забезпечення доступу користувачів до даних, необхідних для ведення бізнесу, і їх використання, навіть якщо ці дані втрачено або пошкоджено.

Управління життєвим циклом даних — передбачає автоматизацію передачі критично важливих даних до офлайн- та онлайн-сховищ.

Управління життєвим циклом інформації — включає оцінку, каталогізацію та захист інформаційних активів з різних джерел, включаючи оцінку збоїв в роботі об'єктів, помилки додатків і користувачів, шкідливі програми та вірусні атаки.

Метод виконання політик (правил) захисту даних. Правила захисту даних регулюють спосіб збору, передачі та використання певних типів даних. Персональні дані включають різні типи інформації, включаючи імена, фотографії, адреси електронної пошти, реквізити банківського рахунку, IP-

адреси персональних комп’ютерів і біометричні дані. Правила захисту даних і конфіденційності відрізняються в різних країнах, штатах і галузях. Недотримання закону може призвести до збитків репутації та грошових штрафи залежно від порушення згідно з інструкціями кожного закону та керуючого органу. Дотримання одного набору правил не гарантує дотримання всіх законів. Крім того, кожен закон містить численні положення, які можуть застосовуватися до одного випадку, але не до іншого, і всі нормативні акти можуть бути змінені. Цей рівень складності ускладнює послідовне та належне впровадження відповідності. Створення правил конфіденційності даних не гарантує, що неавторизовані користувачі не матимуть доступу. Так само ви можете обмежити доступ за допомогою захисту даних, залишаючи конфіденційні дані вразливими. Обидва необхідні для забезпечення безпеки даних. Звідси інша важлива відмінність між конфіденційністю та захистом полягає в тому, хто зазвичай контролює. З міркувань конфіденційності користувачі часто можуть контролювати, якою кількістю їхніх даних ділитися та з ким. Для захисту компанії, які обробляють дані, повинні забезпечити їх конфіденційність. Норми відповідності відображають цю різницю та створені, щоб гарантувати, що запити користувачів щодо конфіденційності виконуються компаніями. Тобто - користувачі контролюють конфіденційність, компанії забезпечують захист.

На основі цього методу формуються: політика захисту даних; стратегія захисту даних; визначаються технології та практики захисту даних для захисту приватних даних.

Що стосується захисту ваших даних, користувач може вибрати з багатьох варіантів зберігання та керування. Рішення можуть допомогти: обмежити доступ, контролювати активність і реагувати на загрози.

Для розуміння складності забезпечення безпеки та конфіденційності даних користувача у логістичної компанії ось деякі з найбільш часто використовуваних практик і технологій: виявлення даних; інвентаризація та класифікація даних; відображення даних; інструменти автоматизованого виявлення; політики запобігання втраті даних; моніторинг і сповіщення; санація; зберігання з вбудованим захистом даних; надмірність; виправлення помилок; контроль доступу; резервне копіювання; локальні та зовнішні резервні копії; інкрементні та повні резервні копії; планування резервного копіювання; моментальні знімки; миттєве відновлення; керування версіями; ефективність зберігання; тиражування; відмово стійкість; реплікація даних (відмова); балансування навантаження; географічна надмірність; брандмауери; виявлення та запобігання вторгненням; контроль додатків; моніторинг руху; автентифікація та авторизація; багатофакторна автентифікація; контроль доступу на основі ролей; керування ідентифікацією та доступом; симетричне, асиметричне та наскрізне шифрування; захист кінцевої точки; антивірус і захист від шкідливих програм; управління пристроєм; керування виправленнями; стирання даних; безпечні методи видалення; політика знищення даних; сертифікація та аудит; аварійного відновлення; аналіз впливу на бізнес; планування аварійного відновлення; тестування та технічне обслуговування та інші.

Висновок.

Таким чином, забезпечення безпеки та конфіденційності даних користувача відіграє життєва важливу роль у бізнес-операціях, розвитку та фінансах. Захищаючи дані, компанії можуть запобігти витоку даних, що може завдати шкоди репутації та краще відповідати нормативним вимогам. Звідси відповідно до бізнес завдань у логістичної компанії ці дві проблеми взаємопов'язані алгоритмами обробки інформації про процеси переміщення товарів (продукції, послуг) для конкретних користувачів. Розгляд взаємопов'язаність двох проблем показав, що проблема забезпечення безпеки даних (захист даних) вживає відповідні заходи, щоб запобігти доступу до будь-яких даних компанії несанкціонованих третіх осіб, а проблема конфіденційності даних базується на властивості конфіденційності, що означає не підлесливість розголосові; довірливість, секретність, суто приватність. Для їх сумісного вирішення існують методи забезпечення безпеки та конфіденційності даних користувача у логістичної компанії, на основі яких використовуються практики і технології.

Перелік посилань:

1. База даних [Електронний ресурс] // Wikipedia. – 31 січня 2023. – Режим доступу до ресурсу: http://surl.li/bqulg

2. Managing data confidentiality // [Електронний ресурс] Режим доступу до ресурсу: https://www1.udel.edu/security/data/confidentiality.html

3. What is Data Confidentiality? // [Електронний ресурс] Режим доступу до ресурсу: https://www.secoda.co/glossary/data-confidentiality

4. What is Cyber Security? // [Електронний ресурс] Режим доступу до ресурсу: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

5. 10 Data Security Best Practices: Simple Methods to Protect Your Data Origin: // [Електронний ресурс] Режим доступу до ресурсу: https://www.ekransystem.com/en/blog/data-security-best-practices

Щавінський Юрій Віталійович
доцент кафедри УІКБ, ННІЗІ ДУІКТ, Київ, Україна
Кудін Ігор Валерійович
студент групи УБДМ-61, ННІЗІ ДУІКТ, Київ, Україна
Порохницький Олександр Андрійович
студент групи УБДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ЕТИЧНІ МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ІНЦИДЕНТАМИ І РИЗИКАМИ

Етичні методи та засоби управління інформаційними інцидентами та ризиками є важливою складовою сучасного управління інформаційною безпекою. Ці методи та засоби дозволяють забезпечити захист інформації від несанкціонованого доступу, використання, розголошення, втрати або зміни. Досліджується питання етичних аспектів управління інформаційними інцидентами і ризиками в контексті сучасного інформаційного суспільства, розв'язання дилем між професійним та корпоративним кодексом. Розглядаються етичні методи та засоби, які можуть бути використані організаціями для забезпечення відповідального та справедливого підходу до управління інформаційною безпекою.

У сучасному світі інформація є однією з найцінніших активів для бізнесу, уряду та суспільства загалом. Проте зростання залежності від інформаційних технологій також призводить до збільшення ризику інформаційних інцидентів, таких як порушення даних, кібератаки та розповсюдження дезінформації. Управління цими ризиками вимагає не лише технічних заходів, але й етичного підходу.

Теми етичного управління ризиками та загрозами у інформаційній сфері є предметом наукових досліджень вітчизняних та зарубіжних фахівців. Вони згадуються у науково-практичній літературі з управління організаційними ризиками, але є дуже мало доказів їх детального аналізу.

Науковці відзначають, що управління ризиками спрямоване на полегшення обміну інформацією та досвідом між країнами та між різними дисциплінами. Його мета – генерувати ідеї та просувати передову практику для тих, хто займається бізнесом управління ризиками. В роботі [1] зазначено, що занадто часто оцінки ризику робляться грубо і наслідки неправильного вчинення можуть бути серйозними, включаючи втрачені можливості, втрату бізнесу, втрату репутації і навіть життя. При цьому управління інформаційними інцидентами повинно базуватися на принципах етики, таких як права людини, конфіденційність і прозорість. Організації повинні визнати важливість захисту приватності користувачів та дотримання етичних стандартів у зборі та обробці інформації [2].

Разом з тим, етичному управлінню ризиками (тобто професійній етиці в управлінні ризиками) сьогодні приділяється набагато менше уваги і рідко виявляється основним об'єктом етичного аналізу.

Етично обґрунтоване управління ризиками включає в себе як управління етичними ризиками, так і етичне управління ризиками (професійна етика). Сьогодні професіонали інформаційної безпеки стикаються зі значними моральними дилемами під час своєї роботи. Як один із засобів управління інцидентами і ризиками, вирішенню таких дилем призначений кодекс професійної етики, який відповідає їхнім проблемам при виконанні функціональних обов’язків. Такий кодекс допомагає внести ясність у складні етичні ситуації а також забезпечує потужний захист від тиску з боку керівників та підлеглих щодо неетичних дій. Разом з тим, етичний кодекс організації або кодекс поведінки компанії (корпоративний кодекс, теж як один із засобів) може суперечити професійному кодексу. У таких випадках науковці стверджують, що професійний кодекс є першим. Наприклад, людина працює інженером або практикуючим лікарем і тому її підписка на відповідні професійні стандарти має першорядне значення. Таким чином, будь-яке етичне звинувачення має виражати конкретне порушення з точки зору принаймні одного розділу професійного кодексу [2].

