ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ»

Тези доповідей

25 жовтня
2024

м. Київ

Рекомендовано до друку кафедрою Сиситем та технологій Державного університету інформаційно-комунікаційних технологійй (протокол № 3 від 06.11.2024 р.)

Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 25 жовтня 2024 року). Навчально-науковий інститут кібербезпеки захисту інформації, Державний університет інформаційно-комунікаційних технологій. Київ, 2024. 251 с. Збірник призначений для науковців, викладачів, докторантів, аспірантів і студентів закладів вищої освіти, фахівців з кібербезпеки та захисту інформації, 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

Березовський Кирил Віталійович
Студент групи БСДМ-63 ННІЗІ ДУІКТ, Київ, Україна
Рудомьотова Марія Андріївна
Студент групи БСДМ-63 ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

Захист кінцевих точок є ключовим елементом сучасної кібербезпеки організації, крім кожного пристрою, який підключається до корпоративної мережі, може стати початковою точкою атаки. Отже питання захисту кінцевих точок організації є нагальним питання при створенні системи кіберзахисту.

Технології захисту кінцевих точок (Endpoint Protection Technologies, EPT) включають антивірусні системи, фаєрволи, рішення для захисту від шкідливого ПЗ та інструменти виявлення та реагування на загрози (Endpoint Detection and Response, EDR). Основне прихначення таких технологій – це спостерігання за моніторингом, проведення аналізу поведінки користувачів і пристроїв, автоматизованим реагуванням на інциденти та виявлення підозрілих дій, знижуючи ризики компрометації. Впровадження таких технологій забезпечить багаторівневий захист, зменшуючи вплив кіберзагроз на бізнес-процеси та інфраструктуру організації.

Захист кінцевих точок є одним із окремих елементів забезпечення кібербезпеки в сучасних організаціях. Кінцеві точки (endpoints) — це будь-які пристрої, які взаємодіють з корпоративною мережею: комп’ютери, ноутбуки, смартфони, планшети, сервери та інші IoT-пристрої. Їх роль у функціонуванні організації надзвичайно важлива, оскільки вони є точками доступу до внутрішніх систем організації, даних і додатків, які є конфіденційними. Саме тому кінцеві точки залишаються головною мішенню для кіберзлочинців, особливо в умовах зростання популярності віддаленої роботи.

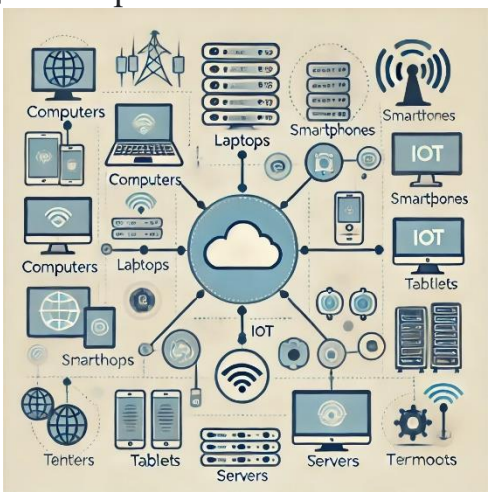


Рис.1. Компоненти кінцевої точки організації

Кінцеві точки є одними з найбільш уразливих елементів організаційної інфраструктури. З використання кінцевої точко користувачі в організації щоденно проводять операційну діяльність, співробітники забезпечують доступ

до важливих корпоративних даних, фінансових звітів і конфіденційної інформації. Якщо кінцева точка скомпрометована, це може призвести до масштабних витоків даних або проникнення в мережу. Тому кінцеві точки змінюють ключову роль у захисті критичної інфраструктури організації, і їх надійна безпека є основою загального кіберзахисту.

У сучасних організаціях використовується безліч останніх точок різного типу, і кожен з них може бути вразливою до атак. Традиційно, кінцеві точки знаходяться під захистом корпоративних мереж і фаєрволів, але з розвитком віддаленої роботи зростає важливість їх індивідуального захисту, особливо в контексті різних загроз.

З розширенням віддаленої роботи кількість атак на кінцеві точки суттєво зросла. За даними статистики, кількість кіберзагроз для віддалених користувачів зросла за перші місяці пандемії COVID-19, коли більшісті компаній перейшли на роботу з дому. тренд зберігається і зараз, що пов1язано з веденням бойових дій в Україні., а для деяких компаній це стало нормою. Однією з причин такого зростання є те, що віддалені працівники часто підключаються до корпоративних ресурсів через незахищені домашні або публічні мережі, що створює додаткові можливості для атаки. Крім того, користувачі можуть використовувати особливі пристрої для доступу до корпоративних систем, які не завжди мають належний рівень захисту. Як результат, кінцеві точки залишаються основними цілями для фішингових атак, атак з використанням шкідливого програмного забезпечення атаки типу «людина посередині» (man-in-the-middle).

Сучасні технології захисту кінцевих точок, орієнтовані на багаторівневий підхід до безпеки, останні атаки на кінцеві точки стають все більш складними.

Отже захист кінцевої точки організації повинен в себе включати наступні технології.

Запобігання загрозам – не дозволяє загрозам проникнути в систему, автоматично перевіряє файли при доступі та виконує цільові перевірки на наявність шкідливих програм у клієнтських системах.

Брандмауер – відстеження передачі даних між комп'ютером, мережевими ресурсами та Інтернетом. Перехоплює підозрілі повідомлення.

Контроль Інтернету – відстежує пошук та перегляд сторінок в Інтернеті у клієнтських системах та блокує веб-сайти та завантаження на основі рейтингу та вмісту безпеки.

Adaptive Threat Protection – аналізує вміст у корпоративному середовищі користувача та визначає, які дії виконувати, використовуючи дані про репутацію файлів, правила та порогові значення репутації.

Перелік посилань:
1. Best Endpoint Protection Platforms URL: https://www.gartner.com/reviews/market/endpoint-protection-platforms
2. Огляд Trellix Endpoint Security (ENS). (2024, October 16). URL: https://docs.trellix.com/ru-RU/bundle/endpoint-security-10.7.x-product-guide-windows/page/GUID-E46B9951-3324-425D-A788-A7933B363E88.html

Бишук Данило Вікторович,
Студент групи БСД-61, ННІЗІ ДУІКТ, Київ, Україна

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ НА ПРИКЛАДІ VECTRA AI

Штучний інтелект (далі – ШІ) стає ключовим інструментом у забезпеченні кібербезпеки корпоративних інформаційних систем, впроваджуючи інноваційні рішення для виявлення, аналізу та реагування на кіберзагрози. Завдяки здатності аналізувати великі обсяги даних, алгоритми машинного навчання можуть ідентифікувати аномалії в поведінці користувачів і систем, що дозволяє швидко виявляти потенційні атаки й нові можливості для виявлення різного типу кіберзагроз та реагування на інциденти.

У цій тезі розглянуто програмний засіб Vectra AI, як приклад ефективного використання штучного інтелекту для забезпечення максимального рівня безпеки в інформаційних системах.

1.Vectra AI: Огляд платформи [1]

Vectra AI є світовим лідером на ринку NDR-рішень (Network Detection and Response) - засобів виявлення загроз в мережевому трафіку та реагування на них в режимі реального часу для хмарних середовищ, SaaS, центрів обробки даних і корпоративних інфраструктур.

За допомогою штучного інтелекту рішення виявляє кібератаки на основі поведінки зловмисника, дозволяє експертам з безпеки всебічно аналізувати інциденти безпеки і визначати приховані загрози за допомогою розширених метаданих безпеки.

Платформа збирає величезні обсяги хмарних та мережевих метаданих, збагачує їх важливою для безпеки інформацією, оптимізованою за допомогою машинного навчання, виявляє в автоматичному режимі активність зловмисників і захищає хости серверів та користувачів від зламу незалежно від їх місцезнаходження.

Vectra AI пропонує комплексний підхід до кібербезпеки, поєднуючи функції виявлення загроз і аналізу даних. Платформа працює на основі аналізу мережевого трафіку та поведінки користувачів, використовуючи машинне навчання для розпізнавання патернів, характерних для кібератак.

2. Можливості Vectra AI для покращення кібербезпеки:

- Безперервний моніторинг: відстеження мережевого трафіку в режимі реального часу, шукаючи різні шаблони(патерни) або поведінку, які можуть вказувати на загрозу безпеці.

- Автоматизоване виявлення загроз: використовуючи розширену аналітику, застосунок визначає та класифікує потенційні загрози безпеки, зокрема зловмисне програмне забезпечення, спроби фішингу та інші шкідливі дії.
- Реагування на інцидент: у разі виявлення загрози, платформа ініціює процес реагування, щоб стримати, пом’якшити та усунути інцидент безпеки.
- Криміналістичний аналіз: керована NDR часто включає детальний криміналістичний аналіз, щоб зрозуміти масштаб і наслідки інциденту безпеки, допомагаючи організаціям посилити рівень безпеки.
- Звітування та рекомендації: регулярні звіти про інциденти безпеки, уразливості та рекомендації щодо покращення безпеки надаються організації для вдосконалення їхньої загальної стратегії кібербезпеки. [2]

3. Перспективи розвитки ШІ у сфері інформаційної безпеки.[3]

Перспективи розвитку Vectra AI включають вдосконалення алгоритмів машинного навчання, що дозволить підвищити точність виявлення загроз і зменшити кількість хибнопозитивних сповіщень. Крім того, розвиток технологій обробки природної мови відкриває нові можливості для аналізу текстових даних, таких як повідомлення електронної пошти, що може покращити виявлення фішингових атак.

Зростаюча популярність концепції "Zero Trust" також вплине на розвиток платформи, спонукаючи до інтеграції нових механізмів автентифікації та контролю доступу. З урахуванням еволюції кіберзагроз, Vectra AI може адаптуватися до нових реалій, зокрема, інтегруючи функції прогнозування загроз на основі аналізу історичних даних.

Зробимо висновки. Vectra AI представляє собою інноваційне рішення в сфері кібербезпеки, що поєднує потужні функції виявлення загроз і реагування на них у реальному часі. Завдяки використанню штучного інтелекту та алгоритмів машинного навчання, платформа забезпечує всебічний аналіз мережевих метаданих і активності користувачів, що дозволяє ефективно виявляти та реагувати на різноманітні кіберзагрози.

Впровадження Vectra AI в корпоративні інформаційні системи демонструє, як штучний інтелект може суттєво покращити кібербезпеку, забезпечуючи проактивний захист від еволюційних загроз, водночас відкриваючи нові горизонти для розвитку в умовах динамічного цифрового середовища.

Перелік посилань:

1. Vectra AI [Електронний ресурс] – Режим доступу до ресурсу: https://nwu.com.ua/vyrobnyky/vectra
2. Network and Detection Response [Електронний ресурс] – Режим доступу до ресурсу: https://www.vectra.ai/topics/network-detection-and-response
3. 2024 Predictions: Generative AI’s Role in Cybersecurity [Електронний ресурс] – Режим доступу до ресурсу: https://www.vectra.ai/blog/2024-predictions-generative-ais-role-in-cybersecurity

Бідник Нікіта Сергійович
студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

КРИПТОГРАФІЧНІ МЕТОДИ ТА СИСТЕМИ ВИЯВЛЕННЯ ЗАГРОЗ (IDS/IPS) ЯК ОСНОВА ТЕХНІЧНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

У статті розглядаються сучасні технічні системи захисту інформації, які є невід'ємною частиною безпеки корпоративних інформаційних систем. Основна увага приділена криптографічним методам захисту, системам виявлення та запобігання вторгненням (IDS/IPS), а також захисту мережевої інфраструктури. Підкреслено важливість інтеграції технічних рішень з управлінськими процесами для забезпечення надійного захисту інформації.

Сучасні корпоративні інформаційні системи стикаються з безпрецедентними загрозами, які вимагають впровадження комплексних технічних систем захисту інформації. Технічні засоби що забезпечують інформаційну безпеку дуже важливимі для захисту конфіденційності, цілісності та доступності даних у цифровому просторі. У цьому контексті, важливим є розвиток та інтеграція новітніх технологій у системи захисту, що забезпечує ефективний бар'єр проти кібератак.

Одним із ключових елементів технічних систем захисту є криптографічні методи. Вони дозволяють надійно шифрувати конфіденційні дані, що мінімізує ризики їх перехоплення або несанкціонованого доступу. Розвиток асиметричних алгоритмів шифрування, таких як RSA та ECC[1, с.52]., значно підвищує рівень захисту та кидає виклик все складнішим загрозам. Крім того, впровадження квантово-стійких алгоритмів шифрування стає все більш актуальним у зв'язку з розвитком квантових обчислювальних технологій.

Ще одним важливим напрямком є системи виявлення та запобігання вторгненням (IDS/IPS)[2, с.15(2-1)]. Ці системи аналізують трафік у реальному часі та можуть ідентифікувати шкідливі дії до того, як вони спричинять шкоду. Новітні рішення в цій сфері базуються на технологіях машинного навчання і штучного інтелекту, дозволяючи підвищити точність виявлення загроз та мінімізувати кількість хибнопозитивних спрацьовувань.

Захист на рівні мережі також залишається важливим аспектом технічних систем. Брандмауери, системи сегментації мережі та засоби шифрування трафіку є важливими елементами захисту від кібератак, спрямованих на мережеву інфраструктуру. Особливу увагу варто приділити безпеці хмарних середовищ, де необхідні додаткові технічні заходи для забезпечення захищеного обміну даними між хмарою та користувачами.

Нарешті, технічні системи захисту не можуть існувати без інтеграції з управлінськими рішеннями. Регулярний аудит безпеки, моніторинг систем, оновлення та патчинг програмного забезпечення – це обов'язкові заходами для підтримки ефективності захисту. Важливу роль відіграє також автоматизація процесів безпеки, яка дозволяє швидко реагувати на інциденти.

Таким чином, технічні системи захисту інформації повинні постійно розвиватися і адаптуватися до нових викликів. Інноваційні технології, поєднані з належним управлінням, здатні забезпечити надійний захист корпоративних інформаційних систем у мінливому кіберсередовищі.

Перелік посилань:

1. Schneier B. Applied cryptography: Protocols, algorithms, and source code in C. 2nd ed. New York : Wiley, 1996. 758 p. (Дата звернення: 14.10.2024)
2. Guide to intrusion detection and prevention systems (IDPS): Recommendations of the National Institute of Standards and Technology / ed. by M. Peter, National Institute of Standards and Technology (U.S.). Gaithersburg, MD : U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 2007. 127 p. (Дата звернення: 14.10.2024)

Бойко Данило Вікторович
Студент групи ТСДМ-62, ДУІКТ, Київ, Україна

КІБЕРБЕЗПЕКА КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ У КОНТЕКСТІ МЕТОДІВ ВИЯВЛЕННЯ ТА ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ WI-FI МЕРЕЖ

Робота присвячена питанням кібербезпеки корпоративних інформаційних систем у контексті захисту Wi-Fi мереж. У дослідженні розглянуто основні загрози, пов'язані з експлуатацією бездротових мереж, зокрема методи несанкціонованого доступу та викрадення даних. Особливу увагу приділено методам виявлення потенційних вразливостей та забезпечення захисту Wi-Fi мереж, які використовуються у корпоративному середовищі. Запропоновано ефективні підходи до захисту інформаційних потоків та управління доступом, включаючи використання сучасних технологій моніторингу мережі, шифрування даних та автентифікації. Робота акцентує увагу на важливості впровадження інтегрованих заходів безпеки для зменшення ризиків несанкціонованого втручання у Wi-Fi мережі компаній.

Ключові слова: кібербезпека, корпоративні інформаційні системи, Wi-Fi мережі, захист даних, виявлення загроз, автентифікація, шифрування, контроль доступу.

Кібербезпека є однією з найважливіших складових ефективного функціонування сучасних корпоративних інформаційних систем, особливо в умовах зростаючої кількості загроз у кіберпросторі. Оскільки компанії все більше покладаються на цифрові технології, безпечна передача даних через бездротові мережі стає критичною необхідністю. Мережі Wi-Fi є незамінним інструментом для корпоративного середовища, забезпечуючи гнучкість доступу до ресурсів і підвищуючи продуктивність співробітників. Однак відкритість і поширеність таких мереж становить значний ризик для інформаційної безпеки, оскільки вони є потенційною мішенню для кіберзлочинців, які прагнуть отримати несанкціонований доступ до корпоративних даних.

Основною проблемою для захисту мереж Wi-Fi є різноманітність методів атак, які використовують кіберзлочинці, починаючи від перехоплення трафіку і закінчуючи використанням вразливостей в протоколах шифрування. Тому важливо

розробляти і впроваджувати ефективні методи виявлення загроз і їх подальшої нейтралізації, а також забезпечувати комплексний захист даних в процесі їх передачі по бездротових каналах. У цьому контексті сучасні технології кібербезпеки пропонують широкий спектр інструментів для захисту Wi-Fi мереж, включаючи моніторинг мережевого трафіку, використання алгоритмів шифрування, методів аутентифікації та контролю доступу [1, с. 14].

З огляду на стрімкий розвиток цифрових технологій та зростання кількості атак на бездротові мережі, проблема забезпечення кібербезпеки корпоративних Wi-Fi мереж є надзвичайно актуальною. Бездротові мережі є невід'ємною частиною інформаційної інфраструктури багатьох підприємств, але їх відкритість і доступність для підключення становлять значну загрозу. Якщо Wi-Fi мережа скомпрометована, можливий витік конфіденційних даних, що може призвести до значних фінансових втрат, шкоди репутації компанії та навіть призупинення її діяльності.

Кібербезпека є критично важливою складовою корпоративних інформаційних систем, особливо в контексті захисту Wi-Fi мереж. Бездротові мережі забезпечують зручний доступ до ресурсів компанії, але водночас створюють ризики для конфіденційності та безпеки даних через можливі атаки.

Важливість кібербезпеки в корпоративних інформаційних системах
У сучасному корпоративному середовищі кібербезпека відіграє ключову роль у забезпеченні стабільної роботи компаній. Зокрема, захист мереж Wi-Fi є важливою складовою загальної стратегії інформаційної безпеки, оскільки бездротові мережі забезпечують легкий доступ до корпоративних ресурсів, але в той же час становлять значні ризики для конфіденційності та цілісності даних.

Ключові загрози для Wi-Fi мереж в корпоративному середовищі
Бездротові мережі вразливі до різних типів атак, найпоширенішими з яких є атаки типу «людина посередині», перехоплення мережевого трафіку, злом шифрування, фальшиві точки доступу та атаки на слабкі механізми аутентифікації. Ці загрози можуть призвести до несанкціонованого доступу до корпоративних даних або повної компрометації систем [2, с. 27].

Методи виявлення загроз у мережах Wi-Fi
Для забезпечення надійної безпеки необхідно використовувати сучасні технології моніторингу мережі, такі як системи виявлення вторгнень (IDS), які здатні виявляти аномальну активність в мережевому трафіку. За допомогою аналізу мережевих пакетів можна виявити спроби перехоплення або злому і визначити підозрілі точки доступу.

Аутентифікація і контроль доступу як частина безпеки Wi-Fi мережі
Надійна автентифікація користувачів є ключовим елементом кібербезпеки. Використання надійних паролів, сертифікатів безпеки та біометричних даних допомагає знизити ймовірність несанкціонованого доступу до мережі. Крім того, сегментація мережі та обмеження доступу до критично важливих ресурсів є важливими заходами безпеки.

Інтегровані рішення для захисту мереж Wi-Fi Комплексний підхід до кібербезпеки включає в себе реалізацію як технічних, так і організаційних заходів. Постійний моніторинг мережевої активності, регулярне оновлення програмного забезпечення та навчання персоналу допомагають мінімізувати ризики і забезпечити високий рівень захисту корпоративних Wi-Fi мереж [3, с. 87].

Актуальність постійного вдосконалення методів кібербезпеки У зв'язку зі швидкими темпами розвитку технологій і збільшенням кількості кіберзагроз, методи захисту Wi-Fi мереж повинні постійно вдосконалюватися. Дослідження нових вразливостей та інноваційні підходи до виявлення і нейтралізації загроз є ключовими аспектами забезпечення стійкої кібербезпеки в корпоративному середовищі.

Багаторівневий підхід до кібербезпеки, що включає сегментацію мережі, VPN та регулярне оновлення системи, може значно знизити ризики кібератак. У зв'язку з постійним розвитком технологій та збільшенням кількості загроз, постійне вдосконалення методів виявлення та захисту Wi-Fi мереж є надзвичайно важливим для забезпечення стійкої кібербезпеки корпоративних інформаційних систем.

Перелік посилань:

1. Сучасні інформаційні технології в кібербезпеці : монографія / А. С. Довбиш, В. К. Ободяк, І. В. Шелехов та ін. ; за ред. В. К. Ободяка, І. В. Шелехова. Суми : Сумський державний університет, 2021. 348 с.
2. Гончарова І.П. Кібербезпека в цифровому освітньому середовищі закладів професійної освіти: електронний навчальний курс. Біла Церква, БІНПО ДЗВО «УМО» НАПН УКРАЇНИ, 2022. 80 с.
3. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.

Бригинець Анастасія Андріївна
студентка групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

СУЧАСНІ ТЕХНОЛОГІЇ ПРИХОВУВАННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВІД АНТИВІРУСНИХ СИСТЕМ

У сучасному світі кількість кібератак стрімко зростає, а методи, які використовують зловмисники, стають все більш витонченими та складними. Шкідливе програмне забезпечення еволюціонує, використовуючи передові технології для обходу антивірусних систем та приховування своєї присутності. Це створює серйозні виклики для фахівців з кібербезпеки та потребує розробки нових підходів до захисту інформаційних систем. У цій роботі досліджуються сучасні технології приховування шкідливого програмного забезпечення від антивірусних систем, аналізуються їх механізми дії та пропонуються шляхи підвищення ефективності засобів захисту.

У 2023 році кількість унікальних загроз, про які повідомили кінцеві користувачі у світових організаціях за різними сімействами загроз, значно зросла (рис. 1). Цей стрімкий ріст свідчить про те, що зловмисники активно розвивають

свої методи, роблячи шкідливе програмне забезпечення все більш витонченим та важко виявлюваним. Збільшення різноманітності та складності таких загроз створює серйозні виклики для антивірусних систем, які змушені постійно адаптуватися до нових технік обходу та приховування. Особливо тривожить те, що сучасні технології дозволяють шкідливому ПЗ залишатися непоміченим протягом тривалого часу, завдаючи значної шкоди інформаційним системам. У зв'язку з цим стає критично важливим досліджувати та аналізувати новітні методи приховування шкідливого програмного забезпечення для розробки ефективних засобів захисту.

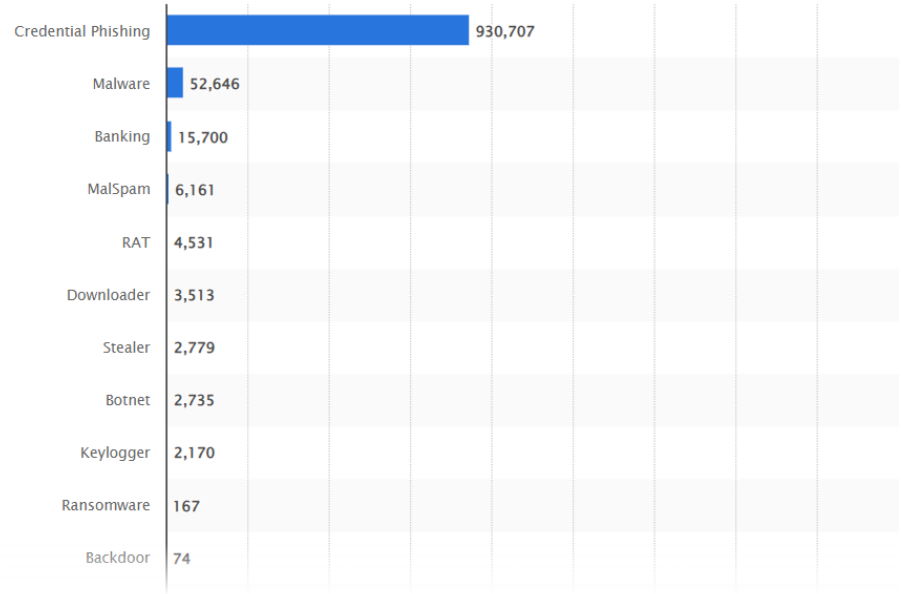


Рис. 1. Кількість унікальних загроз, про які повідомили кінцеві користувачі у світових організаціях у 2023 році, за сімействами загроз [3]

Унікальність шкідливого програмного забезпечення дуже часто є фіктивною, тобто такі програми є просто видозміненими (обфускованими). Обфускація програми - це семантично-зберігаюче перетворення, спрямоване на приведення програми до вигляду, який ускладнює розуміння її алгоритму та структур даних або перешкоджає вилученню певної цінної інформації з тексту програми. Оскільки обфускація може знайти широке застосування в комп'ютерній безпеці, приховуванні інформації та криптографії, вимоги безпеки до програмних обфускаторів стали основним об'єктом інтересу в теорії обфускації програмного забезпечення, починаючи з піонерських робіт в цій галузі[5].

Існують певні техніки обфускації даних. Найпоширеніші з них пов’язані з операваннями цілими числами, рядками та масивами. При обфускації можливо трансформувати дані за допомогою розбиття, злиття, процедурування, кодування тощо.

Розбиття даних розподіляє інформацію однієї змінної на кілька нових змінних. Наприклад, логічна змінна може бути розділена на дві логічні змінні, і за допомогою логічних операцій над ними можна отримати початкове значення. З іншого боку, об'єднання даних об'єднує кілька змінних в одну змінну. [1]

продемонстрували приклад, який об'єднує два 32-бітних цілих числа в одне 64-бітне ціле. [2] запропонували інший метод, який пакує кілька змінних в один простір за допомогою дискретних логарифмів.

Процедуризація даних полягає в заміні статичних даних викликами процедур. Замість зберігання рядків або чисел як фіксованих значень, програма може використовувати функції, які генерують ці дані під час виконання, вказуючи конкретні параметри. Наприклад, для присвоєння значення v змінній і можна використати допоміжну змінну *j*, де $j = f(v)$, а для отримання початкового значення викликати обернену функцію $g(j)$.

Кодування даних за допомогою математичних функцій або шифрів є ефективним методом обфускації. Рядки можуть бути зашифровані афінними шифрами або іншими криптографічними алгоритмами, а числові дані — кодовані через бітові операції, такі як XOR. Після необхідних обчислень результати розшифровуються безпосередньо перед використанням або виведенням, що ускладнює аналіз коду для сторонніх осіб.

Масиви, як одна з найпоширеніших структур даних, можуть бути обфусцьовані різними способами. Один масив можна розбити на кілька підмасивів або об'єднати кілька масивів в один. Також можливо збільшити або зменшити розмір масиву через складання або сплющення. Індекси масивів можуть перетворюватися за допомогою складних функцій, що робить доступ до елементів менш очевидним. Наприклад, елементи масиву можна перемішати за формулою $i \times m \bmod n$, де i — початковий індекс, n — розмір масиву, а m і n — взаємно прості числа.

Додатково, для підвищення рівня приховування можуть використовуватися динамічні структури даних та алгоритми, які змінюють свою поведінку під час виконання. Впровадження таких методів обфускації значно ускладнює реверс-інжиніринг та аналіз програмного забезпечення зловмисниками, підвищуючи його безпеку та стійкість до атак [4].

Отже, сучасне шкідливе програмне забезпечення стає все більш складним і важким для виявлення завдяки використанню різних технік обфускації. Обфускація даних, таких як цілі числа, рядки та масиви, через розбиття, злиття, процедурування та кодування, значно ускладнює аналіз коду та реверс-інжиніринг. Ці методи дозволяють зловмисникам приховувати справжню функціональність програм та уникати виявлення антивірусними системами. Тому розуміння та дослідження цих технік є критично важливим для розробки ефективних засобів захисту та протидії кіберзагрозам. Впровадження нових підходів до аналізу та виявлення обфускованого шкідливого ПЗ допоможе підвищити безпеку інформаційних систем і зменшити ризики, пов'язані з кіберзлочинністю. Загалом, боротьба з сучасними загрозами вимагає постійного вдосконалення методів аналізу та співпраці між дослідниками в галузі кібербезпеки.

Перелік посилань:

1. Collberg C., Thomborson C., Low D. Manufacturing cheap, resilient, and stealthy opaque constructs. *The 25th ACM SIGPLAN-SIGACT symposium*, San Diego, California, United States, 19–21 January 1998. New York, New York, USA, 1998. URL: https://doi.org/10.1145/268946.268962 (date of access: 05.10.2024).
2. Ertaul L., Venkatesh S. Novel obfuscation algorithms for software security. *International Conference on Software Engineering Research and Practice. Citeseer FIPS 19*. URL: https://doi.org/10.6028/nist.fips197.
3. Global unique threats by threat family 2023 | Statista. *Statista*. URL: https://www.statista.com/statistics/1462339/unique-threats-reported-end-users-by-threat-family/ (date of access: 05.10.2024).
4. Layered obfuscation: a taxonomy of software obfuscation techniques for layered security / H. Xu et al. *Cybersecurity*. 2020. Vol. 3, no. 1. URL: https://doi.org/10.1186/s42400-020-00049-3 (date of access: 05.10.2024).
5. The current state of art in program obfuscations: definitions of obfuscation security / N. P. Varnovskiy et al. *Programming and computer software*. 2015. Vol. 41, no. 6. P. 361–372. URL: https://doi.org/10.1134/s0361768815060079 (date of access: 05.10.2024).

Бригинець Олександр Сергійович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

ВРАЗЛИВОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ: НЕБЕЗПЕКА ЗАХИЩЕНИХ СИСТЕМ

У сучасному світі програмне забезпечення є основою практично всіх технологічних рішень. Від мобільних додатків до корпоративних систем, ми щодня покладаємося на програмне забезпечення для виконання різноманітних завдань. Проте зростання популярності і складності програм також супроводжується збільшенням їх вразливостей, які можуть бути використані зловмисниками для атаки на системи.

Вразливості програмного забезпечення можуть виникати з різних причин. Це можуть бути помилки в коді, відсутність необхідних оновлень безпеки або навіть недотримання стандартів розробки. Часто зловмисники експлуатують ці вразливості, щоб отримати доступ до чутливих даних, викрасти інформацію або навіть повністю контролювати системи.

Дослідження показують, що багато зловмисних атак починаються з використання вразливостей, які могли бути усунуті за допомогою простих оновлень. Наприклад, у 2021 році вразливість у протоколі Apache Log4j, що використовується в багатьох веб-додатках, призвела до численних атак на різні компанії, які не встигли вчасно оновити свої системи. Цей інцидент наголосив на важливості регулярного моніторингу та оновлення програмного забезпечення.

Крім того, вразливості програмного забезпечення можуть впливати на безпеку не лише окремих систем, а й цілих організацій. Наприклад, успішна атака на внутрішню систему компанії може призвести до витоку даних клієнтів, що в свою чергу завдає шкоди репутації бізнесу та його фінансовому становищу. Багато організацій недооцінюють важливість захисту своїх програмних рішень, вважаючи, що достатньо мати надійний фаєрвол або антивірус. Проте без

регулярних перевірок на вразливості та оперативного реагування на них, такі системи залишаються відкритими для атак.

Методи захисту від вразливостей програмного забезпечення включають регулярне проведення аудитів безпеки, використання засобів автоматичного виявлення вразливостей та патчів, а також впровадження політики безпеки, що охоплює всі етапи розробки програмного забезпечення. Важливо, щоб усі співробітники організації розуміли значення кібербезпеки і брали участь у створенні безпечного середовища.

Таким чином, вразливості програмного забезпечення становлять серйозну загрозу для безпеки систем. Постійний моніторинг, своєчасні оновлення та обізнаність користувачів можуть суттєво знизити ризик успішних атак. У світі, де технології постійно еволюціонують, важливо тримати руку на пульсі змін і забезпечувати безпеку своїх систем на всіх рівнях.

Перелік посилань:

1. Що таке вразливості програмних продуктів, та якої шкоди через це може зазнати пристрій?. URL: https://cip.gov.ua/ua/faqs/sho-take-vrazlivosti-programnikh-produktiv-ta-yakoyi-shkodi-cherez-ce-mozhe-zaznati-pristrii (date of access: 07.10.2024).
2. Що таке виявлення загроз і реагування на них?. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-threat-detection-response-tdr (date of access: 05.10.2024).
3. Виявлення вразливостей: тестування на проникнення як засіб захисту. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/identifying-vulnerabilities-penetration-testing-as-a-means-of-protection (date of access: 04.10.2024).

Брикса Ігор Ігорович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

ВНУТРІШНІ ЗАГРОЗИ: НЕБЕЗПЕКА ЗСЕРЕДИНИ

Кібербезпека часто асоціюється із захистом від зовнішніх загроз, таких як хакери або шкідливе програмне забезпечення. Проте не менш небезпечними є загрози, що виходять із самої організації — так звані внутрішні загрози. Це ризики, пов'язані з діями співробітників, підрядників або навіть партнерів компанії, які мають доступ до її систем та даних. Внутрішні загрози можуть бути як навмисними, так і випадковими, але їхній потенціал для шкоди надзвичайно високий.

Однією з ключових причин виникнення внутрішніх загроз є людський фактор. Співробітники можуть ненавмисно скомпрометувати систему через недбалість, незнання або помилки. Наприклад, нехтування правилами безпеки, слабкі паролі або використання незахищених пристроїв можуть відкрити двері для зловмисників. Водночас, існують і навмисні дії — ситуації, коли працівники, з незадоволенням або мотивовані фінансовою вигодою, навмисно викрадають дані або зривають роботу системи.

Відомі випадки, коли невдоволені або звільнені співробітники викрадали конфіденційну інформацію або навіть завдавали збитків компаніям, знищуючи важливі дані. Такі дії можуть мати катастрофічні наслідки не тільки для репутації організації, але й для її фінансового стану. За даними аналітичних звітів, внутрішні загрози є однією з головних причин значних витрат на кібербезпеку та відновлення після інцидентів.

Захист від внутрішніх загроз вимагає впровадження комплексних заходів. Це включає в себе не лише технічні рішення, такі як системи моніторингу активності та управління доступом, але й роботу з персоналом. Регулярне навчання співробітників правилам безпеки, проведення інструктажів і тестувань на розпізнавання загроз є важливим елементом запобігання інцидентам. Крім того, важливо впроваджувати політику обмеженого доступу до критично важливих даних і систем, надаючи кожному співробітнику лише ті права доступу, які йому необхідні для виконання робочих обов'язків.

Не менш важливою є культура довіри та відкритості в організації. Виявлення потенційних внутрішніх загроз часто стає можливим завдяки спостереженням колег або менеджерів, які можуть помітити підозрілі дії або зміни в поведінці співробітників. Програми анонімного повідомлення про такі підозри допомагають виявляти проблеми ще до того, як вони перетворяться на серйозні інциденти.

Таким чином, внутрішні загрози є серйозною небезпекою для організацій. Захист від них вимагає поєднання технічних інструментів, ефективної політики безпеки та постійної роботи з персоналом. Лише комплексний підхід може забезпечити надійний захист компанії від загроз, що ховаються всередині.

Перелік посилань:

1. Що таке кібербезпека?. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity (date of access: 07.10.2024).
2. Що таке кібербезпека та з чим її їдять?. URL: https://cybersec.net.ua/statti/615-shcho-take-kiberbezpeka-ta-z-chym-ii-idiat.html (date of access: 05.10.2024).
3. Що таке кібербезпека?. URL: https://nordvpn.com/uk/cybersecurity/what-is-cybersecurity/ (date of access: 04.10.2024).

Брода Кирило Олександрович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

ФІШИНГ ЯК НАЙПОШИРЕНІШИЙ МЕТОД КІБЕРАТАК

У нашій сучасній епосі, де технології проникають у всі сфери життя, фішинг став одним із найбільш поширених і небезпечних видів кібератак. Це не просто технічне поняття — це реальна загроза, з якою щодня стикаються мільйони людей по всьому світу. Фішинг — це форма обману, коли зловмисники намагаються видурити конфіденційну інформацію, видаючи себе за надійні джерела. Уявіть, що ви отримуєте електронний лист, який, на перший погляд, виглядає так, ніби він надійшов від вашого банку. У ньому сказано, що ваш рахунок може бути заблоковано, якщо ви не перейдете за посиланням і не підтвердите свої дані. У такій ситуації легко піддатися паніці і без роздумів виконати вимогу.

Зловмисники вміло використовують емоції для маніпуляцій. Страх, терміновість, навіть надія — все це емоції, які вони експлуатують, щоб змусити жертв діяти швидко, не замислюючись про наслідки. Це робить фішинг одним із найефективніших методів кібератак. За статистикою, близько 90% всіх успішних кібератак починаються з фішингових спроб, що свідчить про те, як важливо бути уважними та обізнаними.

Фішинг не обмежується лише електронною поштою. Сьогодні зловмисники активно використовують соціальні мережі, мобільні додатки та SMS-повідомлення. Соціальний фішинг, наприклад, передбачає використання інформації з ваших акаунтів у соцмережах для створення переконливих повідомлень. А смішинг — це фішинг через SMS, коли ви отримуєте текстове повідомлення з посиланням, яке може призвести до втрати ваших даних. Тож важливо розуміти, що фішинг може приймати різні форми, і його жертвою може стати будь-хто.

Одна з найбільших проблем фішингу полягає в тому, що жодна технологія не може повністю захистити від цієї загрози. Навіть найсучасніші системи безпеки можуть виявитися безсилі, якщо їх користувачі не мають належної обізнаності. Тому навчання та підвищення обізнаності співробітників і користувачів є ключовими аспектами боротьби з цією загрозою. Проводячи регулярні тренінги, можна навчити людей розпізнавати підозрілі повідомлення та вжити необхідних заходів для захисту себе.

Важливо також використовувати технологічні заходи для підвищення безпеки. Наприклад, багатофакторна автентифікація є чудовим способом ускладнити зловмисникам доступ до ваших облікових записів. Це додаткова ланка захисту, яка ускладнює ситуацію, навіть якщо хтось отримав ваш логін і пароль. Встановлення антивірусного програмного забезпечення та фільтрація спаму також можуть суттєво зменшити ймовірність успіху фішингових атак.

Однак не менш важливим є постійний моніторинг і оновлення безпеки систем. Регулярні оцінки вразливостей, тестування на проникнення та аудит безпеки можуть суттєво покращити захист вашої організації. Залучення фахівців з кібербезпеки для проведення таких перевірок допоможе виявити потенційні загрози ще до того, як вони стануть проблемою.

Отже, фішинг залишається однією з найважливіших загроз у сфері кібербезпеки, з якою стикається кожен з нас. У світі, де технології постійно розвиваються, критично важливо підтримувати високий рівень обізнаності серед користувачів і впроваджувати ефективні заходи безпеки. Тільки спільними зусиллями — від індивідуальних користувачів до великих організацій — ми можемо зменшити ризики кібератак і забезпечити безпечніше цифрове середовище.

Перелік посилань:

1. Фішинг допомагає маніпулювати людьми заради даних. Як захиститися від кіберзагроз . URL: https://journal.gen.tech/post/sho-take-socialna-ingeneria (date of access: 07.10.2024).
2. Кібергігієна: як захиститися від фішингу . URL: https://osvita.diia.gov.ua/courses/kibergigiena-ak-zahistitisa-vid-fisingu (date of access: 05.10.2024).
3. Основи кібербезпеки. URL: https://moz.gov.ua/uk/news/osnovi-kiberbezpeki-2 (date of access: 04.10.2024).

Василенко Ярослав Олександрович
Студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД КВАНТОВИХ ЗАГРОЗ: НОВІ АЛГОРИТМИ ШИФРУВАННЯ

Квантові комп'ютери обіцяють здійснити революцію в обчислювальній техніці, проте вони також несуть загрозу сучасним алгоритмам шифрування. Існуючі криптографічні протоколи, такі як RSA, DSA, та ECC, які широко використовуються для захисту даних в мережах, банківських системах та інтернет-транзакціях, можуть бути легко зламані за допомогою квантових алгоритмів, зокрема алгоритму Шора. Цей алгоритм, використовуючи принципи квантової механіки, дозволяє швидко знаходити прості множники великих чисел, що робить традиційні алгоритми факторизації неефективними. Тому виникає необхідність у розробці нових криптографічних рішень, здатних протистояти квантовим атакам і забезпечити безпеку інформації в умовах розвитку квантових технологій.

Зараз більшість систем захисту інформації базуються на складності розв'язання задач, які класичними комп'ютерами вирішити дуже складно або практично неможливо. Наприклад, алгоритми RSA та ECC ґрунтуються на труднощах факторизації великих чисел та обчисленні дискретного логарифма, що є надзвичайно трудомісткими завданнями для класичних обчислювальних машин. Зважаючи на це, ці алгоритми вважалися надійними та безпечними. Однак квантові комп'ютери, за допомогою алгоритму Шора, можуть розв'язувати ці задачі за поліноміальний час, що робить такі системи вразливими.

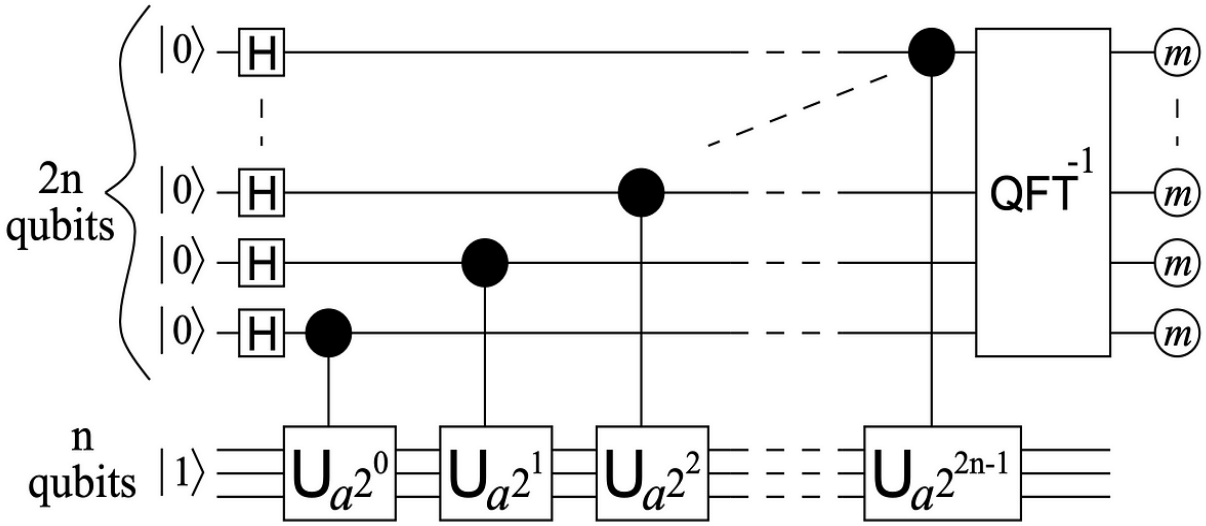


Рис. 1 – Алгоритм Шора

Квантові обчислення дозволяють значно скоротити час, необхідний для зламу традиційних криптографічних алгоритмів, що загрожує безпеці даних в багатьох галузях, включаючи фінансову, медичну та державну.

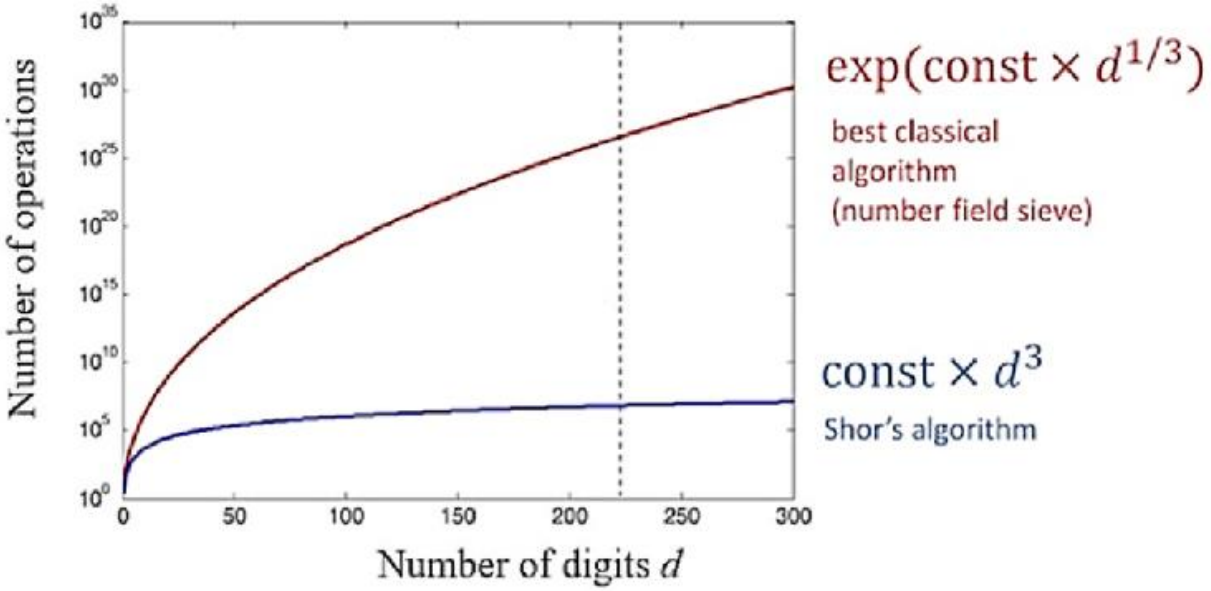


Рис. 2 – Продуктивність класичних та квантових алгоритмів для розкладання простих чисел на множники.

Розробка нових алгоритмів шифрування, які можуть забезпечити захист від квантових загроз, є однією з ключових цілей сучасної криптографії. Постквантова криптографія передбачає створення алгоритмів, які залишатимуться безпечними навіть за умови існування потужних квантових комп'ютерів. Серед перспективних напрямків є криптографія на основі решіток, кодове шифрування, мультипроменеві схеми та шифрування на основі хеш-функцій. Ці алгоритми розроблені на основі задач, які є складними для обчислення навіть за наявності квантових технологій.

1. **Криптографія на основі решіток**: ґрунтується на задачах, що стосуються найкоротшого вектора решітки, які є складними для обчислення навіть на

квантових комп'ютерах. Прикладом такого алгоритму є NTRUEncrypt, що вже зарекомендував себе як надійний варіант для захисту від квантових атак. Такі алгоритми важко зламати, оскільки навіть квантові обчислення не можуть ефективно вирішувати задачі на основі решіток у прийнятний термін.

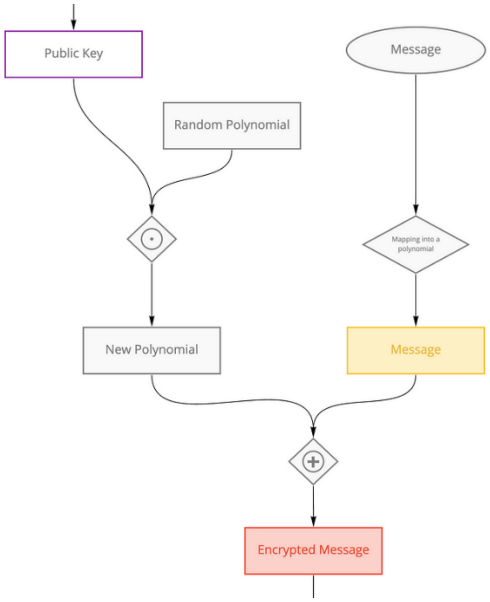


Рис. 3 – Шифрування з допомогою алгоритму NTRU

2. **Кодові шифри**: включають використання кодів для приховування даних. McEliece є одним із найвідоміших алгоритмів цього типу, який вважається стійким до квантових обчислень. Цей підхід використовує коди помилок, що додає додатковий рівень складності при спробі зламу за допомогою квантових методів.

3. **Криптографія на основі мультипроменевих схем**: такі алгоритми використовують геометричні задачі, які важко вирішити квантовими методами. Використання просторових моделей робить ці схеми стійкими до нових атак, оскільки завдання стає значно складнішим для реалізації навіть за допомогою квантових комп'ютерів.

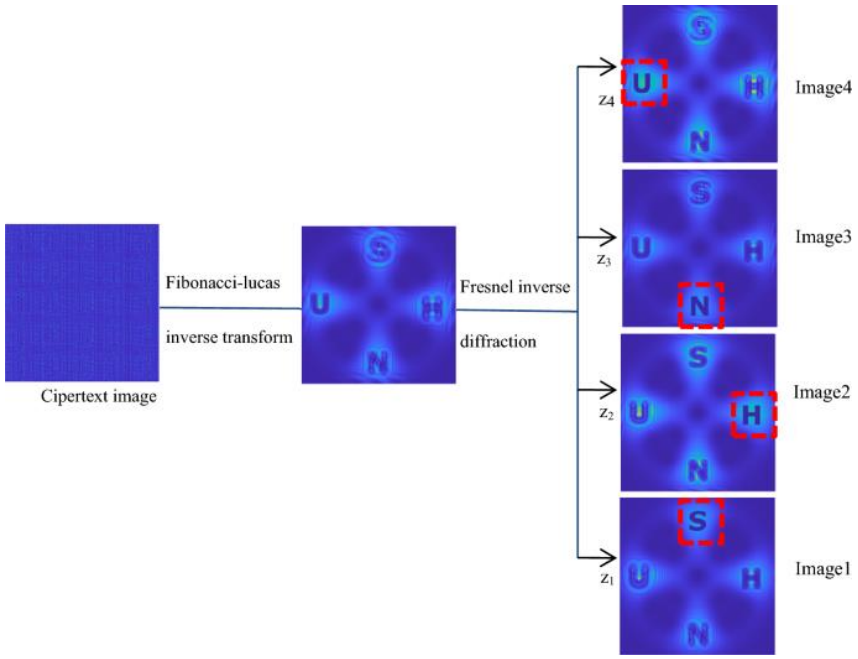


Рис. 5 – Криптографія на основі мультипроменевих схем

4. **Хеш-функції**: шифрування на основі хешів також пропонує безпеку проти квантових атак, оскільки алгоритми, як правило, є незалежними від факторизації або дискретного логарифмування. Такі методи є перспективними, оскільки можуть бути вдосконалені з урахуванням специфіки квантових обчислень.

Постквантова криптографія є важливою частиною досліджень у сфері інформаційної безпеки, оскільки квантові комп'ютери потенційно можуть зламати більшість сучасних криптографічних систем, що наразі забезпечують захист важливих даних. Тому нові алгоритми шифрування, які базуються на складніших математичних задачах, стануть основою для майбутніх систем захисту даних. Міжнародні організації, такі як NIST (Національний інститут стандартів і технологій США), вже працюють над стандартизацією таких алгоритмів, проводячи конкурси та оцінюючи їхню стійкість до можливих атак. Впровадження постквантової криптографії буде важливим кроком для забезпечення довготривалої безпеки інформаційних систем та захисту даних у майбутньому квантовому середовищі.

Загалом, квантові комп'ютери та їхні можливості стимулюють активний розвиток криптографічної науки. Нові методи та підходи повинні враховувати потенціал квантових загроз та забезпечувати стійкість інформаційних систем. Це сприятиме побудові надійних засобів захисту для забезпечення довготривалої безпеки в умовах розвитку квантових технологій.

Перелік посилань:

1. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography. URL: https://csrc.nist.gov/projects/post-quantum-cryptography (дата звернення: 17.10.2024).

2. Shor, P. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science.

Василенко Іван Дмитрович
студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

Технічні системи захисту інформації

У сучасному світі інформація є одним із найважливіших ресурсів, тому забезпечення її захисту стає критично важливим. Порушення інформаційної безпеки може призвести до серйозних наслідків, таких як фінансові втрати, витік конфіденційних даних або компрометація важливих систем. Для захисту інформації розробляються й впроваджуються різноманітні технічні системи, які дозволяють забезпечити безпеку даних від різних загроз.

Основні категорії технічних систем захисту інформації

Технічні системи захисту інформації поділяються на дві основні категорії: апаратні й програмні засоби.

Апаратні засоби захисту включають фізичні пристрої та компоненти, які забезпечують захист інформації на рівні обладнання. До них належать брандмауери (фаєрволи), маршрутизатори з функціями безпеки, криптографічні модулі та інші пристрої, які можуть обмежити доступ до даних.

Приклад: апаратні модулі безпеки (HSM — Hardware Security Module), що використовуються для захисту криптографічних ключів та забезпечення безпечного шифрування даних.

Програмні засоби захисту реалізуються за допомогою програмного забезпечення і забезпечують безпеку інформації шляхом контролю доступу, шифрування, аутентифікації та інших засобів. Вони можуть бути інтегровані у різні системи й платформи для забезпечення захисту даних як у локальних мережах, так і в хмарних середовищах.

Приклад: антивірусні програми, системи виявлення і запобігання вторгнень (IDS/IPS), а також програмне забезпечення для шифрування даних.

Виклики інформаційної безпеки

Основні загрози для інформації включають несанкціонований доступ, атаки типу DDoS, віруси й шкідливе ПЗ, фішинг та інші форми соціальної інженерії. Щоб захиститися від таких загроз, підприємства й організації повинні впроваджувати комплексні рішення для безпеки.

Один з найважливіших аспектів — це забезпечення конфіденційності, цілісності й доступності інформації. Для цього застосовуються багаторівневі підходи, які включають в себе як технічні засоби, так і організаційні заходи.

Приклади впровадження технічних систем захисту

Розглянемо деякі реальні приклади впровадження технічних систем захисту

інформації.

1. *Компанія з електронної комерції* може використовувати шифрування даних під час їх передавання через інтернет, а також брандмауери для захисту від зовнішніх атак. Це дозволяє забезпечити безпечне зберігання й передавання конфіденційної інформації, такої як платіжні дані клієнтів.
2. *Банківські установи* часто використовують апаратні криптографічні модулі HSM для захисту транзакцій та управління криптографічними ключами. Це дозволяє забезпечити безпеку банківських операцій та мінімізувати ризик шахрайства.

Сучасні технології захисту інформації

Сьогодні нові технології, такі як штучний інтелект і машинне навчання, активно використовуються для покращення інформаційної безпеки. Вони дозволяють виявляти складні атаки й аномалії у поведінці користувачів, що підвищує ефективність систем виявлення вторгнень та інших засобів захисту.

Також важливу роль відіграють технології шифрування, які дозволяють надійно захищати дані як у стані зберігання, так і під час передавання. Наприклад, протоколи SSL/TLS забезпечують шифрування з'єднань для захисту передавання даних в інтернеті.

Висновок

Технічні системи захисту інформації є важливим інструментом для забезпечення безпеки даних у сучасному світі. Ефективне застосування як апаратних, так і програмних засобів дозволяє значно знизити ризики витоку інформації та атак зловмисників. З урахуванням швидкого розвитку технологій, необхідність в інноваційних рішеннях для захисту даних постійно зростає.

Перелік посилань:

1. Cryptography: Protocols URL: https://mrajacse.wordpress.com/wp-content/uploads/2012/01/applied-cryptography-2nd-ed-b-schneier.pdf (дата звернення: 15.10.2024).
2. Network Security Essentials: Applications and Standards URL: https://elhacker.info/manuales/Redes/3. Network-security-essentials-4th-edition-william-stallings.pdf (дата звернення: 15.10.2024).

студент групи БСДМ-52, ННІКЗІ ДУІКТ, Київ, Україна

ЕТИКА КІБЕРБЕЗПЕКИ ПРИ ВИКОРИСТАННІ МОБІЛЬНИХ ПРИСТРОЇВ В ОРГАНІЗАЦІЇ

Питання етики виникає у будь-якій сфері діяльності. З розвитком суспільства і необхідності розробляти, впроваджувати і використовувати все складніші інформаційні і кібернетичні системи виникає гостра необхідність для встановлення різноманітних правил для безпеки свого цифрового середовища.

Глобалізація також сприяє посиленню проблеми етики, оскільки можливість працювати на будь-яку компанію зараз доступна по всьому світу. Проблематика виникає не просто на рівні різноманіття культур і відмінності менталітетів – суть питань в тому, щоб, підтримуючи безпеку мобільних девайсів чи сервісів, при цьому не порушувати особисті кордони працівників компанії.

Уведення різноманітних сервісів, які допомагають технічним спеціалістам і фахівцям з кібербезпеки краще контролювати інформаційне середовище компанії – це дуже ефективний метод для раннього виявлення і реагування на загрози інформаційної безпеки, але з точки зору етики також створює деякі проблеми. Технології на базі BYOD (Bring You Own Device) дозволяють фахівцям встановлювати необхідні програми і протоколи для контролю і захисту особистого пристрою користувача, використовуючи який він має доступ до зберігання і обробки даних організації. Проте у кінцевого користувача може виникнути враження наче його в чомусь обмежують і постійно контролюють, що не сприяє хорошому настрою і високій мотивації.

Фахівці щодо ризиків інформаційної безпеки і приватності з CLCT (Center for Long-Term Cybersecurity) також зазначають, що компанії стали впроваджувати більше технологій, що порушують приватне життя працівників [1].

Для прикладу, в анонімній компанії було опитано декілька працівників, вибраних випадковим чином з різних відділів, щодо програм встановлених на кінцевих пристроях користувачів, а саме:

- програма для віддаленого підключення адміністратора;
- антивірусне програмне забезпечення;
- кілька політик, що обмежують використання певних сайтів і програм.

З опитаних більше половини заявили, що мають враження, наче за ними постійно хтось спостерігає, також приблизно третина сказали що відчувають сповільнення роботи свого пристрою після встановлення програм, що заважає їм працювати. Більшість прямо або опосередковано висловили думку, що побоюються за те, що хтось може спостерігати за їхнім особистим життям. Деякі свідчили, що після розмов з адміністратором почуваються так, наче їх за замовчуванням вважають винними в чомусь, що вони ще навіть не зробили, а невелика кількість працівників поділились, що якби знали про це – не прийняли б пропозицію роботи з самого початку.

Також дослідження APA (American Psychological Association) показує, що 56% працівників відчувають стрес, якщо роботодавець постійно контролює їх роботу. Це стосується в основному активних інструментів моніторингу, але

інструменти кібербезпеки часто справляють ефект саме такого контролю [2].

Трохи спрощує подібну проблему надання компанією власного пристрою для роботи з її даними. Мобільний пристрій від компанії згладжує деякі кути проблеми: користувачу не потрібно встановлювати будь-яке програмне забезпечення на особисті пристрої і не виникає загрози несанкціонованого доступу до його персональних даних зі сторони технічних спеціалістів чи фахівців з кібербезпеки. Однак все ще залишаються проблеми як етичні, так і технічного характеру.

З проблем технічного характеру можна виділити можливість віддаленого налаштування пристрою для користувача. Так, ця проблема абсолютно зникає, якщо будь-який спеціаліст з компанії отримає мобільний пристрій у свої руки і налаштує його. Однак якщо треба забезпечити пристроями працівників у віддалених регіонах чи в інших країнах, то питання налаштування пристрою дистанційно стає нагальним.

Дещо допомагають вирішити це питання технології як-от Apple Business Manager та Windows Autopilot, що дають змогу налаштувати політики і встановити потрібне програмне забезпечення на мобільний пристрій одразу, як той вперше буде вийнятий з коробки і підключений до мережі [3][4]. Але проблемою є доступність цих інструментів для багатьох регіонів, зокрема і в Україні.

Ці методи можуть спростити значні виклики етичної складової, але залишаються багато все тих самих питань: працівники відчувають недовіру до себе, мають враження, наче за їх роботою постійно хтось стежить, відчуття гіперконтролю над своєю діяльністю.

По суті, до стандартного набору вимог до кібербезпеки – цілісність, конфіденційність і доступність – в даному випадку додається четвертий фактор, який також впливатиме на ефективність роботи працівників – етичність.

На жаль, на даний час немає чітких підходів до розробки програмного забезпечення для безпеки мобільних пристроїв, як і певних правил для організацій щодо того, які інструменти з яким рівнем контролю можна впроваджувати. Це може бути передумовою введення надто жорстких правил для працівників, що ще більше може впливати на їхній моральний стан.

Компенсувати описані вище незручності можна ввівши деякий ряд правил щодо того, як мають поводити себе спеціалісти з кібербезпеки чи будь-які технічні фахівці, які займаються подібними питаннями в організації. Так, не можна при поясненні необхідності різноманітних обмежень обґрунтовувати їх некомпетентністю кінцевого користувача в питаннях кібербезпеки, краще акцентувати увагу на зовнішніх загрозах. Якщо є потреба у віддаленому підключенні до пристрою користувача, він має бути попереджений про це заздалегідь і особисто давати згоду на підключення через елементи інтерфейсу. Це дасть відчуття контролю працівника над своїм особистим інформаційним простором.

Також, встановивши деякі вимоги до програмного забезпечення, можна

нівелювати деякі проблеми сприйняття цих систем кінцевими користувачами. Наприклад:

- програмне забезпечення має працювати “на фоні” і мати обмежену взаємодію з кінцевим користувачем;
- програми повинні мати мінімальні системні вимоги і використовувати якомога менше ресурсів системи;
- програми мають забезпечувати прозорість своїх дій, зокрема надавати користувачам можливість отримувати інформацію про те, які саме дії та дані обробляються, без порушення їхньої конфіденційності або переривання робочого процесу.

Підсумовуючи, можна сказати, що кібербезпека, без сумніву, повинна мати високий пріоритет, але методи її забезпечення мають бути чітко контрольованими, і вплив на моральний стан працівника компанії має бути зведеним до незначного. Також будь-який фахівець, який працює над покращенням безпекової ситуації у кіберпросторі компанії, має розуміти, як правильно пояснити кінцевим користувачам пристроїв необхідність тих чи інших правил і правильно підбирати програмне забезпечення, зважаючи не тільки на його ефективність, але й на його елементи взаємодії з користувачем.

Попри те, що сучасні технологічні рішення швидко розвиваються, треба проводити роботу над їх доступністю в різних регіонах світу і приведенню їх до напрацьованих стандартів етичних норм.

Перелік посилань:

1. Security & privacy risks of the hybrid work environment - CLTC UC berkeley center for long-term cybersecurity. *CLTC*. URL: https://cltc.berkeley.edu/2022/02/08/security-privacy-risks-of-the-hybrid-work-environment/ (date of access: 17.10.2024).
2. Michele L. Electronically monitoring your employees? It’s impacting their mental health. *https://www.apa.org*. URL: https://www.apa.org/topics/healthy-workplaces/employee-electronic-monitoring (date of access: 17.10.2024).
3. Overview of windows autopilot. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/autopilot/overview (date of access: 17.10.2024).
4. Посібник користувача apple business manager. *Apple Support*. URL: https://support.apple.com/uk-ua/guide/apple-business-manager/welcome/web (дата звернення: 17.10.2024).

Волошин Вадим Сергійович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ISO 27001 – Система менеджменту інформаційної безпеки

Що таке ISO/IEC 27001 – це міжнародний стандарт щодо Системи менеджменту інформаційної безпеки. ISO/IEC 27001 допомагає організаціям різних секторів забезпечувати конфіденційність, цілісність та доступність інформації за рахунок застосування процесу управління ризиками та надає впевненості зацікавленим сторонам у тому, що ризики адекватно оцінюються та управляються. Які ж основні причини розробки та впровадження цього стандарту?

Вони такі:

конфіденційність – забезпечення доступності інформації лише для тих, хто має відповідні повноваження.

доступність – забезпечення доступу до інформації лише авторизованим користувачам та в потрібний момент часу.

цілісність – забезпечення точності та повноти інформації, а також методів її обробки.

Впровадження системи менеджменту інформаційної безпеки допомагає Вам вирішити ці питання та захищає Вашу інформацію від зайвих очей, а також Система менеджменту інформаційної безпеки — інструмент для запобігання втратам підприємства.

Першим стандартом з інформаційної безпеки є прийнятий на державному рівні в 1995 році і розроблений Британським інститутом стандартів BS 7799 – Part 1.

У 1999 році ця версія стандарту була перероблена та передана в Міжнародну Організацію з Сертифікації, а в 2000 році затверджена як міжнародний стандарт ISO/IEC 17799: 2000 (BS 7799-1: 2000).

Останньою версією цього стандарту, прийнятою у 2005 році, є ISO/IEC 17799:2005.

У вересні 2002 року набула чинності друга частина стандарту BS 7799 Part 2.

Друга частина BS 7799 переглядалася в 2002 р., а наприкінці 2005 р. була прийнята ISO як міжнародний стандарт ISO/IEC 27001:2005 «Інформаційні технології — Методи забезпечення безпеки — Системи управліннязалучення інформаційної безпеки — Вимоги».

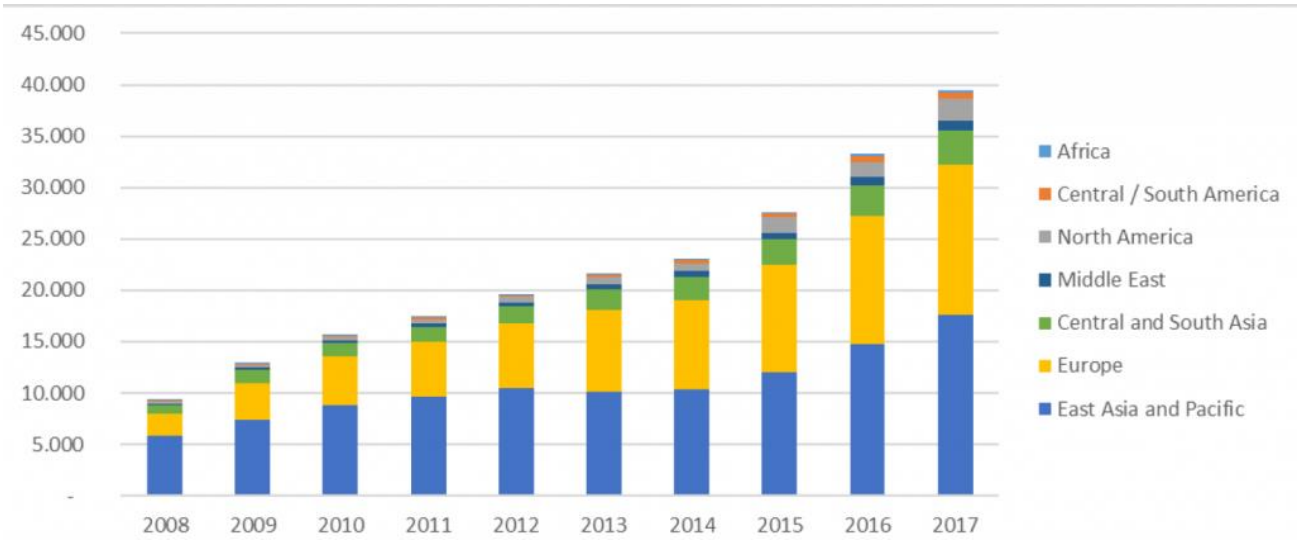


Рис.1. Кількість виданих сертифікатів

	Total valid certificates	Total number of sites
ISO 9001:2015	878 664	1 180 965
ISO 14001:2015	307 059	447 547
ISO IEC 27001:2013	31 910	59 934
ISO 22000:2005 & 2018	32 120	36 105
ISO 45001:2018	11 952	14 607
ISO 13485:2003 & 2016	19 472	24 123
ISO 50001:2011	18 059	46 770
ISO 20000-1:2011	5 327	7 291
ISO 22301:2012	1 506	5 282
ISO 28000:2007	617	666
ISO 39001:2012	547	1 422
ISO 37001:2016	389	1 541

Рис.2. Кількість виданих сертифікатів

Перелік посилань:

1. ISO 27001 – Система менеджменту інформаційної безпеки URL: https://academy.tms.ua/uk/sertificat-ua/standart-iso-27001-systema-menedzhmentu-informatsijnoi-bezpeky/

Ветлицька Олена Сергіївна аспірантка кафедри управління інформаційною та кібернетичною безпекою ДУІКТ, Київ, Україна

ЗАХИСТ ВБУДОВАНИХ СИСТЕМ ВІД ЗАГРОЗ БЕЗПЕКИ НА ОСНОВІ ПОВЕДІНКОВОГО АНАЛІЗУ АПАРАТНИХ КОМПОНЕНТІВ

Центральним обчислювальним компонентом на друкованій платі пристрою є мікропроцесор або мікроконтролер, він здійснює вирішення основного завдання управління, проводить обробку результатів вимірювань, виконує покладені на пристрій алгоритми. Встановлено, що атаки спрямовані на пристрої, припадають на головний обчислювальний вузол цього пристрою. З'ясовано, що для підвищення кіберстійкості пристрою, необхідно створити безпечне середовище для реалізації виконавчого коду обчислювального вузла. Задля більшої безпеки низькоресурсних вузлів використовуються програмні та апаратні підходи. Вони виконують функції захисту інформації криптографічними методами, а також виявляють аномальну поведінку пристрою та вживають заходів, що мінімізують можливу шкоду. У роботі досліджено метод підвищення кіберстійкості вбудованих систем на основі поведінкового аналізу апаратних компонентів за допомогою інтегральної мікросхеми.

Інформаційні технології давно використовують у критичних сферах людської діяльності, в яких ціна збою дуже велика. Обчислювальні системи застосовуються в медицині, енергетиці, логістиці, промисловості, системах контролю доступу та в інших сучасних галузях, що вимагають автоматизацію. Безліч датчиків і систем управління знаходяться в одній мережі, пересилають інформацію і приймають різні рішення, а також можуть мати доступ до мережі інтернет. Успішна атака на такі системи може надати зловмиснику повний контроль над кіберфізичною системою, а його дії можуть призвести до серйозних наслідків. Тому необхідно приділяти особливу увагу до безпеки кожного пристрою.

Поряд із збільшенням масштабів автоматизованих систем збільшується і складність їх компонентів. Вводяться в експлуатацію нові стеки протоколів або розширюються вже існуючі, впроваджуються нові алгоритми та механізми взаємодії між вузлами системи. Вузлом системи зазвичай є мікроконтролерний чи мікропроцесорний пристрій. Безпека систем, що входять в інформаційну систему, визначає безпеку самої інформаційної системи.

Однією з проблем, що призводить до виходу з ладу пристроїв, що вбудовуються, є низька кіберстійкість пристрою [1]. А саме властивість пристрою, що дозволяє йому існувати за умов безперервних, постійних атак. При побудові систем, що вбудовуються, здійснюється розробка електричної схеми, що зв'язує мікропроцесор або мікроконтролер з інтерфейсними мікросхемами, мікросхемами забезпечення живлення і мікросхемами системної логіки. Центральним обчислювальним компонентом на друкованій платі пристрою є мікропроцесор або мікроконтролер, він здійснює вирішення основного завдання управління, проводить обробку результатів вимірювань, виконує покладені на пристрій алгоритми. Атаки, спрямовані на пристрої, припадають на головний обчислювальний вузол цього пристрою. Тому для підвищення кіберстійкості пристрою необхідно створити безпечне середовище для реалізації виконавчого коду обчислювального вузла.

Для більшої безпеки низькоресурсних вузлів можна використовувати як програмні підходи [2, 3], так і апаратні [4]. Ці підходи виконують функції захисту інформації криптографічними методами, а також виявляють аномальну поведінку пристрою та вживають заходів, що мінімізують можливу шкоду.

В рамках роботи пропонується метод підвищення кіберстійкості вбудованих систем на основі поведінкового аналізу апаратних компонентів за допомогою інтегральної мікросхеми.

Перелік посилань:

1. Björck, F., Henkel, M., Stirna, J., Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. У: Rocha, A., Correia, A., Costanzo, S., Reis, L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham.
2. Ovasapyan T. D., Ivanov D. V. Security provision in wireless sensor networks on the basis of the trust model //Automatic Control and Computer Sciences. – 2018. – Т. 52. – №. 8. – С. 1042-1048.
3. Шкоркіна Є.М., Александрова Є.Б. Принципи реалізації симетричних криптографічних алгоритмів на малоресурсних пристроях. // Методи та технічні засоби захисту інформації. - 2020. №29. - 114-115 с.
4. Макаров А.С. Архітектура захисту мікроконтролера. // Проблеми інформаційної безпеки. Комп'ютерні системи. -2019. №2.-94-99 с.

Геселева Наталья Валеріївна
к.т.н., доцент, доцент кафедри
цифрової економіки та системного аналізу,
ДТЕУ, Київ, Україна
Рибачок Ірина Ігорівна
студентка, ДТЕУ, Київ, Україна

ШТУЧНИЙ ІНТЕЛЕКТ: ПОТЕНЦІЙНІ НЕДОЛІКИ ТА ЗАГРОЗИ

За останні кілька років штучний інтелект (далі - ШІ) набув неймовірної популярності. Він може ефективно обробляти та аналізувати великі обсяги даних, автоматизувати завдання та надавати інсайти, які покращують процес прийняття рішень та продуктивність у різних сферах. Але він також несе в собі певну небезпеку, яка стала популярною темою серед ІТ-спеціалістів та науковців з правознавства. Тож чому саме ШІ є небезпечним? І чи можна запобігти цим загрозам?

Перше, про що варто згадати, - це недостатня конфіденційність даних, які використовуються інструментами ШІ. Системи штучного інтелекту часто збирають дані для покращення користувацького досвіду або для навчання моделей штучного інтелекту. В інстаграмі виникла дискусія між художниками, які не хотіли безкоштовно віддавати свої роботи для навчання ШІ від компанії Meta, однак процедура заборони цього виявилась надто складною.

По-друге, ШІ вже використовують у сфері програмування. Він став чудовим помічником як для розробників програмного, так і апаратного забезпечення, тестувальників, аналітиків тощо. Можливості ШІ безмежні: написання коду з нуля, виправлення помилок, автоматизація завдань, оптимізація коду, переклад коду з однієї мови на іншу тощо. Але існують побоювання, що ШІ повністю замінить, наприклад, розробників програмного забезпечення. Але ці побоювання досить легко розвіяти, адже водночас інструменти генеративного ШІ мають і свої недоліки. "Сучасному ШІ все ще бракує людської креативності, інтуїції та знання предметної області, які так необхідні в програмуванні. Хоча ШІ може допомогти з багатьма завданнями кодування і навіть підвищити креативність, концептуалізація складних систем, розуміння бізнес-проблем і прийняття стратегічних рішень - це справа рук людини. Крім того, незважаючи на вражаючі результати, існує низка ризиків і викликів, пов'язаних зі штучним інтелектом, які роблять людський контроль обов'язковим, особливо коли рішення, прийняті за допомогою штучного

інтелекту, можуть мати значні наслідки для людей і суспільства" [1].

По-третє, може виникнути проблема копіювання матеріалу, який створив ШІ, студентами, копірайтерами, навіть письменниками різноманітних творів. Оскільки ШІ навчається на вже написаному та опублікованому контенті, згенерованим текстам бракує креативності, і вони можуть містити типові помилки. Однак уже існують інструменти, так звані детектори ШІ, які можуть виявити, де штучний інтелект був використаний, а де ні. Детектори контенту зі штучним інтелектом - це передові інструменти, що працюють на основі можливостей штучного інтелекту та машинного навчання, призначені для виявлення того, чи створений контент за допомогою таких інструментів, як ChatGPT, Gemini тощо [2]. Незважаючи на те, що ШІ-детектори потребують подальшого вдосконалення, вони вже досягли значного прогресу.

А як щодо органів державної влади? Адже найефективнішим методом у боротьбі зі шкідливим використанням ШІ вважається розробка правових норм. "Регулювання ШІ було в центрі уваги десятків країн, і зараз США та Європейський Союз створюють більш чіткі заходи для управління зростаючою складністю штучного інтелекту. Так, у 2022 році Офіс науково-технічної політики Білого дому (OSTP) опублікував "Білль про права ШІ" - документ, який допоможе відповідально керувати використанням і розвитком ШІ. Крім того, у 2023 році президент Джо Байден видав указ, який зобов'язав федеральні відомства розробити нові правила та інструкції щодо безпеки та захисту ШІ. Хоча правові норми означають, що певні технології ШІ з часом можуть бути заборонені, це не заважає суспільству досліджувати цю сферу" [3].

Отже, ШІ є чудовим інструментом для всіх і, схоже, стане ще більш потужним у майбутньому. Він може трансформувати майже кожну відому нам галузь і навіть створити нові. Однак людство повинно поводитися помірковано з такою потужною технологією, оскільки вона може спричинити багато проблем, якщо не бути обережними.

Перелік посилань:

1. Javier Canales Luna. Will AI Replace Programming? // Datacamp. URL: https://www.datacamp.com/blog/will-ai-replace-programming (дата звернення: 14.10.2024)
2. Pragati Gupta. 7 Best AI Content Detectors in 2024 (Free + Paid) // Writesonic. URL: https://writesonic.com/blog/best-ai-detector (дата звернення: 14.10.2024)
3. 12 Risks and Dangers of Artificial Intelligence (AI) // Builtin. URL: https://builtin.com/artificial-intelligence/risks-of-artificial-intelligence (дата звернення: 14.10.2024)

Голобородько Владислав Сергійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В БЕЗПЕЦІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

Ідентифікація користувачів за допомогою паролів або карт доступу має суттєві вразливості. Користувачі часто використовують слабкі паролі. У відповідь на це, ідентифікації обличчя як частина біометричної аутентифікації стає все більш популярною для забезпечення безпеки в інформаційних системах організацій.

Ідентифікації обличчя. Сучасні системи розпізнавання обличчя базуються на алгоритмах глибинного навчання, які дозволяють аналізувати зображення та відео в режимі реального часу (Рис.1). Вони використовують декілька ключових етапів:

1. Збір даних. Для ідентифікації користувача система спочатку отримує зображення його обличчя через камеру. Це зображення порівнюється з базою даних зареєстрованих облич.
2. Обробка та аналіз. Алгоритми машинного навчання, такі як згорткові нейронні мережі (CNN), використовуються для виявлення унікальних характеристик обличчя, таких як відстань між очима, форма носа, губ, та інші особливості. Це дозволяє створити цифровий відбиток обличчя, яка зберігається в базі даних.
3. Порівняння та ідентифікація. Після обробки зображення система порівнює цифровий відбиток з наявними у базі даних і визначає, чи належить це обличчя зареєстрованому користувачеві. У разі збігу надається доступ до інформаційної системи.

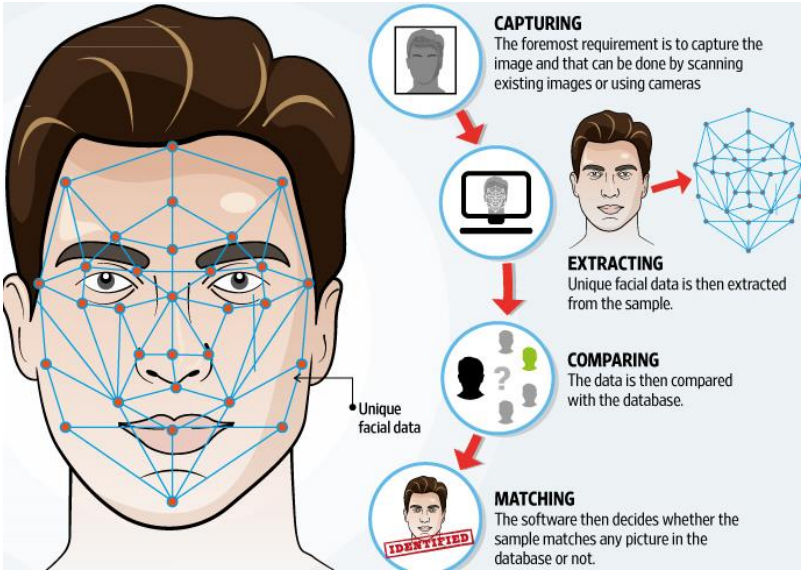


Рис.1- Ідентифікації обличчя

Безпека та виклики:

Попри високу точність, ідентифікація обличчя має певні виклики. Одним із них є захист персональних даних, оскільки біометрична інформація є конфіденційною і її втрата може мати серйозні наслідки. Іншим важливим

аспектом є помилкові результати, що можуть призвести до невірного надання даних або відмови у доступі.

Висновки:

Ідентифікація користувачів за допомогою розпізнавання обличчя є важливою частиною сучасних систем безпеки інформаційних систем організацій. Впровадження цієї технології дозволяє підвищити надійність ідентифікації та зменшити ризики несанкціонованого доступу, завдяки точності алгоритмів ШІ та можливості аналізу поведінкових і фізіологічних даних.

Перелік посилань:

1. Techniques and Challenges of Face Recognition: A Critical Review - Sciencedirect URL: https://www.sciencedirect.com/science/article/pii/S1877050918321252/pdf?md5=b3d92075cede55590f3c9bfaeb90c3b1&pid=1-s2.0-S1877050918321252-main.pdf (дата звернення 15.10.2024)
2. NIST CYBERSECURITY FRAMEWORK 2.0 URL: https://www-innovatrics-com.translate.goog/facial-recognition-technology/?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc (дата звернення 15.10.2024)

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

Інцидент-менеджмент як складова комплексу інформаційної безпеки на підприємстві

Інцидент-менеджмент є важливою складовою комплексного захисту підприємства від кібератак. Практичні підходи до реагування на інциденти включають оперативне виявлення, швидке реагування, усунення наслідків і відновлення систем. Швидка реакція на інциденти дозволяє мінімізувати шкоду, знизити фінансові втрати, захистити конфіденційні дані та забезпечити безперервність бізнесу. Крім того, аналіз інцидентів сприяє вдосконаленню системи захисту, завдяки чому організація стає менш вразливою до потенційних загроз.

У сучасному бізнес-середовищі компанії можуть щодня стикатися з різними загрозами, які можуть призвести до порушення роботи систем, втрати даних та фінансових збитків. Ефективне управління цими загрозами вимагає не лише захисту, а й чіткого реагування на події, які можуть впливати на інформаційну безпеку (ІБ). Організації важливо відрізняти і ефективно сортувати події інформаційної безпеки які, як правило, передують інциденту. Події ІБ являють собою такий стан системи, служби або мережі, що вказує на можливе порушення політики безпеки та заходів безпеки, або раніше невідому ситуацію, яка може мати відношення до кібербезпеки [1]. Події ІБ можуть з’являтися один раз чи з певною періодичністю, наприклад – лист на корпоративну електронну пошту від неавторизованого джерела, незвично високий рівень трафіку на сайт, нетипічний рівень активності авторизованого користувача – все ці події можуть перерости з події до інциденту – одного чи декілька подій ІБ, які із значною ймовірністю вказують на компрометацію бізнес-процесів чи реалізовану загрозу ІБ, наприклад:

– порушення політик, правил чи рекомендацій ІБ;
– помилки користувачів або персоналу;
– позапланові зміни в роботі систем;
– порушення правил доступу;
– системні збої та помилки в роботі програмного забезпечення (ПЗ) та технічних засобів;
– втрата пристроїв, носіїв та ін.

