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

ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ЦИФРОВА ТРАНСФОРМАЦІЯ КІБЕРБЕЗПЕКИ»

Тези доповідей

26 квітня 2024

м. Київ

Зміст

Vladyslav Bakalo
National Aviation University, Kyiv

INFORMATION AND CYBER THREATS OF TODAY

Achievements in the field of high technologies and informatization generate an increase in crime with their use. Interpol experts claim that crime in the World Wide Web has recently been in the lead. Today, cybersecurity and information protection are gaining great importance not only at the state level, which is undoubtedly very important for the security of the country but also in the life of the average Ukrainian.

Modern wars, in particular the one ongoing in Ukraine, reveal not only military and military crimes but also crimes in cyberspace: attacks, hacks, and terrorism. State institutions, private structures, and citizens are chosen for the damage. Their consequences can be considered no less harmful than human and economic losses. DDoS attacks and DoS attacks are an obstacle to obtaining reliable information and its distribution.

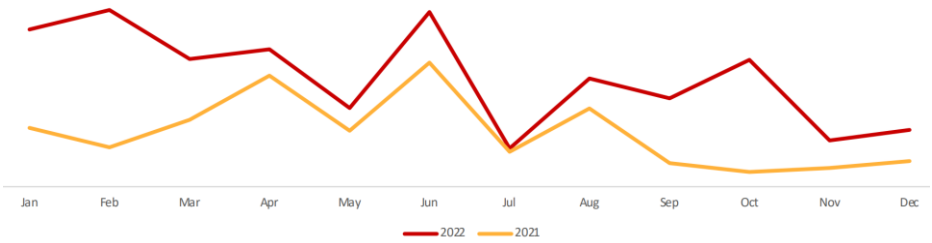


Figure 1 – Monitoring of DDoS attacks

In today's realities, such an important resource as information becomes interesting for a cyber-aggressor and requires a particularly thorough means of protection.

The number of critical information security events originating from russian IP addresses increased by 26% (compared to the same period in 2021).

In Ukraine, the possibilities of the Internet are used everywhere: the unified portal of public services Diya, electronic document management, banking, work of transport, critical infrastructure enterprises, logistics services, informatization of various spheres of life (mobile devices, social networks, Internet banking), which is why cyberspace requires enhanced security.

The subsystem of the operational center for responding to cyber incidents detected about 14 million and processed 78 thousand suspicious information security events, classifying them by the level of danger as follows: high (4%), medium (11%), and low (85%).[1]

Break-ins, blocks, torrents, information fraud, criminal actions related to the purchase of domain names for further resale, spam distribution, and hacker attacks

have a negative impact on the subjects of information relations.

Fraudulent actions on the Internet and networks of mobile operators cause psychological pressure and economic damage to their users.

The State Service of Special Communications and Information Protection of Ukraine has developed a List of categories of cyber incidents using the recommendations of the European Agency for Cyber Security (ENISA Reference Incident Classification Taxonomy, January 2018), which corresponds to the joint document of ENISA and the European Center for Combating Cybercrime of Europol (Common Taxonomy for Law Enforcement and The National Network of CSIRTs):

- Abusive content (Spam, Harmful speech);
- Malicious Code (Virus, Worm, Trojan, Spyware, Dialer, Rootkit, Malware, Botnet drone, Ransomware, Malware configuration);
- Information Gathering (Scanning, Sniffing, Social engineering);
- Intrusion Attempts (Exploiting of known vulnerabilities, Login attempts, New attack signature (exploit));
- Intrusion (Privileged/Unprivileged account compromise, Application compromise, Bot, Defacement, Backdoor);
- Availability (DoS, DDoS, Sabotage, Outage, no malice);
- Information Content Security (Unauthorized access to information, Unauthorized modification of information, Dropzone);
- Fraud (Unauthorized use of resources, Copyright, Masquerade, Phishing).

The list is regularly revised taking into account the practice of its application, the emergence of new categories and types of cyber incidents, as well as information received from cybersecurity providing entities.[2]

One type of fraud is social engineering, which takes advantage of users' credulity and inattention to obtain personal data from currency transfer or exchange services, online stores, and online auctions. At the same time, all kinds of methods of coercion to disclose personal confidential data are used.

The number of information security events in the category "03 Collection of information by an attacker" increased by 2.2 times (compared to the same time period in 2021).

Chatbots imitating an interlocutor or a virtual assistant are gaining popularity. Based on pre-written scripts, thanks to which the bot can immediately give the desired answer, it can spread false information that causes panic and disorientation.

Spam, as a mass mailing of various types of information, is also a threat because it can contain not only computer viruses but messages that spread fakes and negativity.

Various types of phishing are widely used: deceptive, voice, mobile, SMS

phishing, and spoofing. Therefore, Ukrainians most often give money to thieves of their own free will, believing that real sellers, buyers, or even police or bank employees are at the other end of the Internet.

Practice shows that most Ukrainians are infantile Internet users. Therefore, it is urgently necessary to strengthen security measures to combat cyber fraud, in particular, to improve the qualifications of ordinary users of the Internet and financial services, because they become victims of fraud. Attention should be focused on four main stages of countering phishing attacks: making it difficult for attackers to access users; helping users to identify and quickly report suspected phishing messages and calls; self-defense or protection of the organization from the influence of undetected phishing attacks; rapid response to incidents and actions.

Ransomware programs that can destroy documents and other user files, blocking access to the system and important documents, and photos, are actively spreading on the Internet. The insufficient information hygiene of ordinary citizens and the desire to receive news from the war zone encourage the transition to harmful sites.

In the context of cyber protection, the most vulnerable element is a person, since protection at the elementary level depends on it: from the reliability of account passwords to providing other people with personal data appearing in social networks or questionnaires.

Different types of hacker attacks are another type of real threat. For example, the deface changes a website page to another (usually it is the main page, and access to the rest of the site is blocked), and the existing site content is deleted or replaced with the "necessary" one.

Given the fact that cyber threats cannot be confined to one area, this requires all interested parties to have a comprehensive awareness of the risk factors, the skills and abilities to eliminate them, and appropriate measures to prevent cyber attacks before they begin. Ukraine actively engages leading organizations in raising the level of awareness of commercial enterprises and non-profit organizations regarding cyber security at all levels.[3]

Cyber security measures allow users (government, commercial structures, ordinary people) to work productively and communicate freely online, even on different continents. The correct approach to this issue opens access to advanced technologies, stimulates scientific thought, and ultimately affects the quality of life itself.

Thus, strengthening the methods of combating cyber fraud will minimize risks and threats to user information on the Internet and increase the effectiveness of the model of protection against unauthorized access. It is necessary to review some rules for using online services and the behavior of users on the network, which is

extremely appropriate and relevant today.

The security of national information sovereignty, and the neutralization of cyber threats today is an important component of the security of Ukraine in the conditions of martial law.[4] Not only various security structures but also ordinary citizens should be widely involved in this. The war in the country obliges everyone to be a responsible, thoughtful, principled fighter against various types of disinformation, to remember and follow simple rules of information security, bringing victory closer!

References:

1. Report on the work of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks [Electronic resource] – Access mode: https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7.pdf

2. List of categories of cyber incidents [Electronic resource] – Access mode: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv.

3. O. Trofymenko, Yu. Prokop, N. Loginova, O. Zadereyko. Cybersecurity of Ukraine: analysis of the current state. Protection of information. 2019. (vol. 21, № 3).

4. Dovgan O.D., Doronin I.M. Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber protection: monograph. Kyiv: «ArtEk» Publishing House, 2017.

Баранов Андрій Андрійович
студент групи БСД-42,
Державний університет інформаційно-телекомунікаційних технологій,,м.Київ

РОЛЬ SERVICE MESH В ІНФОРМАЦІЙНІЙ ТА КІБЕРНЕТИЧНІЙ БЕЗПЕЦІ НА ПРИКЛАДІ ISTIO SERVICE MESH

Сучасні програми, як правило, створені як розподілені колекції мікросервісів, причому кожна колекція мікросервісів виконує певну окрему бізнес-функцію. Service Mesh — це виділений рівень інфраструктури, який можна додати до своїх програм. Це дозволяє вам прозоро додавати такі можливості, як спостережливість, керування трафіком і безпека, не додаючи їх до власного коду.

Термін «Service Mesh» описує як тип програмного забезпечення, яке ви використовуєте для реалізації цього шаблону, так і безпеку або мережевий домен, який створюється під час використання цього програмного забезпечення[1].

Оскільки розгортання розподілених служб, наприклад, у системі на основі Kubernetes, зростає в розмірах і ускладнюється, це стає важче зрозуміти та керувати ним. Його вимоги можуть включати виявлення, балансування навантаження, відновлення після збоїв, показники та моніторинг. Service Mesh також часто задовольняє складніші операційні вимоги, такі як A/B-тестування, розгортання Canary, обмеження швидкості, контроль доступу, шифрування та

наскрізна автентифікація[1].

Комунікація між послугами — це те, що робить можливим розподілену програму. Маршрутизація цього зв’язку як всередині, так і між кластерами додатків стає дедалі складнішою, оскільки кількість служб зростає. Istio допомагає зменшити цю складність, одночасно зменшуючи навантаження на команди розробників[1].

Istio — це сервісна мережа з відкритим кодом, яка прозоро накладається на існуючі розподілені програми. Потужні функції Istio забезпечують єдиний і ефективніший спосіб захисту, підключення та моніторингу служб. Istio — це шлях до балансування навантаження, міжсервісної автентифікації та моніторингу — з мінімальними або без змін коду служби. Його потужна площина управління забезпечує життєво важливі функції, зокрема[2]:

Безпечний міжсервісний зв’язок у кластері за допомогою шифрування TLS, надійної автентифікації та авторизації на основі ідентифікації

Автоматичне балансування навантаження для трафіку HTTP, gRPC, WebSocket і TCP

Детальний контроль поведінки трафіку з розширеними правилами маршрутизації, повторними спробами, перемиканням після відмови та впровадженням помилок

Підключається рівень політики та API конфігурації, що підтримує контроль доступу, обмеження швидкості та квоти

Автоматичні показники, журнали та трасування для всього трафіку в межах кластера, включаючи вхідний і вихідний трафік кластера

Istio розроблено для розширюваності та може виконувати різноманітні потреби розгортання. Площина керування Istio працює на Kubernetes, і ви можете додавати програми, розгорнуті в цьому кластері, до своєї сітки, розширювати сітку на інші кластери або навіть підключати віртуальні машини чи інші кінцеві точки, що працюють за межами Kubernetes[1].

Можливості безпеки Istio Service Mesh

Мікросервіси потребують особливої безпеки, включаючи захист від атак типу "людина посередині", гнучкі засоби контролю доступу, інструменти аудиту та взаємний TLS. Istio містить комплексне рішення безпеки, яке дає операторам можливість вирішити всі ці проблеми. Він забезпечує надійну ідентифікацію, ефективну політику, прозоре шифрування TLS, а також інструменти автентифікації, авторизації та аудиту (AAA) для захисту ваших служб і даних[2].

Модель безпеки Istio заснована на безпеці за замовчуванням, яка має на меті забезпечити поглиблений захист, щоб дозволити вам розгортати безпечні

програми навіть у ненадійних мережах.