Існують різноманітні етичні методи та засоби управління інформаційними інцидентами та ризиками, такі як:

визначення потенційних загроз безпеці інформації (ідентифікація ризиків);

оцінювання ймовірності виникнення ризикових подій та їх наслідків (аналіз ризиків);

прийняття рішень щодо зменшення ризикових подій та їх наслідків (управління ризиками);

запобігання виникнення інцидентів, пов’язаних з безпекою інформації (попередження інцидентів);

виявлення, дослідження та вирішення проблем, пов’язаних з безпекою інформації (реагування на інциденти);

Для боротьби з інцидентами та ризиками пов’язаними з безпекою інформації, необхідно застосовувати комплексний підхід, який включатиме в себе як технологічну складову (застосування спецзасобів), так і організаційно-адміністративний (розробка положень, правил, стандартів тощо) з обов’язковим врахуванням етичної складової.

Науковці відзначають, що зв'язок між управлінням ризиками та інцидентами і етикою повинен розвиватися ще при підготовці фахівців у навчальних закладах, щоб сприяти прогресивним змінам у бік більш соціально та екологічно відповідальних практик [3].

Для прикладу, одною із освітніх компонентів освітньо-професійної програми підготовки професіонала спеціальності 125 Кібербезпека та захист інформації [4] є навчальна дисципліна «Корпоративна та професійна етика в кібербезпеці», яка забезпечує формування у студентів базових теоретичних знань, необхідних для розуміння проблем професійної та корпоративної етики в управлінні інформаційною та кібербезпекою, практичних навичків застосування етичних засобів і методів управління інформаційними інцидентами і ризиками, етичного вирішення проблем та впровадження заходів протидії кіберінцидентам.

Зв’язки між освітніми компонентами освітньо-професійної програми підготовки фахівця другого (магістерського) рівня вищої освіти у Державному університеті інформаційно-комунікаційних технологій, показані на рисунку 1, підтверджують важливість етичної складової при формуванні компетентностей, необхідних спеціалістам інформаційної безпеки для етичного управління інцидентами і ризиками.

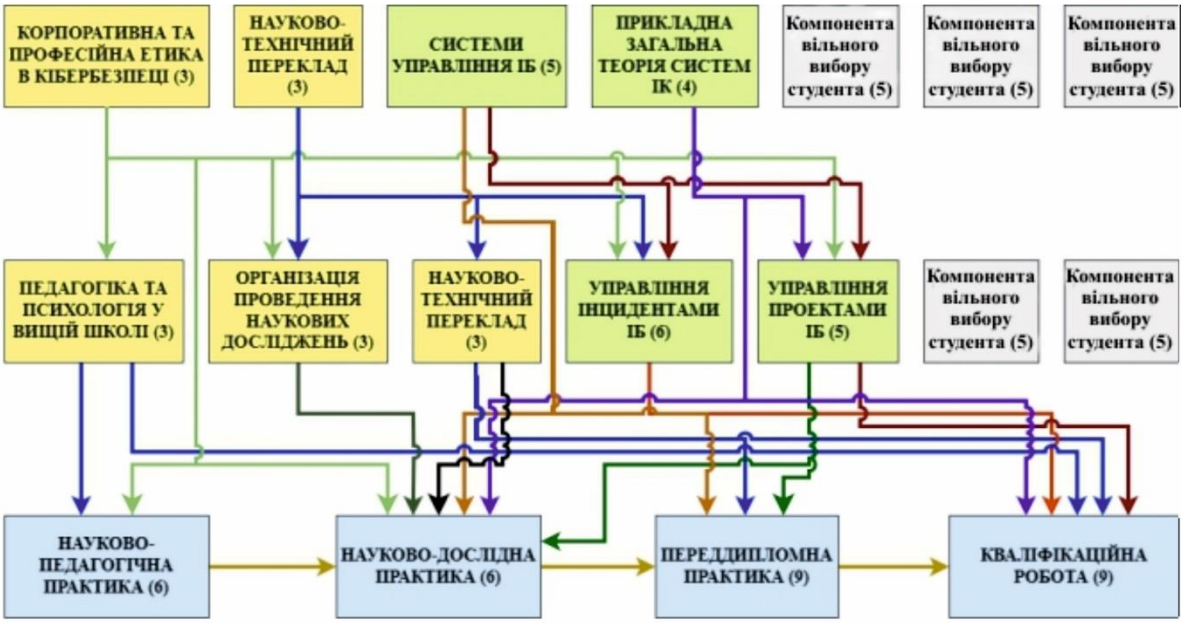


Рис. 1. Зв’язки освітніх компонентів підготовки магістра

Таким чином, етика в управлінні інформаційними інцидентами та ризиками має вирішальне значення для забезпечення довіри та безпеки в інформаційному середовищі. При цьому, етичні методи та засоби допомагають організаціям виявляти, запобігати та реагувати на інциденти відповідальним та справедливим способом. Це сприяє збереженню репутації та довіри користувачів, а також допомагає будувати стійкі та етичні інформаційні системи.

Перелік посилань:

1. S. Tippins, Letter from the Editor. / Risk Management, Vol. 6, No. 3, 2004, c. 7. JSTOR . http://www.jstor.org/stable/3867773.
2. R Francis, A, Armstrong. Ethics as a Risk Management Strategy: The Australian Experience. / Journal of Business Ethics. 45. 2003. Pp. 375-385. Doi: https://doi.org/10.1023/A:1024163831371
3. Guntzburger, Y., Pauchant, T.C. & Tanguy, P.A. Ethical Risk Management Education in Engineering: A Systematic Review. Sci Eng Ethics 23, 323–350 (2017). https://doi.org/10.1007/s11948-016-9777-y .
4. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ. Освітньо-професійна програма другого (магістерського) рівня вищої освіти (оновлена). [Електронний ресурс] Режим доступу: URL: https://duikt.edu.ua/uploads/p_1826_74639802.pdf (дата звернення – 22.10.23).

Щибун Євген Юрійович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ЗАХИСТ ВІД СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ: ЗАХИСТ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ ВІД ЛЮДСЬКОГО ФАКТОРУ

Соціальна інженерія як несумлінний спосіб отримання доступу до цінної корпоративної інформації, нині стала однією з найбільших загроз для інформаційної безпеки підприємств. Ця техніка залучає виключно "людський фактор" і, протистояти їй виявляється вкрай важко. Проте, з прийняттям правильних заходів можливо забезпечити надійний захист корпоративної інформації.

Розуміння соціальної інженерії:

Соціальна інженерія - це методика зловживання психологічними та соціальними маніпуляціями для отримання конфіденційної інформації або доступу до систем і ресурсів. Вона базується на використанні технік, які надають зловмиснику можливість обдурити людей, щоб отримати доступ до інформації, яку зазвичай важко було б отримати шляхом технічних засобів. Спеціалісти з соціальної інженерії використовують методи, такі як підман, фішинг, фізичний доступ та інші маніпуляційні техніки.

Наслідки атак соціальної інженерії:

Втрата конфіденційної інформації: Атаки можуть призвести до витоку конфіденційних даних.

Фінансові втрати: Організації можуть понести фінансові втрати через крадіжку грошей або маніпуляцію фінансами.

Порушення репутації: Вразливості, розкриті атаками соціальної інженерії, можуть негативно вплинути на репутацію підприємства або особи.

Крадіжка ідентичності: Атаки можуть призвести до крадіжки особистої інформації та використання її для шахрайства.

Втрата доступу до систем та обладнання: Зловмисники можуть отримати доступ до систем і обладнання організації та користуватися ним.

Юридичні наслідки: Порушення безпеки даних через соціальну інженерію може призвести до юридичних наслідків та штрафів.

Ефективні контрзаходи для захисту від соціальної інженерії:

Навчання співробітників: Забезпечення інформаційної грамотності співробітників, навчання їх розпізнавати інженерів та потенційні загрози.

Зміцнення політики безпеки: Встановлення строгих правил та процедур для роботи з конфіденційною інформацією, а також для доступу до неї.

Моніторинг та аудит безпеки: Постійне відстеження доступу до інформації, реєстрація спроб незаконного доступу, та аудит систем безпеки.

Використання двофакторної аутентифікації: Захист доступу до систем та інформації за допомогою двох або більше методів перевірки особи.

Фізичний захист: Обмеження фізичного доступу до серверних приміщень та інших важливих зон.

Системи моніторингу та реагування: Розробка систем виявлення та реагування на підозрілі дії або спроби соціальної інженерії.

Своєчасне оновлення та патчі: Забезпечення систем регулярними оновленнями та патчами для закриття вразливостей.

Усвідомлення загроз: Надання працівникам чіткої інформації про потенційні загрози та методи соціальної інженерії.

Підсумовуючи, соціальна інженерія залишається вагомою загрозою для корпоративної інформації через її залучення "людського фактору". Проте, використання ефективних контрзаходів може суттєво зменшити ризики. Розуміння загроз соціальної інженерії та активне впровадження відповідних заходів захисту важливі для забезпечення безпеки корпоративної інформації в

сучасному середовищі.

Перелік посилань:
1. Mitnick, Kevin D., and William L. Simon. "The Art of Deception: Controlling the Human Element of Security." Wiley, 2002 (дата звернення 22.10.2023)
2. Hadnagy, Christopher. "Social Engineering: The Art of Human Hacking." Wiley, 2010 (дата звернення 23.10.2023)
3. Sjouwerman, Stu. "Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails." Wiley, 2015 (дата звернення 23.10.2023)
4. Federal Trade Commission. "How to Recognize and Avoid Phishing Scams." URL: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (дата звернення 24.10.2023)

Юнак Дмитро Олегович
студент групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМИ МОНІТОРИНГУ Й РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ (SOC) В ОРГАНІЗАЦІЇ

В сучасному цифровому світі зростає загроза кібератак і порушень безпеки. Системи моніторингу й реагування на інциденти безпеки (SOC) грають ключову роль у виявленні та запобіганні таким загрозам. Оцінка ефективності SOC допомагає організаціям зрозуміти, наскільки добре їх системи працюють. Ця оцінка включає в себе аналіз часу від виявлення до реагування на інциденти, відповідність стандартам безпеки, якість збору та аналізу даних, а також здатність SOC адаптуватися до нових загроз. Правильна оцінка допомагає підвищити ефективність SOC і зменшити ризики для організації.