Такі обставини можуть завдати шкоди інформаційним активам організації, порушити її роботу, вплинути на її репутацію, мати юридичні наслідки. Ціллю управління інцидентами є мінімізація збитків для організації від витоків даних, несанкціонованого доступу, системних збоїв, кібератак та ін.

Виявлення інциденту ІБ здійснюється за рахунок моніторингу подій ІБ, їх реєстрації та подальшого аналізу. Моніторинг можна проводити як за допомогою спеціалізованого програмного забезпечення (SIEM- та DLP-систем), так і вручну. Останній варіант є доволі клопітливим, окрім того, співробітник (або група реагування) має здійснювати моніторинг цілодобово – деякі інциденти вимагають оперативних захисних дій. Окрім того, на крупних підприємствах кількість подій ІБ може сягати сотень і тисяч за добу, опрацювати такий масив даних надзвичайно важко – в таких випадках, без спеціалізованих систем не обійтись [2]. Спеціалізоване програмне забезпечення дає змогу перехоплювати, збирати та аналізувати інформацію на основі попередньо встановлених правил. Якщо відбувається порушення цих правил безпеки, система автоматично спрацьовує та надсилає повідомлення відповідальній особі для вжиття заходів і визначення рівня критичності. Журнал подій зберігається протягом заздалегідь визначеного часу.

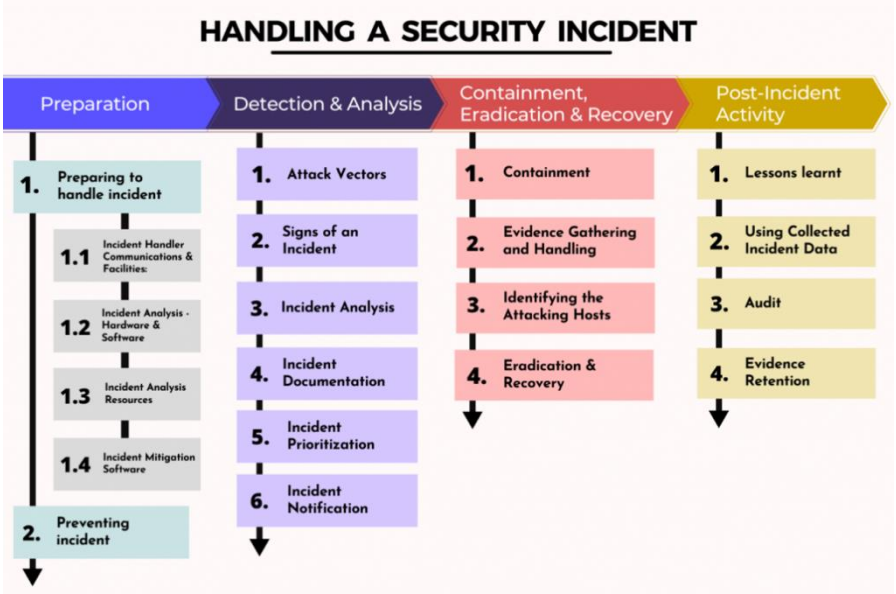


Рис.1 – настанови щодо управління інцидентами, пов'язаними з ІБ [3]

Згідно з *рис.1*, реагування на виявлений інцидент ІБ складається з:

1. Підготовка – цей етап включає документальне забезпечення: необхідно розробити і погодити детальні, зрозумілі та ефективні політики, процедури та інструкції для реагування на інциденти. Потрібно створити сценарії дій, що дозволять команді реагування виконувати визначені кроки залежно від характеру інциденту. Варто регулярно проводити тренування для відпрацювання цих кроків, а також навчати співробітників компанії та команду реагування правильним технічним і організаційним діям під час інцидентів.

2. Виявлення і класифікація - для оцінки інциденту можна використовувати заздалегідь підготовлений перелік можливих типів інцидентів інформаційної безпеки та ознак, що вказують на ймовірність їх виникнення. Ознаки можна умовно поділити на прекурсори та індикатори інцидентів інформаційної безпеки:

- прекурсори — це ознаки, що свідчать про можливість виникнення інциденту в майбутньому (наприклад, сканування портів);
- індикатори — це ознаки, які вказують на те, що інцидент уже відбувся або триває в даний момент (наприклад, сповіщення від засобів захисту інформації, виявлена шкідлива активність або збій в роботі систем).

Виявлення аномалій у мережевому трафіку та поведінці користувачів можна здійснювати за допомогою модуля аналізу поведінки користувачів і сутностей (UEBA — User and Entity Behavior Analytics), який інтегрується із системами захисту інформації (СЗІ) і системами управління інформацією та подіями безпеки (SIEM)[4].

3. Аналізування - аналітик з інформаційної безпеки перевіряє факт появи інциденту. На цьому етапі необхідно провести ідентифікацію та початкове опрацювання, визначивши тип інциденту та категорію. Визначаються кроки для ліквідації інциденту.

4. Стримування - основна мета цього етапу — мінімізувати потенційні збитки та надати час для ухвалення рішень щодо усунення загрози. Це робиться шляхом увімкнення жорсткіших правил на міжмережевому екрані для зараженого пристрою, тимчасового вимкнення деяких сервісів або функцій тощо.

5. Усунення - на цьому етапі здійснюються активні заходи для видалення загрози та запобігання повторним атакам. Це включає в себе видалення шкідливого ПЗ, блокування або змінення зламаних облікових записів (зміна паролів, увімкнення багатофакторної автентифікації), встановлення оновлень і патчів для усунення уразливостей та ін.

6. Відновлення - після видалення загрози потрібно перевірити, чи всі заходи безпеки надійно працюють. Системи повертають до нормального стану, відновлюють з резервних копій або перевстановлюють та налаштовують заново.

7. Етап висновків - аналізуються причини інциденту з метою зменшення ймовірності його повторення. Оцінюється своєчасність і правильність дій персоналу та засобів захисту, а також коригуються політики і процедури. Ведеться журналювання для покращення майбутніх реакцій на інциденти.

У процесі управління інцидентами інформаційної безпеки важливо дотримуватись чіткої послідовності дій, яка наведена вище. Ключовим аспектом є ефективна взаємодія між різними структурними підрозділами компанії та використання спеціалізованого програмного і апаратного забезпечення (як DLP та SIEM системи). Визначення подій та інцидентів інформаційної безпеки допомагає оперативно ідентифікувати потенційні загрози та правильно реагувати на них.

Важливу роль у забезпеченні безпеки відіграють центри інформаційної безпеки (SOC)[5]. Їх головні задачі – моніторинг роботи засобів захисту інформації (СЗІ) та реагування на інциденти. SOC-центри можуть бути внутрішніми (як структурний підрозділ компанії) або зовнішніми (комерційні або аутсорсингові). Фахівці цих центрів постійно контролюють повідомлення, що надходять від технічних засобів, з метою оперативного усунення загроз. Принципи роботи, організації та комплектування центрів SOC доцільно розглянути в наступних роботах.

Перелік посилань:

1. Information technology - Security techniques - Information security incident management (IDT) : ISO/IEC TR 18044:2004. – 76 с.
2. Кібератаки 2022-2023: огляд найбільших інцидентів, та що нас чекає у 2024 році [Електронний ресурс] – 2023. – Режим доступу: https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua
3. NIST SP 800-61 («Керівні настанови щодо управління інцидентами, пов’язаними з комп’ютерною безпекою»)
4. Пасєка І., Северінов О. Проблеми впровадження системи аналітики поведінки користувачів та сутностей // Харківський національний університет радіоелектроніки. – Харків: Україна, 2024. – 2 с.
5. Що таке центр інформаційної безпеки (SOC)? [Електронний ресурс] – Режим доступу: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-a-security-operations-center-soc

Городецький Ігор Олексійович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

МОБІЛЬНІ ЗАГРОЗИ: НОВИЙ ФРОНТ У КІБЕРБЕЗПЕЦІ

У нашій сучасній цифровій епосі, коли смартфони та планшети стали невід'ємною частиною нашого повсякденного життя, мобільні загрози вийшли на перший план у сфері кібербезпеки. За даними останніх досліджень, понад 60% користувачів Інтернету використовують мобільні пристрої для доступу до мережі, що робить їх привабливими цілями для зловмисників. На жаль, популярність цих пристроїв створює нові виклики для безпеки, адже багато з них не мають належного рівня захисту.

Зловмисники використовують різноманітні методи, щоб скомпрометувати мобільні пристрої. Одним із найпоширеніших способів є розповсюдження шкідливих програм, які можуть маскуватися під легітимні додатки. Наприклад, ви можете завантажити додаток, який на перший погляд виглядає корисним — калькулятор, гру або навіть банківський додаток. Проте, в реальності, він може бути заповнений шкідливим кодом, який викрадає вашу особисту інформацію або відстежує ваші дії.

Особливо небезпечним є використання відкритих Wi-Fi мереж, які часто не захищені. Підключаючись до таких мереж, ви наражаєтеся на ризик «людини посередині» (Man-in-the-Middle) атаки. Зловмисник може перехоплювати ваші дані, такі як паролі чи номери кредитних карток, під час передачі інформації. Це робить важливим впровадження протоколів шифрування, таких як VPN, що допомагає захистити вашу інформацію під час використання публічних мереж.

Крім того, соціальний інжиніринг в мобільному середовищі став новою загрозою. Зловмисники можуть надсилати вам повідомлення або дзвонити, представляючись співробітниками банку чи технічної підтримки, намагаючись отримати вашу конфіденційну інформацію. Вони можуть використовувати різні трюки, щоб викликати у вас довіру, і, якщо ви не будете обережними, ви можете стати жертвою шахрайства.

Для протидії цим загрозам важливо вжити кілька простих, але ефективних заходів. По-перше, завантажуйте додатки лише з офіційних джерел, таких як App Store або Google Play. Це знижує ризик інсталяції шкідливих програм. По-друге, регулярно оновлюйте операційну систему та додатки, оскільки виробники постійно випускають патчі безпеки, які усувають вразливості.

Також важливо використовувати надійні паролі та біометричні засоби аутентифікації, такі як відбитки пальців чи розпізнавання обличчя. Ці заходи значно ускладнюють доступ до вашого пристрою для зловмисників. А ще, встановлення антивірусного програмного забезпечення може допомогти виявити та заблокувати шкідливі програми.

Не забувайте й про важливість обізнаності. Відвідування тренінгів з кібербезпеки або читання статей про нові загрози можуть допомогти вам залишатися в курсі ситуації та розпізнавати потенційні ризики.

Отже, мобільні загрози стали новим фронтом у сфері кібербезпеки, і в нашому інтересах бути пильними та обізнаними. У світі, де технології стрімко розвиваються, важливо дотримуватися основних принципів безпеки, щоб захистити свою особисту інформацію та уникнути неприємностей. Тільки спільними зусиллями — як окремих користувачів, так і організацій — ми можемо створити безпечніше цифрове середовище для всіх.

Перелік посилань:

1. ТОП 10 загроз кібербезпеці бізнесу у 2023 році. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023 (date of access: 07.10.2024).
2. ЩОДЕННІ КІБЕРЗАГРОЗИ. URL: https://www.mil.gov.ua/ukbs/shhodenni-kiberzagrozi/ (date of access: 05.10.2024).
3. Принципи безпеки: як захистити віддалений офіс від злому. URL: https://mind.ua/publications/20218986-principi-bezpeki-yak-zahistiti-viddalenij-ofis-vid-zlomu (date of access: 04.10.2024).

Ганусяк Степан Ігорович
студент групи АІКБ, ННІЗІ ДУІКТ, Київ, Україна

Огляд ботнетів та їх життєвого циклу

Ботнет — це мережа комп'ютерів, інфікована шкідливим програмним забезпеченням. Кіберзлочинці використовують ботнет-мережі, які складаються з великої кількості комп'ютерів для різних зловмисних дій без відома користувачів.

Ботнети широко застосовуються для розсилки небажаної пошти, впровадження шпигунського ПЗ та крадіжки особистих даних користувачів. Великі мережі заражених комп'ютерів можуть бути використані для проведення розподілених атак на відмову в обслуговуванні (DDoS), які перевантажують веб-ресурси надмірним трафіком, порушуючи їх нормальну роботу.

Поширення ботнет-малвару відбувається через поштові вкладення, завантаження файлів та фальшиві програми. Кіберзлочинці також експлуатують вразливості, як-от застаріле програмне забезпечення та незахищені інтернет-з'єднання. У сучасному світі об'єктами кібератак все частіше стають не лише комп'ютери, але й інші смарт-пристрої - від камер відеоспостереження та розумних телевізорів до підключених автомобілів.

Ботнети залишаються однією з найсерйозніших кіберзагроз сучасності, що потребує детального вивчення їх життєвого циклу [1, с. 15]. Розуміння етапів розвитку ботнету дозволяє розробляти ефективні методи протидії та захисту інформаційних систем.

Життєвий цикл ботнету починається з етапу початкового зараження систем, що може відбуватися різними шляхами [2, с. 78]. Найпоширенішими методами початкового зараження є фішингові атаки, експлуатація вразливостей програмного забезпечення та соціальна інженерія.

Після успішного зараження системи відбувається встановлення шкідливого програмного забезпечення та його конфігурація [3, с. 45]. На цьому етапі бот намагається закріпитися в системі та забезпечити своє автоматичне завантаження при старті операційної системи.

Наступним кроком є підключення зараженої системи до командно-контрольної інфраструктури ботнету (C&C серверів) [4, с. 112]. Це дозволяє зловмисникам здійснювати централізоване управління мережею заражених комп'ютерів.

Важливим етапом життєвого циклу є підтримка працездатності ботнету через регулярні оновлення шкідливого коду та зміну конфігурації [5, с. 67]. Це допомагає ботнету уникати виявлення антивірусними засобами та адаптуватися до нових

умов функціонування.

Активна фаза життєвого циклу включає виконання різноманітних шкідливих дій: участь у DDoS-атаках, розсилка спаму, збір конфіденційних даних [6, с. 89]. Саме на цьому етапі ботнет завдає найбільшої шкоди.

Сучасні ботнети часто використовують складні механізми шифрування для приховування свого трафіку [7, с. 234]. Це ускладнює їх виявлення традиційними засобами мережевого моніторингу.

Для підтримки життєздатності ботнету зловмисники регулярно оновлюють списки C&C серверів та змінюють протоколи комунікації [8, с. 56]. Це забезпечує стійкість ботнету до спроб його знешкодження.

Важливою особливістю сучасних ботнетів є їх здатність до самовідновлення та реорганізації після втрати частини інфраструктури [9, с. 123]. Це досягається завдяки використанню розподілених архітектур та механізмів резервування.

Завершальним етапом життєвого циклу може бути як примусове знешкодження ботнету правоохоронними органами, так і добровільне припинення його роботи зловмисниками [10, с. 90]. Проте часто інфраструктура знешкодженого ботнету використовується для створення нових шкідливих мереж.

Перелік посилань

1. Бурячок В.Л., Толюпа С.В., Семко В.В. Інформаційна та кібербезпека: соціотехнічний аспект. Київ: ДУТ, 2020. 288 с.

2. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. Київ: Видавнича група BHV, 2019. 608 с.

3. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України. Київ: НІСД, 2021. 156 с.

4. Корченко О.Г., Терейковський І.А., Казмірчук С.В. Системи захисту інформації. Київ: НАУ, 2020. 222 с.

5. Марущак А.І. Інформаційне право: доступ до інформації. Київ: КНТ, 2019. 532 с.

6. Носов В.В., Манжай О.В. Організація та забезпечення інформаційної безпеки. Харків: ХНУВС, 2021. 216 с.

7. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації. Харків: ХНЕУ, 2019. 476 с.

8. Побережний Л.Л. Інформаційна безпека: навчальний посібник. Київ: Кондор, 2020. 290 с.

9. Скулиш Є.Д., Прокоф'єва Д.М. Основи інформаційної безпеки. Київ: НАУ, 2021. 244 с.

10. Юдін О.К., Богуш В.М. Інформаційна безпека держави. Київ: МК-Прес, 2019. 432 с.

Гончаров Максим Ігорович, БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,

м. Київ

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТА АНАЛІЗУ ЗАГРОЗ КОРПОРАТИВНИМ ДОДАТКАМ І API НА БАЗІ РІШЕННЯ AKAMAI API SECURITY

Визначено мету і основні завдання щодо виявлення та аналізу загроз корпоративним додаткам і API організації. Розглянуто зміст технології виявлення та аналізу загроз корпоративним додаткам і API організації.

У технологічному середовищі сучасних організацій, що постійно розвивається, корпоративні додатки і API займають перше місце, забезпечуючи бездоганну взаємодію між різноманітними програмними платформами. У той же час корпоративним додатки і API стикаються з різними загрозами безпеці, які можуть поставити під загрозу цілісність даних, конфіденційність і доступність інформаційних ресурсів організації. Тому, в загальному процесі забезпечення безпеки інформаційних ресурсів організацій, виявлення та аналіз загроз корпоративним додаткам і API займають відповідальне місце.

У Звіті [1] зазначається, що цифровізація бізнесу призводить до швидкого зростання трафіку API, а атаки API зростають такими ж темпами. Безпека API стала абсолютною необхідністю для підприємств, щоб захистити свої повсякденні сервіси та, що найважливіше, дані клієнтів. Однак, коли йдеться про тестування безпеки API у режимі реального часу, воно все ще відносно рідкісне: менше п’ятої частини (18%) респондентів тестують у режимі реального часу. Тим більше дивно, що впевненість у безпеці API підскочила до 94%.

Зростає не тільки інтенсивність атак, але й складність атак означає, що їх стає все важче знайти. Оскільки більше половини розробників (53%) стверджують, що витрачають від 26% до 50% свого часу на рефакторинг і виправлення API [1].

API чутливі до використання вразливостей, зловживань через автоматичні загрози, відмови в обслуговуванні, неправильної конфігурації та атак, які обходять елементи керування автентифікацією та авторизацією тощо. Завдання виявлення та аналізу загроз корпоративним додаткам і API організації дуже гостро постає перед фахівцями з кібербезпеки.

Сучасним підходом є зосередження методів та засобів захисту API на наданні трьох основних можливостей: відкриття API; керування безпекою API; захист під час виконання API (або виявлення та відповідь API). Це відповідає особливостям сучасних продуктів безпеки додатків.

За допомогою рішення Akamai API Security можна підвищити рівень безпеки API. Завдяки належним чином захищеним API команда безпеки може створювати різноманітні продукти, послуги та досвід, які будуть задовольняти потреби клієнтів.

Akamai API Security – це рішення безпеки API, яке пропонує повну видимість всіх API організації шляхом безперервного виявлення та аналізу в реальному часі (рисунок 1), допомагаючи організації повністю відповідати останнім стандартам

NIST Cybersecurity Framework 2.0 і оновленням для всебічного та повного захисту [2, 3].

NIST Cybersecurity Framework 2.0 (NIST CSF 2.0) служить довідником для організацій, які прагнуть покращити безпеку власних інформаційних ресурсів. Стандарт встановлює цілі кібербезпеки загальною мовою, упорядковані за функціями, категоріями та підкатегоріями, які застосовуються до всіх типів організацій – від малого бізнесу до глобальних підприємств. Замість того, щоб приписувати конкретні дії, NIST CSF 2.0 дозволяє організаціям визначати, як найкраще досягти цих цілей у зручний для них спосіб. Порядок цих цілей не вказує на їхню важливість. Кожна ціль є важливою частиною підтримки онлайн-безпеки.

На рисунку 1 показано як рішення Akamai API Security пропонує повний і безперервний нагляд за API, дозволяючи бачити, перевіряти, виявляти та реагувати на проблеми з безпекою API у всій версії програми.

Рішення Akamai API Security може швидко виявити всі API організації – навіть тіньові API – виявити загальні вразливості та проаналізувати поведінку API, щоб фахівці організації могли ефективніше виявляти загрози та зловживання логікою в швидкозростаючих поверхнях атак.

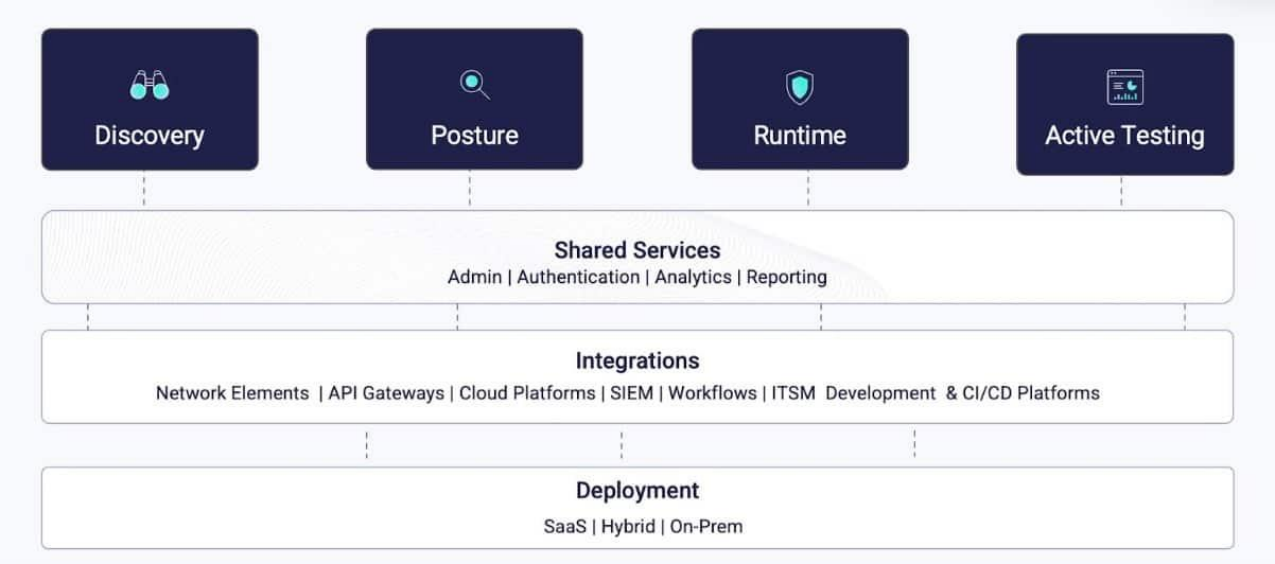


Рис. 1. Основні функції рішення Akamai API Security [2]

Треба відмітити, що не всі постачальники надають повний спектр можливостей виявлення, керування позицією та захисту корпоративних додатків і API під час виконання. Деякі постачальники зосереджені на виявленні вразливостей API і пропонують пропозиції, які включають виявлення, тестування та керування положенням. Інші постачальники зосереджені на захисті під час виконання та забезпечують початкову діяльність із виявлення та категоризації API, а потім відстежують API на наявність шкідливих подій. Постачальники все частіше намагаються усунути прогалини у своїх пропозиціях, або співпрацюючи з постачальниками, які мають додаткові пропозиції в просторі, або розширюючи власні пропозиції [4].

Отже, виявлення та пом’якшення ризиків безпеки API потребує засобів контролю безпеки, які є достатньо складними, щоб подолати складну та швидкозмінну картину загроз. Але не менш важливим є пошук шляхів поширення практик безпеки API на робочі процеси, не пов’язані з безпекою, які впливають на стан безпеки API, наприклад розробка програмного забезпечення та документування.

Перелік посилань:
1. The API Security Disconnect. Research on API security trends in 2023. Research Report. Akamai. URL: https://www.akamai.com/resources/white-paper/the-api-security-disconnect (дата звернення: 30.09.2024).
2. API Security: Reference Architecture. Akamai. URL: https://www.akamai.com/resources/reference-architecture/api-security (дата звернення: 30.09.2024).
3. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP. 29 February 26, 2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення: 30.09.2024).
4. Dionisio Zumerle, Aaron Lord. Market Guide for API Protection, Gartner, 29 May 2024. URL: https://www.gartner.com/doc/reprints?id=1-2I1D4OJD&ct=240708&st=sb (дата звернення: 30.09.2024).

Грімов Денис Геннадійович, БСДМ-63
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНИХ ДОДАТКІВ ВІД ВРАЗЛИВОСТЕЙ НА БАЗІ IMPERVA RASP

Визначено мету і основні завдання щодо виявлення та аналізу загроз корпоративним додаткам і API організації. Розглянуто зміст технології виявлення та аналізу загроз корпоративним додаткам і API організації.

В [1] зазначається, що останнім часом забезпечення безпеки додатків набула власної форми. У той же час, досі немає єдиного стандартного визначення поняття «забезпечення безпеки додатків». Gartner [1, 2] визначає самозахист додатків під час виконання (Runtime Application Self-Protection, RASP) як «технологію безпеки, яка вбудована або пов’язана з додатком чи середовищем виконання додатку та здатна контролювати виконання додатка, а також виявляти та запобігати атакам у реальному часі».

Самозахист додатків під час виконання (RASP) – це інструмент, який може виявляти атаки на додатки під час їх реалізації. Застосування технології RASP може захистити додатки від шкідливих даних і поведінки шляхом аналізу їх поведінки додатків. Якщо поведінка додатка вказує на те, що щось не так, RASP може допомогти зупинити загрозу [3].

Інструмент безпеки RASP контролює додаток, для захисту якого він призначений. RASP працює як мережевий пристрій, але всередині додатка. Незважаючи на те, що RASP не вносить зміни в код додатків, він може

контролювати те, що робить додаток. Завдяки цій можливості RASP може швидко зупинити загрозу до того, як вона завдасть значної шкоди [3].

Наприклад, технологія RASP може зупинити атаки впровадження SQL ін'єкції, запобігаючи виконанню шкідливих інструкцій у базі даних додатка. У цьому типі атаки зловмисник вводить код у додаток, який може вплинути на роботу бази даних. Але оскільки система RASP може виявляти такі атаки, вона може запобігти виконанню шкідливого коду базою даних. Як наслідок, просте рішення RASP може захистити конфіденційну інформацію в базі даних [3].

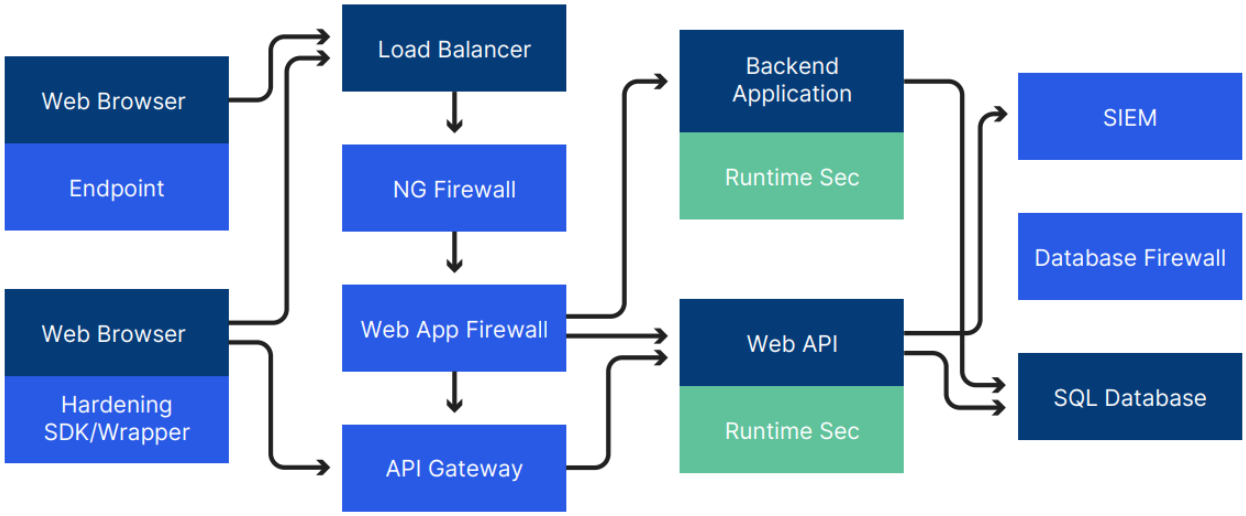


Рис. 1 Приклад веб-додатків, які можуть використовуватися організацією [1]

В [1] зазначається, що більшість організацій сьогодні мають як застаріле, так і нове програмне забезпечення, яке керує їхнім бізнесом, і ці додатки знаходяться в складному середовищі, що охоплює мережу, сам додаток, базу даних і операційну систему. Завдяки додаткам як локальним, так і хмарним, організації перебувають у різних станах цифрової трансформації. Чим старше підприємство, тим більше фрагментоване його середовище.

Фрагментація відбувається в середовищі розробника або DevOps з кількома мовами (JAVA, .NET, Node.js тощо) і кількома базами даних. Фрагментація також спостерігається в безпеці додатків із кількома й часто різними рівнями контролю безпеки, починаючи від статичного, динамічного та інтерактивного тестування безпеки (SAST, DAST, IAST) до самозахисту додатків під час виконання (RASP), а також а захисту периметра на основі мережевих екранів і екранів веб-додатків (WAF) [1].

Національний інститут стандартів і технологій (NIST) визначає самозахист додатків під час виконання (RASP) як засіб керування для зменшення ризику через уразливості безпеки програмного забезпечення. RASP важливий не лише через свою власну функцію, але й у тому, як він відрізняється від інших технологій в екосистемі та/або взаємодіє з ними. Найчастіше RASP доповнює і навіть підвищує ефективність інших засобів.

Усі технології RASP повинні мати можливість працювати в двох різних, але взаємодоповнюючих режимах: моніторингу та захисту [1].

У режимі пасивного моніторингу рішення RASP має використовувати дуже обмежені ресурси додатка, такі як процесор і пам'ять (RAM). Це також має додати мінімальну затримку.

У режимі моніторингу RASP повинен мати можливість генерувати подібні події журналювання, якби він був у режимі активного захисту. Це дозволяє організаціям створювати або отримувати доступ до аналітичного звіту безпеки або «теплової карти» того, де реальні атаки вражають додаток [1].

У режимі активного захисту рішення RASP має використовувати обмежені ресурси додатка для виявлення загроз, одночасно автоматично пом'якшуючи атаки в режимі реального часу та запобігаючи викраденню бази даних. RASP не повинно вимагати значних ресурсів для налаштування чи конфігурації або громіздких наборів правил чи списків визначень. Це повинно додати мінімальну затримку до додатка. У режимі активного захисту RASP має генерувати дієві дані про атаки в реальному часі, а також про те, які дії було виконано для нейтралізації шкідливого або неправильного корисного навантаження [1].

Рішення RASP має два унікальні технічні компоненти: аналіз безпеки та впровадження аналітичного процесора прикладного рівня. Технічна оцінка будь-якого рішення RASP повинна обговорювати переваги та слабкі сторони кожного компонента як окремо, так і разом.

Аналіз загроз додатка – те, як атаки на безпеку виявляються, обчислюються та згодом пом'якшуються, є одним із найважливіших атрибутів RASP, оскільки це впливає на точність і продуктивність, а також на впровадження. Наприклад, загальною проблемою засобів контролю безпеки додатків є поширеність помилкових спрацьовувань і помилково негативних результатів, які виснажують ресурси та створюють величезну кількість шуму.

Чотири основні методології для обчислення атак – це зіставлення шаблонів, евристика, аналіз потоку даних і теоретико-мовна безпека (language-theoretic security, LANGSEC). Кожне рішення RASP виконує аналіз загроз за допомогою іншого підходу (іноді комбінованого) [1].

Реалізація аналітичного процесора може бути шляхом [1]:

використання WAF або проксі для аналізу всього трафіку на відомі загрози безпеці;

втілення інструмента в додаток за допомогою агентів/модулів для перевірки даних під час функціонування;

заміни самої віртуальної машини на таку, яка виконує функції безпеки.

Сервіси RASP зазвичай реалізуються за допомогою другого та третього методів залежно від кількох впливових факторів, таких як постачальник, вимоги до продуктивності, підтримка мови, доступні мережеві та сервісні ресурси та очікуваний результат. Інструменти програми для виконання функцій безпеки (у цьому випадку самозахист під час виконання) включають модифікацію самого

додатка шляхом додавання коду, наприклад, за допомогою плагіна на основі фреймворку [1].

На додаток до плагінів Java і .NET у формі агентів і модулів, продукт на основі RASP має бути простим у розгортанні, обслуговуванні та контролі. Після розгортання RASP має бути швидкою розподіленою системою, що складається з ряду модульних служб, які аналізують і перевіряють усі вхідні дані без будь-яких залежностей від визначень, шаблонів, регулярних виразів, аналізу дефектів або поведінкового навчання.

Для роботи рішень RASP не потрібен сервер команд і керування. Однак якщо сервер існує, він повинен надавати можливість увімкнути та вимкнути функції RASP і перемикатися між режимами моніторингу та захисту без перезавантаження сервера додатків. Сервери RASP повинні мати можливість розгортання на місці, у віртуальних середовищах і в загальнодоступних/приватних хмарах.

Отже, технологія RASP є потужним та інноваційним компонентом для підвищення безпеки корпоративних додатків, враховуючи збільшення кількості розгортань програмного забезпечення та розподілених архітектур додатків організацій. Завдяки технології RASP фахівці з кібербезпеки можуть протистояти атакам під час функціонування додатків та досліджувати способи вбудовування функцій безпеки в них.

Організації, які використовують технологію RASP, зараз отримують потужну інформацію та приймають розумніші рішення щодо розробки додатків, їх безпеки та усунення вразливостей, які мають місце.

Перелік посилань:

1. A Guide to Runtime Application Self-Protection (RASP). Whitepaper. Imperva. URL: https://www.imperva.com/resources/whitepapers/Imperva-A-Guide-to-RASP.pdf (дата звернення: 30.09.2024).

2. How RASP Technology Protects Applications. Cisco AppDynamics. URL: https://www.appdynamics.com/learn/how-rasp-protects-apps (дата звернення: 30.09.2024).

3. What Is Runtime Application Self-Protection (RASP)? Fortinet. https://www.fortinet.com/resources/cyberglossary/runtime-application-self-protection-rasp (дата звернення: 30.09.2024).

Дєдіщев Денис Олегович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

ВРАЗЛИВОСТІ IOT: НЕБЕЗПЕКА БЕЗПОСЕРЕДНЬО У ВАШОМУ ДОМІ

В останні роки Інтернет речей (IoT) став невід'ємною частиною нашого повсякденного життя. Різноманітні пристрої, від смарт-термометрів до розумних дверних замків, покликані зробити наше життя зручнішим і ефективнішим. Проте, разом з перевагами, IoT також приносить із собою серйозні виклики у сфері інформаційної безпеки. Вразливості IoT можуть стати небезпекою безпосередньо у вашому домі, відкриваючи двері для зловмисників.

Один із найголовніших аспектів вразливостей IoT полягає в тому, що багато з цих пристроїв не мають належного рівня захисту. Часто їх виробники економлять на заходах безпеки, що призводить до наявності слабких паролів, відсутності оновлень прошивки та ненадійних систем шифрування. Ці недоліки роблять пристрої легкими цілями для кібератак. Наприклад, зловмисник може використати слабкий пароль для доступу до вашого смарт-термометра, отримуючи таким чином контроль над всією вашою домашньою мережею.

Однією з найпоширеніших атак на IoT-пристрої є атака типу "людина посередині", коли зловмисник перехоплює інформацію між вашим пристроєм і його сервером. У таких ситуаціях зловмисник може отримати доступ до ваших особистих даних або навіть відстежувати ваші дії в режимі реального часу. Це особливо небезпечно, якщо мова йде про пристрої, пов'язані з безпекою вашого дому, такі як відеокамери або системи сигналізації.

Крім того, IoT-пристрої часто збирають величезну кількість даних про користувачів, включаючи інформацію про їх повсякденні звички, місцезнаходження і навіть фінансові дані. У разі компрометації таких пристроїв, ця інформація може потрапити до рук зловмисників, які можуть використати її для здійснення шахрайства або навіть стеження за вами.

Для мінімізації ризиків, пов'язаних з вразливостями IoT, важливо вжити кілька заходів. По-перше, завжди змінюйте стандартні паролі на надійні та унікальні. Використання комбінацій букв, цифр та спеціальних символів ускладнить завдання зловмисникам. Також важливо регулярно перевіряти наявність оновлень прошивки для ваших пристроїв, оскільки виробники часто випускають патчі безпеки для усунення вразливостей.

Використання надійних мережевих заходів, таких як фаєрволи та сегментація мережі, також може суттєво підвищити рівень безпеки. Наприклад, ви можете відокремити IoT-пристрої від основної домашньої мережі, щоб знизити ризик доступу зловмисників до ваших персональних даних. Це особливо корисно, якщо ви маєте кілька IoT-пристроїв, які можуть бути скомпрометовані.

Не менш важливим є і моніторинг активності ваших пристроїв. Встановлення програмного забезпечення для виявлення шкідливих дій допоможе вчасно виявити та заблокувати потенційні загрози. Багато сучасних антивірусних програм мають функції для перевірки безпеки IoT-пристроїв, що дозволяє виявити незвичні активності.

Отже, вразливості IoT становлять серйозну загрозу, що безпосередньо стосується кожного з нас. У світі, де технології постійно розвиваються, важливо бути свідомими цих загроз і вживати заходів для забезпечення безпеки своїх

пристроїв. Лише спільними зусиллями, обізнаністю та впровадженням надійних практик безпеки ми зможемо забезпечити безпечне цифрове середовище в наших домівках.

Перелік посилань:

1. Виклики безпеки IoT: нові рішення та кращі практики. URL: https://itcluster.lviv.ua/itid/vyklyky-bezpeky-iot-novi-rishennya-ta-krashhi-praktyky/ (date of access: 07.10.2024).
2. Поширені атаки на IoT та захист від них. URL: https://corewin.ua/blog/attacks-on-iot-how-protect/ (date of access: 05.10.2024).
3. Кіберзагрози для інтернету речей (IoT): захист смарт-пристроїв. URL: https://wezom.com.ua/ua/blog/kiberzagrozi-dlya-internetu-rechey-iot-zahist-smart-pristroyiv (date of access: 04.10.2024).

Діденко Данило Юрійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

АКТУАЛЬНІСТЬ ВИКОРИСТАННЯ DLP СИСТЕМ ДЛЯ ЗАПОБІГАННЯ ТА ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ВИТОКУ ДАНИХ

У сучасних умовах цифрової трансформації та зростання обсягу інформації, організації зустрічаються з безпрецедентними викликами у забезпеченні захисту конфіденційних даних. Несанкціонований витік інформації може призвести до серйозних фінансових, репутаційних і юридичних наслідків, що робить питання захисту даних критично важливим.

Запобігання витоку даних (DLP Data Leak Prevention)[2] — це ключовий компонент кібербезпеки будь-якої організації, спрямований на виявлення та запобігання несанкціонованій передачі конфіденційної інформації за межі компанії. Рішення DLP проводять моніторинг, виявляють і блокують чутливі дані під час використання (на кінцевих точках), у русі (мережевий трафік) та в стані спокою (зберігання).

Поняття витоку даних

Перш ніж заглиблюватися в методи запобігання та виявлення, важливо зрозуміти, що таке витоки даних, їхній потенційний вплив на організацію та поширені причини виникнення.

Виток даних відбувається, коли конфіденційна або захищена інформація випадково або навмисно розкривається несанкціонованим особам.

Витоки даних можуть мати різні форми, наприклад:

• Випадкове поширення конфіденційної інформації співробітниками;

• Неправильна конфігурація хмарного сховища або баз даних, що призводить до публічного доступу;

• Внутрішні загрози, коли зловмисний працівник або підрядник краде або розголошує дані;

• Кібератаки, під час яких зовнішні зловмисники отримують доступ до системи та викрадають дані;

Витоки даних можуть мати серйозні наслідки для організацій, зокрема:

• Фінансові втрати через штрафи, позови та витрати на відновлення;

• Репутаційні збитки, що призводять до втрати клієнтів, партнерів і інвесторів;

• Втрата інтелектуальної власності та комерційних таємниць;

• Юридичні та регуляторні покарання за недотримання законів про захист даних.

Поширені причини витоків даних

Розуміння основних причин витоків даних є важливим для впровадження ефективних заходів запобігання. До найпоширеніших причин належать:

• Людська помилка: співробітники можуть ненавмисно поділитися конфіденційною інформацією через електронну пошту або інші канали зв’язку, загубити пристрої з важливими даними або стати жертвами соціальної інженерії;

• Слабкі заходи безпеки: недостатній контроль доступу, незашифровані дані та застаріле програмне забезпечення можуть підвищувати ризик витоку даних організації;

• Внутрішні загрози: невдоволені або негативно налаштовані співробітники можуть навмисно викрадати або розголошувати конфіденційні дані;

• Кібератаки: передові загрози, програми-вимагачі та інші кіберзагрози можуть спричинити витоки даних у разі порушення оборонних заходів організації.

Основні компоненти запобігання витоку даних

1. Інспекція контенту та контекстуальний аналіз:

Системи DLP перевіряють дані на наявність чутливої інформації та аналізують контекст їх використання чи передачі. Це включає сканування даних на предмет певних шаблонів, таких як номери кредитних карток, медичні записи чи особисту ідентифікаційну інформацію (PII), забезпечуючи їх конфіденційність і відповідність законам про приватність. Рішення DLP використовують передові алгоритми для ідентифікації та захисту різних типів чутливих даних, забезпечуючи дотримання глобальних норм конфіденційності, таких як GDPR, HIPAA та PCI DSS.

2. Моніторинг активності користувачів:

Моніторинг того, як користувачі взаємодіють із конфіденційними даними, допомагає виявляти потенційні витоки, як випадкові, так і зловмисні дії внутрішніх користувачів. Рішення DLP впроваджують детальний моніторинг активності користувачів, забезпечуючи уявлення про те, як обробляються чутливі дані, і в реальному часі попереджає про ризики витоку.

3. Забезпечення дотримання політик:

Інструменти DLP забезпечують виконання політик безпеки, які визначають, які дані можна передавати, ким і через які канали. DLP дозволяє компаніям визначати й реалізовувати власні політики передачі даних, забезпечуючи повний контроль над потоками конфіденційної інформації.

Основні практики впровадження запобігання витоку даних

- Розробка комплексної політики: встановіть чіткі правила, що визначають, які дані вважаються конфіденційними, і протоколи їх обробки.
- Регулярні аудити та оновлення: проводьте періодичні аудити практик DLP і оновлюйте їх для адаптації до нових загроз і змін в операційній діяльності.
- Освіта та навчання співробітників: співробітників слід навчати протоколам обробки даних і важливості безпеки даних.
- Інтеграція з іншими засобами безпеки: DLP повинна працювати спільно з іншими заходами безпеки, як-от шифрування, системи виявлення вторгнень і брандмауери, для забезпечення багаторівневого захисту.

Висновок

Використання DLP-систем є надзвичайно актуальним для сучасних організацій, оскільки вони забезпечують ефективний захист від несанкціонованого витоку даних, що є серйозною загрозою для бізнесу. Завдяки моніторингу, контролю доступу та виявленню підозрілих дій, DLP допомагає запобігти як зовнішнім, так і внутрішнім загрозам. У світлі зростання кількості кіберзагроз і необхідності дотримання регуляторних вимог, DLP-системи виступають важливим інструментом для збереження цілісності та конфіденційності критичних даних, роблячи їх впровадження важливим компонентом інформаційної безпеки.

Перелік використаних джерел:

1. What are the benefits and challenges of using data leakage detection and prevention (DLP) tools? URL: https://www.linkedin.com/advice/0/what-benefits-challenges-using-data-leakage-detection
2. Data Leak Prevention vs Data Loss Prevention: A Comprehensive Guide to Secure Your Data URL: https://www.endpointprotector.com/blog/data-leak-prevention-vs-data-loss-prevention-guide/
3. NIST Data Loss Prevention URL: https://www.nist.gov/publications/data-loss-prevention
4. 8 Data Leak Prevention Strategies in 2024 URL: https://www.upguard.com/blog/data-leak-prevention-tips#:~:text=%E2%80%8DData%20leak%20prevention%20is,easy%20attack%20vector%20for%20cybercriminals.

Дяченко Владислава Анатоліївна
Студентка ТСДМ -51

ІНТЕГРАЦІЯ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ РОЗВИТКУ ТЕХНОЛОГІЇ «РОЗУМНОГО» МІСТА

Інтернет речей можна вважати новим етапом розвитку Інтернету, де відбувається обмін даними між підключеними фізичними об'єктами, кожен з яких здатний самостійно взаємодіяти з мільярдами інших пристроїв. IoT надає можливість людям дистанційно виконувати різноманітні завдання, що значно полегшує повсякденне життя.

Інтернет речей швидко знайшов застосування в багатьох сферах. Його використовують у системах «розумний» будинок, транспортних системах та концепціях «розумних» містах. Завдяки цій технології промислові структури та системи охорони здоров'я досягли нового рівня розвитку, отримавши змогу кращого контролю над численними процесами та структурами.

«Розумне» місто — це урбаністичний простір, який використовує передові технологічні рішення для розв’язання міських проблем, таких як транспортна система, планування інфраструктури, доступ до медичних послуг, ефективна система адресації будинків тощо. Головним чинником розвитку «розумного» міста є застосування інформаційно-комунікаційних технологій для подолання викликів в межах міської території.

Технологія IoT може значно покращити керування та оптимізацію традиційних громадських послуг, таких як транспорт, паркування, освітлення, моніторинг громадських місць, збереження культурної спадщини, збір сміття, підтримання санітарного стану в лікарнях і школах. Крім того, доступність різноманітних даних, зібраних за допомогою міської IoT, може бути використана для підвищення прозорості, підтримки дій місцевої влади, підвищення обізнаності громадян про стан міста, залучення їх до управління громадськими справами, а також створення нових послуг на основі IoT.

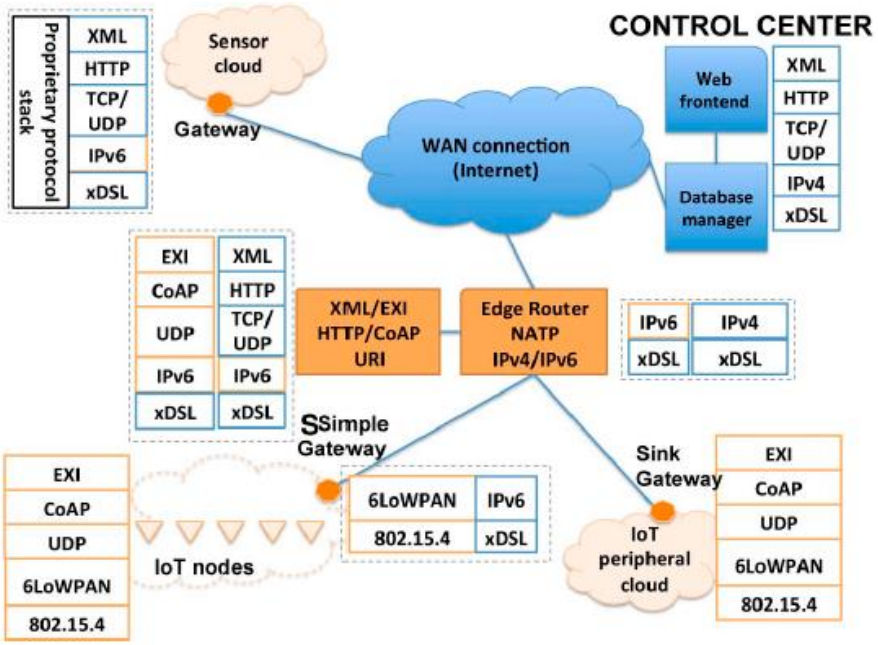


Рис. 1. Архітектура системи міської IoT з використанням різнорівневих протоколів для передачі даних

Більшість сервісів «Розумного міста» базуються на централізованій архітектурі. Різноманітні периферійні пристрої, розміщені по всьому місту, генерують різні типи даних, які передаються через відповідні комунікаційні технології до контрольного центру для їх подальшого зберігання та обробки.

Головною особливістю такої IoT інфраструктури є здатність інтегрувати різноманітні технології з існуючими комунікаційними інфраструктурами, підтримуючи поступову еволюцію IoT із підключенням нових пристроїв та впровадженням нових функцій і послуг. Важливим аспектом є також необхідність забезпечення доступу до зібраних даних для органів влади та громадян з метою підвищення їхньої обізнаності про міські проблеми і стимулювання активної участі в громадських справах.

Рис.1. демонструє зв'язки між різними IoT вузлами, шлюзами, периферійними хмарними сервісами та центральним контролюючим центром, а також протоколи, що використовуються на різних етапах комунікації.

Одним із основних чинників передачі даних у «розумних» містах є оптимізація процесу прийняття рішень у потрібний момент. Це означає, що дані, зібрані з датчиків, аварійних кнопок або сенсорів, а також камер спостереження, збираються та обробляються в режимі реального часу.

Технологія Інтернету речей (IoT) є основою для розвитку «розумних» міст, забезпечуючи ефективний збір і обробку даних у режимі реального часу. Це дозволяє оптимізувати надання громадських послуг, покращувати інфраструктуру та підвищувати прозорість і залучення громадян до управління містом. Центральна роль у цьому належить інформаційно-комунікаційним технологіям, які інтегрують різні пристрої та сервіси, створюючи більш стійкі та ефективні урбаністичні

простори.

Перелік посилань:
1. Internet of Things architecture. [Електронний ресурс] – Режим доступу: https://www.ibm.com/cloud/architecture/architectures/iotArchitecture.
2. P. Rawat, K. Deep, S. Chaudhary. A Review on Internet of Things: Architecture, Security and Future Challenges. IEEE Access. Vol. 9, 2021, pp. 21376-21395.
3. A. Chaudhary, R. Kumar. IoT Applications for Smart Cities: A Survey. Journal of King Saud University - Computer and Information Sciences. 2022. [Електронний ресурс] – Режим доступу: https://doi.org/10.1016/j.jksuci.2022.01.002
4. L. Zhang, Y. Yang, S. Zhang, Z. Wang. Internet of Things Security and Privacy: Architecture, Applications, and Research Directions. IEEE Internet of Things Journal. Vol. 8, 2021, pp. 9646-9660.

Єкімов Іван Віктрович
Студент групи БСДМ-63,ННІЗІ ДУІКТ, Київ, Україна

Менеджмент інформаційної безпеки

У сучасному світі інформаційні технології є основою бізнесу, державного управління та соціальної взаємодії. Підвищення залежності від інформаційних систем та зростання обсягів оброблюваних даних створює нові загрози для інформаційної безпеки. У цьому контексті актуальним є менеджмент інформаційної безпеки (ІБ), який охоплює комплекс заходів і практик, спрямованих на захист інформаційних ресурсів організації від загроз, ризиків і вразливостей.

Менеджмент інформаційної безпеки – це систематичний процес управління ризиками, пов'язаними з інформаційними ресурсами організації, з метою забезпечення їх конфіденційності, цілісності та доступності. Він охоплює як технічні, так і організаційні аспекти, враховуючи сучасні вимоги нормативних актів і стандартів.

Рис. 1 – менеджмент інформаційної безпеки

До основних компонентів менеджменту ІБ належать: оцінка ризиків, розробка політик безпеки, контроль доступу, моніторинг та аудит, а також навчання співробітників. Оцінка ризиків дозволяє аналізувати можливі загрози та вразливості інформаційних систем. Політики безпеки створюють рамки внутрішніх правил і процедур захисту інформації. Контроль доступу забезпечує обмеження на доступ до даних відповідно до ролей і завдань. Моніторинг та аудит гарантують постійний контроль стану інформаційної безпеки, а навчання співробітників підвищує їх обізнаність у сфері кіберзагроз і методів захисту.

Центральним аспектом інформаційної безпеки є управління ризиками. Він складається з ідентифікації загроз, оцінки вразливостей, аналізу впливу інцидентів і реалізації заходів зниження ризиків. Ідентифікація загроз дозволяє виявити потенційні джерела загроз, такі як кіберзлочинці, технічні збої або помилки персоналу. Оцінка вразливостей фокусується на слабких місцях систем, а аналіз впливу – на наслідках можливих інцидентів. Заходи зниження ризиків можуть включати шифрування даних, резервне копіювання або системи відновлення після інцидентів.

Для досягнення високого рівня захисту важливим є використання міжнародних стандартів. Найвідомішим є ISO/IEC 27001[1], який визначає вимоги до систем управління інформаційною безпекою (СУІБ). Він дозволяє організаціям структуризувати процеси захисту інформації та підвищити ефективність управління.

Розвиток нових технологій, таких як хмарні обчислення, Інтернет речей або штучний інтелект, створює нові виклики для інформаційної безпеки. Інтеграція цих технологій у сучасні системи захисту стає все більш важливою. Постійне вдосконалення системи управління інформаційною безпекою дозволить адекватно реагувати на нові загрози.

Менеджмент інформаційної безпеки є основним механізмом захисту інформаційних ресурсів в умовах зростаючих загроз і викликів. Ефективне управління безпекою сприяє мінімізації ризиків втрат даних, збереженню стабільної роботи організацій та захисту їхньої репутації.

Перелік посилань :
1. Стаття від TIC-UKRAINE по темі «Розробка основи стратегії аналізу ризиків для оцінки впливу в системах управління інформаційної безпеки»
https://tic-ua.com/uk/statti/rozrobka-osnovy-strategiyi-analizu-ryzykiv-dlya-oczinky-vplyvu-v-systemah-upravlinnya-informaczijnoyi-bezpeky-pryklad-z-industriyi-it-konsaltyngu-chastyna-1/ [2с зі статі]

Єрьоменко Микита Олексійович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ОСНОВНІ НЕДОЛІКИ ТЕХНОЛОГІЇ ЗАБЕСПЕЧЕННЯ ШИФРОВАНОЇ КОМУНІКАЦІЇ МІЖ ПРИСТРОЯМИ МЕРЕЖІ LORAWAN

LoRaWAN (Long Range Wide Area Network) на сьогоднішній день є однією з найпоширеніших технологій для забезпечення бездротового зв'язку в системах Інтернету речей (IoT) і не тільки. Її популярність зростає завдяки можливості передавати дані на великі відстані з низьким енергоспоживанням. Однак одним із головних недоліків LoRaWAN є використання алгоритму симетричного шифрування, що знижує рівень безпеки і ускладнює процес створення захищеної комунікації. Це також створює ризик для цілісності та конфіденційності даних, оскільки компрометація ключа може призвести до несанкціонованого доступу до мережі.

LoRa (Long Range) — це технологія бездротової модуляції, яка дозволяє передавати дані на великі відстані (до 10-15 км у сільській місцевості) при низькому енергоспоживанні. Вона особливо ефективна для пристроїв Інтернету речей (IoT), які не потребують високої швидкості передачі даних, але працюють в умовах, де критичними є тривалий час автономної роботи та передача інформації на великі відстані. Проте базова технологія LoRa не має вбудованих засобів для забезпечення високого рівня захисту данихю.

Для підвищення рівня безпеки в мережах, побудованих на основі LoRa, була створена технологія LoRaWAN (Long Range Wide Area Network), яка додає мережевий рівень для керування пристроями та їх захисту. LoRaWAN використовує симетричне шифрування AES-128 для захисту даних під час їх передачі між пристроями і мережею. Ця система забезпечує двоетапну автентифікацію — мережеву й прикладну — що ускладнює несанкціонований доступ до даних або втручання в роботу мережі. Хоча цей захист є ефективнішим за базовий захист технології LoRa, однак симетричне шифрування має свої недоліки та накладає обмеження на нецентралізоване управління та маштабування таких мереж.

Принцип забезпечення шифрованої комунікації в LoRaWAN ґрунтується на використанні симетричного шифрування з ключем AppKey, який зазвичай видається виробником пристрою під час його виготовлення. Цей ключ закодований в пристрої і використовується для шифрування даних у мережі LoRaWAN. Для забезпечення можливості приєднання пристрою до мережі, такий самий AppKey має зберігатись і на мережевому сервері тієї мережі, до якої пристрій намагається приєднатись.

Під час приєднання пристрою до мережі, через процес "активація через підтвердження", мережевий сервер та пристрій використовують заздалегідь збережений AppKey для генерації двох інших ключів: Network Session Key (NwkSKey) та Application Session Key (AppSKey).

Ключ NwkSKey відповідають за шифрування комунікації між пристроєм і мережевим сервером. В той час як AppSKey використовується для захищеного

зв’язку між кінцевим пристроєм та сервером застосунків.

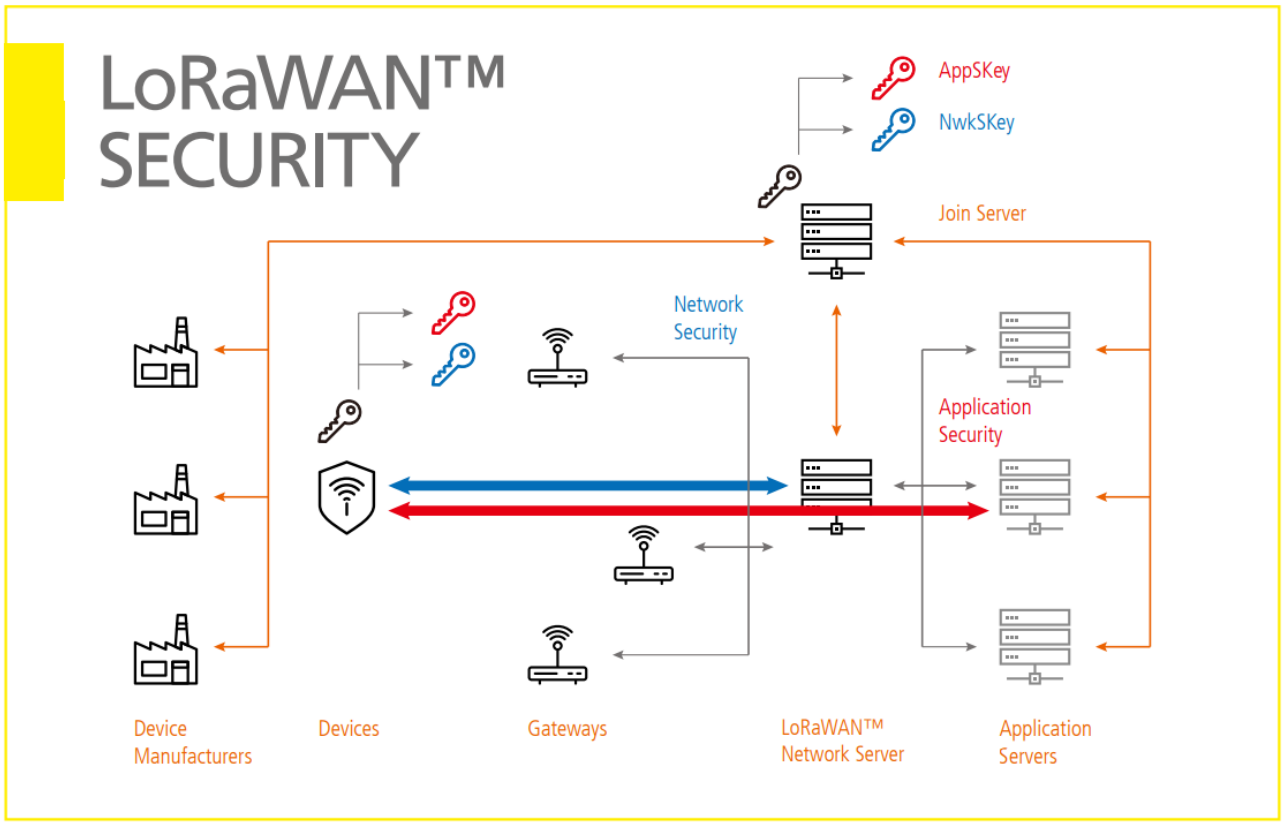


Рис.1 - Діаграма процесу приєднання пристрою до мережі LoRaWAN

Як можна побачити, така система хоч і забезпечує шифрований зв’язок, але має свої обмеження у вигляді необхідності предзберігання AppKey на обох сторонах з’єднання, що значно ускладнює створення нецентралізованої системи на основі LoRaWAN. До того ж надійне зберігання AppKey є критично важливим для безпеки всієї системи, оскільки компрометація цього ключа може призвести до втрати конфіденційності даних.

Для вирішення цієї проблеми може бути використаний алгоритм шифрування з відкритим ключем. Алгоритм шифрування з відкритим ключем (асиметричне шифрування) працює на основі двох математично пов'язаних ключів: відкритого ключа (public key) та приватного ключа (private key). Ці ключі створюються разом, але мають різні функції. Приватний ключ зберігається в таємниці і використовується для дешифрування даних, а відкритий ключ може бути відкрито переданий будь-кому для шифрування передаваємого повідомлення. Такий підхід гарантує безпеку комунікації навіть у разі перехоплення відкритого ключа, оскільки без приватного ключа дешифрування неможливе. Алгоритми, які використовуються для цього методу, включають RSA, ECC (еліптичні криві), та інші.

Такий підхід усуває необхідність завчасного зберігання симетричних ключів на обох сторонах, замінюючи їх динамічно генеруючеюся парою відкритого та

приватного ключів при під’єднанні пристрою до мережі. Це дозволяє уникнути проблем, пов'язаних із компрометацією AppKey, оскільки навіть у разі перехоплення відкритого ключа зловмисник не зможе дешифрувати дані без приватного ключа.

Впровадження шифрування з відкритим ключем підвищить безпеку та надійність систем побудованих на основі LoRa, дозволяючи створювати більш децентралізовані системи. Однак, через обмежену обчислювальну потужність пристроїв IoT, цей підхід потребує оптимізації, щоб зберегти енергоефективність і продуктивність мережі.

Перелік посилань:

1. LoRaWAN Security Whitepaper. URL: https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf (дата звернення: 05.10.2024)
2. Asymmetric Key Cryptography. URL: https://www.geeksforgeeks.org/asymmetric-key-cryptography/ (дата звернення: 08.10.2024)

Забенко Ілля Олексійович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

ЗАГАЛЬНА СИСТЕМА ОЦІНКИ ВРАЗЛИВОСТЕЙ (CVSS): ВЕКТОР РОЗВИТКУ МЕТРИК У ВЕРСІЇ 4.0

У сучасному цифровому світі кількість кібератак та загроз стрімко зростає. Саме тому для спеціалістів з кібербезпеки у компаніях дуже важливо розрахувати серйозність, вірогідність і складність вразливостей та відсортувати їх за рівнем їхньої загальної небезпечності для компанії. Це дуже важливий процес, що дозволяє зосередити увагу на вирішенні найнебезпечніших проблем інформаційно-комунікаційної системи та вчасно запобігти їм не відволікаючись на вирішення не серйозних або малоймовірних загроз.

CVSS - відкритий стандарт, розроблений Національною консультативною радою з інфраструктури США. Він використовується в кожній організації, де є процес управління вразливістю, завдяки якому у свою чергу забезпечується результативна кібербезпека. Саме тому необхідно, щоб фахівці центру протидії кіберзагроз могли розрахувати рівень небезпеки вразливостей.

У новій версії стандарту CVSS змінилася номенклатура. На відміну від попередньої, де було три групи показників, нова версія має чотири: базові метрики, метрики загроз, метрики середовища та додаткові метрики.

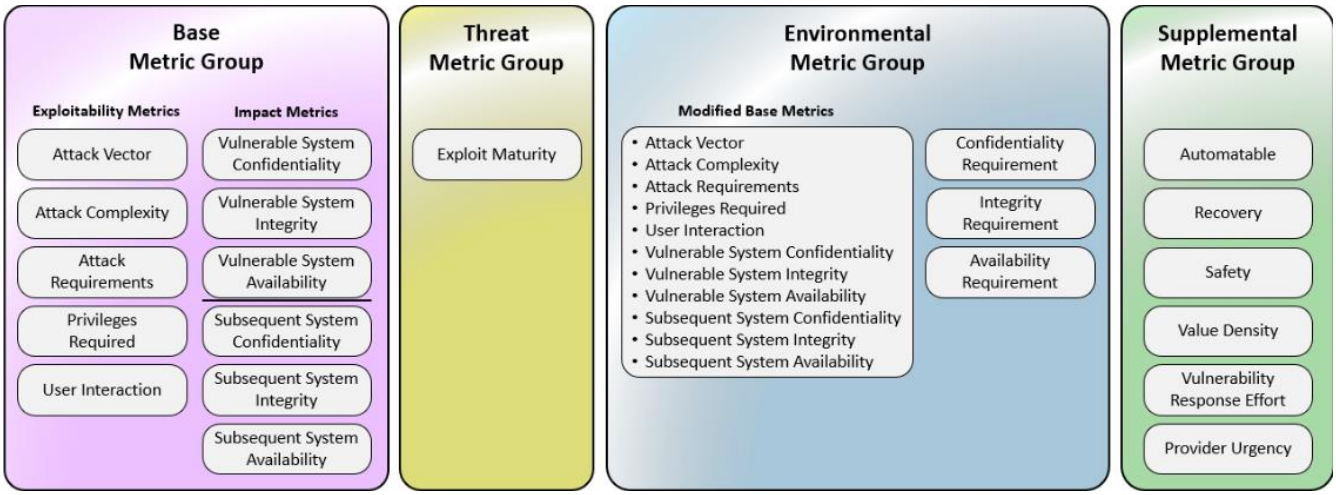


Рис. 1. Групи метрик та їх показники

Група базових метрик являє собою внутрішні характеристики вразливості, які постійні в часі та в різних середовищах користувачів. Вона складається з двох наборів показників: показники можливості експлуатації та показники впливу. Показники можливості експлуатації відображають простоту та технічні засоби, за допомогою яких можна проексплуатувати вразливість. Показники впливу відображають прямі наслідки успішного експлойту для вразливої системи або інших систем, що взаємодіють з вразливою.

Важливо згадати про можливість вимірювання впливу вразливості на інші системи. За це відповідала метрика «Scope», або «Область впливу», яка була ключовим нововведенням у CVSS v3.0, але викликала дуже багато суперечок. У CVSS v4.0 розробники стандарту вирішили цю проблему наступним чином: існуючі метрики визначення впливу стали відповідати лише за вразливу систему, а у разі зміни області впливу на справу вступає нова підгрупа метрик, яка відповідає за вплив на наступні системи.

Метрики загрози, які раніше були відомі як тимчасові метрики, у новій версії стандарту мають дещо інше призначення. Тепер вони безпосередньо відображають можливість експлуатації вразливості, наприклад, підтвердження того, що вразливість раніше не експлуатувалася та що в загальному доступі немає експлойтів або інструкцій її експлуатації. При цьому значення, визначені в цій групі метрик, так само можуть змінюватися з часом.

Метрики середовища являють собою характеристики вразливості, які є унікальними для конкретного середовища функціонування. Вони дозволяють формувати підсумкову оцінку в залежності від важливості порушеного IT-активу, що вимірюється з точки зору безпеки, конфіденційності, цілісності та доступності. Крім того, в цій групі є модифіковані еквіваленти базових метрик. Їм надаються

значення залежно від розміщення системи в інфраструктурі організації та функціонуючих заходів захисту інформації.

Додаткові метрики – це група показників, які дозволяють описати контекст вразливості, а також описати та виміряти її додаткові зовнішні атрибути. Усі метрики у межах цієї групи немає ніякого впливу підсумкову оцінку CVSS. Вони просто передають додаткові зовнішні характеристики вразливості і можуть використовуватися фахівцями з інформаційної безпеки.

Отже, головна перевага CVSS v4.0 над попередніми версіями – більш явний акцент на тому, що при оцінці вразливостей вкрай важливо враховувати інфраструктуру та оточення, в яких функціонує вразливий компонент та брати до уваги цінність активів, що будуть втрачені, змінені або розкриті при реалізації загрози.

Перелік посилань:

1. *Загальна система підрахунку вразливостей версії 4.0: посібник користувача. URL: https://www.first.org/cvss/v4.0/user-guide (date of access: 13.10.2024).*

Задорожний Дмитро Сергійович,
студент групи ТСДМ-61, ННІТ ДУІКТ, Київ, Україна

ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Використання блокчейн-технології у системах електронного голосування забезпечує підвищену безпеку, прозорість і незмінність результатів голосування. Децентралізована структура та криптографічний захист запобігають фальсифікаціям і несанкціонованому доступу. Ця технологія має значний потенціал для зміцнення безпеки виборчих процесів, але також вимагає подальшого дослідження, щоб подолати існуючі технічні виклики.

Блокчейн-технологія, як децентралізований та криптографічно захищений спосіб обробки транзакцій, стала одним із найперспективніших інструментів для покращення безпеки обміну даними в мережі Інтернет. В сучасних умовах швидкого росту технічних інновацій та інформаційних технологій, а також їх активним залученням в наше життя, електронні комунікації стають не тільки зручним, а й необхідним засобом, оскільки вони дають змогу отримати потрібні послуги тут і зараз.

Використання традиційних централізованих систем голосування часто пов'язане з ризиками зловживань, маніпуляцій або махінацій з виборчим процесом. Блокчейн дозволяє вирішити ці проблеми, забезпечуючи незмінність даних, децентралізовану верифікацію та захист від фальсифікацій.

Однією з ключових переваг блокчейн-технології є її незмінність — внесені

до блокчейну дані не можуть бути змінені або видалені, оскільки кожен новий блок пов'язаний з попереднім і містить криптографічний хеш, що робить неможливим несанкціоновані зміни результатів голосування. Усі учасники мають можливість переглядати блоки та транзакції, які в них зберігаються. При цьому, фактичний вміст транзакції залишається захищеним приватним ключем, що гарантує конфіденційність інформації [1]. Кожен блок у ланцюжку містить дані про голоси, які можна перевірити. Прозорість і відкритість блокчейн-систем дозволяють відстежувати всі етапи виборчого процесу в режимі реального часу, що є вагомою перевагою перед традиційними системами голосування. Завдяки цій особливості блокчейн може забезпечити прозорість виборчого процесу, що є однією з основних вимог демократичного голосування.

Блокчейн також забезпечує високий рівень безпеки. Оскільки блокчейн децентралізований і розподілений між багатьма учасниками (нодами), атака на окремий вузол не вплине на загальну безпеку системи, тому що копії блокчейну зберігаються на всіх учасниках мережі. Кожен комп'ютер у блокчейн-мережі зберігає свою копію даних, що означає, що існують тисячі або навіть мільйони таких самих копій, як, наприклад, у Bitcoin. Хакеру потрібно змінити кожну копію одночасно, оскільки в блокчейні немає центральної версії, яку можна легко підробити [2]. Технологія також захищає від атак типу "відмова в обслуговуванні" (DDoS).

Крім того, технологія блокчейн використовує криптографічні алгоритми для захисту персональних даних виборців та забезпечення анонімності голосування. Важливо, що криптографічні методи шифрування гарантують цілісність голосів, тобто навіть якщо атака хакерів відбудеться, вона не призведе до зміни результатів голосування. Блокчейн дозволяє гарантувати, що голос кожного виборця зашифрований і зберігається в незмінному вигляді до завершення виборчого процесу, що забезпечить довіру до результатів.

Незважаючи на значні переваги блокчейн-технології, існують і певні технічні виклики, пов'язані з її застосуванням у масштабованих системах голосування. Однією з ключових проблем є пропускна здатність блокчейн-мережі — кількість транзакцій, які можна обробити за одиницю часу, може бути недостатньою для одночасної обробки великої кількості голосів у виборах на національному рівні.

Обчислювальна потужність вимірюється у хешах на секунду (H/s) і відображає здатність мережі виконувати криптографічні обчислення. Чим вища обчислювальна потужність, тим більше хешів може бути оброблено на секунду, що підвищує шанси майнерів на успішне вирішення математичної задачі для створення нового блоку.

Хоча блокчейн може знизити витрати на транзакційні збори для користувачів, технологія все ж не є безкоштовною. Наприклад, метод «доказ роботи», використовуваний у Bitcoin для верифікації транзакцій, вимагає великих обсягів обчислювальної потужності. У реальному житті енергоспоживання мільйонів комп'ютерів у мережі Bitcoin приблизно дорівнює щорічному

споживанню електроенергії Данії [2].

Для вирішення цієї проблеми дослідники пропонують різні рішення, серед яких використання багатошарових блокчейн-архітектур або впровадження технологій другого рівня, наприклад, Lightning Network для масштабування Bitcoin. Це платіжний протокол другого рівня, який створено для роботи з криптовалютами, такими як Bitcoin або Litecoin. Ця технологія покликана забезпечити швидкі транзакції між учасниками мережі. Lightning Network пропонує ефективне рішення для проблеми масштабованості Bitcoin, дозволяючи зменшити затримки та знизити витрати на транзакції. Важливо зазначити, що питання масштабованості залишається відкритим і потребує подальших досліджень та тестувань на практиці.

Перелік посилань:

1. *Manuilov Y. S. USE OF BLOCKCHAIN TECHNOLOGY IN TELECOMMUNICATIONS. Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences. 2021. № 3. С. 123–127. URL: https://doi.org/10.32838/2663-5941/2021.3/20*
2. *Костюк П.П. ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. Сучасний захист інформації №3(43), 2020. С. 22-28.*

Задорожний Дмитро Сергійович,
студент групи ТСДМ-61, ННІТ ДУІКТ, Київ, Україна

АУТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ У СИСТЕМАХ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Розглядається питання аутентифікації користувачів у системах електронного голосування. Розглянуто актуальність електронного голосування як елементу сучасної демократії, його переваги та ризики, пов’язані з компрометацією облікових даних і підробкою біометричних показників. Описано різні методи аутентифікації, зокрема однофакторні, багатофакторні та біометричні. Визначено основні вимоги до безпеки та проблеми.

Електронне голосування є перспективним засобом проведення виборів, інструментом сучасної демократії, що забезпечує швидкий та зручний спосіб вираження волевиявлення громадян. З розвитком технологій дедалі більше країн переходять до використання електронних засобів як ефективного способу проведення виборів. Електронне голосування дозволяє зменшити витрати на організацію виборів, підвищити оперативність обробки результатів та забезпечити доступність для громадян, зокрема тих, хто перебуває за межами своїх виборчих дільниць або має фізичні обмеження. Однак, поряд із численними перевагами, дане питання викликає значні занепокоєння щодо безпеки і конфіденційності.

З метою забезпечення законності процесу голосування одним із ключових завдань є аутентифікація виборців. Від цього залежить достовірність результатів голосування. Метою впровадження систем аутентифікації є забезпечення

принципів чесності та прозорості.

Сьогодні існує кілька методів аутентифікації, серед яких використання паролів, біометричних даних та інших засобів [1]. Огляд цих способів є важливим для оцінки їх відповідності до вимог безпеки та можливості інтеграції в сучасні системи.

Поняття аутентифікації, методи аутентифікації, вимоги до безпеки

Аутентифікація — це процес підтвердження особи, яка намагається отримати доступ до системи, що, у випадку електронного голосування, є важливим етапом для гарантування легітимності результатів виборів. Основна мета аутентифікації в електронних системах голосування — переконатися, що кожен виборець голосує один раз і що особа, яка здійснює голосування, є саме тим виборцем, за якого себе видає. Існують динамічні та статичні методи аутентифікації, що призначені для перевірки ідентичності користувачів або об'єктів, які намагаються отримати доступ до системи, програми чи ресурсу. Статичні методи аутентифікації базуються на незмінних даних користувача, таких як пароль, PIN-код або відповідь на секретне запитання. Ці дані залишаються постійними і використовуються під час кожної спроби входу. Динамічні методи аутентифікації використовують змінні або одноразові дані. Це можуть бути тимчасові коди, які генеруються для кожної нової сесії [2].

Методи аутентифікації можна умовно поділити на кілька груп:

1. **Однофакторні методи**. До цієї групи належать найбільш прості методи аутентифікації, як-от паролі чи PIN-коди. Їх основна перевага — простота впровадження та використання. Однак ці методи мають значні недоліки щодо безпеки, адже паролі можуть бути вкрадені або скомпрометовані, що створює ризики фальсифікації.

2. **Багатофакторна аутентифікація (MFA)**. Цей метод передбачає використання кількох факторів підтвердження особи, наприклад, комбінації пароля та біометричних даних (відбитки пальців, сканування обличчя). Така система значно підвищує рівень безпеки, адже навіть при компрометації одного фактора інші залишаються захищеними.

3. **Біометричні методи**. Це найбільш надійний спосіб аутентифікації, оскільки він використовує унікальні фізіологічні особливості людини (відбитки пальців, райдужна оболонка ока, голос). Недоліком біометричних систем є вразливість до збоїв через проблеми з технічним обладнанням, а також питання щодо захисту конфіденційних біометричних даних.

Вимоги до безпеки аутентифікації в системах електронного голосування є надзвичайно високими. Вони включають:

- **Конфіденційність**: голосування має бути таємним, а облікові дані виборця не повинні бути доступні третім особам.

- **Надійність**: система повинна гарантувати, що виборці не можуть змінити свій голос або голос інших учасників процесу.
- **Доступність**: система аутентифікації повинна бути доступною для кожного виборця, незалежно від його технічних можливостей або обмежень.

Ризики електронного голосування включають низку проблем. Одним із головних ризиків є компрометація облікових даних виборців. Якщо користувачі не дотримуються належних правил інформаційної безпеки, таких як використання складних паролів або двофакторної аутентифікації, їх облікові дані можуть бути викрадені. Це відкриває можливість несанкціонованого доступу до системи, що загрожує фальсифікацією результатів. Ще однією серйозною проблемою є підробка біометричних даних. Незважаючи на загальну надійність біометричних методів, таких як сканування відбитків пальців або обличчя, існують високотехнологічні способи підробки, що ставить під сумнів безпеку цих технологій. Штучний інтелект вже зараз здатен повністю скопіювати риси обличчя, чого буде достатньо для обману автоматичної системи верифікації. Соціальна інженерія також є значною загрозою, коли зловмисники можуть обманом отримати доступ до облікових даних користувачів через маніпуляції або шахрайство. Тому введення електронного голосування все ще є предметом дискусій, оскільки ще відбувається пошук рішень.

Багатофакторну аутентифікацію можна розглянути як основну концепцію безпеки. Поєднання кількох рівнів захисту — паролів і біометричних даних значно зменшує ризик несанкціонованого доступу до системи. Важливим заходом є захист даних шляхом шифрування та впровадження механізмів для запобігання підробкам. Системи безпеки повинні постійно вдосконалюватися і оновлюватися, щоб мати змогу протистояти новим загрозам, інакше застарілі механізми можуть стати легкою мішенню для зловмисників. Також варто звернути увагу на підвищення обізнаності виборців щодо важливості дотримання правил інформаційної безпеки, адже багато ризиків можна мінімізувати завдяки правильному використанню системи виборцями.

Перелік посилань:

1. Клопотовський Д.О., Писаренко Л.Д., «КЛАСИФІКАЦІЯ МЕХАНІЗМІВ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ І ЇХ ОГЛЯД». Перспективні напрямки сучасної електроніки., КПІ ім. Ігоря Сікорського, ФЕЛ,2017 р., УДК 3.007.3
2. Стасєв Ю. В., Гончаренко К. Г., Мороз В. І. Аналіз методу багатофакторної аутентифікації користувачів інформаційних систем на основі райдужної оболонки ока. Системи обробки інформації. 2023. № 3 (174). С. 63–69. URL:https://doi.org/10.30748/soi.2023.174.09

Задирака Ігор Тарасович, БСДМ-62
Державний університет

інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ІДЕНТИФІКАЦІЇ КЛІЄНТА ТА КЕРУВАННЯ ДОСТУПОМ НА БАЗІ IBM SECURITY VERIFY

Визначено мету і основні завдання щодо ідентифікації клієнта та керування доступом до додатків та сервісів організації. Розглянуто зміст технології ідентифікації клієнта та керування доступом до додатків та сервісів організації на прикладі IBM Security Verify.

У Звіті Verizon Business за 2024 рік підкреслюється, що використання вкрадених облікових записів користувачів займає перше місце серед можливих початкових векторів атак і становить 24% від загального числа найпопулярніших варіантів дій у порушеннях [1]. Microsoft зазначає, що становлення балансу між безперебійним обслуговуванням клієнтів і захистом конфіденційних даних може бути складним [2]. Зі збільшенням частоти та складності витоків даних і розмаїття кіберзагроз потребує вирішення проблема ідентифікації клієнтів та керування їх доступом до додатків та сервісів організацій.

Захистити дані клієнтів, забезпечуючи їх безперебійну роботу, може бути складно. Для цього потрібна надійна система, здатна ефективно керувати та захищати інформацію клієнтів, не ускладнюючи роботу клієнтів. Керування ідентифікацією та доступом клієнта (Customer Identity and Access Management, CIAM) відіграє ключову роль у цьому контексті. CIAM – це набір технологій і процесів, які включають розширені методи безпеки, такі як багатофакторна автентифікація, щоб гарантувати доступ до конфіденційної інформації лише авторизованим особам [2].

Необхідно відмітити, що CIAM дає змогу організації захистити інформацію про клієнтів за допомогою надійних механізмів автентифікації, авторизації та керування даними, а також забезпечити їх безперебійну роботу. Це спрощує взаємодію з користувачем, дозволяючи клієнтам використовувати єдиний набір реєстраційних даних для доступу до різних послуг. CIAM навіть пропонує додаткові рівні безпеки, такі як технологія розпізнавання відбитків пальців або обличчя, щоб покращити захист.

IBM Security Verify дозволяє організаціям надавати сучасні та безпечні засоби ідентифікації та доступу окремим особам, як співробітникам, так і споживачам. Сьогодні портфоліо IBM Security Verify складається з програмного забезпечення та моделей розгортання SaaS із кількома клієнтами для керування доступом, ідентифікації споживача та керування доступом, а також ідентифікації та керування. Керування привілейованим доступом (PAM) надається через IBM Security Verify Privilege.

Рис. 1. Розмаїття специфічних рішень IBM Security Verify [3]

Розширення IDaaS (Identity-as-a-Service) для найбільших організацій надає IBM Security Verify (рис. 1). Оскільки сьогодні клієнти використовують IBM Security Verify SaaS, гнучкість і швидкість використання автентифікації, багатофакторної автентифікації на основі ризиків і керування як послуга прискорилися, що забезпечує більш безпечний і привабливий досвід [3].

У рішенні IBM Security Verify здійснюється автентифікація клієнтів на основі ризиків і реалізовано адаптивний доступ. IBM Security Verify зменшує перешкоди доступу користувачів до веб-додатків без шкоди для безпеки. IBM Security Verify забезпечує створення правила доступу в менеджері політики на основі даних про ризики від IBM Trusteer, зібраних на попередньо визначеній веб-сторінці без коду [4].

Використовуючи усталену та глибоку інформацію з платформи Trusteer IBM Security, оцінка ризику генерується на основі контекстної інформації, наданої користувачем, такої як відбитки пальців пристрою, деталі підключення, місцезнаходження та аномалії поведінки.