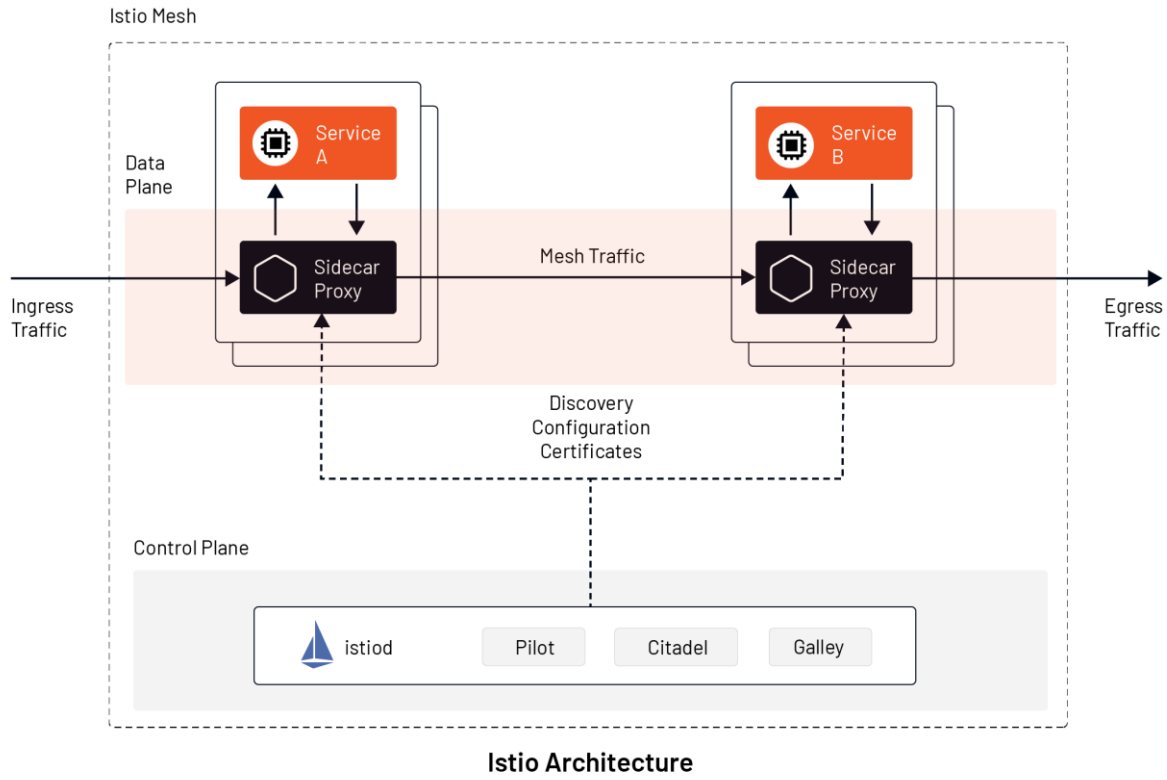


Рис.1 Архітектура Istio Service Mesh

Перелік посилань:

1. About Service Mesh [Електронний ресурс] – режим доступу: https://istio.io/latest/about/service-mesh/
2. What Is a Service Mesh, and Why Do You Need? [Електронний ресурс] – режим доступу: https://tetrate.io/what-is-istio-service-mesh/

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

ТЕХНОЛОГІЯ СКАНУВАННЯ ВЕБЗАСТОСУНКІВ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ЗА ДОПОМОГОЮ SAST-РІШЕННЯ SNYK CODE

Виявлення вразливостей на ранніх стадіях розробки вебзастосунків є ключовим для організації їх безпеки та надійності. Статичний аналіз безпеки застосунків (SAST) відіграє важливу роль у цьому процесі, дозволяючи розробникам ідентифікувати потенційні вразливості без необхідності виконання коду. Використання Snyk Code, як інструменту SAST, дозволяє ефективно аналізувати код на наявність безпекових проблем, забезпечуючи інтеграцію із середовищами розробки та автоматизацію процесу перевірки. Це сприяє оперативному виявленню та усуненню вразливостей, знижуючи потенційні ризики безпеки та витрати на виправлення помилок на пізніших етапах розробки. Застосування Snyk Code сприяє побудові більш безпечних вебзастосунків,

підвищуючи довіру користувачів та відповідність сучасним вимогам безпеки.

Snyk забезпечує інструментарій для статичного аналізу безпеки застосунків (SAST), аналізу компонентів програмного забезпечення (SCA) та аналізу інфраструктури як коду, що дозволяє аналізувати код та налаштування хмарної інфраструктури з метою ідентифікації та виправлення вразливостей. Це досягається через різні методи сканування, включаючи Snyk Open Source для перевірки відкритого програмного коду, Snyk Code для виявлення вразливостей у коді, Snyk Container для аналізу контейнерних образів, та Snyk Infrastructure as Code для оцінки конфігурацій хмарної інфраструктури. Snyk дозволяє виконувати як ручне, так і автоматичне сканування через Snyk CLI, веб-інтерфейс Snyk, Snyk API та перевірки в Pull Request [1]. Деталі щодо типів сканування в залежності від типу розгортання можна знайти в таблиці 1.

Таблиця 1.

Особливості	Snyk Web UI	Snyk CLI	Snyk API	PR Checks
Автоматичне сканування	+	+	+	+
Ручне сканування	+	+	+	-
Локальне сканування	-	+	-	-
Включення в конвеєри CI/CD	-	+	-	-
Отримання результатів, що точно відображають вразливості та конфігурації проєкту	+	+	+	+

Найцікавішим є саме сканування за допомогою інтерфейсу командного рядка за умови інтеграції у середовище розробки, адже саме такий тип пропонує найширший функціонал. Тому розглянемо його детальніше.

Проведемо сканування деякого простого вебзастосунку [2]. Для активації сканування за допомогою SAST-рішення Snyk Code, необхідно виконати команду 1:

$$snyk\ code\ test \quad (1)$$

У результаті сканування буде знайдено ряд вразливостей (рис. 1). Серед них є доволі поширені та небезпечні, як-от ін’єкція коду, підробка міжсайтових запитів, міжсайтовий скриптинг та ін.

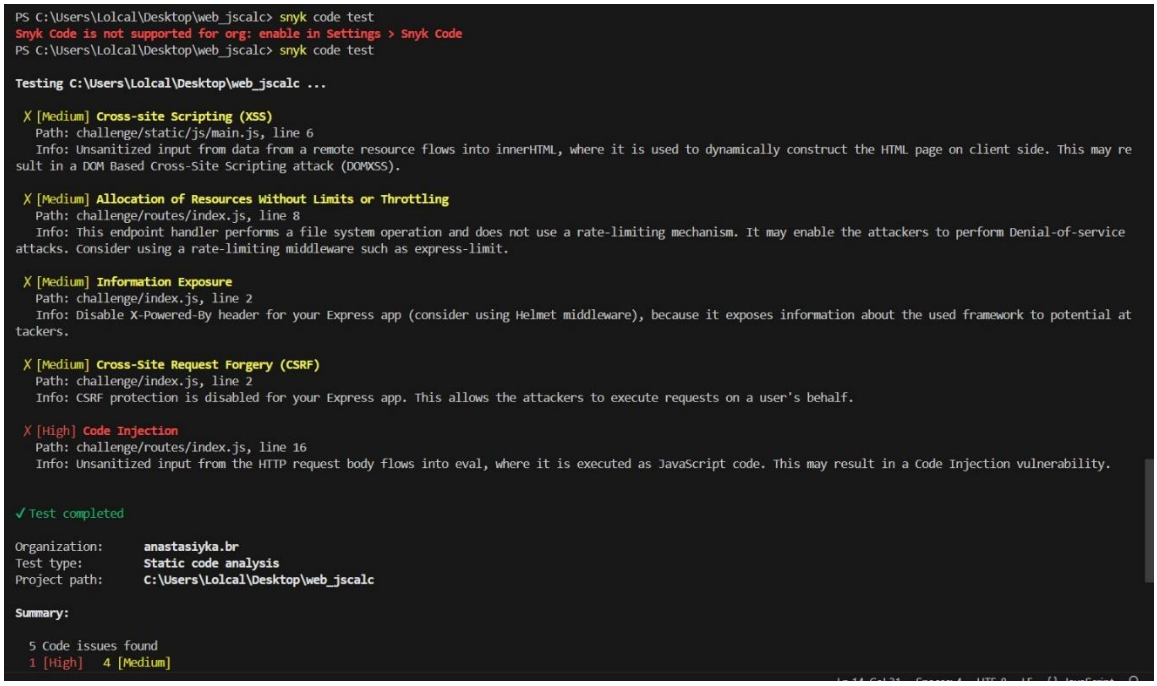


Рис. 1. Знайдені у вебзастосунку вразливості

Розглянемо детальніше вразливість критичного рівня - ін’єкцію коду. Атака на введення коду відбувається, коли зловмисник використовує існуючу вразливість обробки вхідних даних, передаючи спеціальні символи та код безпосередньо до вебзастосунку або сайту. Потім код виконується, потенційно надаючи користувацькій системі доступ до експорту конфіденційних даних, інсталяції шкідливого програмного забезпечення або навіть до інших систем у довіреному внутрішньому мережевому середовищі. Хоча атаки на впровадження коду можуть відбуватися кількома способами, їхньою спільною рисою є надання користувачеві можливості надсилати виконуваний код до програми [3].

Значною перевагою використання рішення Snyk Code є надання рекомендацій щодо пом’якшення впливу вразливості, її попередження і/або виправлення. Тож рекомендаціями щодо попередження є:

• Ніколи не довіряти користувацьким даним - це основоположний принцип, що передбачає потенційну можливість передачі шкідливих значень через будь-яке введення.

• Застосовування принципу найменших привілеїв рекомендується, наприклад, обмеженням доступу користувачів лише до читання, де це можливе, для мінімізації ризиків.

• Важливо уникати передачі необробленого користувацького вводу безпосередньо функціям, віддаючи перевагу параметризованим запитам для вилучення даних. Очищення рядків вводу від спеціальних символів,

використання білих списків для відомих правильних значень та перевірка даних на відповідність очікуваним типам є ключовими заходами безпеки.

•Екранування команд оболонки за допомогою спеціалізованих функцій та усвідомлення можливості ін'єкцій коду через різноманітні канали важливе для захисту систем.

• Забезпечення систем актуальними патчами для усунення відомих вразливостей та навчання всіх членів команди безпечним процедурам обробки даних є важливими кроками для запобігання атакам.

Отже, виявлення вразливостей на ранній стадії розробки вебзастосунків є критично важливим для забезпечення їхньої безпеки та надійності. Використання інструментів статичного аналізу безпеки застосунків, зокрема Snyk Code, дозволяє розробникам ідентифікувати потенційні вразливості до запуску коду, інтегруючи безпеку безпосередньо в процес розробки. Це не тільки знижує потенційні ризики безпеки, але й економить витрати на виправлення помилок у майбутньому, сприяючи розробці більш безпечних вебзастосунків, що відповідають сучасним вимогам безпеки. Snyk надає широкий спектр інструментів для аналізу безпеки, що дозволяє різноманітні способи сканування, включаючи ручне та автоматичне, за допомогою інтерфейсів командного рядка, веб-інтерфейсу, API та перевірок у Pull Request. Особливу увагу заслуговує сканування за допомогою командного рядка, що інтегроване в середовище розробки, надаючи розробникам потужний інструмент для виявлення та вирішення вразливостей ефективно та вчасно.

Перелік посилань:

1. Scan with Snyk. URL: https://docs.snyk.io/scan-with-snyk (дата звернення: 06.04.2024).
2. Vulnerable application - jscalc. URL: https://app.hackthebox.com/ (дата звернення: 06.04.2024).
3. What is code injection? | Tutorial & examples | Snyk Learn. *Snyk Learn*. URL: https://learn.snyk.io/lesson/malicious-code-injection/?loc=ide (дата звернення: 06.04.2024).

Василенко Іван Дмитрович
студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

Безпека хмарних технологій

Безпека хмарних технологій - це сукупність процедур і технологій, призначених для протидії зовнішнім і внутрішнім загрозам безпеці бізнесу. Організації потребують безпеки хмарних технологій, оскільки вони рухаються до своєї стратегії цифрової трансформації та впроваджують хмарні інструменти та сервіси як частину своєї інфраструктури.

Чому безпека в хмарі важлива?

На сучасних підприємствах спостерігається все більший перехід до хмарних середовищ і моделей обчислень IaaS, Paas або SaaS. Динамічний характер управління інфраструктурою, особливо при масштабуванні додатків і сервісів, може спричинити низку проблем для підприємств, якщо вони не забезпечені належними ресурсами для своїх відділів. Ці моделі "як послуга" дають організаціям можливість розвантажити багато трудомістких завдань, пов'язаних з IT.

Оскільки компанії продовжують мігрувати до хмарних технологій, розуміння вимог безпеки для збереження даних стає критично важливим. Хоча сторонні провайдери хмарних обчислень можуть взяти на себе управління цією інфраструктурою, відповідальність за безпеку та підзвітність даних не обов'язково зміщується разом з нею.

За замовчуванням, більшість хмарних провайдерів дотримуються найкращих практик безпеки та вживають активних заходів для захисту цілісності своїх серверів. Однак організаціям необхідно враховувати власні міркування при захисті даних, додатків і робочих навантажень, що працюють у хмарі.

Загрози безпеці стають все більш досконалими, оскільки цифровий ландшафт продовжує розвиватися. Ці загрози безпосередньо націлені на провайдерів хмарних обчислень через загальну недостатню прозорість доступу до даних і їх переміщення в організації. Якщо не вживати активних заходів для покращення безпеки хмарних технологій, організації можуть зіткнутися зі значними ризиками в управлінні та дотриманні нормативних вимог при роботі з інформацією клієнтів, незалежно від того, де вона зберігається.

Безпека хмарних технологій повинна бути важливою темою для обговорення незалежно від розміру вашого підприємства. Хмарна інфраструктура підтримує майже всі аспекти сучасних обчислень у всіх галузях і на різних вертикалях.

Однак успішне впровадження хмарних технологій залежить від впровадження адекватних контрзаходів для захисту від сучасних кібератак. Незалежно від того, чи працює ваша організація в публічному, приватному або гібридному хмарному середовищі, рішення та найкращі практики хмарної безпеки є необхідними для підтримки безперервності бізнесу.