На практиці центр оперативного управління інформаційною безпекою в своїй основі містить 3 компонента – технології, що відповідають за оперативне виявлення та реагування на події та інциденти в системі, процеси, що представляють собою структуровані, налагоджені та відпрацьовані схеми, методи та процедури моніторингу, аудиту та реагування на події та інциденти в системі, а також люди, що є кваліфікованим, навченим та компетентним персоналом, та до складу яких входить група реагування, що працює в режимі 24x7

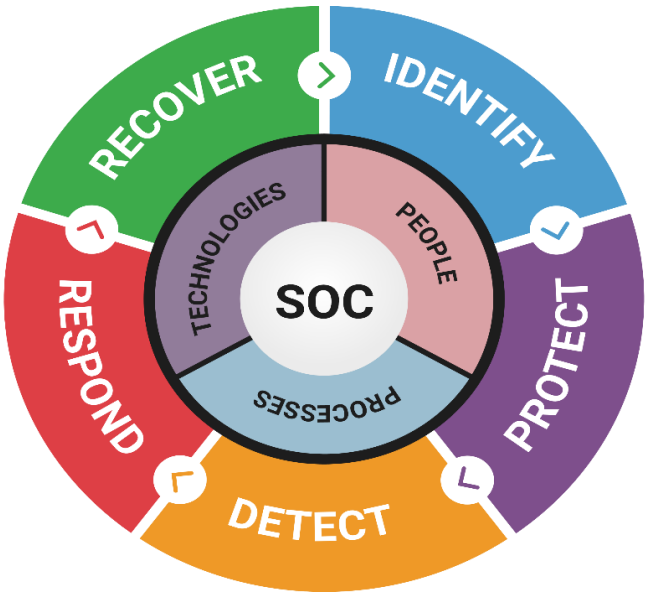


Рис.1. Процеси та ресурси центру кіберзахисту

Завдання Security Operation Centre

- ***Виконувати моніторинг, шукати й аналізувати вторгнення в режимі реального часу.***
- ***Запобігати кіберзагрозам, діючи на випередження: безперервно сканувати комп'ютерні мережі на вразливості та аналізувати інциденти безпеки.***
- ***Швидко реагувати на підтверджені інциденти та унеможливлювати помилкові спрацьовування.***
- ***Формувати звіти про стан безпеки, кіберінциденти і патерни поведінки противника.***
- ***Найбільш трудомістке в роботі SOC - постійно аналізувати великі обсяги даних. Центр забезпечення безпеки збирає, зберігає та аналізує від десятків до сотень мільйонів подій безпеки щодня. Не забуваємо, що все це контролюють експерти: вони включаються в роботу, коли потрібно вирішити, що робити зі знайденою загрозою.***

Перелік посилань:

1. Побудова та аутсорсинг Оперативного Центру Кібербезпеки URL: https://my-itspecialist.com/products/soc (дата звернення: 25.10.2023).
2. What is a Security Operations Center URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/ (дата звернення: 25.10.2023).

Якименко Юрій Михайлович
викладач, доцент кфедри УІКБ, ННІЗІ ДУТ, Київ, Україна

НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Стрімке впровадження інформаційних, комп'ютерних технологій у всі сфери життєдіяльності суспільства та розвиток економіки актуалізує питання визначення обґрунтованих та ефективних шляхів забезпечення інформаційної безпеки. Інформаційна безпека має першорядне значення у зв'язку із значним поширенням атак, яким постійно піддаються як окремі мережі підприємств, так і національні мережі в цілому. Перед керівниками організацій гостро постає проблема втілення термінових заходів щодо захисту своїх активів, оскільки вони, у більшості випадків, не забезпечені навіть базовими механізмами захисту і є нестача професіоналів, здатних їх сформувати, впровадити й експлуатувати. Розглядаються і пропонуються основні підходи підвищення ефективності забезпечення інформаційної безпеки в напрямах - правові, організаційні і технічні заходи та засоби захисту інформації.

Ключові слова: інформаційна безпека, організаційні заходи, технічні заходи, засоби, захист інформації, забезпечення.

Потреби забезпечення інформаційної безпеки (ІБ) формуються під впливом цілої множини факторів: об'єктивних і суб'єктивних, внутрішніх і зовнішніх, прогнозованих і непередбачених тощо. У концентрованій формі вони можуть виступати як деструктивні, що негативно впливають на безпеку. В основі організації, планування й здійснення практичних дій щодо забезпечення ІБ є аналіз концепції загрози, оцінка характеру реальних і потенційних внутрішніх/зовнішніх небезпек і загроз, кризових ситуацій, а також інших несприятливих факторів, які спрямовані до інформації і інформаційних ресурсів будь-якої організації. На практиці основні підходи до захисту інформації і взагалі до забезпечення ІБ здійснюють за трьома основними напрямками: **правовий, організаційний і технічний захист** [1,3].

До **технічних заходів** можна віднести захист від несанкціонованого доступу до комп'ютерних систем шляхом використання спеціальних паролів, шифрування файлів, резервування особливо важливих її підсистем, організацію обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих елементів, контроль електромагнітного й акустичного стану простору, виявлення й пригнічення технічних каналів витоку інформації, монтаж обладнання виявлення й гасіння пожежі, обладнання виявлення води, застосування конструктивних заходів захисту від розкрадань, саботажу або диверсій, установку резервних систем електроживлення; оснащення приміщень замками, установку сигналізацій тощо. Ядром інженерно-технічного напряму є програмно-апаратні засоби захисту інформації. До апаратних засобів відносяться механічні, електромеханічні, електронні, оптичні, лазерні, радіо - і радіотехнічні, радіолокаційні та інші пристрої, системи та споруди, призначені для забезпечення безпеки і захисту інформації. Під програмним забезпеченням безпеки інформації розуміється сукупність спеціальних програм, що реалізують функції захисту інформації та режиму функціонування.

До **організаційних заходів** належать формування політики безпеки організації; охорона об'єктів, які підлягають захисту; ретельний підбір

спеціалістів на відповідні посади і покладання відповідальності на них; наявність плану відновлення працездатності об’єктів, вибір місця розташування об’єкта тощо. На думку фахівців, організаційні заходи відіграють велику роль в створенні надійного механізму захисту інформації, так як можливості несанкціонованого використання конфіденційних відомостей в значній мірі обумовлені не технічними аспектами, а зловмисними діями, недбальством, недбалістю і халатністю користувачів або персоналу захисту. До організаційних заходів належать:

- заходи, здійснювані при проектуванні, будівництві та обладнанні службових і виробничих будівель і приміщень;
- заходи, здійснювані при підборі персоналу;
- організація та підтримка надійного пропускного режиму, охорони приміщень і території, контролю за відвідувачами;
- організація зберігання і використання документів та носіїв конфіденційної інформації;
- організація захисту інформації;
- організація регулярного навчання співробітників.

Одним з основних компонентів організаційного забезпечення ІБ організації є Служба інформаційної безпеки (СІБ). СІБ є органом управління системою захисту інформації.

До **правових заходів** слід віднести розробку нормативних документів, що встановлюють відповідальність за комп’ютерні злочини й злочини в сфері технічного захисту інформації, захисту авторських прав і інше - відповідно до вимог карного й цивільного законодавств, а також судочинства. Правовий рівень захисту інформації передбачає також формування сукупності законодавчих актів, нормативно-правових документів, положень, інструкцій, посібників, вимоги яких є обов'язковими в рамках сфери їх діяльності в системі захисту інформації [2]. Основними законодавчими актами, що регулюють питання інформаційної безпеки організацій, є: Закон України "Про державну таємницю", Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» і Закон України "Про інформацію".

Сформована сукупність інженерно-технічних, організаційних та правових заходів відображається в політиці інформаційної безпеки. Політика безпеки повинна визначати системи захисту інформації і управління ІБ у вигляді сукупності правових норм, організаційних (правових) заходів, комплексу програмно-технічних засобів і процедурних рішень, спрямованих на протидію загрозам безпеці інформації з метою виключення або мінімізації можливих наслідків прояву інформаційних впливів.

Після прийняття того чи іншого варіанту політики ІБ необхідно оцінити рівень безпеки інформаційної системи організації. Оцінка захищеності на практиці проводиться за сукупністю показників, основними з яких є вартість, ефективність, реалізація. Завдання оцінки варіантів побудови системи захисту інформації досить складна, що вимагає залучення сучасних математичних методів багатопараметричної оцінки ефективності, до них відносяться: метод

аналізу ієрархій, експертні методи, метод послідовних поступок і інші [3].

Як **основні види засобів захисту інформації** розглядають:

Засоби фізичного захисту, що включають системи розмежування доступу, засоби захисту мережевої системи, засоби ідентифікації об'єктів, систем електроживлення, засоби архівації, дискові масиви, системи пригнічення побічних електромагнітних випромінювань, акустичних каналів витоку інформації тощо.