У рішенні IBM Security Verify може бути реалізовано вдосконалену багатофакторну автентифікацію. Критично важливі додатки та сервіси організації захищаються за допомогою розширеної багатофакторної автентифікації (MFA) за допомогою FIDO2, QRCode, Mobile Push тощо. Ці типи MFA вбудовуються в корпоративні додатки, щоб працівникам потрібно було завантажити лише один додаток, який надає їм можливість безпечно входити в корпоративні додатки та сервіси за допомогою безпечних методів автентифікації [4].

Збалансування безпеки та досвіду користувача здійснюється через увімкнення адаптивної автентифікації. Визначення потреби в автентифікації за допомогою контекстуалізації користувача на основі місцезнаходження, пристрою, каденції типу та інших контекстних даних [4].

FIDO2 – це набір стандартів і технологій, які можуть запропонувати взаємодіючу сильну автентифікацію на основі PKI як для веб-клієнтів, так і для клієнтів інших корпоративних додатків (включно з мобільними клієнтами).

Коли автентифікація FIDO2 використовується як перший фактор, вона може замінити автентифікацію за іменем користувача та паролем, забезпечуючи надійну,

стійку до фішингу альтернативу, яка також забезпечує взаємодію з кінцевим користувачем. IBM Security Verify підтримує FIDO2 для автентифікації у власних веб-інтерфейсах і для доступу до додатків, інтегрованих через єдиний вхід.

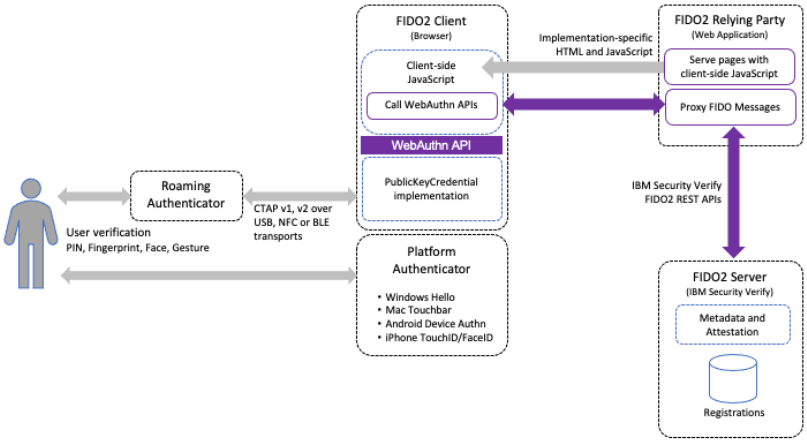


Рис. 2. Архітектура FIDO2 WebAuthn [4]

На рисунку 2 можна побачити, що IBM Security Verify діє як сервер FIDO2. Якщо це використовується для інтеграції автентифікації FIDO2 у спеціальний веб-додаток, веб-додаток передає повідомлення FIDO2 між API WebAuthn браузера та API IBM Security Verify FIDO2 REST.

Отже, використовуючи CIAM, організації можуть ефективно захищати дані клієнтів, посилювати загальні заходи безпеки та запевняти клієнтів у безпеці їхньої особистої інформації.

Перелік посилань:
1. 2024 Data Breach Investigations Report (DBIR). Verizon Business. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 30.09.2024).
2. What is CIAM? Microsoft. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-ciam (дата звернення: 30.09.2024).
3. Milan Patel. Introducing IBM Security Verify Dedicated. September 21, 2021. URL: https://community.ibm.com/community/user/security/blogs/milan-patel/2021/09/21/introducing-ibm-security-verify-dedicated (дата звернення: 30.09.2024).
4. IBM Security Verify Documentation Hub. URL: https://docs.verify.ibm.com/verify (дата звернення: 30.09.2024).

Івахненко Кирило Володимирович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

Технологія забезпечення кібербезпеки мережі на базі рішення Fortinet

Загрози кібербезпеці швидко стають складнішими, оскільки зловмисники використовують нові методи та соціальну інженерію, щоб вимагати гроші від організацій і користувачів, порушувати бізнес-процеси та викрадати або знищувати конфіденційну інформацію. Для захисту від цих дій організаціям потрібні технологічні рішення з кібербезпеки та надійний процес виявлення та запобігання загрозам і усунення порушень кібербезпеки. FortiGate, брандмауер наступного покоління від лідера IT Cyber Security Fortinet, забезпечує максимальний захист від загроз для компаній будь-якого розміру. Використовуючи спеціальні процесори безпеки та аналіз загроз від FortiGuard, брандмауер FortiGate забезпечує неперевершену продуктивність і захист, одночасно спрощуючи мережу.

Будучи ключовим компонентом IT-безпеки бізнесу, брандмауер діє як захист від шкідливого трафіку, захищаючи дані та запобігаючи несанкціонованому доступу.

Брандмауер, такий як FortiGate, має бути ядром мережі, визначаючи, який трафік пропускається у свою мережу, а який — не пропускається.

Поняття FortiGate

FortiGate, брандмауер наступного покоління від лідера IT Cyber Security Fortinet, забезпечує максимальний захист від загроз для компаній будь-якого розміру. Використовуючи спеціальні процесори безпеки та аналіз загроз від FortiGuard, брандмауер FortiGate забезпечує неперевершену продуктивність і захист, одночасно спрощуючи мережу.

Fortinet пропонує моделі брандмауерів FortiGate, щоб задовольнити будь-які вимоги до розгортання, від серії початкового рівня FortiGate-20 для невеликих офісів і роздрібних мереж до серії FortiGate-1500 для великих підприємств.

Функції брандмауера FortiGate

Високопродуктивний захист від загроз, такий як веб-фільтрація, антивірус і контроль програм, гарантує, що бізнес не постраждає від загроз кібербезпеці, таких як шкідливе програмне забезпечення та соціальна інженерія. Захист критично важливих додатків – високомасштабована сегментація та наднизька затримка для захисту сегментів мережі.

Автоматизована оцінка ризиків – автоматизований робочий процес і функції аудиту знімають навантаження на IT-відділ. Оцінки безпеки – застосовуються заходи безпеки «найкращі практики» з рейтингами безпеки, наданими FortiGate.

Незалежно сертифікована постійна розвідка про загрози гарантує захист від відомих і невідомих атак.

Управління безпекою корпоративного класу – дозволяє керувати активами безпеки незалежно від місцезнаходження. Інтеграція Security Fabric – розподіляє загрози по всій інфраструктурі безпеки IT, щоб забезпечити швидкий і автоматизований захист.

Від чого захищає брандмауер FortiGate?

Брандмауер наступного покоління FortiGate може захистити від ряду загроз безпеці, в тому числі:

- Шкідливе програмне забезпечення;
- Шпигунське (сіре) програмне забезпечення;
- Схеми фішингу / соціальної інженерії;
- Фармінгові атаки;
- Віруси обміну миттєвими повідомленнями;
- Однорангові мережі;
- Змішані мережеві атаки;
- Електронна пошта;
- Вторгнення.

Завдяки брандмауеру FortiGate, надає допомогу організаціям ефективно захищати свої інформаційні ресурси, знижувати ризики кіберзагроз і забезпечувати безпечний доступ до мережі.

Перелік посилань:
1. Axians. Complete Guide to FortiGate Firewall. URL: https://www.axians.co.uk/news/complete-guide-to-fortigate-firewalls/ (дата звернення: 15.10.2024)
2. Fortinet. Firewall Definition: What Is a Network Firewall?. URL: https://www.fortinet.com/resources/cyberglossary/firewall (дата звернення: 15.10.2024)

Ігнатенко Владислав Олександрович
студент групи БСДМ-62, ННІКБЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАХИСТУ ОРГАНІЗАЦІЇ ВІД ІНСАЙДЕРСЬКИХ АТАК

У сучасному світі питання захисту організацій від інсайдерських атак набуває все більшої актуальності. Ця робота присвячена дослідженню технологій та методів, спрямованих на виявлення та запобігання внутрішнім загрозам безпеці. Розглянуто сучасні підходи до моніторингу діяльності співробітників, аналізу поведінкових факторів та управління доступом до критичних ресурсів. Запропоновано рекомендації щодо впровадження комплексних систем захисту, що поєднують технічні та організаційні заходи. Результати дослідження можуть бути використані для підвищення рівня інформаційної безпеки в організаціях різного масштабу.

Інсайдерські загрози стали реальністю для цивільних компаній, таких як Tesla, яка зазнала саботажу та крадіжки інтелектуальної власності, та Capital One, яка постраждала від шахрайства. Ще більший суспільний резонанс викликав витік даних у Міністерстві оборони США, здійснений відомими зловмисниками Челсі Меннінг та Едвардом Сноуденом, чия шпигунська та хактивістська діяльність широко відома. Різке збільшення кількості подібних інцидентів в останні роки і незліченна шкода, завдана інсайдерами, повинні служити застереженням для всіх членів спільноти кібербезпеки [2].

Інсайдерська загроза - це тип кібератаки, що походить від особи, яка працює в організації або має санкціонований доступ до її мереж чи систем. Інсайдерською загрозою може бути теперішній або колишній працівник, консультант, член правління або діловий партнер, і вона може бути навмисною, ненавмисною або зловмисною.

Зазвичай під внутрішньою загрозою в кібербезпеці розуміють особу, яка використовує свій санкціонований доступ до даних і ресурсів організації, щоб завдати шкоди обладнанню, інформації, мережам і системам компанії. Вона включає в себе корупцію, шпигунство, деградацію ресурсів, саботаж, тероризм і несанкціоноване розголошення інформації. Це також може стати відправною точкою для кіберзлочинців для запуску шкідливого програмного забезпечення або

атак з вимогою викупу [3].

Інсайдерські загрози стають все більш витратними та частими для організацій. За останні 12 місяців 48% організацій повідомили про зростання кількості інсайдерських атак. Основними факторами підвищення ризику 76% організацій називають зростання бізнесу та складність IT-систем. Вражає те, що 83% організацій зазнали щонайменше однієї інсайдерської атаки, а кількість компаній, які пережили від 11 до 20 таких інцидентів, зросла у 5 разів з 2023 року[1].

Інсайдерські загрози стають все більш актуальними в сфері кібербезпеки, оскільки працівники з легітимним доступом до систем можуть ненавмисно або навмисно завдати шкоди організації. Традиційні методи захисту, спрямовані на зовнішні загрози, не завжди ефективні проти внутрішніх порушників. Тому впровадження новітніх технологій для виявлення та запобігання інсайдерським атакам є критично важливим.

Однак, занадто сильний акцент на технологічних рішеннях може призвести до нехтування людським фактором. Надмірний контроль і моніторинг можуть викликати недовіру серед співробітників та знизити їх мотивацію. Крім того, складність та вартість впровадження таких систем можуть бути непосильними для деяких організацій, особливо малих і середніх підприємств.

Ефективний захист від інсайдерських загроз потребує балансу між технологічними засобами та організаційними підходами. Впровадження політик безпеки, регулярне навчання персоналу та формування культури відповідального ставлення до інформації можуть значно знизити ризики. Сучасні технології, такі як поведінковий аналіз та штучний інтелект, можуть доповнити ці зусилля без надмірного втручання в приватність співробітників.

Отже, протидія інсайдерським атакам вимагає комплексного підходу, що поєднує технічні рішення з людським фактором. Організації повинні інвестувати не лише в технології, але й у розвиток корпоративної культури, яка підкреслює важливість інформаційної безпеки. Лише такий збалансований підхід дозволить ефективно захистити ресурси та дані від внутрішніх загроз.

Таким чином, більше не можна продовжувати недооцінювати проблему інсайдерських загроз. Фірми, організації, установи та уряди повинні очолити і прийняти культурні зміни у своїх підходах до безпеки. Завдяки прийняттю програми протидії внутрішнім загрозам, яка охоплює всі стратегічні підрозділи (включаючи відділ кадрів, юридичний відділ, відділ інформаційної безпеки, відділ кібербезпеки та відділ розвідки), координується керівником служби інформаційної безпеки та підтримується керівниками вищого рівня, можна впровадити систему, здатну запобігати, виявляти та реагувати на нелояльні та/або ненавмисні внутрішні загрози. Таким чином, захист підприємства від внутрішніх загроз є життєво важливою частиною найкращих практик інформаційної безпеки. Дуже важливо, щоб цінні секретні дані та активи компанії були захищені від найбільшої загрози: ворога за воротами [2].

Перелік посилань:

1. 2024 insider threat report | cybersecurity insiders. *Gurucul*. URL: https://gurucul.com/2024-insider-threat-report/ (date of access: 05.10.2024).
2. Mazzarolo, Guerrino & Jurcut, Anca. (2019). Insider threats in Cyber Security: The enemy within the gates. 10.48550/arXiv.1911.09575.
3. What is an insider threat? Definition, types, and prevention | fortinet. *Fortinet*. URL: https://www.fortinet.com/resources/cyberglossary/insider-threats#:~:text=An%20insider%20threat%20is%20a,intentional,%20unintentional,%20or%20malicious. (date of access: 05.10.2024).

Кагарлик Дмитро Тарасович, БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КЛІЄНТІВ ДО ВЕБ-ДОДАТКІВ НА БАЗІ AMAZON COGNITO

Визначено мету і основні завдання щодо управління ідентифікацією та доступом клієнтів до веб-додатків організації. Розглянуто зміст технології управління ідентифікацією та доступом клієнтів до веб-додатків на базі Amazon Cognito.

У Звіті Deloitte [1] зазначається, що у 2023 році понад 8,2 мільярда облікових записів було зламано в усіх галузях із середньою вартістю 4,45 мільйона доларів США за 2023 рік. Найпоширенішими початковими векторами атак були фішинг і викрадення дійсних облікових даних. Дані та інформація, що дозволяє ідентифікувати особу (Personally Identifiable Information, PII), є найбільш цінними для кіберзлочинців, які отримують прибуток, продаючи їх, а також для суб'єктів загрози національній державі, які збирають дані та проводять різноманітну шпигунську діяльність на підтримку своїх відповідних програм національної безпеки. Наприклад, особиста інформація також використовується в складних кампаніях соціальної інженерії для високопоставлених керівників або для вимагання від персоналу, який пройшов спеціальну перевірку. Як наслідок, у 2023 році почастішали колективні позови проти постачальників різних сервісів, які не забезпечують безпеку даних клієнтів [1].

Amazon Cognito – це економічно ефективна служба ідентифікації клієнтів і керування доступом (Customer Identity and Access Management, CIAM), орієнтована на розробників. Він забезпечує безпечне сховище ідентифікаційних даних і параметри об'єднання, які можна масштабувати до мільйонів користувачів. Amazon Cognito підтримує вхід за допомогою постачальників ідентифікаційних даних соціальних мереж і постачальників ідентифікаційних даних на основі SAML або OIDC для чудової взаємодії з клієнтами та пропонує розширені функції безпеки

для захисту клієнтів і бізнесу організації. Він підтримує різні стандарти відповідності, працює на відкритих стандартах ідентифікації (OAuth2.0, SAML 2.0 і OpenID Connect) і інтегрується з розширеною екосистемою зовнішніх і внутрішніх ресурсів розробки та бібліотек SDK [2].

Amazon Cognito – це ідентифікаційна платформа для веб- і мобільних додатків. Це каталог користувачів, сервер автентифікації та служба авторизації для токенів доступу OAuth 2.0 і облікових даних AWS. За допомогою Amazon Cognito можна автентифікувати та авторизувати користувачів із вбудованого каталогу користувачів, з каталогу підприємства та від постачальників ідентифікаційних даних споживачів, таких як Google і Facebook.

Наступні два компоненти складають Amazon Cognito. Вони працюють незалежно або в тандемі, залежно від потреб забезпечення доступу для користувачів веб-додатків організації.

Пул користувачів (рис. 1) створюється, якщо треба автентифікувати та авторизувати користувачів у додатку чи API організації. Пули користувачів – це каталог користувачів із самообслуговуванням і створенням, керуванням і автентифікацією користувачів, керованим адміністратором. Пул користувачів може бути незалежним каталогом і постачальником ідентифікаційної інформації OIDC (Identity Provider, IdP), а також проміжним постачальником послуг (Service Provider, SP) для сторонніх постачальників ідентифікаційної інформації щодо робочої сили та клієнтів. Існує можливість надання системи єдиного входу (Single Sign-On, SSO) у корпоративному додатку для ідентифікаторів співробітників організації в SAML 2.0 і OIDC IdPs з пулами користувачів. Існує можливість надання SSO у корпоративному додатку для ідентифікаторів клієнтів організації в загальнодоступних сховищах ідентифікаційних даних OAuth 2.0 Amazon, Google, Apple і Facebook [2].

Пули користувачів не потребують інтеграції з пулом ідентифікаційних даних. З пулу користувачів можна видавати автентифіковані веб-токени JSON (JWT) безпосередньо в додаток, веб-сервер або API.

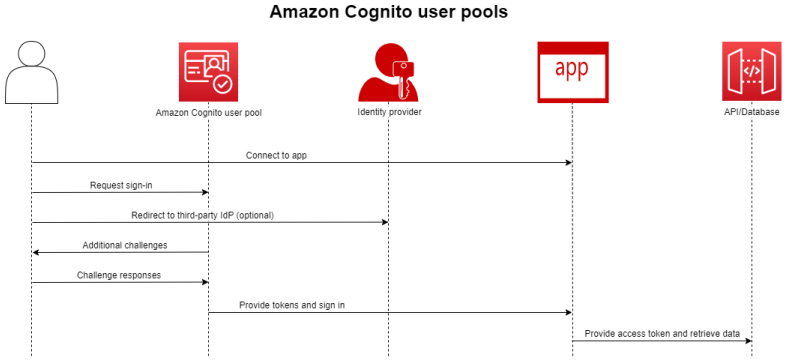


Рис. 1. Застосування пулу користувачів [3]

Пул ідентифікаційних даних (рис. 2) налаштовуються в Amazon Cognito для авторизації автентифікованих або анонімних користувачів для доступу до

інформаційних ресурсів AWS. Пул ідентифікаційних даних видає облікові дані AWS для корпоративного додатка, щоб надавати ресурси користувачам. Автентифікація користувачів здійснюється за допомогою довіреного постачальника ідентифікаційної інформації, наприклад пулу користувачів або служби SAML 2.0. За допомогою цього пулу можуть додатково видаватися облікові дані для гостьових користувачів. Пули ідентифікаційних даних використовують керування доступом як на основі ролей, так і на основі атрибутів, щоб керувати авторизацією користувачів на доступ до ресурсів AWS.

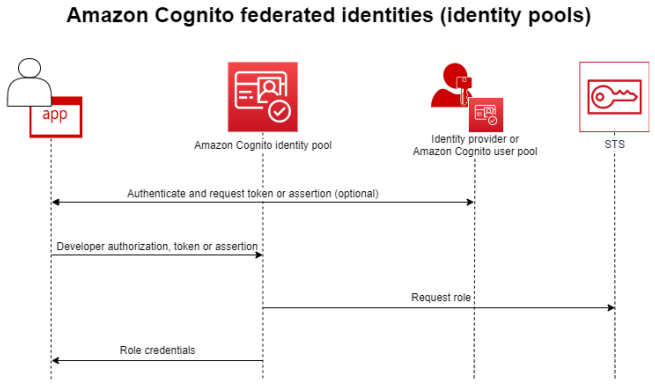


Рис. 2. Застосування пулу ідентифікаційних даних користувачів [3]

Пули ідентифікаційних даних не потребують інтеграції з пулом користувачів. Пул ідентифікаційних даних може приймати автентифіковані претензії безпосередньо від постачальників ідентифікаційних даних працівників і споживачів [3].

Отже, технологія управління ідентифікацією та доступом клієнтів відіграє ключову роль у захисті їх даних, забезпечуючи безперебійну та зручну роботу клієнтів. Використовуючи CIAM, організації можуть ефективно захищати дані клієнтів, посилювати загальні заходи безпеки та запевняти клієнтів у безпеці їхньої особистої інформації.

Перелік посилань:

1. Annual Cyber Threat Trends report: Insights, emerging threats, and their potential impact. Deloitte, 2024. URL: https://www2.deloitte.com/us/en/pages/noindex/cyber/cybersecurity-threat-trends-report-2024-download.html (дата звернення: 30.09.2024).
2. Amazon Cognito features. URL: https://aws.amazon.com/cognito/features/ (дата звернення: 30.09.2024).
3. Amazon Cognito. Developer Guide. URL: https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html (дата звернення: 30.09.2024).

Каленіченко Денис Олександрович, БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,

м. Київ

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ДОСТУПУ ДО КОРПОРАТИВНИХ ДОДАТКІВ ЗА ДОПОМОГОЮ ІНТЕЛЕКТУАЛЬНОЇ БЕЗПЕКИ AKAMAI ENTERPRISE APPLICATION ACCESS

Визначено мету і основні завдання щодо забезпечення безпечного доступу до корпоративних додатків за допомогою інтелектуальної безпеки. Розглянуто зміст технології забезпечення безпечного доступу до корпоративних додатків за допомогою інтелектуальної безпеки Akamai Enterprise Application Access.

Сьогодні кіберзлочинність стала повсюдною та більш витонченою, ніж будь-коли раніше. За даними Forbes, у 2023 році щодня виявляється приблизно 560 000 нових шкідливих програм і кожна організація стикається в середньому з 1248 кібератак на тиждень. Неминучі кіберризики, які можуть спричинити значні фінансові втрати, простої та репутаційні збитки, спонукають компанії посилити свою безпеку. Проте багато компаній мають недостатній рівень безпеки, оскільки вони все ще покладаються лише на антивіруси, брандмауери та спеціальні виправлення, яких уже недостатньо для боротьби з сучасними кіберзагрозами [1].

В [2] зазначається, що оскільки діловий світ змінюється та зростає кількість кіберзагроз, компанії по-новому дивляться на свій кіберзахист. Багато хто зрозумів, що традиційна мережева архітектура, яка ґрунтується на централізованому розташуванні, де всі сторони мали доступ до додатків, робить їх уразливими. Цей підхід до безпеки на основі захисту периметра, припускаючи, що всі всередині нього безпечні, створює ризик кібератак для компаній у сучасному ландшафті мобільних з’єднань і хмари.

Багато компаній звертаються до концепції архітектури нульової довіри, щоб захистити життєво важливі активи. Основним принципом будь-якого проекту Zero Trust є захист мережі. ZTNA – це архітектура, яка надає безпечний доступ до додатків і ресурсів на основі надійної автентифікації, авторизації та контексту. Архітектура ZTNA надає доступ лише до додатків, необхідних користувачам для виконання своєї роботи, а не до всієї мережі. З підходом ZTNA більше не має значення, де знаходяться користувачі – більше немає поняття всередині чи поза периметром. Місце розміщення додатка не має значення – локальна, публічна чи приватна хмара – оскільки автентифіковані користувачі отримують доступ лише до тих додатків, які їм дозволено використовувати [2].

Рішення Akamai Enterprise Application Access і Akamai MFA дозволяють організаціям перейти на архітектуру ZTNA, що може стати важливим і критичним кроком на їхньому шляху до нульової довіри.

Akamai Enterprise Application Access – це проксі-сервер із підтримкою ідентифікації у хмарі. Це гнучкий і адаптований сервіс із детальним прийняттям рішень на основі сигналів у реальному часі, таких як розвідка про загрози,

положення пристрою та інформація про ідентифікацію користувача. Akamai MFA – це служба багатофакторної автентифікації, яка забезпечує найнадійніші рівні автентифікації, щоб гарантувати, що користувач, який запитує доступ, є тим, за кого себе видає.

Розташування пристрою Akamai Enterprise Application Access є ключовою функцією для дозволу, заборони або обмеження доступу користувачів до програм. Рішення працює разом із авторизацією автентифікації та правилами контролю доступу та збирає інформацію про стан пристрою (наприклад, чи ввімкнено брандмауер пристрою, чи на ньому встановлено найновішу операційну систему або чи встановлено антивірусне програмне забезпечення). Це рішення також збирає зовнішні сигнали про загрози від Akamai Secure Internet Access, Carbon Black і CrowdStrike. Є можливість створювати рівні ризику, які дозволяють забороняти або обмежувати функції додатка на основі профілю ризику пристрою. Положення пристрою допомагає переконатися, що пристрої, які отримують доступ до додатків, задовольняють необхідним вимогам безпеки.

Швидкий і безпечний доступ до потрібного додатка для потрібного користувача в потрібний час став складним і комплексним через розподілену природу користувачів і додатків. Визначення користувача розвинулося, щоб означати набагато більше, ніж працівник – користувач може бути постачальником, партнером, клієнтом, підрядником, розробником або колегою з новопридбаної компанії.

Визначення додатка тепер також ширше і може включати кілька типів (застаріле, веб або програмне забезпечення як послуга) і розташування (центр обробки даних, Інтернет або хмара). Доступ до додатків на основі інструментів безпеки мережі Zero Trust Legacy, розроблених відповідно до застарілого уявлення про захищений периметр, не встигає за сучасною потребою в безпечному доступі до додатків. Ці традиційні технології, такі як віртуальні приватні мережі, роблять організації вразливими для атак зловмисників, які переміщуються всередині мережі [3].

Ідеальним рішенням цієї проблеми є таке, яке надає користувачам доступ лише до певних додатків, а не до цілих мереж або сегментів мережі, як це роблять тунелі VPN. Надання безпечного доступу до додатків і ресурсів є ключовим кроком для будь-якої організації, яка переходить на архітектуру Zero Trust [3].

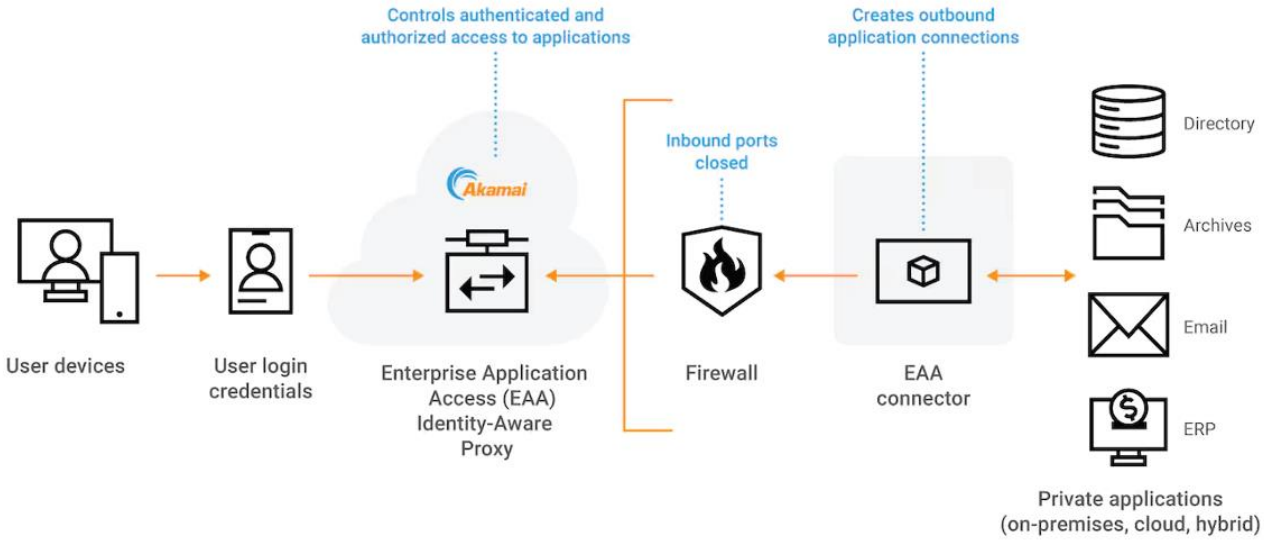


Рис. 1. Архітектура рішення Akamai Enterprise Application Access [3]

Akamai Enterprise Application Access – це повне рішення Zero Trust Network Access (ZTNA), засноване на принципі Zero Trust «ніколи не довіряй, завжди перевіряй» і забезпечує динамічний доступ до додатків на основі ідентифікації, контексту та положення пристрою. Це рішення усуває неявну довіру та забезпечує сувору перевірку ідентифікації та політики доступу з найменшими привілеями для кожного користувача, пристрою чи додатка, незалежно від їх розташування, і підтримує всі хмарні середовища. Akamai Enterprise Application Access зменшує площу атаки підприємства, запобігає бічному переміщенню та спрощує роботу адміністратора завдяки централізованому управлінню політиками [3].

Akamai Enterprise Application Access є повною службою ZTNA, яка надається через Akamai Connected Cloud. Це гнучкий і масштабований сервіс ZTNA з детальним і адаптивним доступом до прийняття рішень на основі ідентифікації користувача та сигналів у реальному часі, таких як розвідка про загрози та положення пристрою.

Akamai Enterprise Application Access об’єднує захист шляхів даних, ідентифікацію та керування доступом, безпеку додатків, багатофакторну автентифікацію, єдиний вхід, а також видимість і контроль керування в уніфіковану службу для всіх розташувань і типів додатків (локальні, інфраструктура як послуга (IaaS) або гібрид). Це рішення підтримує безклієнтські та клієнтські додатки з інтеграцією для Active Directory та постачальників ідентифікаційних даних на основі SAML. Akamai Enterprise Application Access автоматично вставляє оптимізацію продуктивності безпосередньо в шлях додатка, щоб усі додатки були швидкими та відповідними [3].

Основні можливості рішення Akamai Enterprise Application Access [3]: ZTNA як сервіс; доступ до додатка на основі ідентифікації та контексту, незалежно від того, де знаходяться користувачі чи який пристрій вони використовують; положення пристрою для адаптивного доступу на основі ризику; контроль доступу

до додатка незалежно від того, де розміщено додаток (хмара, на локальний мережі, гібридний); інтеграція з наявною інфраструктурою IdP або хмарним IdP Akamai; захищений безклієнтський доступ до додатків для підрядників та інших сторонніх розробників і ситуацій BYOD; пограничний транспорт для високої продуктивності додатка; локальний POP для оптимального доступу до додатків в офісі за допомогою примусового контролю універсальної ZTNA; інтеграція з Akamai MFA для надійної автентифікації користувача; інтеграція з Akamai Secure Internet Access для захисту користувачів і пристроїв від шкідливого вмісту; покращена безпека додатків безпосередньо з Akamai Connected Cloud.

Користувачам потрібні швидкі та чутливі бізнес-додатки. Низька продуктивність призводить до розчарування та різкого збільшення кількості дзвінків у службу підтримки IT. Akamai Enterprise Application Access, створений на базі Akamai Connected Cloud – найбільш розповсюдженої у світі платформи для хмарних обчислень, безпеки та доставки вмісту – підтримує продуктивність найвищого рівня. Завдяки точкам присутності, стратегічно близьким як до користувачів, так і до додатків, продуктивність плавно інтегрується в шлях додатків, забезпечуючи швидкість і ефективність. У свою чергу, Akamai Connected Cloud пропонує 100% доступність SLA, забезпечуючи високу надійність для потреб доступу до корпоративних додатків.

Перелік посилань:
1. Kostiantyn Losinskyi. Enterprise Security in 2023-2024. Ebook. Infopulse. URL: https://infopulsemarketing.blob.core.windows.net/ebooks-reports/infopulse_enterprise_security_2023_2024.pdf (дата звернення: 05.10.2024).
2. A Blueprint for Zero Trust Network Access. Akamai. URL: https://www.akamai.com/resources/white-paper/a-blueprint-for-zero-trust-network-access (дата звернення: 05.10.2024).
3. Enterprise Application Access. Akamai Product Brief. URL: https://www.akamai.com/site/en/documents/product-brief/enterprise-application-access-product-brief.pdf (дата звернення: 05.10.2024).

Карпеченков Микита Павлович
студент групи УБДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА КІБЕРНЕТИЧНУ БЕЗПЕКУ ПІДПРИЄМСТВА

Штучний інтелект в наші дні переживає бурхливий розвиток, що суттєво впливає на різноманітні сфери нашого життя - Від голосових помічників до складних систем автоматизації, і амбіції його використання в повній мірі зможе суттєво змінити вже існуючі нам підходи до забезпечення кібербезпеки підприємств, пропонуючи як нові можливості для захисту інформації, так і вдосконалюючи вже сталі процеси.

Основними причинами загострення питання про впровадження AI є його активне використання зловмисниками у вигляді автоматизації пошуку

вразливостей систем, прискорення розробки вірусів та в перспективі впровадження 5G, IoT, IPv6 та інших мережевих досягнень сприятимуть збільшенню кількості мережевих підключень, що збільшить об’єми надходження інформації в SOC центри, та примноже можливості вибору вектору м’якої атаки.

Порушення з боку третіх осіб стають дедалі складнішими. П'ять років тому зловмисник міг використати загальнодоступне шкідливе програмне забезпечення, щоб атакувати певні комп'ютерні системи, отримати облікові дані підрядників і викрасти дані клієнтів - звісно, безладно, але з чітким джерелом і можливістю відстежити і виправити завдану шкоду. Така атака блідне в порівнянні з сучасними витонченими вторгненнями, в яких інформація, викрадена в однієї компанії, може бути використана для компрометації тисяч її клієнтів і постачальників. Атаки на ланцюги поставок можуть зробити те ж саме, використовуючи найменш захищені вбудовані компоненти складних мереж поставок. Порушення, що не має меж, майже неможливо відстежити і виправити, а активні крадіжки можуть тривати протягом багатьох років.

Безпрецедентна кількість пристроїв, підключених до цих мереж, генерує дані, які необхідно обробляти та захищати, що призводить до заторів даних в SOC. Відстежувати та керувати активами, їх призначенням та очікуваною поведінкою може бути складно, особливо коли ними керують оркестранти сервісів, тому впровадження штучного інтелекту в процеси забезпечення кібернетичної безпеки підприємств є питанням часу.

Надалі відповімо на такі питання:

1. Чи безпечно довіряти ШІ автоматизацію кібербезпеки?;
2. AI в управлінні кіберризиками

Автоматизація кібербезпеки за допомогою штучного інтелекту є безпечною, оскільки вона побудована на існуючих кейсах використання в різних бізнес-середовищах. Наприклад, команди з управління персоналом (HR) та інформаційних технологій (IT) використовують ШІ для адаптації нових співробітників і надання їм ресурсів та відповідного рівня доступу для ефективного виконання своєї роботи. Тобто, Серед переваг автоматизації ШІ в кібербезпеці можна виділити наступні:

1. Усунення людських помилок: Загальним недоліком традиційних засобів захисту є необхідність втручання людини, що може призвести до дорогих людських помилок. Штучний інтелект у кібербезпеці усуває людський фактор з більшості процесів безпеки. Це більш ефективний підхід, оскільки людські ресурси можуть бути перерозподілені туди, де вони найбільш потрібні.
2. Краще прийняття рішень: Автоматизація кібербезпеки допомагає організаціям виявляти та виправляти потенційні недоліки у своїй стратегії безпеки. Таким чином, вони можуть впроваджувати формалізовані процедури, які можуть призвести до створення більш безпечного IT-середовища.

Використання штучного інтелекту в кібербезпеці підприємств може значно підвищити рівень захисту. ШІ може автоматично аналізувати великі обсяги даних, виявляючи аномалії та потенційні загрози, які можуть бути пропущені людиною. Крім того, ШІ здатен передбачати майбутні атаки та адаптуватися до нових загроз, забезпечуючи проактивний захист підприємства. Надалі розглянемо приклади застосування;

1. Безпека мережі - Створення і підтримка політик в декількох мережах вимагає значної кількості часу і зусиль. Організації часто нехтують правильними угодами про імена для своїх додатків і робочих навантажень. Це означає, що командам безпеки доводиться витрачати більше часу на визначення того, які робочі навантаження належать до конкретних програм. ШІ з часом вивчає шаблони мережевого трафіку організації, що дозволяє йому рекомендувати правильні політики та робочі навантаження.
2. Захист пароля та автентифікація - Інструменти штучного інтелекту, такі як CAPTCHA, розпізнавання обличчя та сканери відбитків пальців, дозволяють організаціям автоматично визначати, чи є спроба входу до сервісу справжньою. Ці рішення допомагають запобігти тактикам кіберзлочинності, таким як атаки грубої сили та підробка облікових даних, які можуть поставити під загрозу всю мережу організації.
3. Поведінкова аналітика - Організації можуть впроваджувати поведінкову аналітику на базі штучного інтелекту для покращення процесів пошуку загроз. Вона використовує моделі штучного інтелекту для створення профілів додатків, розгорнутих у їхніх мережах, і обробляє величезні обсяги даних про пристрої та користувачів. Потім вхідні дані можна аналізувати на основі цих профілів, щоб запобігти потенційно шкідливій активності.
4. Контроль виявлення та запобігання фішингу – Машинне навчання дозволяє ШІ вчитися на даних, щоб зробити аналіз більш точним і розвиватися, щоб протистояти новим загрозам. Це також допомагає ШІ краще розуміти, як користувачі спілкуються, їхню типову поведінку та текстові шаблони. Це має вирішальне значення для запобігання більш складним загрозам, таким як фішинг зі списом, коли зловмисники намагаються видати себе за високопоставлених осіб, наприклад, за керівників компаній. Штучний інтелект може перехоплювати підозрілу активність, щоб запобігти фішинговій атаці до того, як вона завдасть шкоди корпоративним мережам і системам.

Штучний інтелект відкриває нові можливості для ефективного управління кіберризиками. Завдяки своїм можливостям ШІ може автоматизувати рутинні завдання, виявляти складні атаки та адаптуватися до нових загроз, що робить його незамінним інструментом для сучасного бізнесу. Ось декілька більш детальних напрямків, де помічник AI зможе допомогти

спеціалістам;

1. AI надає рішення для відображення та запобігання невідомим загрозам, включаючи вразливості, які ще мають бути ідентифіковані або виправлені постачальниками програмного забезпечення.
2. системи штучного інтелекту можуть обробляти та розуміти величезні обсяги даних, які не можуть отримати спеціалісти з безпеки. Таким чином організації можуть автоматично виявляти нові загрози серед величезних обсягів даних і мережевого трафіку, які можуть залишитися непоміченими традиційними системами.
3. окрім виявлення нових загроз, штучний інтелект дозволяє організаціям краще керувати вразливостями. Це допомагає їм ефективніше оцінювати свої системи, покращувати вирішення проблем і приймати кращі рішення. Він також може виявити слабкі місця в мережах і системах, щоб організації постійно зосереджувалися на найважливіших завданнях безпеки.
4. Ручне управління ризиком ряду загроз, відмова в обслуговуванні (DoS), фішингові атаки і програми-вимагачі, може бути складним і трудомістким. Але за допомогою штучного інтелекту організації можуть виявляти різні типи атак у режимі реального часу та ефективно визначати пріоритети та запобігати ризикам.

Перелік посилань

1. AI in Cybersecurity – Uses, Benefits and Challenges - https://www.geeksforgeeks.org/ai-in-cybersecurity/ (дата звернення 05.10.2024)
2. What is AI for cybersecurity? - https://www.microsoft.com/en-us/security/business/security-101/what-is-ai-for-cybersecurity (дата звернення 07.10.2024)
3. Applying Artificial Intelligence to Cybersecurity Beyond the Hype - https://www.fortinet.com/content/dam/fortinet/assets/ebook/eb-applying-artificial-intelligence-to-cybersecurity.pdf (дата звернення 06.10.2024)

Качний Ілля Сергійович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ОГЛЯД АТАКИ AS-REPROASTING, СПРЯМОВАНОЇ НА ПРОТОКОЛ АВТЕНТИФІКАЦІЇ KERBEROS

Kerberos - це протокол, який дозволяє користувачам автентифікуватися в мережі та отримувати доступ до служб після автентифікації. За замовчуванням Kerberos використовує порт 88 і є протоколом автентифікації за замовчуванням для доменних облікових записів, починаючи з Windows 2000. Коли користувач входить до свого комп'ютера, Kerberos використовується для його автентифікації. Він використовується щоразу, коли користувач хоче отримати доступ до служби в мережі. Завдяки Kerberos користувачеві не потрібно постійно вводити свій пароль, а серверу не потрібно знати пароль кожного користувача.

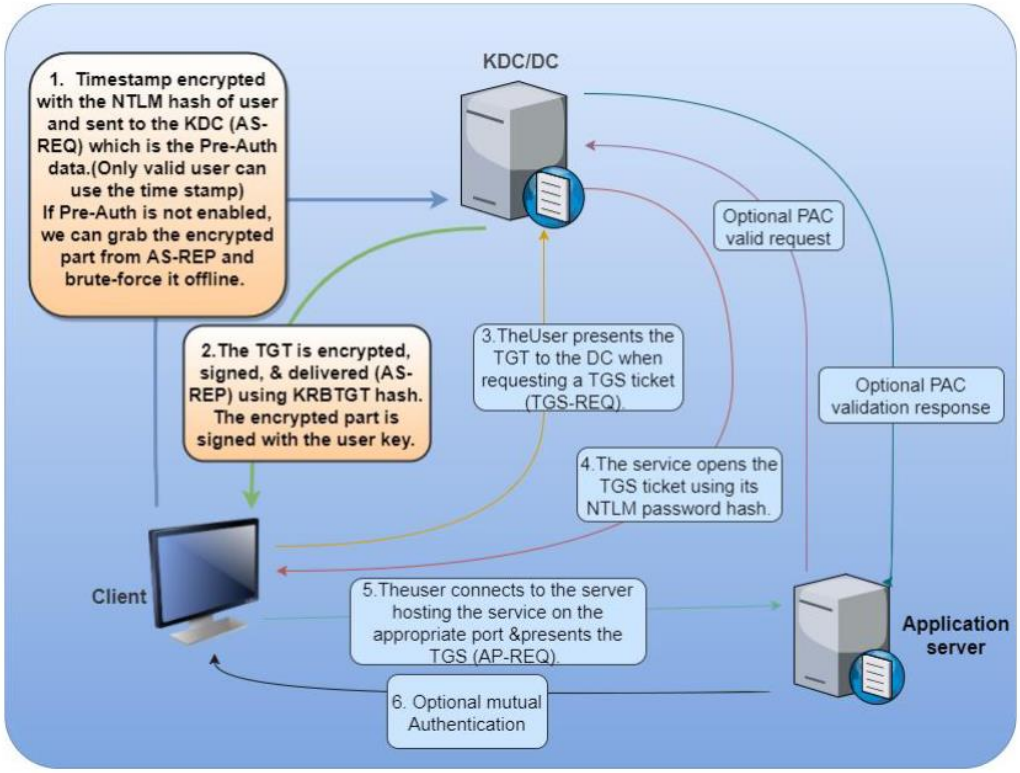


Рис.1. Схема роботи протоколу Kerberos

Коли користувач хоче взаємодіяти з доступними ресурсами в мережі, відбувається наступне:

1. Для початку користувач запитує перший квиток у сервера ключів (KDC), доводячи, що він є тим, за кого себе видає. У цей момент клієнт проходить автентифікацію на KDC. Цей квиток, який називається TGT (Ticket Granting Ticket), є посвідченням особи користувача. Він містить всю інформацію про користувача, таку як ім'я, дата створення облікового запису, інформація про безпеку користувача, групи, до яких належить користувач, тощо. Термін дії цього посвідчення особи, TGT, за замовчуванням обмежений кількома годинами. Цей квиток пред'являється для всіх інших запитів до KDC.

2. Після отримання TGT користувач повинен пред'являти його в KDC щоразу, коли йому потрібно отримати доступ до послуги. Після цього KDC перевіряє, чи дійсний поданий TGT і чи не підроблений він користувачем, і якщо так, то повертає користувачеві квиток на послугу видачі квитків (TGS) або квиток на послугу (ST). Копія інформації про користувача в TGT включається в квиток TGS.

3. Тепер, коли користувач має квиток TGS на певну послугу, він пред'являє цей квиток TGS сервісу, щоб скористатися нею. Сервіс перевіряє дійсність цього квитка, і якщо все гаразд, він зчитує вміст інформації про користувача, щоб визначити, чи має він право користуватися запитуваною послугою. Таким чином, саме сервіс перевіряє права доступу користувача.

AS-REPRoasting - це найпростіша атака на Kerberos, яка націлена на «попередню автентифікацію». Ця атака рідко зустрічається в організаціях, але є

однією з небагатьох атак на Kerberos, які не вимагають попередньої автентифікації. Єдина інформація, яка потрібна зловмиснику - це ім'я користувача, якого він хоче атакувати, яке також можна знайти за допомогою інших методів перебору. Отримавши ім'я користувача, зловмисник надсилає спеціальний пакет AS_REQ (Authentication Service Request) до KDC (Key Distribution Center), видаючи себе за користувача. KDC надсилає назад AS_REP, який містить частину інформації, зашифровану ключем, отриманим з пароля користувача. Ключ можна підібрати методом перебору, щоб отримати пароль користувача.

За допомогою цієї атаки можна отримати Ticket Granting Ticket (TGT) для будь-якого облікового запису, для якого увімкнено параметр «Не вимагати попередньої автентифікації Kerberos».

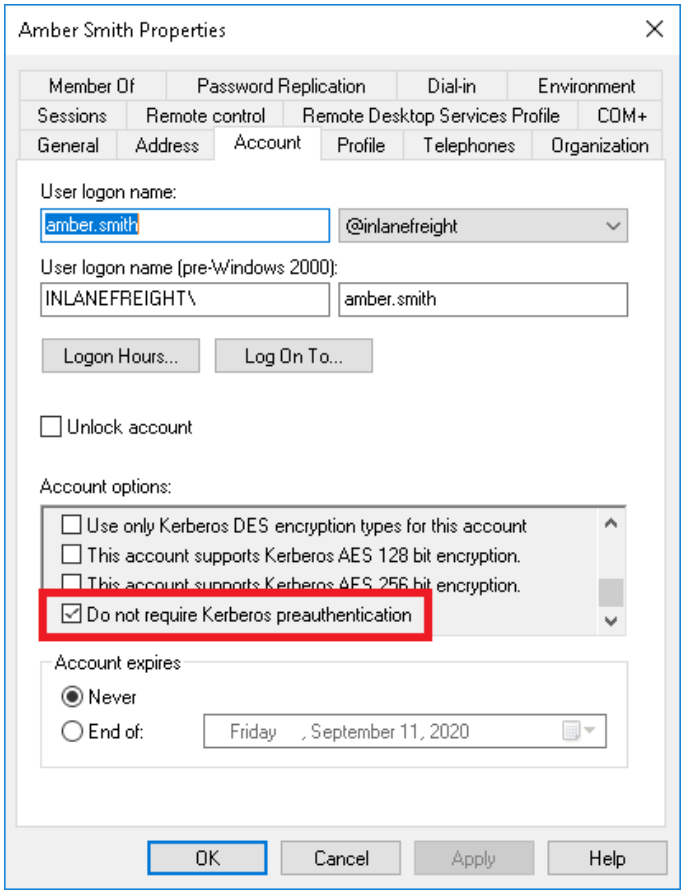


Рис.2. Приклад облікового запису з вимкненою попередньою автентифікацією

Інструмент Rubeus може бути використаний для отримання AS-REP у відповідному форматі для виконання перебору хешу. Ця атака може бути виконана, знаючи лише ім'я облікового запису користувача без встановленої попередньої автентифікації Kerberos.

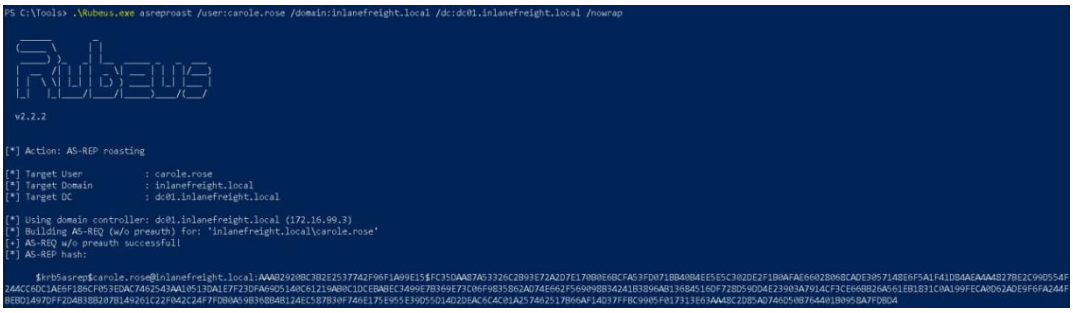


Рис.3. Використання утиліти Rubeus для атаки

В результаті було отримано хеш користувача, який можна спробувати перебрати в офлайн-режимі.

Рис.4. Використання утиліти hashcat для перебору хешу пароля

AS-REPRoasting надає простий спосіб викрасти хеші паролів облікових записів користувачів, які не потребують попередньої автентифікації, без особливих привілеїв. Найкращий спосіб заблокувати атаки AS-REPRoasting - це знайти всі облікові записи користувачів, для яких не потрібна попередня автентифікація Kerberos, а потім увімкнути цей параметр. Ще одним надійним захистом від атак AS-REPRoasting є встановлення довгих, складних паролів, які важко зламати, навіть якщо зловмиснику вдасться їх викрасти. Використання ретельно продуманої парольної політики, особливо для привілейованих облікових записів, є чудовим першим кроком.

Перелік посилань:

1Kerberos Authentication Overview. URL: https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview (дата звернення: 20.10.2024).

2AS-REP Roasting. URL: https://techcommunity.microsoft.com/t5/security-compliance-and-identity/helping-protect-against-as-rep-roasting-with-microsoft-defender/ba-p/2244089 (дата звернення: 20.10.2024).

Клименко Ярослав Валерійович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК КЛЮЧОВА ЗАГРОЗА В КІБЕРБЕЗПЕЦІ

У сучасному світі кількість кібератак стрімко зростає, а методи соціальної інженерії стають усе більш витонченими та складними. Зловмисники використовують психологічні прийоми для маніпулювання людьми, змушуючи їх добровільно розкривати конфіденційну інформацію або

здійснювати дії, що порушують безпеку систем. Фішинг, вішинг, та інші тактики соціальної інженерії еволюціонують, застосовуючи складні сценарії, що апелюють до емоцій, довіри чи навіть страху жертв. Це створює серйозні виклики для фахівців з кібербезпеки, адже на відміну від технічних вразливостей, людський фактор важко передбачити та контролювати. У цій роботі досліджуються сучасні методи соціальної інженерії, аналізуються механізми маніпуляції жертвами та пропонуються шляхи підвищення стійкості до таких атак.

Сучасні інформаційні системи дедалі більше зосереджуються на технологічних аспектах захисту даних, проте людський фактор залишається однією з найслабших ланок у безпеці будь-якої організації. Соціальна інженерія — це техніка маніпулювання людьми з метою отримання конфіденційної інформації або доступу до системи без використання традиційних кіберзломів. Це один із найефективніших методів атаки, оскільки він обходить технічні захисні механізми й орієнтується на психологічні особливості користувачів.

Соціальна інженерія охоплює різні техніки, серед яких фішинг, вішинг (телефонний фішинг), смішинг (фішинг через SMS), а також більш складні атаки, такі як виявлення слабких місць у поведінці співробітників організацій або використання соціальних мереж для отримання інформації про людину. Фішинг, зокрема, є однією з найпоширеніших форм соціальної інженерії, коли зловмисники видають себе за надійні джерела та надсилають користувачам електронні листи або повідомлення з метою збору логінів, паролів або іншої конфіденційної інформації. Більшість успішних фішингових атак пов'язано з недостатньою увагою користувачів до деталей, як-от неправильна адреса відправника, підозрілий зміст повідомлень або використання офіційних логотипів і стилістики.

Одна з найбільших проблем соціальної інженерії полягає в тому, що жодна система безпеки не може повністю захистити організацію від цієї загрози, оскільки вона експлуатує людську природу — довіру, недбалість або страх. Згідно з дослідженнями, приблизно 85% успішних зламів за останні роки були пов'язані із соціальною інженерією, що вказує на критичну важливість підвищення обізнаності серед співробітників щодо цієї загрози.

Методи протидії соціальній інженерії включають регулярне навчання персоналу, використання багатофакторної автентифікації та впровадження політик обмеженого доступу до критично важливої інформації. Навчання є одним із найефективніших засобів протидії, оскільки воно допомагає користувачам розпізнавати потенційні атаки й вживати відповідних заходів. Спеціальні тренінги, симуляції фішингових атак та регулярні перевірки знань працівників можуть значно знизити ризик успішних атак на організацію. Багатофакторна автентифікація (2FA) також є важливою мірою, яка ускладнює зловмисникам отримання доступу до системи, навіть якщо вони вкрали облікові дані користувача.

Отже, соціальна інженерія залишається однією з найважливіших загроз у

сфері кібербезпеки, оскільки вона базується на маніпуляціях і людських помилках. Навчання, підвищення обізнаності та технологічні заходи, такі як багатофакторна автентифікація, є ключовими елементами в боротьбі з цією загрозою. В умовах постійного розвитку методів соціальної інженерії критично важливо підтримувати високий рівень кібербезпеки та забезпечувати постійну співпрацю між технічними фахівцями і працівниками організацій для мінімізації ризиків кібератак.

Перелік посилань:

1. Конхіді Ш. Соціальна інженерія в галузі IT-безпеки: інструменти, тактика та методи / Конхіді Ш. – McGraw-Hill Education, 2014. – 272 с. (date of access: 07.10.2024).
2. Комаров А. TMS управляє життєвим циклів токенов / А. Комаров // CNews. - 2008. - №10. - с. 90-113. (date of access: 07.10.2024).
3. Гаврилов А. Соціальний інжиніринг в дії // Безпека. - 2012. - №3. (date of access: 04.10.2024).

Ковтун Андрій Валерійович
студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

КІБЕРБЕЗПЕКА У СФЕРІ ОХОРОНИ ЗДОРОВ'Я: ЗАХИСТ ПАЦІЄНТСЬКИХ ДАНИХ

У сучасному світі охорона здоров'я стикається з безліччю викликів, і одним з найбільш нагальних є забезпечення кібербезпеки. Від цифрових медичних записів до систем управління лікарнями — усі ці технології зберігають чутливі пацієнтські дані, що робить їх привабливою мішенню для зловмисників. Кібератаки на медичні заклади не лише загрожують безпеці даних, але й можуть мати серйозні наслідки для пацієнтів, на приклад, у випадках, коли відбувається зупинка критично важливих медичних систем.

Згідно з дослідженнями, медичні установи стають жертвами кіберзлочинності частіше, ніж будь-яка інша галузь. Проблема ускладнюється тим, що багато медичних організацій мають застарілі системи, які не отримують регулярних оновлень безпеки. Це створює вразливості, які можуть бути використані для атаки, що в свою чергу може призвести до витоку конфіденційної інформації, такої як медичні записи пацієнтів, результати обстежень і фінансові дані.

Фішинг — один із найбільш поширених методів, які зловмисники використовують для атак на медичні установи. Наприклад, медичні працівники можуть отримати електронні листи, що видають себе за офіційні повідомлення від постачальників програмного забезпечення чи державних установ. Клікнувши на посилання у такому листі, вони можуть ненавмисно завантажити шкідливе програмне забезпечення на систему, що відкриває двері для кібератак.

Окрім цього, важливим аспектом є недостатня обізнаність працівників медичних установ щодо кіберзагроз. Часто співробітники не проходять належне

навчання, що призводить до недбалості у використанні систем безпеки. Регулярні тренінги з кібербезпеки, включаючи симуляції фішингових атак, можуть значно підвищити обізнаність персоналу і зменшити ризики.

Крім того, медичні заклади повинні впроваджувати багатофакторну автентифікацію для доступу до чутливих систем. Це ускладнить зловмисникам отримання доступу, навіть якщо їм вдасться зламати облікові записи співробітників. На додаток до цього, регулярні перевірки та оновлення програмного забезпечення можуть значно підвищити загальний рівень безпеки.

Не менш важливим є і забезпечення безпеки пристроїв Інтернету речей (IoT), які дедалі частіше використовуються в охороні здоров'я. Пристрої, такі як монітори пацієнтів, можуть бути вразливими до кібератак, якщо не мають належного захисту. Вибір надійних виробників і постійний моніторинг безпеки пристроїв є критично важливими для запобігання атакам.

На сьогоднішній день захист пацієнтських даних у сфері охорони здоров'я потребує комплексного підходу, що включає технологічні, організаційні та людські аспекти. Важливо, щоб керівництво медичних установ усвідомлювало серйозність кіберзагроз і інвестувало в сучасні рішення безпеки. Це не лише захистить конфіденційну інформацію, але й збережеться довіра пацієнтів, що є основоположним фактором у будь-якій медичній практиці.

Отже, кібербезпека у сфері охорони здоров'я є невід'ємною частиною сучасної медицини. Без належного захисту даних пацієнтів ризики не лише для особистої інформації, але й для фізичного здоров'я можуть стати критичними. Справжня кібербезпека вимагає зусиль з усіх боків — від керівництва до кожного співробітника, оскільки в сучасному світі кіберзагрози постійно еволюціонують, а від нас залежить, як ми до них підготуємося.

Перелік посилань:

1. Основи кібербезпекиURL: https://moz.gov.ua/uk/osnovi-kiberbezpeki-2 (date of access: 07.10.2024).
2. Питання кібербезпеки у сфері охорони здоров'я та захисту персональних даних обговорили на Національному кластері кібербезпеки. URL: https://www.rnbo.gov.ua/ua/Diialnist/6365.html (date of access: 05.10.2024).
3. Загрози кібербезпеці в галузі охорони здоров'я. URL: https://eska.global/blog/zagrozi-kiberbezpeci-v-galuzi-ohoroni-zdorovya (date of access: 04.10.2024).

Компанець Георгій Сергійович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

КІБЕРЗАГРОЗИ В ХМАРНИХ СЕРЕДОВИЩАХ

Хмарні технології стають невід'ємною частиною сучасного бізнесу, дозволяючи організаціям зберігати дані, управляти додатками та забезпечувати доступ до інформації з будь-якої точки світу. Проте з поширенням хмарних середовищ зростає і кількість нових кіберзагроз, які націлені на ці платформи. Хоча хмарні рішення надають значні переваги, вони також відкривають нові вразливості, які можуть бути використані зловмисниками.

Однією з головних загроз у хмарних середовищах є незахищені конфігурації. Багато організацій використовують хмарні сервіси, не приділяючи достатньої уваги налаштуванню систем безпеки. Це може призвести до того, що конфіденційні дані залишаються відкритими для доступу ззовні, і зловмисники можуть скористатися цими вразливостями. За оцінками експертів, більшість витоків даних у хмарних середовищах відбувається через неправильне налаштування захисних механізмів або слабкі паролі.

Також варто зазначити, що хмарні середовища часто піддаються атакам на рівні інфраструктури. Атаки типу «відмова в обслуговуванні» (DDoS) можуть призвести до того, що хмарні сервіси стають недоступними для користувачів. Оскільки бізнес-процеси все більше залежать від безперебійного функціонування хмарних рішень, такі атаки можуть мати серйозні наслідки для компаній, завдаючи фінансових збитків та підриваючи довіру клієнтів.

Ще однією критичною проблемою є загроза з боку невідповідного управління доступом. У хмарних середовищах багато користувачів і служб мають доступ до даних та ресурсів, і якщо не налаштовані чіткі політики контролю доступу, це може призвести до витоків або несанкціонованого доступу. Важливим аспектом тут є впровадження багатофакторної автентифікації (MFA) та регулярний аудит прав доступу, щоб гарантувати, що лише уповноважені особи мають доступ до критичних даних.

Також хмарні середовища стають мішенню для атак з боку інсайдерів — працівників або підрядників, які можуть зловживати своїми привілеями для викрадення даних або порушення роботи систем. Оскільки багато процесів у хмарі відбуваються поза прямим контролем організації, відстеження активності та моніторинг підозрілих дій є особливо важливими для запобігання інцидентам.

Щоб ефективно протистояти загрозам у хмарних середовищах, організаціям слід впроваджувати комплексні стратегії безпеки. Це включає належне налаштування конфігурацій, регулярні оновлення систем, моніторинг активності, а також навчання працівників щодо ризиків і правильних практик роботи з хмарними сервісами.

Захист хмарного середовища — це спільна відповідальність, яка потребує уваги як з боку провайдерів хмарних послуг, так і з боку організацій, що їх використовують. Лише постійна взаємодія та готовність до нових викликів можуть забезпечити надійний захист від кіберзагроз у хмарі.

Перелік посилань:

1. Що таке Bring Your Own Encryption і чому це важливо. URL: https://gigacloud.ua/blog/navchannja/scho-take-bring-your-own-encryption-i-chomu-ce-vazhlivo (date of access: 07.10.2024).
2. Найкращі практики захисту хмарних сховищ. URL: https://iitd.com.ua/news/najkrashhi-praktiki-zahistu-hmarnih-shovishh/ (date of access: 05.10.2024).
3. Захист хмарного середовища потребує інших підходів. URL: https://ko.com.ua/zahist_hmarnogo_seredovishha_potrebuye_inshih_pidhodiv_147833 (date of access: 04.10.2024).

Компанець Олександр Сергійович, БСДМ-63
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КЛІЄНТІВ ЗА ДОПОМОГОЮ AKAMAI IDENTITY CLOUD

Визначено мету і основні завдання щодо управління ідентифікацією та доступом клієнтів до інформаційних ресурсів. Розглянуто зміст технології управління ідентифікацією та доступом клієнтів за допомогою Akamai Identity Cloud.

У Звіті Imperva [1] зазначається, що атаки захоплення облікового запису є одними з найпоширеніших автоматичних загроз. Вони передбачають використання ботів для спроб несанкціонованого доступу та захоплення облікових записів користувачів за допомогою методів підміни облікових даних і злому, що призводить до крадіжки цифрових даних і значних збитків для організацій. Згідно з даними Aite Group, збитки від крадіжки особистих даних у 2023 році сягнуть 635,4 мільярдів доларів [1]. На рисунку 1 представлені статистичні дані про щомісячні атаки захоплення облікового запису, зафіксовані Imperva за останні два роки.

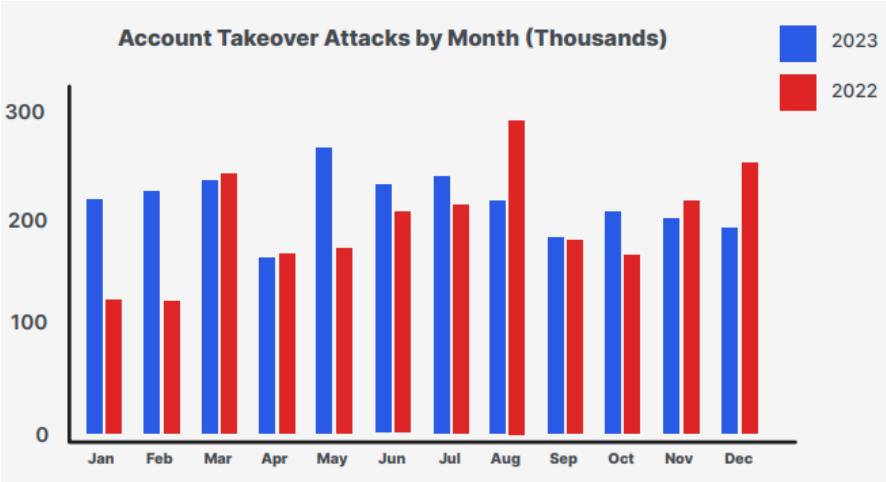


Рис. 1. Статистика щомісячних атак захоплення облікового запису, зафіксовані Imperva [1]

Підприємства використовують рішення ідентифікації клієнтів і керування доступом (Customer Identity and Access Management, CIAM), щоб контролювати доступ до загальнодоступних веб-сайтів і цифрових ресурсів. Рішення CIAM полегшують клієнтам реєстрацію та вхід у онлайн-додатки та служби. Вони допомагають захистити конфіденційність даних і захистити від крадіжки особистих даних та інших видів шахрайства та зловживань. І вони дозволяють клієнтам легко керувати своїми профілями облікових записів і налаштуваннями безпеки самостійно [2].

Рішення CIAM спрощують для компаній додавання функцій реєстрації користувачів і надійного керування ідентифікацією та контролю доступу до корпоративних додатків, орієнтованих на клієнтів. Вони допомагають компаніям покращити взаємодію з клієнтами, посилити безпеку та дотриматися вимог щодо конфіденційності даних, таких як GDPR [2].

Рішення CIAM зазвичай надаються як хмарні служби, які розміщуються та керуються надійною третьою стороною для максимальної простоти, гнучкості та масштабованості. Необхідно підкреслити, що збираючи та обробляючи дані клієнтів, організації повинні дотримуватися багатьох правил захисту даних і конфіденційності. Рішення для керування ідентифікацією, наприклад Akamai Identity Cloud, може допомогти впоратися з цими проблемами.

Розглянемо зміст технології управління ідентифікацією та доступом клієнтів за допомогою Akamai Identity Cloud (рисунок 2) [3]:

1. Кінцевий користувач отримує доступ до цифрових ресурсів компанії з різних каналів (браузерів для настільних комп’ютерів, мобільних додатків, Інтернету речей) часто використовуючи вхід із соціальної мережі.

2. Граничні сервери захищають загальнодоступні веб-додатки, сторінки входу та сторінки реєстрації від DDoS-атак і атак веб-додатків.

3. Керування ботом виявляє та пом’якшує автоматичні загрози, зокрема сканування веб-сторінок і надсилання облікових даних.

4. Платформа Akamai Intelligent Edge і її рішення безпеки захищають Akamai Identity Cloud від зловмисних атак.

5. Akamai Intelligent Edge Platform направляє законний трафік на сторінки реєстрації та входу в цифрові ресурси компанії.

6. Akamai Identity Cloud допомагає підприємствам дотримуватися відповідних норм захисту даних.

7. Akamai Identity Cloud – це рішення ідентифікації як послуги (Identity as a Service, IDaaS), яке дозволяє організаціям надавати кінцевим користувачам контроль над створенням, використанням і керуванням їхніми даними.

8. Центральна база даних профілів клієнтів є єдиним джерелом правдивих відомостей про ідентифікацію кінцевих користувачів і права доступу.

9. Клієнти можуть отримувати доступ, переглядати, редагувати та відкликати згоду за допомогою централізованого самообслуговування.

10. Контроль доступ до рівня окремих полів запису даних як для користувачів, так і для додатків.

11. Akamai Identity Cloud інтегрується зі сторонніми системами для подальшої обробки даних клієнтів, наприклад стека маркетингових технологій.

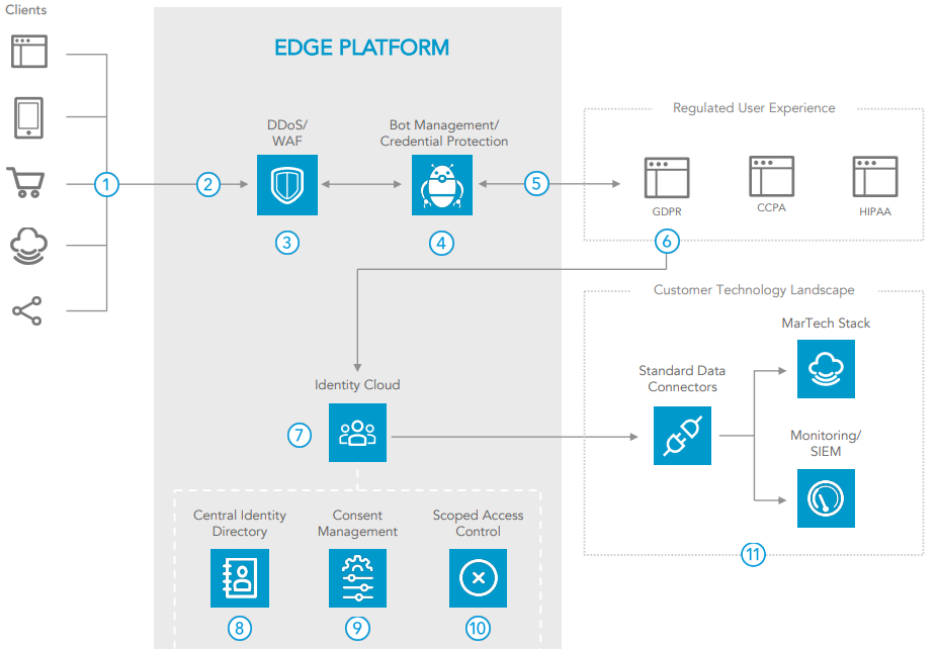


Рис. 2. Схема реалізації технології управління ідентифікацією та доступом клієнтів за допомогою Akamai Identity Cloud [3]

Як продукт керування інформацією та доступом клієнтів (CIAM), основна задача Akamai Identity Cloud полягає в тому, щоб дозволити користувачам створювати облікові записи у корпоративному додатку чи на веб-сайті, а потім мати можливість повернутися на цей веб-сайт чи додаток та увійти до свого облікового запису [4].

Щоб допомогти керувати логінами та реєстраціями, функція розміщеного

входу Akamai Identity Cloud широко використовує як OAuth, так і OpenID Connect, пропонуючи підтримку для таких речей, як різні типи дозволів, різні типи відповідей і режимів, а також широкий спектр областей і претензій (включаючи спеціальні претензії) [4].

Отже, рішення Akamai Identity Cloud забезпечує клієнтам винятковий досвід користувача під час створення, використання та керування особистими обліковими записами. Akamai Identity Cloud дозволяє реалізувати високу масштабованість на основі програмного забезпечення як послуги (SaaS), яке може обробляти сотні мільйонів ідентифікацій. Akamai Identity Cloud реалізує функції сервера для керування обліковими записами та контролювати їх, а також зберігати, аналізувати та звітувати про дані профілів клієнтів. Це рішення працює на всіх додатках і підключених пристроях, щоб уніфікувати та захистити ідентифікаційні дані відповідно до нормативних вимог.

Перелік посилань:

1. 2024 Imperva Bad Bot Report. URL: https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/ (дата звернення: 04.10.2024).
2. What is Customer Identity and Access Management (CIAM)? CyberArk. URL: https://www.cyberark.com/what-is/ciam/ (дата звернення: 04.10.2024).
3. Global Compliance – Customer: Reference Architecture. Akamai. URL: https://www.akamai.com/resources/reference-architecture/global-compliance-customer (дата звернення: 04.10.2024).
4. How Identity Cloud works. Akamai. URL: https://techdocs.akamai.com/identity-cloud/docs/an-introduction-to-identity-cloud (дата звернення: 04.10.2024).

Коровайченко Юрій Юрійович
аспірант групи АІКБ-21, ННІЗІ ДУІКТ, Київ, Україна

ПОРІВНЯННЯ ЕФЕКТИВНОСТІ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ ДЛЯ ДЕТЕКТУВАННЯ ШКІДЛИВОГО ТРАФІКУ

Технологія Машинного навчання зосереджується на розробці алгоритмів і моделей, здатних автоматично вивчати та вдосконалюватись на основі для виконання поставлених завдань. Основні підходи включають контрольоване навчання, де моделі навчаються на заданих даних для прогнозування або класифікації нових зразків, та неконтрольоване навчання, яке шукає приховані структури або патерни у випадкових даних. У сфері мережевої безпеки машинне навчання застосовується для виявлення та класифікації шкідливого трафіку шляхом аналізу великих обсягів мережевих даних та ідентифікації аномалій, що свідчать про потенційні загрози.

Зі зростанням обсягу та складності кіберзагроз традиційні сигнатурні методи виявлення вже сьогодні стали недостатньо ефективними. Машинне навчання пропонує ефективні інструменти для автоматичного виявлення та класифікації шкідливого трафіку, забезпечуючи адаптивність та високу точність. Метою цієї роботи є порівняння ефективності різних моделей машинного навчання у задачі

детектування шкідливого трафіку.

Моделі машинного навчання що пропонуються для розгляду

Детектування шкідливого трафіку за допомогою машинного навчання охоплює широкий спектр моделей, кожна з яких має свої переваги та недоліки. Основні моделі, що пропонуються до розгляду - наступні:

1. Logistic Regression;
2. Decision Trees;
3. Random Forest;
4. Support Vector Machines;
5. Naive Bayes algorithm;
6. Gradient Boosting.

Аналіз моделей машинного навчання

Logistic Regression є однією з найпростіших і найпоширеніших моделей машинного навчання, яка використовується для задач бінарної класифікації, включаючи детектування шкідливого трафіку. Вона базується на статистичному методі, який оцінює ймовірність належності об'єкта до певного класу за допомогою логістичної функції. Дана модель передбачає лінійну комбінацію вхідних ознак, яка потім перетворюється в значення 0 і 1, що інтерпретується як ймовірність належності до класу. Недоліки Logistic Regression полягають у її обмеженій здатності моделювати складні нелінійні залежності між ознаками. У випадках, коли дані мають складні патерни або взаємодії між ознаками, модель може не досягати високої точності порівняно з більш складними алгоритмами, такими як Decision Trees**.**

Decision Trees є однією з найбільш інтуїтивних моделей машинного навчання для класифікації та регресії, включаючи детектування шкідливого трафіку. Вони представляють собою ієрархічну структуру, де кожен вузол відповідає за перевірку певної ознаки, а гілки ведуть до подальших рішень або кінцевих класів. Переваги Decision Trees включають простоту розуміння та інтерпретації, а також здатність обробляти як числові, так і категоріальні дані без необхідності попередньої нормалізації. Недоліки полягають у схильності до перенавчання, особливо при використанні глибоких моделей, що може знижувати їхню узагальнюваність. Для покращення стабільності та точності часто використовують ансамблеві методи, такі як Random Forest. Decision Trees забезпечують кращу точність порівняно з простішими моделями, однак їхня ефективність може бути підвищена шляхом комбінування з іншими техніками машинного навчання.

Random Forest є ансамблевим методом машинного навчання, який поєднує кілька дерев рішень для підвищення точності та зменшення ризику перенавчання. Кожне дерево навчається на випадковій вибірці даних і випадковій підмножині ознак, що забезпечує різноманітність моделей і покращує їхню загальну

продуктивність. Переваги Random Forest включають високу точність, стабільність результатів та здатність ефективно обробляти великі обсяги даних з багатьма ознаками. Недоліки полягають у більшій обчислювальній складності порівняно з окремими Decision Trees та меншій інтерпретованості моделі. Random Forest перевершує прості моделі, такі як Logistic Regression чи Decision Trees, завдяки своїй здатності ефективно виявляти складні патерни в даних.

Support Vector Machines є ефективною моделлю машинного навчання, що використовуються для класифікації та регресії. Основна ідея SVM полягає в знаходженні гіперплощини, яка найкраще розділяє різні класи даних з максимальною відстанню між найближчими точками кожного класу (підтримувальними векторами). Переваги SVM включають високу точність та ефективність при роботі з високорозмірними даними та складними патернами завдяки використанню різних функцій. Недоліки полягають у високій обчислювальній складності при великих наборах даних та складності вибору оптимального ядра і налаштування гіперпараметрів. Враховуючи великі обсяги мережевого трафіку – цей недолік є критичним для даної моделі, в задачах виявлення шкідливого трафіку.

Naive Bayes algorithm є простим і швидким методом класифікації, що базується на теоремі Байєса з припущенням незалежності між ознаками. Він може використовуватись для виявлення шкідливого трафіку завдяки своїй ефективності при роботі з великими наборами даних. Переваги алгоритму включають легкість реалізації, високу швидкість навчання та здатність ефективно працювати навіть при невеликій кількості наявних зразків даних. Недоліки полягають у припущенні повної незалежності ознак, що може знижувати точність моделі при наявності корельованих ознак.

Gradient Boosting є ансамблевим методом машинного навчання, який комбінує кілька слабких моделей, зазвичай дерев рішень, для створення ефективної моделі. Він працює шляхом послідовного додавання дерев, кожне з яких навчається виправляти помилки попередніх моделей шляхом мінімізації функції втрат. Переваги Gradient Boosting включають високу точність, здатність виявляти складні патерни та адаптивність до різних типів даних. Недоліки полягають у високій обчислювальній складності та потребі ретельного налаштування гіперпараметрів.

Виклики та перспективи машинного навчання

Порівняльний аналіз показав, що ансамблеві методи на основі дерев рішень, зокрема **Random Forest** та **Gradient Boosting**, є одними з найефективніших моделей машинного навчання для детектування шкідливого трафіку. Вони забезпечують високу точність та стабільність результатів завдяки комбінуванню декількох дерев рішень, що дозволяє ефективно виявляти як відомі, так і нові загрози.

Інші моделі, в свою чергу, демонструють або високу точність завдяки

високій обчислювальній складності, або недостатню точність.

Для подальшого покращення систем детектування рекомендується комбінувати ансамблеві методи з іншими техніками машинного навчання, а також оптимізовувати їхню обчислювальну ефективність для інтеграції у реальні системи кібербезпеки з високим навантаженням.

Перелік посилань:

1. **Hastie, T., Tibshirani, R., & Friedman, J.** (2009). *The Elements of Statistical Learning*
2. **Bishop, C. M.** (2006). *Pattern Recognition and Machine Learning*
3. **Sommer, R., & Paxson, V.** (2010). *Outside the closed world: On using machine learning for network intrusion detection*
4. **Breiman, L.** (2001). *Random forests. Machine Learning.*
5. **Lang, B., & Liu, H.** (2019). *Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey*

Корчук Дмитрій Вікторович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ВАЖЛИВІСТЬ ВИКОРИСТАННЯ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ ТА СУТНОСТЕЙ В СУЧАСНИХ КОРПОРАТИВНИХ МЕРЕЖАХ

В умовах швидкого зростання кібератак та постійного розвитку технологій, корпоративні мережі стикаються з новими викликами в сфері інформаційної безпеки. Традиційні методи захисту, такі як брандмауери, антивірусні програми та системи виявлення вторгнень, вже не можуть забезпечити належного рівня захисту від сучасних загроз. Зокрема, зростає кількість складних атак, які використовують внутрішні ресурси організацій, зокрема облікові записи користувачів. Тому впровадження нових підходів до виявлення аномальної активності та аналізу поведінки користувачів стає критично важливим. Одним із таких рішень є аналіз поведінки користувачів та сутностей.

Аналіз поведінки користувачів та сутностей.

UEBA - термін, вперше введений компанією Gartner у 2015 році, є розвитком аналізу поведінки користувачів (UBA). [1] Якщо UBA відстежувала лише моделі поведінки кінцевих користувачів, то UEBA також відстежує об'єкти, що не є користувачами, такі як сервери, маршрутизатори та пристрої Інтернет речей (IoT), на предмет аномальної поведінки або підозрілої активності, що може свідчити про загрози безпеці або атаки.

UEBA ефективно виявляє внутрішні загрози зловмисних інсайдерів або хакерів, які використовують скомпрометовані облікові записи і можуть бути непоміченими іншими інструментами безпеки, оскільки вони імітують авторизований мережевий трафік.

Використання UEBA з іншими системами безпеки.

UEBA використовується в операційних центрах безпеки (SOC) разом з іншими інструментами корпоративної безпеки, а функціональність UEBA часто включається в такі рішення корпоративної безпеки, як системи управління

інформацією і подіями інформаційної безпеки (SIEM), захист кінцевих точок (EDR), розширене виявлення і реагування (XDR), а також управління ідентифікацією та доступом (IAM).

Три основні компоненти UEBA:

1. Аналітика збирає, аналізує та сортирує дані про те, що вона визначає як нормальну поведінку користувачів та об’єктів. Система створює профілі того, як кожен з них зазвичай діє щодо використання додатків, активності спілкування та завантаження, а також мережевого трафіку. Потім формуються статистичні моделі, які застосовуються для виявлення аномальної поведінки.

2. Інтеграція з іншими продуктами та системами безпеки, що вже існують, є обов'язковою, оскільки організації ростуть і розвиваються. Перевага UEBA полягає в тому, що він не призначений для усунення чи заміни існуючих продуктів безпеки, які використовуються на підприємстві. При належній інтеграції системи UEBA можуть порівнювати дані, зібрані з різних джерел, включаючи журнали, дані перехоплення пакетів та інші набори даних, і інтегрувати їх, щоб зробити систему більш надійною.

3. Презентація - це процес інформування про результати роботи системи UEBA та розробка відповідної реакції. Він може відрізнятися в різних організаціях. Деякі системи UEBA просто створюють сповіщення для працівника або IT-адміністратора, щоб запропонувати подальше розслідування. Інші системи UEBA налаштовані на негайні дії - наприклад, на автоматичне вимкнення мережевого з'єднання для цього працівника через підозру в компрометації облікового запису.

Машинне навчання в UEBA.

UEBA використовує алгоритми машинного навчання та статистичний аналіз для виявлення аномальної поведінки у мережі. Після того, як UEBA створює статистичну модель для очікуваної поведінки та дій кожного суб'єкта в мережі, він може дослідити дані та оцінити всі дії відповідно до цих моделей. [2]

За допомогою викраденого пароля зловмисник може проникнути в систему. Однак UEBA відстежує всю поточну діяльність і вловлює тонкі відмінності між поведінкою всередині вашої організації. Прикладом поведінкових відмінностей може бути об'єднання в групи за принципом «рівний-рівному»: UEBA створює статистичну модель поведінки не лише для кожного користувача, але й для команд або визначених груп тощо. Наприклад, якщо хтось у команді отримує доступ до незвичного для нього файлу, але решта членів команди отримує доступ до цього файлу регулярно, така поведінка не позначається і не стає помилковим спрацьовуванням, оскільки вона не є ненормальною для команди. UEBA відстежує ці тонкі відмінності і створює модель порівняння, зменшуючи кількість хибних спрацьовувань, коли людина робить щось нове, що в іншому випадку є поширеною практикою в команді. Це значно підвищує рівень корпоративної безпеки.

Щойно зловмисник увійде в систему за допомогою викраденого пароля, UEBA порівняє деталі того, що відбувається, з моделлю поведінки справжнього власника пароля. Щоб залишитися непоміченим, хакер повинен успішно

повторити звичайний шаблон поведінки іншої людини. Як тільки його дії розходяться зі моделлю поведінки, UEBA вказує на це.

Завдяки своїй здатності обробляти великі обсяги даних, машинне навчання значно краще здатне виявляти сучасні загрози, ніж людина-аналітик. Воно також може ідентифікувати та кількісно оцінити поведінкові моделі, які людина-аналітик, можливо, не врахувала.

Результатом є виявлення аномалій у всіх ваших системах, таких як додатки, мережі, файлові операції та дії користувачів. Всі аномалії, які виходять за рамки попереднього шаблону, документуються як потенційно ризиковані. Потім організація отримує інформацію за допомогою автоматизованих сповіщень, а потенційні загрози пріоритезуються за важливістю, що полегшує управління ними.

Машинне навчання також може розпізнати щось незвичне - навіть коли активність ще не зрозуміла. За задумом, машинне навчання продовжує «вчитися» і підлаштовується під поведінку легітимних користувачів.

Важливість наявності UEBA в корпоративних мережах.