Які існують проблеми з безпекою в хмарі?

Відсутність видимості.

Легко втратити контроль над тим, як і хто отримує доступ до ваших даних, оскільки доступ до багатьох хмарних сервісів здійснюється за межами корпоративних мереж і через третіх осіб.

Багатокористувацьке середовище.

Публічні хмарні середовища містять кілька клієнтських інфраструктур під однією парасолькою. Як наслідок, існує ймовірність того, що ваші хмарні сервіси можуть бути скомпрометовані зловмисниками як супутній збиток при націлюванні на інші бізнеси.

Управління доступом і тіньові IT.

Хоча підприємства можуть успішно керувати та обмежувати точки доступу в локальних системах, адміністрування таких самих рівнів обмежень може бути складним завданням у хмарних середовищах. Це може бути небезпечно для організацій, які не впроваджують політику використання власних пристроїв (BYOD) і дозволяють нефільтрований доступ до хмарних сервісів з будь-якого пристрою або геолокації.

Відповідність нормативним вимогам.

Управління нормативно-правовою відповідністю часто є джерелом плутанини для підприємств, які використовують загальнодоступні або гібридні хмарні розгортання. Загальна відповідальність за конфіденційність і безпеку даних все ще лежить на підприємстві, а надмірна залежність від сторонніх рішень для управління цим компонентом може призвести до дорогих проблем з дотриманням нормативних вимог.

Неправильні конфігурації.

Значна частина порушених записів може бути пов'язана з неправильною конфігурацією активів, що робить ненавмисний інсайдер ключовою проблемою для середовищ хмарних обчислень. Неправильні конфігурації можуть включати залишення адміністративних паролів за замовчуванням або нестворення належних налаштувань конфіденційності.

Які існують типи хмарних рішень для безпеки?

Управління ідентифікацією та доступом (IAM).

Інструменти та сервіси управління 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 поєднання сповіщень про усунення несправностей, шифрування даних та інших превентивних заходів для захисту всіх збережених даних, як у стані спокою, так і 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 свої протоколи мережевої безпеки, що дозволяє 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 хмарної безпеки і надають організаціям інструменти, сервіси та протоколи, необхідні для прискорення відновлення втрачених даних і відновлення нормальної роботи бізнесу.

Висновок

Безпека в хмарному середовищі є критично важливою для сучасних підприємств, оскільки вони переходять до хмарних моделей обчислень. Перехід до хмари дозволяє підприємствам розгортати додатки та сервіси без значних витрат на обладнання та управління ним. Однак цей перехід також створює нові виклики з точки зору безпеки даних.

Успішне впровадження хмарних технологій залежить від того, наскільки ефективно підприємство впроваджує адекватні контрзаходи для захисту від сучасних кібератак та збереження безперервності бізнесу. Тому безпека в хмарному середовищі повинна бути важливою темою для обговорення незалежно від розміру підприємства.

Перелік посилань

1. What is cloud security? URL: https://www.ibm.com/topics/cloud-security (дата звернення 16.04.2024)
2. What is Cloud Security? Understand The 6 Pillars URL: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security (дата звернення 16.04.2024)

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

ВПЛИВ ЦИФРОВИХ ТЕХНОЛОГІЙ НА СТІЙКІСТЬ ЛАНЦЮГІВ ПОСТАВОК

У роботі досліджено важливість забезпечення стійкості ланцюгів поставок на сучасному етапі розвитку, а також виокремлено її основні критерії (прозорість, динамічність, гнучкість, міцність, надійність, керованість, вирівнювання). Проведено дослідження впливу різних цифрових технологій, таких як Blockchain technology, Cloud Services, Big Data, IoT, Machine Learning, Mobile App, Augmented and Virtual reality, Digital Twins, на стійкість ланцюгів поставок. За результатами дослідження виявлено, на які саме критерії стійкості ті чи інші технології впливають.

Згідно з ринковими прогнозами, 76 % населення світу має доступ до Інтернету; понад 50 % активно використовують соціальні мережі; 43 % підприємств використовують розширену аналітику великих даних; а також 90 % інтернет-користувачів роблять покупки онлайн. Очікується, що до 2025 р. в усьому світі буде близько 30,9 мільярда пристроїв, підключених до Інтернету речей. У результаті трансформуються багато галузей у напрямку надання більш якісних продуктів і послуг.

Традиційний ланцюжок поставок визначається як лінійна модель, яка працює добре в передбачуваних і стабільних умовах. Однак мінливе, невизначене, складне та неоднозначне зовнішнє середовище, в якому ми живемо сьогодні, і яке поступово переходить у крихкий, тривожний, нелінійний та незбагненний стан, ставить перед ланцюгами поставок нові умови для ефективного функціонування. Високоефективними сьогодні можна вважати тільки ті ланцюги постачань, які можуть швидко підлаштовуватися під умови, що швидко змінюються, здатні зберігати безвідмовне функціонування незважаючи на агресивність впливу зовнішнього середовища, забезпечувати прозорість і доступність процесів для всіх учасників ланцюга, адекватно реагувати на керуючий вплив і дотримуватися балансу інтересів усіх ланок ланцюга, тобто стійкі ланцюги постачань.

Зауважимо, що саме стійкість на сьогодні, на думку більшості

експертів, є найважливішою характеристикою ланцюгів поставок.

Поняттю стійкості приділяли доволі багато уваги в загальній теорії систем, як одній з інтегральних властивостей, яку розглядали як "здатність системи реагувати на зміни довкілля і, як і раніше, зберігати приблизно таку саму поведінку протягом певного періоду часу". Значно пізніше Блекхерст Дж. визначає стійкість як "здатність системи повернутися у вихідний стан або перейти до нового, більш високоефективного і бажаного стану" [1]. Широкого поширення поняття "стійкість ланцюга поставок" набуло в останні кілька десятиліть завдяки підвищенню невизначеності, нестабільності, складності та неоднозначності на світових ринках. Так, П. Друкер трактує дане поняття як "здатність відновлюватися і пристосовуватися до змін зовнішнього і внутрішнього середовища, що призводять до генерування додаткової цінності для всіх зацікавлених осіб - кінцевих споживачів, акціонерів, держави і суспільства в цілому" [2]. Ponis S.T. і Koronis E. уявляють стійкість як "здатність заздалегідь планувати та проєктувати мережу ланцюга постачань для прогнозування несподіваних руйнівних (негативних) подій, реагувати адаптивно на збої за умови збереження контролю над структурою і функціями та переходити до міцнішого становища, якщо це можливо, більш сприятливого, ніж було до події, яка сталася, і в такий спосіб, здобуваючи конкурентну перевагу". З позиції Wieland A. і Wallenburg C. Стійкість - це "Здатність ланцюга поставок впоратися зі змінами та залишити нестабільне становище, що передбачає реактивний або проактивний характер взаємодії з навколишнім середовищем" [3].

Як основні критерії стійкості ланцюга поставок можна виділити такі:

- Прозорість (visibility) - можливість у реальному часі відстежувати рух матеріального потоку в ланцюзі поставок.
- Динамічність (agility) - можливість швидкого відновлення ланцюга поставок після збурювального впливу (компенсація нецілеспрямованих впливів).
- Гнучкість (flexibility) - здатність швидко підлаштовуватися під мінливі умови внутрішнього і зовнішнього середовища.
- Міцність / Робастність (robustness) - здатність чинити опір впливу внутрішніх і зовнішніх збурень.
- Надійність (reliability) - здатність зберігати значення характеристик своєї діяльності у встановлених межах (можливість безвідмовного нормального функціонування ланцюга поставок).

- Керованість (controllability) - здатність адекватно (очікувано) реагувати на керуючий вплив.
- Вирівнювання / Розподіл (alignment) - здатність ланцюга вирівнювати (балансувати) інтереси всіх своїх ланок (компаній).

Забезпечення стійкості ланцюга поставок завдяки дотриманню наведених критеріїв дасть змогу підвищити точність прогнозів і скоротити рівень запасів у ланцюзі, передбачити можливі розриви в постачанні, забезпечити високий рівень сервісу на всіх стадіях руху потоку і дотримуватися прийнятного рівня витрат як у виробничих ланках, так і у ланках, що забезпечують продажі та логістику.

Варто зазначити, що ланцюжки поставок не можуть бути перебудовані відразу, оскільки ринок визначається сильною конкуренцією, ціновими обмеженнями, короткостроковим ринковим попитом і динамічними моделями попиту. Щоб ефективно справлятися зі зростаючими перешкодами, ланцюжки поставок мають стати інтелектуальними. Так, певної популярності починає набувати концепція SCM (Supply Chain Management) 4.0, яка використовує проривні цифрові технології, поряд із високим рівнем застосування роботів [4]. При цьому зазначимо, що немає усталеного переліку цифрових технологій, обов'язкових до застосування в ланцюгах поставок згідно з новою концепцією.

Отже, дослідження показало, що найбільший вплив на стійкість ланцюга поставок мають такі цифрові технології, як Big Data (Великі дані) та IoT (Інтернет речей). Саме ці технології дають змогу організовувати прозорість ланцюгів завдяки забезпеченню трекінгу та трейсингу вантажів; підвищують надійність ланцюгів, беручи участь в оптимізації маршрутів, удосконаленні процесів вантажопереробления на складі та покращенні завантаження потужностей, забезпеченні безпеки руху інформаційних потоків; підсилюють гнучкість ланцюгів, допомагаючи в прискоренні руху товарів і оптимізації запасів у них і в прогнозуванні змін у ланцюзі.

Загалом, можна зробити висновок про наявність залежності між стійкістю ланцюгів поставок і присутністю в них цифрових технологій. При цьому варто наголосити на важливості технологічної, технічної, організаційної та психологічної готовності ланцюгів поставок до впровадження в їхню діяльність цифрових технологій.

Перелік посилань

1. Blackhurst J., Wu T., O'grady P. (2004) Network-based approach to mod-elling uncertainty in a supply chain // Int. J. Prod. Res. 2004, V. 42. – P. 1639 – 1658.

2. Ponis, S.T. & Koronis, E. (2012). Supply chain resilience: definition ofconcept and its formative elements. The journal of applied business research,28 (5), 921-930.
3. Wieland, A. & Wallenburg, C.M. (2012). Dealing with supply chain risks: linking risk management practices and strategies to performance. Interna- tional Journal of Physical Distribution& Logistics Management, 42 (10), 887-905.
4. Ilhaam Omar (2022) Digital supply chain 4.0: a comparative advantage for enterprises, ISE Magazine, October 2022, P. 32-37.

Гайдур Ксенія Володимирівна
Студентка групи БСДМ-51, ННІТ, ДУІКТ, Київ, Україна
Гайдур Галина Іванівна
Доктор технічних наук, професор, ННІЗІ, ДУІКТ, Київ, Україна

Захист від фішингових атак за допомогою штучного інтелекту

У сучасному цифровому світі будь яка нова технологія може бути використана для розвитку кіберзлочинності, але й завдяки тій самій технології можна покращити методи захисту від шахрайства в онлайн просторі. Саме таким інструментом став розвиток технології штучного інтелекту, завдяки своїй здатності аналізувати великі обсяги даних, розпізнавати складні патерни та машинному навчанню, яке постійно адаптує до нових задач.

Фішинг це одна з найпопулярніших форм атак, за весь час існування Інтернету він набув багато форм і видів. Завдяки ньому зловмисники підробляють легітимні веб-сайти та електронні повідомлення, викликають довіру у користувачів задля отримання їх конфіденційних даних, як от паролі, номери кредитних карток чи особиста інформація.

Саме поєднання фішингу та із технологією штучного інтелекту є золотою жилою для фішингу [1], оскільки кіберзлочинці, які накопичують зламані дані зі зламаних веб-сайтів, можуть використовувати технологію штучного інтелекту, щоб зчитувати ці дані та організовувати їх у цілеспрямовану фішингову атаку.

Фішинг — це складна атака соціальної інженерії, основна мета якої спонукати одержувача до негайних дій, головним чином завантажити вкладений файл або ж натиснути посилання. Цей один клік може призвести до зараження шкідливим програмним забезпеченням, що може призвести до викрадення конфіденційних даних. Для виявлення та запобігання фішингу вже існують певні інструменти та методи, а одним із найкращих є штучний інтелект (ШІ)

Як вже було сказано раніше, ШІ здатний аналізувати великі обсяги даних, розпізнавати складні патерни і постійно покращується за допомогою машинного навчання. Тож як саме ШІ виявляє фішинг [2]?

1. Пошук аномалій і попереджувальних сигналів

Однією з основних ознак фішингової атаки є помітне відчуття терміновості в повідомленні, тож завдяки розпізнаванню тексту та його аналізу ШІ може точніше розпізнати чи є це повідомлення небезпечним, а головне подати сигнал про фішинг на основі поведінки електронної пошти (наприклад, підроблені відправники) і мети повідомлення (наприклад, термінові теми).