Програмні засоби захисту, у тому числі антивірусні програми, криптографічні засоби захисту інформації, системи розмежування повноважень, програмні засоби контролю доступу.

Адміністративні міри захисту включають контроль доступу в приміщення, розробку стратегії безпеки організації і планів дій у надзвичайних ситуаціях тощо.

Що стосується підходів до реалізації захисних заходів щодо забезпечення ІБ, то склалася трьох стадійна розробка таких заходів:

-вироблення вимог до забезпечення ІБ,

-визначення способів захисту від загроз ІБ,

-визначення функцій, процедур і засобів безпеки, що реалізуються у вигляді механізмів захисту.

Реалізація вищеперелічених заходів, що забезпечують безпеку інформації і інформаційних ресурсів, істотно підвищує ефективність всього процесу забезпечення ІБ в організації.

Перелік посилань:

1.Телекомунікаційні системи та мережі. Том 1. Структура й основні функції.- URL: https://www.znanius.com/3849.html.

2. Кавун С. В. Інформаційна безпека: підручник / С. В. Кавун, , В.В. Носов, О.В. Мажай. . - Харків : Вид. ХНЕУ, 2009. - 352 с. - URL: http://www.repository.hneu.edu.ua/jspui/handle/123456789/3068

3.Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с. URL: https://dut.edu.ua/uploads/l_2230_88161692.pdf.

Якубович Ігор Віталійович
Студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

РОЛЬ КІБЕРБЕЗПЕКИ В СУЧАСНОМУ БІЗНЕСІ

Тема "Роль кібербезпеки у сучасному бізнесі" розглядає важливість забезпечення кібербезпеки для сучасних підприємств і бізнесів, відзначаючи, що кібербезпека стала невід'ємною складовою успішної діяльності в умовах росту кіберзагроз та цифрової трансформації. Теза обговорює необхідність інвестування в заходи кібербезпеки, основні аспекти захисту даних та інфраструктури, а також відзначає важливість підготовки персоналу та розробки стратегії реагування на кіберінциденти.

Сучасний бізнес не може існувати без ефективної кібербезпеки, яка є невід'ємною частиною його діяльності. Кіберзагрози постійно еволюціонують і стають все більш вишуканими, завдаючи серйозних збитків компаніям та їх

клієнтам. У цьому контексті, інвестування в кібербезпеку стає обов'язковим завданням для бізнесу, оскільки недостатні заходи можуть призвести до великих фінансових втрат, втрати довіри клієнтів і навіть припинення діяльності компанії.

Перше завдання бізнесу в сфері кібербезпеки полягає в розумінні актуальних загроз і визначенні власних потреб у цій області. Зловмисники використовують різні методи, такі як фішинг, віруси, атаки на службові мережі та інші. Тому необхідно регулярно оцінювати ризики та слабкі місця в інфраструктурі компанії та розробляти стратегію забезпечення кібербезпеки.

Захист важливих даних та інформації про клієнтів є пріоритетом для бізнесу. Шляхом зашифрування даних, використанням механізмів аутентифікації та регулярним резервним копіюванням, компанії можуть мінімізувати ризики втрати конфіденційної інформації. Паралельно з цим, важливо вчасно виявляти та реагувати на можливі порушення безпеки, що вимагає наявності системи моніторингу та систем для виявлення вторгнень.

Для підвищення кібербезпеки, бізнес повинен інвестувати в навчання персоналу. Всі співробітники повинні бути обізнані з основними принципами кібербезпеки, вміти визначати підозрілу активність та повідомляти про неї. Організації також можуть використовувати методи тестування на практиці, які допомагають перевірити рівень обізнаності та навичок персоналу.

Бізнес повинен дбати про забезпечення доступу до важливої інформації лише авторизованим особам. Для цього використовуються системи контролю доступу та аутентифікації. Додаткові рівні захисту, такі як багаторівнева аутентифікація, допомагають запобігти несанкціонованому доступу.

Зберігання даних в безпечних місцях, регулярне оновлення програм та операційних систем, вжиття заходів для захисту мережі та інфраструктури — це лише декілька засобів, які бізнес може використовувати для забезпечення кібербезпеки.

Бізнес повинен також бути готовим до відповіді на можливі кібератаки. Розробка плану реагування на інциденти та проведення тренувань для персоналу допомагають зменшити можливі наслідки подібних ситуацій.

Загалом, кібербезпека є необхідним елементом сучасного бізнесу. Недостатній рівень захисту може призвести до серйозних фінансових втрат і втрати довіри клієнтів. Тому інвестування в кібербезпеку повинно бути пріоритетом для будь-якої компанії, яка цінує свою стійкість та довіру споживачів.

Бізнес також повинен враховувати факт, що кіберзагрози постійно змінюються. Це означає, що стратегії та технології кібербезпеки повинні постійно оновлюватися та адаптуватися до нових умов.

Інвестиції в кібербезпеку також можуть сприяти покращенню репутації компанії в очах клієнтів і партнерів. Захист конфіденційної інформації і персональних даних свідчить про відповідальний підхід до бізнесу і покликаний зберегти довіру клієнтів.

У світі, де цифрова трансформація стає невід'ємною частиною практично

будь-якої галузі, кібербезпека стає справжньою ключем до успіху. Втрати від кібератак можуть бути надзвичайно великими, але правильний підхід до кібербезпеки дозволить бізнесу зменшити ризики та забезпечити стійкість у цифровому середовищі.

Узагальнюючи, бізнес повинен розглядати кібербезпеку як стратегічну ініціативу, яка вимагає системного підходу, інвестицій та зобов'язання до постійного вдосконалення. Кібербезпека має стати не лише технічним завданням, але і частиною корпоративної культури та відповідальності перед клієнтами та партнерами. Тільки в такий спосіб бізнес зможе залишатися конкурентоспроможним і надійним в цифровому світі.

Перелік посилань:

1. Кібербезпека бізнесу це не лише технічні заходи URL: https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/
2. What is Cybersecurity and Its Importance to Business URL: https://www.nu.edu/blog/what-is-cybersecurity/#:~:text=The%20Growing%20Importance%20of%20Cybersecurity%20for%20Businesses&text=One%20of%20the%20primary%20reasons,records%2C%20and%20proprietary%20intellectual%20property
3. Why Cybersecurity Is So Important For Business URL: https://elearningindustry.com/why-cybersecurity-is-so-important-for-business

Яловик Денис Володимирович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Технічні системи захисту інформації в сучасному цифровому світі є критично важливими для забезпечення конфіденційності, цілісності та доступності інформації, а їхній розвиток та вдосконалення стають нагальним завданням у контексті зростаючих кіберзагроз.

Захист від кібератак: Технічні системи захисту інформації, такі як брандмауери, інтрузійні детектори та антивірусне програмне забезпечення, грають важливу роль у захисті комп'ютерних систем від кібератак. Наприклад, "FireEye" - це відома компанія, що надає послуги з виявлення та реагування на кіберзагрози.

Шифрування даних: Технології шифрування, які застосовуються в багатьох системах зберігання та обміну даними, забезпечують конфіденційність інформації. Наприклад, "End-to-End" шифрування в месенджерах, таких як WhatsApp і Signal, дозволяє користувачам спілкуватися без можливості прослуховування повідомлень третіми особами.

Захист мережевих інфраструктур: Системи захисту мережевих інфраструктур, які виявляють та запобігають атакам, можуть захистити важливі організаційні ресурси від порушення. Продукти, такі як "Cisco ASA" та "Palo Alto Networks," допомагають управляти мережевою безпекою.

Захист вбудованих систем: У сучасному світі вбудовані системи захисту інформації використовуються в автономних автомобілях, медичних пристроях та інших сферах. Прикладом є "Tesla Autopilot," який використовує комплексну

систему захисту для забезпечення безпеки під час автопілотування.

Перелік посилань:
1. "End-to-End Encryption in Messaging Apps" - https://www.eff.org/deeplinks/2018/03/end-end-encryption-messaging-apps
2. "Cisco ASA" - https://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa/index.html

Ясманович Дмитро Євгенійович
Державний університет інформаційно-комунікаційних технологій

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В BLOCKCHAIN-ТЕХНОЛОГІЯХ

Анотація

У цій статті розглядаються актуальні проблеми кібербезпеки в контексті blockchain-технологій. Розглянуто важливі аспекти, такі як приватність даних, смарт-контракти, атаки на мережу, а також недоліки самої технології. Зрозуміти ці проблеми та навчитися захищати себе та ваші цифрові активи від них стає надзвичайно важливим у сучасному світі кібербезпеки.

Актуальні проблеми кібербезпеки в Blockchain-технологіях

Blockchain-технологія обіцяє революцію в багатьох галузях, включаючи фінанси, логістику, медицину та багато інших. Вона вже дала поштовх розвитку криптовалют, таких як Bitcoin та Ethereum, і стала важливим інструментом для забезпечення децентралізованих угод і зберігання даних. Однак разом з усією своєю обіцянкою blockchain також приносить ряд проблем і загроз, які стосуються кібербезпеки. Давайте глибше розглянемо ці актуальні проблеми та можливі шляхи їх вирішення.