Кількість фішингових атак та атак з використанням соціальної інженерії зростає з кожним роком. У світі кібербезпеки, кількість атак зросла на 65% в період з 2019 до 2021 року, і у 2023 році фішинг продовжує залишатися однією з найбільш поширених кіберзагроз. [3]

Соціальна інженерія та фішингові атаки. Ці стратегії атакують не апаратне забезпечення організації, а її людей, переконуючи співробітників переходити по посиланням, завантажувати програмне забезпечення та надсилати паролі. Зараження одного комп'ютера - це лише початок потенційно масштабної кібератаки. UEBA прагне виявити навіть найменші прояви незвичної поведінки та запобігти переростанню невеликої фішингової схеми у масштабний витік даних.

Компрометація облікових засобів у компаніях є серйозною проблемою, яка продовжує зростати. У 2023 році кількість випадків компрометації даних зросла на 72% у порівнянні з 2022 роком, досягнувши рекордних 3,205 інцидентів. Це включає атаки на паролі, облікові записи, а також кібератаки, пов'язані з фішингом і крадіжкою ідентифікаційних даних. Значна частина компрометацій сталася через соціальну інженерію та недостатній захист від атаки на облікові дані, такі як багатофакторна автентифікація (MFA) та моніторинг привілейованих акаунтів. [4]

Також спостерігається зростання атак на привілейовані облікові записи. Наприклад, 63% організацій заявили, що доступ до важливих ресурсів у них недостатньо захищений. Злочинці активно використовують такі вразливості, як неправильна конфігурація MFA або викрадення облікових записів через фішинг.

Ці компрометації часто призводять до великих фінансових втрат, з середньою вартістю одного інциденту близько 4.62 мільйонів доларів. Це також впливає на час відновлення систем після атаки, який може тривати до 11 місяців.

Перелік посилань:
1. What is user and entity behavior analytics (UEBA)? URL: https://www.ibm.com/topics/ueba
2. What is User and Entity Behavior Analytics? A complete guide to UEBA, how it works, and its benefits URL: https://www.logpoint.com/en/blog/ueba-user-and-entity-behavior-analytics/
3. 81 Phishing Attack Statistics 2024: The Ultimate Insight URL: https://www.getastra.com/blog/security-audit/phishing-attack-statistics/
4. Identity Theft Resource Center 2023 Annual Data Breach Report Reveals Record Number of Compromises; 72 Percent Increase Over Previous High URL: https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/

Кривець Данило Олександрович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

Захист від фішингових атак в організаціях: основні підходи та інструменти

У сучасному світі фішингові атаки продовжують залишатися одними з найнебезпечніших видів загроз для організацій. Зловмисники націлюються на облікові дані співробітників та конфіденційну інформацію, використовуючи соціальну інженерію та фальшиві вебсайти для отримання доступу до корпоративних систем [1].

Як фішингові атаки націлюються на організації?

Фішингові атаки здійснюються через електронні листи, SMS або повідомлення в соціальних мережах. Зловмисники часто маскуються під надійні джерела, такі як банки чи урядові установи, змушуючи користувачів відкривати шкідливі посилання або завантажувати небезпечні файли [2].

Фішингові атаки є надзвичайно небезпечним інструментом для кіберзлочинців, які намагаються отримати доступ до критично важливої інформації. Основні цілі фішингових атак охоплюють широкий спектр даних, що можуть бути використані як для негайного отримання фінансової вигоди, так і для довгострокових шахрайських схем. Нижче наведені ключові цілі, на які спрямовані фішингові атаки:

1. **Облікові дані користувачів**: Одна з найчастіших цілей фішингових атак це отримання імен користувачів і паролів. Зловмисники намагаються викрасти ці дані для доступу до облікових записів, таких як корпоративні системи, банківські рахунки, поштові скриньки або соціальні мережі. Використання викрадених облікових даних дозволяє їм отримати повний контроль над ресурсами, до яких має доступ жертва [1].
2. **Фінансова інформація**: Зловмисники активно націлюються на дані платіжних карток, банківські реквізити та інші фінансові відомості. Фінансова інформація може бути використана для шахрайських операцій, зняття грошей або продажу цих даних на чорному ринку. Поширеною

практикою є підробка банківських вебсайтів або платіжних систем для збору конфіденційних відомостей [2].

3. **Клієнтські бази даних**: Організації зберігають величезну кількість інформації про своїх клієнтів, включаючи контактні дані, історію покупок та інші персональні дані. Фішингові атаки можуть бути спрямовані на отримання доступу до цих баз даних з метою їхнього продажу або використання для подальших атак на клієнтів [3].
4. **Системи внутрішнього документообігу**: Зловмисники також часто націлюються на внутрішні корпоративні документи та системи документообігу. Викрадені дані можуть включати комерційні таємниці, стратегії компаній, юридичні документи або проекти договорів, що може завдати значної шкоди бізнесу. Крім того, ці документи можуть бути використані для шантажу або інших видів атак [4].

Методи виявлення фішингових атак

Фішингові атаки залишаються основним інструментом кіберзлочинців для отримання доступу до конфіденційної інформації. Сучасні методи виявлення таких атак базуються на аналізі змісту повідомлень, поведінкових ознаках та використанні штучного інтелекту. Один із найпоширеніших методів виявлення фішингу полягає у перевірці тексту електронних листів на наявність підозрілих ознак, таких як неправильна граматика, підозрілі посилання або неправдиві доменні імена [1]. Інструменти для аналізу вмісту автоматично сканують повідомлення, шукаючи характерні ознаки фішингових атак. Фішингові атаки часто спрямовані на перенаправлення користувачів на підроблені вебсайти, де зловмисники можуть збирати їх облікові дані. DNS та URL-фільтри допомагають визначати підозрілі або відомі шкідливі домени, блокуючи їх доступ до користувача [2]. Метод поведінкового аналізу використовує моделі поведінки користувачів для виявлення аномалій.

Наприклад, якщо система помічає, що користувач несподівано намагається увійти з іншої країни або через незвичний пристрій, це може бути ознакою фішингової атаки [3]. Такий аналіз допомагає виявити спроби несанкціонованого доступу навіть у випадках, коли фішингові повідомлення успішно пройшли через інші бар’єри. Штучний інтелект (AI) та машинне навчання відіграють важливу роль у сучасних системах виявлення фішингу. AI здатен автоматично навчатися на великій кількості фішингових зразків, покращуючи точність і швидкість виявлення нових загроз [4]. Це дозволяє системам адаптуватися до нових методів фішингових атак. Навіть якщо фішингова атака вдається отримати облікові дані користувача, впровадження багатофакторної автентифікації (MFA) може запобігти доступу до системи. MFA забезпечує додатковий рівень захисту, вимагаючи підтвердження

через інший канал, наприклад, SMS або мобільний додаток [5].

Методи захисту від фішингових атак

Захист від фішингових атак потребує впровадження багаторівневої стратегії, що включає як технічні, так і поведінкові заходи. Ось основні методи, які допомагають ефективно протидіяти фішинговим атакам:

Освітні програми для співробітників: Одним із найбільш ефективних засобів захисту є навчання персоналу. Співробітники повинні бути обізнані щодо методів фішингових атак, ознак підозрілих електронних листів та правильних дій у випадку їх виявлення. Регулярні тренінги, тестові фішингові атаки та інформування щодо нових загроз дозволяють зменшити ризик успішного фішингу в організації [1]. Багатофакторна автентифікація (MFA): Використання багатофакторної автентифікації є потужним інструментом для захисту облікових записів. Навіть якщо зловмисники отримали логін і пароль користувача, MFA додає додатковий рівень захисту, вимагаючи підтвердження особи через додатковий канал, такий як SMS або мобільний додаток [2].

Антифішингові фільтри: Сучасні антифішингові фільтри здатні автоматично виявляти й блокувати шкідливі електронні листи та повідомлення до того, як вони досягнуть користувача. Такі фільтри аналізують зміст повідомлень, їх відправників, домени та інші фактори для визначення ймовірності фішингової атаки [3]. Регулярне оновлення програмного забезпечення: Оновлення програмного забезпечення — це важливий захід для захисту від фішингових атак, оскільки застаріле ПЗ часто має вразливості, які можуть бути використані зловмисниками. Своєчасне оновлення браузерів, операційних систем, плагінів та антивірусного програмного забезпечення допомагає запобігти використанню відомих вразливостей [4].

Фішингові атаки залишаються однією з найбільш поширених і небезпечних загроз у сфері кібербезпеки. Зловмисники використовують різноманітні техніки для викрадення облікових даних, фінансової інформації та доступу до внутрішніх систем компаній. Для ефективного захисту від таких атак необхідно впроваджувати багаторівневі заходи безпеки, які включають освітні програми для співробітників, використання багатофакторної автентифікації, антифішингові фільтри та регулярне оновлення програмного забезпечення. Запобігання фішинговим атакам вимагає не лише технічних засобів, але й підвищення обізнаності користувачів про можливі загрози. Завдяки комплексному підходу до захисту, організації можуть значно зменшити ризик компрометації даних і забезпечити безпечну роботу своїх інформаційних систем.

Перелік посилань:

1. Захист від фішингових атак в організаціях. URL: https://www.cybersecurityguide.org/phishing (дата звернення: 12.10.2024).
2. Фішинг та соціальна інженерія в кібербезпеці. URL: https://www.phishing.org/social-engineering (дата звернення: 12.10.2024).
3. Навчання співробітників для захисту від фішингу. URL: https://www.phishingtraining.com (дата звернення: 12.10.2024).
4. Методи багатофакторної автентифікації. URL: https://www.mfa-security.org (дата звернення: 12.10.2024).
5. Антифішингові фільтри та захист електронної пошти. URL: https://www.email-security.com (дата звернення: 12.10.2024).

Куліш Єгор Олександрович,
студент групи ТСДМ-61, ННІТ ДУІКТ, Київ, Україна

ЕФЕКТИВНІСТЬ ЧОРНИХ СПИСКІВ У ЗАПОБІГАННІ DDOS-АТАКАМ

У сучасному цифровому середовищі DDoS-атаки (Distributed Denial of Service) стали однією з найпоширеніших загроз для інформаційних систем. Ці атаки, що використовують зловмисний трафік для перевантаження ресурсів цільових серверів, можуть призвести до значних фінансових втрат, зниження довіри клієнтів та навіть зупинки критично важливих сервісів. Атакуючи мережу з багатьох джерел одночасно, зловмисники ускладнюють завдання захисту.

У відповідь на ці виклики розроблено кілька методів захисту, серед яких чорні списки (blacklists) є одним із найпоширеніших і найефективніших способів блокування шкідливого трафіку. Чорні списки дозволяють виявляти та блокувати IP-адреси, які мають історію шкідливих дій, забезпечуючи перший рівень захисту для мережевих ресурсів. У цій тезі буде розглянуто принципи роботи чорних списків, їх переваги та недоліки, а також їх роль у запобіганні DDoS-атакам у контексті зростаючих кіберзагроз.

Процес роботи чорних списків

1. **Додавання записів до чорних списків.** Системи безпеки, такі як брандмауери, Layer 2 брандмауери, IPS (системи запобігання вторгненням) або віртуальні системи, створюють власні чорні списки на основі трафіку, який вони перевіряють [1]. Кожна система має свій окремий чорний список, що дозволяє їй оперативно реагувати на виявлені загрози.
2. **Комунікація в кластерах.** У випадку кластерів систем існує один чорний список для всього кластера. Вузли в кластері обмінюються інформацією про чорні списки під час своїх синхронізаційних комунікацій. Це забезпечує узгодженість даних про шкідливі IP-адреси серед усіх компонентів системи [1].
3. **Запити на внесення до чорного списку.** Лог-сервери надсилають запити на внесення IP-адрес до чорного списку у відповідь на кореляцію виявлених подій. Коли одна система надсилає запит на внесення адреси до чорного списку іншій, лог-сервер передає цей запит до менеджерського сервера [1].
4. **Управління чорними списками.** Менеджерські сервери обробляють команди на внесення адрес до чорного списку, які надходять від адміністраторів, а

також запити, отримані від лог-серверів. Важливо зазначити, що між різними віртуальними системами не існує прямої комунікації, тому вони не можуть надсилати запити на внесення адрес до чорного списку один одному [1].

5. **Виконання правил доступу.** Системи реалізують записи своїх чорних списків відповідно до правил доступу. Кожен запис у чорному списку існує лише на визначений термін, після чого його видаляють, і відповідні з'єднання знову дозволяються. Тривалість блокування визначається під час створення запису [1].

6. **Перевірка з'єднань.** Правила доступу порівнюють вхідні з'єднання з чорним списком. Якщо IP-адреси та порти в одному з записів чорного списку збігаються, з'єднання скасовується. Якщо з'єднання не відповідає жодному з правил доступу або пов'язаним записам чорного списку, перевіряється наступне правило доступу в політиці [1].

Головні функції методу чорних списків

- **Блокування шкідливих адрес:** Основна функція чорних списків полягає в блокуванні відомих шкідливих IP-адрес, що допомагає зменшити загрозу з боку DDoS-атак.
- **Моніторинг трафіку:** Системи, які використовують чорні списки, зазвичай мають механізми для моніторингу та аналізу вхідного трафіку, щоб виявляти нові загрози.
- **Аналіз загроз:** Деякі системи на основі чорних списків можуть також здійснювати глибший аналіз поведінки трафіку, щоб виявити аномалії і, відповідно, внести нові IP-адреси до чорного списку.

Переваги методу чорних списків

- **Простота впровадження:** Чорні списки легко впроваджуються в існуючу інфраструктуру без значних змін в архітектурі системи безпеки.
- **Швидкість реакції:** Блокування IP-адреси може бути здійснено швидко, що є критично важливим під час DDoS-атак.
- **Зменшення навантаження на ресурси:** Блокуючи шкідливий трафік, чорні списки зменшують навантаження на сервери та мережеві пристрої, що покращує загальну продуктивність системи.

Недоліки методу чорних списків

- **Підміна IP-адрес:** Зловмисники можуть використовувати техніки підміни IP-адрес (IP spoofing), що дозволяє їм обійти чорні списки, надсилаючи трафік з нових адрес.
- **Ботнети:** У разі атак з використанням ботнетів, зловмисники можуть розподіляти трафік по великій кількості IP-адрес, що ускладнює їх виявлення і блокування.
- **Додавання легітимних з’єднань до чорного списку (помилкове спрацьовування):** Існує ймовірність того, що легітимні користувачі можуть бути випадково заблоковані, якщо їх IP-адреса буде внесена до чорного списку через помилку [2].

- **Необхідність регулярного оновлення:** Для підтримки ефективності чорних списків важливо їх регулярне оновлення, що потребує додаткових ресурсів і зусиль.

Таблиця 1

Рівень успіху та зменшення обсягу даних для прогнозованого чорного списку

День	Тривоги	Прогнозовані тривоги	Успішні прогнози	Відсоток успіху	Зменшений об'єм трафіку
2019-03-11	1,708,733	51,239	31,958	62.37%	1.87%
2019-03-12	1,664,723	46,721	30,322	64.90%	2.81%
2019-03-13	1,548,186	53,906	32,899	61.03%	3.48%
2019-03-14	1,607,630	45,637	30,039	65.82%	2.84%
2019-03-15	1,710,095	47,481	31,234	65.78%	2.78%

Продовження таблиці 1

Рівень успіху та зменшення обсягу даних для прогнозованого чорного списку

День	Тривоги	Прогнозовані тривоги	Успішні прогнози	Відсоток успіху	Зменшений об'єм трафіку
2019-03-16	1,776,168	53,656	35,735	66.60%	3.02%
2019-03-17	1,699,081	50,061	33,325	66.57%	2.95%

У таблиці 1 наведено зведення оброблених сповіщень , кількість прогнозів і відсоток успішних прогнозів за день. Кількість прогнозів – це кількість сповіщень, передбачених на основі даних за певний день із застосуванням правил, отриманих у попередні дні. Кількість успішних прогнозів – це кількість прогнозованих сповіщень, для яких ми спостерігали передбачене сповіщення в даних. Коефіцієнт успіху – це відношення успішно передбачених сповіщень до всіх прогнозованих сповіщень. Значення дуже схожі для кожного дня, коливаючись близько 50 000 прогнозів, 32 000 успішних прогнозів і 65 % успіху, за винятком першого дня, який використовувався лише для видобутку, а не для оцінки. Нарешті, останній стовпець показує число прогнозованих сповіщень у відсотках від кількості всіх оброблених сповіщень, які ілюструють зменшення обсягу даних[3].

Метод чорних списків є ефективним інструментом у боротьбі з DDoS-атаками, забезпечуючи швидке виявлення та блокування шкідливих IP-адрес. Завдяки простоті впровадження, чорні списки зменшують навантаження на

мережеві ресурси, проте їхня ефективність обмежена через можливість підміни IP-адрес і атаки з ботнетів.

У майбутньому розвиток чорних списків може включати інтеграцію з технологіями машинного навчання для автоматичного оновлення на основі нових загроз. Комбінування чорних списків з іншими методами захисту, такими як аналіз аномалій і геоблокування, дозволить створити комплексний підхід до захисту від DDoS-атак.

Перелік посилань:

1. Forcepoint : Traffic inspection policies : Blacklisting IP addresses : Blacklisting traffic and how it works : Blacklisting process. [Електронний ресурс]. – Режим доступу: https://help.forcepoint.com/ngfw/en-us/6.10.100/GUID-98D4F598-7158-4820-A3B2-FE998A541E0F.html (дата звернення: 17.10.2024)
2. Forcepoint : Traffic inspection policies : Blacklisting IP addresses : Blacklisting traffic and how it works. [Електронний ресурс]. – Режим доступу: https://help.forcepoint.com/ngfw/en-us/6.10.100/GUID-DBC47C5F-D3E5-451E-AC59-411471342DEB.html (дата звернення: 17.10.2024)
3. ResearchGate : Predictive Cyber Situational Awareness and Personalized Blacklisting: A Sequential Rule Mining Approach. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/340128962_Predictive_Cyber_Situational_Awareness_and_Personalized_Blacklisting_A_Sequential_Rule_Mining_Approach#pff (дата звернення: 17.10.2024)

Лагутін Денис Євгенійович, БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ВХОДУ СПІВРОБІТНИКІВ ДО КОРПОРАТИВНИХ ДОДАТКІВ ЗА СТАНДАРТОМ FIDO2 НА ПРИКЛАДІ AKAMAI MFA

Визначено мету і основні завдання щодо забезпечення безпечного входу співробітників до корпоративних додатків. Розглянуто зміст технології забезпечення безпечного входу співробітників до корпоративних додатків за стандартом FIDO2 на прикладі Akamai MFA.

Verizon [1] зазначає, що компрометація облікових даних користувачів є основним методом отримання первинного доступу зловмисниками. Згідно з [1], компрометація облікових даних є особливо ефективною тактикою для ініціювання витоку даних, однієї з категорій інцидентів кібербезпеки. У разі порушення даних заходи безпеки, які захищають дані, обходяться або стають скомпрометованими, що призводить до несанкціонованого доступу. Порушення даних може стосуватися інформації, що дозволяє ідентифікувати особу (PII), фінансових записів, інтелектуальної власності або комерційної таємниці.

Verizon [1] виявив, що скомпрометовані облікові дані є більш поширеною

стратегією витоку даних, ніж фішинг або використання вразливостей. За даними Verizon [1], 31% зломів за останні 10 років стосувалися викрадених облікових даних. У [1] також зазначається, що різні галузі стикаються з різними рівнями компрометації облікових даних, причому такі сектори, як охорона здоров'я та фінанси, є цілями для зловмисників через конфіденційний характер їхніх даних.

Додавання багатофакторної автентифікації (Multi-Factor Authentication, MFA) як додаткового рівня безпеки входу значно знижує ризик, але багато сучасних рішень MFA мають значні недоліки безпеки. Зловмисники можуть легко маніпулювати поточними методами вторинної автентифікації та обійти їх за допомогою простих методів фішингу або соціальної інженерії.

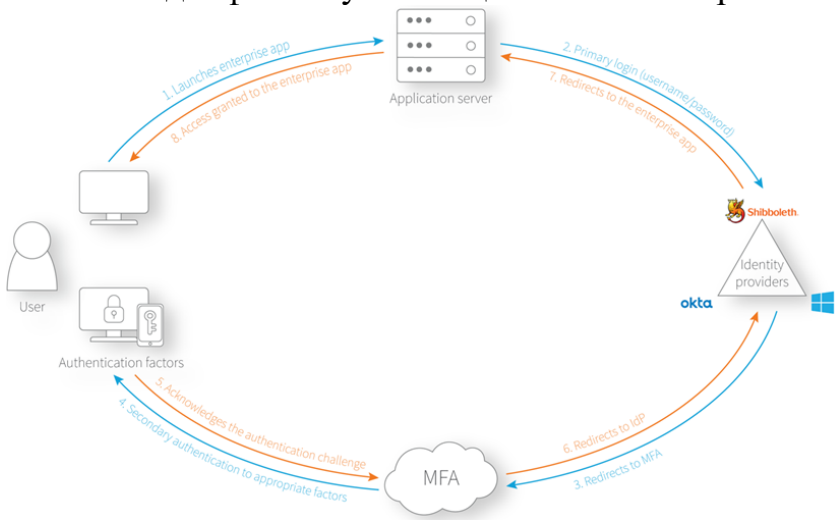


Рис. 1. Схема процесу автентифікації в Akamai MFA [2]

Akamai MFA – це служба багатофакторної автентифікації, яка допомагає організаціям встановити довіру до користувача, перш ніж дозволити доступ до захищених програм і ресурсів. Він забезпечує віддалений доступ для робочої сили та захищає облікові записи працівників. Akamai MFA можна інтегрувати з наявним постачальником ідентифікаційної інформації (IdP) і додати додатковий рівень безпеки до внутрішніх ресурсів організації. Це вимагатиме від користувачів підтверджувати свою особу за допомогою незалежних методів автентифікації [4].

На рисунку 1 представлено концептуальну модель процесу автентифікації, яка реалізована в рішенні Akamai MFA.

Akamai MFA – це комплексне рішення для багатофакторної автентифікації, побудоване на основі стандарту FIDO2. Для еквівалентного рівня керування доступом організації потрібно спочатку розгорнути рішення багатофакторної автентифікації, а потім купувати, розповсюджувати та керувати апаратними ключами безпеки FIDO2, що значно збільшує витрати та ускладнює роботу. Апаратні ключі безпеки часто призводять до поганої взаємодії з кінцевим користувачем, оскільки люди втрачають або забувають свої ключі, що вимагає додаткових дзвінків у службу підтримки IT і знижує продуктивність користувачів [3].

Стандарт FIDO2 – це метод автентифікації, розроблений FIDO Alliance, що містить два компоненти: WebAuthn (W3C) і CTAP (FIDO Alliance). Основні особливості FIDO2 [4]:

облікові дані автентифікації на основі пар закритих/відкритих ключів;

жодних спільних секретів – приватний ключ генерується автентифікатором FIDO2, зберігається в захищеному апаратному забезпеченні автентифікатора, і його не можна експортувати чи змінювати. Під час реєстрації на сервер (веб-сайт) надсилається лише відкритий ключ;

виклики автентифікації доставляються агенту користувача (браузеру), який додає контекст про виклик, а потім доставляє його до підключеного автентифікатора FIDO2, який дозволяє виявити машину посередині;

автентифікатори платформи (прив'язані до платформи та доступні лише на цьому пристрої) та роумінгові автентифікатори (які можна використовувати на будь-якому пристрої).

Рішення безпеки для вдосконалення MFA, яке гарантує, що його неможливо обійти, будується на основі застосування протоколу FIDO2. Це рішення працює, створюючи криптографічний зв'язок між спробою автентифікації та викликом MFA. Це означає, що зловмисники не можуть використовувати вкрадені або скомпрометовані облікові дані або змусити користувачів вводити свої облікові дані на підробленій сторінці входу. Цей метод робить практично неможливим скомпрометувати MFA (рисунок 2) [4].

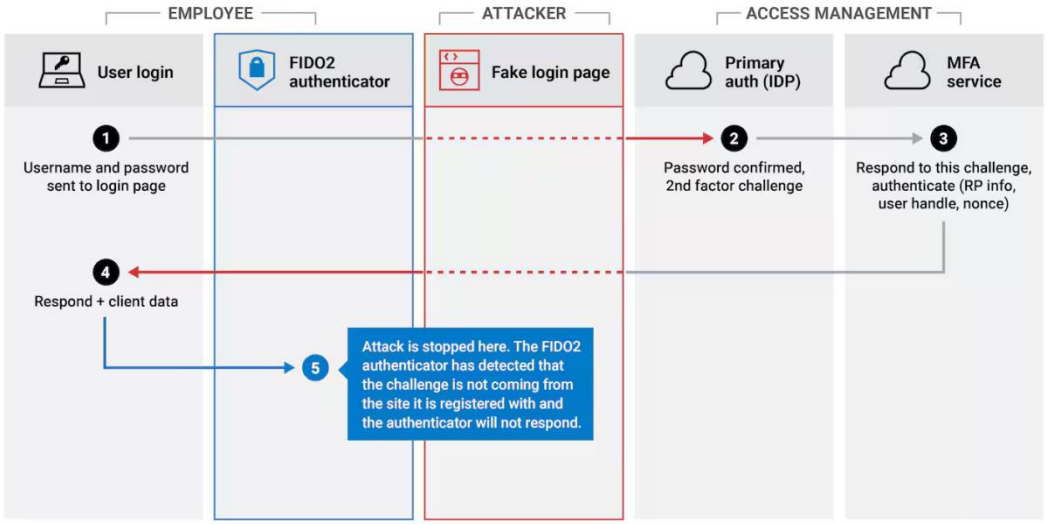


Рис. 2. Схема блокування підробленої сторінки входу за допомогою FIDO2 [4]

Отже, зловмисники часто використовують скомпрометовані або викрадені ідентифікаційні дані користувачів, щоб отримати доступ до облікових записів співробітників або систем організацій. Додавання багатофакторної автентифікації до системи ідентифікації та керування доступом додає додаткові рівні безпеки, які посилюють автентифікацію користувачів, що зменшує ризик захоплення

облікового запису, що часто може призвести до витоку даних або атак програм-вимагачів. Надійна автентифікація є важливим компонентом систем безпеки організацій, таких як Zero Trust і SASE, і вона відіграє важливу роль у безпеці віддаленої роботи співробітників.

Перелік посилань:

1. 2024 Data Breach Investigations Report. Verizon. URL: https://www.verizon.com/business/resources/reports/dbir/#takeaways (дата звернення: 30.09.2024).
2. Manage Akamai MFA. Akamai techdocs.. URL: https://techdocs.akamai.com/mfa/docs/manage-mfa (дата звернення: 30.09.2024).
3. Akamai MFA: Product Brief. Akamai. URL: https://www.akamai.com/resources/product-brief/akamai-mfa (дата звернення: 30.09.2024).
4. Akamai MFA. Akamai. URL: https://www.akamai.com/products/akamai-mfa#accordion-747ed8e568-item-8cb800dfdf (дата звернення: 30.09.2024).

Лазарєв Єгор Геннадійович
студент групи БСД-31, ННІЗІ ДУІКТ, Київ, Україна

Подолання Проблеми Зниження Ефективності Традиційних Спам-Фільтрів проти Новітніх Фішингових Атак

Традиційні спам-фільтри, які раніше ефективно захищали від небажаних електронних листів, стикаються з новими викликами в умовах зростаючої складності фішингових атак. Сучасні фішингові атаки стають дедалі витонченішими, що дозволяє їм обходити стандартні засоби захисту і завдавати значної шкоди як користувачам, так і організаціям.

Проблема зниження ефективності спам-фільтрів

1. **Адаптивність фішингових атак**: Хакери постійно вдосконалюють свої методи, використовуючи реалістичні повідомлення, які імітують легітимні листи від банків, компаній або державних установ.
2. **Обхід простих правил**: Більшість традиційних спам-фільтрів покладаються на сигнатури, чорні списки та ключові слова. Новітні фішингові атаки використовують спеціально підготовлені тексти або зображення, які можуть легко обходити ці перевірки.
3. **Соціальна інженерія**: Сучасні фішинг-атаки використовують персоналізовані повідомлення, зловживаючи психологічними методами, щоб змусити користувачів розкрити конфіденційну інформацію або виконати шкідливі дії.

Новітні фішингові техніки

1. **Spear phishing**: Атаки на конкретних осіб або організації, що базуються на ретельно зібраній інформації про ціль.
2. **Whaling**: Цілеспрямовані атаки на високопосадовців або ключових співробітників з метою отримання доступу до критичної інформації.

3. **Фішинг через соціальні мережі**: Використання повідомлень у соціальних мережах для обману користувачів і отримання доступу до їх акаунтів.
4. **Обфускація URL**: Зловмисники використовують техніки маскування URL, де легітимний вигляд посилання приховує фішингову адресу.

Методи подолання проблеми

1. **Використання штучного інтелекту (AI) і машинного навчання (ML)**:
   - Сучасні системи безпеки на основі AI аналізують поведінкові патерни електронних листів, що допомагає виявляти новітні фішингові атаки навіть без використання сигнатур.
   - AI-алгоритми можуть швидко навчатися новим загрозам і автоматично адаптувати фільтри для блокування нових типів фішингових атак.
2. **Аналіз на основі контексту**:
   - Спам-фільтри можуть використовувати аналіз контенту та контексту електронних листів для розпізнавання підозрілих елементів, як-от підроблені URL, невідповідні заголовки або неприродні шаблони спілкування.
   - Контекстуальний аналіз дозволяє виявляти атаки, які проходять повз традиційні системи на основі сигнатур.
3. **Багатофакторна автентифікація (MFA)**:
   - Використання багатофакторної автентифікації може значно знизити ефективність фішингових атак, оскільки навіть при отриманні логіна і пароля зловмисник не зможе увійти без додаткового підтвердження особистості.
4. **DMARC, SPF, DKIM**:
   - Впровадження цих протоколів для перевірки справжності відправника електронних листів допомагає знизити ймовірність фішингових атак, які використовують підроблені адреси.
5. **Підвищення обізнаності користувачів**:
   - Навчання користувачів виявляти ознаки фішингу, такі як підозрілі посилання, невідповідні запити на конфіденційну інформацію та зміни у спілкуванні.
   - Регулярні тренінги та симуляції фішингових атак можуть значно підвищити пильність користувачів.

Висновок

Для подолання проблеми зниження ефективності традиційних спам-фільтрів у боротьбі з новітніми фішинговими атаками необхідний комплексний підхід. Використання сучасних технологій, таких як AI та ML, впровадження

багатофакторної автентифікації та підвищення обізнаності користувачів є ключовими кроками до забезпечення надійного захисту від фішингових атак.

Перелік посилань:

1. **Role of DMARC, SPF, DKIM in Email Authentication and Phishing Prevention**. Available at: https://dmarc.org/overview/

Лисаченко Аліна Вячеславівна, БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФРАСТРУКТУРИ DNS НА БАЗІ AKAMAI EDGE DNS

Визначено мету і основні завдання щодо захисту корпоративної інфраструктури DNS. Розглянуто зміст технології захисту корпоративної інфраструктури DNS на базі Akamai Edge DNS.

Сервери системи доменних імен (Domain Name System, DNS) перетворюють доступні для читання імена хостів доменів, як-от *www.companywebsite.com*, на IP-адреси, які можуть читати машини. DNS-сервери мають важливе значення для забезпечення позитивного досвіду перегляду, а також для швидкого й надійного інтернет-з'єднання з веб-сайтами, API та програмним забезпеченням корпоративних додатків, розміщених у хмарі [1].

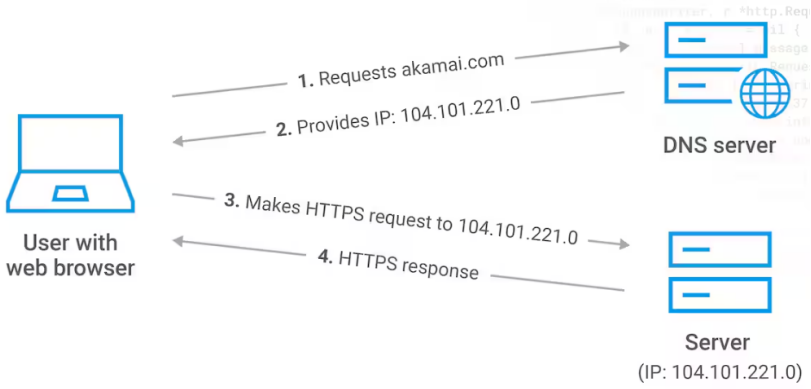


Рис. 1. Принцип роботи DNS-сервера [1]

Існують чисельні загрози для DNS-серверів у вигляді будь-яких типів атак, які ставлять під загрозу доступність, швидкість і продуктивність служб DNS. До них належать DNS-флуд, які переповнюють DNS-сервери запитами на ресурси, що робить сервери недоступними для законних запитів. Підробка DNS або отруєння кешу – це тип кібератаки, яка перенаправляє трафік на шахрайський веб-сайт. DNS-

тунелювання використовує дані, закодовані в DNS-запитах і відповідях, щоб захопити DNS-сервер і дозволити зловмисникам керувати ним віддалено.

Тому, захист DNS-серверів є критично важливим бізнес-пріоритетом для команд безпеки організацій. Оскільки DNS дозволяє корпоративним користувачам отримувати доступ до веб-додатків і API організації, будь-яка загроза корпоративним DNS-серверам також є загрозою бізнес-операціям, прибутковості та довірі клієнтів і партнерів [1].

Продукт Akamai Edge DNS – це хмарне рішення, яке забезпечує доступність 24/7, покращує швидкість реагування та покращує стійкість DNS-серверів, оскільки вони захищаються від найбільших DDoS-атак.

Akamai Edge DNS – це авторитетна служба DNS. Це рішення забезпечує безпечну, високопродуктивну, масштабовану та високодоступну крайову службу для авторитетного DNS. Akamai Edge DNS використовує глобальне розгортання Akamai тисяч серверів імен у кількох мережах, використовує IP Anycast і покладається на власну реалізацію протоколу DNS як загального компонента Akamai Intelligent Platform.

Рішення Akamai Edge DNS доповнює існуючі веб-інфраструктури, незалежно від того, розгортаються вони в приватному центрі обробки даних чи публічній хмарі, з’єднуючи користувачів із бажаним пунктом призначення.

Akamai Edge DNS використовує модель IP anycast для відповіді на запити DNS. Це означає, що замість того, щоб покладатися на два чи три DNS-сервери, клієнти Akamai можуть отримати доступ до тисяч серверів імен, розгорнутих у більш ніж 4100 точках присутності по всьому світу. IP anycast спрямовує запити від кінцевих користувачів до найближчої точки присутності для вирішення, забезпечуючи швидшу продуктивність, більший масштаб і більш різноманітний розподіл. Хоча використання IP anycast не є унікальним для Akamai, ми також сегментуємо сервери імен і точки присутності в кілька хмар IP anycast, роблячи Edge DNS еквівалентним кільком автономним постачальникам DNS з точки зору доступності, масштабу та розподілу. На рисунку 2 показано схему реалізації технології Akamai Edge DNS [2].

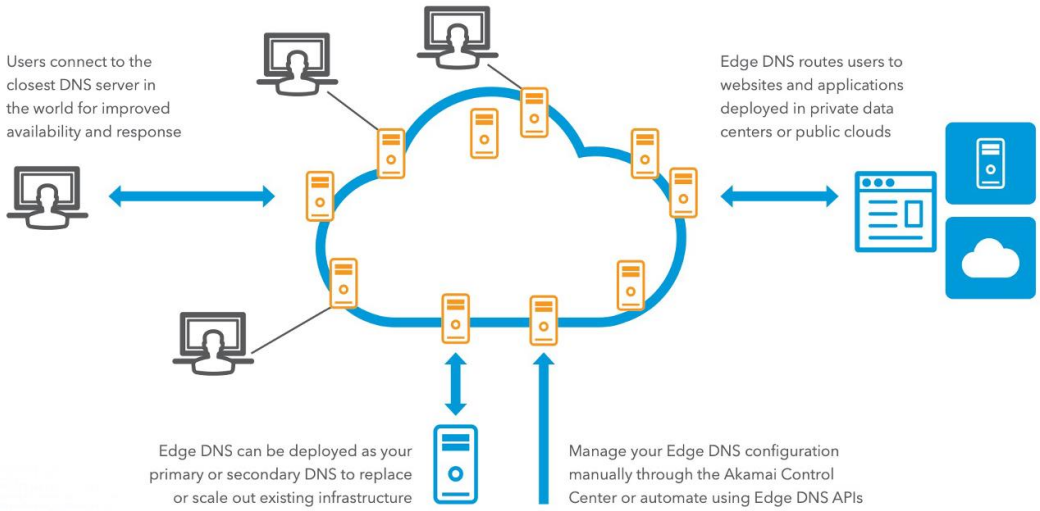


Рис. 2. Схема реалізації технології Akamai Edge DNS [3]

Функції рішення Akamai Edge DNS включають наступне [2]:

запатентована реалізація протоколу DNS, яка використовує всесвітню інфраструктуру DNS Akamai;

підтримка первинної та вторинної зон;

DNSSEC, якщо Akamai Edge DNS придбано з опцією безпеки;

Zone apex mapping, що скорочує час пошуку DNS для веб-сайтів на інтелектуальній платформі;

псевдоніми зон, які базуються на ресурсних записах іншої зони Akamai Edge DNS;

підтримка серверів персональних імен, які можуть вказувати на IP-адреси Akamai Edge DNS Anycast. IP Anycast надає кінцевим користувачам децентралізовану службу DNS. За допомогою IP Anycast можна створити логічний сервер імен, який складається з кількох фізичних серверів імен, розгорнутих у кількох мережах і на різних континентах;

API для програмного доступу до звітних даних і керування зонами;

служби доставки журналів для доступу до журналів транзакцій;

забезпечення вимог відповідно RFC 1034 і 1035.

Необхідно відмітити, що IP anycast – це техніка мережевої маршрутизації, при якій кілька ідентичних мережевих вузлів розгортаються в розподіленій мережі для надання єдиної спільної IP-адреси. Усі вузли відповідають на ту саму IP-адресу, а трафік направляється до найближчого вузла на основі протоколів маршрутизації, що забезпечує користувачам найнижчу затримку та найвищу доступність.

Ролі, які найчастіше відповідають за керування Akamai Edge DNS, це адміністратори сайту, менеджери проектів і постачальники технічної підтримки.

Отже, Akamai Edge DNS надає хмарне DNS-рішення, яке допомагає

організаціям підвищити доступність, продуктивність і відмовостійкість розв'язання DNS і покращити взаємодію з користувачами для своїх веб-сайтів і додатків. Рішення Akamai Edge DNS доповнює існуючі веб-інфраструктури, незалежно від того, розгортаються вони в приватному центрі обробки даних чи публічній хмарі, швидко й ефективно з'єднуючи користувачів із бажаним пунктом призначення.

Рішення Akamai Edge DNS використовує глобальну мережу DNS Akamai, яка включає тисячі серверів імен, розгорнутих у сотнях точок присутності (PoP) у понад 40 країнах. У будь-якому регіоні точки присутності Akamai розподіляються між кількома мережами для резервування та охоплення як на географічному, так і на мережевому рівнях.

Перелік посилань:

1. What Are DNS Servers? Akamai. URL: https://www.akamai.com/glossary/what-are-dns-servers (дата звернення: 01.10.2024).
2. Welcome to Edge DNS. Akamai. URL: https://techdocs.akamai.com/edge-dns/docs/welcome-edge-dns (дата звернення: 01.10.2024).
3. AKAMAI Product Brief. Edge DNS – Comprehensive DNS Security Akamai. URL: https://www.akamai.com/resources/product-brief/edge-dns (дата звернення: 01.10.2024).

Магомедалі Джавідан Бояддін огли
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна
Шандровський Ярослав Ігорович
Студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ З ВИКОРИСТАННЯМ ДВОХФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

У сучасному світі кібербезпеки захист інформаційних ресурсів організацій є критично важливим завданням. Одним із найефективніших методів підвищення безпеки доступу до корпоративних даних є застосування додактових методів автентифікація. Цей підхід ґрунтується на поєднанні двох різних факторів автентифікації для підтвердження особи користувача, що суттєво знижує ризики несанкціонованого доступу.

Захист інформаційних ресурсів організації є одним з головних пріоритетів у сучасному кіберсвіті. Використання паролів для автентифікації користувачів, хоча і є традиційним підходом, часто недостатньо забезпечує безпеку, оскільки паролі можуть бути викрадені або перехоплені. Для підвищення рівня безпеки широко застосовується двофакторна автентифікація (2FA), яка базується на поєднанні двох різних факторів для підтвердження особи.

Загалом, автентифікація ґрунтується на трьох ключових факторах (Рис. 1):

- Те, що користувач знає: Наприклад, пароль або PIN-код;

- Те, чим користувач є: Біометричні дані, такі як відбиток пальця або розпізнавання обличчя;
- Те, що користувач має: Фізичний об'єкт, наприклад, мобільний телефон або USB-ключ.

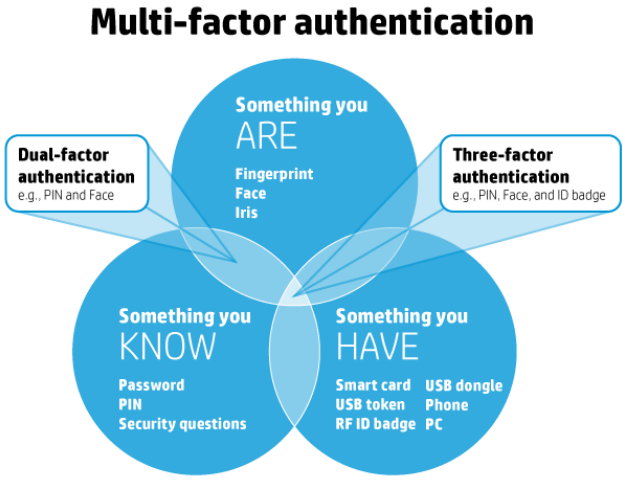


Рис.1. Основні фактори автентифікації

Двофакторна автентифікація полягає у використанні двох з цих трьох факторів, що значно підвищує безпеку доступу до інформаційних ресурсів. Наприклад, при знятті грошей в банкоматі, користувач використовує банківську картку (фактор «те, що ви маєте») та PIN-код (фактор «те, що ви знаєте»).

Одним з найпоширеніших методів реалізації 2FA є використання одноразових кодів (OTP), які генеруються мобільними додатками, такими як Google Authenticator. Ці коди генеруються на основі секретного ключа, що передається сервером під час налаштування 2FA, та часу або лічильника. OTP є одноразовим і діє протягом обмеженого часу, зазвичай 30 секунд, що ускладнює його перехоплення або підробку.

Окрім OTP, дедалі більше організацій використовують фізичні токени, такі як апаратні ключі безпеки (наприклад, YubiKey), які забезпечують додатковий рівень захисту, особливо проти фішинг-атак. При використанні апаратного токена для автентифікації зловмисник не може отримати доступ до системи навіть при наявності пароля, оскільки йому потрібен сам фізичний пристрій.

Головною перевагою 2FA є значне підвищення рівня захисту облікових записів користувачів. Навіть якщо пароль буде викрадено або зламано, для доступу до системи необхідно мати другий фактор, наприклад, мобільний телефон або токен. Це ускладнює проведення атак, спрямованих на крадіжку паролів, таких як атаки з перехопленням даних (Man-in-the-Middle), фішинг або атаки з використанням кейлоггерів.

Також, важливо зазначити, що сучасні системи 2FA можуть використовувати додаткові заходи безпеки, такі як аналіз місцезнаходження користувача або

поведінкову біометрію, для виявлення підозрілої активності та запобігання несанкціонованому доступу.

Незважаючи на свої переваги, двофакторна автентифікація має певні обмеження. Наприклад, користувачі можуть втратити доступ до другого фактора, такого як телефон або токен, що призведе до блокування доступу до їх облікових записів. Крім того, використання SMS як другого фактора не є повністю безпечним через можливі атаки на операторів мобільного зв'язку.

Окремо варто зазначити проблеми зручності: багатьом користувачам 2FA здається занадто складною або обтяжливою у використанні, що може призводити до відмови від активації цього методу захисту.

Загалом, двофакторна автентифікація є ефективним інструментом для захисту інформаційних ресурсів організацій від кібератак. Використання двох різних факторів для підтвердження особи значно ускладнює доступ для зловмисників, навіть якщо пароль було викрадено. Однак, для забезпечення максимального рівня безпеки, важливо правильно обирати методи 2FA та враховувати можливі ризики, пов'язані з втратою доступу до другого фактора.

Перелік посилань:

1. What is Multi-Factor Authentication (MFA)? URL: https://aws.amazon.com/what-is/mfa/ (дата звернення: 23.10.2024).

2.Multifactor Authentication URL: https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661 (дата звернення: 23.10.2024).

Максутов Марсель Олександрович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

ЗАГРОЗИ КРИПТОВАЛЮТАМ: НОВИЙ ВИД ШАХРАЙСТВА

Криптовалюти, такі як Bitcoin, Ethereum та інші, стрімко набирають популярність як засоби інвестицій та електронних платежів. Проте разом із зростанням інтересу до криптовалют збільшується і кількість загроз, які пов’язані з цими цифровими активами. Відсутність централізованого регулювання, анонімність і незворотність транзакцій створюють сприятливий ґрунт для нових видів шахрайства та кібератак, які націлені на власників криптовалют та біржі, що їх обслуговують.

Однією з найпоширеніших загроз є фішинг та соціальна інженерія, спрямовані на крадіжку криптовалютних ключів або доступу до гаманців. Зловмисники створюють підроблені платформи або надсилають шахрайські листи, прикидаючись легітимними криптобіржами або сервісами. Метою таких атак є обманом змусити користувачів ввести свої приватні ключі або логіни, що надає зловмисникам можливість отримати доступ до їх криптовалютних активів. Особливо небезпечними є фішингові атаки на мобільні додатки, де користувачі можуть менше звертати увагу на деталі безпеки.

Ще однією поширеною загрозою є шкідливі програми, що спеціалізуються на крадіжці криптовалют. Такі програми, як правило, проникають у системи через заражені файли або сайти і можуть непомітно викрадати ключі доступу до криптовалютних гаманців. Деякі з них навіть здатні змінювати адреси отримувачів транзакцій у гаманцях користувачів, перенаправляючи кошти на рахунки зловмисників. Наприклад, шкідливі програми, відомі як "криптоджекери", використовують ресурси зараженого комп'ютера або смартфона для видобутку криптовалют без відома власника, що знижує продуктивність пристрою та завдає фінансових збитків.

Небезпеку також становлять атаки на криптовалютні біржі та платформи обміну. Ці майданчики часто є мішенню для масштабних зламів, що можуть призвести до втрати мільйонів доларів у криптовалюті. Напади на біржі включають крадіжку активів через вразливості в системі безпеки або інсайдерські зловживання. Нерідко після таких атак біржі не в змозі компенсувати збитки своїм клієнтам, що призводить до великих фінансових втрат. Відомі інциденти зламу Mt. Gox та інших платформ доводять, що безпека криптовалютних бірж залишається серйозною проблемою.

Також слід зазначити появу нових видів шахрайства, пов'язаних із початковими пропозиціями монет (ICO). Шахраї створюють фіктивні проекти, залучаючи інвесторів через підроблені обіцянки про величезні прибутки. Коли сума коштів накопичується, шахраї зникають, залишаючи інвесторів без вкладених коштів. Цей тип шахрайства нагадує класичні фінансові піраміди, проте в середовищі криптовалют такі схеми набувають нових форм через складність відстеження транзакцій і відсутність регулювання.

Захист від загроз криптовалютам вимагає підвищеної обережності та впровадження належних заходів безпеки. Зокрема, користувачам варто використовувати апаратні гаманці, які зберігають ключі в автономному режимі, що унеможливлює доступ до них через інтернет. Крім того, важливо бути уважним до деталей, уникати фішингових листів і сайтів, а також використовувати багатофакторну автентифікацію для входу на біржі. Кріптобіржам та платформам обміну, у свою чергу, слід інвестувати в надійні системи безпеки, регулярно проводити аудити і забезпечувати прозорість операцій для клієнтів.

Таким чином, криптовалюти стають привабливою ціллю для зловмисників через специфічні особливості їх функціонування. Проте належний захист, обізнаність користувачів та дотримання базових принципів безпеки можуть значно знизити ризики, пов'язані з використанням криптовалют.

Перелік посилань:

1. Ризик є: 9 чинників для блокування криптовалют. URL: https://mind.ua/openmind/20256085-rizik-e-9-chinnikiv-dlya-blokuvannya-kriptovalyut (date of access: 07.10.2024).
2. Анонімні криптовалюти й криптоміксери: етика та законність. URL: https://www.h-x.technology/ua/blog-ua/anonymous-cryptocurrencies-crypto-mixers-ethics-legislation-ua (date of access: 05.10.2024).
3. Правовий захист операцій із криптовалютами: примарний чи реальний?. URL: https://unba.org.ua/publications/6558-pravovij-zahist-operacij-iz-kriptovalyutami-primarnij-chi-real-nij.html (date of access: 04.10.2024).

Матвєєв Олександр Андрійович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ ВІДДАЛЕНИХ КОРИСТУВАЧІВ

З кожним роком все більше організацій переходять на віддалений режим роботи, що вимагає впровадження нових технологій для забезпечення безпеки інформаційних систем. Віддалений доступ до корпоративних ресурсів створює додаткові ризики для конфіденційних даних через можливість використання незахищених мереж. Основні загрози включають перехоплення трафіку, компрометацію облікових записів, зараження шкідливим програмним забезпеченням та порушення нормативних вимог. Окрім зовнішніх кіберзагроз, значну небезпеку становлять внутрішні загрози, що виникають через недбалість або некомпетентність самих користувачів. Віддалені працівники часто використовують власні пристрої для доступу до корпоративних ресурсів, що підвищує ризик компрометації даних через невідповідність цих пристроїв стандартам безпеки. Наприклад, відсутність актуального антивірусного програмного забезпечення, використання слабких паролів або незашифрованих каналів зв'язку може стати ключовою вразливістю. Тому важливо впроваджувати політику **BYOD (Bring Your Own Device)**, яка визначатиме правила використання особистих пристроїв для роботи та вимоги до їхнього захисту.

Одним із найважливіших аспектів захисту інформаційних систем для віддалених користувачів є використання **багатофакторної автентифікації (MFA)**. MFA забезпечує високий рівень безпеки шляхом використання декількох факторів перевірки: пароля, біометричних даних та одноразових кодів. Це значно знижує ймовірність несанкціонованого доступу до системи навіть у випадку компрометації одного з факторів. Наприклад, багато сучасних хмарних платформ, таких як **AWS** або **Microsoft Azure**, підтримують вбудовані інструменти для реалізації багатофакторної автентифікації, що робить цей процес простішим для інтеграції. Іншим важливим елементом захисту є **використання VPN (Virtual Private Network)**. VPN створює захищений тунель між віддаленим користувачем і

корпоративною мережею, що дозволяє шифрувати всі передані дані. Це забезпечує захист від перехоплення трафіку навіть у випадку використання публічних мереж. VPN також допомагає приховати реальне місцезнаходження користувача, що може бути корисним для запобігання атак з використанням географічної ідентифікації.

Не менш важливим аспектом є **шифрування даних**. Шифрування на рівні файлів та дисків дозволяє захистити інформацію як під час її передачі, так і в стані спокою. Це особливо актуально для віддалених користувачів, які можуть зберігати частину даних на власних пристроях або передавати інформацію через незахищені мережі. Надійне шифрування гарантує, що навіть у випадку перехоплення даних вони будуть недоступними без ключа для розшифрування. **Моніторинг та реагування на кіберінциденти** є важливим елементом стратегії захисту віддалених користувачів. Системи моніторингу безпеки, такі як **SIEM (Security Information and Event Management)**, дозволяють аналізувати події в реальному часі та виявляти підозрілу активність. Це дозволяє організаціям своєчасно реагувати на інциденти, мінімізуючи можливі збитки. Розробка чітких процедур реагування на інциденти є важливою частиною загальної стратегії кібербезпеки, оскільки навіть найкращі системи захисту не можуть гарантувати повну безпеку. Окрім технічних засобів захисту, організаціям слід звертати увагу на **освітню роботу серед працівників**. Багато кібератак спрямовані на соціальну інженерію, тому навчання працівників розпізнаванню фішингових повідомлень та інших загроз є необхідною частиною стратегії безпеки.

Впровадження таких рішень дозволяє значно підвищити рівень захисту інформаційних систем організації та забезпечити безпечний доступ віддалених користувачів до корпоративних ресурсів. Хоча технології кіберзахисту постійно розвиваються, ключем до успіху залишається комплексний підхід, що включає технічні, організаційні та освітні заходи.

Перелік посилань:
1. Організація безпечної роботи співробітників з дому. URL: https://www.eset.com/ua/about/newsroom/press-releases/security-tips/organizatsiya-bezopasnoy-raboty-sotrudnikov-iz-doma-osnovnyye-pravila-dlya-zashchity/
2. Технічні заходи в інформаційній безпеці. URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/tehnichni-zahodi-v-informacijnij-bezpeci
3. Інформаційна безпека підприємства та основні засади захисту. URL: https://iitd.com.ua/news/shho-take-informacijna-bezpeka-pidpriiemstva-ta-jaki-osnovni-zasadi-zahistu-danih-isnujut/

Мацкевич Владислав Вікторович
Державний університет інформаційно-

комунікаційних технологій
Україна, Київ

Захист хмарних інформаційно-телекомунікаційних платформ

Хмарні інформаційно-телекомунікаційні платформи — це комплекс технологій і сервісів, що забезпечують передачу, обробку, зберігання та управління даними через інтернет за допомогою хмарних рішень. Вони об'єднують інфраструктуру, програмне забезпечення і комунікаційні ресурси, надаючи можливість користувачам і організаціям отримувати доступ до ресурсів за запитом без необхідності інвестувати у фізичне обладнання.

Основні компоненти таких платформ включають:

Інфраструктура як сервіс (IaaS) — оренда обчислювальних ресурсів (сервери, сховища, мережеві компоненти) через хмару.
Платформа як сервіс (PaaS) — надання середовища для розробки, тестування та розгортання додатків без управління фізичною інфраструктурою.
Програмне забезпечення як сервіс (SaaS) — доступ до готових програм через інтернет, таких як системи електронної пошти, CRM тощо.

Хмарні інформаційно-телекомунікаційні платформи є невід'ємною частиною сучасної цифрової інфраструктури. Проте, вони залишаються вразливими до низки кіберзагроз, таких як несанкціонований доступ, витоки даних, атаки на інфраструктуру та вразливості віртуалізації

Сучасні підходи захисту інформаційно-телекомунікаційних платформ.

1. **Багаторівневе шифрування даних**: Це підхід до шифрування, який використовує кілька рівнів захисту для підвищення безпеки даних. Він забезпечує шифрування даних на різних етапах:

- **У стані спокою** (на фізичних носіях або в базах даних),
- **Під час передачі** (між користувачем і хмарою або між різними компонентами системи),
- **На рівні окремих додатків або файлів**. Такий підхід дозволяє мінімізувати ризики несанкціонованого доступу або перехоплення даних на будь-якому етапі їх обробки.

2. **Контроль доступу на основі ролей (RBAC)**: RBAC (Role-Based Access Control) — це модель управління доступом, де права і привілеї користувачів визначаються їх ролями в системі. Замість надання індивідуальних прав кожному користувачу, їм призначаються ролі, кожна з яких має певний набір дозволів. Це спрощує управління доступом у великих організаціях і знижує ризик помилок. Наприклад, у хмарній платформі адміністраторам можуть

бути надані всі права, а звичайним користувачам — обмежений доступ до певних даних або функцій.

3. **Моніторинг аномальної активності**: Це процес постійного спостереження за системами для виявлення незвичайної або підозрілої поведінки, яка може свідчити про кіберзагрозу. Для цього використовуються спеціальні алгоритми та системи, які аналізують мережевий трафік, поведінку користувачів і активність програмного забезпечення.
4. **Використання технологій блокчейн для забезпечення прозорості операцій**: Блокчейн — це децентралізована і незмінна технологія зберігання даних, де кожна операція записується в ланцюжок блоків і підтверджується учасниками мережі. Для забезпечення безпеки та прозорості в хмарних системах, блокчейн може використовуватись для:

- **Реєстрації всіх операцій із даними**: будь-яка зміна даних або транзакція записується в блокчейн, що забезпечує її відстежуваність і незмінність.
- **Запобігання шахрайству**: оскільки всі операції прозорі і доступні для перевірки, можна легко виявити спроби фальсифікації або зловживань. Це робить систему більш надійною і забезпечує довіру між учасниками без потреби в посередниках.

Висновок:

Хмарні інформаційно-телекомунікаційні платформи є критично важливими для сучасних організацій, оскільки вони забезпечують гнучкість, масштабованість та економічну ефективність для обробки і передачі даних. Їхнє широке застосування в різних галузях, від бізнесу до критичної інфраструктури, робить питання їхнього захисту пріоритетним для забезпечення безперебійної роботи та запобігання кіберзагрозам.

Їх захист вимагає комплексного підходу, який включає багаторівневе шифрування для захисту даних на всіх етапах, контроль доступу на основі ролей (RBAC) для ефективного управління правами користувачів, моніторинг аномальної активності для вчасного виявлення загроз, а також використання технологій блокчейн для забезпечення прозорості та надійності операцій. Такий підхід дозволяє мінімізувати ризики кіберзагроз і забезпечити високий рівень безпеки в хмарних середовищах.

Перелік посилань:

1. Бідюк, П. І., Кузьменко, О. В. (2017). **Інформаційна безпека в хмарних обчислювальних системах**. *Наукові праці Національного авіаційного університету. Серія: Інформатика, кібернетика та обчислювальна техніка*, 3(42), 56-61.
2. Довгань, Л. О., Мірошниченко, С. В. (2019). **Методи захисту інформації в хмарних середовищах**. *Вісник Черкаського державного технологічного університету. Технічні науки*, (3), 45-50.
3. Олійник, А. І. (2020). **Моделі та методи контролю доступу в інформаційно-телекомунікаційних системах**. *Збірник наукових праць Харківського національного університету радіоелектроніки*, 15(2), 32-37.

4. Сидоренко, О. П., Кравець, А. М. (2018). **Безпека хмарних обчислень: проблеми і рішення**. *Інформаційні технології і засоби навчання*, 68(6), 149-161.

Менчинський Богдан Олександрович
Студент групи БСДМ-63 ННІЗІ ДУІКТ, Київ, Україна

ЧОМУ ВАЖЛИВО УПРАВЛЯТИ МОБІЛЬНИМИ КОРИСТУВАЧАМИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Управління мобільнимии користувачами корпоративної інформаційної системи стає все більш складним у зв'язку зі зростаючим числом кінцевих точок та застосовуваних інформаційних технологій. Уніфіковане управління кінцевими точками (Unified Endpoint Management, UEM) є комплексним підходом для управління пристроями кінцевих точок в організації з єдиної консолі. Реалізація технології уніфікованого управління кінцевими точками створює умови забезпечення багатьох сучасних функцій захисту.

Використання мобільних пристроїв для виконання бізнес-задач організацій стало нормою. Все бульше працівників організацій для виконання цих задач використовують свої пристрої, які з огляду на кібербезпеку можуть бути потенційно не надійними, коли мова йде про доступ до інформаційних ресурсів інформаційної системи організації. Тому організаціям важливо впроваджувати в своїх організаціях технології управління мобільними користувачами інформаційної системи.

Використання мобільних простроїв розширює можливості використання концепції BYOD, і організації повинні зрозуміти, що BYOD не можна ігнорувати. BYOD надають організаціям конкурентну перевагу, тому їх слід включити до їхї IT-стратегії, якщо вони хочуть залишатися актуальними в цифрову еру. Розумні пристрої є доступними та дозволяють користувачам працювати практично з будь-якого місця, значно підвищуючи гнучкість до доступу. Співробітники можуть працювати швидше завдяки знайомству зі своїми пристроями, створюючи сплеск продуктивності, що є однією з головних причин впровадження BYOD.

Хоча BYOD надає переваги працівникам і бізнесу, його використання створює численні проблеми для організацій. BYOD підключаються до точок доступу до мережі на робочому місці, що відкриває організації для потенційних атак, які проникають через пристрої. Оскільки пристрої є приватною власністю, IT стикається з проблемою, як захистити свої інформаційні активи та конфіденційні дані від злому, втрати чи неналежного використання.

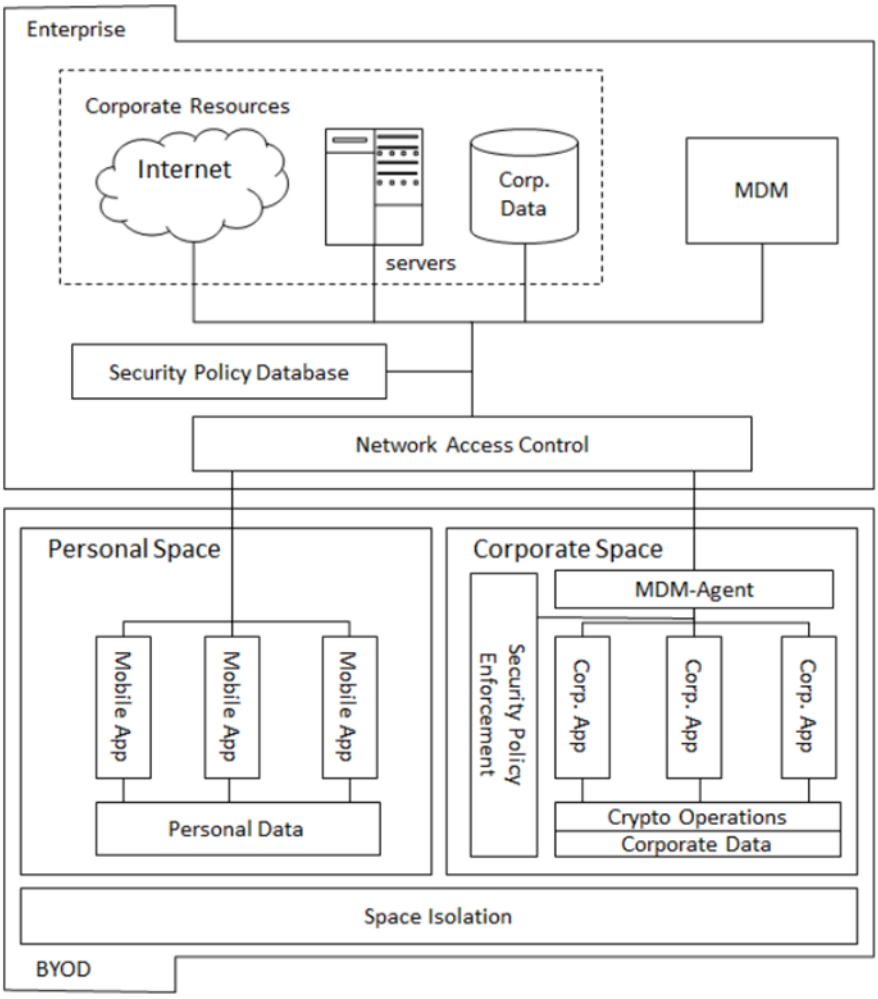
Безпека BYOD має важливе значення для захисту інформаційної системи організації. Захистити BYOD також складно через їх унікальність. Існує кілька рішень, спрямованих на вирішення проблем безпеки BYOD.

Рішення безпеки BYOD має відповідати наведеним нижче вимогам:

- Ізоляція простору;

- Захист корпоративних даних;
- Застосування політики безпеки.

Ці вимоги забезпечують бажаний контроль доступу, конфіденційність і керування політикою безпеки на BYOD. Ідеальне рішення BYOD має відповідати всім цим трьом вимогам безпеки рис.1



Як показано на рис.1., вимоги до безпеки BYOD для доступу до інформаційної системи організації допримуються. Структура включає дві сторони: корпоративну та BYOD [1].

Корпоративна сторона включає різні корпоративні ресурси, такі як Інтернет, сервери та корпоративні дані, і забезпечує контроль доступу для BYOD для доступу до цих ресурсів. Запити на доступ надаються або відхиляються відповідно до політики безпеки підприємства. Підприємство також включає систему керування пристроями, наприклад MDM, для керування BYOD.

Отже для забезпечення безпеки роботи організації важливу роль відіграє концепція використання мобільних пристроїв .

Перелік посилань

1. Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory. [Електронний ресурс] – Режим доступу: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1051&context=jmwais

2. BRING YOUR OWN DEVICE ORGANISATIONAL INFORMATION SECURITY AND PRIVACY. [Електронний ресурс] – Режим доступу: https://researchrepository.murdoch.edu.au/id/eprint/25699/1/bring_your_own_device.pdf
3. Risk Management in the Era of BYOD. [Електронний ресурс] – Режим доступу: https://cups.cs.cmu.edu/soups/2013/risk/Yang-RP-IT-2013.pdf

Мешко Ярослав Юрійович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ВАЖЛИВІСТЬ НАВЧАННЯ ПЕРСОНАЛУ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кібербезпека сучасного бізнес середовища відіграє ключову роль для забезпечення стійкості компаній перед кіберзагрозами. Але навіть найсучасніші технології не можуть гарантувати повного захисту, якщо персонал не обізнаний у даній сфері. Навчання персоналу у сфері інформаційної безпеки є важливим елементом комплексної стратегії захисту даних компанії. Працівники мають бути обізнані щодо поточних загроз, методів реагування на майбутні інциденти, а також практик запобігання кіберзлочинам. Це включає знання про різні види атак, належне управління паролями, шифрування даних і дотримання політик безпеки.

Згідно із дослідженнями у 2023 році 70% помилок спричинені через необізнаність працівників у сфері кібербезпеки. Тому дуже важливо забезпечити регулярне навчання персоналу, щоб підвищити обізнаність про можливі загрози та навчити правильним діям у випадку кібератак.

Важливість навчання полягає в наступних пунктах:

- запобігає витоку даних, так як навчений персонал з меншою ймовірністю допуститься помилок, які можуть призвести до витоку даних. До прикладу працівники можуть розпізнавати заражені посилання, фішингові електронні листи, або підозрілі дії, що свідчать про витік даних. 1 із 3 випадків витоку даних, пов'язані із фішингом;
- покращує довіру клієнтів, оскільки навчені працівники можуть надати кращі послуги клієнтам щодо безпеки даних та заходів компанії щодо захисту інформації;
- покращує дисципліну та дотримання правил, оскільки навчання допомагає працівникам краще розуміти внутрішні політики безпеки та важливість їхнього виконання. Це формує відповідальне ставлення до роботи з інформаційними системами, мінімізуючи ризик порушень;
- підвищує рівень соціальної відповідальності Вашої організації, так як компанія демонструє, що несе відповідальність за Ваші особисті та фінансові дані;
- економія коштів, оскільки запобігання злому через навчання з питань безпеки є набагато ефективнішим з точки зору витрат, ніж фінансові та юридичні витрати, пов’язані з інцидентами [1,2].

Задля того, щоб краще засвоїти навички роботи з кіберінцидентами, можна

застосовувати такі варіанти навчання:

- наочні посібники, які швидко передають складну інформацію, не перевантажуючи людей;
- імітація фішингу, де персонал отримуватиме фіктивні листи, які імітують справжні загрози, щоб навчитись їх розпізнавати та правильно реагувати на них;
- різноманітні тренінги, особливо на теми крадіжка особистих даних, надійні паролі та багатофакторна автентифікація, соціальна інженерія, безпечний перегляд, шкідливе програмне забезпечення, GDPR і конфіденційність даних, тощо;
- комп'ютерне навчання, яке може приймати різні форми, від текстових до аудіо, відео та тестів. Навчання має впливати на довгострокову поведінку безпеки та зменшувати ризик злому [2].

Навчання персоналу має бути безперервним процесом, оскільки загрози змінюються і нові методи атак з'являються щодня. Експерти рекомендують провести початкове навчання, згодом його посилювати. Також рекомендується щокварталу або раз на півроку повторювати навчання, тоді як після великих інцидентів безпеки може знадобитися негайне навчання [3].

Окрім постійного навчання необхідно вводити системи оцінювання знань працівників з питань кібербезпеки. Організації можуть використовувати такі інструменти, SABR (Security Awareness and Behaviour Research) - поінформованість про безпеку та дослідження поведінки. Таке дослідження допомагає оцінити знання працівників, виявити прогалини, які потребують покращення. Постійне оцінювання та коригування є важливими для того, щоб навчання залишалося ефективним [3].

Як висновок можна зазначити, регулярне навчання не лише підвищує рівень обізнаності серед ризиків, але й формує культуру безпеки у компанії, що сприяє проактивному підходу до захисту даних. Інвестиції у навчання персоналу дозволяють виявити недоліки у системах безпеки, зменшувати ймовірність помилок персоналу і швидше реагувати на інциденти. Тому систематичне навчання є необхідною умовою для забезпечення надійного захисту інформації.

Перелік посилань:

1. The Importance of Employee Training in Cybersecurity URL: https://grayscale.my/the-importance-of-employee-training-in-cybersecurity/ (дата звернення: 06.10.2024).
2. Security Awareness: 7 reasons why security awareness training is important in 2023 URL: https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/ (дата звернення: 06.10.2024).
3. Why is it important to support my staff with security awareness training? URL: https://thesecuritycompany.com/the-insider/why-is-it-important-to-support-my-staff-with-security-awareness-training/ (дата звернення: 06.10.2024).

Миронов Вадим Ігорович
студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

ПЕРЕВАГИ ФУНКЦІЙ МАШИННОГО НАВЧАННЯ ТА ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМАХ ЗАХИСТУ КІНЦЕВИХ ТОЧОК

Кожний користувач комп'ютера, ноутбука або смартфона має діло із кінцевою точкою. Через роботу із інтернетом ці пристрої стають потенційними цілями зловмисників. Компрометація пристрою може призвести до крадіжки даних або встановлення віддаленого контролю. Для захисту кінцевих точок використовують EDR-системи. Зі збільшенням кількості пристроїв складніше враховувати всі аспекти безпеки. На допомогу приходять XDR-системи, що об'єднують захист кінцевих точок, мережі та хмарних сервісів, використовуючи штучний інтелект для виявлення складних атак, що можуть пройти непоміченими традиційними засобами захисту.

Штучний інтелект грає велику роль в сучасних системах захисту інформації. Це також стосується систем захисту кінцевих точок. Порівнюючи з традиційними системами, де основою захисту була людина, сучасні рішення дозволяють автоматизувати процеси завдяки використанню машинного навчання. Це забезпечує краще попередження та реагування на складні загрози. Серед основних переваг сучасних систем над традиційними хотілося б наголосити на:

1. Використанні алгоритмів поведінкового аналізу та виявлення аномалій для розпізнавання зловмисних дій, що допоможе відстежити підозрілі дії користувача та заблокувати обліковий запис до його компрометації;
2. Аналізувати та виявляти ризики та вразливості в хмарному середовищі. Особливо актуально в сучасному житті, коли компанії використовують хмарні рішення для покриття своїх потреб(Microsoft 365, Google Workspace, Jira, Confluence тощо);
3. Допомогати командам безпеки краще аналізувати події, які відбуваються на кінцевих точках: визначати пріоритет загроз залежно від рівня потенційної шкоди, автоматично реагувати на інциденти за допомогою правил, допомагати розслідувати інциденти;
4. Захищати, блокувати та сповіщати спеціалістів із інформаційної безпеки про витік чутливих даних за межі компанії;
5. Допомагає покращити ефективність спеціалістів відділу інформаційної безпеки за рахунок виконання рутинної роботи.
6. Виявляти потенційні ризики: невідомі пристрої, застаріле ПО та ОС, незахищені чутливі дані.

Якщо передивитись всі пункти, можна помітити одну важливу властивість, а саме – зменшення обсягу роботи для спеціалістів відділу кібербезпеки, щоб дозволити їм вирішувати важливіші справи, дослідити складніші загрози. Дослідженню складних загроз будуть допомагати оптимізовані звіти. Вони будуть підкреслювати важливі параметри, які допоможуть відредагувати політики безпеки та підвищити ефективність заходів з реагування. Завдяки цьому спеціалісти зможуть оперативно виявляти слабкі місця у захисті та приймати відповідні дії для їх усунення. Це дозволить фахівцям швидко інтерпретувати дані, виявляти ключові тенденції та приймати обґрунтовані рішення для забезпечення безпеки. Завдяки цьому, процес аналізу стане більш ефективним, а реагування на потенційні

загрози—більш своєчасним та точним.

Важливо відмітити зменшення кількості помилкових сповіщеня завдяки алгоритмам машинного навчання, що також дозволяє аналітикам отримувати точну інформацію про актуальні загрози, знижуючи навантаження на спеціалістів, економлячи час на фільтрацію повідомлень. Це особливо важливо при інтеграції систем захисту кінцевих точок з іншими рішеннями, такими як SIEM.

Завершуючи розгляд переваг сучасних систем захисту кінцевих точок, варто окремо виділити роль штучного асистента, який діє подібно до Copilot for Security. Цей асистент на базі штучного інтелекту виконує функції справжнього спеціаліста, допомагаючи командам безпеки ефективніше справлятися зі своїми завданнями. Він фактично стає членом команди, який здатний як реагувати на загрози, так і допомагати аналітикам приймати рішеня. У разі загрози, може порекомендувати власнику дії, які зможуть попередити подальшу атаку, адже він містить в собі знання про найкращі практики у галузі захисту інформації. Його допомога буде дуже актульна як молодшим співробітникам, які тільки поглинають інформацію про сучасні загрози, так і вправним охоронцям кіберпростору. Він може покривати декілька ролей:

1. Комутуючий ланцюг, який завдяки інтеграції з різними системами (наприклад: Microsoft Teams), може працювати як координаційний центр, допомагаючи відділам обмінюватися інформацією, планувати дії та розподіляти завдання.

2. Вчитель, який навчить та підкаже, як краще протидіяти загрозі в різних ситуаціях завдяки великій базі знань, на якій він навчений;
3. Молодший співробітник, який буде виконувати рутинні задачи та створювати звіти по виконаній роботі;

Я впевнений, що це тільки початок, в подальшому системи захисту кінцевих точок будуть мати при собі великий арсенал інструментів, щоб протидіяти загрозам в кіберпросторі. Такі асистенти є важливим кроком у боротьбі з кіберзагрозами, забезпечуючи автоматизацію, підвищення точності та кращу адаптацію до нових загроз у сучасному світі, що стрімко змінюється.

Штучний інтелект у кібербезпеці не тільки сприяє виявленню та запобіганню загрозам, але й трансформує підходи до їх вирішення, роблячи захист активнішим, адаптивнішим та менш залежним від людського фактору. Це дозволяє фахівцям кібербезпеки сфокусуватися на більш складних завданнях, віддаючи рутинну роботу в руки надійного цифрового помічника.

Перелік посилань:

1. Що таке ШІ для кібебезпеки URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-ai-for-cybersecurity (дата звернення: 04.10.2024).
2. Чим EDR відрізняється від XDR URL: https://www.microsoft.com/uk-ua/security/business/security-101/edr-vs-xdr (дата звернення: 04.10.2024).
3. Захисний комплекс Microsoft Copilot URL: https://www.microsoft.com/uk-ua/security/business/ai-machine-learning/microsoft-copilot-security (дата звернення: 04.10.2024).

Нагорний Микита Артемович
студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

ДОСЛІДЖЕННЯ МЕТОДІВ ОЦІНКИ РИЗИКІВ БЕЗПЕКИ В СИСТЕМІ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ. Зі швидким розвитком комп'ютерних технологій загрози інформаційній безпеці стають більш комплексними і різноманітними. Саме тому, все більш нагальними постають питання здійснення гідного рівня безпеки в сучасних системах захисту інформації (СЗІ). Особливо це є актуальним у сучасних умовах повномасштабного вторгнення в Україну, де боротьба відбувається на всіх напрямах, у тому числі й інформаційному. Збої, руйнування чи компрометація інформаційних систем можуть негативно вплинути на будь-які бізнес-процеси, що призводить до матеріальних збитків. Безперервність виконання є ключовою характеристикою життєздатності СЗІ. Оцінка можливих ризиків є одним із ключових пунктів у разі застосування СЗІ. Вона дозволяє визначити загрози й вразливості, що можуть вплинути на інформаційні активи, а також допомагає розробити заходи для їхньої мінімізації, забезпечуючи ефективний захист і безперервність діяльності будь-якої організації.

Мета і методологія досліджень. На основі вивчення наукових літературних джерел, дослідити й оцінити найпоширеніші методики визначення ризиків у безпеці СЗІ.

Результати досліджень. Оцінка ризиків для безпеки СЗІ починається з вибору методики. Найпоширенішими, на сьогодні, є: методології *NIST Risk Management Framework (RMF), Frap (Facilitated Risk Analysis Process), Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation), CRAM (CCTA Risk Analysis and Management Method), FMEA (Failure Modes and Effect Analysis), COBIT (Control Objectives for Information and Related Technologies)*; стандарти *ISO (International Organization for Standardization)* і *AS / NZS ISO* 31000-2009.

У свою чергу методологія *RMF,* яка розроблена Національним інститутом стандартів і технологій США, забезпечує структуру для управління ризиками інформаційних систем протягом усього їхнього життєвого циклу. Вона допомагає організаціям ідентифікувати ризики, впроваджувати контрольні заходи й підтримувати безпеку своїх систем. Безпосередньо пов'язаними з менеджментом ризиків у цій методології є стандарти *NIST SP 800-30 "Guide for Conducting Risk Assessments»; NIST SP 800-39 "Managing Information Security Risk»; NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations»; NIST SP 800-137 "Information Security Continuous Monitoring»*.

Для прикладу розглянемо властивості для стандарту *NIST SP 800-30*. Перевагами цього стандарту, за результатами досліджень вчених Харківського національного університету радіоелектроніки є: простота впровадження, гнучкість до специфічних потреб і до обробки ризиків, докладний опис ризиків, підтримка програмного забезпечення для обробки результатів. Разом з тим, цей стандарт має кілька обмежень щодо тривалості процесу аналізу й оцінки ризиків, а також обмежену шкалу оцінювання (трирівневу).

Організація *ISO (International Organization for Standardization)* розробила одну із найчастіше використовуваних серій стандартів. Із якої, безпосередньо дотичними до менеджменту ризиків є слідуючі: *ISO/IEC 27005: 2018 "Information technology – Security techniques – Information security risk management»*; *ISO/IEC 27102: 2019 "Information security management – Guidelines for cyber-insurance»*; Серія стандартів *ISO / IEC* 31000: 2018, з яких особливо вартий уваги є *ISO/IEC* 31010: 2019 "*Risk management – Risk assessment techniques»*.

Одним із прикладів використання цих стандартів є методологія *CRAMM*. Застосування ця методологія знаходить здебільшого у великих організаціях і державних установах. Вона має: триетапний підхід до управління ризиками; гарно підходить під різні типи організацій; надає можливість візуалізувати ризики; забезпечує докладний аналіз активів, ризиків і заходів контролю; може оцінити вплив ризиків на бізнес-процеси. Варто також зазначити, що вона складна і довга в реалізації, а також потребує досвідченості персоналу.

Наступною, не менш популярною, є методологія *OCTAVE*. Основні її характеристики: найбільш поширена і може бути застосована практично усюди, незалежно від розміру; використовує не тільки стандарти *ISO*, але й *NIST*; не потребує програмного забезпечення; гнучка, із фокусом на основних ризиках. Порівняно із *CRAMM* методологія *OCTAVE* суттєво швидша в реалізації, але все ще вважається досить складною і так само потребує досвідченості персоналу.

Також варта уваги методологія *COBIT*. До її характеристик відносяться: процесний підхід, орієнтований на цілі організації й менеджмент ризиками; має інструмент *COBIT Framework* із готовими шаблонами і рекомендаціями; відповідає бібліотеці практик *ITIL (Information Technology Infrastructure Library)*, використовує модель внутрішнього контролю *COSO (Committee of Sponsoring Organizations of the Treadway Commission)* і стандарти *ISO* 27001; є досить гнучкою, проте, може бути занадто витратною для малих організацій. Для реалізації ця методологія потребує багато часу і навичок.

Висновки. Захист інформаційних даних, є надзвичайно важливим для безпечного функціонування будь-яких державних і бізнес структур. У світі існує багато різних методологій для захисту інформації, застосування кожної з них визначається потребами тієї чи іншої установи. Кожна з методологій має свої позитивні й негативні сторони. На основі проведеного аналізу можна стверджувати, що ключем до успішної оцінки ризиків СЗІ, з метою протидії

останнім, для захисту інформації є поєднання окремих аспектів різних методологій.

Перелік посилань:

1. Потій, О.В. Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки / О.В. Потій, Ю.І. Горбенко, О.А. Замула, К.В. Ісірова. – 2021. – Моделі, методи та засоби захисту інформації в інформаційно-комунікаційних системах. – DOI:10.30837/rt.2021.3.206.01. – URL: https://nure.ua/wp-content/uploads/2021/Scientific_editions/radio_engineering_206/3.pdf (дата звернення: 15.10.2024).

2. Панченко, В. А. Менеджмент інформаційної безпеки комерційного підприємства / В. А. Панченко. – 2019. – Центральноукраїнський науковий вісник. Економічні науки. – Вип. 3(36). – С. 219–228. – DOI: https://doi.org/10.32515/2663-1636.2019.3(36). – URL: http://economics.kntu.kr.ua/pdf/3(36)/23.pdf (дата звернення: 14.10.2024).

Шуклін, Г. В. Методика оцінювання інформаційних загроз в умовах інформаційного протиборства / Г. В. Шуклін, Б. А. Кравченко, В. А. Ковальчук. – 2022. – Сучасний захист інформації. – № 4(52). – DOI: 10.31673/2409-7292.2022.040002. – URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2659 (дата звернення: 15.10.2024).

Корченко, О. Г. Менеджмент інформаційної безпеки: навчальний посібник / О. Г. Корченко, М. Є. Шелест, С. В. Казмірчук, Ю. М. Ткач, Є. В. Іванченко. – Чернігів, 2019. – URL: https://ir.stu.cn.ua/bitstream/handle/123456789/19244/Менеджмент%20інформ.%20безп.%20New%20booklet%201.pdf?sequence=1&isAllowed=y (дата звернення: 16.10.2024).