2. Аналіз контексту повідомлення

Перевірка повідомлення на основі контексту з врахуванням наявності чи відсутності попередньої розмови.

3. Розуміння, як користувачі спілкуються

Злочинці можуть знати типову поведінку жертви чи, наприклад, їх знайомих, їхні текстові шаблони, а також те, який контекст повідомлень вони використовують. Тобто шахраї імітують когось за для отримання бажаного їм результату, що виявити традиційними методами майже неможливо.

Проте людський фактор залишається [3] і відіграє вирішальну останню лінію захисту, адже саме людина обирає звернути увагу на повідомлення про небезпеку від ШІ чи все таки перейти за «безпечним посиланням»

Тож, застосування штучного інтелекту у сфері кібербезпеки, зокрема в боротьбі з фішингом, демонструє значний потенціал у покращенні захисту від цієї, складної для виявлення традиційними методами, форми кібератак. Саме ШІ забезпечує швидке виявлення підроблених веб-сайтів та фішингових повідомлень, виявлення аномальної поведінки користувачів і ефективне реагування на нові фішингові загрози, що забезпечує більшу безпеку онлайн-середовища й сприяє підвищенню довіри користувачів до цифрових технологій.

Ганусяк Степан Ігорович

студент групи АІКБ, ННІЗІ ДУІКТ, Київ, Україна

Моніторинг систем кінцевих точок в SOC

Моніторинг кінцевих точок має вирішальне значення для забезпечення безпеки корпоративної мережі. Цей тип моніторингу передбачає аналіз мережевого трафіку та кінцевих точок на потенційні загрози та вторгнення. Завдяки моніторингу в реальному часі та аналітиці безпеки моніторинг кінцевих точок може запобігти атакам і зменшити шкоду.

Із зростанням кіберзагроз і роботи віддалено компанії повинні мати

комплексну стратегію, щоб забезпечити безпеку, контроль і підтримку своїх кінцевих точок. Згідно з даними звіту Verizon Data Breach Investigations Report 43% кібератак націлені на компанії малого бізнесу і 66% організацій відчувають зростання загроз для кінцевих точок. Часто вони не мають жодних засобів захисту, а зловмисники можуть використовувати їх, щоб проникати в системи великих компаній.

Деякі з головних аспектів, які слід враховувати для ефективного рішення моніторингу кінцевих точок, включають:

Єдиний моніторинг

Визначальною якістю ефективної стратегії є те, що вона враховує кожну кінцеву точку, якою користується в організації.

Управління ідентифікацією

Вирішальним для будь-якої стратегії кібербезпеки є забезпечення того, щоб доступ до важливої інформації мали лише користувачі, які мають дозвіл на доступ до неї. Це вимагає захисту конфіденційних даних за допомогою систем входу.

Сучасний ландшафт загроз означає, що керування кінцевими точками потребує надійного керування ідентифікацією та доступом. Це включає такі елементи керування, як:

- Впровадження політики доступу з найменшими привілеями, які обмежують на основі потреб бізнесу.
- Надійні вимоги до пароля, наприклад складність і довжина.
- Протоколи багатофакторної автентифікації (MFA).
- Регулярне та часте оновлення облікових даних.
- Суворе регулювання та моніторинг облікових записів користувачів.

Керування виправленнями та моніторинг ризиків третіх сторін

Ефективна кібербезпека передбачає не лише впровадження заходів

безпеки, але й регулярну їх оцінку та перевірку, щоб переконатися, що вони працюють так, як очікується.

Надійний патч, орієнтований на кінцеву точку, вимагає:

- Реєстрація, керування та підтримка запису всіх компонентів в IT-середовищі, включаючи програмне забезпечення, облікові записи користувачів і пристрої.
- Моніторинг нерегулярного використання пристроїв.
- Сертифікація відповідності для кожного пристрою.

Моніторинг і зниження ризиків

Надійне керування вразливостями вимагає детального аналізу та моніторингу програмного та апаратного забезпечення для виявлення та пом’якшення ризиків, перш ніж вони стануть атаками. Це означає, що потрібно індексувати доступні дані, як-от CVE, скорочення від Common Vulnerabilities and Exposures..

Однак потрібно користуватись не лише публічними ресурсами. Соціальна інженерія, як-от фішинг, є найпоширенішим векторам кібератак. Першою лінією захисту від таких атак є брандмауер. Однак більш просунуті атаки вимагають проактивного веб-фільтра на всіх кінцевих точках.

Відповідь на атаку в реальному часі

Усунути всі напади неможливо. Дуже важливо, щоб був план пом’якшення цих інцидентів у режимі реального часу.

Ось чому кероване виявлення та реагування (MDR) є останнім ключовим компонентом сильної стратегії керування кінцевими точками. Ефективна програма MDR зосереджена не тільки на моніторингу потенційних загроз і вразливостей, але й на активному виявленні фактичних атак на мережу та кінцеві точки та реагуванні на них.

Зробимо висновки. Ефективна стратегія моніторингу кінцевих точок має важливе значення для зменшення та пом’якшення загроз. Захист цих пристроїв вимагає стратегічного підходу, і моніторинг кінцевих точок має вирішальне

значення

Однак за допомогою правильних інструментів і стратегій можна створити надійну систему керування кінцевими точками для захисту всіх пристроїв у мережі.

Перелік посилань:

1. Моніторинг кінцевих точок: найкраще керівництво з безпеки та відповідності підприємств https://www.splunk.com/en_us/blog/learn/endpoint-monitoring.html (дата звернення 18.04.2024)
2. Що таке кінцева точка? https://www.microsoft.com/uk-ua/security/business/security-101/what-is-an-endpoint (дата звернення 18.04.2024)

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

Поради щодо ефективного вибору інструменту для сканування хмарних інформаційних ресурсів на вразливості

У світі, де кібербезпека набуває все більшого значення, сканування вразливостей стає неодмінною частиною ведення бізнесу. Сканування має бути регулярним, проводитися у визначений час і охоплювати всі можливі ресурси компанії. З розвитком хмарних обчислень важливість своєчасного сканування вразливостей зростає. Вибір ефективного сканера вразливостей для хмарних ресурсів залежить від потреб компанії, і може значно підвищити її безпеку.

1. Які методи сканування використовує інструмент? (статичний аналіз, динамічний аналіз, тестування на проникнення, машинне навчання). Чи може він виявляти глибоко приховані вразливості на додаток до типових проблем?

Статичний аналіз , який досліджує код до його запуску, виявляючи потенційні вразливості. Динамічний аналіз, який досліджує код під час його виконання, відстежуючи його поведінку та виявляючи вразливості. Тестування на проникнення, яке імітує атаки для перевірки стійкості систем до реальних загроз. Машинне навчання, яке використовується для прогнозування та виявлення нових, невідомих вразливостей. Ефективний сканер повинен використовувати комбінацію цих методів для виявлення як поширених, так і глибоко прихованих вразливостей.

2. З якими хмарними провайдерами інтегрується сканер? (AWS, Azure, GCP, Alibaba Cloud). Як інтеграція спрощує процес сканування та управління вразливостями?

Сканер, який інтегрується з вашим хмарним провайдером (AWS, Azure, GCP, Alibaba Cloud), може автоматично виявляти та класифікувати хмарні ресурси. Запускайте сканування за розкладом або на вимогу, збирайте та аналізуйте дані про вразливості, отримуйте сповіщення про виявлені проблеми. Інтеграція значно спрощує процес сканування та управління вразливостями.

3. Які рекомендації щодо усунення недоліків пропонує сканер? (чіткі, практичні, детальні). Чи пропонує він посилання на ресурси та інструменти для виправлення?

Сканер повинен пропонувати чіткі, практичні та детальні рекомендації щодо усунення вразливостей. Корисними будуть посилання на ресурси та інструменти для усунення вразливостей.

4. Чи пропонується безплатна версія сканера? Які функції доступні у безплатній версії? Чи буде безплатної версії достатньо для ваших потреб?

Деякі сканери пропонують безкоштовну версію з обмеженими функціями. Оцініть, чи буде достатньо безкоштовної версії для ваших потреб. Зверніть увагу на доступні функції, такі як. кількість сканувань, типи сканувань, обмеження хмарних ресурсів.

5. Наскільки легко користуватися сканером? Який рівень підтримки пропонує виробник?

Сканер має бути зручним і простим у використанні. Виробник повинен пропонувати якісну підтримку, таку як документація, навчальні матеріали, форуми та обслуговування клієнтів.

Перелік посилань:

1. Everything You Need to Know About Cloud Vulnerability Scanning | Symphony Solutions. *Symphony Solutions*. URL: https://symphony-solutions.com/insights/cloud-vulnerability-scanning

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

THE NIST CYBERSECURITY FRAMEWORK 2.0 CORE В СТРАТЕГІЇ КІБЕРБЕЗПЕКИ МІНЕСТЕРСТВА ОБОРОНИ США

NIST Cybersecurity Framework 2.0 — це комплексний підхід до управління ризиками кібербезпеки в секторах критичної інфраструктури, включаючи оборонну промисловість.

Національний інститут стандартів та технологій (NIST) Cybersecurity Framework надає високий, стратегічний погляд на життєвий цикл управління кібербезпекою в організації. Міністерство оборони (DoD) США інтегрує такі рамки для покращення своєї стратегії кібербезпеки, захисту чутливих даних і забезпечення національної безпеки.

Одним із ресурсів, доступних у сфері DIB (Рада оборонних інновацій), є Фреймворк кібербезпеки Національного інституту стандартів і технологій (NIST CSF). Зараз Національний інститут стандартів і технологій працює над випуском NIST CSF 2.0, який надасть технічну допомогу щодо вирівнювання регулятивних актів з міжнародними стандартами та NIST CSF. Міністерство може сприяти інтересам у сфері кібербезпеки, ділячись експертизою, специфічною для сектору DIB, та сприяючи координації політики (Рис.1).

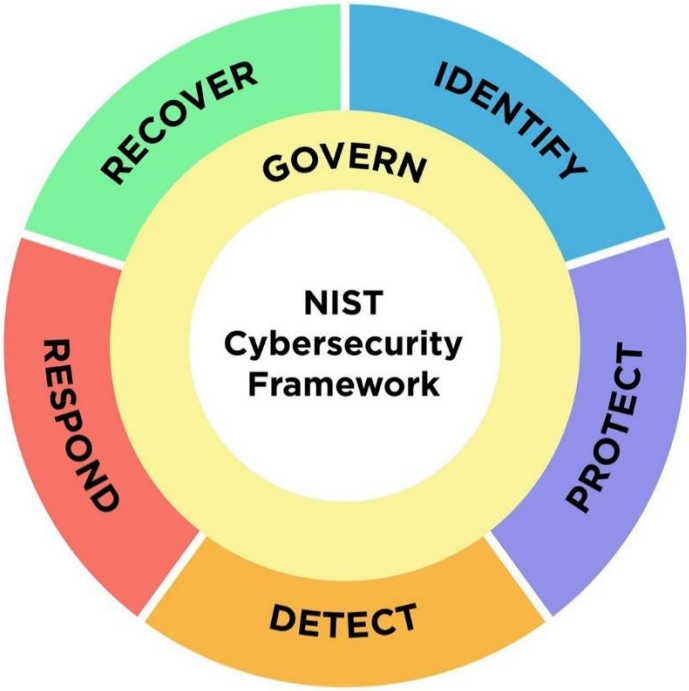


Рис.1. The NIST Cybersecurity Framework 2.0 Core

Важливість NIST Cybersecurity Framework 2.0 для DoD Міністерство оборони США.

Уніфікований підхід до управління ризиками:

Встановлює стандартизовану систему управління ризиками, яка зрозуміла у всіх відділах, покращуючи взаємодію та злагодженість реакцій.

Дотримання стандартів та норм:

Допомагає підтримувати відповідність федеральним регуляціям та стандартам, забезпечуючи відповідність всіх операцій найвищим протоколам безпеки.

Покращення стану безпеки:

Надає методології для ідентифікації, захисту, виявлення, реагування та відновлення після кібербезпечних загроз, значно покращуючи загальний стан безпеки DoD.

Основні складові рамки.

Ідентифікація: Розуміння систем, активів, даних та можливостей, що є критично важливими для національної безпеки.

Захист: Впровадження заходів безпеки для забезпечення надання критично важливих інфраструктурних послуг.

Виявлення: Розробка здатностей для ідентифікації кібербезпечних подій.

Реагування: Виконання відповідних дій у відповідь на виявлені кібербезпечні події.

Відновлення: Підтримка стійкості та відновлення можливостей або послуг, пошкоджених в результаті кібербезпечного інциденту.