1. Приватність даних та анонімність

Однією з головних переваг blockchain є його транспарентність. Усі транзакції записуються в блокчейні і стають загальнодоступними. Проте ця транспарентність може стати вадою, коли мова йде про захист особистих даних. Всі угоди і транзакції можуть бути відстежені, що створює проблеми з приватністю та конфіденційністю користувачів. Деякі blockchain-мережі розробляють рішення для забезпечення конфіденційних транзакцій та шифрування даних, але ці проблеми ще потребують подальшого вдосконалення.

2. Смарт-контракти та програмні помилки

Смарт-контракти, які автоматизують угоди на blockchain, стали однією з найважливіших функцій цієї технології. Однак вони також вразливі на програмні помилки. Навіть найдрібніша помилка у смарт-контракті може призвести до втрати великих сум грошей або використання мережі для злочинних цілей. Програмісти повинні бути особливо уважними при створенні та аудиті смарт-контрактів. Компанії, що використовують blockchain, також повинні вдосконалювати механізми перевірки контрактів та забезпечення їх безпеки.

3. Атаки на мережу

Blockchain мережі стали ціллю для кібератак. Атаки 51% і атаки поділу мережі можуть вразити функціонування мережі та навіть забезпечити можливість зміни чи скасування транзакцій. Для захисту від таких атак важливо мати велику та активну спільноту користувачів, яка готова відстоювати цінності blockchain. Багато мереж використовують різні механізми консенсусу, такі як доказ роботи (Proof of Work) та доказ спільноти (Proof of Stake), для запобігання атакам.

4. Соціальна інженерія і шахрайство

Соціальна інженерія є однією з найпоширеніших загроз кібербезпеці в будь-якій галузі, включаючи blockchain. Зловмисники можуть використовувати соціальні методи для отримання доступу до особистих ключів або виконання фішингових атак. Обережність і освіченість користувачів є ключовими для уникнення таких загроз. Важливо наголосити, що захист власного ключа і заходи безпеки повинні бути на першому плані для кожного користувача blockchain.

Висновок

Blockchain-технологія відкриває перед нами безліч можливостей, проте вона також потребує ретельного вивчення і заходів забезпечення кібербезпеки. Щоб впевнено використовувати blockchain для зберігання важливої інформації і здійснення фінансових операцій, необхідно розуміти ці проблеми і вживати заходи їх вирішення. Безпека завжди має бути на першому плані, навіть у світі криптовалют і децентралізованих систем. Лише з розумінням цих проблем і спільними зусиллями користувачів і розробників ми можемо забезпечити надійну кібербезпеку в blockchain-технологіях і використовувати їх повний потенціал для створення безпечних інноваційних рішень.

Таким чином, при розвитку та використанні blockchain-технологій, ми маємо бути уважними до цих проблем і постійно вдосконалювати методи захисту для забезпечення безпеки цієї важливої технології.

Джерела:

1. https://www.analyticsinsight.net/top-10-blockchain-security-concerns-for-2023/#:~:text=The%20risk%20of%20cyberattacks%2C%20the,security%20issues%20that%20blockchain%20presents.

Марченко Віталій Вікторович
д.ф.,доцент кафедри ІКБ, ННІЗІ ДУІКТ, Київ, Україна
Коліда Володимир Петрович
аспірант групи АІКБ-11, кафедри ІКБ, ННІЗІ ДУІКТ, Київ, Україна

МЕТОД ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В КОРПОРАТИВНІЙ МЕРЕЖІ НА ОСНОВІ МЕТОДІВ МАШИННОГО НАВЧАННЯ В РЕАЛЬНОМУ ЧАСІ

Корпоративна мережа – це комунікаційна система, яка належить чи керується одною організацією відповідно до правил цієї організації, головним призначенням якої є підтримка роботи підприємства, що володіє даною мережею. Сучасні технологічні вирішення, які забезпечують зв'язок у корпоративних мережах, також відкривають шлях для нових видів кіберзагроз. Відсутність належних заходів безпеки може призвести до серйозних втрат даних та репутаційних втрат для організацій. У цьому контексті методи машинного навчання виявляються ключовими в ідентифікації та запобіганні шкідливому програмному забезпеченню (ШПЗ).

Шкідливе програмне забезпечення (ШПЗ) стало однією з найбільших загроз кібербезпеці в сучасному світі, впливаючи на мільйони користувачів та підприємств щодня. За даними Packetlabs тільки за першу половину 2022 року було запущено 2.8 мільярди атак зловмисним програмним забезпеченням, більше половини ШПЗ складають троянські програми а кожного дня створюється приблизно 300 тисяч нових шкідливих програм[2].

Ідентифікація зловмисних доменів і IP-адрес у режимі реального часу має важливе значення для запобігання фішингу, програм-вимагачів, троянів та інших кіберзагроз. Традиційний підхід – покладання на канали репутації домену для категоризації та ідентифікації зловмисних доменів є занадто неточним, оскільки алгоритми генерації доменів (DGA) дозволяють зловмисникам швидко створювати нові домени, які не мають репутації[1]. У той же час користувачі продовжують переходити на шкідливі домени, що імітують відомі бренди (такі як microsoftt[dot]com або amazonlink[dot]online), відсутність репутації яких також робить ненадійним виявлення лише за допомогою каналів репутації.

Алгоритми глибокого навчання в реальному часі вирішують обидві проблеми. Алгоритми запобігають доступу до доменів, зареєстрованих DGA , ідентифікуючи ці нові домени, які рідко відвідуються користувачами, і мають шаблони букв, загальні для DGA. Вони блокують кіберсквотінг , шукаючи домени з буквами, схожими на відомі бренди. А алгоритми запобігають імітації бренду , перевіряючи частини веб-сторінки, такі як іконку, зображення та текст.

Метод виявлення шкідливого програмного забезпечення в реальному часі на основі машинного навчання має ряд переваг перед традиційними методами. Він може бути більш ефективними в виявленні нових видів шкідливого програмного забезпечення, оскільки він не покладається на наявність сигнатур шкідливого програмного забезпечення. Крім того, він може бути більш масштабованими, оскільки може працювати з великими обсягами даних. Дані мережевої активності (трафік, протоколи, порти), процеси, поведінка

програмного забезпечення аналізуються в реальному часі і ці дані використовуються для навчання моделі, яка може розпізнати поведінку ШПЗ.

Метод виявлення шкідливого програмного забезпечення в корпоративній мережі на основі машинного навчання в реальному часі представляє собою складну систему, яка використовує ряд технологій для надійного захисту мережі від атак та загроз. Починаючи зі збору даних про мережевий трафік та інші системні активності, цей метод включає в себе аналіз цих даних, використання алгоритмів машинного навчання для виявлення незвичайних паттернів та аномалій, і надання реакції на виявлені загрози у реальному часі.

Важливо відзначити, що цей підхід використовує алгоритми класифікації для розпізнавання зловмисних активностей та аналізу аномалій для виявлення незвичайних зразків трафіку в мережі. Система також повинна вміти відрізняти нормальну активність від потенційно шкідливої, використовуючи різноманітні методи аналізу в режимі реального часу без необхідності зберігання всіх даних. Також важливо мати систему сповіщень, яка негайно інформує адміністраторів про виявлені загрози, і можливість автоматично реагувати на ці загрози, забезпечуючи негайне втручання та захист від можливих атак. Цей метод дозволяє компаніям забезпечити високий рівень кібербезпеки та захистити свої дані та ресурси в реальному часі від широкого спектру загроз. Цей підхід дозволяє виявляти ШПЗ в реальному часі, забезпечуючи надійний рівень безпеки корпоративної мережі.

Перелік посилань:

1. Cato Networks Revolutionizes Network Security with Real-Time, Machine Learning-Powered Protection | Cato Networks URL: https://www.catonetworks.com/news/cato-revolutionizes-network-security-with-real-time-machine-learning-powered-protection/

2. 239 Cybersecurity Statistics (2023) | Packetlabs URL: *https://www.packetlabs.net/posts/239-cybersecurity-statistics-2023/*

Коврига Максим Віталійович
студент групи УБД-41, ННІЗІ ДУІКТ, Київ, Україна

ПОБУДОВА ТИПОВОЇ МОДЕЛІ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ БАНКУ

З стрімким розвитком інформаційних технологій, та активному використанні комп'ютерних систем майже у всіх сферах людської діяльності, стрімко зростає й цінність генерованої, в процесі експлуатації цих систем, інформації. Тому на сьогодні, питання безпечного збереження інформаційних ресурсів є одним з найактуальніших. Одним з головних чинників побудови ефективних систем безпеки є аналіз можливих ризиків пов'язаних з інформаційною безпекою. Однак, за умови що в різних сферах діяльності чинниками утворення ризику можуть слугувати багато факторів, постає необхідність у використанні ефективних методик аналізу, охоплюючи великий об'єм вхідних даних.