Назаренко Валерія Дмитрівна
студентка групи БСД-12, ННІЗІ ДУІКТ, Київ, Україна

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ОДИН З ВПЛИВОВІШИХ ІНСТРУМЕНТІВ ОТРИМАННЯ ЧУТЛИВИХ ДАНИХ. ОСНОВНІ ВИДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Соціальна інженерія (social engineering) – це надзвичайно потужний та діючий інструмент, який, використовують для здійснення цілей різноманітного характеру. Найчастіше цей вектор атаки використовують як спосіб доставки шкідливого програмного забезпечення або проникнення у мережу, але іноді він є кінцевою ціллю, наприклад в атаках, напрямлених на те, щоб оманою змусити жертву надати конкретну чутливу інформацію (логіни/паролі, відповіді на ключові питання, такі як дівоче прізвище матері, компромат, номера банківських карт тощо). В більшості випадках не важливий рівень захищеності приладу або інформації, людський фактор все ще є вразливою ціллю. За даними інфографіки від Verizon [1] за 2023 рік 74% всіх порушень частково були пов'язані з людською помилкою, зловживанням привілегіями, використанням викрадених облікових даних та соціальною інженерією. Зважаючи на це, нижче приведені деякі популярні загрози, які використовуються зловмисниками за допомогою соціальної інженерії.

Претекстінг (pretexting). Згідно концепції соціальної інженерії, претекстінг – це акт видачі себе за когось, відігравання певної ролі. Тобто іншими словами, це набір дій, що відпрацьовані за певним, заздалегідь складеним сценарієм, в результаті чого жертва може піти на контакт із зловмисником та видати потрібну йому інформацію або вчинити певну дію. Найчастіше цей вид атаки передбачає використання текстових або голосових засобів по типу відомих месенджерів тощо.

Для здійснення цієї атаки зловмиснику потрібно заздалегідь мати деяку інформацію про потенційну жертву (наприклад, ім'я, посаду на роботі, назву проєктів, над якими вона працює, дату народження і т.п), тобто виникає потреба в

проведенні OSINT операції.

Розвідка за відкритими джерелами (open soutce intelligence, OSINT). Це збір інформації, в конкретному випадку про особу, за відкритими ресурсами, такими як газети/журнали, пошукові системи, документи з різних регулюючих органів, соціальні мережі, реклама, спостереження тощо.

Фішинг та цільовий фішинг. Техніка інтернет-шахрайства, спрямована на отримання конфіденційної інформації користувачів – авторизаційних даних систем. Поширеним видом фішингових атак є відправка фальшивих електронних листів, наприклад, від імені банку, освітньої установи або інших організацій. Часто в таких листах міститься форма для введення персональних даних (пароля, пін-коду, номера банківської карти тощо) або ж шкідливі посилання [2, с. 19].

Звичайні фішингові листи не адресовані конкретній особі, тобто зловмисники проводять розсилку за численними «злитими» адресами користувачів, на відміну від листів, складених для цільового фішингу.

Троянський кінь. Цей вид атаки ґрунтується на емоціях потенційної жерти, наприклад, на страху, цікавості тощо. Зловмисник надсилає користувачу, наприклад, електронного листа, у вкладенні до якого міститься посилання на оновлення програми, ключ до виграшу або компромат на співробітника. Насправді у вкладенні міститься шкідливе ПО, яке після запуску користувачем надасть зловмиснику простір для подальших дій, таких як збір або зміну інформації.

Дорожнє яблуко. Цей метод є різновидом троянського коня і полягає у використанні фізичних носіїв (флешки і т.п.). Зазвичай, зловмисник підкидає такий носій у загальнодоступних місцях на території підприємства/компанії (їдальнях, кафе, паркувальних місцях, туалетах тощо). Для того, щоб співробітник зацікавився предметом, зловмисник може нанести на носій логотип компанії або якийсь підпис, наприклад, «Звіт з податкової». Після того, як жертва під’єднає заражений носій до свого або корпоративного пристрою, запускається шкідливе ПО.

Зворотна соціальна інженерія. В цьому випадку зловмисник створює такі умови, за яких жертва буде сама змушена звернутися до нього. Наприклад, зловмисник може надіслати лист із контактами «служби підтримки» і через деякий час створити оборотні негаразди на пристрої особи. В більшості випадків користувач звернеться за контактами, представленими у такому листі (зателефонує за номером, опише проблему у зворотньому листі тощо). В процесі «виправлення» проблеми зловмисник може отримати необхідні йому дані.

В результаті аналізу описаних методів, можна виділити деякі психологічні концепції, які використовують зловмисники в процесі створення зв’язку із жертвою: маніпуляція, впливовість, взаєморозуміння, авторитет, емпатія тощо.

Перелік посилань:

1. Джо Грей. Социальная инженерия и этичный хакинг на практике / пер. с англ. В. С. Яценкова. – К.: Print2print, 2023. – 226 с.: ил.

2. Verizon Infographics 2023 https://www.verizon.com/business/resources/ja/infographics/2023-dbir-infographic.pdf (дата звернення: 19.10.2024).

Негоденко Віталій Петрович
аспірант, ФІТтаМ , КСУ імені Б. Грінченка,
Київ, Україна

МЕТОДИ MACHINE LEARNING ДЛЯ ВИЯВЛЕННЯ КІБЕРАТАК В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Останнім часом використання методів машинного навчання стало популярним для виявлення кібератак. Машинне навчання виявляється особливо ефективним у аналізі даних та прогнозуванні результатів подій на основі наявних вибіркових даних, що використовуються для побудови відповідної моделі з метою прийняття правильних рішень [1]. Основними завданнями алгоритмів машинного навчання є класифікація та прогнозування наявності або відсутності вивченого екземпляра з використанням навчальних даних.

Розрізняють чотири типи методів машинного навчання: навчання під наглядом, без нагляду, напів під наглядом і з підкріпленням.

Підхід до навчання під наглядом характеризується аспектом розпізнавання образів, який використовує набір позначених екземплярів, які вважаються навчальними даними з відповідним бажаним результатом. За допомогою позначених екземплярів на етапі навчання виводиться прогностична модель для класифікації нових наборів даних. Це досягається шляхом введення мічених екземплярів у певний алгоритм машинного навчання. Деякі з цих підходів машинного навчання, включають дерева рішень, штучну нейронну мережу, K-найближчий сусід (KNN), метод опорних векторів (SVM), прихована модель Маркова (HMM) та інші. Даний підхід використовують до виявлення шкідливих веб-сторінок, які є одним із аспектів кіберпростору, схильних до зловмисних атак.

Існує техніка множинного навчання, яка розглядає вдосконалення підходу кластерного центру та найближчого сусіда (CANN) [2], [3]. Цей підхід під назвою ICANN використовує два керованих алгоритми машинного навчання, тобто алгоритм класифікації k-осередків і алгоритм k-найближчого сусіда. Етапи підходу включають попередню обробку даних, кластеризацію k-середніх, навчання та класифікацію. Нормалізація або попередня обробка лінійно перетворює дані на основі мінімального та максимального набору функцій. За цим процесом негайно слідує кластеризація попередньо обробленого набору даних за допомогою алгоритму кластеризації k-Means. Дані групуються в тестові та навчальні набори даних шляхом присвоєння найбільш схожих даних певному кластеру. П’ять кластерів генеруються на основі кількості типів атак і одного нормального з’єднання в наборі даних NSL-KDD [4].

Підхід до навчання без контролю працює шляхом виявлення шаблонів у

немаркованому наборі даних, який використовується як навчальні дані, щоб прийняти правильні рішення щодо класифікації в наборі нових екземплярів. Зазвичай це передбачає використання кластерів для визначення класів, до яких належать екземпляри. Так в [5] показано, що систему виявлення аномалій представляють рядок атаки, або нормальне з'єднання.

Використання неконтрольованого навчання забезпечує ефективну техніку для класифікації нових екземплярів за допомогою порогу для визначення атаки та звичайних даних під час побудови моделі. На цьому етапі можна чітко визначити суттєвий недолік підходу, заснований на тому факті, що звичайні з'єднання різняться в неоднорідних мережах, і тому профілі побудови нормальної поведінки можуть значно погіршитися. Це значне відхилення в моделях поведінки та характеристиках однієї мережі по відношенню до інших мереж може призвести до неефективної моделі, яка незмінно вимагатиме належного налаштування параметрів та оптимізації відповідно до вимог конкретного мережевого середовища.

Підхід до напівконтрольованого машинного навчання моделює нормальну поведінку за допомогою попередньо позначеного набору даних. В [6] запропонувано двоетапний напівконтрольований статистичний підхід для виявлення мережевих аномалій. Техніка будує імовірнісну модель з використанням попередньо позначених нормальних випадків. Ця модель використовується для оцінки відхилення від нормальної поведінки за допомогою заздалегідь визначеного порогу. На другому етапі використовується ітераційний процес для зменшення частоти помилкових тривог, використовуючи відстань подібності та швидкість дисперсії початкових класифікацій імовірнісної моделі.

Підхід навчання з підкріпленням – це підхід до машинного навчання, який дозволяє програмному агенту, такому як сенсорний вузол, навчатися, взаємодіючи зі своїм середовищем. Даний підхіж є важливим у контексті розпізнавання образів, оскільки воно дозволяє програмним агентам створювати враження від їхньої взаємодії з навколишнім середовищем, щоб виконувати найкращі дії з довгостроковою винагородою [7]. Автори застосували нечітке Q-навчання для виявлення та запобігання вторгненням у WSN. Дана техніка використовує комбінацію кооперативної теорії ігор і алгоритмів нечіткого Q-навчання для виявлення атак DDoS. Цей підхід моделює провали, базову станцію та зловмисника в стратегічній грі для трьох гравців таким чином, що гра активується, коли потік пакетів спрямовується на вузол-жертву. Але дана модель потребує цілісного вдосконалення для покращення можливостей прийняття рішень, особливо щодо скорочення нових атак.

Висновки. Розвиток різноманітності загроз і розповсюдження складних методів ухилення, вкрай важливо мати підхід, здатний вивчати кілька рівнів представлень, що відповідають різним рівням абстракцій, щоб ці рівні утворювали каскад концепцій. За допомогою цих концепцій приховані рівні можуть служити вхідними даними для наступного рівня та в процесі розробки представлень

функцій у внутрішніх рівнях для отримання точних або майже точних результатів для виявлення та прогнозування багатоетапних кібератак. Отже, механізм захисту від атак може швидко адаптуватися та вчитися на попередньому досвіді на основі кількох зразків, щоб зробити висновки та виявити ймовірність нових атак, а також скоротити їх у реальному часі.

Перелік посилань:

1. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection”, IEEE Communications Surveys & Tutorials, vol. 18, no. 2, (2016), pp. 1153-1176.
2. W. C. Lin, S. W. Ke and C. F. Tsai, “CANN: An intrusion detection system based on combining cluster centers and nearest neighbors”, Knowledge-based systems, vol. 78, (2015), pp. 13-21.
3. H. Shapoorifard and P. Shamsinejad, “A Novel Cluster-based Intrusion Detection Approach Integrating Multiple Learning Techniques”, International Journal of Computer Applications, vol. 166, no. 3, (2017), pp. 13-16.
4. Ayei E. Ibor, Florence A. Oladeji, Olusoji B. Okunoye A Survey of Cyber Security Approaches for Attack Detection, Prediction, and Prevention // International Journal of Security and Its Applications Vol. 12, No. 4 (2018), pp.15-28 http://dx.doi.org/10.14257/ijsia.2018.12.4.02
5. J. Song, H. Takakura, Y. Okabe and K. Nakao, “Toward a more practical unsupervised anomaly detection system”, Information Sciences, vol. 231, (2013), pp. 4-14.
6. N. B. Aissa and M. Guerroumi, “Semi-supervised statistical approach for network anomaly detection”, Procedia Computer Science, vol. 83, (2016), pp. 1090-1095.
7. S. Shamshirband, A. Patel, N. B. Anuar, M. L. M. Kiah and A. Abraham, “Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks”, Engineering Applications of Artificial Intelligence, vol. 32, (2014), pp. 228-241.

Олейников Олександр Дмитрович
студент групи БСДМ-63, ННІКБЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ МЕРЕЖЕВИХ АТАК НА ОСНОВІ XDR

У сучасну цифрову епоху мережеві атаки стають все більш складними та частішими, що створює серйозні виклики для кібербезпеки. Extended Detection and Response (XDR) постає як інноваційна технологія, здатна ефективно виявляти та реагувати на сучасні загрози. Розуміння принципів роботи XDR та його переваг над традиційними засобами захисту є ключовим для побудови надійної системи безпеки. Впровадження XDR-рішень може значно підвищити здатність організацій протидіяти складним кіберзагрозам.

У сучасному цифровому світі мережеві атаки стають все більш складними та частішими, створюючи серйозні виклики для кібербезпеки. Технологія Extended Detection and Response (XDR) пропонує інноваційний підхід до виявлення та реагування на ці загрози. У цій роботі розглядається застосування XDR для підвищення ефективності захисту інформаційних систем від сучасних кіберзагроз.

XDR забезпечує виявлення та реагування на інциденти, пов'язані з безпекою,

на різних рівнях інформаційно-технологічного середовища. Він збирає інформацію, а потім автоматично з'єднує дані з кінцевих точок, електронної пошти, хмарних робочих навантажень, серверів, а також мереж, щоб виявити приховані загрози і дозволити експертам з безпеки швидко дослідити їх і відреагувати на них [4].

XDR об'єднує дані з розрізнених рішень безпеки, щоб вони могли працювати разом, покращуючи видимість загроз і скорочуючи час, необхідний для виявлення атаки та реагування на неї. XDR дозволяє проводити розширені криміналістичні дослідження та відстежувати загрози в різних доменах з однієї консолі.

Процес роботи цього типу рішень можна умовно поділити на три кроки:

Крок 1. Поглинання та нормалізація обсягів даних з кінцевих точок, хмарних робочих навантажень, ідентифікаційних даних, електронної пошти, мережевого трафіку, віртуальних контейнерів тощо.

Крок 2. Аналіз та кореляція даних для автоматичного виявлення прихованих загроз за допомогою передових технологій штучного інтелекту (ШІ) та машинного навчання (МН).

Крок 3. Розподіл даних про загрози за ступенем серйозності, щоб мисливці за загрозами могли швидко аналізувати і сортувати нові події, а також автоматизувати розслідування і заходи реагування [2].

Крім того, XDR централізує робочі процеси виявлення, розслідування, пошуку та реагування на загрози, дозволяючи аналітикам з безпеки переключатися між робочими процесами без переходу на інший інструмент [1].

Отже, технологія Extended Detection and Response (XDR) є ключовим інструментом у сучасній кібербезпеці, що дозволяє ефективно виявляти мережеві аномалії. XDR об'єднує дані з різних джерел, таких як кінцеві точки, мережеві пристрої та хмарні сервіси, створюючи цілісний огляд всієї інфраструктури. Це сприяє швидшому виявленню загроз і зменшенню часу реагування на інциденти.

Однак традиційні засоби захисту часто працюють ізольовано, що призводить до пропуску складних багатовекторних атак. Без інтегрованого підходу організації ризикують не помітити критичні загрози. XDR вирішує цю проблему, надаючи можливість кореляції даних між різними системами та виявлення прихованих аномалій.

Ключовою можливістю XDR є використання штучного інтелекту та машинного навчання для аналізу поведінкових патернів. Це дозволяє не лише виявляти відомі загрози, але й ідентифікувати нові, раніше невідомі атаки. Таким чином, XDR забезпечує проактивний підхід до кібербезпеки, підвищуючи загальний рівень захисту.

Водночас впровадження XDR може стикатися з викликами, такими як складність інтеграції та потреба в додаткових ресурсах. Без належної підготовки та інвестицій організації можуть не отримати повну користь від цієї технології. Проте, переваги XDR у виявленні мережевих аномалій та реагуванні на них значно переважають потенційні труднощі, роблячи його необхідним компонентом

сучасної стратегії кібербезпеки. [3]

Зважаючи на ключові можливості XDR у виявленні мережевих аномалій, зростає потреба в ефективних та інноваційних рішеннях. Теза полягає в тому, що ринок XDR активно розвивається завдяки підвищеному попиту на комплексні засоби кібербезпеки. Антитеза вказує на те, що велика кількість постачальників може ускладнити вибір оптимального рішення для конкретної організації.

Ринок XDR стрімко розвивається, причому платформи та послуги XDR пропонують як відомі постачальники систем безпеки, так і стартапи. Нижче наведені деякі відомі постачальники XDR та їхні технології, перелічені в алфавітному порядку [1]:

- Bitdefender GravityZone XDR.
- Carbon Black XDR.
- Cisco XDR.
- Cortex XDR (Palo Alto Networks).
- CrowdStrike Falcon Insight XDR.
- Cybereason XDR.
- Elastic Security for XDR.
- IBM Security QRadar XDR.
- Kaspersky Extended Detection and Response.
- Microsoft Defender XDR.
- Singularity XDR (SentinelOne).
- Sophos XDR.
- Trellix XDR.
- Trend Vision One XDR (Trend Micro).

На підставі проведеного аналізу можна зробити висновок, що технологія XDR є критично важливою для сучасних організацій у протидії складним кіберзагрозам. Її здатність об'єднувати дані з різних джерел і використовувати передові технології штучного інтелекту та машинного навчання підвищує ефективність виявлення та реагування на атаки. Незважаючи на можливі виклики впровадження, такі як складність інтеграції та необхідність додаткових ресурсів, переваги XDR значно перевищують потенційні труднощі. Тому інтеграція XDR у стратегію кібербезпеки є необхідним кроком для забезпечення надійного захисту інформаційних систем.

Перелік посилань:

1. Kerner S. M. What is extended detection and response (XDR)?. Security. URL: https://www.techtarget.com/searchsecurity/definition/extended-detection-and-response-XDR (date of access: 05.10.2024).

2. What is XDR? Extended detection & response - crowdstrike. crowdstrike.com. URL: https://www.crowdstrike.com/cybersecurity-101/what-is-xdr/ (date of access: 05.10.2024).

3. XDR for networks. Trend Micro Products & Solutions | TrendDefense.com. URL: https://www.trenddefense.com/datasheets/ds-xdr-for-networks.pdf (date of access: 05.10.2024).

4. XDR: the evolution of endpoint security solutions - superior extensibility and analytics to satisfy the organizational needs of the future / A. S. George et al. International journal of advanced research in science, communication and technology. 2021. P. 493–501. URL: https://doi.org/10.48175/ijarsct-1888 (date of access: 05.10.2024).

Отруба Денис Віталійович
студент групи БСД-12, ННІЗІ ДУІКТ, Київ, Україна

ВІРУСИ

Комп'ютерні віруси залишаються однією з найбільш небезпечних і поширених загроз для інформаційної безпеки в сучасному цифровому середовищі. З моменту появи першого вірусу у 1980-х роках, вони еволюціонували від простих програм, які викликали незначні збої, до складних шкідливих програм, здатних викрадати конфіденційні дані, шифрувати файли з метою отримання викупу, впливати на функціонування цілих організацій, а також проникати в критичні інфраструктури. Ці програми можуть поширюватися різними шляхами — через електронну пошту, заражені вебсайти, змінні носії, а також через соціальні інженерні методи, які експлуатують людські слабкості.

Захист від вірусів потребує комплексного підходу, який включає впровадження надійного антивірусного програмного забезпечення, регулярні оновлення систем, резервне копіювання даних, а також навчання користувачів щодо безпечного користування Інтернетом. Розуміння різних типів вірусів, таких як трояни, черв'яки, шпигунські програми та програми-вимагачі, дозволяє ефективніше виявляти загрози і швидко реагувати на них. З огляду на постійний розвиток технологій та методів атак, стратегія кіберзахисту має бути динамічною та постійно адаптуватися до нових викликів.

Види вірусів:
- Шкідник
- Знищувач
- Хробак
- Жарт
- Комбінований

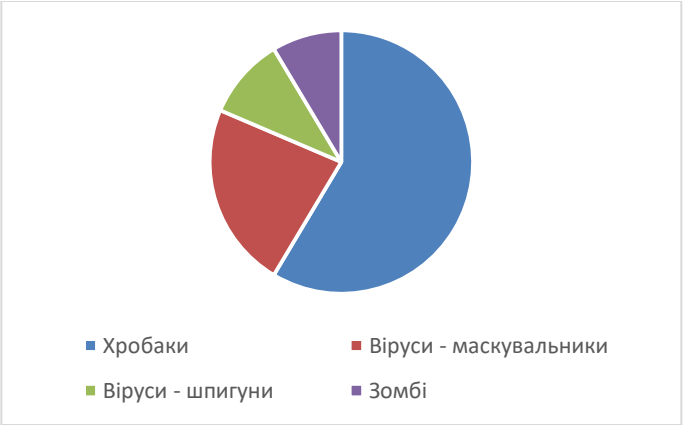


Рисунок.1. Найпопулярніші віруси в використанні кібератак

Перелік посилань:

1. uk.wikipedia.org
2. zillya.ua
3. cyberpolice.gov.ua

Парфенюк Тетяна
студентка групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

ЗАСТОСУВАННЯ РОЛЬОВОЇ МОДЕЛІ ДОСТУПУ ДЛЯ КЕРУВАННЯ ПРИВІЛЕЙОВАНИМИ ОБЛІКОВИМИ ЗАПИСАМИ

Згідно з дослідженням, рольова модель доступу (RBAC) є одним із найефективніших підходів для захисту привілейованих облікових записів, які часто залишаються критичною вразливістю в організаціях. Використання RBAC дозволяє мінімізувати ризики за рахунок чіткого розмежування прав доступу, відповідно до посадових обов'язків користувачів, що забезпечує дотримання принципу найменших привілеїв. Це означає, що кожен користувач отримує лише необхідні для роботи дозволи, що значно знижує ймовірність зловживань привілеями. Основними компонентами RBAC є ролі, дозволи, користувачі та відносини між ними, що забезпечує централізоване керування доступом та регулярний контроль за привілеями. Це підвищує ефективність внутрішнього контролю і сприяє відповідності сучасним вимогам безпеки та аудиту.

Застосування рольової моделі доступу (RBAC) є одним із найбільш ефективних підходів для управління привілейованими обліковими записами, що дозволяє знизити ризики безпеки та забезпечити відповідність сучасним вимогам комплаєнсу. Основою RBAC є чітке розмежування доступу на основі ролей, що представляють посадові функції або обов'язки користувачів. Ключові компоненти RBAC включають ролі, дозволи, користувачів, а також відносини між ролями та дозволами, що спрощує управління доступом та привілеями в організації.

Ролі у RBAC представляють певні набори дозволів, необхідні для виконання користувачами їхніх робочих обов'язків. Дозволи, у свою чергу, визначають конкретні права на виконання дій на ресурсах, наприклад, читання, запис або зміну даних. Призначення користувачам відповідних ролей згідно з їх посадовими обов'язками забезпечує дотримання принципу "найменших привілеїв", що означає мінімізацію доступу до лише тих ресурсів, які необхідні для роботи. Такий підхід знижує ймовірність зловживань привілейованими правами та підвищує ефективність внутрішнього контролю.

Можна виділити ключові компоненти RBAC: ролі, дозволи, користувачі, відносини між ролями та дозволами.

Ключові компоненти рольової моделі доступу (RBAC) тісно пов'язані з реалізацією принципу найменших привілеїв, що полягає в наданні користувачам лише тих прав доступу, які необхідні для виконання їхніх робочих завдань. Ось як кожен компонент сприяє дотриманню цього принципу:

Ролі представляють набір дозволів, які відповідають конкретним посадовим обов'язкам користувача. Користувач отримує доступ до системи не безпосередньо через окремі дозволи, а через ролі, що обмежує його доступ лише до функцій,

потрібних для виконання конкретних завдань. Це виключає можливість надання надмірного доступу до інших ресурсів.

Дозволи визначають конкретні дії, які може виконувати користувач (наприклад, читання, запис, зміна). Дозволи прив'язуються до ролей, що дозволяє чітко обмежити можливості користувачів виконувати тільки ті операції, які необхідні для їхньої ролі. Таким чином, принцип найменших привілеїв реалізується через ретельне визначення мінімально необхідних прав для кожної ролі.

Користувачі асоціюються з ролями на основі їхніх робочих обов'язків. Це забезпечує те, що користувач отримує тільки ті дозволи, які відповідають його ролі, без доступу до додаткових ресурсів або операцій, що не стосуються його функцій.

Відображення прав доступу до ролей дозволяє централізовано керувати дозволами для великої кількості користувачів. Оскільки дозволи прив'язуються до ролей, а не до окремих користувачів, це спрощує процес забезпечення того, щоб кожен користувач мав тільки ті привілеї, які йому потрібні.

Таким чином, рольова модель доступу (RBAC) забезпечує дотримання принципу найменших привілеїв завдяки централізованому контролю ролей та дозволів, чіткій ієрархії прав доступу і регулярному перегляду привілеїв, що мінімізує можливості для зловживання або випадкових дій користувачів.

Перелік посилань:

1Role-Based Access Control (RBAC): A Key to Streamlined Access Management. URL: Role-Based Access Control: Simplifying Access Security Management (дата звернення: 26.09.2024)
2The Definitive Guide to Role-Based Access Control (RBAC). URL: The Definitive Guide to Role-Based Access Control (RBAC) | StrongDM (дата звернення: 01.10.2024)

Петрова Олександра Сергіївна
студентка групи БСД-22,, ННІЗІ ДУІКТ, Київ, Україна

СТАНДАРТИЗАЦІЯ ТА ПРАКТИКИ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ СИСТЕМАХ

У тезах розглянуто роль стандартизації у забезпеченні кібербезпеки корпоративних інформаційних систем. Акцент зроблено на важливості міжнародних стандартів, таких як ISO 27001, для впровадження ефективної інформаційної безпеки.

Корпоративні інформаційні системи є основою сучасного бізнесу. Вони потребують захисту від кіберзагроз через постійне використання складних мереж та інтеграцію різних пристроїв, включно з мобільними. Стандартизація процесів безпеки дозволяє підвищити ефективність захисту, забезпечити відповідність законодавству та полегшити впровадження політик інформаційної безпеки.

1. **ISO/IEC 27001 як основа інформаційної безпеки**
   Стандарт ISO/IEC 27001 надає структуровану основу для розробки, впровадження та управління системами інформаційної безпеки, мінімізуючи ризики для цілісності, конфіденційності та доступності даних.
2. **NIST Framework для управління кіберризиками**
   Рамкова модель NIST допомагає ідентифікувати, захищати, виявляти, реагувати та відновлюватися після кіберінцидентів, полегшуючи управління ризиками для організацій будь-якого розміру.
3. **Вплив GDPR на корпоративну безпеку даних**
   Загальний регламент про захист даних (GDPR) встановлює суворі вимоги до обробки персональних даних, сприяючи прозорості та відповідальності в корпоративних практиках управління даними.
4. **Зменшення ризиків мобільної безпеки за допомогою стандартів**
   Інтеграція мобільних пристроїв у корпоративні системи створює нові вразливості, які можна ефективно управляти за допомогою стандартів ISO 27001 та NIST, забезпечуючи безпечне зберігання та передачу даних.
5. **Стандартизація як конкурентна перевага**
   Компанії, що впроваджують визнані стандарти безпеки, не лише відповідають вимогам регуляторів, але й підвищують довіру клієнтів та партнерів, отримуючи конкурентні переваги на ринку.

ВИСНОК

Стандартизація є ключовим інструментом у боротьбі з сучасними кіберзагрозами. Впровадження міжнародних стандартів, таких як ISO 27001 та NIST, підвищує стійкість корпоративних систем до атак та забезпечує відповідність законодавству. Урахування безпеки мобільних пристроїв є невід'ємною частиною ефективної СУІБ.

Перелік посилань:

1. ISO/IEC 27001. Information Security Management Systems. URL: ISO.com.
2. NIST Cybersecurity Framework. URL: NIST.gov.
3. General Data Protection Regulation (GDPR). URL: EU GDPR.
4. Смартфони та корпоративна інформація: основні ризики та як їм запобігти. URL: Softline.

STANDARDIZATION AND INFORMATION SECURITY PRACTICES IN CORPORATE SYSTEMS

This paper explores the role of standardization in ensuring the cybersecurity of corporate information systems. Emphasis is placed on the importance of international standards, such as ISO 27001, for implementing effective information security.

Corporate information systems form the backbone of modern business operations. These systems require protection from cyber threats due to the increasing complexity of networks and the integration of various devices, including mobile ones. Standardization

improves the efficiency of security processes, ensures regulatory compliance, and simplifies the implementation of security policies.

1. **ISO/IEC 27001 as the Foundation of Information Security**
   The ISO/IEC 27001 standard provides a structured framework for developing, implementing, and managing information security systems, minimizing risks to data integrity, confidentiality, and availability.
2. **NIST Framework for Cyber Risk Management**
   The NIST Cybersecurity Framework guides the identification, protection, detection, response, and recovery from cyber incidents, facilitating effective risk management for organizations of all sizes.
3. **GDPR's Impact on Corporate Data Security**
   The General Data Protection Regulation (GDPR) enforces strict requirements for personal data processing, promoting transparency and accountability in corporate data management practices.
4. **Mitigating Mobile Security Risks through Standards**
   The integration of mobile devices into corporate systems introduces new vulnerabilities, effectively managed using ISO 27001 and NIST frameworks to ensure secure data storage and transmission.
5. **Standardization as a Competitive Advantage**
   Companies that implement recognized security standards not only meet regulatory requirements but also enhance customer trust and gain a competitive edge in the market.

CONCLUSION

Standardization plays a vital role in strengthening the cybersecurity of corporate information systems. Adopting and implementing standards such as ISO 27001, NIST, and GDPR ensures better risk management, regulatory alignment, and the protection of business-critical data. Addressing the risks associated with mobile devices is essential to a comprehensive cybersecurity strategy.

REFERENCES:

1. ISO/IEC 27001. Information Security Management Systems. URL: ISO.com.
2. NIST Cybersecurity Framework. URL: NIST.
3. General Data Protection Regulation (GDPR). URL: EU GDPR.
4. Smartphones and Corporate Information: Key Risks and How to Prevent Them. URL: Softline.

Поліщук Артем Сергійович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

Технологія впровадження DevSecOps з використанням Sonarqube

Анотація: В умовах сучасної розробки програмного забезпечення питання безпеки стає все більш критичним. Традиційні підходи, які включають заходи безпеки на пізніх етапах розробки, більше не відповідають вимогам часу, оскільки не забезпечують достатнього захисту від новітніх загроз. DevSecOps — це підхід, що інтегрує безпеку на всіх етапах процесу розробки, забезпечуючи швидку і надійну ідентифікацію та усунення вразливостей. Метою цієї роботи є дослідження технології DevSecOps та її впровадження з використанням SonarQube для автоматизованого статичного аналізу коду та інтеграції у CI/CD процеси за допомогою таких інструментів, як GitLab та Jenkins.

Підходи до розробки програмного забезпечення зазнали значних змін у зв’язку зі зростанням кількості кібератак та вимог до безпеки. Зараз розробники не можуть дозволити собі впроваджувати безпеку лише на останніх етапах життєвого циклу програмного забезпечення. Необхідність впровадження безпеки від самого початку розробки призвела до появи нових методологій, серед яких особливе місце займає DevSecOps — підхід, що поєднує розробку, операційну діяльність і безпеку.

DevSecOps змінює традиційні підходи до інформаційної безпеки шляхом її інтеграції у процес безперервної розробки. Він сприяє підвищенню продуктивності команд розробки, знижуючи кількість вразливостей у вихідному коді. Одним з основних інструментів для реалізації DevSecOps є SonarQube, що забезпечує глибокий статичний аналіз коду та виявлення потенційних загроз ще на ранніх етапах розробки.

Поняття DevSecOps

DevSecOps — це практика, що об’єднує розробку (Dev), безпеку (Sec) та операційні процеси (Ops) в єдиному конвеєрі. Основним принципом є забезпечення того, щоб безпека не була додатковим етапом, а невід'ємною частиною всієї розробки програмного забезпечення. Це досягається за допомогою автоматизації процесів безпеки, що дозволяє виявляти потенційні загрози та вразливості на кожному етапі розробки. Впровадження безпеки стає обов’язковим елементом кожного циклу: від написання коду до його розгортання та експлуатації. [1]

Переваги DevSecOps полягають у:

- Швидкому виявленні вразливостей завдяки безперервній інтеграції інструментів безпеки.
- Автоматизації процесів безпеки, що дозволяє скоротити час на тестування та усунення загроз.
- Підвищенні загальної надійності програмного забезпечення за рахунок інтеграції перевірок безпеки на ранніх етапах. [3]

SonarQube: можливості та інтеграція

SonarQube є одним із найпотужніших інструментів для статичного аналізу вихідного коду, що дозволяє виявляти помилки та вразливості в коді. Його головними функціями є:

- Виявлення помилок коду (баги, проблеми продуктивності).

- Аналіз технічного боргу, що дозволяє командам відстежувати ділянки коду, які можуть ускладнити підтримку та масштабування системи.

- Визначення уразливостей безпеки, таких як SQL-ін’єкції, проблеми з доступом та некоректна обробка даних.

- Підтримка понад 25 мов програмування, включаючи Java, C#, Python, JavaScript тощо.

SonarQube легко інтегрується з такими інструментами CI/CD, як GitLab і Jenkins, що забезпечує автоматичну перевірку якості коду під час кожного коміту. Завдяки інтеграції з GitLab, SonarQube може автоматично запускати аналіз при створенні Pull Requests або Merge Requests, а вбудовані звіти дозволяють відстежувати якість та безпеку коду в реальному часі. [2]

Інтеграція з GitLab

GitLab забезпечує повну інтеграцію з DevOps процесами, дозволяючи автоматизувати всі етапи розробки — від написання коду до його розгортання. SonarQube може бути налаштований як частина пайплайнів у GitLab, автоматично перевіряючи кожен коміт на наявність потенційних загроз. Це забезпечує миттєвий зворотний зв'язок для розробників і дозволяє швидко виправляти виявлені помилки. [5]

Інтеграція з Jenkins

Jenkins є найпоширенішим інструментом для автоматизації процесів CI/CD. Завдяки плагіну SonarQube для Jenkins, можливо легко інтегрувати аналіз коду на кожному етапі пайплайну. Під час збірки коду Jenkins запускає перевірку коду за допомогою SonarQube і надає розробникам звіти про стан безпеки та якості коду. Цей процес дозволяє автоматично відстежувати дотримання стандартів безпеки та знижує ймовірність потрапляння вразливостей у фінальний продукт. [4]

Впровадження DevSecOps з використанням SonarQube значно покращує якість та безпеку програмного забезпечення завдяки безперервному аналізу коду та інтеграції з інструментами CI/CD. Така система дозволяє розробникам виявляти і усувати вразливості на ранніх етапах розробки, що в свою чергу знижує ризики і забезпечує надійний захист програмних продуктів. Інтеграція SonarQube з GitLab та Jenkins забезпечує автоматизацію процесу безпеки, що є ключовим аспектом у сучасних підходах до розробки. Завдяки таким рішенням, команди можуть досягати високого рівня безпеки і якості, не знижуючи продуктивності.

Перелік посилань:

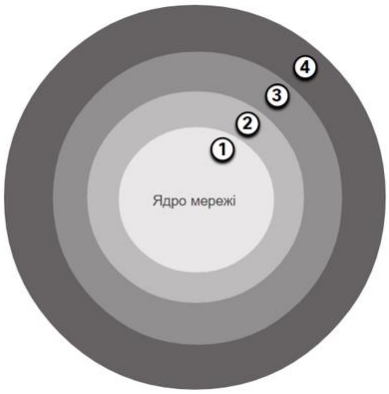
1. Kim, G., Humble, J., Debois, P., Willis, J. *The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations*. Portland: IT Revolution Press, 2016. 490 с.
2. SonarSource. SonarQube Documentation [Електронний ресурс]. – Режим доступу: https://docs.sonarqube.org/latest/
3. Fitzgerald, P. *DevSecOps: A Guide for DevOps Engineers*. O’Reilly Media, 2019. 340 с.
4. Jenkins User Documentation [Електронний ресурс]. – Режим доступу: https://www.jenkins.io/doc/
5. GitLab Documentation [Електронний ресурс]. – Режим доступу: https://docs.gitlab.com/

Сайчук Вадим Дмитрович
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

Технологія забезпечення мережевої безпеки на базі Cisco.

Технологія забезпечення мережевої безпеки - сукупність програмних, технічних та організаційних засобів для забезпечення безперебійної роботи усіх ресурсів мережі та доступу до інформаційних сервісів користувачам у корпоративних мережах. В сучасних інформаційних системах кожну секунду проходить мільйони пакетів даних, частина з яких є небезпечна для інформаційного середовища. Враховуючи на постійно зростаючі загрози спеціалісти з мережевої безпеки щодня розробляють, тестують та впроваджують в роботу нові методи захисту. 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. Це протистояння спонукає організації витрачати все більше коштів на захист своїх даних у мережі.

Будь-яку мережу можна схематично описати як багаторівневе ядро захисту.



1. Безпека ядра мережі – захищає від зловмисного програмного забезпечення та аномалій трафіку, забезпечує дотримання мережевих політик і забезпечує надійність.

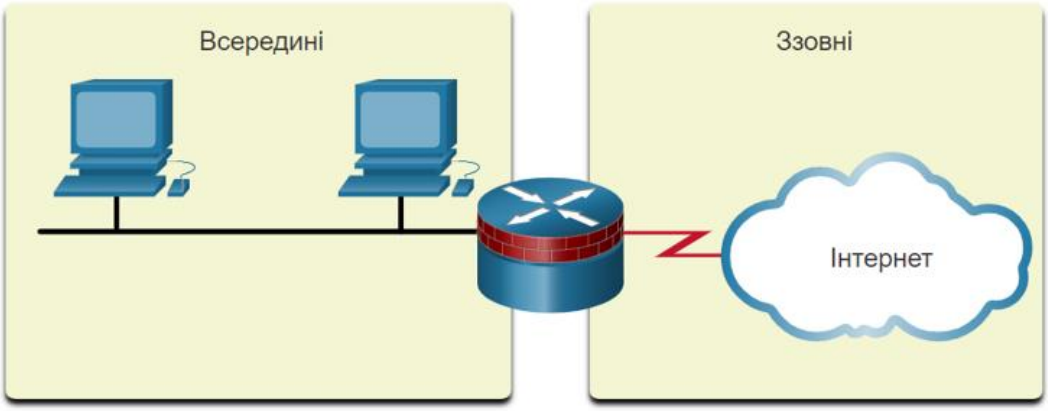
2. Охорона периметра – захищає межі між зонами.

3. Комунікаційна безпека – забезпечує надійність інформації.

4. Безпека кінцевої точки – забезпечує відповідність ідентифікації та політик безпеки пристрою.

Взявши за приклад мережеве обладнання компанії Cisco, яке є доволі ефективним рішенням для забезпечення мережевої безпеки, в своє чергу вимагає значних коштів на реалізацію даного захисту, яке розтягнеться у часі для реалізації, та буде потребувати велику кількість людських ресурсів і умінь.

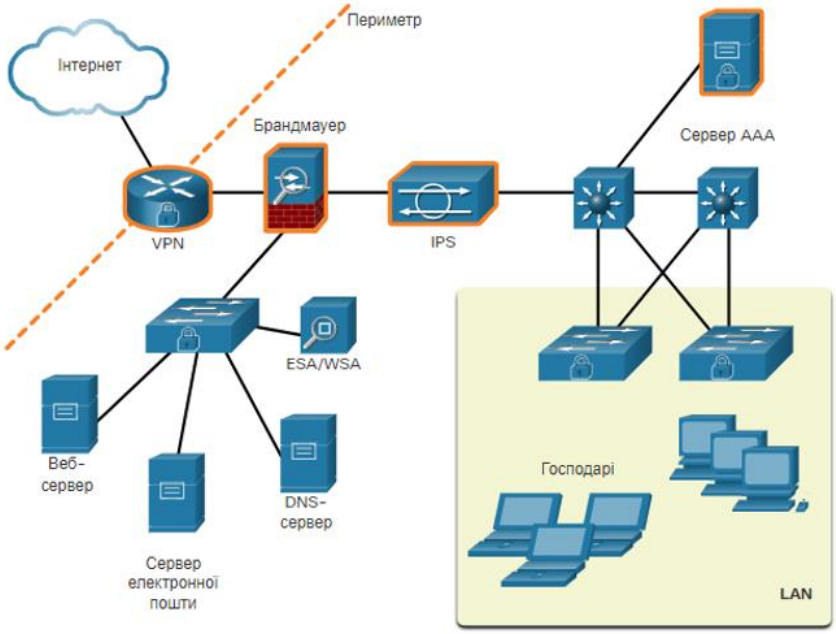
На першому етапі необхідно з технічної точки зору спроектувати мережу, визначити першочергові задачі для її захисту та визначитись із обладнанням. Основною задачею захисту мережі є захист вторгнень з мережі Інтернет. Для даної задачі використовують Брандмауер (firewall). Ці пристрої використовуються, як для захисту мережі в цілому, так і для захисту окремих комп’ютерів у даній мережі. Лінійка брандмауерів Cisco доволі різноманітна та розрахована на різний бюджет.



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.

У інформаційних системах брандмауер може бути на основі як програмного так і апаратного забезпечення, який забезпечує зв’язок між локальними (безпечними) та небезпечними (Інтернет) мережами.

Для організації безпеки у середині мережі за часту використовують маршрутизатори та комутатори, які мають великий функціонал для налаштування правил безпеки.



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.

Можна зробити висновок, що технологія забезпечення мережевої безпеки є необхідною мірою захисту в сучасному цифровому світі. Вона повинна постійно

розвиватись та удосконалюватись, тому що кіберзлочинці все частіше знаходять нові і нові методи атак на мережу, з метою подальшого її контролю та заволодінню конфіденційною інформацією.

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.
4) ДСТУ 3396.1-96 ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Information protection. Technical protection of information. Order of carrying out the works. Чинний від 01.07.1997 р.

Семерич Олена Сергіївна, БСДМ-63
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНИХ ВЕБ-ДОДАТКІВ І API НА БАЗІ IMPERVA WEB APPLICATION FIREWALL

Визначено мету і основні завдання щодо захисту корпоративних веб-додатків і API. Розглянуто зміст технології захисту корпоративних веб-додатків і API на базі Imperva Web Application Firewall.

У Звіті [1] зазначається, що за останній рік автоматизовані загрози викликали 30% атак API. Серед них 17% атак було здійснено поганими ботами, які використовували вразливості бізнес-логіки, 13% атак було здійснено іншими видами автоматичних загроз. Атаки на бізнес-логіку використовують недоліки в дизайні та реалізації додатків, що дозволяє зловмисникам маніпулювати законними функціями та потенційно отримати доступ до конфіденційних даних або облікових записів користувачів.

Погані боти взаємодіють із додатками таким чином, щоб імітувати дії законних користувачів, що ускладнює їх виявлення та блокування. Вони використовують бізнес-логіку, використовуючи призначені функції та процеси додатків, а не її технічні вразливості. Погані боти сприяють високошвидкісному зловживанню, неправильному використанню та атакам на веб-сайти, мобільні додатки та API. Вони дозволяють операторам ботів, зловмисникам, недобросовісним конкурентам і шахраям брати участь у зловмисних діях. Такі дії, як сканування веб-сайтів, конкурентоспроможний аналіз даних, збір особистих і фінансових даних, спроби входу грубою силою, скальпінг, шахрайство з цифровою рекламою, атаки на відмову в обслуговуванні, спам, шахрайство з транзакціями та інші подібні дії можуть завдати шкоди бізнесу. Ці дії споживають пропускну здатність, уповільнюють роботу серверів і викрадають конфіденційні дані, що призводить до фінансових втрат і шкоди репутації компанії [1].

Брандмауери веб-програм (Web Application Firewall, WAF) є критично

важливим захистом для веб-сайтів, мобільних додатків і API. Вони відстежують, фільтрують і блокують пакети даних до та з веб-додтаків, захищаючи їх від загроз. WAF розроблено (навчено) для виявлення та захисту від небезпечних недоліків безпеки, які найчастіше зустрічаються в веб-трафіку. Це робить їх необхідними для онлайн-бізнесу, як-от роздрібна торгівля, банки, охорона здоров'я та соціальні мережі, яким необхідно захищати конфіденційні дані від несанкціонованого доступу. WAF можна розгортати як мережеві, хостові або хмарні рішення, забезпечуючи видимість даних додатків на прикладному рівні HTTP [2].

Оскільки веб- і мобільні додатки та API схильні до ризиків безпеки, які можуть порушити роботу або виснажити ресурси, брандмауери веб-додатки призначені для протидії поширеним веб-експлойтам, таким як шкідливі роботи. WAF захищають від загроз, які можуть впливати на доступність, безпеку або ресурси, включаючи експлойти нульового дня, ботів і шкідливе програмне забезпечення [2].

WAF може бути програмним забезпеченням, пристроєм або послугою. Він аналізує HTTP-запити та застосовує набір правил для визначення, які частини цієї розмови є доброякісними, а які – шкідливими [3].

Основними частинами HTTP-розмов, які аналізує WAF, є запити GET і POST. Запити GET використовуються для отримання даних із сервера, а запити POST використовуються для надсилання даних на сервер для зміни його стану.

WAF можуть бути на основі хоста, мережі або хмари і зазвичай розгортаються через зворотні проксі та розміщуються перед додатком чи веб-сайтом (або кількома додатками та сайтами) (рисунок 1) [4].

WAF можуть працювати як мережеві пристрої, серверні плагіни або хмарні служби, перевіряючи кожен пакет і аналізуючи логіку прикладного рівня (рівень 7) відповідно до правил, щоб відфільтрувати підозрілий або небезпечний трафік [4].

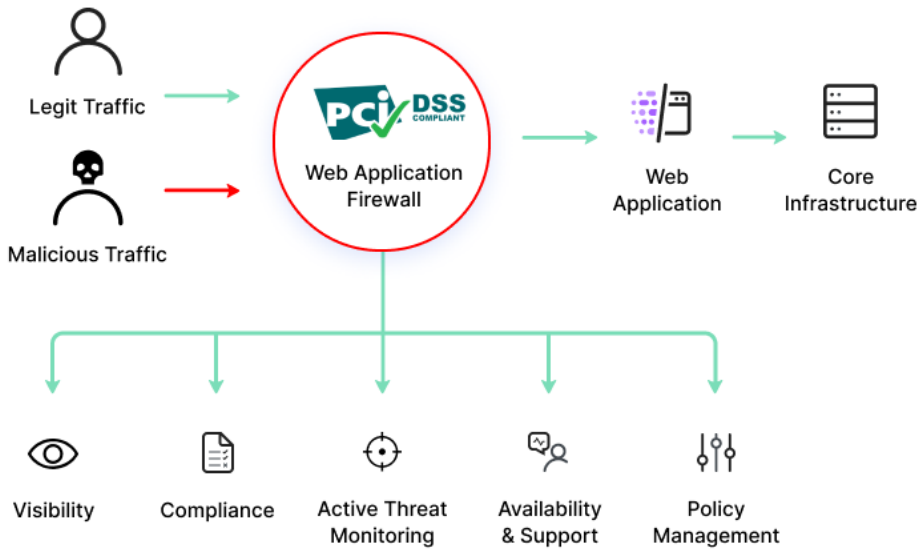


Рис. 1. Місце WAF в архітектурі веб-додатків [4]

WAF зазвичай пропонують такі функції та можливості [4]:

виявлення атак на основі бази даних сигнатур. Сигнатури атак – це шаблони, які можуть вказувати на зловмисний трафік, включаючи типи запитів, аномальні відповіді сервера та відомі шкідливі IP-адреси. Раніше WAF покладалися переважно на бази даних шаблонів атак, які були менш ефективними проти нових або невідомих атак;

аналіз трафіку за допомогою штучного інтелекту. Алгоритми штучного інтелекту дозволяють аналізувати поведінку моделей трафіку, використовуючи базові показники поведінки для різних типів трафіку для виявлення аномалій, які вказують на атаку. Це дозволяє виявляти атаки, які не відповідають відомим шаблонам шкідливих дій;

профілювання додатка. Це передбачає аналіз структури додатка, включаючи типові запити, URL-адреси, значення та дозволені типи даних. Це дозволяє WAF ідентифікувати та блокувати потенційно шкідливі запити;

налаштування WAF. Адміністратори можуть визначати правила безпеки, що застосовуються до трафіку додатка. Це дозволяє організаціям налаштовувати поведінку WAF відповідно до своїх потреб і запобігати блокуванню законного трафіку;

механізми кореляції. Вони аналізують вхідний трафік і сортують його за відомими сигнатурами атак, профілюванням додатків, аналізом ШІ та спеціальними правилами, щоб визначити, чи слід його блокувати;

платформа захисту від DDoS. Є можливість інтегрувати хмарну платформу, яка захищає від розподіленої атаки відмови в обслуговуванні (DDoS). Якщо WAF виявляє DDoS-атаку, він може передати трафік на платформу захисту від DDoS, яка може впоратися з великою кількістю атак;

забезпечення мережі доставки контенту (CDN). WAF розгортаються на межі мережі, тому WAF, розміщений у хмарі, може забезпечити CDN для кешування веб-сайту та скорочення часу його завантаження. WAF розгортає CDN у кількох точках присутності (PoP), які розподілені по всьому світу, тому користувачі обслуговуються з найближчої точки присутності.

WAF можуть використовувати позитивну або негативну модель безпеки або комбінацію двох [4]:

Позитивна модель безпеки WAF передбачає білий список, який фільтрує трафік відповідно до списку дозволених елементів і дій. Все, що не входить до списку, блокується. Перевагою цієї моделі є те, що вона може блокувати нові або невідомі атаки, яких розробник не передбачав.

Негативна модель безпеки WAF передбачає чорний список (або список заборони), який блокує лише певні елементи – дозволено все, що не входить до списку. Цю модель легше реалізувати, але вона не може гарантувати, що всі загрози будуть усунені. Це також вимагає ведення потенційно довгого списку шкідливих

сигнатур. Рівень безпеки залежить від кількості реалізованих обмежень.

Рішення SecureSphere WAF компанії Imperva захищає веб-додатки, забезпечуючи захист і контроль над критично важливими даними.

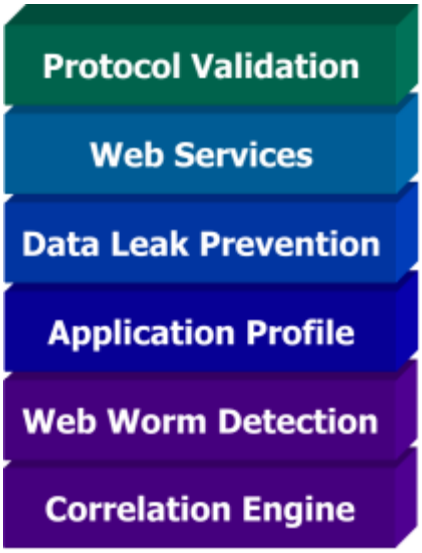


Рис. 2. Модель захисту, яка реалізується SecureSphere WAF [5]

Модель захисту, яка реалізується SecureSphere WAF, показано на рисунку 2, містить наступні рівні захисту [5]:

перевірка протоколу – фільтрує порушення протоколу HTTP та атаки, які використовують переваги протоколу HTTP. Наприклад, спроба зробити переповнення буфера за допомогою аномально великого заголовка HTTP-запиту;

сигнатури атак – ідентифікує відомі додатки, платформи та мережеві атаки. SecureSphere має базу даних із понад 6500 сигнатурами, яка регулярно оновлюється експертами Центру захисту додатків;

запобігання витоку даних – виявляє конфіденційні дані, такі як дані кредитних карток або особисту інформацію, коли вони виходять із веб-сайту. Часто це законно, але іноді це означає витік даних. SecureSphere може спостерігати, як конфіденційні дані виходять із додптка, а адміністратори можуть переконатися, що ці дані використовуються законно;

профіль додатка – SecureSphere порівнює фактичне використання додатка з очікуваним використанням у моделі, щоб визначити підозрілі випадки або підозрілу поведінку користувача;

виявлення веб-хробаків – SecureSphere використовує розширені алгоритми для зупинки атак веб-додатків Zero-day;

кореляційний механізм – кореляція подій і автоматизована базова лінія забезпечують SecureSphere WAF потужною вертикальною інтеграцією та аналізом даних за допомогою механізму перевірки кореляційних атак.

Отже, WAF мають вирішальне значення для безпеки онлайн-бізнесу. Вони захищають конфіденційні дані, запобігають витоку та впровадженню шкідливого

коду на сервер і відповідають вимогам, таким як Стандарт безпеки даних платіжних карток (PCI DSS). Оскільки організації все більше використовують веб-додатки та пристрої IoT, зловмисники намагаються націлитися на їхні вразливості. Інтеграція WAF з іншими інструментами безпеки має створювати надійну стратегію захисту інформаційних ресурсів організацій.

Перелік посилань:

1. 2024 Imperva Bad Bot Report. URL: https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/ (дата звернення: 30.09.2024).
2. Kinza Yasar. Web application firewall (WAF). TechTarget. URL: https://www.techtarget.com/searchsecurity/definition/Web-application-firewall-WAF (дата звернення: 30.09.2024).
3. What is a WAF? Cisco. URL: https://www.cisco.com/site/us/en/learn/topics/security/what-is-web-application-firewall-waf.html (дата звернення: 30.09.2024).
4. What Is WAF. Imperva. URL: https://www.imperva.com/learn/application-security/what-is-web-application-firewall-waf/ (дата звернення: 30.09.2024).
5. Web Application Firewall User Guide. Multi Layer Protection. URL: https://docs.imperva.com/bundle/v15.2-waf-user-guide/page/377.htm (дата звернення: 30.09.2024).

Сич Микола Валентинович
Старший викладач, ННІЗІ ДУІКТ, Київ, Україна

Захист Інтернет Речей (IoT) від Кіберзагроз

З розвитком технологій Інтернету Речей (IoT), з'являються нові можливості для підвищення ефективності як у побуті, так і в промисловості. Водночас збільшується кількість вразливостей і кіберзагроз, які можуть бути спрямовані на пристрої IoT. Захист IoT від кіберзагроз стає критично важливим завданням у сфері кібербезпеки.

Інтернет Речей (IoT) — це мережа фізичних пристроїв, транспортних засобів, будівель та інших об'єктів, які оснащені датчиками, програмним забезпеченням та іншими технологіями для обміну даними через інтернет. Кожен з цих об'єктів має унікальний ідентифікатор (ID) і здатен взаємодіяти з іншими пристроями без участі людини.

Проблеми безпеки IoT:

1. **Відсутність стандартів безпеки**: Багато IoT-пристроїв створюються без урахування належних заходів кібербезпеки, що призводить до вразливостей.
2. **Велика кількість підключених пристроїв**: Оскільки кількість IoT-пристроїв постійно зростає, кожен новий пристрій може стати точкою входу для хакерів.

3. **Низький рівень захищеності**: Більшість IoT-пристроїв мають обмежені можливості для обчислень і пам'яті, що ускладнює реалізацію ефективних захисних рішень.

Основні кіберзагрози для IoT:

1. **DDoS-атаки**: Зловмисники можуть використовувати скомпрометовані IoT-пристрої для організації атак на великі мережі або сервіси, як це сталося у випадку з атакою Mirai Botnet.
2. **Злом та підробка даних**: Недостатньо захищені пристрої IoT можуть бути зламані, що дозволить зловмисникам отримати контроль над ними або підробити важливі дані.
3. **Атаки на конфіденційність**: Пристрої, які збирають особисті або конфіденційні дані, можуть стати мішенню для хакерів, що призводить до порушення конфіденційності користувачів.

Методи захисту IoT:

1. **Аутентифікація та авторизація**:
   - Використання багатофакторної автентифікації для доступу до IoT-пристроїв може запобігти несанкціонованому доступу.
   - Впровадження механізмів авторизації для забезпечення того, що лише довірені користувачі можуть керувати пристроями.
2. **Шифрування даних**:
   - Використання шифрування для захисту даних, які передаються між IoT-пристроями та хмарними сервісами або іншими пристроями, допоможе запобігти перехопленню та модифікації інформації.
3. **Оновлення програмного забезпечення**:
   - Регулярні оновлення прошивки та програмного забезпечення IoT-пристроїв для виправлення вразливостей, виявлених після початку використання пристрою.
   - Автоматичне або напівавтоматичне оновлення дозволить підтримувати пристрої в актуальному стані без участі користувачів.
4. **Сегментація мережі**:
   - Розподіл IoT-пристроїв по окремих підмережах допоможе мінімізувати ризики поширення атак з одного скомпрометованого пристрою на інші.
5. **Моніторинг та виявлення аномалій**:
   - Встановлення систем для моніторингу трафіку IoT і виявлення підозрілих активностей, що можуть свідчити про атаку або злом.

Висновок

Захист пристроїв IoT від кіберзагроз є важливим завданням для забезпечення безпеки сучасного цифрового світу. Комплексний підхід, який включає шифрування, аутентифікацію, оновлення програмного забезпечення та моніторинг мережі, допоможе зменшити ризики кіберзагроз і підвищити рівень захисту для користувачів IoT.

Перелік посилань:

1. Cisco. What is the Internet of Things (IoT)? Cisco. URL: https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html (дата звернення: 15.10.2024).
2. IEEE. Internet of Things (IoT) - IEEE Internet of Things. IEEE. URL: https://iot.ieee.org/ (дата звернення: 15.10.2024).

Сідоров Ярослав Валерійович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

ЗАГРОЗИ В ОБЛАСТІ ЕЛЕКТРОННОЇ КОМЕРЦІЇ: ЗАХИСТ ДАНИХ СПОЖИВАЧІВ

Електронна комерція стала невід'ємною частиною нашого життя, забезпечуючи зручність покупок та доступ до глобального ринку. Однак разом із зростанням кількості онлайн-транзакцій збільшується і кількість кіберзагроз, що ставлять під удар особисті дані споживачів. Захист даних у сфері електронної комерції є ключовим завданням для компаній, які прагнуть зберегти довіру клієнтів і захистити себе від репутаційних та фінансових збитків.

Однією з основних загроз у сфері електронної комерції є крадіжка даних платіжних карток. Кіберзлочинці використовують різні методи, щоб отримати доступ до цієї інформації: від фішингових атак, що імітують справжні платіжні системи, до використання шкідливого програмного забезпечення, яке перехоплює дані під час транзакцій. Часто такі атаки націлені на незахищені або вразливі онлайн-магазини, які не використовують сучасні методи шифрування або багатофакторну автентифікацію.

Ще одна серйозна загроза — це атаки на особисті кабінети користувачів. Паролі, що використовуються на кількох платформах одночасно, значно підвищують ризик компрометації облікових записів. Зловмисники можуть використовувати методи грубої сили для зламу або застосовувати техніки соціальної інженерії, щоб виманити логіни та паролі у недосвідчених користувачів.

Серед інших поширених загроз є атаки типу "людина посередині" (MITM), коли зловмисники перехоплюють дані між користувачем і сервером, що може призвести до крадіжки фінансової інформації або зміни даних замовлень. Це часто трапляється на небезпечних Wi-Fi мережах, де шифрування є недостатнім або відсутнім взагалі.

Також важливо звертати увагу на загрози пов'язані з шахрайськими транзакціями. Злочинці використовують викрадені кредитні картки або підроблені платіжні дані для здійснення покупок в онлайн-магазинах. Це може не лише призвести до фінансових втрат для споживачів, але й негативно позначитися на репутації інтернет-магазину, який не зміг запобігти такому шахрайству.

Щоб захистити дані споживачів, інтернет-магазини повинні впроваджувати комплексні заходи безпеки. Перш за все, це використання SSL-сертифікатів для шифрування даних під час транзакцій, впровадження багатофакторної автентифікації для додаткового рівня захисту та регулярне оновлення систем безпеки. Крім того, важливим є забезпечення резервного копіювання даних і проведення регулярних аудитів безпеки для виявлення потенційних вразливостей.

Компанії також повинні проводити навчальні програми для своїх співробітників, щоб ті могли вчасно виявляти підозрілі активності та знати, як реагувати на потенційні загрози. Регулярні тренінги та симуляції кіберзагроз допоможуть значно зменшити ризик зломів через людський фактор.

Крім того, споживачі самі повинні бути обачними. Рекомендується використовувати унікальні паролі для кожної платформи, перевіряти легітимність вебсайтів перед введенням платіжних даних і уникати здійснення покупок через публічні мережі Wi-Fi без додаткових заходів безпеки, таких як VPN.

Отже, у світі електронної комерції захист даних споживачів є вирішальним фактором для забезпечення довіри та сталого розвитку бізнесу. Без належних заходів безпеки кіберзагрози можуть призвести до серйозних наслідків, включно з фінансовими втратами та втратою репутації компаній. Захист від цих загроз вимагає системного підходу, де залучені і компанії, і самі споживачі.

Перелік посилань:

1. КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ
2. URL: https://ippi.org.ua/sites/default/files/2024-2.pdf (date of access: 07.10.2024).
3. Сучасний стан економіки України: проблеми та перспективи розвитку. URL: https://dspace.kntu.kr.ua/server/api/core/bitstreams/6d742518-faf8-4970-998d-92e857ecca56/content (date of access: 05.10.2024).
4. Новий «захист прав споживачів»: e-commerce варто підготуватись. URL: https://mind.ua/openmind/20259926-novij-zahist-prav-spozhivachiv-e-commerce-varto-pidgotuvatis (date of access: 04.10.2024).

Скрицький Марк Єрвандович, БСДМ-61
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО СЕРВІСІВ ТА РЕСУРСІВ AMAZON WEB SERVICES

Визначено мету і основні завдання щодо управління доступом користувачів до хмарних сервісів та ресурсів. Розглянуто зміст технології управління доступом користувачів до сервісів та ресурсів Amazon Web Services.

Сьогодні організації все більше використовують необмежені можливості хмарних технологій для свого бізнесу та розміщують власні сервіси та інформаційні ресурси в хмарі. Однак ризики для безпеки, пов'язані з їх зростаючим використанням, є комплексними і не обмежуються лише організованою злочинністю. Неналежне управління ідентифікацією та доступом користувачів, неправильні конфігурації та ненавмисне розкриття хмарних даних працівниками також є одними з найбільших загроз.

У Звіті [1] зазначається, що в епоху, коли хмарні обчислення стали основою IT-інфраструктури, спеціалісти та організації з кібербезпеки стикаються із загрозами, що постійно змінюються. Ці виклики різноманітні й охоплюють усе: від захисту багатохмарних середовищ і забезпечення захисту даних до пом’якшення вразливостей хмари. Але вони також підкреслюють виражену прогалину в навичках у робочій силі з кібербезпеки. Зі збільшенням складності хмарних екосистем зростає потреба в передових, орієнтованих на хмару стратегіях і навичках кібербезпеки.

Оскільки компанії все більше використовують численні хмарні сервіси, проблема підтримки безпеки на різноманітних платформах стає гострішою. У 2024 році безпека багатохмарних середовищ залишається складним завданням, головним завданням якого є захист даних і конфіденційність, як відзначили 55% учасників опитування. Це незначне збільшення порівняно з 52%, спостережуваним у 2023 році, що свідчить про зростання обізнаності та занепокоєння щодо захисту інформації на різних хмарних платформах. Проблема володіння належними навичками для розгортання та керування рішеннями в усіх хмарних середовищах слідкує за нею, хоча спостерігається зниження з 58% у 2023 році до 51% у 2024 році.

AWS пропонує широкий спектр послуг, але деякі з них набули популярності завдяки своїй корисності та продуктивності [2]:

Amazon EC2 (Elastic Compute Cloud) забезпечує масштабовану обчислювальну потужність у хмарі. Це дозволяє користувачам запускати сервери та збільшувати чи зменшувати потужність залежно від їхніх вимог;

Amazon S3 (проста служба зберігання) пропонує масштабоване сховище

об’єктів для резервного копіювання даних, архівування та аналітики. Воно відоме своєю довговічністю, доступністю та масштабованістю;

AWS Lambda дозволяє користувачам запускати код без підготовки та керування серверами. Сервіс використовується для створення безсерверних програм і автоматизації завдань;

Amazon RDS (служба реляційної бази даних) полегшує налаштування, роботу та масштабування реляційної бази даних у хмарі. Вона забезпечує економічну ємність із змінним розміром;

Amazon CloudFront це служба швидкої мережі доставки вмісту (CDN), яка безпечно доставляє дані, відео, програми та API клієнтам у всьому світі з низькою затримкою;

AWS Identity and Access Management (IAM) має вирішальне значення для безпечного керування доступом до сервісів AWS. Він допомагає створювати користувачів і групи AWS і керувати ними, а також використовує дозволи, щоб дозволяти та забороняти їхній доступ до ресурсів AWS.

AWS IAM забезпечує точний контроль доступу у всіх сервісах AWS. За допомогою IAM ви можете вказати, хто може отримувати доступ до певних сервісів та ресурсів та за яких умов. Завдяки політикам IAM ви керуєте дозволами для співробітників та систем, надаючи дозволи з найменшими привілеями [3].

Загальний принцип роботи AWS IAM показано на рисунку 1. За допомогою IAM можна керувати дозволами AWS для співробітників та робочих навантажень. Для співробітників рекомендується використовувати AWS Single Sign-On (AWS SSO), щоб керувати доступом до облікових записів AWS та дозволами в межах облікових записів. З AWS SSO можна легко призначати ролі та політики IAM і керувати ними в масштабах всієї організації. Для робочих навантажень використовуються ролі та політики IAM та надаються лише необхідні дозволи.

Рис. 1. Загальний принцип роботи AWS IAM [3]

Модель контролю доступу на основі атрибутів (ABAC) – це стратегія авторизації, яка визначає дозволи на основі атрибутів. У AWS ці атрибути називаються тегами. Ми можемо прикріплювати теги до ресурсів IAM, зокрема до

сутностей IAM (користувачів або ролей), а також до ресурсів AWS. Ми можемо створити одну політику ABAC або невеликий набір політик для своїх керівників IAM. Ці політики ABAC можуть бути розроблені для того, щоб дозволити операції, коли тег принципала збігається з тегом ресурсу. ABAC корисний у середовищах, які швидко розвиваються, і допомагає у ситуаціях, коли управління політикою стає громіздким [3].

Рис. 2. Архітектура системи єдиного входу [4]

Єдиний вхід (SSO) – це рішення автентифікації, яке дозволяє користувачам входити в декілька програм і веб-сайтів за допомогою одноразової автентифікації користувача. Враховуючи те, що сьогодні користувачі часто отримують доступ до програм безпосередньо зі своїх браузерів, організації надають пріоритет стратегіям керування доступом, які покращують як безпеку, так і взаємодію з користувачем. SSO забезпечує обидва аспекти, оскільки користувачі можуть отримати доступ до всіх ресурсів, захищених паролем, без повторних входів після перевірки їхньої особи [4].

Отже, збільшення як дистанційної роботи, так і зовнішніх сховищ і послуг швидко розширило довіру організацій до хмари. Хмарні середовища стали цінними цілями для зловмисників. Оскільки організації продовжують переміщувати дані та послуги в ці середовища, зловмисники можуть скористатися перевагами загальнодоступних хмар доступу, які часто надають. В таких умовах, технологія керування ідентифікацією та доступом набуває вирішального значення для захисту хмарних ресурсів організацій від зловмисників.

Перелик посилань:

1. 2024 Cloud Security Report. Cybersecurity Insiders. URL: https://www.isc2.org/-/media/5C011B9E35624F309CB4D00EA1A22FED.ashx (дата звернення: 10.10.2024).
2. What is AWS? Complete Guide to Amazon Web Services. GoGeekz. URL: https://gogeekz.com/what-is-aws-complete-guide-to-amazon-web-services/ (дата звернення: 10.10.2024).
3. AWS Identity and Access Management. User Guide. 2024. URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/iam-ug.pdf (дата звернення: 10.10.2024).
4. What is SSO (Single-Sign-On)? AWS. URL: https://aws.amazon.com/what-is/sso/ (дата звернення: 10.10.2024).

Собчук Андрій Валентинович
доцент кафедри інформаційної та кібернетичної безпеки ННІЗІ ДУІКТ, Київ, Україна
Степанченко Богдан Сергійович
аспірант ННІЗІ ДУІКТ, Київ, Україна
Пихнівський Роман Олегович
аспірант кафедри інтегральних та диференціальних рівнянь,
Київський національний університет імені Тараса Шевченка, Київ, Україна

ІДЕНТИФІКАЦІЇ КІБЕРЗАГРОЗ З ВИКОРИСТАННЯМ ЕВОЛЮЦІЙНИХ МОДЕЛЕЙ

Еволюційні моделі нині використовують для виявлення аномалій в роботі систем виявлення кіберзагроз для прогнозування ймовірності та типу атаки, яка може статися, з метою оптимізації конфігурації систем кіберзахисту об’єктів критичної інфраструктури. Використання еволюційних математичних моделей може допомогти у прогнозуванні можливих наслідків атаки, розробці ефективних заходів захисту та якісно оцінити вплив атаки, що сприятиме прийняттю кращих рішень щодо кібербезпеки. Розроблено математичний апарат для ідентифікації кіберзагроз та визначення стратегій мінімізації ризиків несанкціонованого доступу зловмисників до інформаційних ресурсів мережі, що ґрунтується на методах якісної теорії систем дифереціальних рівнянь з імпульсною дією. Отримано конструктивні умови стійкості та асимптотичної стійкості SIR-моделі, яка є математичною моделлю вразливості мережі в наслідок агресивних дій зловмисників.

Стрімкий розвиток технологій характеризується постійним зростанням загроз несанкціонованого доступу до інформаційної інфраструктури. З кожним роком кількість кібератак зростає, а їх наслідки можуть бути катастрофічними [1]. Кіберзлочинці використовують різноманітні методи та технології, щоб отримати доступ до конфіденційної інформації, зламати системи управління та порушити роботу мережевої інфраструктури. Україна, особливо в період агресивної війни, є ключовою мішенню для кібератак як з боку злочинних державних утворень так і численних кримінальних груп.

Наслідки кібератак можуть бути дуже серйозними – від втрати конфіденційної інформації та порушення роботи компанії до руйнування критичної інфраструктури [2], фінансових збитків, загрози для життя і здоров’я людей та втрати функціональної стійкості [3] інформаційної інфраструктури підприємств. Тому дуже важливо захистити свої дані та

системи від кібератак. Першочерговим завданням для створення ефективної стратегії моделювання кібератак є аналіз ризиків. Це включає в себе оцінку потенційних цілей атак, типів атак, які можуть бути використані, та можливих наслідків атак.

Традиційні методи виявлення кіберзагроз базуються на тому, що аналізується мережевий трафік для виявлення підозрілої активності з широким використанням так званих систем виявлення вторгнень (IDS) та систем запобігання вторгненням (IPS) [4]. Водночас широко використовується аналіз журналів безпеки для виявлення ознак атаки та системи кореляції подій (SIEM). Аналіз аномалій передбачає виявлення аномалій у поведінці користувачів або систем [5].

На доповнення арсеналу традиційних методів все частіше застосовують еволюційні моделі. Еволюційні моделі можуть бути навчені на історичних даних для виявлення аномалій, які можуть свідчити про кібератаку, використані для прогнозування ймовірності та типу атаки, яка може статися, для оптимізації конфігурації систем кіберзахисту тощо. Математично еволюційні моделі досліджують застосовуючи апарат якісної теорії диференціальних рівнянь. Саме використання еволюційних математичних моделей допомогає у прогнозуванні можливих наслідків атаки, розробці ефективних заходів захисту та якісно оцінити вплив атаки, що сприятиме прийняттю кращих рішень щодо кібербезпеки.

Розроблено математичний апарат для ідентифікації кіберзагроз та визначення стратегій мінімізації ризиків несанкціонованого доступу зловмисників до інформаційних ресурсів мережі, що ґрунтується на методах якісної теорії систем дифереціальних рівнянь з імпульсною дією. Методами фазової площини, вивчаються особливості поведінка складних них систем, математичні моделі яких представлено системами диференціальних рівнянь з імпульсною.

Отримано конструктивні умови стійкості та асимптотичної стійкості SIR- моделі, яка є математичною моделлю вразливості мережі в наслідок агресивних дій зловмисників. Встановлено умови мінімізації уразливостей елементів мережі через реалізацію різних стратегій зменшення кількості уражених пристроїв. Встановлено, що загрозостійкість мережі обернено пропорційно визначається відношенням швидкості вразливості пристроїв у мережі до вибувших і відновлених пристроїв та отримано оцінку періоду оновлення програмного забезпечення для захисту від кіберзагроз.

Перелік посилань:

1. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. DOI: 10.15587/978-617-7319-31-2
2. V. Pichkur, O. Laptiev, I. Polovinkin, A. Barabash, A. Sobchuk and I. Salanda, "The Method of Managing Man-generated Risks of Critical Infrastructure Systems Based on Ellipsoidal Evaluation," *2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, 2022, pp. 133-137, doi: 10.1109/ATIT58178.2022.10024244.
3. Собчук А. В., Барабаш О. В., Мусієнко А. П. Методи оцінки функціонально стійкої безпровідної сенсорної мережі. Телекомунікаційні та інформаційні технології. 2019. – №3. – С. 46–54. DOI: 10.31673/2412-4338.2019.034654
4. Valentyn Sobchuk, Roman Pykhnivskyi, Oleg Barabash (2024) Sequential IDS for Zero-Trust Cyber Defence of IoT/IIoT Networks. // Advanced InformationSystems. 2024. Vol.8, No.3. p. 92-99. https://doi.org/10.20998/2522-9052.2024.3.11
5. O. Laptiev, A. Musienko, V. Nakonechnyi, A. Sobchuk, S. Gakhov and S. Kopytko, "Algorithm for Recognition of Network Traffic Anomalies Based on Artificial Intelligence," *2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Istanbul, Turkiye, 2023, pp. 1-5, doi: 10.1109/HORA58378.2023.10156702.

Сторожук Сергій Сергійович
Студент групи БСДМ-61 ННІЗІ ДУІКТ, Київ, Україна

НЕОБХІДНІСТЬ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ КОНТРОЛЮ ДОСТУПУ КОРПОРАТИВНОЇ МЕРЕЖІ

У сучасному світі інформаційні технології стають основою бізнес-процесів для забезпечення безпеки корпоративних мереж і мають критичне значення. Однією з ключових складових цієї безпеки є технологія контролю доступу, з використанням якої визначається хто і які ресурси може використовувати в межах мережі. В умовах зростаючих загроз кібербезпеки, необхідність впровадження ефективної системи контролю доступу стає не лише рекомендованою практикою, а й обов'язковою умовою.

Контроль доступу до корпоративної мережі є однією з ключових у сфері кібербезпеки. У сучасному світі, де компанії все більше залежать від інформаційних систем та цифрових даних, безпека інформації стає стратегічним питанням для будь-якої організації. Технології контролю доступу до корпоративної мережі відіграють критичну роль у захисті даних, мінімізації ризиків витоку інформації та запобіганні несанкціонованого доступу до конфіденційних ресурсів. Дане дослідження розглядає необхідність застосування технологій контролю доступу до корпоративної мережі та їх важливість для забезпечення безпеки інформації в сучасному бізнесі.

Рис.1. Складові технології контролю доступу

На рис. 1 показано складові, які повинні бути враховані при організації досту до мережі. Контроль доступу до корпоративної мережі включає в себе наступні заходи:

1. Захист від несанкціонованого доступу

Одним із головних завдань технологій контролю доступу є запобігання несанкціонованому доступу до ресурсів корпоративної мережі. Незалежно від розміру організації, всі компанії стикаються з ризиком того, що зловмисники або внутрішні співробітники можуть отримати доступ до конфіденційної інформації. Це може призвести до витоку критично важливих даних, таких як комерційні таємниці, персональні дані клієнтів або фінансова інформація.

Технології контролю доступу дозволяють обмежити доступ до певних ресурсів, грунтуючись на ідентифікації та автентифікації користувачів. Вони визначають, хто має право отримати доступ до певних систем і ресурсів, встановлюючи правила для входу в мережу. Завдяки цьому організації можуть забезпечити, що тільки авторизовані особи мають доступ до чутливої інформації.

2. Моніторинг доступу

Ще одна важлива функція технологій контролю доступу – це можливість проведення аудиту та моніторингу всіх спроб входу до мережі. Такий моніторинг дозволяє виявляти підозрілі дії та швидко реагувати на загрози, що можуть виникнути. Наприклад, якщо зафіксовано декілька невдалих спроб входу, це може свідчити про спробу атаки. Системи контролю доступу фіксують кожен випадок автентифікації, надаючи адміністраторам можливість перевірити активність користувачів.

3. Розмежування доступу

Застосування технологій контролю доступу дозволяє ефективно розмежувати доступ різних користувачів до інформаційних ресурсів компанії. Не кожен співробітник повинен мати доступ до всієї інформації організації. Технології контролю доступу дозволяють налаштувати права доступу таким чином, щоб кожен користувач мав доступ лише до тих ресурсів, які необхідні йому для виконання його завдань в корпоративній мережі. Це знижує ризик несанкціонованого використання конфіденційних даних, особливо в великих організаціях, де працює багато співробітників із різними ролями та повноваженнями.

4. Захист від внутрішніх загроз

Внутрішні загрози є однією з найбільш небезпечних категорій ризиків для будь-якої організації. Співробітники можуть використовувати свої повноваження для отримання доступу до чутливих даних з корисливих мотивів або через недбалість. Технології контролю доступу дозволяють мінімізувати ці ризики, забезпечуючи чітке розмежування прав доступу та впровадження багаторівневого захисту. Тобто застосування IAM або PAM.

5. Впровадження багатофакторної автентифікації

Сучасні системи контролю доступу також часто використовують багатофакторну автентифікацію (MFA), що значно підвищує рівень безпеки. Багатофакторна автентифікація поєднує кілька елементів для підтвердження особи користувача, таких як пароль, одноразовий код на мобільному телефоні або біометричні дані. Це дозволяє захистити мережу навіть у випадках, коли один із факторів (наприклад, пароль) був скомпрометований.

6. Підтримка мобільних пристроїв та віддалених користувачів

З розвитком мобільних технологій та віддаленої роботи, контроль доступу до корпоративної мережі стає ще більш важливим. Сьогодні багато співробітників працюють віддалено або використовують особисті пристрої для доступу до корпоративної мережі. Це створює нові виклики для безпеки, оскільки мобільні пристрої можуть бути вразливими до атак або втрачатися.

Отже, технологія контролю доступу є критично важливою для забезпечення безпеки корпоративних мереж. В умовах сучасних загроз і вимог до конфіденційності даних підприємства повинні приймати активні заходи для впровадження ефективних систем контролю доступу. Це не лише дозволить захистити важливу інформацію, але й забезпечити стабільність та безперервність бізнес-процесів у довгостроковій перспективі. В остаточному підсумку інвестиції в технологію контролю доступу є інвестиціями у безпеку, надійність і репутацію компанії.

Перелік посилань:

1. Контроль доступу до мережі URL: https://www.arubanetworks.com/faq/what-is-network-access-control/ (дата звернення: 26.09.2023).
2. Identity Services Engine URL: 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: 28.09.2023).
3. Архітектура ISE URL: https://smbitsolutions.wordpress.com/2012/07/12/cisco-identity-services-engine/ (дата звернення: 01.10.2023).
4. Доступ до певних сегментів мережі URL: https://www.routexp.com/2020/03/cisco-ise-cisco-identity-services-engine.html
5. http://blog.51sec.org/2019/12/ise-studying-notes.html (дата звернення: 30.09.2023).

Табула Нікіта Юрійович
студент групи БСД-14, ДУІКТ, Київ, Україна.

БЛОКЧЕЙН ТА ЗАХИСТ ДАНИХ

Блокчейн стає все більш популярною технологією для забезпечення захисту даних у різних галузях. Його унікальні властивості, такі як децентралізація, прозорість та незмінність інформації, роблять його ідеальним інструментом для боротьби з кібератаками та забезпечення конфіденційності. Це робить блокчейн надійним інструментом для забезпечення захисту в фінансових системах, охороні здоров'я та державному управлінні.

Основною перевагою блокчейну є децентралізація. У традиційних системах дані зазвичай зберігаються в одному центрі, що робить систему вразливою до атак. Наприклад, зламавши центральний сервер, зловмисники можуть отримати доступ до всіх даних. У блокчейні дані розподіляються між багатьма вузлами (комп'ютерами) мережі. Це означає, що для того, щоб отримати доступ до інформації або змінити її, зловмисникам доведеться зламати більшість вузлів одночасно, що практично неможливо на практиці.
Блокчейн гарантує, що після запису дані не можуть бути змінені або видалені без сповіщення всіх учасників системи. Це особливо важливо в контексті захисту чутливих або юридично значимих даних, таких як фінансові транзакції або медичні записи. У разі будь-якої спроби змінити запис у

блокчейні вся мережа буде негайно повідомлена, що запобігає маніпуляціям з інформацією.

Блокчейн є перспективним рішенням для підвищення безпеки мобільних пристроїв у бізнес-середовищі. Його використання дозволяє мінімізувати ризики, пов'язані з несанкціонованим доступом до даних і фішинговими атаками, що є важливим кроком у забезпеченні конфіденційності інформації.

Перелік посилань:

1. Захист даних на смартфонах: виклики та рішення. URL: https://cybersecurity.ua/smartphones (дата звернення: 21.10.2024).
2. Blockchain and Mobile Security. URL: https://securityinblockchain.org (дата звернення: 18.10.2024).

Терно Ярослав Анатолійович
студентка групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ РІШЕННЯ TREND VISION ONE

У сучасних умовах цифрової трансформації, коли кількість кіберзагроз постійно зростає, організації стикаються з необхідністю вдосконалення своїх підходів до захисту інформації. Традиційні системи безпеки, засновані на реактивних методах, більше не здатні повною мірою забезпечувати належний рівень захисту. Нові загрози, такі як атаки "нульового дня", складні цільові атаки (APT), фішинг, зловмисне програмне забезпечення та атаки на хмарні сервіси, потребують більш інтелектуальних і проактивних рішень.

Одна з багатьох перспективних технологій у боротьбі з цими викликами — це Extended Detection and Response (XDR), яка інтегрує дані з різних джерел для забезпечення розширеного виявлення загроз та швидкого реагування на них. Однією з передових платформ у цій сфері є Trend Vision One,

Архітектура захисту на основі XDR (Extended Detection and Response) у контексті управління ризиками поверхні атаки. Платформа включає захист електронної пошти, кінцевих точок, хмарної інфраструктури, мереж, даних та ідентифікацій, з інтеграцією інтелекту загроз і автоматизації процесів в рамках Zero Trust Architecture [1, 1].

Рис.1. Архітектура захисту на основі XDR (Extended Detection and Response)

Один із ключових принципів цього рішення — це **Zero Trust Architecture**, яка ґрунтується на ідеї постійного підтвердження довіри кожному учаснику процесу доступу. Це дозволяє запобігти несанкціонованому доступу та зловживанням, навіть якщо загроза знаходиться всередині корпоративної мережі.