Застосування в стратегії кібербезпеки DoD.

Інтеграція з військовими протоколами:

Гнучка природа Рамки NIST дозволяє її безпроблемно інтегрувати з існуючими стратегіями оборони та тактичними операціями.

Навчання та освіта:

Збільшує обізнаність та навчання у галузі кібербезпеки на всіх рівнях DoD, від фронтових оперативників до вищих керівників.

Розподіл ресурсів:

Допомагає у пріоритизації та розподілі ресурсів більш ефективно, забезпечуючи, що найважливіші активи захищені на найвищому рівні безпеки.

Безперервне вдосконалення:

Рамка сприяє циклу безперервного перегляду та удосконалення, що є критично важливим для адаптації до розвиваючого ландшафту кіберзагроз.

Інтеграція таких рамок забезпечує надійний захист проти все більш

складних кіберзагроз, зберігаючи цілісність та конфіденційність чутливої інформації національної безпеки. Це стратегічне застосування відповідає ширшим національним та міжнародним ініціативам з кібербезпеки, сприяючи створенню безпечнішого глобального кіберпростору.

Зробимо висновки.

Досягнення поставлених цілей у цій стратегії потребує координації зусиль всіх підрозділів МО США відповідно до Національної стратегії оборони (NDS), Національної стратегії кібербезпеки та Кіберстратегії МО США. Захист критичної інформації оборони та збереження конкурентної переваги вимагає від Міністерства інвестування в заходи щодо зміцнення кібербезпеки DIB. Успішна реалізація Стратегії кібербезпеки промислового комплексу оборонних матеріалів МО США передбачає залучення зовнішніх структур.

Перелік посилань:

1. Defense Industrial Base Cybersecurity Strategy 2024 - DoD CIO URL: https://dodcio.defense.gov/Portals/0/Documents/Library/DIB-CS-Strategy.pdf (дата звернення 10.04.2024)

2. NIST CYBERSECURITY FRAMEWORK 2.0 URL: https://www.nist.gov/system/files/documents/2022/10/03/NIST_CSF_update_Fact_Sheet.pdf (дата звернення 10.04.2024)

Гончаров Максим Ігорович
Студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ У СИСТЕМАХ ВІРТУАЛІЗАЦІЇ

Завдяки широкому розповсюдженню та простоті використання систем віртуалізації для прискорення розгортання клієнтських інфраструктур зросли також інциденти безпеки щодо доступності та цілісності таких систем.

Системи віртуалізації мають широке розповсюдження серед інструментів провайдерів в теперішній час. Це обумовлено необхідністю швидкого розгортання необхідної інфраструктури під технічне завдання замовника і потребує від технічних спеціалістів не лише вміння їх розгортання та налаштування, але і зобов'язує власників інформаційно-комунікаційних систем турбуватись про безпеку.

Термін *безпеки віртуальних систем* неможливо охарактеризувати одним чітким виразом через складність побудови та велику кількість можливих

варіантів побудови та вразливостей операційних систем та програмних рішень і продуктів, що можуть бути реалізовані як на самих віртуальних системах, так і по відношенню до серверів віртуалізації (наприклад ESXi та Vsphere). Зважаючи на неможливість чітко охарактеризувати визначення, більш доцільним вважається навести декілька базових принципів реалізації безпеки, які забезпечать більш швидкий процес організації розслідування та реагування на кібератаки та інциденти безпеки. До таких принципів можна віднести:

Обмеження доступу до мережевого сегменту серверів віртуалізації та його логування. На основі мінімально необхідних вимог щодо адміністрування серверного обладнання систем віртуалізації проектується окремий сегмент мережі, доступ до якого будуть мати лише чітко визначені хости з IP адресами, що будуть в ACL списках мережевого обладнання. Для реалізації логування необхідно обрати окремий від систем віртуалізації хост для налаштування сервісу syslog за, щонайменше період часу в 180 і більше днів.

Реалізація багатофакторної аутентифікації. Через необхідність віддаленого адміністрування та\або налаштування систем у сьогоднішніх реаліях російсько-української війни, пандемії COVID-19 та інших викликів, що унеможливлюють безпосереднє фізичне перебування всередині інфраструктури все більш поширеною стає практика налаштування VPN сервісів, що реалізують віддалене підключення всередині мережі та подальший доступ до необхідного обладнання. Для підвищення стану захищеності таких з'єднань необхідно налаштовувати багатофакторну аутентифікацію.

Своєчасне оновлення ПЗ та матеріально-технічної бази. Виходячи з практики проведення розслідування кіберінцидентів та кібератак багато власників ураженої інфраструктури виконують цей пункт лише частково, забуваючи про необхідність підтримання фізичного обладнання у належному стані. Таким чином після оновлення ПЗ рано чи пізно виникає проблематика неможливості подальшого оновлення через застарілі компоненти комп'ютерного обладнання – процесор, оперативна пам'ять, фізичні інтерфейси. Окремою групою слід виділити персональні робочі місця працівників та їх ПК – неприпустимим є використання застарілих ОС та їх несвоєчасне оновлення, що може призвести до витоку конфіденційних даних або їх втраті\недоступності.

Регулярне проведення тренувань з персоналом організації. Найбільш незахищеним, та таким, що призводить до більшості кіберінцидентів та кібератак залишається людський фактор. Регулярне проведення тестувань та тренувальних розсилань фішингових повідомлень, або відпрацювання run-book\play-book з реагування на кіберінциденти підвищує стан захищеності

організації та сприяє подальшому проведенню розслідування інцидентів.
Виходячи з усього вищесказаного можна зробити висновок, що розслідування кіберінцидентів пропорціонально залежить від початкових налаштувань та побудови ураженої мережі. Проведення розслідування кібератак потребує ретельного вивчення та розуміння інфраструктури жертви, якісної характеристики причетної до інциденту інформації та оперативного реагування на дії зловмисників, тому задля проведення більш якісного розслідування необхідно моделювати інциденти та реалізацію їх усунення або дослідження.

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

ТЕХНІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Технічні системи захисту інформації (ТЗІ) відіграють важливу роль у сучасному цифровому середовищі. В даній роботі розглядаються різноманітні аспекти їхньої ролі, включаючи шифрування, криптографію, фізичні методи захисту та інші аспекти захисту даних. Вона також досліджує важливість технічних систем захисту інформації для підприємств у забезпеченні безпеки, надійності та конфіденційності їхніх інформаційних ресурсів.

Технічні системи захисту інформації – це комплекс заходів, спрямованих на захист інформації від несанкціонованого доступу, викрадення, модифікації, знищення, а також від несанкціонованого впливу. ТЗІ є складовою комплексної системи захисту інформації (КСЗІ), яка включає в себе також організаційні та правові заходи [1].

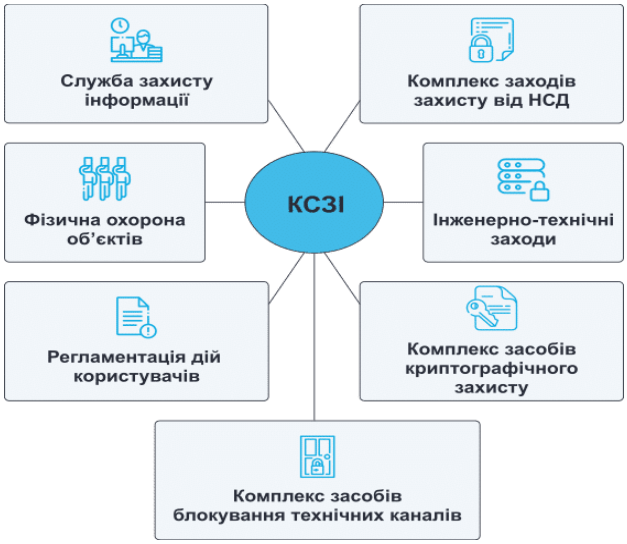


Рис.1 – Складові КСЗІ

Технічний захист інформації в автоматизованих системах і засобах обчислювальної техніки, призначених для формування, пересилання, приймання, перетворення, відображення та зберігання інформації, забезпечується комплексом конструкторських, організаційних, програмних і технічних заходів на всіх етапах їх створення й експлуатації [2, с.1]. Вони включають в себе [3]:

Фізичні заходи захисту. Використовуються для зовнішнього захисту засобів обчислювальної техніки та територій. Вони створюють фізичні перешкоди на можливих шляхах проникнення і доступу до компонентів інформаційних систем.

Апаратні засоби захисту. Вбудовуються в блоки електронних систем обробки та передачі даних для внутрішнього захисту засобів обчислювальної техніки, таких як термінали, пристрої введення та виведення даних, процесори.

Програмні та програмно-апаратні засоби захисту. Необхідні для виконання логічних і інтелектуальних функцій захисту, які вмонтовані до складу програмного забезпечення системи. Апаратно-програмні засоби захисту поєднують у собі програмні та апаратні засоби.

Криптографічні методи захисту. Використовуються з метою забезпечення конфіденційності та цілісності даних під час їх передачі або зберігання. Ці методи включають різні техніки шифрування даних, що дозволяють ефективно захищати інформацію від несанкціонованого доступу.

Впровадження комплексу ТЗІ в підприємство дозволяє здійснити наступні методи захисту інформації:

- Використання захищеного обладнання, яке має вбудовані заходи безпеки для запобігання несанкціонованого доступу до даних.
- Регламентування роботи користувачів, технічного персоналу, програмних засобів, елементів баз даних і носіїв інформації з обмеженим доступом, що передбачає розмежування доступу до конфіденційної інформації.
- Регламентування архітектури автоматизованих систем і засобів обчислювальної техніки з метою забезпечення високого рівня безпеки.
- Інженерно-технічне оснащення споруд і комунікацій, які використовуються для експлуатації автоматизованих систем і засобів обчислювальної техніки, з метою забезпечення фізичної безпеки.
- Пошук, виявлення і блокування закладних пристроїв, що можуть використовуватися для несанкціонованого отримання доступу до інформації або її підміни.

В області технічного захисту інформації важливим етапом є атестація об’єкта захисту, яка є підтвердженням наявності необхідних умов для

ефективного захисту інформації. Зокрема, ці умови можуть перешкоджати фізичному проникненню чи забезпечувати маскування інформації в разі проникнення. Для цього використовуються різноманітні технічні засоби, такі як замки, грати на вікнах, захисна сигналізація, генератори шуму, мережеві фільтри та інші. Технічні засоби відрізняються високою надійністю та стійкістю до зовнішніх впливів, що дозволяє їм ефективно виконувати свої функції незалежно від суб'єктивних факторів. Наприклад, екрановані приміщення спрямовані на зниження потужності електромагнітного випромінювання та зміну структури електромагнітного поля з метою запобігання витоку інформації.

Комплекс технічного захисту інформації є необхідним елементом для забезпечення безпеки та конфіденційності даних в сучасних інформаційних системах. Включаючи фізичні, апаратні та програмні заходи, цей комплекс створює систему захисту, яка забезпечує відповідність вимогам безпеки й захищає інформацію від різноманітних загроз.

Використання технічних засобів захисту, таких як шифрування, захищене обладнання, системи виявлення вторгнень та інші, допомагає ефективно захищати інформаційні ресурси від несанкціонованого доступу та зберігати їх конфіденційність.

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

SOD RISKS MANAGEMENT

Segregation of duties (SoD) is an internal control designed to prevent error and fraud by ensuring that at least two individuals are responsible for the separate parts of any task.

SoD entails the breakdown of tasks that could typically be managed by a single individual into multiple components, ensuring that no individual holds sole authority over them.

Also referred to as separation of duties, SoD stands as a cornerstone of enterprise control systems. Its core principle lies in the allocation of different segments of a task or transaction to distinct individuals, thereby preventing any single person from acquiring complete or excessive control and subsequently misusing it for unauthorized purposes like fraud or embezzlement.

The practice of segregating duties finds widespread application in areas like payroll management, where the risks of fraud and error loom large. By dispersing

responsibilities and tasks, organizations aim to minimize such risks. For instance, in payroll operations, it's common to assign one employee to handle accounting tasks while another oversees check approval or funds disbursement.

The need for segregation of duties

The rationale behind SoD is grounded in the belief that the operation of a business should not rely on the actions of a single individual. Instead, it advocates for shared responsibilities, dispersing critical functions among multiple personnel or departments to mitigate the risk of fraudulent or unethical behavior. SoD is integral to enterprise risk management and compliance efforts, including adherence to regulations such as the Sarbanes-Oxley Act of 2002 (SOX).

By preventing the consolidation of control, SoD mitigates the potential for abuse and unethical conduct. By distributing critical processes among multiple parties, organizations reduce the likelihood that any single employee or external entity, either independently or in collusion, could engage in activities such as fund misappropriation, corporate espionage, retaliatory actions, or financial manipulation.