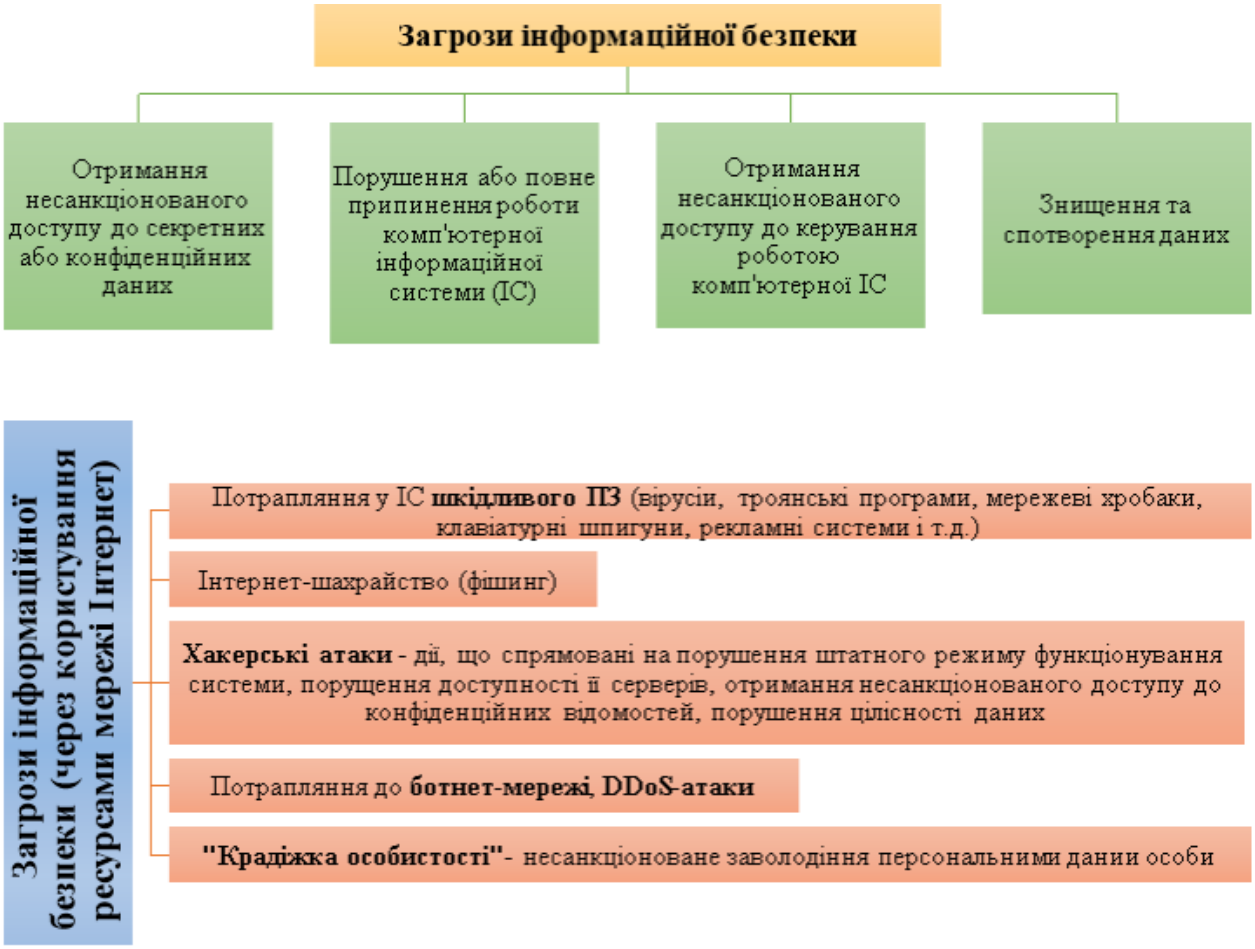


Рис.1. Загрози інформаційної безпеки

Перелік посилань:

1. Вступ теми URL: https://ela.kpi.ua/bitstream/123456789/57065/1/Synytsin_Bakalavr.pdf (дата звернення: 30.10.2023) [1 с8]
2. Загрози інформаційній безпеці URL: https://naurok.com.ua/informaciyna-bezpeka-zagrozi-pri-roboti-v-interneti-i-h-uniknennya-116853.html (дата звернення: 30.10.2023)

Романчук Владислав
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАХИСТУ WEB-ДОДАТКІВ ЗА ДОПОМОГОЮ WAF

Технологія захисту веб-додатків з використанням WAF (Web Application Firewall) є важливою складовою сучасної кібербезпеки. WAF допомагає виявляти та блокувати різноманітні атаки, такі як SQL-ін'єкція та кросс-сайтовий скриптінг, перед тим як вони досягнуть веб-додатку. Ця технологія допомагає підвищити безпеку, забезпечити високу доступність та підвищити репутацію бренду. WAF стає необхідним інструментом для захисту веб-сайтів і додатків у цифровому середовищі.

В сучасному світі, де інтернет відіграє ключову роль у практично всіх аспектах життя і бізнесу, безпека веб-додатків стає надзвичайно важливою. Зловмисники намагаються використовувати різноманітні атаки, щоб отримати доступ до конфіденційної інформації, завдати шкоди бізнесу та порушити роботу веб-сайтів. Для захисту веб-додатків і їх користувачів використовуються різні методи, але однією з найефективніших технологій є веб-протокол захисту (Web Application Firewall, WAF).

Web Application Firewall (WAF) - це технологічний захисний інструмент, призначений для виявлення та блокування потенційно небезпечних HTTP-запитів до веб-додатків. WAF використовує різні методи аналізу для досягнення цієї мети:

1. Сигнатурний аналіз: WAF перевіряє вхідні запити на відповідність відомим атакам та шаблонам атак, використовуючи підписи. Якщо відома атака виявляється, запит блокується.

2. Аналіз вмісту: WAF аналізує вміст HTTP-запитів та відповідей на наявність атак, перевіряючи вміст на наявність підозрілих або заборонених ключових слів.

3. Інтелектуальний аналіз трафіку: WAF використовує алгоритми машинного навчання та евристичні методи для виявлення аномального трафіку. Це дозволяє виявляти нові атаки, які не відомі в попередніх сигнатурах.

Основна перевага використання WAF полягає в тому, що він фільтрує трафік перед тим, як він дістанеться до веб-додатку. Це дозволяє блокувати атаки ще до того, як вони зможуть використовувати вразливості в додатку. Такий попередній захист дозволяє мінімізувати ризики для безпеки і захистити веб-додаток від різноманітних атак, таких як SQL-ін'єкція, кросс-сайтовий скриптінг (XSS), атаки з використанням файлових завантажень і багато інших, забезпечуючи високий рівень безпеки для користувачів та даних.WAF використовується як великими корпораціями, так і малими підприємствами, а також індивідуальними розробниками для захисту їх веб-додатків та інформації. Ось деякі з переваг використання WAF:

1. Захист від різноманітних атак: WAF виявляє та блокує широкий спектр атак, включаючи атаки на основі векторів введення, виведення та аутентифікації.

2. Мінімізація вразливостей: Використання WAF допомагає виявляти та усувати вразливості в коді веб-додатку, що покращує загальну безпеку.

3. Забезпечення високої доступності: WAF може фільтрувати трафік та виключати атаки, що допомагає уникнути перебоїв у роботі веб-сайту та забезпечити надійну доступність.

4. Підвищення репутації бренду: Захищений веб-сайт створює довіру серед користувачів, оскільки їм відомо, що їхні дані та інформація захищені.

5. Законодавчий вимоги: Деякі регулятори вимагають від підприємств використовувати захисні технології, включаючи WAF, для дотримання стандартів безпеки даних.

У світі, де загрози для веб-додатків надто різноманітні та небезпечні,

використання WAF стає надзвичайно важливим елементом захисту. Ця технологія допомагає не лише захистити веб-додаток від потенційних загроз, але й забезпечує спокій

Перелік посилань:
1. What is a WAF? | Web Application Firewall explained URL https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/ (дата звернення: 01.11.2023).
2. Як Web Application Firewall захищає вебдодатки від хакерських атак? URL: https://hub.kyivstar.ua/articles/yak-web-application-firewall-zahyshhaye-vebdodatky-vid-hakerskyh-atak (дата звернення: 01.11.2023).

Кучма Ольга Миколаївна,
аспірант, Державний Податковий Університет, м. Ірпінь, Україна
Котух Євген Володимирович,
д. н. з держ управління, доцент, професор кафедри кримінальних розслідувань,
Державний Податковий Університет, м. Ірпінь, Україна

КОНЦЕПЦІЯ ЖИТТЕВОГО ЦИКЛУ РИЗИКУ В ЗАБЕЗПЕЧЕННІ ЗАХОДІВ ПУБЛІЧНОГО ІТ-АУДИТУ

Публічний ІТ аудит стає важливим заходом забезпечення ефективності використання публічних коштів проектів інформатизації. Безпека та ефективність державних інформаційних ресурсів, об’єктів критичної інфраструктури та об’єктів критичної інформаційної інфраструктури є основними пріоритетами в досягненні сформульованих стратегічних цілей Одним з суттєвих факторів ефективності та якості проведення ИТ аудиту є необхідність його методологічного забезпечення на високому рівні. Саме профілювання ризиків, визначення, гнучке управління та впровадження ризик-правил в програмне забезпечення як інструмента підтримки заходів здійснення аудиту дасть можливість впровадити життєвій цикл профілів ризику та забезпечити актуальними даними, щодо ризиків в процесі ИТ аудиту проектів інформатизації.

15 вересня 2023 року Уряд схвалив проект Закону про Державний бюджет України на 2024 рік. Цифрова трансформація пріоритетних галузей та сфер суспільного життя отримала 2,5 млрд грн (+2,1 млрд грн до 2023). У бюджеті вперше враховано інноваційні проекти для забезпечення сектору безпеки і оборони з бюджетом 1,5 млрд грн, застосунок “Мрія” - доступ до знань з будь-якого куточку світу отримає 142 млн грн [1].