Завдяки інтеграції **штучного інтелекту (AI)** платформа Trend Vision One дозволяє підприємствам отримати глибшу прозорість подій та активів у своїй IT-інфраструктурі, забезпечуючи раннє виявлення загроз та швидке реагування на інциденти. Основні переваги включають:

- *Межурівнева підтримка гібридного середовища:* Trend Vision One захищає кожен рівень різноманітної IT-інфраструктури організації**,** включаючи кінцеві точки, сервери, електронну пошту, хмарні сервіси, мережі, 5G та OT (операційні технології). Унікальна перевага Trend полягає в тому, що він може використовувати широту та глибину своїх можливостей у галузі хмарної безпеки, мережевої безпеки, електронної пошти та безпеки кінцевих точок прямо на платформі. Платформа також підтримує гібридні середовища; надання організаціям можливості захищати свої активи у всіх середовищах — хмарних, гібридних чи локальних — без шкоди для безпеки чи можливості розширення до XDR.

- *Інтеграція зі сторонніми екосистемами:* Протягом останнього року Trend Vision One потроїла свою інтеграційну екосистему зі сторонніми та партнерськими мережами. Зусилля з інтеграції, що вживаються спільнотою, дозволяють підприємствам використовувати інтеграцію для просування організацій із забезпечення безпеки за рахунок консолідованої видимості та аналізу, а також спрощеної автоматизації

та оркестрації робочих процесів.

- *Global Threat Intelligence:* в основі платформи лежить провідна глобальна аналітика загроз компанії. З 16 дослідницькими центрами у всьому світі; сотні дослідників погроз; та Trend Micro™ Zero Day Initiative™ – програма винагороди за виявлення помилок номер один у світі – глобальна та локальна інформація поповнює платформу, щоб допомогти клієнтам залишатися на крок попереду зловмисників. Інтелектуальні дані про тенденції розкривають інформацію про глибокі порушення безпеки та вразливості завдяки аналізу загроз у режимі реального часу, профілюванню суб'єктів загроз та наскрізному моніторингу кампаній для швидкого розуміння та припинення спроб атак [3, 3].

- *Керовані послуги з виявлення та реагування (MDR):* Trend Vision One доповнює внутрішні ресурси організацій, надаючи комплексні послуги з пошуку загроз, реагування на інциденти та цілодобовий моніторинг. Це дозволяє ефективно протидіяти атакам і швидко нейтралізувати їх вплив.

Таким чином, **Trend Vision One** з використанням AI надає організаціям інструменти для комплексного підходу до захисту активів і управління кібер ризиками. Завдяки інтелектуальному аналізу загроз та автоматизації процесів, платформа дозволяє підприємствам залишатися захищеними від складних та динамічних загроз, зберігаючи при цьому гнучкість і масштабованість їхньої безпеки.

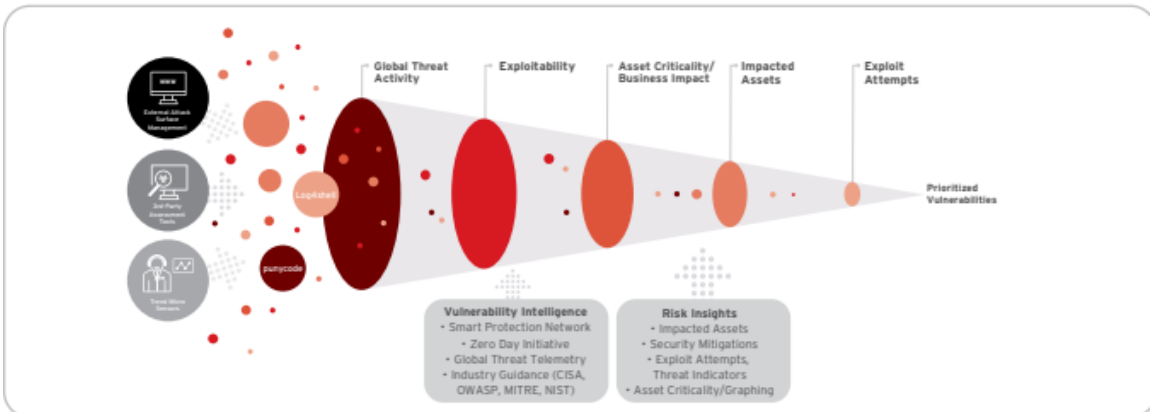


Рис.2. Схема процесу оцінки та пріоритизації вразливостей в інформаційній системи.

Це схема процесу оцінки та пріоритизації вразливостей в інформаційній системі, яка базується на поєднанні **глобальної активності загроз** та **інформації про вразливості**. Схема демонструє, як загрози проходять через декілька етапів аналізу та оцінки до того, як вразливості стають пріоритетними для виправлення.

1. *Глобальна активність загроз (Global Threat Activity):* Інформація про глобальну активність кіберзагроз потрапляє в процес аналізу. Це включає дані з різних джерел, таких як **Smart Protection Network**, **Zero Day Initiative**, **глобальна телеметрія загроз**, а також індустріальні рекомендації (OWASP, NIST, CISA).
2. *Оцінка експлуатованості (Exploitability):* На цьому етапі система оцінює, наскільки вразливість може бути використана кіберзловмисниками.
3. *Оцінка критичності активів (Asset Criticality/Business Impact):* Далі відбувається аналіз впливу вразливості на критичні активи організації, що визначає, які активи піддаються ризику.
4. *Вражені активи (Impacted Assets):* Цей етап визначає, які саме активи в організації можуть постраждати від конкретних вразливостей.
5. *Спроби експлуатації (Exploit Attempts):* Завершальний етап оцінює, чи відбулися спроби експлуатації вразливостей. На основі цієї інформації формується список пріоритетних вразливостей для виправлення [2, 2].

Схема також містить блоки **Risk Insights** (інсайти ризиків), які включають в себе дані про вражені активи, заходи безпеки, спроби експлуатації та атрибути загроз.

Таким чином, завдяки комплексному підходу, що поєднує інтелектуальні технології, автоматизацію і глобальну обізнаність про загрози, платформа **Trend Vision One** забезпечує надійний захист організацій у світі складних кіберризиків, дозволяючи їм бути на крок попереду зловмисників.

Перелік посилань:

1. Trend Vision One URL: https://trendmicro.com/en_us/business.html.
2. Solution Brochure Trend Vision One™ URL: www.trendmicro.com/en_us/business/products/one-platform.html?modal=s8a-btn-read-soln-brief-38e459 (дата звернення: 26.09.2023).
3. Trend Micro запускає Trend Vision One з Next-Gen XDR та AI Capabilities URL: https://itpro.ua/post/trend_micro_zapuskaie_trend_vision_one_z_next_gen_xdr_ta_ai_capabilities/ (дата звернення: 18.06.2023).

Тимофєєв Артем Вікторович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

МЕНЕДЖМЕНТ ІФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека є однією із важливих складових глобальної безпеки, невід'ємною умовою глобалізації та одним із факторів впливу глобальних процесів на всі сфери діяльності. Дедалі більше посилюється роль інформаційної безпеки у процесі глобалізації і, навпаки, вплив глобальних процесів на інформаційну безпеку та взаємопов'язану з нею економічну, національну та глобальну безпеку в умовах побудови інформаційного суспільства – нового ступеня розвитку людства.

Особливості необмеженого і неконтрольованого впливу, несанкціонованого доступу, а також виникнення комп'ютерних вірусів та інших загроз, викликають необхідність у забезпеченні інформаційної безпеки, яка є головною частиною економічної безпеки держави та національної безпеки в цілому. Життєдіяльність суспільства, його інформаційна безпека залежить від стабільного функціонування, живучості, надійності та готовності інформаційно-телекомунікаційних мереж. Завдяки стрімкому технологічному прогресу постає низка життєво важливих питань щодо організації процесів оброблення, зберігання, поширення та захисту інформації в глобальних інформаційно-комунікаційних системах. Бо саме інформаційні технології та розвинена інфраструктура телекомунікацій відіграють сьогодні вирішальну роль у забезпеченні зростання продуктивності виробництва, адміністративного і господарського управління, у розширенні 3 інформаційної взаємодії між людьми, поширенні масової інформації, процесі інтелектуалізації суспільства. Інформаційна безпека має важливе значення для того, щоб інформаційні технології могли відповідати очікуванням ділового світу, споживачів і урядів та щоб дійсно надавали всі ті потенційні вигоди, що їх забезпечують інформаційно-комунікаційні технології. Складовими частинами глобальної безпеки є: національна, економічна, політична, інформаційна, технічна, фізична, соціальна, військова, екологічна, ресурсна, продовольча, енергетична, фінансово-грошова, цінова, демографічна, пожежна, медична, психологічна, психічна, кримінальна безпеки.

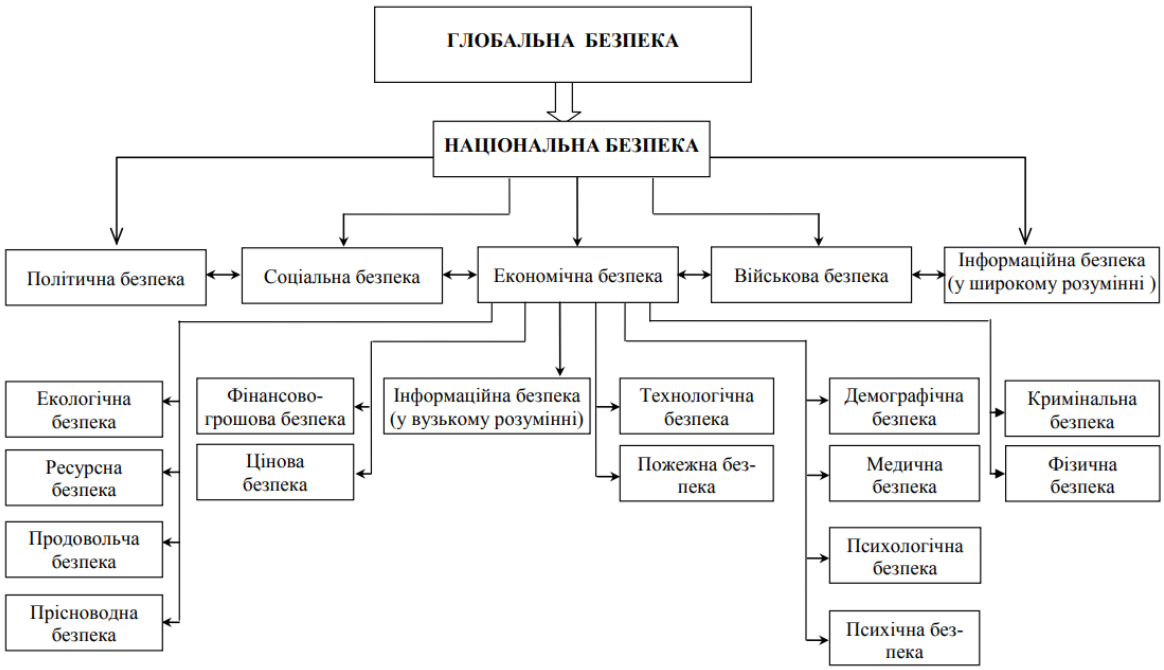


Рис. 1 – Складові глобальної системи

Таким чином робим висновки. Становлення суспільства нового типу дуже гостро ставить питання інформаційної безпеки простору держави, людини, суспільства, а також створення ефективної системи забезпечення прав громадян і соціальних інститутів на вільне одержання, поширення і

використання інформації. Це питання неможливо обійти, тим більше, що воно стає дуже актуальним зараз і для нашої країни.

Перелік посилань
1. Якименко І.З. Менеджмент інформаційної безпеки. Тернопіль : КЛ, 2019. 136с. URL: http://dspace.wunu.edu.ua/bitstream/316497/36025/1/%D0%9C%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82_I%D0%91_%D0%AF%D0%BA%D0%B8%D0%BC%D0%B5%D0%BD%D0%BA%D0%BE_%D0%BB%D0%B5%D0%BA%D1%86ii.pdf (дата звернення: 10.10.2024)

Тищенко Вадим Олексійович, БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНИХ API НА БАЗІ IMPERVA API SECURITY

Визначено мету і основні завдання щодо захисту корпоративних API. Розглянуто зміст технології захисту корпоративних API на прикладі Imperva API Security.

Інтерфейси прикладного програмування (Application Programming Interface, API) служать протоколом зв’язку між різними програмними компонентами. API стали основою для розробки сучасного програмного забезпечення, дозволяючи різним додаткам і організаціям взаємодіяти й обмінюватися даними.

Однак ця підвищена залежність від API також відкрила нові шляхи для кібератак. Атаки API – це тип кіберзагроз, коли зловмисник використовує вразливі місця в API, щоб завдати шкоди системі. Зловмисник може отримати несанкціонований доступ, маніпулювати даними або навіть скомпрометувати основний сервер. Ці атаки можуть бути серйозними та завдати шкоди, оскільки API часто мають доступ до конфіденційних даних і критичних системних функцій [1].

Атаки API становлять загрозу не лише безпеці системи, але й конфіденційності інформації її користувачів. Вони можуть призвести до розголошення або крадіжки особистих даних, а також до фінансових втрат. Оскільки все більше і більше додатків використовують API для різноманітних функцій, розуміння та пом’якшення атак API стало нагальною необхідністю в ландшафті кібербезпеки.

Кількість корпоративних API зростає в геометричній прогресії завдяки проектам цифрової трансформації, створюючи новітню поверхню для атак, яку команди безпеки намагаються контролювати. В таких умовах необхідно запобігати витоку даних і зловживанням API за допомогою комплексного виявлення API всіх кінцевих точок і класифікації конфіденційних даних. На рисунку 1 показано API як основну точку входу для зловмисників, які прагнуть

отримати доступ до цінних даних організації [2].

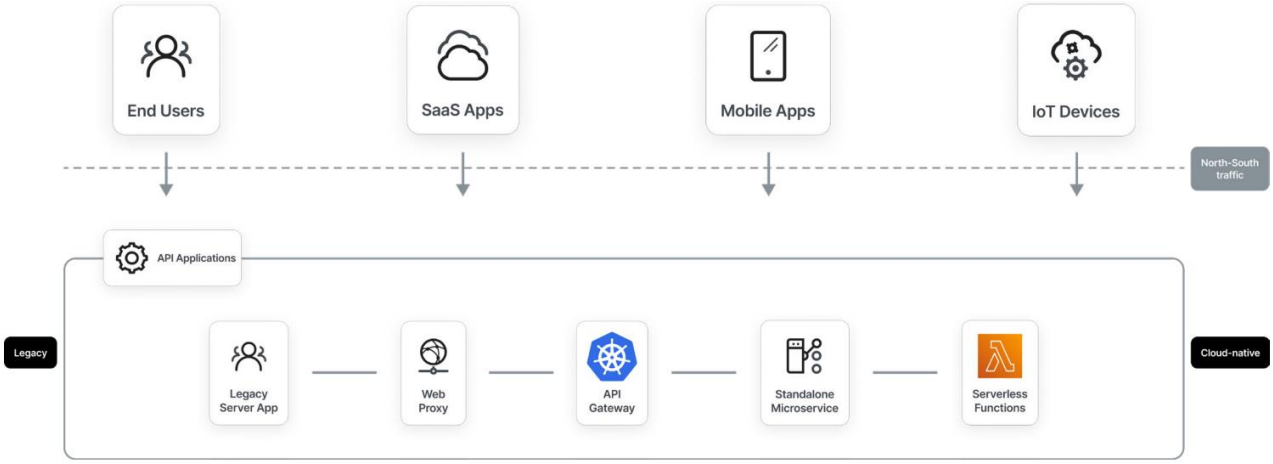


Рис. 1. API як основна точка входу для зловмисників [2]

Imperva [3] пропонує комплексний підхід до захисту критично важливих додатків і API у режимі реального часу за допомогою платформи WAAP (Web Application and API Protection) (рисунок 2). Крім того, для клієнтів, які перебувають поза межею, Imperva пропонує рішення для виявлення корпоративних API у центрі обробки даних і захисту у режимі реального часу за допомогою шлюзу WAF. Цей підхід полегшує завдання безпеки API для клієнтів, а також прискорює їхній час для досягнення своїх цілей.

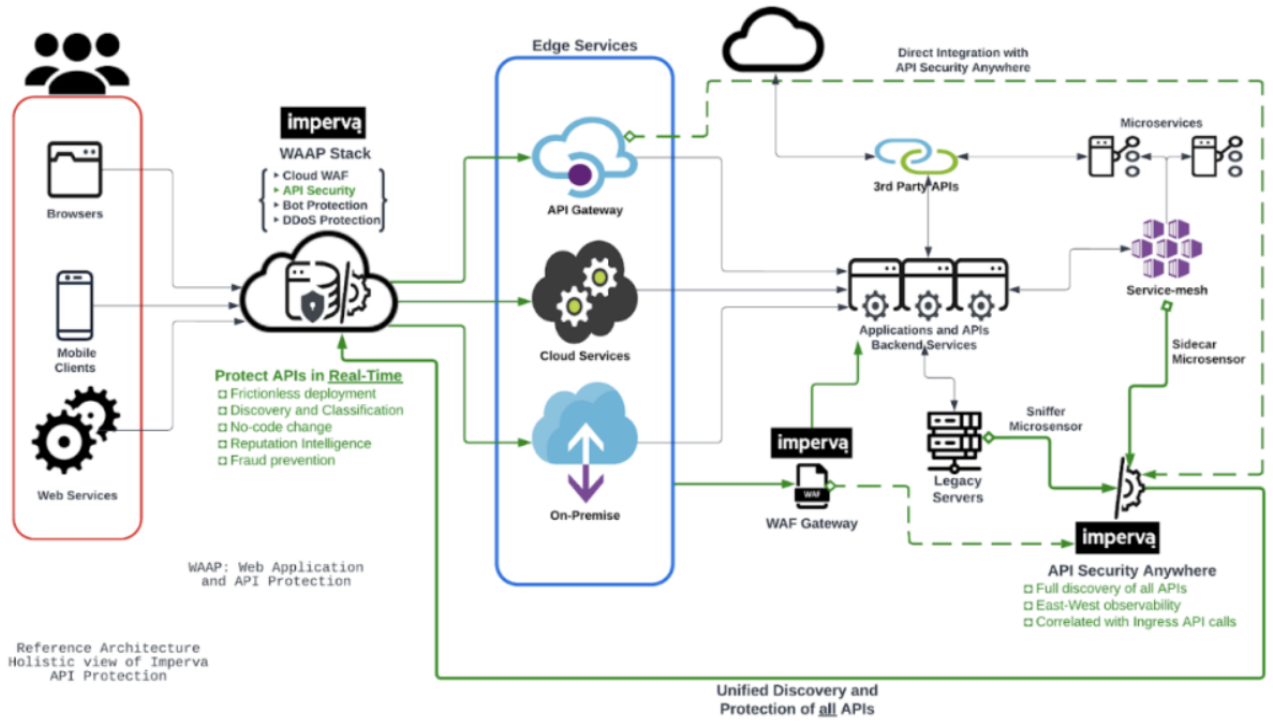


Рис. 2. Архітектура платформи WAAP [3]

Рішення Imperva API Security забезпечує безперервний захист усіх API за допомогою глибокого виявлення та класифікації для виявлення всіх загальнодоступних, приватних і тіньових API. Воно також захищає від атак на

бізнес-логіку та багатьох інших загроз OWASP API. Це просте в розгортанні рішення дає змогу командам безпеки впроваджувати позитивну модель безпеки API.

Imperva API Security забезпечує повну видимість API, автоматично виявляючи кінцеві точки API та оцінюючи ризики. Він класифікує конфіденційні API, використовуючи дані про виклики, які відображаються в зручному для користувача інтерфейсі, уможливлюючи проактивні заходи безпеки для захисту API під загрозою. Команди безпеки можуть застосовувати політики на основі оцінки ризиків, не сповільнюючи розвиток системи. Постійний моніторинг забезпечує своєчасне реагування на зміни, сприяючи швидшому безпечному випуску програмного забезпечення.

Imperva API Security пропонує різноманітні варіанти розгортання для задоволення різноманітних операційних потреб, доступні як доповнення до корпоративного Cloud WAF або як частина пропозиції API Security Anywhere. Imperva API Security Anywhere можна розгортати в різних середовищах, включаючи інші хмарні платформи, локальні або гібридні налаштування, і доступний у двох варіантах керування: з хмарним керуванням або з автономним керуванням [2].

Imperva API Security пропонує гнучкі варіанти розгортання для ефективного керування API та безпеки, зокрема [2]:

інтеграція з провідними шлюзами API, такими як Kong, Mulesoft, Azure APIM Gateway і Apigee, для спрощеного розгортання та керування;

інтеграція в архітектуру мікросервісів;

доступність як датчик безпеки для перевірки API у середовищах Kubernetes;

доступність як автономний сніфер мережі;

інтеграція з проксі, такими як F5.

Отже, за своєю природою API розкривають критично важливу бізнес-логіку та конфіденційну інформацію, таку як дані користувача, облікові дані автентифікації та фінансові транзакції, і все частіше стають мішенню для зловмисників. API можуть стати точками входу для зловмисників, які прагнуть використати вразливі місця чи слабкі місця або викрити базову інфраструктуру та ресурси підприємства. Тому надійні заходи безпеки API необхідні для захисту даних від несанкціонованого доступу, маніпуляцій або викриття, щоб забезпечити їх конфіденційність і зберегти довіру користувачів і зацікавлених сторін, а також забезпечити конфіденційність, цілісність і доступність API.

Перелік посилань*:*

1. Ofer Hakimi. API Attacks: 6 Common Attacks and How to Prevent Them. Pynt. August 14, 2024. URL: https://www.pynt.io/learning-hub/api-security-guide/api-attacks (дата звернення: 30.09.2024).

2. Imperva API Security. Imperva. Datasheet. URL: https://www.imperva.com/resources/datasheets/Imperva-API-Security-DS_V5.pdf (дата звернення: 30.09.2024).

3. Luke Babarinde. Gain Control of Rapidly Securing Your Critical APIs Without Worrying About Your Backend Stack. Imperva, Oct 19, 2022. https://www.imperva.com/blog/gain-control-of-rapidly-securing-your-critical-apis-without-worrying-about-your-backend-stack/ (дата звернення: 30.09.2024).

Туренко Т.С.

студентка курсу БСД-13 факультету Навчально-науковий інститут захисту інформації

Державного університету інформаційно-комунікаційних технологій

Атака типу «людина посередині

У світі кібербезпеки атаки типу «людина посередині» (MITM) становлять серйозну загрозу, адже злочинці можуть безперешкодно перехоплювати вашу інформацію. Цей текст розкриває, як саме працюють такі атаки, які методи використовують зловмисники, і як ви можете захистити свої дані. Дізнайтеся про ефективні стратегії безпеки, щоб уникнути небезпечних пасток і забезпечити захист своєї особистої інформації. Ваша безпека в ваших руках — залишайтеся обережними та інформованими!

Кіберзлочинність сьогодні набуває різноманітних форм, проте одна з найдавніших і найнебезпечніших — це атака типу Man-In-The-Middle (MITM). Дослівно, це означає «людина посередині» і вказує на ситуацію, коли зловмисник перехоплює комунікацію між двома сторонами, видаючи себе за одного з учасників. Цей вид кіберзлочину є не лише поширеним, але й здатним завдати значної шкоди.

Уявіть, що ви на корпоративі, де обговорюють важливі питання бізнесу. Раптом один із колег, замість того, щоб залишити дискусію в серйозному руслі, починає розповідати кумедні анекдоти про свою домашню кішку, намагаючись викликати сміх у присутніх. Його спроба розрядити атмосферу перетворюється на щось кумедне, але також і досить не доречне. Хоча він мав добрі наміри, його "атака" в центрі важливої бесіди відволікає всіх від справи і викликає легке здивування.

Цей приклад показує, як атака типу «людина посередині» може з’являтися в повсякденному житті. У кібербезпеці атака типу man-in-the-middle (MITM), що буквально означає «людина посередині» – це тип кібератаки, при якому зловмисники перехоплюють розмову або передачу даних шляхом підслуховування, або прикидаючись його легальним учасником. Жертві здаватиметься, що відбувається стандартний обмін інформацією, але, вставивши себе в «середину» схеми забезпечення розмови чи передачі, зловмисник може непомітно перехопити інформацію.

Метою атаки MITM є перехоплення чутливих даних, таких як банківські рахунки, номери карток або логіни, для подальших злочинів, як-от крадіжка особистих даних чи шахрайські транзакції. Через те, що атаки проводяться в реальному часі, їх важко виявити до моменту завдання шкоди. Зловмисники можуть миттєво використовувати отримані дані, що робить наслідки особливо небезпечними.

Зловмисник не обов’язково повинен мати доступ комп’ютера , фізично чи віддалено. Він або вона можуть просто сидіти в тій самій мережі, що і Ви, і тихо перебирати дані. MITM може навіть створити свою власну мережу і обманом спонукати Вас використовувати її.

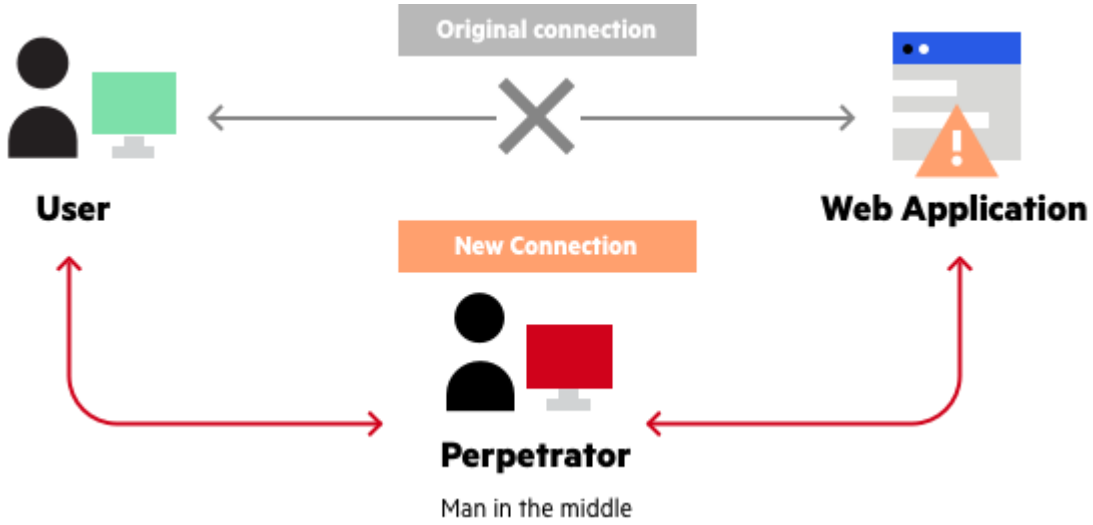


Рис.1(атака типу «людина посередині)

Успішна атака MITM включає дві конкретні фази: перехоплення і дешифрація:
1. Перехоплення: На цьому етапі зловмисник впроваджується між двома сторонами, які обмінюються даними, зазвичай шляхом створення фальшивої точки доступу (наприклад, підробленої Wi-Fi мережі) або перенаправлення трафіку через свій пристрій. Учасники комунікації не підозрюють, що їхні повідомлення перехоплюються і не надходять безпосередньо до одержувача.
2. Дешифрація: Багато сервісів шифрують дані для захисту (HTTPS – ваш надійний захист). Але хакери є винахідливими: вони можуть встановити підроблені сертифікати безпеки, і ви будете вважати, що ваші дані захищені, тоді як вони читають усе, як розгорнуту книгу. У результаті ваші паролі, номери кредитних карток і особисті повідомлення опиняються в їхніх руках.
Ці два етапи разом дають злочинцю повний контроль над передачею даних, що дозволяє їм отримати доступ до чутливої інформації або змінювати її для подальших атак.

Трюки, які використовують хакери:

- Фальшивий Wi-Fi: найпопулярніший трюк. Якщо ви підключаєтесь до публічної мережі, переконайтесь, що це не "підробка".

  (Зловмисники можуть створити підроблені Wi-Fi точки доступу з правдоподібними назвами, щоб обманути користувачів і змусити їх підключитися до них. Після підключення зловмисники можуть відстежувати і збирати дані користувачів, включаючи історію перегляду, облікові дані для входу та особисту інформацію.)

- Підроблені сертифікати: хакери можуть створити сертифікати безпеки, які виглядають як справжні, але насправді вони перенаправляють ваші дані до них.
- Переадресація DNS: зловмисники можуть перенаправляти вас з легітимних сайтів на свої клони, що дозволяє їм отримувати ваші дані.

Як захиститися від атаки "людина посередині" (MITM):
1. Використовуйте VPN: Шифрує весь інтернет-трафік, роблячи його недоступним для хакерів навіть у публічних мережах.
2. Перевіряйте "https://" та сертифікати: Завжди переконуйтесь, що сайт використовує захищене з'єднання (HTTPS), особливо при введенні конфіденційних даних.
3.Уникайте публічних Wi-Fi: Не використовуйте публічні мережі для проведення фінансових або особистих операцій.
4. Вимикайте автоматичне підключення до Wi-Fi: Уникайте випадкових підключень до незнайомих мереж, які можуть бути фальшивими.
5. Використовуйте двофакторну аутентифікацію (2FA): Додатковий захист облікових записів навіть при викраденні паролів.
6.Оновлюйте програмне забезпечення: Регулярні оновлення закривають вразливості, які хакери можуть використовувати для MITM-атак.7. Сильні паролі та менеджери паролів: Використовуйте унікальні складні паролі для кожного облікового запису, зберігаючи їх у менеджері.8. Будьте уважні до підозрілих з'єднань: Перевіряйте повідомлення, що вимагають введення даних або підтвердження платежів через нові сайти.
9.DNS через HTTPS (DoH): Захищає ваші запити до DNS-серверів від перехоплення та маніпуляцій.
10. Фізичний захист пристроїв: Не залишайте свої пристрої без нагляду, щоб уникнути встановлення шкідливих програм для MITM.
Висновок:
Атака "людина посередині" (MITM) — це серйозна загроза в світі кібербезпеки, де хакери можуть перехоплювати ваші дані. Це як якщо б хтось підслуховував вашу розмову у кафе, використовуючи свої знання, щоб викрасти вашу особисту інформацію. Але існує безліч способів, як захистити себе, які ми сьогодні розглянули. Отже, пам'ятайте, ваша безпека в ваших руках. Якщо ви будете уважними і обізнаними, зможете уникнути пасток і захистити свої дані від кіберзлочинців.

Перелік посилань:

Cisco, Cybercalm, https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM.

Хавер Анюта Вячеславівна
аспірантка групи АІКБ-11, Кафедри ІКБ ДУІКТ, Київ, Україна

BASIC PROCESS CONTROL TA SYSTEMS SAFETY INSTRUMENTED SYSTEMS – ЯК ОСНОВНІ ЦІЛІ СПЕЦІАЛЬНОГО ТРОЯНСЬКОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ОБ'ЄКТА КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Сучасний кіберзахист інформаційних систем технологічного середовища об'єктів критичної інфраструктури вимагає проактивного захисту від впливу спеціального троянського програмного

забезпечення. Прикладом, що засвідчує небезпеку застосування такого методу кібератак на українські системи промислового управління є діяльність російської хакерської групи Sandworm (APT44) (ШПЗ Blackenergy, NotPetya та інш.).

Найбільш важливим завданням для кіберзахисту технологіяних інформаційних систем об'єктів критичної інфраструктури є збереження сталості та безпеки функціонування виробничого процесу, збої в якому можуть призвести до значних наслідків, відмов, великих фінансових збитків та навіть техногенних катастроф. Основні технологічні процеси об'єкта критичної інфраструктури, зазвичай, зосереджені нижче 3-го рівня моделі Purdue.

Ключові слова: кібербезпека об'єктів критичної інфраструктури, системи промислової автоматизації і управління (Industrial Automation and Control System), спеціальне троянське програмне забезпечення, Basic Process Control Systems (BPCS), Safety Instrumented Systems (SIS), Інтегрована система управління та безпеки (Integrated Control and Safety System).

Діяльність хакерських груп, що спонсоруються державами продовжує становити основну загрозу для сталого функціонування інформаційних систем промислової автоматизації і управління об'єктів критичної інфраструктури України. В зв'язку з цим при виборі засобів і методів захисту об'єктів критичної інфраструктури від кіберзагроз необхідно враховувати поточну кон'юнктуру в кіберпросторі, яка не виключає застосування субєктами загрози спеціального троянського програмного забезпечення (далі – СТПЗ) з метою здійснення кібершпіонажу або (та) проведення деструктивних кібератак по об'єктах критичної інфраструктури України. Можна припустити, що при проведенні подібної кібератаки основною ціллю суб'єктів загрози на етапі постексплуатації є технологічна система та її складові.

За даними MITRE ATT&CK for Industrial Control Systems: Design and Philosophy (2020) найчастіше ціллю хакерів в технологічній системі є наступні три основні інформаційні підсистеми рівня 3 і нижче моделі Purdue: Basic Process Control Systems (BPCS), Safety Instrumented Systems (SIS), Engineering and Maintenance Systems (EMS) [1].

Розглянемо BPCS та SIS більш детальніше.

Інтерес суб'єктів загрози до отримання доступу до BPCS та SIS обґрунтований перш за все функціоналом цих підсистем та безпосередньою близькістю до фізичного обладнання виробничого процесу.

Розглянемо основні функції BPCS та SIS.

Головна функція BPCS полягає у здійсненні моніторингу технологічного процесу і управлінні ним. На цьому рівні, зазвичай, працює (може бути розгорнуто) одна з наступних технологій (систем) промислового управління та моніторингу: Programmable logic controller (PLC), Supervisory Control and Data Acquisition (SCADA), Distributed control system (DCS). Вибір однієї з них залежить від необхідного масштабу та інших конкретних потреб підприємства. Важливим аспектом є те, що з рівнем BPCS можуть інтегруватися системи вищого рівня, наприклад, такі як система виконання виробництва (MES) і системи планування ресурсів підприємства (ERP) [2]. Такі системи вищого рівня, зазвичай, розгорнуті в корпоративному сегменті, тому наявність фізичних та логічних зв'язків між промисловою та корпоративною мережами повинна бути надійно захищена, щоб унеможливити використання такого зв'язку суб'єктом загрози для подальшого бічного переміщення.

SIS відповідає за безпеку експлуатації об’єкта, контроль аварійних процедур і у разі виникнення аномалій, приведення виробничого процесу до безпечного стану. Зазвичай SIS виконує декілька функцій безпеки Safety Instrumented Function (SIF). Варто відзначити, що SIS не є активною підсистемою і втручається в процес лише при виникненні небезпечних умов.

Типовими прикладами SIS є:

система аварійного відключення;

система захисного відключення;

система захисного блокування;

система вогню та газу.

Стандартами функціональної безпеки для SIS є IEC 61508 та IEC 62061.

BPCS в залежності від рішення завдяки якому вона реалізована, зазвичай, складається з наступних компонентів: датчики, контроллери та виконавчі механізми від яких підсистема отримує вхідну інформацію. Внутрішню обробку та обчислення вона виконує в контроллері DCS (SCADA), а потім надсилає вихідні дані на регулюючий клапан. BPCS має інтегрований Human Machine Interface для управління системою з віддаленого місця, який зазвичай розташований в диспетчерській.

SIS, зазвичай, складається з вхідних елементів (наприклад, датчиків, передавачів), одного або кількох логічних вирішувачів (наприклад, програмованих логічних контролерів (PLC), релейних логічних систем) і одного або кількох кінцевих елементів (наприклад, запобіжних клапанів, автоматичних вимикачів).

Щоб завдати шкоду виробничому процесу суб’єкт загрози має знешкодити SIS, щоб вона не завадила встановлювати параметри, які відмінні від норми для BPCS. В контексті вищезазначеного, важливо відмітити важливість паралельної побудови BPCS та SIS, окремими, а не комплексними рішеннями (бажано з використанням рішень різних виробників для кожної з систем) (що передбачено стандартом ANSI/ISA 84.00.01-2004 11.2.10).

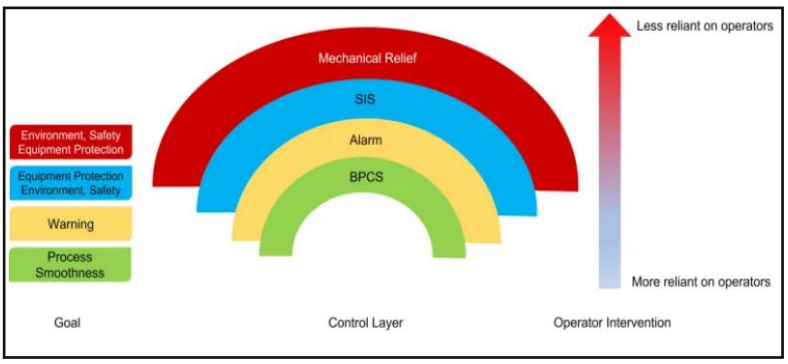


Рис. 1 Умовна діаграма забезпечення безпеки технологічного процесу при виявленні небезпеки

Якщо виробничий процес виходить з під контролю (Рис.1) – BPCS оголошується тривога.

Таке оповіщення покликано попередити оператора про необхідність вжити більш рішучих заходів для виправлення небезпечної ситуації. Коли аномалія процесу все ще продовжує швидко рухатися до небезпечного рівня, тоді SIS бере

на себе контроль над пристроєм. Якщо й дія SIS виявиться неефективною кінцевим рівнем захисту є система рельєфу (relief system). Система рельєфу представляє собою механічну систему для захисту станції, навколишнього середовища, а також операторів та іншого персоналу. У сукупності BPCS, сигналізація та SIS називаються Integrated Control and Safety System (ICSS).

Виходячи з вищезазначеного, для моніторингу безпечності функціонування технологічного процесу на об'єкті критичної інфраструктури та виявлення дії СТПЗ на BPCS та SIS необхідно здійснювати моніторинг стану параметрів їх компонентів на основі поведінкової аналітики. Для вибору необхідних параметрів вищезазначених систем пропонується дослідити та в подальшому використати окремі тактики "MITRE ICS tactics" та їх техніки, які покривають рівень 3 і нижче моделі Purdue та передбачають, що суб'єкт загрози вже проник в промислову систему та володіє деякою інформацією про неї, яку отримав на попередніх етапах кібератаки [3]. Моніторинг параметрів, які буде обрано в результаті аналізу пропонується здійснювати з використанням відкритого програмного забезпечення аналізу даних і машинного навчання.

Перелік посилань:
1. MITRE ATT&CK: Design and Philosophy – [Електрон.Ресурс] –Режим доступу: https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf;
2. DCS vs SCADA: Understanding the Differences and Benefits s –[Електрон.Ресурс] –Режим доступу: DCS vs SCADA: Understanding the Differences and Benefits | NMSC (nextmsc.com);
3. Командування та управління, Тактика TA0101 - ICS | MITRE ATT&CK® –[Електрон.Ресурс] –Режим доступу: https://attack.mitre.org/tactics/TA0101/

Хацько Микита Вікторович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

НЕБЕЗПЕКИ ШТУЧНОГО ІНТЕЛЕКТУ: ПОДВІЙНИЙ НІЖ

Штучний інтелект (ШІ) відкриває величезні можливості для розвитку технологій, бізнесу та суспільства загалом, але разом із цим несе й значні загрози, які часто недооцінюються. ШІ — це подвійний ніж: з одного боку, він може підвищити ефективність систем безпеки, автоматизувати складні процеси, допомогти в аналітиці великих даних та швидко реагувати на загрози. З іншого боку, саме його можливості можуть бути використані для створення нових видів кіберзагроз, маніпуляцій та підриву безпеки.

Однією з найбільших небезпек ШІ є автоматизація кіберзлочинів. Зловмисники вже використовують штучний інтелект для вдосконалення своїх атак. Наприклад, за допомогою ШІ можна автоматично генерувати фішингові повідомлення, які адаптуються до жертви, створюючи ілюзію довіри. ШІ також дозволяє вдосконалювати техніки соціальної інженерії, оскільки може аналізувати великі обсяги інформації про людину з відкритих джерел та використовувати її для персоналізованих атак. Ці алгоритми стають розумнішими, що ускладнює розпізнавання фішингу навіть досвідченим користувачам.

Ще один аспект небезпеки ШІ — його використання для кібератак на масштабному рівні. ШІ може значно пришвидшити та автоматизувати процес виявлення вразливостей у системах, полегшуючи кіберзлочинцям проникнення в мережі організацій. Наприклад, за допомогою спеціалізованих алгоритмів можна швидко знайти слабкі місця в коді програмного забезпечення або ідентифікувати вразливі пристрої в мережі, що дає змогу зловмисникам проводити атаки з набагато меншою участю людини.

Небезпека також полягає в тому, що штучний інтелект може бути використаний для створення діпфейків — відео та аудіоматеріалів, які можуть реалістично підробляти голоси та обличчя людей. Це відкриває нові можливості для маніпуляцій і шахрайства. Уявіть ситуацію, коли шахрай надсилає фальшивий відеозапис керівника компанії з вимогою здійснити терміновий переказ коштів. Подібні сценарії вже траплялися, і розвиток діпфейків лише ускладнює їх розпізнавання.

Крім того, існує ризик "перекосу" алгоритмів ШІ. Це ситуації, коли штучний інтелект неправильно інтерпретує інформацію або робить неправильні висновки на основі навчальних даних, що може призвести до серйозних помилок у системах безпеки або управління. У випадках, коли ШІ контролює критичні інфраструктури або процеси, такі помилки можуть мати катастрофічні наслідки.

ШІ також може сприяти підвищенню рівня нерівності та соціальних проблем. Автоматизація багатьох процесів може призвести до втрати робочих місць, що створить нові соціальні виклики, зокрема в питаннях безпеки. Зі зростанням автоматизації злочинних дій, людська участь стає все менш необхідною, що робить кіберзагрози ще небезпечнішими.

Проте ШІ може бути й потужним інструментом захисту, якщо використовується відповідально. Системи штучного інтелекту можуть допомагати у виявленні кіберзагроз у режимі реального часу, аналізувати аномальні поведінкові патерни в мережах та автоматично реагувати на потенційні атаки. Це дозволяє фахівцям із кібербезпеки зосередитися на стратегічних аспектах захисту.

Таким чином, штучний інтелект, без сумніву, є потужним інструментом як для захисту, так і для здійснення кібератак. Залишаючись на передовій технологічних інновацій, необхідно пам’ятати про дві сторони цього явища і постійно працювати над тим, щоб мінімізувати його небезпеки, використовуючи його можливості на благо.

Перелік посилань:

1. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/the-role-of-ai-in-cybersecurity-anticipating-and-preventing-attacks (date of access: 07.10.2024).
2. І знову про штучний інтелект. Допомога, загроза чи пусті балачки?. URL: https://yur-gazeta.com/publications/practice/inshe/i-znovu-pro-shtuchniy-intelekt-dopomoga-zagroza-chi-pusti-balachki.html (date of access: 05.10.2024).
3. Дезінформація та штучний інтелект: (не)видима загроза сучасності. URL: https://cedem.org.ua/analytics/dezinformatsiya-shtuchnyi-intelekt/ (date of access: 04.10.2024).

Ходацький Володимир Юрійович
студент групи ІПЗ-32, ФІТ КНУ, Київ, Україна

ІЗОЛЯЦІЯ ТА БЕЗПЕКА ПОТОКІВ В ОПЕРАЦІЙНИХ СИСТЕМАХ

Проблема безпеки операційних систем у сучасних умовах інформаційної ери набуває надзвичайної важливості. Із зростанням складності програмних середовищ та поширенням багатозадачності підвищується потреба в забезпеченні надійної ізоляції та безпеки процесів і потоків в операційних системах. Потоки виконання (або threads), які представляють собою підмножини процесів, відіграють ключову роль у досягненні високої продуктивності та ефективного розподілу ресурсів системи. Проте саме через багатопоточність виникає ряд загроз безпеці, зокрема ризик витоків даних та атак на ресурси системи.

Перш ніж переходити до розгляду механізмів безпеки та ізоляції потоків, необхідно чітко визначити їхню сутність та роль у контексті операційної системи. Потік є одиницею виконання, яка виконується всередині процесу. Кожен потік має власний стек, регістри і лічильник команд, але він спільно використовує ресурси процесу, такі як пам’ять і відкриті файли. Завдяки цьому потоки забезпечують паралельне виконання завдань і є основним інструментом для досягнення високої продуктивності в багатоядерних процесорах.

Основною перевагою потоків є їхня легкість порівняно з процесами. Створення нового потоку займає менше ресурсів, ніж створення нового процесу, оскільки потоки розділяють спільний адресний простір процесу. Проте саме цей аспект багатопоточності є також джерелом ризиків для безпеки.

Ізоляція потоків в операційних системах

Ізоляція процесів і потоків — це ключовий механізм, який забезпечує стабільність операційної системи та захищає її від шкідливих або некоректних дій програм. Традиційно, в операційних системах ізоляція досягається на рівні процесів, що мають власний адресний простір. Проте у випадку потоків, які ділять один адресний простір, цей підхід неможливий, і тому застосовуються інші методи ізоляції, такі як:

Стекова ізоляція потоків: Кожен потік у процесі має свій власний стек для зберігання локальних змінних і контексту виконання. Операційна система

гарантує, що кожен потік має доступ лише до власного стека і не може втручатися в стеки інших потоків. Це важливо для запобігання помилок типу «переповнення буфера», які можуть призвести до збоїв у роботі програми або атаки на систему.

Ізоляція даних через механізми синхронізації: Взаємодія між потоками в одному процесі відбувається через спільні дані. Для того щоб запобігти одночасному доступу кількох потоків до цих даних, використовуються механізми синхронізації, такі як м’ютекси, семафори, монітори і бар'єри. Вони дозволяють обмежити доступ до спільних ресурсів, забезпечуючи коректну та безпечну їхню обробку.

Для зниження ризиків, пов'язаних з неконтрольованим доступом потоків до спільних ділянок пам'яті, сучасні операційні системи використовують різноманітні стратегії захисту. Це включає механізми розмежування прав доступу до різних ділянок пам'яті (запис, читання, виконання), а також технології запобігання виконанню коду з некоректних ділянок пам'яті (NX-bit).

Загрози безпеці в багатопотокових середовищах

Оскільки потоки ділять спільні ресурси процесу, це створює певні загрози для безпеки, особливо в умовах помилок у синхронізації або спеціальних атак, що експлуатують паралельність виконання. Однією з головних загроз у багатопоточних середовищах є ризик витоків даних між потоками. Якщо один потік отримує доступ до конфіденційних даних, які не призначені для нього, це може призвести до серйозних наслідків, зокрема до порушення приватності або неправомірного використання даних.

“Race condition” — це ситуація, коли кілька потоків одночасно намагаються доступитися до одного ресурсу, і результат залежить від порядку їх виконання. Такі атаки можуть призводити до непередбачуваних змін в роботі програми, витоків інформації або навіть виконання шкідливого коду. Для запобігання цьому застосовуються блокування та інші механізми синхронізації.

У деяких випадках зловмисники можуть використовувати кеш-пам'ять або інші спільні ресурси для отримання конфіденційної інформації. Наприклад, у багатоядерних системах потоки можуть ділити кеш процесора, і зловмисник може спостерігати за поведінкою кеша для отримання доступу до ключової інформації, такі атаки називаються “cache timing attacks”.

Методи забезпечення безпеки потоків

З метою мінімізації ризиків у багатопоточних середовищах операційні системи використовують кілька підходів до забезпечення безпеки.

Застосування технологій захисту пам'яті, таких як апаратні механізми віртуалізації або маркування прав доступу до сторінок пам'яті, дозволяє значно знизити ризик некоректного доступу потоків до даних. Це включає як класичні механізми сторінкової ізоляції (“paging”), так і новітні технології, зокрема механізми контролю доступу до виконуваного коду.

Одним із напрямків мінімізації ризиків багатопоточності є використання безпечних мов програмування, таких як Rust або Ada, які пропонують вбудовані механізми захисту від помилок синхронізації та переповнення буферів.

У сучасних процесорах все більше уваги приділяється вбудованим механізмам безпеки. Наприклад, технології Intel SGX або ARM TrustZone дозволяють виконувати критичні процеси у ізольованому середовищі навіть на рівні потоків, забезпечуючи таким чином додатковий захист.

Перспективи розвитку ізоляції та безпеки потоків

У майбутньому варто очікувати подальшого розвитку методів ізоляції та безпеки потоків, зокрема через інтеграцію з хмарними обчисленнями, машинним навчанням і технологіями штучного інтелекту. Важливим напрямком є дослідження нових способів захисту від атак на кеш та інші спільні ресурси, а також розробка нових апаратних технологій захисту.

В кінці, можна зробити висновок, що ізоляція та безпека потоків є невід'ємною складовою забезпечення стабільної та безпечної роботи операційних систем, особливо в умовах сучасних загроз і підвищених вимог до продуктивності. Подальший розвиток механізмів захисту та синхронізації в багатопоточних середовищах є важливим напрямком наукових досліджень і технологічного прогресу в галузі операційних систем.

Перелік посилань:

1. Таненбаум А.С., Бос Г. "Операційні системи: розробка та реалізація". – К.: Пітер, 2015.
2. Столлінгс В. "Операційні системи: внутрішні механізми і принципи проектування". – Pearson, 2018.
3. Моріс К., Шварц М., Грус Д., Мангард С. "Просунуті проблеми безпеки у багатопотокових системах".
4. Керрік М. "Інтерфейс програмування в Linux: посібник з програмування систем Linux і UNIX". – No Starch Press, 2010.
5. Росс Дж. Андерсон. "Інженерія безпеки: Керівництво з побудови надійних розподілених систем"

Чечик Марина Олексіївна,
студентка групи БСД-42, ННІЗІ ДУТ, Київ, Україна

АКТУАЛЬНІ ВРАЗЛИВОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ОЦІНКА РИЗИКІВ ТА ЗАХИСТ

Критична інфраструктура є одним з найважливіших елементів сучасного суспільства, який забезпечує безперервне функціонування важливих галузей, таких як енергетика, транспорт, телекомунікації, водопостачання та інші. Одним із основних аспектів забезпечення безпеки є виявлення та усунення ризиків експлуатації вразливостей, що можуть бути використані зловмисниками для атак і компрометації систем. Почати насамперед варто з

аналізу актуальних вразливостей, що притаманні підприємствам критичної інфраструктури.

Програмні вразливості. Застаріле програмне забезпечення є першою причиною експлуатації старих вразливостей зловмисниками, а відсутність регулярних оновлень залишає вразливості відкритими для зловмисників. Крім того, застаріле програмне забезпечення може бути несумісним із сучасними технологіями безпеки, такими як двофакторна аутентифікація або сучасні шифрувальні протоколи, що робить новітні інструменти безпеки неефективними [1]. Недостатнє шифрування та аутентифікація призводить до порушень конфіденційності та цілісності. Використання ключів недостатньої довжини, наприклад, 56-бітові ключі, підвищує ризик успішної атаки грубої сили шляхом перебору (далі - bruteforce). Також відсутність багатофакторної аутентифікації збільшує ризик успішних атак на облікові записи, оскільки зловмисну достатньо заволодіти лише паролем (одним фактором). Використання застарілих протоколів аутентифікації (NTLM, CHAP або PtPP), може призвести до компрометації облікових записів через старі вразливості.

Апаратні вразливості. Фізичні вразливості, такі як відсутність зонування або доступ до обладнання сторонніх осіб, дозволяють зловмисникам отримати контроль над інфраструктурою. Фізичні атаки на трансформатори, системи охолодження, датацентри або комунікаційне обладнання можуть призвести до масштабних перебоїв у енергопостачанні, зв'язку і функціонуванні загалом. Також слід пам’ятати, що викрадення або втрата носіїв даних може призвести до витоку конфіденційної інформації і компрометації чутливих даних. Недосконалості в мікропроцесорах та інших апаратних компонентах можуть бути використані для атак, що викликають фізичні пошкодження і повне знищення. Також, щоб отримати інформацію про обчислення мікропроцесора, зловмисники використовують вимірювання електромагнітних сигналів, які процесор створює під час роботи. Недоліки у внутрішніх механізмах процесорів, таких як керування перериваннями, доступ до хешу або керуванням пам'яті, можуть бути використані для обходу рівнів привілеїв і контролю доступу.

Ретельний технічний аналіз вразливостей та пов’язаних з ними ризиків допомагає ідентифікувати перелічені ризики та вжити відповідні заходи захисту. Наприклад, вирішення проблеми застарілого програмного забезпечення в закладах критичної інфраструктури вимагає стратегічного підходу та застосування комплексних заходів.

• Впровадити інструменти централізованого керування оновленнями та автоматизації цього процесу, щоб мінімізувати людське втручання.

• Проводити освітні заходи для підвищення обізнаності персоналу в питаннях базової безпеки.

• У разі, якщо уникнути використання застарілого ПЗ чи його компонентів неможливо, рекомендується ізолювати ризики, використовуючи технології віртуалізації та контейнеризації.

Вирішення вразливостей, пов'язаних з недостатнім шифруванням та аутентифікацією, вимагає впровадження сучасних методів та технологій

безпеки, адже алгоритми шифрування є загальнодоступними і не передбачають фінансових витрат. Замість застарілих алгоритмів, таких як DES або RC4 варто перейти на сучасні аналоги, такі як AES (Advanced Encryption Standard) з ключами довжиною 256 біт. Також, щоб знизити ризики атаки bruteforce, рекомендується впровадити блокування облікових записів після кількох невдалих спроб входу [2].

Подолання апаратних вразливостей, таких як фізичні ризики та недосконалості в мікропроцесорах, вимагає комплексного підходу. Зокрема, для обмеження доступу до обладнання, важливо створити фізичні контрольовані зони з обмеженим доступом для критичних об'єктів. Доступ до функцій низького рівня, таких як BIOS або UEFI, має бути обмеженим шляхом застосування паролів і засобів контролю доступу. Для забезпечення надійного функціонування обладнання потрібно проводити регулярне обслуговування та перевірку його стану, що дозволяє виявляти потенційні несправності та своєчасно їх усувати. Впровадження останніх патчів безпеки та оновлень процесорів (лише тих, що надаються офіційними виробниками) також сприяє мінімізації ризиків експлуатації відомих вразливостей. В свою чергу для захисту обладнання від електромагнітних атак (через електромагнітні, електричні та індуктивні канали витоку інформації), рекомендується застосовувати екранування, використовуючи заземлені металеві шафи та контейнери [3].

Багатофункціональним рішенням для підприємств критичної інфраструктури, в яких часто обмежені ресурси і немає можливості використовувати новітні системи захисту, можуть стати бюджетні системи моніторингу та реагування на інциденти, що відповідають базовим вимогам безпеки. Розглянемо Windows Event Viewer — інструмент, вбудований у Windows, що дозволяє переглядати системні журнали подій, пов'язані з операційною системою, службами, додатками та іншим обладнанням. Дані, отримані в результаті роботи цього інструменту, можна фільтрувати і експортувати для аналізу в інших системах. Поєднуючи Windows Event Viewer зі скриптовою мовою PowerShell, можна реагувати на небажані чи неочікувані події у системі, створивши таким чином власну унікальну IDS (Intrusion Detection System) [4].

Шляхом глибокого аналізу програмних та апаратних вразливостей, ризиків їхньої експлуатації, та встановлення відповідних заходів захисту, можливо забезпечити високий рівень безпеки для критичної інфраструктури та особистих даних. Важливо зазначити, що управління ризиками - це комплексний підхід, що об’єднує в собі багато аспектів, і не пропонує одного універсального рішення. Застосування сучасних технологій, поєднання знань із практичними навичками, а також постійне вдосконалення стратегій безпеки є ключовими аспектами у забезпеченні надійності та стійкості цифрових систем підприємств критичної інфраструктури сучасному світі.

Перелік посилань:
1. Vulnerable and outdated components https://learn.snyk.io/lesson/vulnerable-and-outdated-components/
2. M10: Insufficient Cryptography https://owasp.org/www-project-mobile-top-10/2023-risks/m10-insufficient-cryptography
3. Василюк Володимир, Об'єкти захисту інформації. Методи та засоби захисту інформації, 2006. 93 с.
4. Windows Event Logs | TryHackMe URL: https://igorsec.blog/2023/08/02/windows-event-logs-tryhackme/.

Чміленко Олександр Анатолійович, БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ НА БАЗІ QRADAR ADVISOR WITH WATSON

Визначено мету і основні завдання щодо розслідування кіберінцидентів за допомогою штучного інтелекту. Розглянуто зміст технології розслідування кіберінцидентів за допомогою штучного інтелекту на базі QRadar Advisor with Watson.

Сьогодні багато організацій проходять процес цифрової трансформації, яка супроводжується такими проблемами, як зростаюча складність їхньої IT-інфраструктури, величезні обсяги конфіденційних даних, поширених у багатьох хмарах, і дедалі більша нестача кваліфікованих людей для роботи з ними. Навіть потужні команди безпеки великих компаній, які працюють у центрі безпеки на платформі SIEM, не можуть впоратися з останніми цифровими ризиками та швидким зростанням кількості та складності сучасних кібератак.

Реакцією ринку безпеки на це є новий клас інструментів аналізу безпеки, які використовують потужність машинного навчання, щоб зменшити кількість хибних спрацьовувань та інших шумів, створюваних традиційними SIEM, і надати аналітику безпеки невелику кількість контекстно-збагачених сповіщень, які ранжуються за оцінками ризику, та часто супроводжуються дієвими рекомендаціями щодо пом’якшення.

Швидкий розвиток додатків для машинного навчання та штучного інтелекту в останні роки підштовхнув багатьох компаній до ідеї, що їхніх перевантажених аналітиків безпеки незабаром буде повністю замінено штучним інтелектом, який бореться з кіберзагрозами та зломами без втручання людини. Але така перспектива здається досить далекою від реальності з кількох причин: від властивих обмежень алгоритмів машинного навчання до численних юридичних та етичних наслідків застосування автономного штучного інтелекту.

Недоліками SIEM систем є те, що лише спостереження за подіями безпеки не допомагає аналітикам оцінювати кожну виявлену загрозу: через

кількість ручних завдань і різноманітних інструментів, необхідних для ретельного аналізу, аналітики втрачають надто багато дорогоцінного часу. Найчастіше їм доводиться мати справу з сотнями чи тисячами сповіщень, і просто немає часу, щоб правильно розглянути кожне.

Сьогодні можливості рішення IBM QRadar SIEM розширюються шляхом використання алгоритмів машинного навчання для кореляції кількох подій безпеки, значного зменшення кількості помилкових спрацьовувань і забезпечення автоматизованої оцінки ризику кожної події.

Платформа IBM QRadar Security Intelligence Platform забезпечує уніфіковану архітектуру, яка поєднує інформацію про безпеку з керуванням подіями, виявленням у реальному часі розширених загроз, атак і взломів, криміналістичним аналізом і реагуванням на інциденти, а також автоматизованою відповідністю нормативним вимогам.

QRadar Advisor із Watson інтегрує платформу QRadar Security Analytics Platform із когнітивним штучним інтелектом Watson для виконання повністю автоматизованих криміналістичних розслідувань інцидентів безпеки, значно покращуючи продуктивність аналітиків і забезпечуючи швидке реагування на кіберзагрози.

Додаток IBM QRadar Advisor with Watson дає змогу аналітикам безпеки проводити послідовні розслідування та швидше й рішучіше розширювати інциденти, що призводить до скорочення часу очікування та підвищення ефективності аналітиків [1].

Додаток IBM QRadar Advisor with Watson надає можливості для:

створення пріоритетності розслідувань із найбільшим ризиком;

швидкого фільтрування та сортування даних на основі критичності;

Рис. 1. Штучний інтелект відкриває нове партнерство між аналітиками безпеки та їхніми технологіями [1]

розслідування інцидентів відповідно до розширеного зворотного зв’язку IBM Watson, використовуючи внутрішні та зовнішні канали аналізу загроз;

проведення послідовних та глибших досліджень інцидентів;

автоматичного розслідування за допомогою підключених спостережуваних за допомогою аналітики перехресних розслідувань і виходу за межі поточного потенційного інциденту;

уникнення дублювання зусиль;

визначення, чи потрібно виконувати додаткове налаштування у випадку кількох повторюваних розслідувань, ініційованих однаковими подіями;

візуалізації того, як відбулася та прогресувала атака, рівень достовірності для кожної прогресії, які тактики мали місце та які тактики ще можуть бути використані за допомогою моделі ATT&CK MITRE;

застосування переваг Easy Incident Scoring, щоб надати своїм аналітикам швидший і рішучий процес ескалації;

підвищення ефективності аналітика та зменшення MTTD і MTTR.

В [1] наводиться приклад, що аналітики Sogeti Luxembourg змогли скоротити час розслідування з двох-трьох годин до двох-трьох хвилин. Це дорогоцінний час, який аналітики можуть краще витратити на подальше дослідження реальних загроз і додавання багатшого контексту до своїх розслідувань. Багато інших клієнтів використовують штучний інтелект, щоб збільшити зусилля своєї команди безпеки. А за допомогою штучного інтелекту вони можуть залучати менш кваліфікованих працівників для заповнення ролей аналітиків рівня 1, сприяючи тому, щоб поточні аналітики рівня 1 могли зосередилися на обов'язках рівня 2 і збільшували зусилля своїх команд [1].

В [2] відмічається, що початковий випуск додатка QRadar Advisor with Watson дозволив Watson збирати, читати та розуміти структуровані та неструктуровані дані безпеки із зовнішніх джерел, а також надавати найбільш релевантну інформацію аналітикам, щоб допомогти їм зрозуміти, що вже відомо та опубліковано щодо конкретної загрози. Тепер QRadar Advisor також вчиться на діях, які виконуються в середовищі клієнтів – як події, що відбуваються в реальному часі, так і те, що відбувалося з певними типами подій історично. Дві нові можливості, які IBM представляє для QRadar Advisor, включають [2]:

моделі усунення загроз: QRadar Advisor використовує нові алгоритми для побудови моделі для конкретних типів загроз на основі дій і результатів попередніх подібних подій, які сталися в організації. Коли надходить нове розслідування, цю модель можна використовувати, щоб допомогти виключити помилкові спрацьовування або допомогти аналітику вирішити, чи слід розповсюдити загрозу як зловмисне програмне забезпечення, викрадання даних або інші конкретні типи загроз. Ця можливість стає все розумнішою, чим більше її використовують, навчаючись і адаптуючись на основі взаємодії з аналітиками;

аналітика перехресних розслідувань: у Центрі безпеки компанії (SOC) кілька аналітиків можуть працювати над різними порушеннями, які пов'язані одне з одним, або сповіщення протягом багатьох місяців можуть бути частиною довгострокової змагальної кампанії. Ця можливість дозволяє QRadar Advisor знаходити спільні риси в розслідуваннях за допомогою когнітивних міркувань і автоматично групувати пов'язані дослідження, щоб уникнути дублювання зусиль, а також надавати повніший контекст для допомоги в розслідуванні.

На рисунку 2 показано схему функціонування рішення QRadar Advisor

with Watson.

Рис. 2. Порядок функціонування QRadar Advisor with Watson [3]

QRadar Advisor with Watson працює в три етапи [3]:

коли платформа QRadar Security Intelligence виявляє інцидент безпеки, аналітик може призначити його QRadar Advisor with Watson для розслідування. QRadar Advisor спочатку збирає більш детальний контекст про цей інцидент, аналізуючи локальні дані, доступні в QRadar. Потім він консультується з Watson for Cyber Security, щоб отримати зовнішню інформацію та виявити загрози на основі окремих спостережень, пов'язаних з інцидентом;

Watson for Cyber Security досліджує свою базу знань – зібрану із сотень тисяч джерел у формі веб-сайтів, форумів із безпеки, бюлетенів тощо – для формування свого розуміння інциденту безпеки. Потім він використовує міркування, щоб виявити додаткову інформацію та інші об'єкти загрози, пов'язані з початковим інцидентом, наприклад шкідливі файли, підозрілі IP-адреси, шахрайські об'єкти та зв'язки між ними;

далі QRadar Advisor with Watson уточнює інформацію, яку він отримує від Watson for Cyber Security, щоб зосередитися на ключових відомостях, що стосуються поточного інциденту. Нарешті, аналітик може виконати подальші дії на основі інформації, представленої QRadar Advisor with Watson, і надіслати інформацію про інцидент разом із підтверджуючими доказами групі реагування.

Отже, зростаюча кількість досліджень вказує на те, що організації, які впроваджують засоби штучного інтелекту безпеки та автоматизації, отримують трансформаційні операційні переваги. Завдяки цим технологіям примноження сили компанії можуть виявляти кіберінциденти та реагувати на них з більшою швидкістю, що може значно зменшити вартість і вплив кіберінцидентів.

Перелік посилань:

1. IBM QRadar Advisor with Watson. Automate your SOC with AI. IBM Security Solution Brief. URL: https://www.globalservices.com.tn/photos/817.pdf (дата звернення: 30.09.2024).

2. IBM QRadar Advisor with Watson Expands Knowledge of Cybercriminal Techniques. Global Brands Magazine. URL: https://www.globalbrandsmagazine.com/ibm-qradar-advisor-with-watson-expands-knowledge-of-cybercriminal-techniques/ (дата звернення: 30.09.2024).
3. Vijay Dheap. IBM QRadar Advisor with Watson: Revolutionizing the Way Security Analysts Work. URL: https://securityintelligence.com/ibm-qradar-advisor-with-watson-revolutionizing-the-way-security-analysts-work/ (дата звернення: 30.09.2024).

Чумак Михайло Олександрович
Студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ХМАРНИХ СЕРЕДОВИЩАХ

У зв'язку з розвитком технологій і швидким переходом до цифрових рішень, хмарні обчислення стали невід'ємною частиною сучасних корпоративних систем. Хмарні сервіси дозволяють зберігати та обробляти великі обсяги даних із мінімальними витратами, забезпечуючи гнучкість та масштабованість для бізнесів. Проте, поряд із цими перевагами, постає критичне питання — захист персональних даних. Використання хмарних середовищ додає нові виклики щодо кібербезпеки, оскільки підвищується ризик несанкціонованого доступу, втрати чи викрадення даних.

Однією з найпоширеніших і найбільш небезпечних загроз є витік даних. Це може статися через неправильну конфігурацію хмарних сервісів, недостатню захищеність або атаки на сервери, де зберігаються дані. Наприклад, якщо політики доступу неправильно налаштовані, зловмисники можуть отримати доступ до конфіденційної інформації.

Хмарні сервіси широко використовують інтерфейси програмування додатків для взаємодії між різними системами та додатками. Вразливості в API можуть бути експлуатовані зловмисниками для викрадення персональних даних або втручання в роботу систем. Атаки на API можуть включати SQL-ін'єкції, міжсайтові скрипти або атаки на автентифікаційні токени.

Несанкціонований доступ до хмарних систем — ще одна серйозна загроза. Якщо зловмисники отримують доступ до облікових записів адміністратора чи користувачів, вони можуть використовувати ці дані для несанкціонованих дій, що може призвести до викрадення чи модифікації даних. Ці атаки можуть здійснюватися через фішингові атаки або вразливості в механізмах автентифікації.

Співробітники організацій або партнери, які мають доступ до хмарних систем, можуть стати джерелом загрози для захисту персональних даних. Внутрішні загрози можуть виникати через зловживання правами доступу або через випадкові дії, що призводять до витоку інформації.

Для мінімізації ризиків, пов'язаних із захистом персональних даних у хмарних середовищах, слід застосовувати багаторівневий підхід до кібербезпеки. Основні методи включають шифрування, моніторинг активностей, а також регулярні аудити безпеки.

Шифрування є однією з основних технологій захисту даних у хмарі.

Використання сучасних криптографічних алгоритмів, таких як AES (Advanced Encryption Standard), дозволяє забезпечити конфіденційність інформації навіть у разі її перехоплення або доступу до неї неавторизованих користувачів. Важливо зашифровувати як дані "в стані спокою", так і "під час передачі".

Ефективне управління доступом до хмарних ресурсів має критичне значення для захисту персональних даних. Для цього використовуються політики мінімальних привілеїв, що забезпечує доступ користувачів тільки до тих ресурсів, які їм необхідні для виконання робочих завдань. Додатково важливо впроваджувати багатофакторну аутентифікацію (MFA), яка додає додатковий рівень захисту, вимагаючи від користувачів надання двох або більше факторів для доступу до системи.

Постійний моніторинг активностей у хмарних середовищах дозволяє виявляти аномальні дії та попереджати атаки до того, як вони завдадуть шкоди. Інструменти моніторингу, такі як AWS CloudTrail або Google Cloud Audit Logs, надають можливість відстежувати дії користувачів та зберігати журнали для проведення аудитів. Важливо також проводити регулярні аудити безпеки для виявлення можливих вразливостей і впровадження відповідних заходів для їх усунення.

Крім захисту даних, важливо забезпечити безпеку всієї хмарної інфраструктури. Це включає захист серверів, баз даних та віртуальних машин від атак, таких як DDoS або атаки на вразливості в системах віртуалізації. Хмарні постачальники часто пропонують інструменти для захисту інфраструктури, наприклад AWS Shield або Azure Security Center.

Захист персональних даних у хмарних середовищах є критичним завданням для забезпечення кібербезпеки корпоративних систем. Основними загрозами є витік даних, вразливості в API, несанкціонований доступ та внутрішні загрози. Щоб мінімізувати ці ризики, слід впроваджувати сучасні технології шифрування, багатофакторну аутентифікацію, постійний моніторинг та аудит, а також ефективне управління інцидентами. Лише комплексний підхід до безпеки дозволить гарантувати збереження конфіденційних даних та протистояти сучасним кіберзагрозам.

Перелік посилань:

1. Hashizume, K., et al. "An analysis of security issues for cloud computing." Journal of Internet Services and Applications URL: https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5 (дата звернення: 16.10.2024).
2. ENISA. "Cloud Computing: Benefits, Risks, and Recommendations for Information Security." European Network and Information Security Agency URL: https://www.enisa.europa.eu/ (дата звернення: 16.10.2024).
3. Stallings, W. "Cryptography and Network Security: Principles and Practice." URL: https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf (дата звернення: 16.10.2024).

Шайкова Анастасія Олегівна
Студентка групи БСДМ-61, ННІКЗІ ДУІКТ, Київ, Україна

ZERO TRUST NETWORK ACCESS (ZTNA) НА БАЗІ РІШЕНЬ CISCO: АРХІТЕКТУРА, БЕЗПЕКА ТА ПЕРЕВАГИ

З ростом кількості віддалених користувачів та хмарних сервісів, традиційні методи захисту мереж стають менш ефективними. Модель Zero Trust Network Access (ZTNA) змінює підхід до безпеки, застосовуючи принцип «ніколи не довіряй, завжди перевіряй», що дозволяє знизити ризики несанкціонованого доступу. Рішення Cisco в області ZTNA забезпечують надійний та динамічний захист, який відповідає потребам сучасних підприємств, допомагаючи мінімізувати кібератаки і захистити критичні дані.

Нульова довіра – це стратегічний підхід до безпеки, який базується на концепції усунення довіри з мережевої архітектури організації. Довіра не є постійною. Більше не можна вважати, що внутрішні об’єкти заслуговують на довіру, що ними можна безпосередньо керувати, щоб зменшити ризик безпеки, або що достатньо перевірити їх один раз. Модель безпеки з нульовою довірою змушує ставити під сумнів припущення про довіру при кожній спробі доступу.

Традиційні підходи до безпеки припускають, що всьому, що знаходиться всередині корпоративної мережі, можна довіряти. Реальність така, що це припущення більше не відповідає дійсності завдяки мобільності, BYOD (Bring Your Own Device), IoT (Internet of Things), впровадженню хмарних технологій, розширенню співпраці та зосередженню уваги на відмовостійкості бізнесу. Модель нульової довіри розглядає всі ресурси як зовнішні і постійно перевіряє довіру, перш ніж надати лише необхідний доступ [1].

Ключем до комплексної нульової довіри є поширення безпеки на все мережеве середовище з такими прикладами, як:

- Доступ співробітників до конфіденційних додатків, як в корпоративній мережі, так і за її межами.
- Підрядники та гості, які використовують мережеву інфраструктуру.
- Зв’язок між додатками.
- Зв’язок між промисловими системами управління.

Що виділяє Cisco серед інших рішень у контексті Zero Trust Network Access (ZTNA), це її комплексний підхід до забезпечення безпеки, який поєднує в собі кілька ключових переваг [2]:

Широкий спектр рішень: Cisco пропонує повний спектр технологій для реалізації ZTNA, включаючи Cisco Secure Access by Duo, Cisco Umbrella, Cisco Identity Services Engine (ISE) та Cisco Secure Network Analytics. Це дозволяє створювати єдину систему контролю доступу з багатофакторною автентифікацією, безпечним доступом до хмарних ресурсів та аналітикою мережевого трафіку.

Багатофакторна автентифікація (MFA): Duo від Cisco забезпечує потужну багатофакторну автентифікацію, яка знижує ризик компрометації облікових даних і гарантує, що доступ до корпоративних систем отримують лише перевірені користувачі на перевірених пристроях.

Хмарний захист і безпека віддалених користувачів: Cisco Umbrella надає безпечний інтернет-шлюз і захищає від загроз в інтернеті, навіть коли користувачі працюють віддалено. Це дозволяє зменшити залежність від VPN і забезпечити захист для будь-якого пристрою незалежно від його місця розташування.

Контроль доступу на основі політик: Cisco ISE дозволяє гнучко управляти доступом до мережі на основі політик. Це включає сегментацію

мережі, що знижує ризики всередині організації, ізолюючи потенційні загрози.

З акцентом на такі важливі елементи, як багатофакторна автентифікація, динамічний контроль доступу, шифрування даних і ретельна сегментація мережі, рішення ZTNA, побудовані на базі Cisco, пропонують повний захист для бізнес-мереж. Крім того, рішення Cisco легко інтегруються у вже існуючі IT-інфраструктури, що дозволяє компаніям розширювати безпеку відповідно до своїх потреб [2].

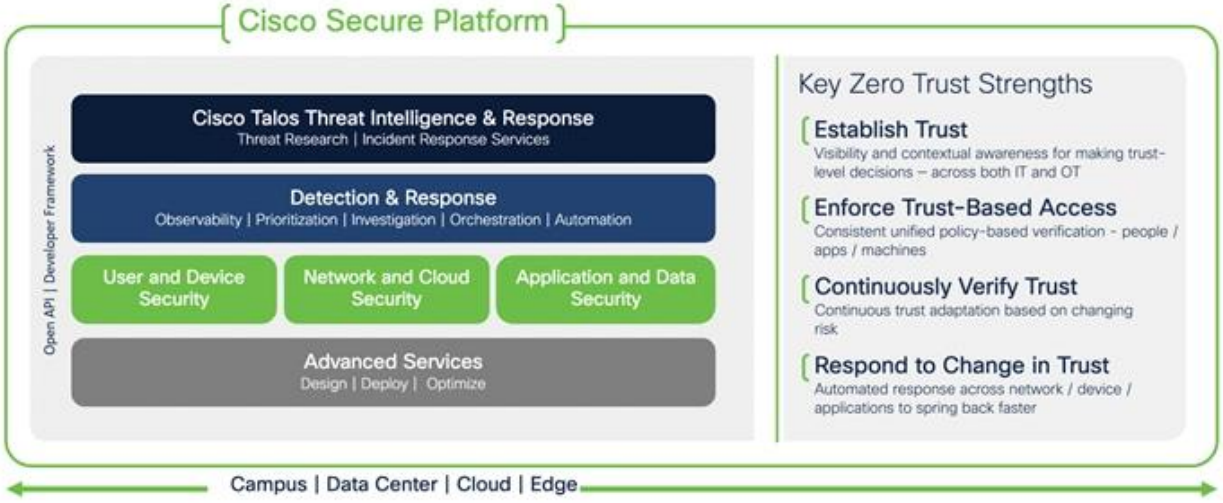


Рис. 1 – Cisco Zero Trust Framework

Перелік посилань:

1. Cisco Zero Trust Architecture Guide [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/zt-ag.html.

2. Zero Trust Access by Cisco [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/site/us/en/solutions/security/zero-trust-access/index.html.

Шандровський Ярослав Ігорович
Студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна
Чайківський Віталій Володимирович
Студент групи БСД-42, ННІЗІ ДУІКТ, Київ, Україна

СКЛАДНОСТІ ВПРОВАДЖЕННЯ СУЧАСНИХ СИСТЕМ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ

Сучасні системи кібербезпеки стикаються з необхідністю одночасно забезпечувати високий рівень захисту та підтримувати зручність і ефективність бізнес-процесів. Особливе значення має управління привілейованим доступом, яке дозволяє контролювати доступ до критичних ресурсів

організації. Основним викликом є пошук балансу між автоматизацією процесів безпеки та можливістю ручного втручання у надзвичайних ситуаціях. Це потребує впровадження гнучких рішень, здатних забезпечити безперервний доступ до систем навіть у випадку технічних збоїв або кіберінцидентів.

У сучасному світі, де кібербезпека стає все більш критичною, організації стикаються з постійною необхідністю балансувати між забезпеченням надійного захисту своїх інформаційних систем та збереженням ефективності робочих процесів. Одним з ключових інструментів у цьому контексті є системи управління привілейованим доступом (Privileged Access Management, PAM), які покликані забезпечити контрольований та безпечний доступ до критичних ресурсів організації.

PAM-системи відіграють важливу роль у захисті корпоративних мереж та даних, надаючи можливість адміністраторам централізовано керувати привілейованими обліковими записами та контролювати доступ до ключових систем. Однак, незважаючи на їх очевидні переваги, впровадження та використання PAM-систем супроводжується рядом викликів, які потребують ретельного аналізу та вирішення.

Одним з головних викликів при використанні PAM-систем є досягнення оптимального балансу між безпекою та зручністю використання. З одного боку, максимальне обмеження прямого доступу користувачів до цільових систем значно підвищує рівень захисту. З іншого боку, такий підхід може суттєво ускладнити роботу в нестандартних ситуаціях, коли потрібен швидкий доступ до ресурсів. Це створює ризик того, що в критичний момент адміністратори можуть зіткнутися з неможливістю оперативно вирішити проблему через обмеження, накладені PAM-системою.

Інший важливий аспект – це пошук правильного співвідношення між автоматизацією процесів безпеки та збереженням можливості ручного контролю. Повна автоматизація може усунути людський фактор з рівняння безпеки, але водночас може призвести до втрати гнучкості в управлінні доступом. Навпаки, надмірна довіра до ручного керування збільшує ризик людських помилок та зловживань. Знаходження золотої середини між цими крайнощами є складним завданням, яке вимагає ретельного планування та постійного моніторингу.

У світлі цих викликів стає очевидною необхідність у більш гнучких та адаптивних рішеннях для управління привілейованим доступом. Ідеальна система повинна забезпечувати високий рівень безпеки, не жертвуючи при цьому оперативністю та ефективністю роботи. Вона має бути достатньо гнучкою, щоб адаптуватися до різних сценаріїв використання, включаючи нестандартні та надзвичайні ситуації. Крім того, така система повинна легко інтегруватися в існуючу IT-інфраструктуру організації, мінімізуючи вплив на усталені бізнес-процеси.

Пропонується розглянути метод «Розбитого скла» (англ. «Break glass»), який застосовується у разі настання критичної ситуації, зокрема технічні збої та/або кібератаки, для оперативного надання доступу привілейованому

користувачів до цільової системи. Походження даного терміну тісно корелюється з реальним життям, оскільки при настанні пожежі спершу необхідно розбити скло, щоб активувати сигналізацію.

Зазвичай засоби захисту для контролю привілейованих користувачів (далі – PAM) використовують сховища паролів, які є потенційною точкою відмови. Оскільки, у разі недоступності сховища паролів, користувачі не зможуть отримати доступ до цільових систем – комунікація з якими реалізована за допомогою PAM. Відповідно система стає недоступною. Водночас, у разі впровадження методу «Розбитого скла» доступ надається через спеціальний обліковий запис, який створюється заздалегідь. Такому обліковому запису зазвичай надаються привілейовані права доступу до критичних систем.

Варто зазначити, що використання облікових записів для «Розбиття скла» дозволено обмеженій кількості осіб, за вмотивованої необхідності. Даний процес повинен регламентуватися відповідними внутрішніми розпорядчими документами, зокрема планами реагування на інциденти інформаційної безпеки. Необхідно регулярно здійснюватися періодичне тестування можливості автентифікації даним методом.

У разі необхідності доступу до цільових систем, але впроваджений інструмент PAM недоступний – використовується метод «Break Glass» (див. **Помилка! Джерело посилання не знайдено.**). Наприклад:

- Рішення PAM недоступне через технічне обслуговування;
- Кібератака або непередбачений простій рішення PAM.

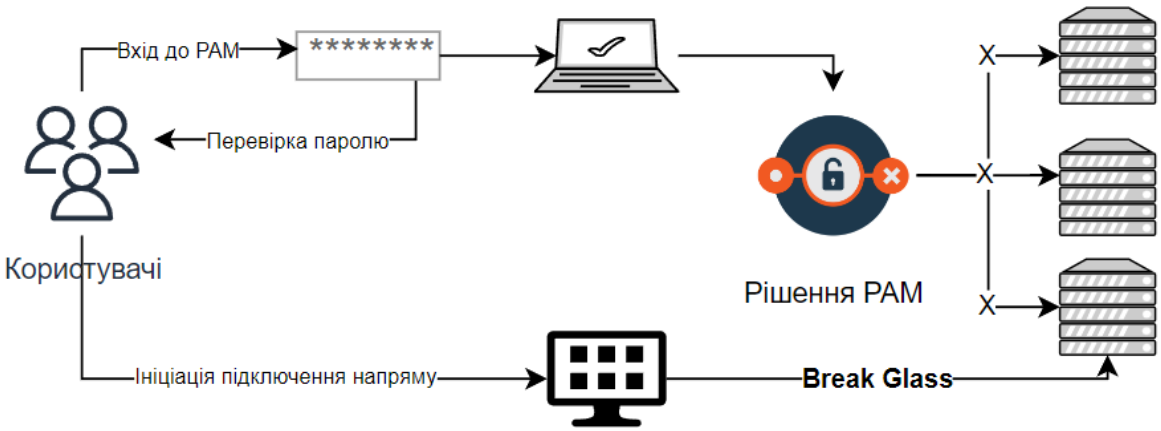


Рис. 1 – Концептуальний приклад використання «Break Glass»

Перелік посилань:

1. Microsoft Security 101: Privileged Access Management (PAM) URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-privileged-access-management-pam (дата звернення 16.10.2024).
2. Break Glass Explained: Why You Need It for Privileged Accounts URL: https://www.strongdm.com/blog/break-glass (дата звернення 16.10.2024).
3. Break Glass Procedure: Granting Emergency Access URL: https://hipaa.yale.edu/security/break-glass-procedure-granting-emergency-access-critical-ephi-systems (дата звернення 16.10.2024).