SoD is prevalent in various business domains beyond finance and accounting. Examples include warehouse operations, real estate transactions, and software development, where distinct individuals or teams handle different aspects of a process to enhance security and accountability.

Common examples of segregation of duties in enterprise settings

Segregation of duties is a common concept in financial and accounting processes. Payroll is one example where the segregation of duties works well and is even desirable.

Another example is in a warehouse, where the person receiving goods from a supplier and the person authorizing payment to the supplier are two different employees. Similarly, the person maintaining inventory records does not physically control the inventory, which reduces the possibility of inventory theft or incorrect reporting.

A third example is within the real estate business, where the person selling a property or other fixed asset to a customer cannot record the sale or collect the payment from the customer. Since a different person is in charge of recording the sale and receiving payment, the separation of duties ensures that the person completing the sale cannot take an illegal cut from customers or deny the organization the full revenue from the sale of the asset.

Yet another example is in software development. A developer creates the code but doesn't have the authority to also deploy it into production. Someone else reviews and approves the code and then moves it into production. The idea is to prevent the release of unauthorized code, whether it's done maliciously or accidentally.

The following are some other examples of SoD applications:

- transaction authorizations or approvals;
- receiving and maintaining asset custody;
- reconciliation activities related to bank statements, checking accounts and booking entries to the general ledger;
- depositing cash;
- approving timecards or timesheets.

In general, organizations can enforce SoD in any financial, IT, cybersecurity, software or other process/business function that can have a critical impact on an enterprise's business, revenues, reputation or customer relationships.

Challenges and drawbacks of segregation of duties

While SoD enhances security, it can also introduce challenges. Dividing tasks may impact operational efficiency, increase costs, and complicate processes, particularly in smaller organizations with limited staffing. Consequently, organizations often apply SoD selectively to areas with the highest risk exposure, balancing control measures with operational needs and resource constraints.

Furthermore, the implementation of SoD can lead to increased operational costs, complexity, and staffing requirements. Consequently, organizations often choose to apply SoD selectively, focusing on the most vulnerable or mission-critical aspects of their operations. These are the areas where the risk of fraud and theft is most pronounced and poses the greatest threat to the organization's financial stability, security, reputation, or regulatory compliance.

However, smaller organizations may encounter difficulties in achieving effective segregation of duties due to limited personnel available to perform different parts of a task. In such cases, one individual may be responsible for overseeing an entire process, such as payroll management, where a single employee handles both accounting functions and check authorization.

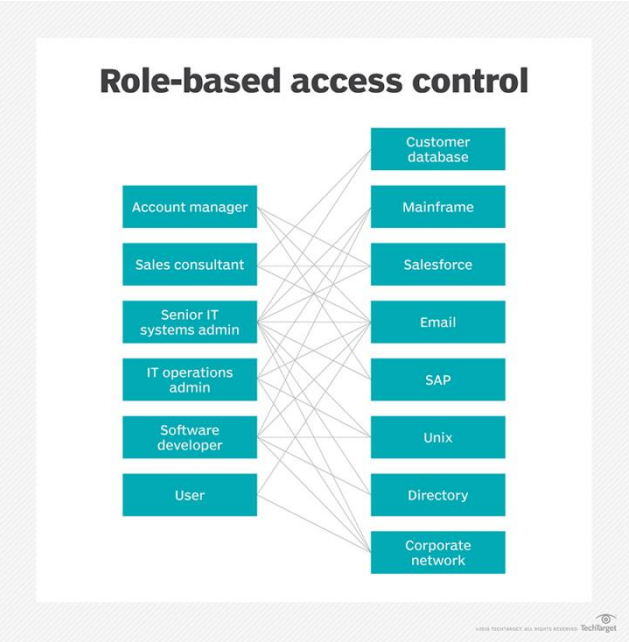
Despite these challenges, SoD remains a vital component of internal control frameworks, helping organizations safeguard their assets, maintain data integrity, and uphold compliance standards. By promoting accountability, transparency, and oversight, SoD contributes to the overall integrity and trustworthiness of organizational operations. Thus, while it may require careful planning and resource allocation, the benefits of implementing SoD far outweigh the associated challenges.

Important concepts in segregation of duties

There are two important concepts in segregation of duties: SoD conflicts and SoD violations.

SoD conflicts. When an individual can potentially act in their own interest and against the company's interests, it can result in an SoD conflict. This simply means that they have multiple roles in a process, which allows them to perform a combination of important activities that could potentially harm the integrity of the process and, ultimately, the organization.

To prevent such issues, organizations should check for and analyze potential SoD conflicts. Strong controls should be implemented to prevent conflicts and to protect the company from individuals engaging in criminal activity. One way to prevent SoD conflicts is to implement role-based access control (Picture 1). An authorized person should analyze each role for both intra-role and inter-role SoD overlaps.



Picture 1. Implementing role-based access control can help prevent segregation of duties conflicts.

SoD violations. An SoD violation occurs when an employee abuses their role and access – usually deliberately – to perform a prohibited action. The prohibition may be in place due to internal company policy or an external industry regulation. A violation typically occurs when the user has or gains control over more process steps than they are allowed and then misuses that access for their own benefit.

For example, an organization may have a rule that the person approving timesheets is not allowed to also distribute paychecks. But when someone takes advantage of a control weakness to do both activities for fraudulent purposes, it becomes an SoD violation.

An example of a violation due to an external regulation is a senior leader, such as a CEO or CFO, manipulating financial statements in violation of SOX regulations; this can result in hefty fines for the company and a prison sentence for that employee.

The segregation of duties matrix

Implementing SoD can be a complex endeavor. Compliance managers reduce the complexity with a segregation of duties matrix. The matrix enables managers to clearly separate the various roles, responsibilities and risks in the organization. They can also identify potential conflicts and resolve them before any potential damage to the organization occurs.

The SoD matrix plots user roles on both the X and Y axes to clearly show SoD conflicts. It also maps activities and duties to roles within the workflow to help compliance teams segregate incompatible duties.

Below is an example of an SoD matrix for an employee compensation process (Picture 2), where a checkmark signifies that the role has responsibility for the task.

Procedure/ function	User group (role)	Hire employee	Change compensation	Change benefits	Create paycheck
Hire employee	1	√			
Change compensation	2		√	√	
Change benefits	3		√	√	
Create paycheck	4				√

Picture 2. SoD matrix for an employee compensation process

In the matrix above, the person in charge of hiring employees cannot also be in charge of changing compensation or creating paychecks. Similarly, the person in charge of changing benefits cannot hire employees.

Here's another example of an SoD matrix for a software development process (Picture 3).

Procedure/ function	User group (role)	Develop software	Test software	Make data backups	Push code to production
Develop software	1	√			
Test software	2		√		
Make data backups	3			√	
Push code to production	4				√

Picture 3. SoD matrix for a software development process

The software developer is not allowed to test software, push the code to production

or make data backups. Similarly, the person who pushes code to production cannot carry out the other three tasks.

Organizations can create SoD matrices by hand or with spreadsheet software, such as Excel. However, they are most commonly generated automatically using enterprise resource planning (ERP) software.

References:

1. What is Segregation of Duties (SoD)? https://www.nextlabs.com/what-is-segregation-of-duties-sod (дата звернення 31.03.2024)
2. Segregation of duties (SoD): https://channel4it.com/publications/ostann-onovlennya-delinea-server-suite-znizhu-rizik-zagroz-bekdoru-na-serverah.html (дата звернення 31.03.2024)

Діденко Данило Юрійович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

ПОБУДОВА SOC

Багато великих організацій на власному досвіді переконалися, що ефективне виявлення та реагування на інциденти кібербезпеки має бути одним із ключових елементів їхніх стратегій управління ризиками. Однак впровадити таку спроможність надзвичайно складно: технологічна та процесна інтеграція є складною, а організаціям, як правило, бракує людей та/або навичок для проєктування, розгортання і, зрештою, експлуатації ефективних операційних центрів безпеки (SOC).

Що таке Security Operations Center

Перш ніж дізнатися, як побудувати операційний центр безпеки (Security Operations Center), дуже важливо спочатку дізнатися трохи більше про те, що таке SOC. Security Operations Center - це центральний "хаб", в якому команди IT та кібербезпеки організації беруть участь у виявленні, аналізі та реагуванні на загрози. Він відповідає за моніторинг, виявлення, реагування і пом'якшення загроз та інцидентів кібербезпеки. Основна мета SOC - забезпечити безпеку інформаційних систем і даних організації.

Операційний центр безпеки (SOC) здійснює моніторинг і захист цифрових активів, координує зусилля для захисту організації від кібератак і критичних загроз, а також вживає заходів у разі необхідності. Створення центру безпеки вимагає значних інвестицій в персонал і технології і може виглядати недоцільним для малого та середнього бізнесу. Проте, якщо ви дійсно хочете захистити свою організацію - це правильний вибір, і всі зусилля будуть того варті.

Основні функції SOC

- Моніторинг: SOC постійно моніторить і аналізує велику кількість даних, включаючи системні журнали, мережевий трафік, активність користувачів, та інші джерела, з метою виявлення потенційних загроз та інцидентів безпеки.
- Виявлення загроз: SOC використовує спеціальні системи виявлення вторгнень (Intrusion Detection Systems, IDS) та виявлення аномалій (Anomaly Detection Systems), щоб вчасно виявляти вторгнення, зловживання та інші загрози безпеці.
- Реагування на інциденти: Після виявлення потенційних загроз або інцидентів безпеки, персонал SOC забезпечує швидку реакцію для нейтралізації загрози, мінімізації збитків та відновлення нормального функціонування систем.
- Інцидентний аналіз та дослідження: Після завершення реагування на інцидент, SOC проводить детальний аналіз подій, щоб встановити причини та методи атак, а також розробляє заходи для запобігання подібним інцидентам у майбутньому.
- Управління загрозами: SOC використовує різноманітні інструменти та методи для управління ризиками та загрозами безпеки, включаючи розвиток стратегій безпеки, впровадження заходів захисту та моніторинг їх ефективності.
- Впровадження та оновлення заходів захисту: SOC відповідає за впровадження та оновлення систем безпеки, таких як фаєрволи, антивіруси, системи виявлення вторгнень тощо, для забезпечення захисту інформації та інфраструктури від потенційних загроз.

Побудова SOC за 7 кроків

Побудова SOC (Security Operations Center) може бути складним і непростим процесом. Однак, шлях до створення надійного та ефективного SOC, який відповідатиме конкретним потребам вашої організації, можна умовно поділити на 7 кроків:

1. Визначення цілей та завдань. Почніть з визначення цілей і завдань вашої SOC. Які конкретні ризики безпеки ви хочете зменшити? Які KPI ви будете використовувати для вимірювання успіху? Чітке визначення цілей і завдань допоможе вам розробити SOC, яка відповідатиме конкретним потребам

вашої організації.

2. Розробка стратегії безпеки. Розробіть комплексну стратегію безпеки, яка окреслить ваші процеси виявлення інцидентів, реагування на них та звітування. Вона повинна включати процедури обробки інцидентів безпеки, розвідку загроз і регулярний аудит безпеки.

3. Визначення бюджету та ресурсів. Побудова SOC вимагає значних витрат часу та грошей. Заздалегідь визначте свій бюджет і ресурси, щоб мати змогу виділити необхідні кошти та персонал для побудови і підтримки SOC.

4. Визначення ключових активів. Визначте ключові активи, які захищатиме ваша SOC, такі як сервери, бази даних і додатки. Визначте рівень ризику, пов'язаний з кожним активом, щоб визначити пріоритетність заходів безпеки.

5. Вибір інструментів та технологій. Виберіть інструменти та технології, які ви будете використовувати для підтримки SOC, такі як системи управління інформацією та подіями безпеки (SIEM), системи виявлення та запобігання вторгненням і платформи для розвідки загроз. Обирайте інструменти, які добре інтегруються один з одним і забезпечують моніторинг та оповіщення в режимі реального часу.

6. Створення та навчання команди. Найміть команду кваліфікованих фахівців, які мають необхідні знання та досвід для управління інцидентами безпеки. Забезпечте постійні можливості для навчання та розвитку, щоб ваша команда була в курсі новітніх технологій та тенденцій.

7. Тестування та вдосконалення SOC. Тестуйте та вдосконалюйте свою SOC, щоб переконатися, що вона ефективно виявляє та реагує на інциденти безпеки. Проводьте аудит безпеки та симуляції, щоб визначити області для вдосконалення.

У підсумку, створення SOC вимагає ретельного планування, інвестицій у правильні інструменти та технології, а також кваліфікованої команди професіоналів. Дотримуючись цих 7 кроків, ви зможете створити надійну та ефективну SOC, яка ефективно захистить цифрові активи вашої організації від кіберзагроз.