ІТ-системи та процеси є критично важливими для успішного функціонування держави в еру цифрової трансформації. Тому забезпечення їхньої кібербезпеки та кіберготовності є одним із пріоритетних завдань. Однією зі стратегічних цілей в Стратегії кібербезпеки України, яка затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021, визначено потребу розбудови кіберготовності та системи кіберзахисту [2] наступним шляхом:

- запровадження та реалізація чітких та зрозумілих для всіх зацікавлених сторін заходів щодо національної кіберготовності в інтересах забезпечення економічного добробуту та захисту прав і свобод кожного громадянина України.
- посилення кіберготовності, що полягатиме у здатності всіх зацікавлених сторін, насамперед суб'єктів сектору безпеки і оборони, своєчасно й ефективно

реагувати на кібератаки, забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявляти та усувати передумови їх виникнення, забезпечивши тим самим кіберстійкість, передусім об'єктів критичної інформаційної інфраструктури (далі – ОКІІ).

- створення національної системи управління інцидентами.

Безпека та ефективність державних інформаційних ресурсів (ДІР), об’єктів критичної інфраструктури (ОКІ) та ОКІІ є основними пріоритетами в досягненні сформульованих стратегічних цілей. Одним із інструментів для забезпечення безпеки та ефективності ІТ-систем та процесів є аудит [3]. ІТ аудит – це перевірка ІТ-систем та процесів з метою виявлення та усунення ризиків, які можуть призвести до фінансових втрат, порушення конфіденційності та цілісності або інших негативних наслідків. Методологічне забезпечення проведення ІТ аудиту є важливим фактором його якості та ефективності [4].

Для проведення ефективного ІТ аудиту необхідно розуміти життєвий цикл ризику. Життєвий цикл ризику – це процес, який включає в себе етапи: ідентифікації, оцінки, управління та моніторинг. Профілювання ризиків є одним з ключових елементів методологічного забезпечення ІТ аудиту. Профіль ризику – це сукупність відомостей про області, індикатори ризику та заходи контролю, необхідні для запобігання або мінімізації ризиків. Постійно змінні людські, технологічні та зовнішні фактори приводять до змін методологічного забезпечення ідентифікації та профілювання ризиків, реалізації функціонала керування ризиками в програмному забезпеченні. Це обумовлює необхідність концептуалізації життєвого циклу ризику в забезпеченні заходів публічного ІТ аудиту. Автори пропонують наступний підхід до керування профілем ризику (див. рис. 1).

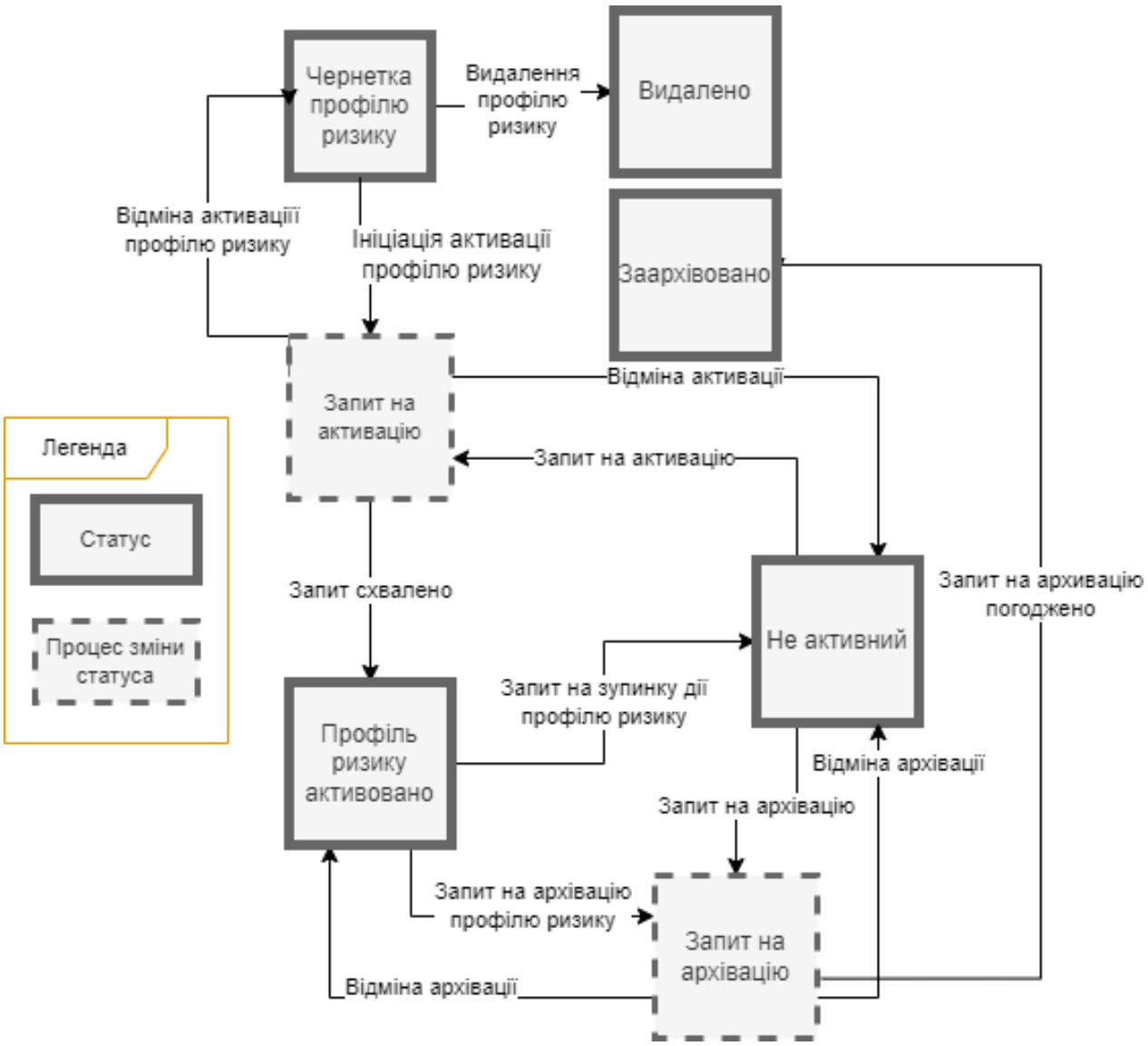


Рис. 1 – Життєвий цикл профілю ризику в інформаційній системі ризик-менеджменту

Життєвий цикл профілю ризику в інформаційний системі з функціоналом ризик-менеджменту можна розділити на основні етапи з відповідними статусами:

- створення профілю (Статус: Чернетка профілю ризика) – початковий етап циклу, що створює профіль ризику та всі артефакти (ризик-правила, індикатори, передумови, заходи контролю та моніторингу);
- активація профілю (Статус: Профіль ризику активовано) – етап циклу, що активує профіль ризику. Система в цьому статусі оперує артефактами ризику в завданні ідентифікації ризиків серед доступних системі даних;
- деактивація профілю (Статус: не активний) – етап циклу, що дозволяє призупинити активність профілю ризику та не враховувати ризик-правила цього профілю в ідентифікації ризиків;
- видалення профілю (Статус: видалено) – етап циклу, що дозволяє видалити чернетку профілю ризику до його активації;

- архівація профілю (Статус: заархівовано) – етап циклу, що дозволяє заархівувати профіль ризику та не використовувати його в актуальній виборці даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Урядовий портал. Єдиний веб-портал органів виконавчої влади України [Електронний ресурс] – Режим доступу. https://www.kmu.gov.ua/news/uriad-skhvalyv-proekt-derzhavnoho-biudzhetu-na-2024-rik-vid-biudzhetu-viiny-do-ekonomiky-peremohy
2. Стратегія кібербезпеки України. [Електронний ресурс]. – Режим доступу. https://zakon.rada.gov.ua/laws/show/447/2021?find=1&text=%D0%BF%D0%BE%D1%81%D0%BB%D1%83#w1_1
3. Пліс Г.В., Котух Є.В., Нехороших Д.М., Халімов Г.З., Кучма О.М. Аудит інформаційної безпеки як необхідна складова управління в державних установах. [Електронний ресурс]. – Режим доступу. http://db.kh.ua/index.php/db/article/view/117
4. Котух Є.В. Кібербезпека у публічному секторі : монографія. Харків : Колегіум, 2021. 271 с.

Москвін Микита Валерійович
студент групи БСДМ-61,
ННІЗІ ДУІКТ, Київ, Україна

КОНТРОЛЬ ДОСТУПУ ДО МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ CISCO IDENTITY SERVICES ENGINE

Кожен користувач корпоративної мережі повинен отримувати відповідні послуги до мережі. Отримати доступ до корпоративної мережі – це завжди була важлива задача для інформаційних технологій. На сьогоднішній день, завдяки сучасним технологіям, таким як Cisco Identity Services Engine (ISE), фахівці з кібербезпеки мають можливість налаштовувати і контролювати доступ до мережі більш ефективно та безпечно.