Щеглова Олена Андріївна
Студентка групи ТСДМ-61, ННІТ ДУІКТ, Київ, Україна

НАЙВІДОМІШІ КІБЕРАТАКИ НА ІОТ ПРИСТРОЇ

З кожним роком кількість IoT пристроїв збільшується у геометричній прогресії. Зі збільшенням попиту – збільшується необхідність у забезпеченні безпечного середовища для їх використання, що вимагає впровадження ефективних заходів кібербезпеки, захисту даних і управління мережевими інфраструктурами. Для побудови стратегії варто розглянути найвідоміші кібератаки на IoT пристроїв.

IoT, як і усі інші технології, можуть бути вразливими до кібератак. Серед поширених атак виділяють три основні: Mirai, Стакснет та Ланцюгова реакція. Розглянувши поведінку кожної атаки, можна підібрати профілактичні технології та процеси, щоб гарантувати безпеку IoT технологій.

Mirai — це назва зловмисного програмного забезпечення, яке заразило пристрої Linux IoT у серпні 2016 року. Атака відбулася у формі ботнету, який спричинив масовий шторм розподіленої атаки на відмову в обслуговуванні (Distributed Denial-Of-Service attack). Цілі високого рівня включали Krebs on Security, популярний блог безпеки в Інтернеті; Dyn, дуже популярний і широко використовуваний провайдер DNS для Інтернету; і Lonestar cell, великий оператор зв'язку в Ліберії. До менших цілей входили італійські політичні сайти та сервери Minecraft у Бразилії. DDoS на Dyn мав вторинні наслідки для інших надзвичайно великих провайдерів, які користувалися їхніми послугами, таких як сервери Sony Playstation, Amazon, GitHub, Netflix, PayPal, Reddit і Twitter. Загалом у рамках колективу ботнетів було заражено 600 000 пристроїв IoT [1].

Вихідний код Mirai був оприлюднений на хакерських форумах. З джерела та за допомогою слідів і журналів дослідники з’ясували, як діяла та розгорталася атака Mirai:

1. Сканування жертв: спочатку було виконано швидке асинхронне сканування за допомогою пакетів TCP SYN для перевірки випадкових адрес IPV4. Він спеціально шукав SSH/Telnet TCP-порт 23 і порт 2323. Якщо після сканування порт виявленно успішно, то відбувалося підключення та перехід на другу фазу.

Mirai містить жорстко закодований чорний список адрес, яких слід уникати. Чорний список складався з 3,4 мільйона IP-адрес і містив IP-адреси, що належать Поштовій службі США, Hewlett-Packard, GE і Міністерству оборони США. Mirai міг сканувати зі швидкістю близько 250 байт на секунду. Це відносно низький показник для ботнету. Атаки, як SQL Slammer генерував сканування зі швидкістю 1,5 Мбіт/с, головною причиною чого було те, що пристрої IoT зазвичай мають набагато більш обмежену потужність обробки, ніж настільні та мобільні пристрої.

2. З’єднання через Telnet: на цьому етапі Mirai намагався встановити функціональний сеанс Telnet із жертвою, надіславши випадковим чином 10

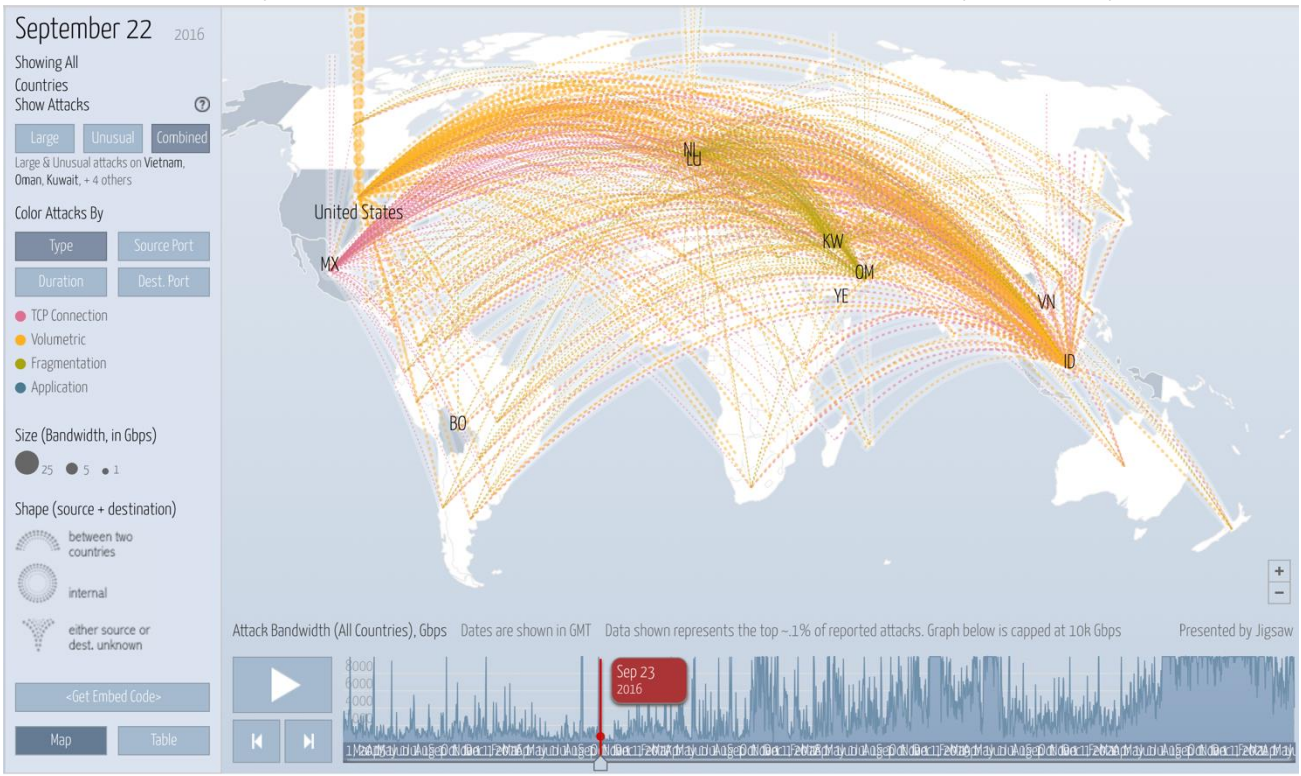
пар імені користувача та пароля, використовуючи атаку за списком із 62 пар. Якщо вхід був успішним, Mirai зареєструвала хост на центральному сервері C2. Пізніші розробники Mirai розвинули бота для запуску видалення виконаного коду.

3. Інфікувати: програма-завантажувач була відправлена потенційній жертві з сервера. Він відповідав за ідентифікацію операційної системи і інсталяцію шкідливого програмного забезпечення для конкретного пристрою. Потім він шукав інші конкуруючі процеси за допомогою порту 22 або 23 і вбивав їх (разом з іншим шкідливим програмним забезпеченням, яке вже могло бути присутнім на пристрої). Потім двійковий файл завантажувача було видалено, а ім'я процесу було замасковано, щоб приховати його присутність. Зловмисне програмне забезпечення не зберігалося в постійному сховищі та не вимагало перезавантаження. Тепер бот перебував у стані бездіяльності, доки не отримав команду на атаку.

Цільові пристрої складалися з IP-камер, відеореєстраторів, побутових маршрутизаторів, телефонів VOIP, принтерів і приставок. Вони складалися з 32-розрядних ARM, 32-розрядних MIPS і 32-розрядних двійкових файлів зловмисного програмного забезпечення X86, тобто мали специфічні складові для успішної атаки [2].

Перше сканування було здійснено 1 серпня 2016 року з веб-сайту хоста в США. Сканування тривало 120 хвилин, перш ніж було знайдено хост із відкритим портом і паролем у списку. Через одну додаткову хвилину було заражено ще 834 пристрої. Протягом 20 годин було заражено 64 500 пристроїв. Mirai розповсюджувався за 75 хвилин. Більшість заражених пристроїв, які перетворилися на ботнети, були розташовані в Бразилії (15,0%), Колумбії (14,0%) і В'єтнамі (12,5%), хоча цілі DDoS-атак були в інших регіонах.

Шкода була обмежена DDoS-атаками. Атаки відбувалися у вигляді



SYN-флудів, GRE IP-флудів, STOMP-флудів і DNS-флудів. Протягом п'яти місяців 15 194 окремих команд атаки були видані серверами C2 і вразили 5 042 Інтернет-сайти. 21 вересня 2016 року ботнет Mirai здійснив масову DDoS-атаку на сайт блогу Krebs on Security і згенерував трафік 623 Гбіт/с. Це стало найгіршою DDoS-атакою за всі часи [3].

Рис. 1. Розповсюдження атаки Mirai DDoS на Krebs on Security

Stuxnet був першою відомою задокументованою кіберзброєю, випущеною для довгострокового пошкодження активів Ірану. У цьому випадку це був хробак, який був випущений, щоб пошкодити програмовані логічні контролери Siemens (PLC) на базі SCADA та використовував прописаний шлях для зміни швидкості обертання двигунів під безпосереднім керуванням програмованого логічного контролеру. Розробники зробили все можливе, щоб гарантувати, що вірус буде націлений лише на пристрої зі швидкістю обертання підлеглих приводів зі змінною частотою, підключених до ПЛК Siemens S7-300, що обертаються на 807 Гц і 1210 Гц, оскільки вони зазвичай використовуються для насосів і газових центрифуг для збагачення урану [4].

Імовірно, атака почалася в квітні або березні 2010 року. Процес зараження відбувався за такими кроками:

1. Початкове зараження: хробак розпочався з зараження хост-машини

на операційній системі Windows, використовуючи вразливості, виявлені під час попередніх вірусних атак. Вважається, що він поширився через вставлення USB-накопичувача в пристрої. Він використовував чотири експлойти нульового дня одночасно (безпрецедентний рівень складності). Експлойти використовували руткіт-атаку з використанням коду режиму користувача та режиму ядра та встановлювали викрадений, але належним чином підписаний та сертифікований драйвер пристрою від Realtek. Цей підписаний драйвер режиму ядра був необхідний, щоб приховати Stuxnet від обережних антивірусних пакетів.

2. Атака та поширення: після встановлення через руткіт хробак

почав шукати в системі Windows файли, типові для контролера Siemens SCADA, WinCC/PCS 7 SCADA, також відомого як Step-7. Якщо хробак знаходив програмне забезпечення для керування Siemens SCADA, він намагався отримати доступ до Інтернету через C2, використовуючи неправильні URL-адреси, щоб завантажити новіші версії свого програмного забезпечення. Потім він заглибився у файлову систему, щоб знайти файл під назвою #7otbdx.dll, який служив критичною бібліотекою зв’язку між машиною Windows і програмованим логічним контролером. Stuxnet встав між системою WinCC і s7otbdx.d11, щоб діяти як зловмисник-посередник. Вірус почав свою роботу із запису нормальної роботи центрифуг.

3. Знищення: коли він вирішив скоординувати атаку, він відтворив

попередньо записані дані в системах SCADA, у яких не було підстав вважати, що щось скомпрометовано або поводиться нестабільно. Stuxnet завдав шкоди, маніпулюючи програмованими логічними контролерами двома різними

скоординованими атаками, щоб пошкодити весь масив іранського об’єкта. Пошкодження роторів центрифуги відбувалося повільно з часом, з кроком у 15 або 50 хвилин, розділених 27 днями нормальної роботи. Це призвело до неправильного збагачення урану, а також до тріщин і руйнування роторних труб у центрифугах.

Вважається, що понад 1800 центрифуг для накопичення урану були виведені з ладу та пошкоджені в результаті нападу на головний іранський завод зі збагачення в Натанзі, Іран [5].

Ланцюгова реакція — це наукове дослідження, яке демонструє новий тип кібератак, зосереджених на сітчастих мережах PAN, які можна виконати без будь-якого підключення до Інтернету. Крім того, це показує, наскільки вразливими можуть бути віддалені датчики та системи керування. Вектором атаки були лампочки Philips Hue, як правило, в будинках споживачів, якими можна керувати через Інтернет і додатки для смартфонів. Експлойт можна масштабувати до атак на розумне місто та ініціювати, просто вставивши один інфікований розумний світильник [6].

Світильники Philips Hue використовують протокол Zigbee для встановлення сітки. Системи освітлення Zigbee підпадають під програму під назвою Zigbee Light Link (ZLL), щоб забезпечити стандартний метод взаємодії освітлення. Повідомлення ZLL не шифруються та не підписуються, але шифрування використовується для захисту ключів, якими обмінюються, якщо до сітки додається індикатор. Цей головний ключ відомий кожному в альянсі ZLL, і згодом стався витік. ZLL також змушує лампочки, що приєднуються до сітки, бути дуже близько до ініціатора. Це запобігає захопленню ліхтарів сусіда. Zigbee також пропонує метод бездротового перепрограмування; однак пакети мікропрограми зашифровані та підписані.

План атаки складався б з чотирьох етапів:

1. Атака порушила б шифрування та підпис пакета прошивки бездротового перепрограмування.
2. Він напише та розгорне зловмисне оновлення мікропрограми до однієї лампочки з використанням зламаних ключів шифрування та підпису.
3. Зламана лампочка приєднається до мережі на основі вкраденого головного ключа та використає безпеку близькості через виявлений дефект нульового дня в широко використовуваній частині Atmel AtMega.
4. Після успішного приєднання до сітки Zigbee він надсилає файли сусіднім джерелам світла та швидко їх заражає. Це розширилося б на основі теорії перколяції та заразило б усі міські популяції систем освітлення.

Zigbee використовує AES-CCM для шифрування оновлень мікропрограми бездротового перепрограмування. Щоб зламати шифрування мікропрограми, зловмисники використовували кореляційний аналіз потужності і диференціальний аналіз потужності.

Це складна форма атаки, коли такий пристрій, як апаратне забезпечення контролера лампочки, розміщується на столі та вимірює потужність, яку він споживає. Завдяки складному контролю можна виміряти динамічну

потужність, яку використовує центральний процесор, що виконує інструкцію або переміщує дані (наприклад, коли виконується алгоритм шифрування). Це називається простим аналізом потужності, у якому все ще дуже важко зламати ключ.

Замість того, щоб намагатися визначити один біт за раз під час злому ключа, кореляційний аналіз потужності може розрізняти побайтові величини. Сліди потужності фіксуються осцилографом і розбиваються на два набори. Перший набір припускає, що проміжне значення, яке зламано, встановлено на 1, а інший набір припускає, що воно встановлено на 0. Віднімаючи середнє значення цих наборів, виявляється справжнє значення проміжного значення [7, с. 388–397].

Використовуючи як диференціальний аналіз потужності, так і кореляційний аналіз потужності, дослідники зламали систему освітлення Philips Hue наступним чином:

1. Дослідники використовували кореляційний аналіз потужності для зламу AES-CBC. Зловмисники не мали ні ключа, ні вектора ініціалізації.
2. Вони використали диференціальний аналіз потужності, щоб зламати

режим лічильника AES-CTR, щоб порушити шифрування комплекту програмного забезпечення. Дослідники виявили 10 локацій, які, здавалося, виконує AES-CTR, що створює в 10 разів більше можливостей.

3. Потім вони зосередилися на зламі захисту Zigbee Proximity для

приєднання до мережі. Експлойт нульового дня був результатом перевірки вихідного коду Atmel для завантажувача на системі на чипі. Переглянувши код, вони виявили, що перевірка близькості була дійсною під час запуску запиту на сканування в Zigbee. Якщо вони почали з будь-якого іншого повідомлення, перевірку близькості було б пропущено. Це дозволяло їм приєднуватися до будь-якої мережі.

Справжня атака може змусити інфіковану лампочку заразити інші в радіусі кількох сотень метрів корисним навантаженням, щоб усунути можливість оновлення мікропрограми кожної лампочки, щоб їх ніколи не можна було відновити. Пристрої фактично опинилися б під зловмисним контролем і повинні бути знищені. Дослідники змогли побудувати повністю автоматизовану систему атаки та під'єднати її до дрона, який систематично літав у радіусі освітлення Philips Hue в середовищі кампусу та захоплював кожен з них.

Перелік посилань:

1. Приклад із атаки ботнету Mirai 2016 року. URL: https://medium.com/@d21dcs151/a-case-study-on-mirai-botnet-attack-of-2016-4b66630e6508
2. Новий вид ботнету Mirai «Okiru» шукає набір на основі ARM. URL: https://www.theregister.com/2018/01/16/arc_iot_botnet_malware/
3. The internet of stings. URL: https://www.economist.com/science-and-technology/2016/10/08/the-internet-of-stings
4. Stuxnet: A Breakthrough. URL: https://community.broadcom.com/symantecenterprise/communities/community home/librarydocuments/viewdocument?DocumentKey=550505c5-c38a-4e0c-b590-f731bb3a60ad&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

5. Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report. URL: https://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/8
6. Hacked Cameras, DVRs Powered Today's Massive Internet Outage. URL: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/
7. Differential Power Analysis: підручник / P. Kocher, J. Jaffe, B. Jun. – San Francisco “Cryptography Research”, 1999. – С. 388–397

Катков Юрій Ігорович
доктор технічних наук, професор кафедри комп’ютерних наук,
ННІТ, ДУІКТ, Київ, Україна,
Щербаков Євген Миколайович,
студент групи КНДМ-61, ННІТ, ДУІКТ, Київ, Україна.

АНАЛІЗ КРИТИЧНОСТІ ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ МЕТОДІВ КІБЕРБЕЗПЕКИ ПІД ЧАС МОДЕЛЮВАННЯ РОЗПІЗНАВАННЯ ДОРОЖНЬОЇ СИТУАЦІЇ

Анотація. На основі систем машинного навчання створюються моделі моделювання розпізнання дорожніх ситуацій. Ці моделі забезпечують: аналіз зображень з камер та інших сенсорів для виявлення перешкод, інших транспортних засобів, пішоходів та дорожніх знаків; обробку даних від лідара, радара та інших сенсорів, щоб створити точну модель оточення; прогнозування динаміки руху транспортних засобів і пішоходів. Але системи машинного навчання можуть зазнавати різні види атак для обману цих моделей або підриву їхньої ефективності. Такі атаки особливо небезпечні в контексті створення або розпізнання критичних дорожніх ситуацій. Тому виникає завдання метою якого є - визначення відносно процесу моделювання розпізнання дорожніх ситуацій: критичного впливу механізмів атак на систему машинного навчання; підходів щодо виявлення цих атак; рекомендацій щодо захисту системи машинного навчання від цих атак. Ключові слова: моделювання, машинне навчання, кібербезпека.

І. Критичній вплив механізмів атак на систему машинного навчання:

На систему машинного навчання може бути атаки [1,2]. Кожен вид атак має свої особливості механізмів критичного впливу. Тому розглянемо [3,4,5]:

1. Атаки під час навчання (Poisoning Attacks). Цей тип атак відбувається під час етапу навчання моделі. Основна мета атаки – включити шкідливі або неправильні дані в навчальний набір, що призводить до створення моделі з помилковими висновками. Механізм дії атак наступний: 1) *Підміна даних навчання*: зловмисник додає до навчального набору шкідливі приклади, що спонукають модель робити неправильні прогнози на певні типи вхідних даних; 2) *Підміна метаданих*: може включати зміну стандартних форм (етикеток, ярликів) або категорій даних, що спонукає модель навчатися на хибних зв'язках. Наприклад, у системі розпізнавання дорожніх знаків зловмисник додає в навчальні дані приклади неправильно класифікованих знаків (наприклад, стандартна форма знаку "Стоп" помічено як "Обмеження швидкості"), що призводить до помилкової інтерпретації знаків під час використання моделі в реальному житті.

2. Адаверсаріальна атака (adversarial attacks) чи атака на етапі використання (Evasion Attacks). Ця атака спрямована на введення специфічне підготовлених вхідних даних, щоб модель зробила неправильний висновок під час використання. Механізм дії таких атак наступний. Зловмисник вносить адаверсаріальні дані. Це дані схожі на звичайні, але при цьому призводять до серйозних помилок класифікації. Вони спеціально підібрані щоб змінити вхідні дані, які не помітні для людини, але вводять модель в оману. Приклад її дії наступний. Невелика зміна в зображенні дорожнього знаку "Стоп" (наприклад, кілька пікселів) може зробити так, що модель більше не розпізнає знак правильно, навіть якщо для людини він виглядає як звичайний "Стоп".

3. Модельні атаки (Model Inversion і Model Extraction). Ці атаки орієнтовані на отримання конфіденційної інформації з моделі машинного навчання або її точного копіювання. Існує дві моделі таких атак: *Model Inversion (інверсія моделі),* коли зловмисник намагається відновити вхідні дані або їхні характеристики на основі вихідних прогнозів моделі - це дозволяє зловмиснику отримати конфіденційні дані; *Model Extraction (витяг моделі)*, коли зловмисник намагається клонувати модель, надсилаючи до неї запити й аналізуючи вихідні результати - це дозволяє зловмиснику створити копію оригінальної моделі без доступу до внутрішньої структури або алгоритмів.

4. Атаки зворотного зв'язку (Backdoor Attacks). Цей тип атак передбачає інтеграцію спеціального тригера або "бекдора" в модель під час навчання, який залишається неактивним, доки не з'явиться специфічний сигнал або вхідні дані, які активують шкідливу поведінку моделі. Приклад дії наступний. Зловмисник може додати спеціальний малюнок або об'єкт у навчальні дані, який модель буде ігнорувати під час нормальної роботи. Проте, коли цей малюнок з'явиться в реальних даних, модель починає робити помилки або слідувати заданим інструкціям.

5**. Атаки з перекласифікацією (Label Flipping Attacks).** У цьому випадку зловмисник спеціально змінює етикетки (ярлики) в навчальному наборі, що може ввести модель в оману. Це може трапитися через внутрішні витоки даних або навмисну зміну ярликів у великих базах даних, що використовуються для навчання.

ІІ. Методи виявлення атак на систему машинного навчання.

Виявлення атак на систему машинного навчання та сенсори є важливим етапом забезпечення їх безпеки. Оскільки атаки можуть бути складними і прихованими, їх виявлення вимагає застосування різноманітних методів. Існують наступні підходи і технології для виявлення атак:

1. Методи аналізу аномалій (Anomaly Detection). Аномальні шаблони можуть вказувати на атаку, особливо якщо вхідні дані раптово змінюються або виглядають незвично порівняно зі звичайними даними. Для виявлення аномалій використовують такі методи: a) *Кластеризація:* розділення вхідних даних на групи, де аномалії виявляються як точки, що не належать жодній групі; b) *Статистичний аналіз:* обчислення відхилень, середнього та інших

статистичних показників для оцінки нормальності вхідних даних; c) *Метод автоенкодери (autoencoders):* виявлення незвичайних шаблонів у вхідних даних чи виявлення аномалій через відмінності між вихідними і вхідними даними. Наприклад, для виявлення атаки на систему камер автомобіля можна тренувати модель на базових візуальних даних і виявляти будь-які незвичайні варіації, що можуть бути наслідком атаки, наприклад, маніпуляція зображенням.

2. Метод моніторингу на рівні сенсорів. Сенсори є частиною системи машинного навчання. Регулярний моніторинг сенсорних сигналів на наявність нестандартних або дивних поведінкових шаблонів допомагає виявити атаки на рівні апаратного забезпечення або комунікацій між сенсорами наступних видів: a) *детектування фізичних впливів:* наприклад, виявлення сторонніх електромагнітних впливів на датчики або порушення нормальних фізичних характеристик сигналів (як у випадку з акустичними або лазерними атаками); b) *Порівняння між сенсорами*: якщо система використовує кілька сенсорів для збору даних (наприклад, камера та лідар), результати одного сенсора можна порівняти з іншим для виявлення невідповідностей. Наприклад, якщо дані з GPS і лідара не збігаються під час руху транспортного засобу, це може свідчити про атаку на GPS (спуфінг). В цьому випадку можна активувати додаткові перевірки для підтвердження реальності координат.

3. Метод виявлення атаки на основі сигнатур (Signature-Based Detection). Цей підхід полягає у використанні попередньо відомих моделей або "сигнатур" атак. Для виявлення атаки аналізують вхідні дані та порівнюють їх з відомими шаблонами атак. Це ефективно для виявлення вже відомих атак. Тому створюються *бази даних сигнатур* - такі системи використовують бази даних з прикладами типових атак, що дозволяє швидко їх розпізнавати, якщо атака відома заздалегідь. Але є недолік: цей підхід менш ефективний проти нових або невідомих атак, оскільки бази даних сигнатур не можуть містити інформацію про них.

4. Метод аналізу взаємодії між компонентами системи машинного навчання. У багатьох системах машинного навчання з використанням сенсорів дані передаються між різними компонентами (дані, алгоритм оптимізації, модель, особливості (Features), навчання (Training), перевірка (Validation), тестування (Testing), гіперпараметри (Hyperparameters), результати (Predictions/Outputs)). Ці компоненти працюють разом для створення системи, здатної автоматично вчитися на основі даних і приймати обґрунтовані рішення чи передбачення. Атака може бути виявлена через порушення нормальної послідовності або інтенсивності взаємодії між ними. Тому виконується: a) *аналіз комунікацій*: вивчення обміну даними між сенсорами та центральною системою для виявлення аномальних або підозрілих запитів; b) *перевірка автентичності даних*: використання криптографічних методів для верифікації автентичності вхідних даних або сигналів від сенсорів. Наприклад, перевірка автентичності сигналів від датчиків руху може допомогти виявити маніпуляції, такі як відправлення фальшивих даних від датчика, що був атакований.

5. Метод моніторингу поведінки моделі (Model Behavior Monitoring). Цей підхід орієнтований на виявлення аномальних рішень, які робить модель машинного навчання, що може свідчити про атаку або несправність. Він дозволяє виконувати: перевірку вихідних результатів моделі на основі очікуваних результатів; порівняння між результатами різних моделей для виявлення спроби обману. Наприклад, якщо автономний автомобіль починає приймати несподівані або дивні рішення (наприклад, різко змінювати швидкість або рухатись непередбачувано), це може бути ознакою атаки на сенсори або модель машинного навчання. Для виявлення таких дій можна порівняти поведінку з раніше тренованими шаблонами.

6. Метод диференційованої приватності (Differential Privacy). Цей підхід дозволяє захищати дані і модель від атак через додавання випадкових шумів до вхідних даних або результатів моделі. Це ускладнює спроби виявити конфіденційну інформацію або маніпулювати моделлю. Метод призначеній для: a) *Анонімізації даних*: допомагає захистити від атак, спрямованих на витяг інформації про окремі дані з навчальної моделі; b) *Захисту від "модельних інверсій":* запобігає зловмисникам у відтворенні приватних даних на основі поведінки моделі.

7. Метод фізична безпека сенсорів. Іноді атака може бути пов'язана з фізичним доступом до сенсорів або їх зламом. Важливо контролювати доступ до пристроїв і використовувати методи захисту на рівні апаратного забезпечення, а саме: a) *Фізичного екранування* сенсорів для захисту від електромагнітного випромінювання або лазерних атак; b) *Антивандальні корпуси* для захисту сенсорів від фізичного втручання.

8. Метод мультисенсорного підтвердження (Sensor Fusion Validation). Системи, які використовують кілька сенсорів для збору даних (наприклад, автономні автомобілі з камерами, лідарами, радарами), можуть використовувати взаємопідтвердження для виявлення аномалій. Якщо один сенсор "бачить" щось підозріле, але інші не підтверджують це, це може свідчити про атаку на один із сенсорів. Наприклад, якщо камера автомобіля виявляє пішохода, але лідар або радар не підтверджують його наявність, це може бути ознакою атаки на камеру.

III. Рекомендації щодо захисту системи машинного навчання від атак

Захист моделей машинного навчання від атак є важливою задачею, особливо в контексті систем, де критичною є точність і безпека, якими є автономні транспортні засоби. Існує кілька методів захисту моделей машинного навчання від різних типів атак, включаючи атаки на навчання, використання, і отримання конфіденційних даних.

Основні підходи до захисту моделей машинного навчання від атак:

1. Адаверсаріальне навчання (Adversarial Training). Це один із найефективніших методів захисту від адаверсаріальних атак (evasion attacks). Суть полягає у тому, що під час навчання моделі до навчального набору додають спеціально створені шкідливі приклади (адаверсаріальні приклади).

Це робить модель стійкішою до малих змін у вхідних даних.

2. Регуляризація та обмеження складності моделі. Складні моделі (особливо нейронні мережі з великою кількістю параметрів) більш вразливі до атак. Щоб зменшити ризик, можна використовувати методи регуляризації: a) *L2- та L1-регуляризація*, яка допомагають зменшити ризик перенавчання моделі і роблять її менш чутливою до аномальних входів; b) *Dropout і Noise Injection* (введення випадкових шумів у дані або параметри під час навчання) роблять модель стійкішою до невеликих варіацій у вхідних даних.

3. Фільтрація та очищення даних (Data Sanitization). Атаки на етапі навчання (poisoning attacks) часто використовують підміну даних, щоб порушити роботу моделі. Важливо фільтрувати та очищати дані перед їх використанням для навчання наступними методами: *Аналіз даних на аномалії*, що може виявити потенційно шкідливі приклади, які відрізняються від основного набору; b) *Перевірка даних* на валідність та достовірність, особливо якщо дані отримуються з різних відкритих джерел.

4. Захист навчального набору (Training Data Protection). Якщо зловмисник має доступ до навчальних даних, він може модифікувати або додати шкідливі приклади. Ось кілька способів захисту: a) *Хешування даних:* використання криптографічних хешів для перевірки цілісності даних; b) *Шифрування*: використання шифрування для зберігання навчальних даних або їх передачі; c) *Контроль доступу*: обмеження доступу до даних лише для авторизованих користувачів.

5. Стійкі алгоритми та захищені архітектури. Для цього треба застосовувати наступні методи: a) *Захищені варіанти моделей*: можна використовувати стійкі до атак алгоритми, які розроблені спеціально для забезпечення захисту від певних типів атак, наприклад **Tree Ensembles** або деякі варіанти нейронних мереж; b) *Differential Privacy (диференційована приватність):* цей метод дозволяє додавати шум до даних, що використовуються для навчання, щоб зменшити можливість витоку інформації про конкретні приклади.

6. Model Watermarking (Водяні знаки на моделі). Цей метод дозволяє вбудовувати у модель специфічний «водяний знак», щоб перевіряти легітимність моделі та виявляти її копії або несанкціоноване використання. Водяний знак може бути прихованим патерном, який модель розпізнає лише під час виконання певного запиту.

7. Моніторинг і виявлення аномалій. Запуск системи в реальному часі може включати постійний моніторинг її роботи на предмет аномальних поведінкових шаблонів, які можуть свідчити про атаку. Він може отримувати дані на основі аналіз трафіку та вхідних даних на аномалії, а також виявлення аномальних патернів у результатах моделі, що можуть сигналізувати про атаки з зовнішніх джерел або спроби введення шкідливих даних.

8. Ensemble Models (Ансамблі моделей). Використання ансамблю різних моделей може забезпечити додатковий захист. Якщо одна модель вразлива до атаки, інші моделі в ансамблі можуть "перекрити" її помилки. В результаті, ансамбль моделей стає менш вразливим до атак на одну конкретну модель.

9. Backdoor Defense (Захист від атак із використанням бекдорів). Для запобігання атакам, що використовують бекдори (задні двері), можна застосовувати такі методи: a) *Оцінка поведінки моделі при введенні рідкісних або специфічних входів* для виявлення прихованих тригерів; b) тестування моделей на наявність бекдорів перед їх розгортанням.

10. Аудит і валідація моделей. Періодичний аудит моделей і тестування на наявність вразливостей може виявити слабкі місця ще до того, як вони будуть використані зловмисниками. Також важливо регулярно проводити: a) *Пенетраційне тестування* моделей, імітуючи атаки, щоб виявити їхні слабкі місця; b) *Тестування на стійкість* моделі до різних видів атак та аномальних вхідних даних.

11. Контроль доступу до моделі. Обмеження доступу до самої моделі є важливим фактором для забезпечення безпеки. Для цього треба виконувати: a) *Авторизацію та автентифікацію користувачів*, які можуть взаємодіяти з моделлю; b) *Шифрування запитів* до моделі та її відповідей для захисту від підслуховування та підміни.

Висновки

Для виявлення атак на систему машинного навчання потрібен комплексний підхід, який поєднує різні методи, такі як аналіз аномалій, моніторинг сенсорних сигналів, верифікація даних і мультисенсорне підтвердження. Кожна система потребує індивідуального налаштування методів безпеки, в залежності від її призначення, щоб мінімізувати ризики та вчасно виявляти атаки.

Захист від атак на систему машинного навчання може використовуватися наступні методи: адаптація моделей (використання методів регуляризації або алгоритмів, стійких до атак, таких як защищене навчання (secure learning)); фільтрація даних (перевірка і очищення даних перед навчанням моделі); аналіз на наявність аномалій (виявлення нестандартних патернів у вхідних даних або вихідних результатах); адаверсаріальне навчання (включення шкідливих прикладів у навчальний процес для підвищення стійкості моделі до подібних атак).

Захист моделей машинного навчання від атак — це багаторівнева задача, яка вимагає поєднання кількох методів і підходів. Ефективний захист залежить від глибокого розуміння можливої загрози, постійного моніторингу та використання захищених алгоритмів і інфраструктури. Таким чином, атаки на систему машинного навчання стають все складнішими, і для їхнього запобігання необхідно розробляти нові підходи та інструменти захисту моделей.

Перелік посилань:

1. Traffic Monitoring Solutions/ [Електронний ресурс] / режим доступу: https://asuratechnologies.com/solutions/traffic-monitoring-solutions/?utm_campaign=21353082681&adgroupid=160085175021&utm_source=google&utm_term=traf

fic%20control&gad_source=1&gclid=Cj0KCQjwmt24BhDPARIsAJFYKk2WCS08Ypt3udAPTli81UPiqsBV1qKnGBq3RDMpj6o2TIYqIdtJqeAaAmpAEALw_wcB / (date of access: 20.10.2024).
2. Generic Probabilistic Interactive Situation Recognition and Prediction: From Virtual to Real / [Електронний ресурс] / режим доступу: https://ieeexplore.ieee.org/document/8569780 / (date of access: 20.10.2024)
3. *E. Anthi, L.Williams, M.Rhode, P.Burnap, A.Wedgbury* Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems/ [Електронний ресурс] / режим доступу: https://www.sciencedirect.com/science/article/pii/S2214212620308607/ (date of access: 20.10.2024)
4. *A.Paracha, J.Arshad, M. Ben* Machine learning security and privacy: a review of threats and countermeasures / EURASIP Journal on Information Security, Article number: 10 (2024)/ [Електронний ресурс] / режим доступу: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-024-00158-3/ (date of access: 20.10.2024)
5. *A Survey, T.Yusuke Kawamoto, K.Miyake, K. Konishi, Y. Oiwa* Threats Vulnerabilities, and Controls of Machine Learning Based Systems / [Електронний ресурс] / режим доступу: https://arxiv.org/pdf/2301.07474 / (date of access: 20.10.2024)
6. Threat Detection Methods and Best Practices - Snowflake/ [Електронний ресурс] / режим доступу: https://www.snowflake.com/guides/threat-detection-methods / (date of access: 20.10.2024)
7. Top 5 Methods of Protecting Data/ [Електронний ресурс] / режим доступу: https://www.titanfile.com/blog/5-methods-of-protecting-data / (date of access: 20.10.2024)

Щибун Євген Юрійович
Студент групи БСДМ-61 *ННІЗІ ДУІКТ, Київ, Україна*

АТАКИ НА ЛАНЦЮГ ПОСТАВОК SUPPLY CHAIN

Атака на ланцюг поставок – це кібератака, що здійснюється, використовуючи довіру між компанією-виробником та її клієнтами. [4-5]. Така атака завдає шкоду організації, з орієнтиром на слабкі місця у ланцюгу постачання. Зловмисник намагається атакувати один або кілька компонентів процесу розробки чи доставки поставок. Прикладом такої атаки є використовання підроблені чіпи, що задіяні у виробництві комп'ютера або мережевого обладнання. Або, атака може запровадити скомпрометований код у програмному засобі, що не викликає підозри. Є цілий ряд різних сценаріїв та методів, але головне, що ця атака використовує надійні канали для проникнення, щоб досягти своїх цілей. Розглянемо детально компоненти управління ланцюжком поставок [1], які показано на рис.1.

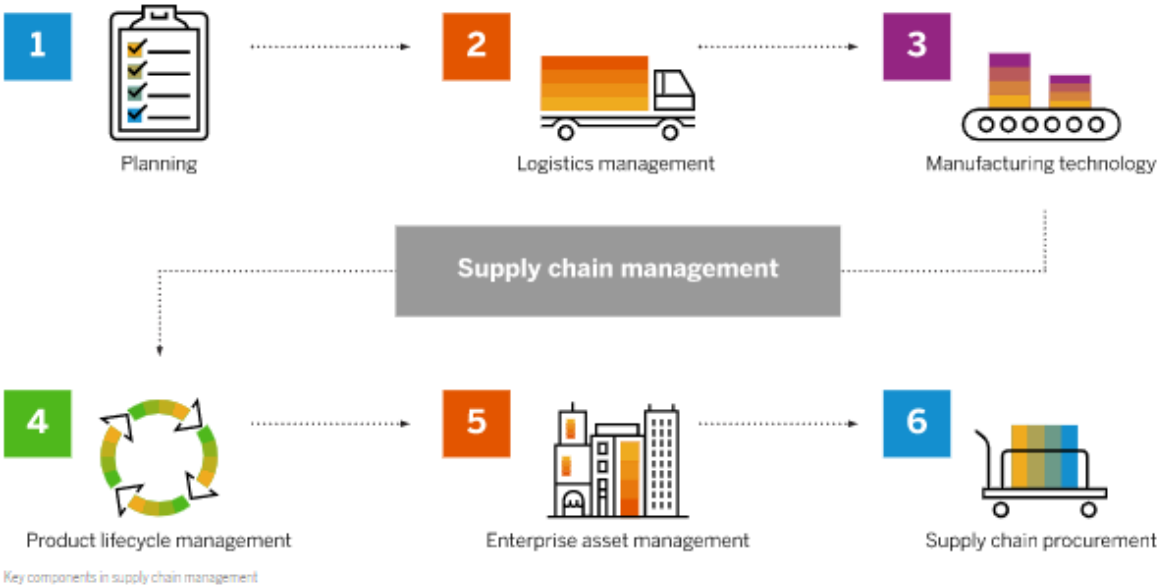


Рис.1. Компоненти управління ланцюжком поставок

Склад компонентів управління ланцюжком поставок :

- Планування ланцюжка поставок;
- Управління логістикою;
- Технологія виробництва;
- Управління життєвим циклом продуктів (PLM);
- Закупівлі в рамках ланцюжка постачання.

Визначено переваги управління ланцюжком постачання, а саме:

Зростання продуктивності. Системи управління активами підприємства та діагностичне обслуговування підвищують ефективність обладнання та систем.

Скорочення витрат на ланцюжок постачання. Прогнозна аналітика позбавляє необхідності гадати в умовах, коли кожна помилка може коштувати дуже дорого — жодних зайвих витрат на занадто великі запаси та ризики дефіциту.

Підвищення гнучкості та стійкості ланцюжка поставок. Тенденції та ситуація на ринку можуть змінитися будь-якої миті, тому велике значення мають стійкі системи SCM, здатні адаптуватися до будь-якої ситуації.

Підвищення якості продукції. Відділи досліджень та розробок отримують прямий доступ до відгуків покупців, що дозволяє проектувати продукти відповідно до потреб клієнтів.

Розглядаються наступні типи атак на ланцюг поставок:

Навмисна руйнівна установка (в тому числі заміна, зміна та впровадження шкідливого ПО) HW, SW або FW в критично важливі компоненти ІКТ.

Розглянуті часові рамки атак включають:

У будь-який час протягом життєвого циклу придбання системи, включаючи попереднє придбання, придбання або підтримку.

Проаналізувавши компоненти управління ланцюжком поставлок

віділено точки атаки в ньому, а саме:

розташування (див. рис. 2): місця розробки системи та програмного забезпечення і їхні внутрішні процеси та середовища; наприклад, інтегровані середовища розробки (IDE).

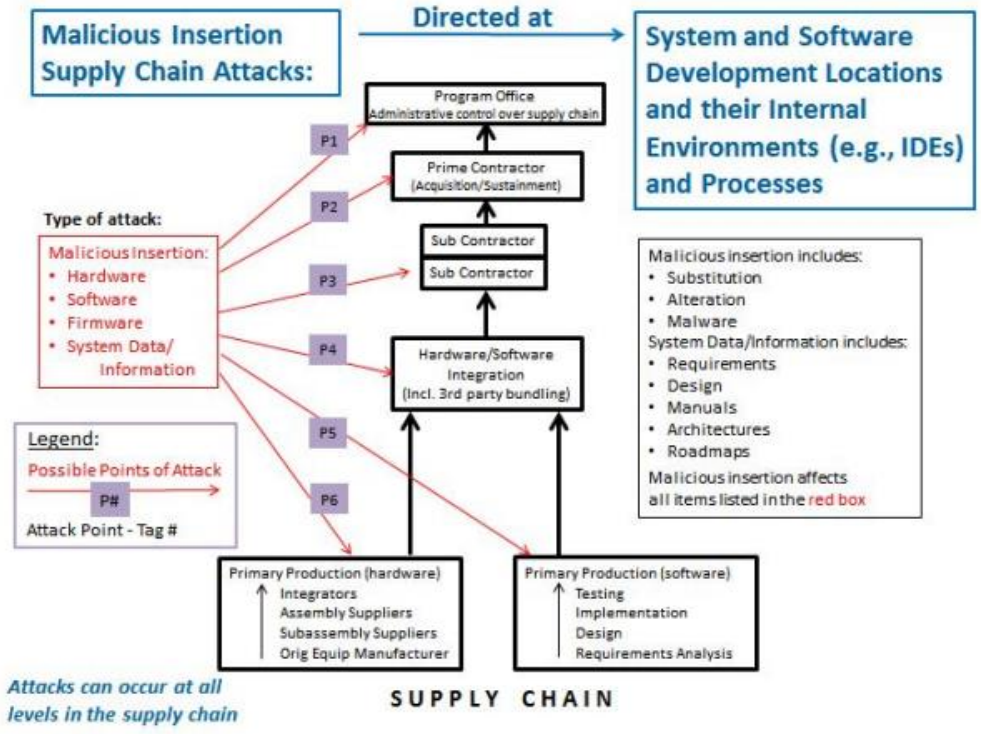


Рис.2. Точки атаки – розташування ланцюга поставок

- шкідлива діяльність, яка відбувається в будь-якому місці ланцюга поставок, включаючи інструменти розробки та процеси, що належать/використовуються цим сайтом/об’єктом.
- розташування ланцюга постачання включає офіс програми, головного підрядника та всі рівні субпідрядників/субпостачальників та інтеграторів (включені до цих категорій діяльність з підтримки на місцях; наприклад, склади запчастин та діяльність з підтримки програмного забезпечення; та їх постачальники).
- між місцями (див. рис. 2): зв'язки ланцюга поставок.
- шкідлива активність, яка відбувається у фізичному потоці між місцями ланцюга поставок (тобто логістичні мережі покупців і постачальників).
- шкідлива діяльність, яка відбувається в рамках потоку інформації та даних ланцюга поставок (тобто зовнішні ІКТ/IDE-середовища покупця та постачальника).

Перелік посилань:

1. Ланцюг поставок URL: https://www.sap.com/central-asia-caucasus/products/scm/what-is-supply-chain-management.html?url_id=text-central-asia-caucasus-404-reclink .

2. M. Blackmer. Attacking the Weakest Link in the Supply Chain — Cisco Blog изд. — 2023 URL: https://blogs.cisco.com/security/ attacking-the-weakest-link-in-the-supply-chain? dtid=osscdc000283.

3. P. Moorhead. That Time Of Year Again: Cisco Systems Releases Its Annual Cybersecurity Report — Forbes. — 2018. URL: https:// www.forbes.com/sites/patrickmoorhead/2018/ .

4. Cyber-security risks in the supply chain — Cert-uk вид. — 2021. URL: https://www. cert.gov.uk/wp-content/uploads/2015/02/ Cyber-security-risks-in-the-supply-chain .

5. R. WAUGH. The terrifying rise of cyber crime: Your computer is currently being targeted by criminal gangs looking to harvest your personal details and steal your money. — Mail Online вид. — 2013. URL: https://www.dailymail. co.uk/home/moslive/article-2260221/ Cyber-crime-Your-currently-targeted-criminal-gangs-lohtml.

Юрик Дмитро
студент групи БСД-11

Антивірусні та антишпигунські програми

Для захисту даних і пристроїв комп'ютера від шкідливих програм використовують спеціальне програмне забезпечення – антивірусні програми.

Антивірусна програма — це програма, яка захищає пристрої від вірусів і шкідливого ПЗ. Вона виконує сканування файлів, виявляє загрози, блокує їх і видаляє. Антивірус також постійно стежить за підозрілою активністю і регулярно оновлює базу вірусів для захисту від нових загроз.

Сучасні антивірусні програми – це комплексні програми, що мають набір модулів для захисту від різних загроз. Крім комплексних програм, є програми для швидкого сканування комп'ютера на наявність шкідливих програм і їх знешкодження. Такі програми називають сканерами. Немає на 100% універсальних антивірусів. Це пояснюється постійною появою нових вірусів та загроз.

Основні завдання антивірусів:

- Сканування файлів: Перевірка на наявність вірусів.
- Виявлення загроз: Ідентифікація шкідливого ПЗ.
- Видалення шкідливих програм: Очищення системи.
- Моніторинг у реальному часі: Постійний захист від загроз.
- Оновлення баз: Підтримка актуальних вірусних сигнатур.

Якщо комплексну антивірусну програму встановлено на вашому комп'ютері, то під час увімкнення ПК вона буде однією з перших автоматично завантажуватися в оперативну пам'ять комп'ютера і виконувати операції з перевірки наявності шкідливих програм і блокування їх дій. При цьому в Області сповіщень з'явиться значок цієї програми. В останніх версіях операційної системи Windows програма антивірусного захисту Windows Defender (англ. захисник) входить до складу ОС, і перевірка системи на ураження шкідливими програмами здійснюється автоматично з певною періодичністю.

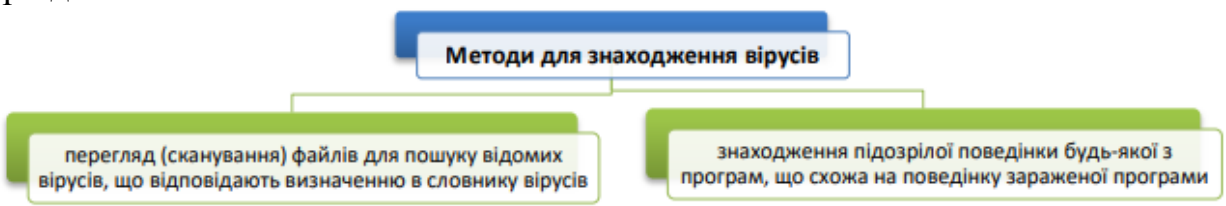


Рис.1

До популярних антивірусів належать такі програми, як Zillya!, Avira,

Bitdefender, AVG, Avast, ESET та ін.

Класифікація антивірусних програм

Антивірус	Опис
Детектори	Виявляють файли, заражені вірусами
Лікарі (фаги)	«Лікують» заражені програми або диски, видаляючи із заражених програм вірусний код
Ревізори	Спочатку запам'ятовують стан програм і дисків, а потім порівнюють їх поточний стан з попереднім і повідомляють про виявлені невідповідності
Фільтри	Перехоплюють ті звернення до системи, які віруси використовують для розмноження і заподіяння шкоди
Монітори	починають свою роботу при запуску операційної системи, постійно знаходяться в пам'яті комп'ютера і здійснюють автоматичну перевірку файлів
Вакцини	виконують імунізацію системи (файлів, каталогів), блокуючи дію вірусів

Рис.2

Антишпигунські програми — це тип захисного програмного забезпечення, яке спеціалізується на виявленні, блокуванні та видаленні шпигунського програмного забезпечення. Шпигунське ПЗ призначене для прихованого збору інформації про дії користувача без його відома, що може призвести до крадіжки персональних даних, паролів, фінансових даних або компрометації конфіденційності.

Як захистити свої дані від шпигунських програм?

За допомогою цих шкідливих програм зловмисники можуть здійснювати сканування файлів на жорсткому диску, отримувати інформацію про веб-сайти, які відвідував користувач та викрадати паролі або номери рахунків під час їх введення. Саме тому спеціалісти ESET рекомендують використовувати рішення з модулем Антишпигун. Функція Антишпигун забезпечує надійний захист даних від несанкціонованого доступу зловмисників.

Основні функції антишпигунських програм:

1. **Виявлення шпигунських програм**: Антишпигунське ПЗ сканує систему для виявлення програм, які можуть таємно відслідковувати діяльність користувача, наприклад, записувати натискання клавіш (кейлогери) або збирати інформацію про інтернет-активність.
2. **Захист від крадіжки особистих даних**: Антишпигунські програми блокують спроби шпигунського ПЗ викрасти особисті або фінансові дані (наприклад, паролі, дані кредитних карток, логіни).
3. **Моніторинг системи в реальному часі**: Ці програми постійно відстежують активність у системі, щоб виявити підозрілу поведінку, яка може свідчити про спробу зібрати конфіденційну інформацію.
4. **Запобігання встановленню небажаних програм**: Вони захищають пристрої від встановлення шпигунських програм через вразливості в програмах або заражені файли.
5. **Очищення системи**: Антишпигунське ПЗ не лише виявляє загрози, а й видаляє шпигунське програмне забезпечення, запобігаючи подальшому шпигунству.

6. **Оновлення баз загроз**: Регулярні оновлення гарантують, що програма може виявляти новітні види шпигунського ПЗ, оскільки ці загрози постійно еволюціонують.

Приклади антишпигунських програм:

- **Malwarebytes**: Популярний інструмент для виявлення та видалення різних типів шпигунських програм.
- **Spybot Search & Destroy**: Відомий своєю ефективністю у боротьбі зі spyware, особливо рекламним ПЗ.
- **SUPERAntiSpyware**: Ще одне ефективне рішення для захисту від шпигунського та рекламного ПЗ

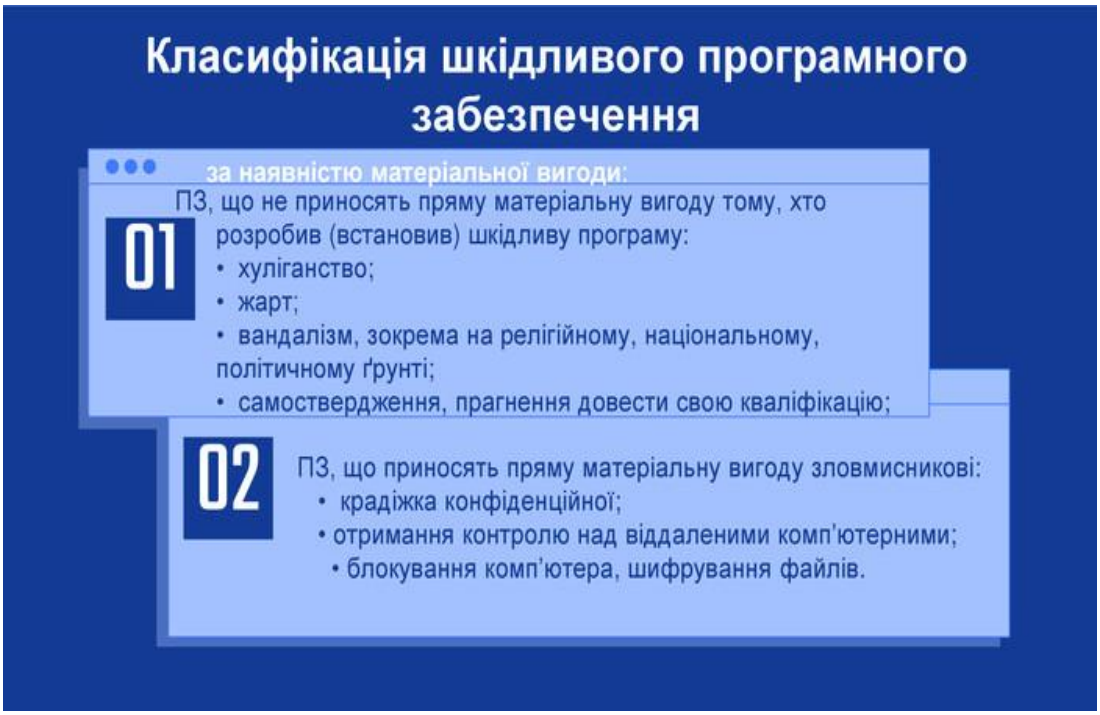


Рис.3

Антивірусні та антишпигунські програми є необхідними інструментами для забезпечення безпеки комп'ютерних систем та захисту особистої інформації. В умовах постійно зростаючих кіберзагроз їх використання стає надзвичайно актуальним, а свідомий вибір та належне використання цих програм можуть значно знизити ризики.

Перелік посилань:

https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D1%96%D1%80%D1%83%D1%81%D0%BD%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0

Воротняк Микита Олегович
Студент групи БСДМ-62 *ННІЗІ ДУІКТ, Київ, Україна*
Юхимович Анатолій Васильович
Студент групи БСДМ-63 *ННІЗІ ДУІКТ, Київ, Україна*
Селітрарь Олександр Олександрович
Студент групи БСДМ-63 ННІЗІ ДУІКТ, Київ, Україна

ПІДХОДИ ДО УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

Привілейований доступ все частіше використовується організаціями щоб захищати свою інфраструктуру та ефективно вести свій бізнес. Використання технологій привілейованого доступу надає захист конфіденційним даним та ключовій інфраструктурі. Ризик безпеки, пов'язаний з привілеями, в сучасних бізнес-середовищах швидко зростає. Це відбувається оскільки системи, додатки, хмарні середовища, гібридні середовища, DevOps, автоматизація процесів і роботи IoT стають все більш взаємопов'язаними. Сьогодні майже всі складні атаки засновані на привілейованих облікових даних для доступу до найбільш конфіденційних даних, служб та інфраструктури. Привілейований доступ може підірвати роботу компанії, якщо їм будуть зловживати.

У сучасних умовах розвитку інформаційних технологій забезпечення кібербезпеки інформаційних систем організацій є однією з ключових проблем. Привілейований доступ надається користувачам, що виконують критичні функції з управління інфраструктурою та конфігурацією інформаційної системи, тому контроль над таким доступом є важливим для запобігання витокам даних, несанкціонованому доступу та іншим видам кіберзлочинів. Розглянемо основні підходи до управління привілейованим доступом, які включають впровадження політик мінімальних прав, багаторівневої автентифікації, моніторинг дій та автоматизацію управління доступами (рис.1).

1. Політика мінімальних привілеїв

Принцип мінімальних привілеїв (Least Privilege Principle) є основою ефективного управління привілейованим доступом. Така політика передбачає надання користувачам лише тих прав доступу, які необхідні для виконання конкретних завдань. Це зменшує ризик зловживань та випадкових помилок, які можуть призвести до небажаних наслідків, таких як зміни в конфігурації системи або доступ до конфіденційної інформації. Політика мінімальних привілеїв дозволяє скоротити поверхню атак і обмежує можливість компрометації системи через привілейовані облікові записи.

2. Багаторівнева автентифікація

Використання багаторівневої автентифікації (Multi-Factor Authentication, MFA) є важливим компонентом забезпечення безпеки доступу до привілейованих облікових записів. MFA вимагає наявності кількох факторів для підтвердження особи користувача, таких як пароль, токен або біометричні дані. Це значно підвищує рівень безпеки, оскільки зловмисники не зможуть отримати доступ до облікового запису лише через компрометацію пароля. Багаторівнева автентифікація також дозволяє зменшити ризики,

пов'язані з фішингом та іншими формами соціальної інженерії.

3. Моніторинг та аудит дій привілейованих користувачів

Важливим підходом до управління привілейованим доступом є моніторинг і аудит дій користувачів з привілейованими правами. Це включає ведення журналів доступу та запис дій адміністраторів у реальному часі. Таким чином, організація може відстежувати будь-які аномальні дії та вчасно реагувати на потенційні загрози. Автоматизовані системи моніторингу можуть також використовувати штучний інтелект для виявлення нетипових поведінкових патернів, що вказують на можливе порушення безпеки.

4. Управління доступом через рольові моделі

Рольове управління доступом (Role-Based Access Control, RBAC) є ефективним інструментом для оптимізації процесу привілейованого доступу. У межах цього підходу права доступу надаються на основі ролей, які відповідають функціональним обов'язкам користувача в організації. Це дозволяє зменшити ризики, пов'язані з людським фактором, та спрощує управління доступом, оскільки не потрібно надавати індивідуальні права для кожного користувача окремо. Усі користувачі, що мають однакові функціональні обов'язки, отримують однакові привілеї.

5. Використання PAM-рішень

Для ефективного управління привілейованим доступом у багатьох організаціях використовують спеціальні рішення, такі як Privileged Access Management (PAM). PAM-рішення надають централізований контроль над привілейованими обліковими записами, дозволяючи автоматизувати процеси надання та відкликання доступів, а також забезпечують надійний моніторинг та аудит дій користувачів. PAM-рішення дозволяють значно знизити ризики, пов'язані з несанкціонованим доступом, і підвищують ефективність управління безпекою.

Рис.1.1 Ключові кроки до створення комплексного PAM

Отже, управління привілейованим доступом є критичним елементом безпеки інформаційних систем організацій. Ефективне впровадження політики мінімальних привілеїв, багаторівневої автентифікації, моніторингу

дій користувачів, використання рольових моделей та спеціалізованих PAM-рішень дозволяє значно підвищити рівень безпеки та знизити ризики, пов'язані з несанкціонованим доступом до критичних ресурсів. Застосування цих підходів разом із сегментацією та ізоляцією доступу забезпечує надійний захист від внутрішніх і зовнішніх загроз.

Перелік посилань:
1. Призначення PAM URL: https://delinea.com/blog/privileged-users (дата звернення 07.10.2024).
2. Звіт Verizon. Класифікація інцидентів URL: https://www.verizon.com/business/resources/reports/dbir/2023/incident-classification-patterns-intro/ (дата звернення 17.10.2024).
3. Jones, C. (2023). Discover the top ten best privileged access management solutions. URL: https://expertinsights.com/insights/the-top-10-privileged-access-management-pam-solutions (дата звернення 17.10.2024).

Яловик Денис Володимирович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ПОБУДОВА OPEN WORLDWIDE APPLICATION SECURITY PROJECT (OWASP)

В умовах швидкого розвитку технологій і зростаючої кількості кіберзагроз, діяльність OWASP залишається надзвичайно актуальною. Вона допомагає не лише професіоналам у галузі безпеки, але й усім учасникам процесу розробки програмного забезпечення, щоб створювати надійні й безпечні продукти.

Організація пропонує різноманітні ресурси, включаючи посібники, інструменти для тестування безпеки, а також платформи для обміну досвідом між фахівцями. Зокрема, проект OWASP Top Ten забезпечує розробників критично важливими знаннями про найпоширеніші вразливості веб-додатків, такі як SQL-ін'єкції, міжсайтовий скриптинг (XSS) та проблеми з автентифікацією.

OWASP активно працює над підвищенням обізнаності в сфері кібербезпеки, організовуючи конференції, семінари та тренінги, які дозволяють фахівцям покращувати свої навички та знання. У світі, де кібератаки стають дедалі складнішими, важливо, щоб усі учасники розробки програмного забезпечення, від аналітиків до тестувальників, усвідомлювали важливість безпеки та впроваджували відповідні практики у свою роботу.

Історія та місія

OWASP був заснований у 2001 році з метою підвищення обізнаності щодо безпеки веб-додатків. Основна місія організації полягає в тому, щоб зробити безпеку програмного забезпечення більш доступною для всіх, від розробників до бізнесу.

Основні компоненти OWASP

1. **Глобальна спільнота**:

- OWASP має місцеві глави в багатьох країнах, що дозволяє створити міжнародну мережу професіоналів.
- Спільнота активно залучає волонтерів до розробки ресурсів, проведення заходів та обміну знаннями.

2. **Проєкти**:
   - **OWASP Top Ten**: Це список десяти найбільш критичних вразливостей веб-додатків, який оновлюється кожні кілька років. Він слугує інструментом для розробників і керівників безпеки для оцінки ризиків.

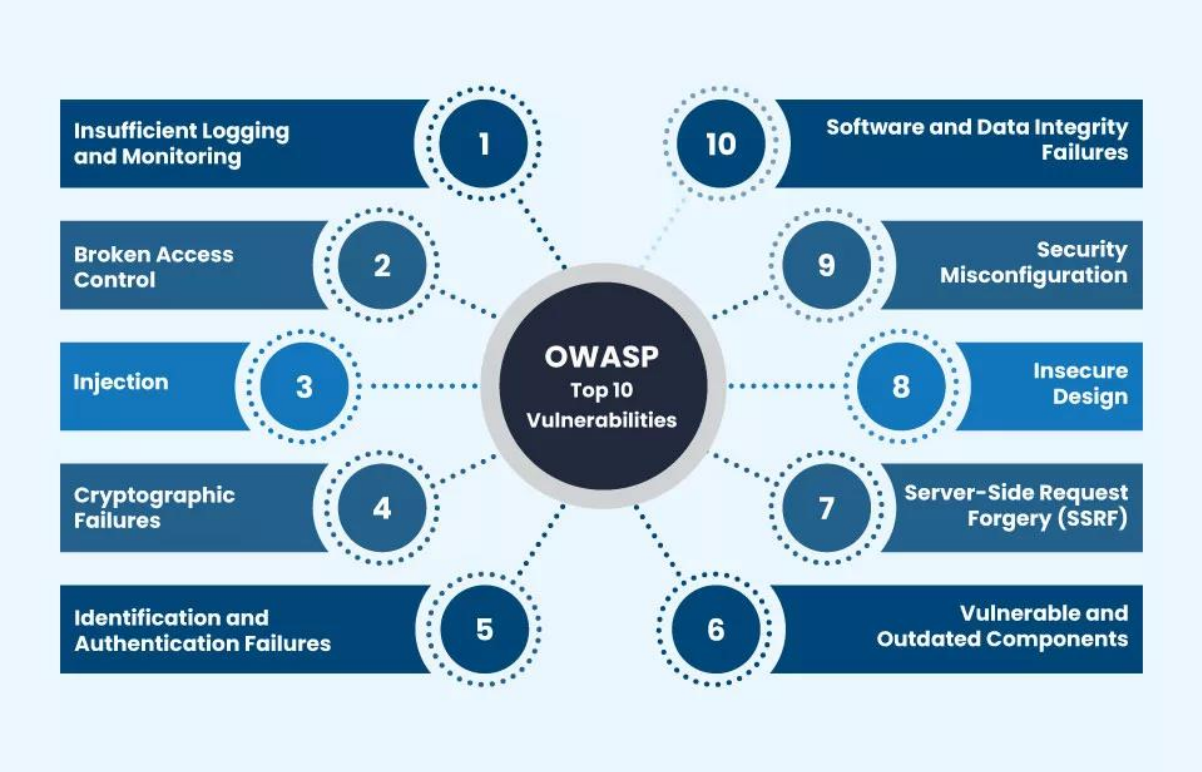


Рис.1 “Список десяти найбільш критичних вразливостей веб-додатків OWASP”

   - **OWASP ZAP (Zed Attack Proxy)**: Безкоштовний інструмент для тестування безпеки веб-додатків, що дозволяє автоматизувати виявлення вразливостей.
   - **OWASP ASVS (Application Security Verification Standard)**: Стандарт, що визначає рівні безпеки веб-додатків та критерії їх перевірки.

3. **Освітні ресурси**:
   - OWASP надає безкоштовні матеріали, такі як навчальні курси, книги та вебінари, які охоплюють різні аспекти безпеки програмного забезпечення.
   - Проводяться тренінги та семінари, що дозволяють поглибити знання у сфері безпеки.

4. **Події та конференції**:

- OWASP організовує щорічні конференції, такі як **OWASP AppSec**, на яких експерти діляться новинами, трендами та кращими практиками.
- Регулярні локальні зустрічі та семінари дозволяють обговорювати актуальні питання безпеки в зручному форматі.

OWASP не лише формує стандарти безпеки, але й сприяє розвитку спільноти, яка прагне до підвищення безпеки в цифровому середовищі. У результаті цього, організації можуть знижувати ризики, пов'язані з кіберзагрозами, і забезпечувати безпечніше використання технологій у повсякденному житті.

Перелік посилань:
1. About the OWASP Foundation. URL: https://owasp.org/about/ (дата звернення: 16.10.2024).
2. OWASP Top 10 Vulnerabilities. URL: https://certera.com/blog/mitigating-the-owasp-top-10-vulnerabilities/ (дата звернення: 16.10.2024).

Яценко Денис Дмитрович
студентк групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ WEB-САЙТІВ

Сучасні технології для виявлення вразливостей на веб-сайтах є критично важливими для корпоративного середовища. Компанії використовують веб-додатки для обміну конфіденційною інформацією, що робить їх привабливими цілями для кіберзлочинців. Вразливості в системах можуть призвести до витоку даних, фінансових втрат або підриву репутації.Інтеграція веб-додатків у корпоративні системи збільшує ризики проникнення зловмисників через уразливості. Це може дати їм доступ до внутрішніх мереж, баз даних або критичних систем. Крім того, зростання віддаленої роботи підвищує ймовірність атак на недостатньо захищені пристрої співробітників.

Для атак зловмисники використовують різні технології та методи для ураження вразливостей сайтів, в результаті чого отримуючи захищену інформацію або заважають коректній роботі сайту.

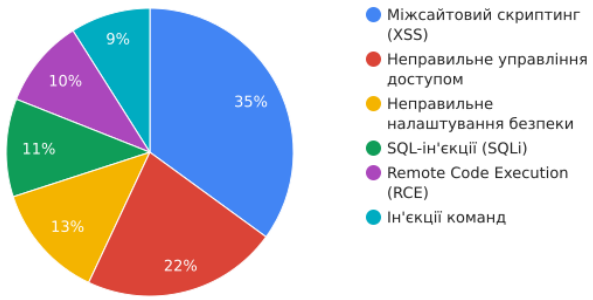


Рис.1. Вразливості якими частіше всього користуються зловмисники

Щоб запобігти використання злочинцями вразливостей потрібно

завчасно проводити аудит WEB-сайту для виявлення цих вразливостей. З цим нам допоможуть:

1. Сканери вразливостей наприклад: OWASP ZAP, Netsparker;
2. Автоматизоване тестування безпеки, такі методи як: SAST, DAST;
3. Аналіз вихідного коду, ручним або автоматичний;
4. Контейнеризація та ізоляція середовища, приклад інструментів Clair, Trivy;
5. Тестування на проникнення (Penetration Testing).

Перелік посилань:

1. Welcome to the OWASP Top 10 — 2021 [Електронний ресурс] – Режим доступу: https://owasp.org/Top10/
2. Vulnerable and outdated components (A6) | Secure against the OWASP Top 10 for 2021 [Електронний ресурс] – Режим доступу : https://support.f5.com/csp/article/K17045144
3. K39707080: Insecure design (A4) | Secure against the OWASP Top 10 for 2021 [Електронний ресурс] – Режим доступу: https://support.f5.com/csp/article/K39707080

Яцентій Богдан Богданович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

АТАКИ НА КРИТИЧНУ ІНФРАСТРУКТУРУ: ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

У сучасному цифровому світі критична інфраструктура, що включає енергетичні системи, водопостачання, транспорт, охорону здоров’я та фінансові мережі, стає мішенню для кіберзлочинців і державних акторів. Атаки на такі системи можуть мати серйозні наслідки для безпеки країни, економіки та суспільства загалом. Цілями можуть бути як фізичні об’єкти, так і цифрові системи, що їх контролюють, і результатом таких атак може стати порушення роботи життєво важливих послуг або навіть катастрофічні наслідки для населення.

Одним із найвідоміших прикладів атаки на критичну інфраструктуру є кібератака на електромережі України у 2015 році. Ця атака залишила сотні тисяч людей без електроенергії та виявила вразливість національних енергетичних систем до цифрових загроз. Подібні атаки можуть паралізувати країну, впливаючи на всі сектори суспільного життя — від охорони здоров'я до транспорту. З кожним роком кіберзлочинці вдосконалюють свої методи, а кіберзагрози стають дедалі серйознішими.

Одним з найбільших викликів є те, що критична інфраструктура часто працює на застарілих системах, які не були спочатку розроблені для інтеграції з інтернетом або захисту від кіберзагроз. Внаслідок цього ці системи мають серйозні вразливості, які можуть бути експлуатовані зловмисниками. Крім того, велика кількість обладнання є взаємозалежним, що створює ефект доміно

— атака на одну частину системи може призвести до масштабного збою в інших сегментах інфраструктури.

Крім того, атаки на критичну інфраструктуру часто стають інструментом державного шантажу або кібервійни. Держави-агресори можуть використовувати кіберінструменти для підриву економіки іншої країни, впливаючи на політичну стабільність і викликаючи соціальні потрясіння. Це додає новий рівень складності до питань національної безпеки, оскільки кіберпростір стає новим полем для міжнародних конфліктів.

Методи атак на критичну інфраструктуру можуть варіюватися від шкідливих програм, таких як Stuxnet, які впливають на фізичне обладнання, до складних багатоступеневих кібератак, що використовують соціальну інженерію та експлуатацію вразливостей у програмному забезпеченні. Часто зловмисники прагнуть отримати доступ до систем управління технологічними процесами (ICS), які контролюють роботу інфраструктурних об’єктів, таких як електростанції, водопостачання та транспортні мережі.

Для захисту критичної інфраструктури необхідно впроваджувати комплексні заходи безпеки. Це включає оновлення та модернізацію застарілих систем, впровадження багатошарових засобів захисту, таких як мережеві сегментації, шифрування даних та контроль доступу. Крім того, важливо забезпечити тісну співпрацю між державними та приватними секторами, оскільки велика частина критичної інфраструктури перебуває у приватній власності. Підвищення рівня обізнаності працівників щодо кіберзагроз, регулярні аудити безпеки та впровадження систем моніторингу для виявлення потенційних загроз на ранніх стадіях також є важливими елементами стратегії захисту.

Крім технічних заходів, велике значення має також міжнародна співпраця у сфері кібербезпеки. Розвиток глобальних ініціатив і угод може допомогти зменшити ризик міжнародних кібератак та забезпечити колективну безпеку. Оскільки загроза атаки на критичну інфраструктуру є глобальною, необхідні спільні зусилля для того, щоб зменшити вразливості та мінімізувати ризики.

Отже, атаки на критичну інфраструктуру представляють серйозну загрозу національній безпеці. Сучасний світ залежить від безперервної роботи ключових інфраструктур, і їхній захист повинен бути одним із пріоритетів державної політики та міжнародної співпраці. Тільки шляхом впровадження надійних кіберзахисних заходів і розбудови міжнародних партнерств можна знизити ризики та забезпечити стійкість критичних систем до кібератак.

Перелік посилань:

1. Що таке об'єкти критичної інфраструктури. URL: https://smarttender.biz/terminy/view/ob-yekti-kritichnoyi-infrastrukturi/ (date of access: 07.10.2024).
2. Занадто критична інфраструктура URL: https://yur-gazeta.com/publications/practice/transportne-pravo/zanadto-kritichna-infrastruktura.html (date of access: 05.10.2024).
3. Об'єкти критичної інфраструктури: детальний аналіз та відповіді на поширені питання. URL: https://smarttender.biz/blog/view/ob-yekti-kritichnoyi-infrastrukturi-detalniy-analiz-ta-vidpovidi-na-poshireni-pitannya/ (date of access: 04.10.2024).

Ячина Анастасія Сергіївна
студентка групи БСД-11, ННІЗІ ДУІКТ, Київ, Україна

ПРАКТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Тема:Атака типу «людина посередині»

Кіберзлочинність сьогодні поширена в різних формах, але однією з найстаріших і найнебезпечніших є атака типу **Man-In-The-Middle** (MITM). Дослівно це перекладається як «**людина посередині**», тобто коли злочинець виступає в ролі **посередника при передачі інформації**. Цей тип кіберзлочину є розповсюдженим та руйнівним. Пропонуємо ознайомитися з основними фактами про MITM та способами захисту від цієї атаки.

«Людина посередині» (Man-in-the-Middle, MitM) — вид атаки, коли зловмисник здійснює атаку, щоб витягти інформацію з вашого з'єднання з інтернетом. Вони розривають ваше з'єднання на дві частини, створюючи своє власне зашифроване з'єднання з вами й з сервером, до якого ви звертаєтеся. За допомогою цього з'єднання вони можуть прочитати ваші дані, змінити їх або навіть відправити власні дані від вашого імені. Щоб захиститися від цих атак, ми можемо використовувати протокол HTTPS.

Це захищений протокол, який шифрує дані, які ви надсилаєте через інтернет, тому зловмисники не зможуть їх прочитати. Проте зростання мобільності створює нові ризики, оскільки деякі мобільні додатки можуть використовувати незахищені протоколи для з'єднання з інтернетом, що робить їх більш вразливими до атак MitM. [Література: https://it-osvita.diia.gov.ua/task/item/21cadbcd-2818-4752-acd2-324d3af66ece]

Будь-яка особа або організація може стати об'єктом нападу MITM, але більшість цих злочинів має спільну мету: фінансова вигода. Банки та банківські додатки є популярними цілями для атак MITM, тому хакери намагаються інтегрувати зловмисний код на цільовий сайт, який здатний перехопити легітимний трафік. Це не означає, що злочинцям цікаві лише фінансові установи: будь-яка інформація, що здатна принести прибуток

злочинцю, може бути привабливою для нього. Сюди входять облікові записи соціальних мереж, облікові дані інтернет-магазинів, конфіденційні бази даних, тощо.

Нижче перелічені основні типи атак Man-in-the-middle:

1. Фальшиві точки доступу — це точки бездротового доступу, встановлені без відома адміністратора для перехоплення трафіку і викрадення даних користувачів, що автоматично підключаються до Wi-Fi.
2. Address resolution spoofing — атака в локальних мережах через протокол ARP, де зловмисник видає себе за легітимний вузол і перехоплює трафік.
3. mDNS spoofing — це атака, в якій зловмисники можуть підмінити мережевий запит на пристрій, щоб перехопити дані.
4. DNS spoofing — підробка DNS-запитів, що змушує користувачів підключатися до фальшивих сайтів для викрадення облікових даних.

Захист від атак типу MITM вимагає кількох дій, кожна з них має важливе значення.

• Не дозволяйте комп'ютерам або мобільним пристроям **автоматично підключатися** до Wi-Fi-мереж, переконайтеся, що вони підключаються тільки до відомих та перевірених мереж Wi-Fi.
• Переконайтеся, що всі точки доступу, які ви контролюєте, **захищені та зашифровані**.
• Якщо ви підключаєтеся до невідомої або загальнодоступної мережі WiFi, **обов'язково використовуйте VPN-канал** для захисту вашого трафіку.
• Ніколи не надсилайте конфіденційну інформацію на веб-сайт, який **не використовує захищений протокол HTTPS** (URL-адреса сайту починається з https: //).
• Додайте **другий спосіб автентифікації** до всіх облікових записів, які підтримують таку технологію.
• Будьте обережні щодо будь-яких електронних листів, в яких вам пропонується **перейти по веб-посиланню на інший сайт**.
• Переконайтеся, що операційна система на комп'ютерах **своєчасно оновлюється**, щоб запобігти нападам MITM, які використовують вразливості ОС.
• Встановіть найновішу **антивірусну програму** та переконайтесь, що вона налаштована на регулярну перевірку комп'ютера.

І хоча навіть такі засоби не зможуть вас назавжди захистити від атаки MITM або інших кібератак, це, як мінімум, значно зменшить кіберризики та переконає
злочинців, що вони лише змарнують час, якщо спробують вас атакувати.

Перелік посилань:

https://www.imena.ua/blog/man-in-themiddle/https://www.imena.ua/blog/man-in-the-middle/]

Гирба Олеся Федорівна
студентка ТСДМ-61

АНАЛІЗ ОСОБЛИВОСТЕЙ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У ТЕЛЕКОМУНІКАЦІЙНІЙ ІНФРАСТРУКТУРІ

Перші застосування технології блокчейн з'явилися на платформах для криптовалютних платежів. Ця ж технологія почала набувати популярність та використовуватися для підтримки платіжних операцій у сфері телекомунікацій. Наприклад, у деяких країнах телекомунікаційні оператори почали надавати своїм клієнтам послуги мобільних платежів, такі як сервіс грошових переказів M-Pesa від Safaricom в Африці, Revolut в Великобританії, G-Cash у Філіппінах, Paytm в Індії тощо. Потупово блокчейн почав розглядатися як альтернатива інфраструктурі бекенд-системи [1].

Технологія блокчейн також може сприяти здійсненню платежів та інших транзакцій між телекомунікаційними операторами. Наприклад, з 2015 року французький оператор Orange здійснив інвестиції в компанію Chain, яка розробляє приватні блокчейн-мережі для телекомунікаційних компаній. У лютому 2017 року японська компанія Softbank і американський оператор Sprint запустили консорціум із розробником програмного забезпечення TBCASoft для створення блокчейн-додатків. Консорціум мав на меті створення платформи для міжоператорських платежів, яка б об'єднувала бекенд-системи операторів для обробки оптових платежів за роумінг і роздрібних платежів за поповнення рахунків. Теоретично такі мережі можуть використовувати смарт-контракти для автоматизації виконання угод про роумінг між операторами, надаючи можливість у режимі реального часу здійснювати авторизацію, виставлення рахунків та платежі. Це може допомогти запобігти шахрайству в роумінгу та зменшити кількість суперечок між операторами [2].

Деякі стартапи прагнуть піти ще далі, використовуючи мікроплатежі на базі блокчейн для фінансування mesh-мереж. Наприклад, компанія Ammbr має на меті створити комунальну mesh-мережу, де учасники з'єднують зовнішні маршрутизатори та внутрішні точки доступу до інтернету, щоб забезпечити покриття останньої милі. Ця mesh-мережа використовує неліцензовані частоти спектру, а також частоти, які не використовуються локально, такі як вільні телевізійні частоти. Користувачі платять за доступ за допомогою блокчейн-платежів, що стимулює учасників встановлювати маршрутизатори. Результуючі фіксовані бездротові мережі можуть допомогти розширити покриття широкосмугового доступу на нові території (за умови наявності

фіксованої основної мережі та доступних діапазонів спектру), особливо в тих випадках, коли розгортання було обмежено нестачею капіталу або юридичними питаннями, такими як отримання дозволів на будівництво [3].

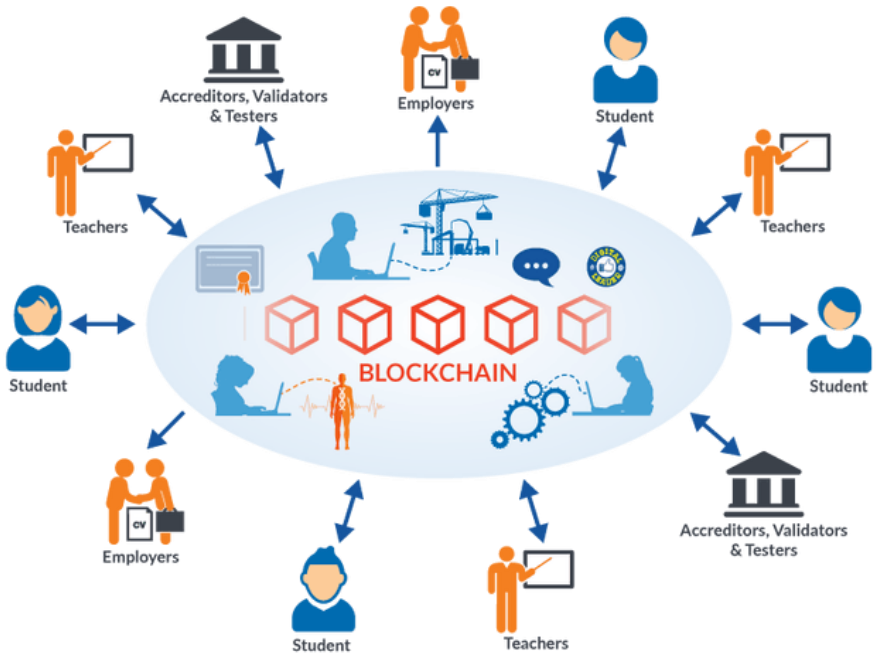


Рис.1. Сфери впровадження технології блокчейн

Крім обробки платежів, технологія блокчейн може підтримувати нові послуги, що генерують дохід. Наприклад, телекомунікаційні оператори можуть запропонувати послугу цифрової ідентифікації, яка дозволить їхнім абонентам безпечно входити до додатків або на вебсайти сторонніх провайдерів. Така послуга може бути побудована на основі приватного ключа, що зберігається на пристрої кожного абонента, а телекомунікаційні оператори керуватимуть блокчейн-реєстром, який зіставляє ці ключі з ідентифікаторами абонентів.

У майбутньому блокчейн і смарт-контракти також можуть бути використані для автоматизації мікроплатежів між пристроями (machine-to-machine), таких як оплата електричними автомобілями за заряд на автономних зарядних станціях [4].

Перелік посилань:

1. B. Mafakheri, T. Subramanya, L. Goratti, R. Riggio. «Blockchain-based Infrastructure Sharing in 5G Small Cell Networks.» 15th International Conference on Network and Service Management (CNSM). Pp. 320–325. 2021.

2. Gupta S. Singh. «Blockchain Integration in Telecommunications: Opportunities and Challenges.» IEEE Access, vol. 9, pp. 81012–81023, 2021. DOI: 10.1109/ACCESS.2021.3073859.

3. «Blockchain in Telecoms: Redefining Network Security and Efficiency.» Omdia Market Insights. [Електронний ресурс] – Режим доступу: https://www.omdia.com/resources/blockchain-telecoms-redefining-network-security-2021

4. Cedric Dib. «Blockchain Technology in Telecom Industry: Emerging Trends and Applications.» RCR Wireless News, 2022. [Електронний ресурс] – Режим доступу: https://www.rcrwireless.com/20220210/blockchain-telecom-emerging-trends-2022

Щавінський Юрій Віталійович
канд. техн. наук, доцент, доцент кафедри УКЗІ ННІКЗІ ДУІКТ Київ, Україна,
Будзинський Олександр Володимирович
Аспірант, ННІКЗІ ДУІКТ, Київ, Україна

TECHNOLOGICAL REQUIREMENTS FOR THE PROTECTION OF CORPORATE DATABASES IN CONNECTION WITH THE DEVELOPMENT OF NETWORK INFRASTRUCTURE

The modern development of the network infrastructure significantly affects the requirements for corporate databases (DB). The increase in the amount of data transferred, the growth in the number of users and connected devices, as well as the emergence of new technologies such as 5G, cloud computing and the Internet of Things (IoT), create new challenges for database management. In this connection, there is a need to review traditional approaches to the design and operation of corporate databases in order to increase their efficiency, reliability and security.