Перелік посилань:

1. Building a Security Operations Centre (SOC) URL: https://www.ncsc.gov.uk/collection/building-a-security-operations-centre (дата звернення 08.04.2024)

2. 7 Steps to Building A Security Operations Center (SOC) URL: https://logrhythm.com/blog/7-steps-to-build-your-security-operations-center (дата звернення 08.04.2024)

3. 4 Steps to Building a Security Operations Center URL: https://underdefense.com/blog/4-steps-to-building-a-security-operations-center (дата звернення 08.04.2024)

Додонов Кірілл Михайлович, студент групи БСДМ-51,
Кузьменко Андрій Олександрович, аспірант групи АІКБ-11,
ННІЗІ ДУІКТ, Київ, Україна

АКТУАЛЬНІСТЬ ВИКОРИСТАННЯ SIEM-СИСТЕМ В КОРПОРАТИВНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

SIEM представляє ключову зміну в еволюції кібербезпеки, допомагаючи організаціям завчасно виявляти, аналізувати та реагувати на загрози безпеці до того, як це зроблять зловмисники. Ці системи збирають дані журналу подій із різних джерел, використовуючи аналіз у реальному часі, щоб усунути шум і підтримати ефективні команди безпеки.

SIEM визначається як платформа кібербезпеки, яка централізує інформацію про безпеку з кількох кінцевих точок, серверів, додатків та інших джерел, щоб допомогти контролювати IT-інфраструктуру, перевіряти аномалії в режимі реального часу, сповіщати фахівців із безпеки щоразу про аномальну подію та зберігати докладні дані журнали всіх подій (аномальних, несприятливих або звичайних) – часто з використанням таких інструментів, як бази даних аналізу загроз, штучний інтелект, автоматизація тощо.

Security Information & Event Management (SIEM) — це рішення, яке поєднує два старих інструменти: SIM (Security Information Management) і SEM (Security Event Management). Сучасні системи SIEM також містять технології оркестрування безпеки, автоматизації та реагування (SOAR) і аналізу поведінки користувачів і об’єктів (UEBA) для автоматизації реагування на загрози та виявлення загроз на основі аномальної активності відповідно.

Разом вони прискорюють виявлення та вирішення подій та інцидентів безпеки в IT-середовищі. SIEM пропонує фахівцям з кібербезпеки повну та консолідовану картину загальної безпеки цифрової інфраструктури та бачення дій у їх IT-середовищі.

Щоб захиститися від складніших кібератак у цифровій економіці, компанії повинні контролювати та захищати свої дані. До SIEM аналітики безпеки вручну аналізували мільйони фрагментованих і розділених бітів даних для кожної програми та точки безпеки. Таким чином, SIEM може прискорити реагування та виявлення кібератак, роблячи розслідування аналітиків безпеки більш ефективними та точними.

Функції централізованого збору, категоризації, моніторингу, синхронізації та аналізу програмного забезпечення SIEM підвищують швидкість і точність реагування на події безпеки. Це полегшує моніторинг у режимі реального часу та усунення несправностей IT-інфраструктури IT-командами.

Фреймворки SIEM відрізняються за функціональними можливостями, але часто містять такі основні функції:

- Керування журналами: системи SIEM збирають величезну кількість даних у централізованому місці, упорядковують їх, а потім вирішують, чи вказують вони на ризик, вторгнення чи проникнення.
- Кореляція подій: потім матеріал аналізується, щоб знайти зв’язки та тенденції, щоб можна було виявити можливі небезпеки та швидко на них реагувати.
- Моніторинг і реагування на інциденти: системи SIEM відстежують проблеми безпеки в мережі організації та пропонують попередження та перевірки всіх дій, пов’язаних з інцидентами.
- Зберігання даних: SIEM зберігає довгострокові історичні дані для полегшення аналізу відповідності, відстеження та звітування. Особливо важливо в судово-медичній експертизі, яка може відбутися через роки після інциденту.
- Автоматизація SOC: використовуючи інтерфейси прикладного програмування (API), SIEM може взаємодіяти з іншими системами безпеки та дозволяти персоналу безпеки розробляти автоматизовані ігри та процеси для реагування на певні події.
- Інформаційні панелі та візуалізації: SIEM створює візуалізацію, яка дає змогу окремим особам досліджувати дані про події, розпізнавати тенденції та виявляти поведінку, яка відхиляється від типових процедур або потоків подій.

Системи SIEM можуть зменшити кіберризик за допомогою різних випадків використання, зокрема виявлення аномальної поведінки користувачів, відстеження шаблонів використання, обмеження спроб доступу та створення звітів про відповідність.

- Використання рішення SIEM має низку переваг:
- Розширена видимість - об'єднання всіх журналів організації у локальних і хмарних додатках, серверах, базах даних тощо для отримання більш глибокого розуміння користувачів, кінцевих точок, трафіку, активності і т.д., що дозволяє підтримувати контроль над мережею і за її межами в міру масштабування компанії.
- Нормалізація даних - Різноманітні технології, що використовуються у середовищі організації, генерують тонни даних у різних форматах. Хоча не кожне рішення SIEM збирає, аналізує і нормалізує дані автоматично, багато з них пропонують постійний аналіз для підтримки різних типів даних. Це дозволяє легко співвідносити дані для аналізу та розслідування загроз.

- Кореляція журналів - на додаток до збору журналів, SIEM може корелювати їх для аналізу. Це дозволяє створювати оповіщення, тенденції та звіти про безпеку. Журнали, які охоплюють кілька хостів, надають набагато багатший контекст, який допоможе отримати інформацію про події безпеки. Організація може співвіднести такі події, як підозріла активність DNS, незвична активність портів на маршрутизаторах і брандмауерах, загрози для кінцевих точок або антивірусів тощо, щоб виявити потенційну атаку.
- Виявлення загроз - кореляція та аналіз призводить до виявлення загроз та оповіщення. Після того, як SIEM буде належним чином налаштована і адаптована до середовища організації, можна виявити ознаки компрометації або загрози, які можуть призвести до порушення безпеки. Деякі SIEM постачаються з попередньо налаштованим набором правил оповіщення за замовчуванням. Важливо знайти правильний баланс між помилковими спрацьовуваннями та помилковими відмовами, щоб зменшити зайві сповіщення.
- Відповідність нормативним вимогам - Багато нормативних документів, що охоплюють різні галузі, такі як HIPAA, CMMC, NIST, FFIEC, PCI DSS тощо, вимагають від організацій збирати та зберігати історію журналів аудиту протягом певного періоду часу, виявляти загрози та реагувати на них, а також регулярно створювати звіти про безпеку для аудиторів.

SIEM, яку можна широко інтегрувати з різними платформами, продуктами постачальників, локальними і хмарними додатками, сервісами та інфраструктурою, дозволить вам отримати найширше охоплення моніторингу безпеки. Це означає відсутність прогалин у системі моніторингу, більше даних для співставлення та аналізу з метою виявлення загроз, а також скорочення часу на виявлення та реагування на загрози.

Перелік посилань:

1. BasuMallick C. 9 Reasons Why SIEM is Important For Your Organization - Spiceworks. *Spiceworks*.URL: https://www.spiceworks.com/it-security/data-security/articles/security-information-and-event-management/ (дата звернення: 04.04.2024).
2. The Top 5 Benefits of Using SIEM | Stellar Cyber. *XDR network, internet, cybersecurity software & solutions*. URL: https://stellarcyber.ai/learn/benefits-of-siem/ (дата звернення: 06.04.2024).
3. What Is SIEM and What Are the Benefits?. *Blumira*. URL: https://www.blumira.com/glossary/what-is-siem/ (дата звернення: 08.04.2024).

Дорохін Орест Олександрович
студент групи АІКБ-125, ННІЗІ ДУІКТ, Київ, Україна

ЕМПІРИЧНА ОЦІНКА АНСАМБЛІВ ТА ТРАДИЦІЙНИХ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ВЕБ-АТАК

Атаки на кібербезпеку, націлені на програмне забезпечення, стали прибутковими та популярними цілями для кіберзлочинців. В даній статті описується підґрунтя для подальшого заглиблення в тему застосування моделей машинного навчання для запобігання атакам на корпоративні веб додатки напротивагу існуючим сигнатурним та евристичним методам.

Програмний рівень OSI став привабливою та поширеною мішенню для хакерів, які використовують загрози, орієнтовані на експлуатацію веб-атак, та ініціюють атаки, які можуть поставити під загрозу критичні функції корпоративних веб-додатків, такі як конфіденційність, цілісність та доступність. Для запобігання таким атакам застосовуються системи безпеки, а саме системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS). Коли методи IDS або IPS впроваджується для захисту веб-додатків, вони отримують назву брандмауерів веб-додатків (WAF) [1].

WAF, засновані на сигнатурах, такі як ModSecurity, є найбільш поширеним типом [2]. Ці системи ефективно виявляють відомі атаки з низькою частотою помилкових спрацювань (FPR), але вони не можуть виявити невідомі атаки, такі як атаки "нульового дня". На відміну від цього, системи, засновані на аномаліях, краще виявляють невідомі атаки, але вони генерують вищий FPR [3]. Таким чином, традиційні сигнатурні та аномальні системи виявлення та запобігання атакам не є придатними для гарантування безпеки сучасних веб-додатків.

Одним з найпопулярніших підмножин ШІ є рішення, засновані на машинному навчанні (ML). Однак традиційні моделі ML часто дають високий FPR та FNR для кібератак, які стають все складнішими [14].

Щоб вирішити проблему традиційних ML-підходів, методи ансамблю є одними з найважливіших напрямків в дослідженнях машинного навчання для виявлення кібератак [1]. Головна ідея використання ансамблів класифікаторів полягає в тому, що агрегування прогнозів від кількох окремих класифікаторів дає кращі результати виявлення [4]. Згідно з дослідженням “A survey of intrusion detection systems based on ensemble and hybrid classifiers” [6], існують два типи методів ансамблю: (1) однорідний ансамбль, заснований на базових моделях одного типу, наприклад, Random Forest (RF), і (2) різнорідний ансамбль, який включає різні типи базових моделей, наприклад, Support Vector Machine (SVM), K-Nearest Neighbors (KNN) та Decision Tree (DT) [1].

Останнім часом методи ансамблю широко використовуються в різних галузях, включаючи кібербезпеку [5]. Однак потреба в належному, високопродуктивному ML-алгоритмі в галузі кібербезпеки залишається невирішеною проблемою дослідження [5]. Численними дослідженнями показано, що оцінка ефективності технік, заснованих на навчанні, залежить від додатка та реалізації. Тому все ще є потреба в бенчмарку технік ансамблю та базових класифікаторів в контексті виявлення веб-атак [7].

Методами оцінки ефективності ансамблю в виявленні веб-атак та порівняння їх з окремими класифікаторами, є такі метрики оцінки як: точність (A), повнота (R), влучність (P), F-значення (F1), FPR, FNR, ROC-крива, час навчання та прогнозування (TT та PT). В якості датасету доцільно використовувати два з найбільш використовуваних публічних та реалістичних наборів даних про веб-атаки, що на данний момент представлені ECML/PKDD 2007 та CSIC HTTP 2010, щоправда їх застарілість часто викликає критику, але наявність публічних відкритих датасетів цінується високо через їх дефіцитність, а їх використання необхідне для надійного порівняння продуктивності сучасних ML-методів.

Полягаючись в своїй основі на принцип, що об'єднання прогнозів кількох класифікаторів виправляє помилки, вироблені кожним класифікатором, і призводить до кращої продуктивності, більшість недавніх досліджень зосереджувалися на використанні методів ансамблю, а не окремих класифікаторів. Це сприяє покращенню продуктивності виявлення веб-атак. Через емпіричну оцінку підходів ансамблю та окремих класифікаторів для виявлення веб-атак в корпоративних веб-додатках, можливо дослідити та заповнити цю дослідницьку прогалину. Наступні дослідницькі питання на думку автора є основними для подальшого ефективного вивчення в темі захисту корпоративних веб-додатків за допомогою машинного навчання:

1. Чи підходять методи ансамблю для виявлення веб-атак?
2. Який метод ансамблю найкраще підходить для виявлення веб-атак?
3. Наскільки ефективні методи навчання ансамблю в порівнянні з техніками однокласифікації для виявлення веб-атак?

Підсумовуючи, відповідь на ці три основні питання зможе допомогти вченим та практикам у складній задачі вибору найбільш відповідного алгоритму для виявлення веб-атак серед алгоритмів машинного навчання.