Cisco Identity Services Engine (ISE) - це інтегрована система для аутентифікації, авторизації та обліку користувачів у корпоративних мережах. Ця технологія дозволяє створювати політики доступу, які визначають, хто, куди і як може підключатися до мережі. Для Cisco ISE є ролі у контролі доступу, які складаються з аутентифікації, авторизації, обліку (рис1.1).

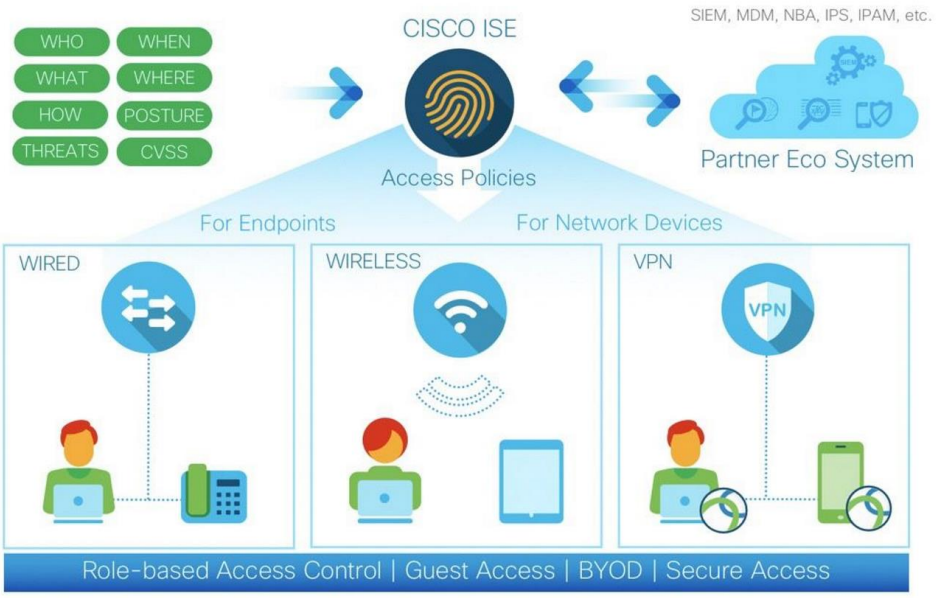


Рис 1. Роль Cisco Identity Services Engine

Роль аутентифікації полягає в тому, що Cisco ISE дозволяє перевіряти легітимність користувачів, вимагаючи від них ідентифікаційні дані, такі як ім'я користувача та пароль.

Роль авторизації полягає в тому, що за допомогою Cisco ISE можна встановлювати права доступу для користувачів, визначаючи, які ресурси та служби вони можуть використовувати.

Роль обліку обліку полягає в тому, що система веде журнали активності користувачів, що допомагає виявляти потенційні загрози та аудитувати дії користувачів.

Основні переваги щодо кібербезнеки, які надаються при використанні технології Cisco Identity Services Engine заключаються в наступному:

Cisco ISE допомагає запобігти несанкціонованому доступу до мережі та захищає від загроз інформаційні активи компанії.

Детектування і реагування на аномалії допомагають вчасно виявляти інциденти та вживати необхідні заходи безпеки.

Масштабованість та інтеграція яку забезпечує Cisco ISE заключається в тому, що вона може бути інтегрованою з іншими системами безпеки та інфраструктурними рішеннями, що робить її відмінним вибором для великих компаній та корпорацій. Cisco Identity Services Engine дозволяє ефективно керувати доступом до мережі навіть в умовах великого обсягу користувачів та пристроїв.

З точки зору адміністрування Cisco ISE надає графічний інтерфейс для налаштування політик доступу, що спрощує процес управління безпекою мережі. Адміністратори можуть легко визначати нові політики, редагувати існуючі та відслідковувати активність користувачів (рис 2).

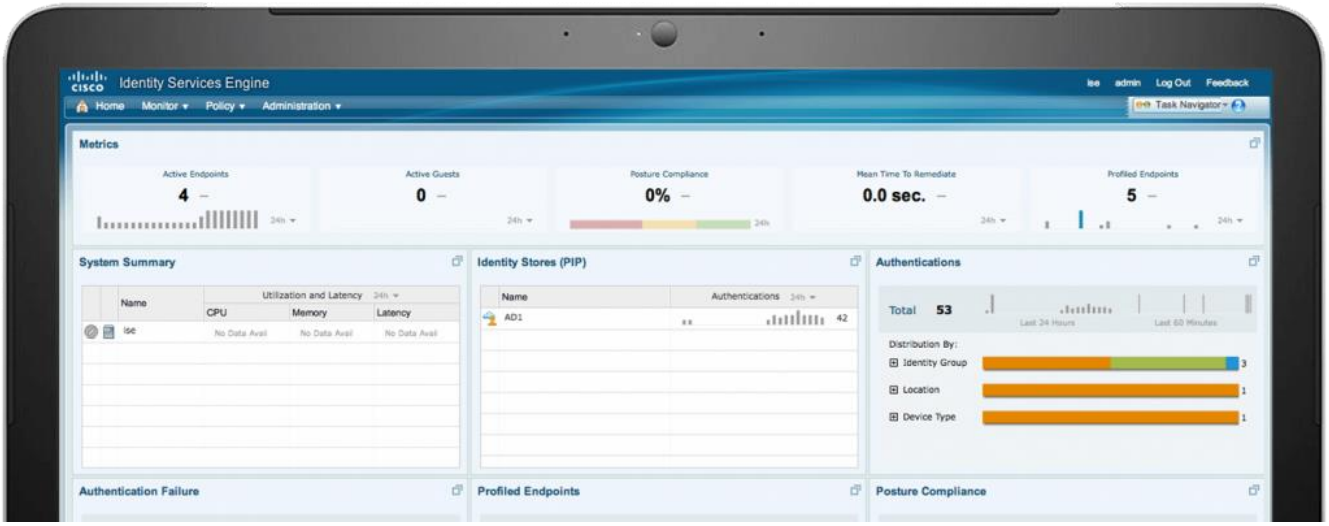


Рис.2. Консоль Cisco Identity Services Engine

Тож підведемо підсумок: Cisco Identity Services Engine є потужним інструментом для контролю доступу до мережі, який сприяє підвищенню безпеки, зручності адміністрування та масштабованості мережевих інфраструктур. Використання цієї технології дозволяє організаціям забезпечити безпеку та ефективність своїх мереж, а також реагувати на сучасні виклики в галузі кібербезпеки.

Перелік посилань
1. Cisco Identity Services Engine UR: https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0/b_ISE_admin_30_overview.html (дата звернення 02.10.2023)
2. Консоль Cisco ISE URL: https://habr.com/ru/companies/tssolution/articles/520222/(дата звернення 03.10.2023)

Платоненко Оксана Едуардівна
студентка групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

Управління привілейованим доступом до інформаційної системи - це важлива складова інформаційної безпеки, яка допомагає забезпечити, що лише вповноважені користувачі отримують доступ до конфіденційної інформації та ресурсів.

Привілеюваний доступ означає отримання повних або розширених прав доступу до системи, даних або ресурсів, який зазвичай надається адміністраторам та іншим важливим користувачам.

Управління привілеєваним доступом полягає в установленні, моніторингу та забезпеченні безпеки цих прав (Рис.1).

Рис.1. Привілейований доступ. Основні принципи

До основних принципів управління привілейованим доступом відноситься:

Мінімізація прав. Це є принцип "найменшого призначення", який передбачає, що користувачам надаються лише ті права, які необхідні для виконання їхніх обов'язків.

Прозорість та відслідковування. Всі дії привілейованих користувачів повинні бути відслідковані та журналюватися для аудиту та аналізу безпеки.

Ревізія та оновлення. Права доступу повинні періодично переглядатися, а також оновлюватися відповідно до змін в обов'язках користувачів.

Ідентифікація та аутентифікація. Перед наданням привілейованого доступу користувачі повинні бути ідентифіковані та аутентифіковані для підтвердження їхньої ідентичності. Двофакторна аутентифікація є важливим засобом підвищення безпеки при вході в систему.

Управління паролями. Паролі повинні бути складними, унікальними та періодично змінюватися. Використання парольних менеджерів може допомогти у безпеці паролів.

Програмне забезпечення для управління доступом. Інструменти, такі як системи керування доступом (IAM), допомагають автоматизувати та спростити процес управління привілейованим доступом. IAM системи дозволяють легко додавати, видаляти та змінювати права доступу користувачів.

Загрози та відповідь на інциденти. Управління привілейованим доступом також включає в себе планування та реагування на інциденти, такі як несанкціонований доступ або компрометація облікових записів.

Таким чином зробимо висновки. Ефективне управління привілейованим доступом є ключовою складовою інформаційної безпеки та допомагає забезпечити захист конфіденційної інформації та ресурсів в інформаційній системі. Дотримання принципів мінімізації прав, аутентифікації та періодичного оновлення прав допомагає зменшити ризики та забезпечити безпеку усієї системи.

Перелік посилань

1. Привілейований доступ. Чому це важливо і як його контролювати URL: https://ko.com.ua/privilejovanij_dostup_chomu_ce_vazhlivo_i_yak_jogo_kontrolyuvati_129976 (дата звернення 02.10.2023)
2. Привілейований доступ Delinea URL: https://channel4it.com/publications/ostann-onovlennya-delinea-server-suite-znizhu-rizik-zagroz-bekdoru-na-serverah.html (дата звернення 03.10.2023)