Today, the technological requirements for protecting corporate databases have significantly changed due to the development of modern network infrastructure, including cloud computing, the Internet of Things (IoT), distributed computing, virtualization, and mobile technologies.

The development of network infrastructure leads to an increase in the volume of data stored and processed by corporate databases. Therefore, horizontal scaling capabilities, which provide increased data storage capacity and performance by adding new nodes to the cluster, are essential. Flexible architectural solutions, which allow for quick adaptation to changes in business needs and system loads, have also gained particular importance.

Given the continuous operation of modern organizations, corporate databases must ensure high data availability without downtime. To achieve this, as noted by researchers [1-2], it is necessary to implement strategies for backup, recovery, and system resilience. Clustering and data replication technologies have become key tools for maintaining uninterrupted operation and protecting against data loss in case of hardware or software failures.

With the growth in data volume and the number of transactions executed in corporate systems, the speed of information processing becomes a critical factor. Databases should support query optimization, data caching, and indexing, as well as the use of modern in-memory computing technologies, which can significantly accelerate the execution of complex queries and data analysis.

The development of network infrastructure is accompanied by an increase in cyber threats, making the security of corporate databases a priority. It is important to implement multi-layered security mechanisms, including data encryption during storage and transmission, multi-factor authentication, and access management [3]. Additionally, integration with intrusion detection systems (IDS) and monitoring is

necessary for timely detection and neutralization of potential attacks.

The transition to cloud solutions allows organizations to ensure the flexibility and scalability of their databases [3]. The use of cloud services, such as AWS, Azure, or Google Cloud, reduces the costs of maintaining on-premises hardware, enabling companies to scale resources according to their needs. Hybrid architectures, which combine on-premises and cloud solutions, provide additional reliability and data security.

With the spread of IoT, there is a need to process massive volumes of data coming from various devices in real time. Big Data technologies, such as Hadoop and Apache Spark, help ensure the storage and processing of large amounts of unstructured data. These solutions allow for effective data analysis and utilization for business decision-making [4].

Modern technological requirements for protecting corporate databases must consider not only internal threats but also numerous external factors, including new forms of cyberattacks, the growth of data volume, and integration with cloud and distributed systems:

- encryption at the storage level (at rest), encryption during transmission (in transit), for example during transmission between the user and the server, for example, via SSL/TLS protocols;
- encryption at the level of individual elements (individual fields for additional protection of sensitive data);
- in addition to multi-factor authentication, also the delineation of access rights based on user roles to limit access to sensitive data (RBAC) and limit privileged access to data and monitor the actions of users with elevated rights to prevent internal threats;
- division of the network infrastructure into small segments, which allows to limit the traffic between them and reduce the potential impact of an attack (network micro-segmentation);
- use of secure tunnels for remote access to corporate databases, which ensures communication security (VPN);.
- use of machine learning algorithms to analyze behavioral patterns and identify suspicious actions that may indicate possible threats (user behavior analysis (UBA);
- use of a SIEM system (Security Information and Event Management) to consolidate data on security events and system logs for anomaly detection and prompt response;
- regular backup of data with ensuring their encryption;
- use of secure protocols for the integration of corporate databases with cloud infrastructures, monitoring and management of the configuration of cloud databases to prevent security breaches due to incorrect settings;
- use of network-level and application-level security measures to prevent attacks such as SQL injection, Cross-Site Scripting (XSS), etc.;
- assessment of the state of security of corporate bases during periodic audits for compliance with the requirements of international standards (ISO/IEC 27001, GDPR, PCI DSS, etc.).

Thus, the development of network infrastructure sets new technological requirements for corporate databases, forcing organizations to adapt their systems to ensure high scalability, performance, availability, and security. The implementation of modern data management technologies is an important step towards building an efficient and stable information infrastructure for enterprises. Meeting these requirements will allow companies to minimize the risks of data leakage, loss, or damage, thereby ensuring the stable and secure operation of their information systems.

List of links:

3. Toni Taipalus. Database management system performance comparisons: A systematic literature review,Journal of Systems and Software, Volume 208, 2024, 111872, https://doi.org/10.1016/j.jss.2023.111872.
4. Senyo K., Addae E., Boateng R. Cloud computing research: A review of research themes, frameworks, methods and future research directions, International Journal of Information Management, Volume 38, Issue 1, 2018, Pages 128-139, https://doi.org/10.1016/j.ijinfomgt.2017.07.007.
5. Khan, S., & Alsaeedi, A. (2020). Cloud Database Management Systems: A Review. Journal of Cloud Computing.
6. Patel, H. (2021). The Role of Big Data and Cloud Computing in Modern Business Environments. Information Systems Journal.

Матісько Денис Федорович
студинт групи ТСДМ-61, ННІТ ДУІКТ, Київ, Україна

БЕЗПЕКА В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ НА ОСНОВІ ПРОГРАМНО-ВИЗНАЧЕНИХ МЕРЕЖ (SDN)

Програмно-визначені мережі надають мультисервісним мережам значну гнучкість і контроль, що дозволяє покращити захист від сучасних загроз. Централізоване управління, автоматизація політик безпеки та сегментація трафіку є ключовими перевагами SDN у забезпеченні безпеки. Однак важливо враховувати виклики, пов'язані з безпекою контролера та API, для забезпечення стабільної та захищеної роботи мережі.

Програмно-визначені мережі (SDN) швидко стають однією з ключових технологій у мультисервісних мережах завдяки своїй здатності динамічно управляти трафіком і забезпечувати високий рівень гнучкості мережевих операцій. З огляду на сучасні загрози безпеці та зростаючу складність мережевої інфраструктури, SDN стає важливим інструментом для покращення безпеки мультисервісних мереж.

Одним із найбільших викликів для безпеки мультисервісних мереж є їх різноманітність і складність. Об'єднання кількох технологій передачі даних, таких як IP/MPLS, LTE, Wi-Fi, і навіть 5G, потребує не лише підтримки високої якості обслуговування (QoS), але й ефективного захисту від атак, зокрема DDoS, маніпуляцій із маршрутизацією та несанкціонованого доступу до даних.

З традиційними підходами до управління мережею складно забезпечити швидке реагування на загрози. Натомість, використання програмно-визначених мереж дозволяє централізувати управління мережею та автоматично вносити зміни в конфігурацію системи у випадку виявлення аномальної активності або атак.

SDN пропонує низку унікальних переваг для забезпечення безпеки мультисервісних мереж [1]:

1. **Централізоване управління мережею**. Використання SDN дозволяє контролювати всі елементи мережі з єдиного центру управління, що забезпечує гнучкість у реагуванні на загрози. Це також дозволяє швидко виявляти та блокувати підозрілу активність у реальному часі.

2. **Автоматизація політик безпеки**. Однією з основних переваг SDN є можливість автоматизованого впровадження політик безпеки. Замість того, щоб вручну налаштовувати безпекові механізми на кожному маршрутизаторі чи комутаторі, адміністратори можуть створювати єдині правила для всієї мережі, які автоматично застосовуються до всіх її елементів.
3. **Сегментація трафіку**. Завдяки гнучкому управлінню маршрутизацією, SDN дозволяє сегментувати трафік на різні зони безпеки, що значно зменшує ризики поширення загроз у разі компрометації окремого сегмента. Це дозволяє захистити критичні сервіси та додатки від потенційних атак.

4. **Інтеграція з інструментами моніторингу**. SDN легко інтегрується з інструментами моніторингу трафіку та системами виявлення вторгнень (IDS/IPS). Це дозволяє не лише відстежувати аномалії у реальному часі, але й автоматично приймати відповідні заходи для усунення загроз.

Хоча SDN значно підвищує рівень безпеки мультисервісних мереж, технологія має свої виклики. Наприклад, централізоване управління може стати мішенню для зловмисників, оскільки компрометація контролера SDN може вплинути на всю мережу. Тому важливо забезпечити надійний захист контролера, включно з багаторівневою аутентифікацією та шифруванням з'єднань між контролером і мережевими елементами.

Також важливою задачею є забезпечення безпеки API, що використовуються для управління мережею через SDN. Відкритість API може стати точкою входу для зловмисників, тому потрібно впроваджувати обмеження доступу і моніторинг використання цих інтерфейсів.

З розвитком концепції **Zero Trust Network** та інших інновацій у сфері безпеки, SDN відіграє ключову роль у впровадженні сучасних стандартів

захисту мережі [2]. Важливим напрямком є інтеграція SDN з технологіями штучного інтелекту для автоматизованого аналізу поведінки користувачів та трафіку з метою виявлення нових типів загроз. Також зростає інтерес до впровадження SDN у хмарні середовища, де гнучке управління мережею дозволяє підвищити безпеку та адаптивність хмарних додатків.

Перелік посилань:

1. Li, X., & Chen, L. CENTRALIZED SECURITY CONTROL IN SDN: CHALLENGES AND SOLUTIONS. Berlin: Springer. 2021. С. 33 – 36.
2. Kreutz, D., Ramos, F. M., Verissimo, P. *TOWARDS SECURE AND DEPENDABLE SDNs*. IEEE Communications Magazine. 2018. № 8. С. 103 – 109.

Матісько Денис Федорович
студент групи ТСДМ-61, ННІТ ДУІКТ, Київ, Україна

АНАЛІЗ БЕЗПЕКИ В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ НА БАЗІ ТЕХНОЛОГІЙ CISCO

Забезпечення безпеки мультисервісних мереж є складним завданням, яке потребує інтегрованого підходу. Cisco пропонує комплексні рішення, які включають ідентифікацію загроз, захист, моніторинг, реагування та відновлення мережі після інцидентів. Використання цих технологій дозволяє забезпечити високий рівень безпеки, захистити критично важливі дані та мінімізувати ризики для бізнесу.

У сучасному світі, де кількість мережевих сервісів постійно зростає, загрози для інформаційної безпеки стають все більш різноманітними та складними. Особливо критичною є безпека мультисервісних мереж, які забезпечують інтеграцію різноманітних послуг та технологій, що використовуються в корпоративних середовищах, фінансових установах і державних організаціях. Відсутність належного захисту може призвести до серйозних наслідків, таких як втрата конфіденційних даних, значні фінансові збитки, порушення роботи сервісів та завдання шкоди репутації організації.

Компанія Cisco пропонує комплексний підхід до забезпечення безпеки, заснований на сучасних технологіях та рішеннях, що охоплюють усі етапи захисту мережі. Цей підхід включає ідентифікацію загроз, захист мережі, виявлення потенційних інцидентів, швидке реагування на атаки та відновлення систем після кібератак.

Перший етап забезпечення безпеки полягає у виявленні потенційних загроз. Для цього Cisco розробила програмно-обумовлену систему сегментації мережі – Cisco TrustSec. Ця технологія дозволяє точно ідентифікувати користувачів та пристрої, які підключаються до мережі, а також здійснювати контроль доступу до мережевих ресурсів на основі безпеки контексту.

Завдяки використанню TrustSec, адміністратори можуть запроваджувати політики безпеки на основі ролей користувачів або пристроїв, що значно підвищує рівень захищеності мережі, мінімізуючи ризик несанкціонованого доступу або впровадження шкідливого програмного забезпечення.

Другим етапом є безпосередній захист мультисервісної мережі. Cisco пропонує широкий спектр рішень для забезпечення безпеки, зокрема брандмауери нового покоління (NGFW), системи запобігання вторгнень (IPS), системи захисту від шкідливого програмного забезпечення (AMP) та аналітичні платформи. Завдяки цим рішенням, організації можуть вчасно блокувати атаки, запобігати витоку даних та аналізувати потенційні загрози.

Системи безпеки Cisco забезпечують постійний моніторинг мережі в режимі реального часу. Особливу роль у цьому відіграє платформа Cisco Talos – глобальна дослідницька мережа, що аналізує загрози та надає оновлення для захисту мережі. Talos здатен виявляти загрози на ранніх етапах і автоматично реагувати на них, що мінімізує час реакції на інцидент.

У випадку виявлення інциденту, Cisco пропонує комплексне рішення для швидкого реагування та усунення загрози. Системи, такі як Cisco SecureX та Cisco Umbrella, дозволяють ізолювати заражені пристрої, проводити розслідування інцидентів та мінімізувати вплив атак на бізнес-процеси. Вони також інтегруються з іншими платформами для збору аналітики та оптимізації процесу реагування на інциденти.

Завершальний етап забезпечення безпеки – відновлення роботи мережі після інциденту. Cisco пропонує інструменти для відновлення даних, управління вразливостями та впровадження заходів щодо підвищення стійкості мережі до майбутніх атак. Важливою складовою є створення резервних копій мережевих конфігурацій та використання інструментів аналізу ризиків, що дозволяє суттєво зменшити ризики повторних атак.

Перелік посилань:

1. Zhang, Y., & Fang, Y. SECURITY IN WIRELESS MESH NETWORKS. New York: CRC Press. 2020. №. 4, С. 142-167. URL: https://www.routledge.com/Security-in-WirelessMeshNetworks/ZhangZhengHu/p/book/9780367452605?srsltid=AfmBOool_LB8uTkqf3U9-SIpmXpOiRihQT2Ucj1vWgUs45kkzHk97Srm.
2. Bhaiji, Y. *NETWORK SECURITY TECHNOLOGIES AND SOLUTIONS*. Cisco Press. 2008. С. 422 – 440. URL: https://books.google.com.ua/books/about/Network_Security_Technologies_and_Soluti.html?id=DiQfAQAAIAAJ&redir_esc=y.

Матіська Денис Федорович
студинт групи ТСДМ-61, ННІТ ДУІКТ, Київ, Україна

ІНТЕГРАЦІЯ ХМАРНИХ ТЕХНОЛОГІЙ З МУЛЬТИСЕРВІСНИМИ МЕРЕЖАМИ CISCO

Інтеграція хмарних технологій з мультисервісними мережами Cisco надає нові можливості для забезпечення надійної та безпечної передачі даних у різних сценаріях використання. Використання гнучких хмарних платформ та інтелектуальних систем управління трафіком дозволяє підвищити ефективність і продуктивність мережі, що є важливим аспектом у сучасній телекомунікаційній індустрії.

У сучасних умовах стрімкого розвитку телекомунікаційних технологій та збільшення попиту на мультимедійні сервіси зростає важливість хмарних технологій як одного з ключових елементів мультисервісних мереж. Хмарні рішення від Cisco дозволяють ефективно інтегрувати різноманітні технології та сервіси, забезпечуючи надійність, гнучкість і безпеку для користувачів.

Одним із найбільших викликів є масштабованість мережі, особливо в умовах зростання кількості підключених пристроїв та сервісів. Інтеграція хмарних рішень потребує ефективного управління ресурсами, щоб забезпечити безперебійну роботу сервісів і підтримку необхідного рівня якості обслуговування (QoS). Також важливою є безпека даних, що передаються через хмарні рішення, адже відкриті канали зв’язку можуть стати мішенню для зловмисників.

Хмарні платформи Cisco, такі як **Cisco CloudCenter** та **Cisco Meraki**, надають широкі можливості для інтеграції мультисервісних мереж. Однією з ключових переваг є **масштабованість** цих рішень, яка дозволяє операторам гнучко збільшувати або зменшувати ресурси в залежності від навантаження. Завдяки автоматизації мережевих операцій, Cisco Meraki дозволяє швидко розгортати нові сервіси та управляти ними через єдиний хмарний інтерфейс, що суттєво знижує витрати на обслуговування мережі [1].

Хмарні рішення Cisco також забезпечують **інтелектуальне управління трафіком**. Використання механізмів штучного інтелекту для аналізу та оптимізації трафіку в реальному часі дозволяє мінімізувати затримки та втрати пакетів, що є критично важливим для сервісів, які працюють в реальному часі, таких як VoIP або відеоконференції.

Ще одна важлива перевага – це **спрощене управління** мережею за допомогою автоматизації процесів моніторингу та адміністрування. Cisco CloudCenter дозволяє операторам централізовано керувати мультисервісними мережами, зокрема через інтеграцію хмарних рішень із традиційною мережевою інфраструктурою, забезпечуючи швидке реагування на зміну умов трафіку або вимог до якості обслуговування (QoS).

Важливим аспектом є забезпечення безпеки даних, що передаються через хмарні сервіси. Технології Cisco використовують багаторівневі протоколи шифрування та аутентифікації, що забезпечують захист даних на всіх етапах їх передачі. Крім того, використання віртуальних приватних

мереж (VPN) та інших інструментів дозволяє запобігти несанкціонованому доступу до даних [2].

Завдяки інтеграції хмарних рішень, мультисервісні мережі стають більш гнучкими та адаптивними до змін у вимогах користувачів і бізнесу. Використання хмарних платформ дозволяє операторам телекомунікацій швидко масштабувати мережу, забезпечувати якість обслуговування навіть при зростанні навантаження, а також мінімізувати ризики безпеки.

Перелік посилань:

1. Smith, J., Thomas, R. CLOUD INTEGRATION IN MULTISERVICE NETWORKS: SOLUTIONS AND CHALLENGES. New York: IEEE Press. 2019. С. 83 – 86.
2. Zhang, L., & Wang, P. *SCALABILITY AND SECURITY IN CLOUD-BASED MULTISERVICE NETWORKS*. London: Springer. 2018. С. 126 – 128.

Бойко Анна Олександрівна
асистент кафедри СТКБ, ННІКБЗІ, ДУІКТ, Київ, Україна

ВИКОРИСТАННЯ МЕТОДУ ГРАДІЄНТНОГО БУСТИНГУ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Градієнтний бустинг - це техніка машинного навчання (ML), яка використовується для задач регресії та класифікації. Градієнтний бустинг став популярним завдяки своїй здатності обробляти складні взаємозв'язки в даних і захищати від надмірної підгонки. Використовуючи цю техніку, дослідники даних можуть підвищити точність прогнозування та швидкість роботи своїх моделей ML.

Градієнтний бустинг - це метод ансамблевого машинного навчання, який об'єднує набір слабких моделей в одну, більш точну та ефективну модель прогнозування. Ці слабкі моделі, як правило, є деревами рішень, тому алгоритми зазвичай називають деревами рішень з градієнтним прискоренням (GBDT). Алгоритми з градієнтним підсиленням працюють ітеративно, послідовно додаючи нові моделі, причому кожне нове додавання має на меті вирішити помилки, допущені попередніми моделями. Остаточний прогноз агрегату являє собою суму індивідуальних прогнозів усіх моделей. Градієнтний бустинг поєднує в собі алгоритм градієнтного спуску і метод бустингу, причому в його назві є посилання на кожен компонент.

Цей процес навчання використовує підхід «сила в числах», що дозволяє аналітикам даних оптимізувати довільні диференційовані функції втрат. Градієнтний бустинг використовується для вирішення складних задач регресії та класифікації. При регресії кінцевий результат являє собою середнє значення всіх слабких учнів. При роботі з задачами класифікації кінцевий результат моделі може бути обчислений як клас з більшістю голосів від слабких моделей, що навчаються.

Інші методи бустінгу, такі як AdaBoost та XGBoost, також є популярними методами ансамблевого навчання.

XGBoost - це турбована версія градієнтного бустінгу, розроблена для оптимальної швидкості обчислень і масштабованості. XGBoosting використовує кілька ядер в центральному процесорі, щоб забезпечити паралельне навчання під час тренування моделі.

AdaBoost, або адаптивне прискорення, підлаштовується під послідовність слабких учнів до даних. Ці слабкі навчальні елементи, як правило, є пеньками рішень, тобто деревом рішень з одним розщепленням і двома кінцевими вузлами. Цей метод працює рекурсивно, визначаючи неправильно класифіковані точки даних і автоматично коригуючи їх, щоб зменшити помилки навчання. AdaBoost повторює цей процес, поки не згенерує найсильніший предиктор [1].

Градієнтний бустинг використовує наступні інструменти:

1. Дерево рішень, яке є регресійною моделлю, що пов'язує значення цільової змінної з різними незалежними змінними через повторювані двійкові розбиття

2. Техніка бустингу, яка є адаптивним методом поєднання декількох простих моделей, таких як дерева рішень, для обчислення більш точних прогнозів.

Алгоритм поєднує ці інструменти в ітеративний спосіб, виконуючи наступні кроки:

1. Будується дерево рішень, яке підлаштовується під історичні дані.

2. Якщо це не повністю пояснює варіації цільової змінної (наприклад, історію продажів), розраховуються непояснені залишкові похибки, і на наступній ітерації визначається нове дерево рішень, яке пояснює варіації залишків.

3. Цей процес виконується кілька разів, так що все менші і менші залишкові помилки використовуються як вхідні дані в додаткових деревах.

4. Дерева рішень об'єднуються в остаточну модель, де кожному дереву надається певна вага. Прогноз є зваженою сумою прогнозів окремих дерев [2].

Застосування градієнтного бустингу в кібербезпеці забезпечує потужний інструмент для виявлення загроз, що значно перевершує традиційні методи за точністю, швидкістю і стійкістю до нових видів атак. Завдяки ітеративному підходу, при якому кожен новий класифікатор спрямований на виправлення помилок попереднього, градієнтний бустинг створює сильну модель на основі множини слабких класифікаторів, що робить його ефективним у розпізнаванні складних аномалій у кіберсистемах.

У кібербезпеці градієнтний бустинг часто використовується для задач виявлення шкідливих активностей у мережевому трафіку, аномальної поведінки користувачів та загроз, які маскуються під нормальні запити. Його здатність виявляти нові види атак особливо цінна в умовах постійно змінюваного середовища кіберзагроз. Використання бустингу дозволяє поєднати різні моделі, такі як дерева рішень, щоб ідентифікувати навіть слабкі сигнали загрози, мінімізуючи хибнопозитивні спрацьовування та підвищуючи адаптивність системи.

Метод градієнтного бустингу також дозволяє працювати з великими обсягами даних, які властиві сучасним кіберсистемам, що особливо актуально для аналізу потокових даних у реальному часі. У випадках атак на корпоративні веб-додатки або складні шпигунські кампанії, цей метод забезпечує необхідну гнучкість та масштабованість, необхідні для автоматизованої обробки і аналізу даних з високою ефективністю. Таким чином, градієнтний бустинг стає основою для інноваційних підходів до кіберзахисту, забезпечуючи високу ефективність і надійність сучасних систем виявлення загроз.

Перелік посилань:

1. What Is Gradient Boosting? URL: https://www.snowflake.com/guides/what-gradient-boosting/
2. Gradient Boosting of Decision Trees URL: https://help.sap.com/docs/SAP_INTEGRATED_BUSINESS_PLANNING/feae3cea3cc549aaa9d9de7d363a83e6/a2a3eada1d954aeaaaa8259ac2720767.html

Краєвський Владислав Юрійович
студент групи БСДМ-62, ННІКБЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ НА БАЗІ ZERO TRUST

Zero trust - це стратегія безпеки для сучасних мультихмарних мереж. Замість того, щоб зосереджуватися на периметрі мережі, модель безпеки з нульовою довірою впроваджує політики безпеки для кожного окремого з'єднання між користувачами, пристроями, додатками та даними.

Підхід zero trust важливий, оскільки традиційна модель мережевої безпеки вже не є достатньою. Стратегії zero trust призначені для більш складних, високорозподілених мереж, які сьогодні використовує більшість організацій.

Протягом багатьох років підприємства зосереджувалися на захисті периметрів своїх мереж за допомогою брандмауерів та інших засобів контролю безпеки. Користувачі всередині периметра мережі вважалися надійними і мали вільний доступ до додатків, даних і ресурсів.

Цифрова трансформація усунула традиційну концепцію мережевого периметру. Сьогодні корпоративні мережі виходять за межі локальних локацій та мережевих сегментів. Сучасна корпоративна екосистема включає хмарні середовища, мобільні сервіси, центри обробки даних, пристрої Інтернету речей (IoT), додатки як послугу (SaaS) і віддалений доступ для співробітників, постачальників і ділових партнерів.

З такою розширеною поверхнею атаки підприємства стають більш вразливими до витоку даних, програм-вимагачів, інсайдерських загроз та інших видів кібератак. Периметр мережі більше не є чіткою, безперервною лінією, і засоби захисту на основі периметра не можуть закрити всі прогалини. Більше того, суб'єкти загроз, які отримують доступ до мережі, можуть скористатися неявною довірою для здійснення латеральних рухів, щоб знайти

і атакувати критичні ресурси.

У 2010 році аналітик Джон Кіндерваг з Forrester Research представив концепцію «zero trust» як основу для захисту ресурсів підприємства за допомогою суворого контролю доступу. Нульова довіра зміщує фокус з периметра мережі і зосереджує контроль безпеки на окремих ресурсах.

Кожна кінцева точка, користувач і запит на з'єднання розглядаються як потенційна загроза. Замість того, щоб давати користувачам повну свободу дій при проходженні через периметр, вони повинні проходити автентифікацію та авторизацію щоразу, коли підключаються до нового ресурсу. Ця безперервна перевірка допомагає гарантувати, що тільки легітимні користувачі можуть отримати доступ до цінних мережевих активів [1].

Основні принципи zero trust

Доступ з найменшими привілеями

Принцип доступу з найменшими привілеями гарантує, що користувачам надається мінімальний рівень доступу, необхідний для виконання їхніх робочих функцій. Це зменшує поверхню атаки, обмежуючи потенційну шкоду, яка може бути завдана, якщо обліковий запис буде скомпрометовано.

Мікросегментація

Мікросегментація передбачає поділ мережі на менші ізольовані сегменти. Кожен сегмент може мати власні засоби контролю доступу та політики безпеки, що ускладнює зловмисникам латеральне переміщення в мережі.

Безперервний моніторинг та перевірка

Нульова довіра вимагає постійного моніторингу дій користувачів і пристроїв. Це передбачає оцінку стану безпеки в режимі реального часу та аналіз поведінки для виявлення аномалій і потенційних загроз. Безперервна перевірка гарантує, що користувачі та пристрої підтримують відповідність вимогам безпеки з плином часу.

Багатофакторна автентифікація (MFA)

Багатофакторна автентифікація додає додатковий рівень безпеки, вимагаючи декількох форм перевірки перед наданням доступу. Зазвичай це включає щось, що користувач знає (пароль), щось, що у нього є (маркер безпеки), і щось, чим він є (біометрична перевірка).

Компоненти архітектури zero trust

Управління ідентифікацією та доступом (IAM)

Системи IAM мають вирішальне значення для архітектури нульової довіри, оскільки вони керують ідентифікацією користувачів і контролюють доступ до ресурсів. Вони гарантують, що тільки автентифіковані та авторизовані користувачі отримують доступ до певних ресурсів.

Мережева інфраструктура

Мережева інфраструктура в моделі нульової довіри включає вдосконалені системи брандмауерів, захищені шлюзи та засоби контролю доступу до мережі. Ці компоненти працюють разом, щоб забезпечити дотримання політик безпеки та сегментувати мережу.

Безпека кінцевих точок

Кінцеві точки часто є найслабшою ланкою в системі кібербезпеки. Нульова довіра вимагає надійних заходів захисту кінцевих точок, включаючи антивірусне програмне забезпечення, інструменти виявлення та реагування на загрози та регулярне управління виправленнями.

Безпека даних

Безпека, орієнтована на дані, передбачає захист даних у стані спокою, під час передачі та використання. Шифрування, засоби запобігання втраті даних (DLP) та суворий контроль доступу є важливими компонентами безпеки даних у моделі zero trust [2].

Однією з основних технологій для реалізації стратегії нульової довіри є доступ до мережі з нульовою довірою (ZTNA). Як і віртуальна приватна мережа (VPN), ZTNA забезпечує віддалений доступ до додатків і сервісів. На відміну від VPN, ZTNA з'єднує користувачів лише з тими ресурсами, до яких вони мають дозвіл, а не підключає їх до всієї мережі.

ZTNA є ключовою частиною моделі SASE (secure access service edge), яка дозволяє компаніям надавати прямі, безпечні з'єднання з низькою затримкою між користувачами та ресурсами.

У широкому розумінні, політика безпеки з нульовою довірою працює шляхом постійної перевірки та автентифікації з'єднань між користувачами, додатками, пристроями та даними.

Впровадження стратегії zero trust в організації може бути складним завданням. Йдеться не про встановлення одного рішення з нульовою довірою. Zero trust вимагає планування і реалізації в широкому спектрі функціональних областей, включаючи політики ідентифікації та доступу, рішення безпеки і робочі процеси, автоматизацію, операції і мережеву інфраструктуру [1].

Перелік посилань:

1. IBM. What Is Zero Trust? | IBM. IBM - United States. URL: https://www.ibm.com/topics/zero-trust
2. What is zero trust architecture? - HotBot. *HotBot: Smarter Answers. AI Made Easy, Ask Your Question Now.* URL: https://www.hotbot.com/answers/what-is-zero-trust-architecture

Мишко Андрій Андрійович

студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

Технологія виявлення аномалій у корпоративній мережі за допомогою IDS з використанням ML

Актуальність теми обумовлена зростанням складності та масштабів сучасних кібератак, які часто обходять традиційні системи виявлення вторгнень (IDS). Використання машинного навчання (ML) для виявлення аномалій у мережах пропонує новий підхід, який дозволяє підвищити ефективність виявлення загроз шляхом аналізу великих обсягів даних у реальному часі та виявлення прихованих закономірностей.

Мета роботи

Розробка та дослідження технології виявлення аномалій у корпоративних мережах за допомогою систем IDS із інтеграцією методів машинного навчання. Оцінка ефективності комбінованого використання IDS та ML для покращення виявлення аномальних активностей.

Основні завдання

1. Огляд існуючих підходів до виявлення аномалій у корпоративних мережах із застосуванням традиційних IDS.
2. Дослідження можливостей використання ML-алгоритмів для виявлення аномалій.
3. Розробка інтегрованої системи, що поєднує функціонал IDS (на базі Snort або Suricata) та інструменти ML (Scikit-learn або TensorFlow).
4. Оцінка ефективності системи на реальних мережевих даних із використанням ключових метрик, таких як точність, повнота та F1-міра.

Методологія дослідження

Для реалізації поставлених завдань використовуються наступні підходи та інструменти:

- **IDS-системи**: Snort та Suricata, що є потужними інструментами для аналізу мережевого трафіку та базуються на правилах для виявлення аномалій.
- **Інструменти ML**: Бібліотеки **Scikit-learn** та **TensorFlow** для побудови моделей, що здійснюють класифікацію мережевих даних на аномальні та нормальні.
- **Збір даних**: Використання тестових датасетів, таких як **NSL-KDD** або **CICIDS**, для навчання та оцінки моделей.
- **Аналіз даних**: Попередня обробка логів мережевого трафіку, створення ознак для ML та використання методів зниження розмірності, таких як PCA.

Огляд теоретичних основ

Традиційні IDS-системи використовують сигнатурний або поведінковий підхід для виявлення аномалій. Проте обмеження сигнатурного підходу включають відсутність можливості виявлення невідомих атак. Використання машинного навчання дозволяє покращити виявлення, застосовуючи алгоритми класифікації (наприклад, **Random Forest**, **Support Vector Machines**) та методи глибокого навчання, такі як **нейронні мережі**.

Розробка та інтеграція системи

1. **Архітектура системи**: IDS (Snort або Suricata) здійснює попередній аналіз трафіку та передає логи для подальшої обробки алгоритмами ML.
2. **Алгоритми навчання**: Після збору та обробки даних модель навчається розпізнавати шаблони аномальної поведінки. Вибір алгоритму визначається експериментальними даними та аналізом продуктивності моделей.
3. **Інтеграція**: Взаємодія між IDS та компонентом ML реалізується за допомогою обміну даними через API або файли, що дозволяє автоматизувати передачу та аналіз інформації.

Експериментальна частина

Для тестування системи використовується симуляція різних сценаріїв атак (наприклад, DoS, сканування портів) та нормальних мережевих подій. Вимірюються такі ключові показники:

- **Точність (Accuracy)** — співвідношення правильно класифікованих випадків до загальної кількості випадків.
- **Повнота (Recall)** — частка справжніх позитивних випадків, які були правильно виявлені.
- **F1-міра** — гармонійне середнє між точністю та повнотою.

Результати та обговорення

Очікується, що інтеграція ML з IDS дозволить покращити здатність системи виявляти нові та невідомі типи атак, підвищуючи гнучкість і адаптивність системи. Аналіз результатів показує, наскільки ефективним є підхід порівняно з традиційними методами, та визначає шляхи оптимізації моделі.

Висновки

Запропонований підхід демонструє перспективність використання методів машинного навчання для розширення функціональності традиційних IDS-систем. У результаті дослідження надано рекомендації щодо використання різних ML-алгоритмів для підвищення точності виявлення та забезпечення кібербезпеки корпоративних мереж.

Подальші перспективи дослідження

Розширення роботи передбачає дослідження можливостей застосування глибоких нейронних мереж для покращення якості виявлення аномалій, інтеграцію з іншими системами захисту та створення автоматизованої системи реагування на виявлені інциденти.

Перелік посилань:

1. Wazuh Documentation URL: https://documentation.wazuh.com (дата звернення:15.10.2024).
2. Osquery Official Site URL: https://osquery.io (дата звернення: 15.10.2024).
3. Scikit-learn User Guide URL: https://scikit-learn.org/stable/user_guide.html (дата звернення: 15.10.2024).
4. TensorFlow Tutorials URL: https://www.tensorflow.org/tutorials (дата звернення: 15.10.2024).
5. Suricata IDS Documentation URL: https://suricata.io/documentation/ (дата звернення: 17.10.2024).
6. Snort Users Manual URL: https://www.snort.org/documents (дата звернення:17.10.2024).

Сідько Дмитро Вікторович
студент групи БСДМ-63, ННІКБЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНИХ ТЕХНОЛОГІЙ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Безпека хмарних технологій - це сукупність процедур і технологій, призначених для протидії зовнішнім і внутрішнім загрозам безпеці бізнесу. Організації потребують хмарної безпеки, оскільки вони рухаються до своєї стратегії цифрової трансформації та включають хмарні інструменти та сервіси як частину своєї інфраструктури.

«Хмара» або, точніше, “хмарні обчислення” - це процес доступу до ресурсів, програмного забезпечення та баз даних через Інтернет і поза межами локальних апаратних обмежень. Ця технологія дає організаціям гнучкість при масштабуванні своїх операцій, передаючи частину або більшість функцій управління інфраструктурою стороннім хостинг-провайдерам.

Найпоширенішими та найпоширенішими сервісами хмарних обчислень є

IaaS (Інфраструктура як послуга): Пропонує гібридний підхід, який дозволяє організаціям управляти деякими своїми даними і додатками на місці. У той же час, він покладається на хмарних провайдерів для управління серверами, обладнанням, мережею, віртуалізацією та потребами у сховищах.

PaaS (Платформа як послуга): Дає організаціям можливість спростити розробку та доставку додатків. Це відбувається завдяки наданню власної платформи для додатків, яка автоматично керує операційними системами, оновленнями програмного забезпечення, сховищем та допоміжною інфраструктурою в хмарі.

SaaS (програмне забезпечення як послуга): Надає хмарне програмне забезпечення, розміщене в Інтернеті і, як правило, доступне на основі підписки. Сторонні провайдери керують усіма потенційними технічними проблемами, такими як дані, проміжне програмне забезпечення, сервери та сховища. Така схема допомагає мінімізувати витрати на IT-ресурси та оптимізувати функції обслуговування й підтримки [1].

Типи хмарних рішень для забезпечення безпеки

Управління ідентифікацією та доступом (IAM)

Інструменти та сервісиуправління ідентифікацією та доступом (IAM)

дозволяють підприємствам розгортати протоколи на основі політик для всіх користувачів, які намагаються отримати доступ як до локальних, так і до хмарних сервісів. Основна функціональність IAM полягає у створенні цифрових ідентифікаторів для всіх користувачів, щоб їх можна було активно контролювати та обмежувати, коли це необхідно, під час усіх взаємодій з даними.

Запобігання втраті даних (DLP)

Служби запобігання втраті даних (DLP) пропонують набір інструментів і послуг, призначених для забезпечення безпеки регульованих хмарних даних. Рішення DLP використовують комбінацію сповіщень про усунення несправностей, шифрування даних та інших превентивних заходів для захисту всіх збережених даних, незалежно від того, перебувають вони в стані спокою чи в русі.

Управління інформацією та подіями безпеки (SIEM)

Управління інформацією та подіями безпеки (SIEM) - це комплексне рішення для оркестрування безпеки, яке автоматизує моніторинг, виявлення та реагування на загрози в хмарних середовищах. Технологія SIEM використовує технології на основі штучного інтелекту (ШІ) для кореляції даних журналів на різних платформах і цифрових активах. Це дає IT-командам можливість успішно застосовувати протоколи мережевої безпеки, дозволяючи їм швидко реагувати на будь-які потенційні загрози.

Безперервність бізнесу та аварійне відновлення

Незалежно від превентивних заходів, які організації вживають для своїх локальних і хмарних інфраструктур, витоки даних і руйнівні збої в роботі все одно можуть відбуватися. Підприємства повинні мати можливість швидко реагувати на нещодавно виявлені вразливості або значні системні збої в найкоротші терміни. Рішення для аварійного відновлення є основою безпеки хмарних технологій і надають організаціям інструменти, сервіси і протоколи, необхідні для прискорення відновлення втрачених даних і відновлення нормальної роботи бізнесу [2].

Безпека хмарних технологій в основному зосереджена на тому, як впроваджувати політики, процеси і технології разом, щоб вони забезпечували захист даних, підтримували відповідність нормативним вимогам і забезпечували контроль над конфіденційністю, доступом і автентифікацією для користувачів і пристроїв.

Постачальники хмарних послуг зазвичай дотримуються моделі спільної відповідальності, що означає, що за безпеку хмарних обчислень відповідає як постачальник хмарних послуг, так і ви -клієнт. Думайте про це як про структуру відповідальності, яка визначає, які завдання з безпеки належать до компетенції постачальника хмарних послуг, а які - до обов'язків клієнта. Розуміння того, де закінчуються обов'язки провайдера і починаються організації, має вирішальне значення для побудови стійкої стратегії безпеки хмарних технологій.

Перелік посилань:

1. What Is Cloud Security? | Google Cloud. Google Cloud. URL: https://cloud.google.com/learn/what-is-cloud-security
2. IBM. Cloud Security | IBM. IBM - United States. URL: https://www.ibm.com/topics/cloud-security

Шулімова Дар'я Денисівна
асистент кафедри СТКБ, ННІКБЗІ ДУІКТ, Київ, Україна

ШТУЧНИЙ ІНТЕЛЕКТ У КІБЕРБЕЗПЕЦІ: ВДОСКОНАЛЕННЯ ПРОЦЕСІВ ВИЯВЛЕННЯ ЗАГРОЗ ТА АВТОМАТИЗАЦІЇ ЗАХИСТУ

Штучний інтелект здійснив революцію в багатьох галузях, зокрема в кібербезпеці. Однією з головних загроз у цифровому просторі є веб-зловмисне програмне забезпечення, яке є імплантатом зловмисного програмного забезпечення на нешкідливих і законних веб-сайтах, призначених для шкоди, крадіжки або порушення систем нічого не підозрюючих відвідувачів веб-сайту. Це можуть бути віруси, хробаки, трояни та програми-вимагачі.

Штучний інтелект забезпечує надзвичайну швидкість аналізу та здатність виявляти закономірності й аномалії у величезних обсягах даних, таких як мережевий трафік, журнали системної діяльності та поведінкові дані користувачів. Ця здатність миттєвого виявлення, навіть найдрібніших відхилень від норми, дозволяє реагувати на загрози швидше та більш ефективно, ніж це можливо за допомогою традиційних методів. Завдяки проактивному аналізу та прогнозуванню, ШІ сприяє побудові більш надійної системи кіберзахисту, яка може передбачити атаки до того, як вони стануть критичними.

Однією з найбільших переваг використання ШІ є адаптивність його алгоритмів. Завдяки можливості навчатися на базі минулих атак, аналізуючи специфічні методи зловмисників, системи на основі ШІ стають здатними оперативно оновлювати стратегії захисту, зберігаючи організації на крок попереду кіберзлочинців. Така адаптивність особливо важлива в умовах, коли методи атак постійно еволюціонують, і традиційні засоби виявлення стають менш ефективними.

Завдяки автоматизації багатьох рутинних завдань ШІ підвищує ефективність роботи аналітиків кібербезпеки, дозволяючи їм зосередитись на складніших питаннях та стратегічному плануванні. ШІ забезпечує значно вищу точність обробки даних, зменшуючи ризик упущення критичних загроз та знижуючи кількість помилкових сповіщень, що є особливо актуальним в умовах зростаючого обсягу кіберзагроз.

ШІ також дозволяє вдосконалити моніторинг користувацької поведінки. Наприклад, він може аналізувати щоденну активність користувачів, виділяючи незвичні дії, що можуть сигналізувати про внутрішню загрозу або компрометацію облікового запису. Завдяки цьому безпекові команди можуть отримувати своєчасні сповіщення про підозрілі дії, такі як несанкціоновані спроби доступу до конфіденційних даних, що дозволяє вчасно реагувати на потенційні загрози.

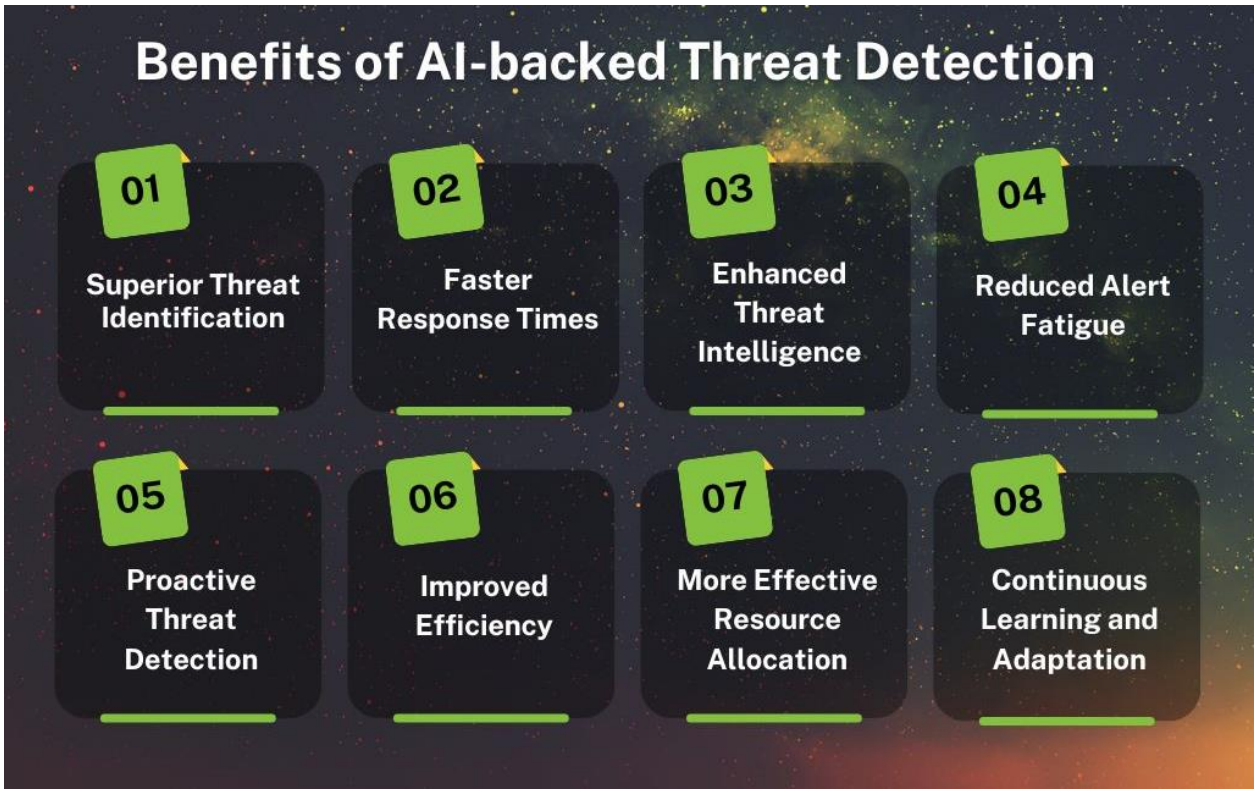


Рис. 1. Переваги виявлення загроз за допомогою ШІ

Хоча переваги ШІ у кібербезпеці є суттєвими, варто зазначити і недоліки, з якими стикаються фахівці. По-перше, ефективність ШІ у виявленні загроз значною мірою залежить від якості наявних даних. У випадку, якщо дані містять помилки чи мають упереджений характер, це може призвести до хибно позитивних чи негативних результатів, що негативно вплине на безпеку. Також складність деяких алгоритмів ШІ може стати проблемою з точки зору прозорості: розуміння того, чому система класифікувала конкретну активність як загрозу, є важливим для довіри користувачів до таких систем.

Іншим аспектом є вразливість самих систем ШІ до атак. Наприклад, зловмисники можуть спробувати обійти захист, створюючи «нормальні» зразки поведінки, які насправді є атаками. Висока складність впровадження та підтримки таких систем також вимагає від фахівців глибоких знань і досвіду в налаштуванні та адаптації алгоритмів.

Незважаючи на виклики, потенціал ШІ для кібербезпеки з кожним роком тільки зростає. Інноваційні методи, наприклад пояснювальний ШІ (Explainable AI), який здатен пояснювати свої рішення, або обчислення із захистом конфіденційності (Privacy-Preserving AI), дозволяють зберігати прозорість процесу і захищати персональні дані користувачів. З розвитком методів аналізу поведінки, автоматизації та оркестрації, а також появою нових напрямів, таких як захист периферійних пристроїв (edge computing security), ШІ стає не тільки інструментом для виявлення загроз, але й платформою для вдосконалення всіх аспектів кібербезпеки.

Таким чином, використання ШІ у кібербезпеці є надзвичайно перспективним напрямом, здатним забезпечити високий рівень захисту від загроз, автоматизувати та спрощувати процеси кіберзахисту та мінімізувати ризики, пов’язані з людським фактором.

Перелік посилань:
1. https://www.sangfor.com/blog/cybersecurity/role-of-artificial-intelligence-ai-in-threat-detection
2. https://www.dekeneas.com/blog/role-of-ai-in-detecting-web-malware.html

Сидоренко Володимир Дмитрович
Студент групи БСДМ-62 ННІЗІ ДУКІТ, Київ, Україна

Технологія розширеного виявлення загроз кінцевим точкам та реагування на них

Згідно зі звітом Sophos 2024 Threat Report, організації стикаються зі складнощами у виявленні загроз через зростання кібератак на віддалені робочі середовища. Програми-вимагачі залишаються головною загрозою, часто націленою на малі підприємства, які вразливі через брак ресурсів та фахівців.

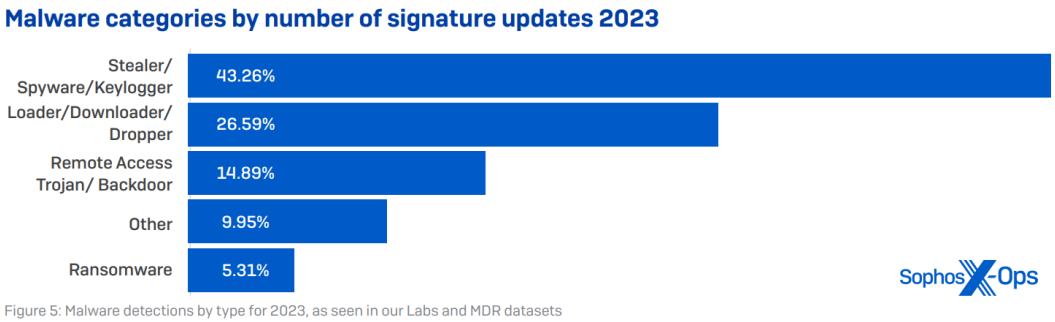


Рис. 1. Категорії шкідливих програм за кількістю оновлень сигнатур 2023

Кіберзлочинці використовують "зловмисне ПЗ як послугу", що спрощує доступ до шкідливих програм через підпільні ринки. Завдяки змінам безпеки Microsoft, методи розповсюдження ПЗ еволюціонували до використання файлів PDF, OneNote та веб-реклами.

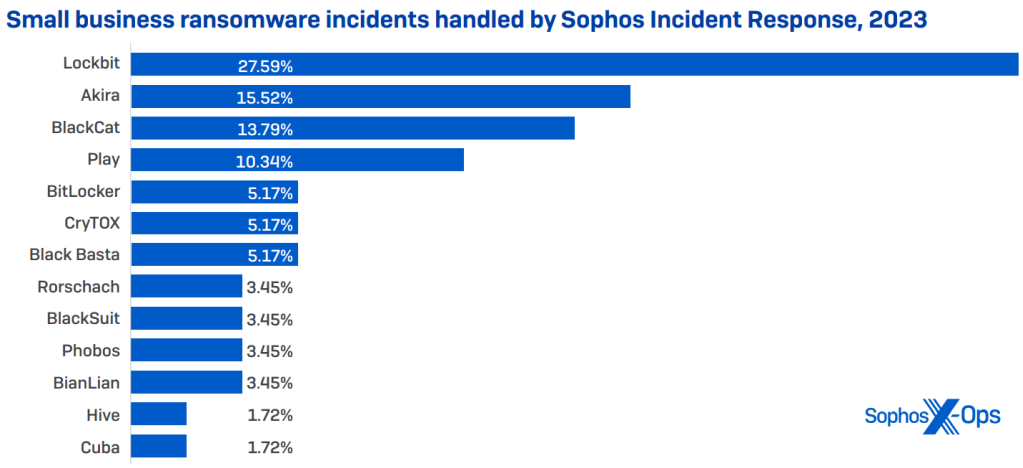


Рис. 2. Інциденти програм-вимагачів для малого бізнесу, оброблені Sophos Incident Response, 2023

Малі підприємства зазнають значного ризику від таких атак, які можуть призвести до закриття бізнесу.

EDR забезпечує командам безпеки контроль і моніторинг кінцевих точок, виявлення некерованих пристроїв, зменшення ризиків, реальний час аналізу підозрілої активності, а також блокування загроз. Завдяки машинному навчанню EDR виявляє складні атаки, інтегрується з SIEM і SOAR для автоматизації реагування. Це допомагає мінімізувати час виявлення та реагування на інциденти, дозволяє швидко ізолювати заражені системи та аналізувати післяінцидентні дані для підвищення безпеки [1].

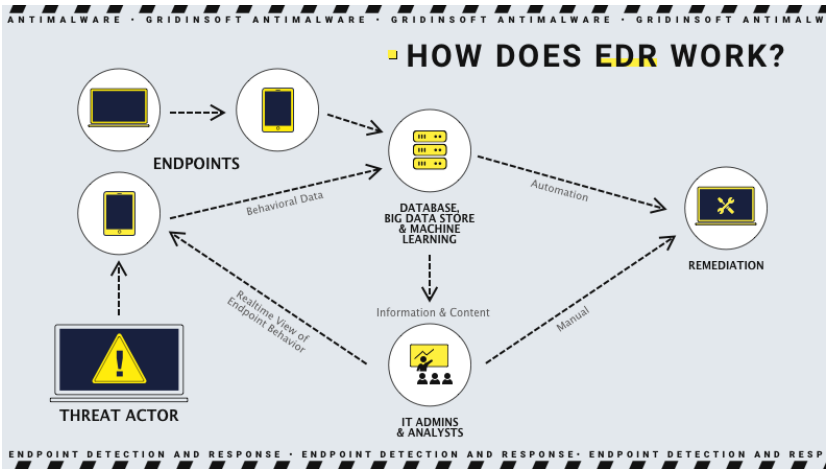


Рис. 3. Принцип роботи розширеного виявлення загроз на кінцеві

EDR відповідає стандартам NIST та використовує MITRE ATT&CK для точного визначення тактик атак. EDR використовує машинне навчання для аналізу даних з кінцевих точок, допомагаючи виявляти складні загрози, включно з "безфайловими" атаками. Система інтегрується з SIEM та SOAR для ефективного моніторингу й автоматизації процесів реагування. EDR також забезпечує постінцидентний аналіз, дозволяючи досліджувати проникнення загроз і розробляти кращі політики безпеки [2]. Переваги включають зменшення часу на виявлення (MTTD) та реагування (MTTR), швидку нейтралізацію загроз і постійне оновлення для протидії новим атакам. EDR базується на стандартах NIST CSF та використовує MITRE ATT&CK для покриття різних технік атак.

Figure 1: Magic Quadrant for Endpoint Protection Platforms

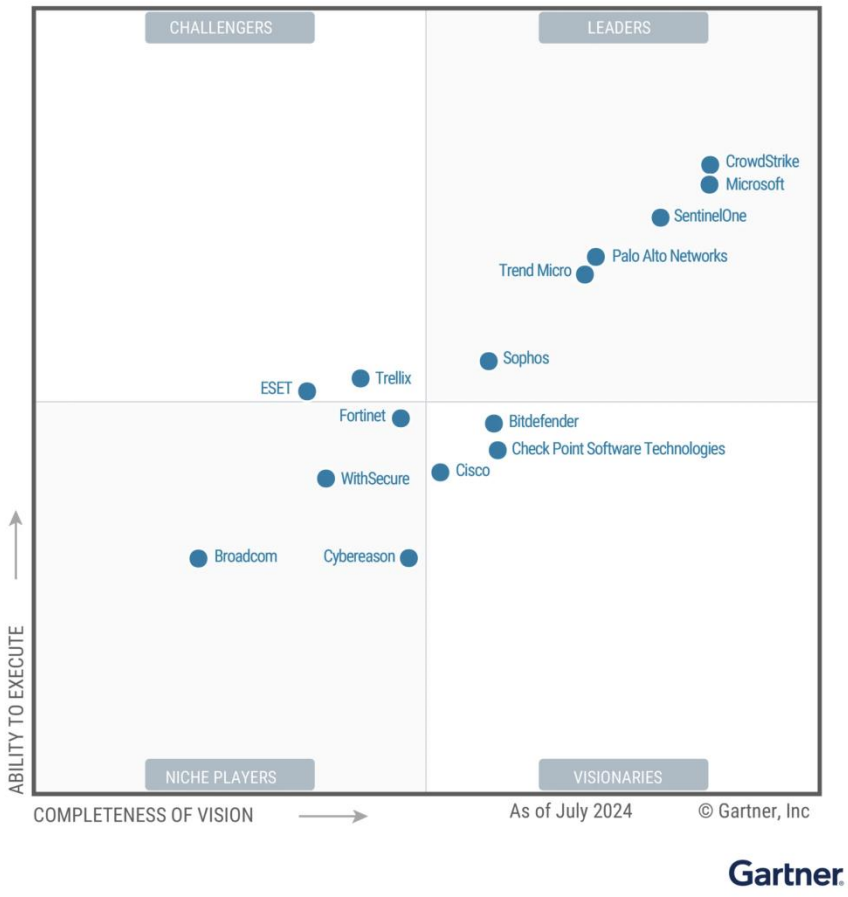


Рис. 4. Магічний квадрант Гартнера станом на 2024 рік для платформ з технологіями розширеного виявлення загроз кінцевим точкам

Також, в EDR-рішеннях лідирують такі продукти:

CrowdStrike Falcon – хмарне рішення, що використовує штучний інтелект для швидкого виявлення та реагування на загрози. Переваги: швидке розгортання, мінімальний вплив на систему, аналіз загроз у реальному часі, захист від атак без файлів та мобільних загроз.

SentinelOne – автоматизує виявлення, реагування та відновлення після атак. Підходить для організацій, що потребують швидкої реакції. Містить судово-медичні функції та простий у використанні [2].

Microsoft Defender for Endpoint – інтегрований з екосистемою Microsoft, використовує AI для захисту кінцевих точок. Підтримує різні ОС, забезпечує автоматизацію реагування та детальний аналіз інцидентів.

Ці компанії є лідерами в галузі завдяки своїм інноваційним підходам до виявлення загроз і реагування на інциденти, а також постійному розвитку своїх технологій.

Перелік посилань:

1. Sophos 2024 Threat Report. URL: https://assets.sophos.com/X24WTUEQ/at/wwf5phjtj9bjvmpqqsbfxc/sophos-2024-threat-report.pdf (дата звернення 15.10.2024)
2. Лідери 2024. Магічний квадрант Гартнера. URL: https://www.paloaltonetworks.com/blog/2024/09/a-leader-in-the-2024-gartner-magic-quadrant-for-epp/ (дата звернення 15.10.2024)

Шпортко Дмитро Вікторович
Студент групи БСДМ-62, ННІЗІ ДУІКТ, Київ, Україна

Технологія уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile

Звіт Verizon Mobile Security Index 2024 року висвітлює важливі питання безпеки мобільних пристроїв, зокрема у критично важливих секторах інфраструктури, зростанні IoT та розвитку штучного інтелекту. Він також показує розрив між уявленнями респондентів про мобільний захист і реальністю, де більшість вважає, що захист є надійним, хоча насправді атаки

та порушення часто мають серйозні наслідки. Респонденти повідомляють про зростаючу роль мобільних пристроїв у роботі організацій, зокрема через віддалену і гібридну роботу, а також про збільшення їх доступу до конфіденційної інформації [1].

92% організацій підтримують віддалену роботу, і більшість працівників цінують гнучкість. Мобільні пристрої стають важливішими для бізнесу: 50% зазначають, що вони мають більший доступ до конфіденційної інформації, ніж рік тому. У зв'язку з цим, мобільна безпека стає пріоритетом, оскільки більше пристроїв підключається до корпоративних мереж, що збільшує складність екосистем і загрози для безпеки[1].

Інтернет речей (IoT) також розширює свої можливості, допомагаючи в різних галузях, від охорони здоров'я до промисловості, що підвищує потребу в стратегіях безпеки для цих пристроїв[1].

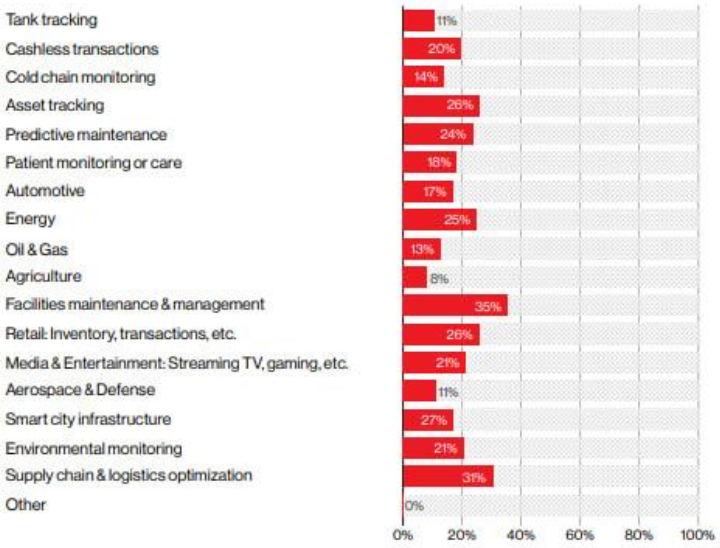


Рис. 1. Використання датчиків або пристроїв IoT

Національний інститут стандартів і технологій (NIST) визначає критичну інфраструктуру як основну частину економіки та безпеки суспільства, що робить її мішенню для атак. Зростаюче використання IoT-пристроїв у цих секторах підвищує кіберризики. Пристрої IoT використовуються для моніторингу та керування системами в різних галузях, таких як енергетика, транспорт і охорона здоров'я, підвищуючи ефективність

і безпеку [1].

Проте, багато з цих пристроїв мають слабкий захист і вразливі до атак, що розширює поверхню потенційних загроз. Їх часто не контролюють належним чином, а деякі пристрої мають застаріле обладнання та слабкі паролі за замовчуванням. Це створює серйозні проблеми для безпеки, особливо у критичних інфраструктурах, де відсутність оновлень та стандартів збільшує ризики [1].

Управління мобільними пристроями (MDM) — це ключовий інструмент для забезпечення безпеки корпоративних даних на мобільних пристроях, таких як смартфони, планшети та ноутбуки [1].

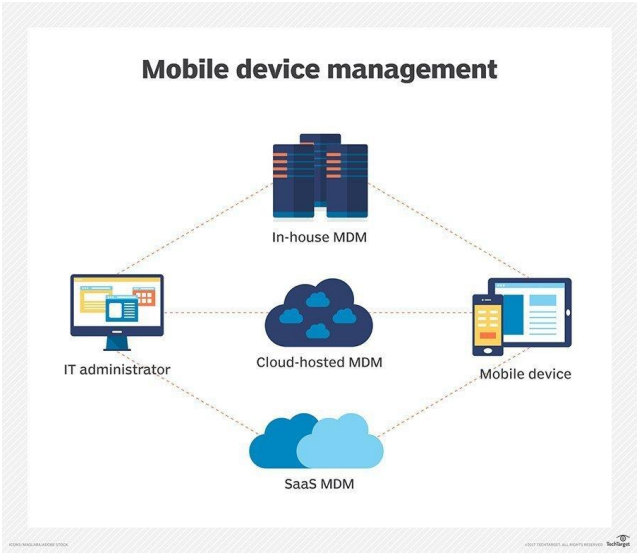


Рис. 2. Структура управління мобільними пристроями

В умовах поширення віддаленої роботи, MDM дозволяє IT-відділам і службам безпеки ефективно контролювати пристрої, захищати дані та забезпечувати продуктивність співробітників. MDM включає програмне забезпечення, політики та процеси для керування доступом, захисту даних і програм, а також моніторингу поведінки пристроїв. Важливими функціями є встановлення паролів, відстеження пристроїв, а також можливість видалення даних у разі крадіжки чи втрати. MDM є важливою складовою мобільної безпеки, дозволяючи організаціям мінімізувати ризики кіберзагроз [1].

Рис. 3. магічний квадрант Гартнера за 2017 рік для платформ з технолгоіями уніфікованого керування безпекою корпоративних мобільних пристрої

VMware Workspace ONE – комплексна платформа для управління мобільними пристроями та безпекою корпоративних даних. Вона забезпечує централізоване управління кінцевими точками, підтримує MDM, IAM, Zero Trust безпеку, шифрування даних та умовний доступ. Це рішення допомагає компаніям захищати пристрої, додатки та дані через єдину платформу з можливістю віддаленого управління.

Ivanti (MobileIron) – рішення для управління мобільними пристроями, додатками та контентом, яке включає функції MDM, UEM, Zero Trust, шифрування та захист від мобільних загроз. Платформа дозволяє контролювати доступ до корпоративних ресурсів, забезпечує шифрування даних і виявлення загроз в режимі реального часу.

BlackBerry UEM – рішення для управління мобільними пристроями та захисту даних з підтримкою багатофакторної автентифікації, шифрування, контейнеризації та Zero Trust. Платформа забезпечує гнучке масштабування, контроль доступу та моніторинг відповідності політикам безпеки на різних пристроях і платформах.

Ці компанії стали лідерами галузі завдяки своїм новаторським рішенням у сфері керування безпекою корпоративних мобільних пристроїв. Їх успіх зумовлений не лише високою ефективністю поточних технологій, але й

постійним вдосконаленням своїх платформ, щоб відповідати динамічним викликам сучасної кібербезпеки. Завдяки безперервному впровадженню інновацій, вони здатні передбачати нові типи загроз і вчасно адаптувати свої стратегії, що дозволяє їм зберігати конкурентну перевагу та відповідати потребам найвимогливіших клієнтів.

Перелік посилань:

1. Звіт 2024 Mobile Security Index URL: https://www.verizon.com/business/resources/reports/mobile-security-index/
2. What is mobile device management (MDM)? URL: https://www.ibm.com/topics/mobile-device-management

Веселков Нікіта Леонідович
аспіранта групи АІКБ-21, ННІЗІ ДУІКТ, Київ, Україна

ПРОЦЕСИ РОЗГАЛУЖЕНИХ SOC КОМАНД ПІД ЧАС РЕАГУВАННЯ ТА РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

Розглянуто особливості організації роботи розгалужених SOC команд під час реагування на кіберінциденти та їх розслідування, включаючи інтеграцію процесів збору даних, аналізу подій та координації між різними групами. Окреслено ключові компоненти та підходи, що сприяють підвищенню ефективності SOC в умовах розподіленої інфраструктури та складних кіберзагроз.

Ключові слова: SOC, розгалужені команди, реагування на інциденти, кіберрозслідування, координація, автоматизація.

Сучасні кіберзагрози вимагають від Центрів операцій з кібербезпеки (SOC) не лише швидкого реагування, а й здатності до синхронізованої роботи між кількома розгалуженими командами. Організація ефективних процесів між підрозділами, розподіленими територіально або функціонально, є ключовим викликом. У даній тезі представлено підходи до побудови процесів реагування та розслідування кіберінцидентів у таких умовах.

Організація SOC-команд має забезпечити виконання чотирьох основних етапів процесу реагування, визначених у NIST SP 800-61 Rev. 2: підготовка, виявлення та аналіз, реагування, а також післяінцидентний аналіз [3].

1. Підготовка (Preparation):
   - Визначення політик реагування на інциденти, їх впровадження та регулярний перегляд.
   - Підготовка та оновлення Playbook'ів для кожного типу інциденту (наприклад, DDoS, malware-атака, компрометація облікового запису).
   - Використання SIEM-систем (наприклад, Splunk, IBM QRadar) для автоматичного збору подій.

- Симуляції та тренінги: регулярне проведення тренінгів і симуляцій атак для підвищення готовності персоналу та систем.

2. Виявлення та аналіз (Detection and Analysis):
   - Моніторинг мережі та систем у реальному часі за допомогою SIEM та SOAR-рішень (Security Orchestration, Automation, and Response).
   - Використання автоматизованих інструментів кореляції подій для фільтрації та пріоритизації інцидентів.
   - Збір форензічних даних (мережеві логи, dump пам’яті, дані з дисків) відповідно до NIST SP 800-86.
3. Реагування (Containment, Eradication, and Recovery):
   - Впровадження стратегій ізоляції уражених систем для запобігання подальшому розповсюдженню загроз.
   - Автоматичне блокування підозрілої активності (IP-адреси, хеші файлів) через SOAR.
   - Проведення форензічного аналізу та документування результатів для юридичних цілей або внутрішніх розслідувань.
4. Післяінцидентний аналіз (Post-Incident Activity):
   - Проведення пост-інцидентних розборів (Post-Mortem) для визначення ефективності заходів реагування.
   - Внесення змін до Playbook'ів та навчальних матеріалів на основі висновків розслідування.
   - Оновлення політик та процедур згідно з новими стандартами та рекомендаціями, зокрема ISO/IEC 27035:2011.

Як керівник SOC-команди, я розумію, що розгалужені команди повинні діяти як єдиний організм, де кожен підрозділ виконує свою чітко визначену роль. Важливим завданням у такій структурі є забезпечення ефективної координації між командами, які можуть працювати у різних часових зонах і на різних рівнях інфраструктури. З мого досвіду, для цього необхідно інтегрувати сучасні комунікаційні платформи з інструментами управління інцидентами, а також побудувати процеси на основі міжнародних стандартів і практик.

Для швидкої комунікації ми використовуємо Microsoft Teams, що дозволяє об'єднати всіх учасників процесу на єдиній платформі. Це забезпечує не лише миттєвий обмін повідомленнями, але й створення каналів для окремих інцидентів, де кожна зміна статусу події фіксується в режимі реального часу. Крім того, Teams інтегрується з нашими SIEM- та SOAR-системами, що дозволяє автоматично отримувати сповіщення про критичні події без затримок. Наприклад, коли система виявляє аномальну активність у мережі, інформація одразу потрапляє до відповідної групи в Teams, що прискорює процес реагування.

Координація процесу розслідування інцидентів відбувається через інцидент-менеджмент платформу ServiceNow. Це рішення дає можливість структуровано розподіляти завдання між підрозділами, а також контролювати виконання в реальному часі. Важливо, щоб у таких системах кожен крок

команди був зафіксований – це дозволяє не лише тримати процес під контролем, але й проводити ретельний післяінцидентний аналіз. Завдяки інтеграції з SOAR, певні рутинні дії, як-от ізоляція хостів чи блокування підозрілих IP-адрес, виконуються автоматично, звільняючи ресурси аналітиків для більш глибинної роботи.

Важливим аспектом управління SOC є дотримання міжнародних стандартів, таких як ISO/IEC 27035, які структурують увесь процес управління інцидентами – від виявлення загрози до післяінцидентного аналізу. Дотримання цих стандартів не лише підвищує ефективність реагування, а й забезпечує відповідність регуляторним вимогам, що критично важливо для захисту даних. З моєї практики, стандартизований підхід допомагає уникнути хаосу під час реагування на великі інциденти та забезпечує послідовність дій навіть у кризових ситуаціях.

Модель MITRE ATT&CK стала для нас ключовим інструментом аналізу та прогнозування загроз. Вона дозволяє структурувати всі можливі тактики й техніки зловмисників, що ми використовуємо для налаштування наших Playbook’ів. Це дає можливість прогнозувати наступні кроки нападника та готувати відповідні контрзаходи. Наприклад, ми аналізуємо попередні інциденти з використанням MITRE ATT&CK і на основі цього змінюємо правила детектування, щоб адаптуватися до нових атак.

Автоматизація процесів через штучний інтелект та машинне навчання є невід'ємною частиною роботи нашого SOC. Використання цих технологій дозволяє аналізувати величезні обсяги даних і виявляти аномалії, які можуть свідчити про потенційні загрози. Наприклад, наші системи UEBA аналізують поведінку користувачів і виявляють відхилення, що можуть свідчити про компрометацію облікового запису. Крім того, завдяки машинному навчанню ми постійно вдосконалюємо алгоритми детектування, що допомагає значно зменшити кількість хибних спрацювань.

Такий підхід до управління SOC дозволяє не лише ефективно реагувати на загрози, але й активно готуватися до можливих атак, прогнозуючи дії зловмисників. Ключовим для мене як керівника є забезпечення балансу між автоматизацією та людським контролем: ми використовуємо сучасні технології, але водночас покладаємося на досвід і компетенції наших аналітиків. Це забезпечує високий рівень стійкості нашої інфраструктури й дозволяє ефективно захищати організацію навіть у найскладніших умовах.

Організація SOC у розподіленому середовищі вимагає тісної координації між командами, впровадження передових технологій та відповідності міжнародним стандартам. Автоматизація процесів реагування, інтеграція SOAR-рішень та регулярні тренування дозволяють забезпечити високу ефективність роботи. Розвиток внутрішніх стандартів безпеки та залучення міжнародного досвіду є необхідними умовами для побудови стійкої системи кіберзахисту.

Перелік посилань:

7. ISO 18788.

8. ISO/IEC 27035:2011.
9. NIST SP 800-86.
10. MITRE ATT&CK Framework.

Іванкін Віктор Андрійович
студент групи АІКБ-11, ННІЗІ ДУІКТ, Київ, Україна

ZERO TRUST АРХІТЕКТУРА ЯК МОДЕЛЬ БЕЗПЕКИ ДЛЯ СУЧАСНИХ ОРГАНІЗАЦІЙ

Управління інформаційною безпекою є критично важливим питанням для всіх, хто працює з технологіями або піддається ризику порушень безпеки, оскільки наслідки цих вразливостей можуть бути критичними. Багато організацій стикаються з постійними загрозами витоку даних, що може призвести до серйозних компрометації конфіденційної інформації. Оскільки загрози безпеці розвиваються, організації повинні постійно працювати над захистом своїх даних. Впровадження системи безпеки відіграє вирішальну роль у захисті інформації як співробітників, так і клієнтів, пропонуючи впевненість у тому, що конфіденційні дані залишаються в безпеці. Вибір правильної системи безпеки для компанії є життєво важливим, хоча це може бути складним процесом, що вимагає ретельного врахування різних факторів.

В епоху стрімкої цифрової трансформації потреба в надійних та адаптивних системах безпеки є більш нагальною, ніж будь-коли. Зі зростанням залежності від хмарних сервісів, віддаленої роботи та поширенням мобільних пристроїв організації стають більш вразливими до кіберзагроз. Традиційні моделі безпеки, засновані на припущенні, що будь-чому в мережі можна довіряти, більше не є достатніми. Порушення зсередини мережі та скомпрометовані облікові дані дали зрозуміти, що потрібен інший підхід. Ця потреба призвела до появи архітектури безпеки Zero Trust.

Мета цієї роботи - дослідити архітектуру Zero Trust, вивчити її основні принципи та переваги для сучасних організацій.

Архітектура Zero Trust - це модель безпеки, яка передбачає, що жоден об'єкт, як всередині, так і поза мережею, не заслуговує на довіру за своєю суттю. На відміну від традиційних моделей безпеки на основі периметра, які зосереджені на захисті від зовнішніх загроз, довіряючи тим, хто знаходиться всередині мережі, Zero Trust працює за принципом «не довіряти нікому за замовчуванням». Він вимагає постійної перевірки кожного запиту на доступ, щоб переконатися, що суб'єкт, чи то користувач, чи то пристрій, має дозвіл на доступ до мережевих ресурсів. Такий підхід знижує ризик внутрішніх загроз і зовнішніх атак, оскільки безпека застосовується рівномірно по всій мережі.

Впроваджуючи сувору автентифікацію, контроль доступу та постійний моніторинг, Zero Trust гарантує, що користувачі мають лише той рівень доступу, який їм потрібен у будь-який момент часу.

Основні складові Zero Trust

1. Автентифікація та авторизація

Zero Trust наголошує на суворих процесах автентифікації та авторизації для перевірки ідентичності користувачів і пристроїв перед наданням їм доступу. Багатофакторна автентифікація (MFA) є ключовою особливістю цієї моделі, яка вимагає від користувачів підтверджувати свою особу за допомогою різних засобів, таких як паролі, біометричні дані або апаратні токени. На додаток до MFA, Zero Trust покладається на контекстне управління доступом, де рішення про доступ приймаються на основі інформації в реальному часі, такої як дії користувача, типи пристроїв або геолокація.

2. Мікросегментація

Фундаментальним аспектом Zero Trust є сегментація мережі, яка ділить мережу на менші ізольовані сегменти з жорстко контрольованими правилами доступу. Обмежуючи доступ до різних частин мережі, мікросегментація не дає зловмисникам просуватися далі, якщо їм вдасться проникнути в один сегмент. Кожен сегмент розглядається як незалежний об'єкт, і доступ до нього надається лише користувачам або пристроям, які відповідають суворим критеріям безпеки.

3. Безперервний моніторинг

Zero Trust не зупиняється на початковій автентифікації. Вона вимагає постійного моніторингу активності користувачів і пристроїв для виявлення будь-яких ознак аномалій або підозрілої поведінки. Цей безперервний моніторинг дозволяє командам безпеки швидко реагувати на потенційні загрози, зупиняючи зловмисників до того, як вони встигнуть завдати шкоди. Аналізуючи поведінку в режимі реального часу, наприклад, несподівані спроби входу в систему або незвичайні шаблони доступу до файлів, Zero Trust допомагає запобігти несанкціонованому доступу та порушенням, забезпечуючи проактивний підхід до кібербезпеки.

Але й існують недоліки впровадження Zero Trust:

- Складність впровадження: повна перебудова існуючої мережевої інфраструктури організації;
- Проблеми масштабування: може бути важко впровадити мікросегментацію у великих взаємопов'язаних мережах, не спричиняючи збоїв у повсякденній роботі;
- Людський фактор: співробітники можуть чинити опір новим процесам і більш суворим заходам контролю доступу.

Приклади впровадження Zero Trust в організаціях

Впровадження Zero Trust в Google мало значний вплив на загальний стан безпеки компанії. Google покращила здатність компанії захищатися від внутрішніх загроз, обмежити латеральне переміщення зловмисників і адаптуватися до зростаючої потреби в безпеці віддаленої роботи. Більше того, застосовуючи суворі процеси автентифікації та верифікації, Google знизив ризик витоку даних через скомпрометовані облікові дані, продемонструвавши потенціал Zero Trust для посилення безпеки і в інших організаціях. Успіх Zero

Trust залежить від постійного моніторингу та адаптивних політик безпеки, які вимагають постійних інвестицій як в технології, так і в персонал, які Google вчасно роблять.

Висновки

Архітектура Zero Trust пропонує значний прогрес у порівнянні з традиційними моделями безпеки на основі периметра, забезпечуючи посилений контроль, гнучкість і захист від сучасних кіберзагроз. Працюючи за принципом «не довіряй нікому», Zero Trust гарантує, що доступ до конфіденційних даних і систем надається лише після суворої автентифікації та безперервної перевірки. Її ключові компоненти, такі як багатофакторна автентифікація, мікросегментація та безперервний моніторинг, разом забезпечують багаторівневий захист від зовнішніх та внутрішніх загроз.

Зростаюча витонченість кібератак, а також зростаюче використання хмарних сервісів і віддаленої роботи зробили впровадження Zero Trust необхідним для сучасних організацій. Вона ефективно усуває вразливості в застарілих системах, мінімізуючи поверхню атаки, запобігаючи латеральному переміщенню в мережах і адаптуючись до динамічних, гібридних середовищ.

Перелік посилань:

11. National Institute of Standards and Technology (NIST). (2020). *NIST Special Publication 800-207: Zero Trust Architecture*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
12. Google Cloud. (2020). *BeyondCorp: A New Approach to Enterprise Security*. https://cloud.google.com/blog/products/identity-security/introducing-beyondcorp-enterprise
13. O'Neill, P. (2020). *Zero Trust Security: What It Is, and Why It Matters*. https://www.csoonline.com/article/3564582/zero-trust-security-what-it-is-and-why-it-matters.html
14. Microsoft Security. (2021). *Zero Trust Security: A Comprehensive Guide*. https://www.microsoft.com/security/blog/2021/03/11/zero-trust-security-a-comprehensive-guide/

Назаренко Валерія Дмитрівна
студентка групи БСД-12, ННІЗІ ДУІКТ, Київ, Україна

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ОДИН ІНСТРУМЕНТІВ ОТРИМАННЯ ЧУТЛИВИХ ДАНИХ. ОСНОВНІ ВИДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Соціальна інженерія (social engineering) – це надзвичайно потужний та діючий інструмент, який, використовують для здійснення цілей різноманітного характеру. Найчастіше цей вектор атаки використовують як спосіб доставки шкідливого програмного забезпечення або проникнення у мережу, але іноді він є кінцевою ціллю, наприклад в атаках, напрямлених на те, щоб оманою змусити жертву надати конкретну чутливу інформацію (логіни/паролі, відповіді на ключові питання, такі як дівоче прізвище матері, компромат, номера банківських карт тощо). В більшості випадках не важливий рівень захищеності приладу або інформації, людський фактор все ще є вразливою ціллю. За даними інфографіки від Verizon [1] за 2023 рік 74% всіх порушень частково були пов’язані з людською помилкою, зловживанням привілегіями, використанням викрадених облікових даних та соціальною інженерією. Зважаючи на це, нижче приведені деякі популярні загрози, які використовуються зловмисниками за допомогою соціальної інженерії.

Види соціальної інженерії.

Претекстінг (pretexting). Згідно концепції соціальної інженерії, претекстінг – це акт видачі себе за когось, відігравання певної ролі. Тобто іншими словами, це набір дій, що відпрацьовані за певним, заздалегідь складеним сценарієм, в результаті чого жертва може піти на контакт із зловмисником та видати потрібну йому інформацію або вчинити певну дію. Найчастіше цей вид атаки передбачає використання текстових або голосових засобів по типу відомих месенджерів тощо.

Для здійснення цієї атаки зловмиснику потрібно заздалегідь мати деяку інформацію про потенційну жертву (наприклад, ім'я, посаду на роботі, назву проєктів, над якими вона працює, дату народження і т.п), тобто виникає потреба в проведенні OSINT операції.

Розвідка за відкритими джерелами (open soutce intelligence, OSINT). Це збір інформації, в конкретному випадку про особу, за відкритими ресурсами, такими як газети/журнали, пошукові системи, документи з різних регулюючих органів, соціальні мережі, реклама, спостереження тощо.

Фішинг та цільовий фішинг. Техніка інтернет-шахрайства, спрямована на отримання конфіденційної інформації користувачів – авторизаційних даних систем. Поширеним видом фішингових атак є відправка фальшивих електронних листів, наприклад, від імені банку, освітньої установи або інших організацій. Часто в таких листах міститься форма для введення персональних даних (пароля, пін-коду, номера банківської карти тощо) або ж шкідливі посилання [2, с. 19].

Звичайні фішингові листи не адресовані конкретній особі, тобто зловмисники проводять розсилку за численними «злитими» адресами користувачів, на відміну від листів, складених для цільового фішингу.

Троянський кінь. Цей вид атаки ґрунтується на емоціях потенційної жерти, наприклад, на страху, цікавості тощо. Зловмисник надсилає користувачу, наприклад, електронного листа, у вкладенні до якого міститься посилання на оновлення програми, ключ до виграшу або компромат на співробітника. Насправді у вкладенні міститься шкідливе ПО, яке після запуску користувачем надасть зловмиснику простір для подальших дій, таких як збір або зміну інформації.

Дорожнє яблуко. Цей метод є різновидом троянського коня і полягає у використанні фізичних носіїв (флешки і т.п.). Зазвичай, зловмисник підкидає такий носій у загальнодоступних місцях на території підприємства/компанії (їдальнях, кафе, паркувальних місцях, туалетах тощо). Для того, щоб співробітник зацікавився предметом, зловмисник може нанести на носій логотип компанії або якийсь підпис, наприклад, «Звіт з податкової». Після того, як жертва під'єднає заражений носій до свого або корпоративного пристрою, запускається шкідливе ПО.

Зворотна соціальна інженерія. В цьому випадку зловмисник створює такі умови, за яких жертва буде сама змушена звернутися до нього. Наприклад, зловмисник може надіслати лист із контактами «служби підтримки» і через деякий час створити оборотні негаразди на пристрої особи. В більшості

випадків користувач звернеться за контактами, представленими у такому листі (зателефонує за номером, опише проблему у зворотньому листі тощо). В процесі «виправлення» проблеми зловмисник може отримати необхідні йому дані.

В результаті аналізу описаних методів, можна виділити деякі психологічні концепції, які використовують зловмисники в процесі створення зв'язку із жертвою: маніпуляція, впливовість, взаєморозуміння, авторитет, емпатія тощо.

Перелік посилань:

1. Джо Грей. Соціальна інженерія та етичний хакінг на практиці / пер. з англ. В.С. Яценкова. – К.: Print2print, 2023. – 226 с.
2. Verizon Infographics 2023. URL: https://www.verizon.com/business/resources/ja/infographics/2023-dbir-infographic.pdf (дата звернення: 19.10.2024).