Перелік посилань:

1. Desmet, L., Piessens, F., Joosen, W., Verbaeten, P., 2006. Bridging the gap between web application firewalls and web applications. In: Proceedings of the Fourth ACM Workshop on Formal Methods in Security, pp. 67–77, URL: https://doi.org/10.1145/1180337.1180344 (дата звернення 02.04.2024)

2. A distributed deep learning system for web attack detection on edge devices, IEEE Trans. Industr. Inf., 16 (3) (2019), pp. 1963-1971
3. Jemal, I., Haddar, M.A., Cheikhrouhou, O., Mahfoudhi, A., 2021. Performance evaluation of Convolutional Neural Network for web security. Comput. Commun. 175, 58–67, URL: https://doi.org/10.1016/j.com (дата звернення 02.04.2024)
4. Improving malware detection using big data and ensemble learning. Comput. Electr. Eng., 86 (2020), p. 106729
5. Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation. Comput. Sci. Rev., 39 (2021), p. 100357
6. A survey of intrusion detection systems based on ensemble and hybrid classifiers. Comput. Sec., 65 (2017), pp. 135-152
7. Caruana, R., Niculescu-Mizil, A., 2006. An empirical comparison of supervised learning algorithms. In: Proceedings of the 23rd International Conference on Machine Learning, pp. 161–168, URL: https://doi.org/10.1145/1143844.1143865 (дата звернення 02.04.2024)

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

SECURITY OF CLOUD TECHNOLOGIES

Cloud security encompasses a range of measures and practices designed to protect data, applications, and infrastructure hosted in cloud environments. It is crucial to understand challenges posed by shared responsibility models and the need for robust security protocols to safeguard against data breaches and unauthorized access. Ultimately, effective cloud security strategies are crucial for ensuring confidentiality, integrity, and availability in the cloud.

Cloud security is a responsibility shared between the cloud provider and the customer. There are three categories of responsibilities in the shared responsibility model: responsibilities that are always assigned to the provider, responsibilities that are always assigned to the customer, and responsibilities that depend on the service model: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) (Figure.1), such as cloud email.

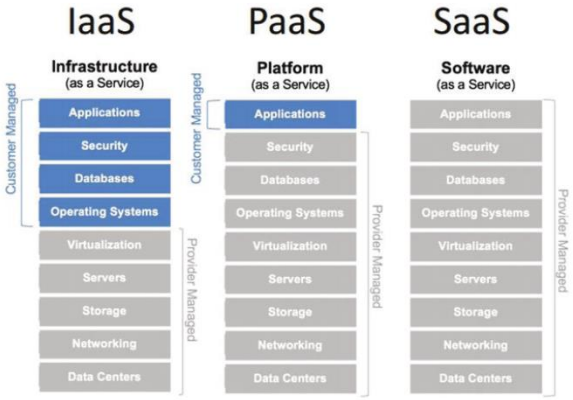


Figure.1 – Iaas, Paas, and SaaS

The security responsibilities that always fall to the provider are related to protecting the infrastructure itself, as well as accessing, patching, and configuring the physical nodes and physical network on which compute instances, storage, and other resources run.

Security responsibilities that are always placed on the customer include managing users and their access privileges (identity and access management), protecting cloud accounts from unauthorised access, encrypting and securing cloud information resources, and managing security levels (compliance).

The core principle of cloud security is Zero Trust principle. Zero Trust principle is to not automatically trust anyone or anything on or off the network and to verify (i.e. authorise, verify and protect) everything. Zero Trust, as an example, promotes a lowest privilege management strategy in which users are only granted access to the resources they need to fulfil their responsibilities. Similarly, it encourages developers to properly secure web applications. For example, if a developer has not blocked ports consistently or implemented "need-to-know" permissions, a hacker who takes over the application will have privileges to retrieve and modify data from the database. Zero Trust networks also use micro-segmentation to make cloud network defences much more granular. Micro-segmentation creates protected zones in data centres and cloud environments, separating workloads from each other, protecting everything within the zone, and enforcing policies to protect traffic between zones.

Although cloud providers such as Amazon Web Services (AWS) and Microsoft Azure (Azure) offer a variety of cloud security features and services, only an integrated stack of cloud and third-party security tools provides the consolidated security visibility and detailed policy-based control that's needed to implement industry best practices:

Groups and roles.

Work with groups and roles, rather than at the individual IAM level, to make it easier to update IAM definitions as business requirements change. Grant only the minimum privileges to access assets and APIs that a group or role needs to perform its tasks.

Logical isolation.

Set up business-critical resources and applications in logically isolated sections of your provider's cloud network. Implement subnets to micro-segment workloads

from each other with detailed security policies on subnet gateways.

Application protection.

Protect all applications (and especially distributed cloud applications) with a next-generation web application firewall. It will inspect and monitor traffic to and from web application servers in detail.

Enhanced data protection.

Protect data with encryption at all transport layers, secure file shares and communications, continuous compliance risk management, and good storage hygiene.

Threat intelligence.

AI-powered abnormality detection algorithms are used to identify unknown threats, which are then forensically analysed to determine their risk profile. Real-time alerts for intrusions and policy violations reduce remediation time, sometimes even triggering automatic remediation workflows.

Перелік посилань:

1. Cloud Computing and Distance Learning in Computer Science. URL: https://www.researchgate.net/publication/350783406_Cloud_Computing_and_Distance_Learning_in_Computer_Science (accessed 26.03.2024)
2. What is Cloud Security? URL: https://www.kaspersky.co.uk/resource-center/definitions/what-is-cloud-security (accessed 27.03.2024)

Єкімов Іван Вікторович

Студент групи БСДМ-53,ННІЗІ

ДУІКТ, Київ , Україна

Менеджмент інформаційної безпеки

Менеджмент інформаційної безпеки (МІБ) є стратегічним підходом до управління заходами, спрямованими на захист конфіденційності, цілісності та доступності інформації в організації. Цей систематичний підхід визначається як система, спрямована на забезпечення безпеки інформації від усіх можливих загроз. Сучасні технології роблять підприємства більш залежними від інформації, що робить інформаційну безпеку ще більш критичною.

Основна мета МІБ полягає у встановленні ефективних політик, процедур та технологічних рішень для мінімізації ризиків порушення безпеки даних та

забезпечення стійкості до кіберзагроз. Він вимагає розробки та впровадження ефективних політик, процедур і технологій, що мінімізуватимуть ризики порушення безпеки даних та забезпечать стійкість до кіберзагроз. Тільки через цей систематичний підхід організації можуть зберегти довіру клієнтів, захистити конфіденційні дані та забезпечити стійкість до кіберзагроз.

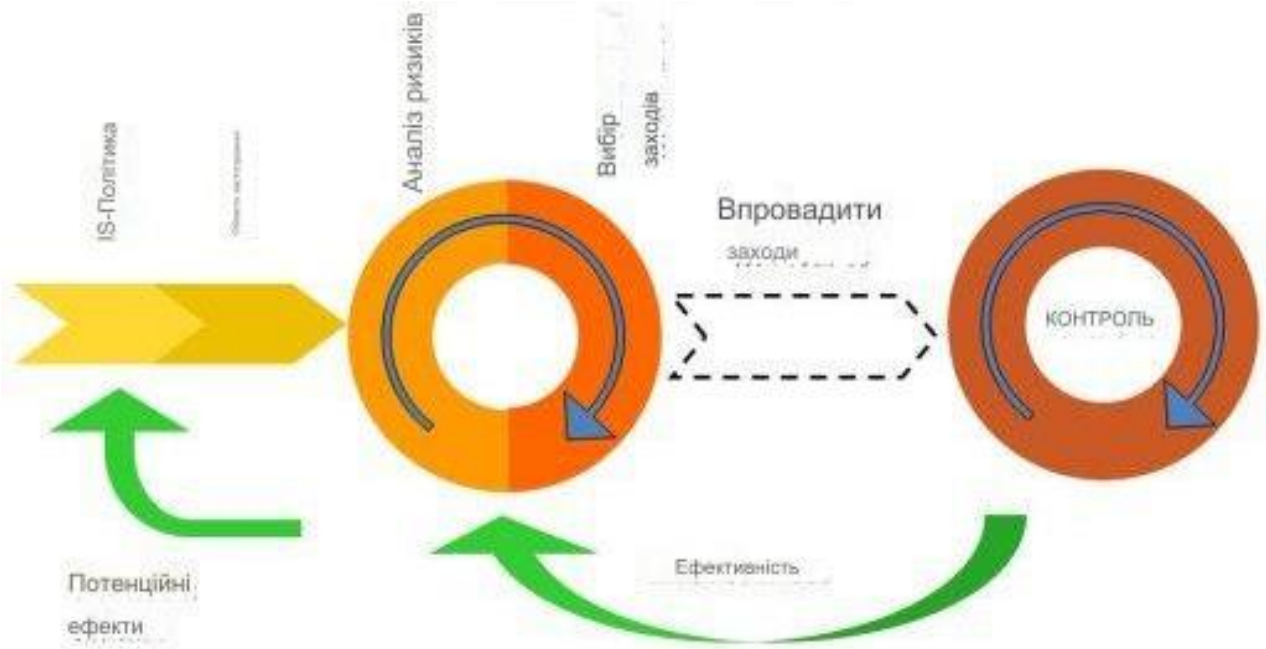


Рис. 1. Системи менеджменту інформаційної безпеки

В епоху зростаючої цифрової залежності, забезпечення безпеки інформації стає невід'ємною частиною успішної діяльності будь-якої організації. Менеджмент інформаційної безпеки вимагає комплексного підходу та систематичних стратегій для забезпечення конфіденційності, цілісності та доступності інформації. У цьому есе ми розглянемо ключові аспекти цієї проблеми, а також виклики, які виникають у контексті управління інформаційною безпекою.

Перш за все, ефективне управління інформаційною безпекою передбачає розробку чітких політик та процедур, які регулюють доступ до конфіденційної інформації. Це включає в себе створення правил доступу, обмеження привілеїв, шифрування даних та контроль над змінами в інформаційних системах. Без

належної політики безпеки ризик порушення конфіденційності та цілісності даних збільшується.

Другим важливим аспектом є навчання та підготовка персоналу. Люди часто є слабким ланцюгом у забезпеченні безпеки інформації через недбалість або несвідомість стосовно потенційних загроз. Тому важливо проводити регулярні навчання та тренінги з питань кібербезпеки, щоб персонал був усвідомлений загроз та знав, як правильно діяти в разі виявлення підозрілих ситуацій.

Однак, на шляху до ефективного управління інформаційною безпекою виникають виклики. Швидкі темпи розвитку технологій ускладнюють захист інформації, оскільки нові технології часто вносять нові потенційні загрози. Крім того, кіберзлочинці постійно змінюють свої підходи та тактики, щоб обійти захисні механізми, що ставить під загрозу безпеку інформації.

Узагальнюючи, менеджмент інформаційної безпеки є складним завданням, яке вимагає не лише технічних знань, але й стратегічного мислення та управлінських навичок. Забезпечення безпеки інформації вимагає постійного вдосконалення, гнучкості та готовності реагувати на зміни в загрозах та технологіях. Тільки через це організації можуть зберегти довіру клієнтів, захистити конфіденційні дані та забезпечити стійкість до кіберзагроз.

Однією з ключових аспектів менеджменту інформаційної безпеки є постійна оцінка та моніторинг існуючих заходів безпеки. Це включає в себе аудит безпеки, ідентифікацію потенційних уразливостей та аналіз інцидентів безпеки. Підтримка актуальності та ефективності заходів безпеки є важливою складовою успішного менеджменту інформаційної безпеки.

Крім того, розвиток інноваційних технологій, таких як штучний інтелект, blockchain та квантові обчислення, відкриває нові можливості для забезпечення інформаційної безпеки. Ці технології можуть використовуватися для виявлення загроз, автоматизації захисних заходів та підвищення надійності систем безпеки даних.

Нарешті, створення культури безпеки в організації є ключовим елементом успішного менеджменту інформаційної безпеки. Це включає в себе постійну освіту та навчання персоналу, підтримку свідомого ставлення до безпеки даних серед працівників на всіх рівнях та створення системи поощрення за внесок у підвищення безпеки інформації.

Перелік посилань:

1. Система менеджмент інформаційної безпеки URL : https://anitechconsulting.com.au/what-is-information-security-management-system-isms/
2. Чим займається менеджер по інформаційній безпеці URL : https://www.freelancermap.com/blog/career-insights-info-security-manager/
3. Управління інформаційної безпеки URL: https://www.atatus.com/glossary/information-security-management/

Жеребило Віталій Олександрович
студент групи УБДМ-51
ННІЗІ, ДУІКТ,Київ,Україна

Створення моделі культури кібербезпеки в організації

Створення моделі культури кібербезпеки в організації — це процес розробки та впровадження стратегій, політик, навчання та свідомого підходу до забезпечення безпеки в інформаційних технологіях серед персоналу. Вона включає у себе освіту, навчання, моніторинг та постійне оновлення політик та процедур, щоб забезпечити захист інформації від потенційних загроз.

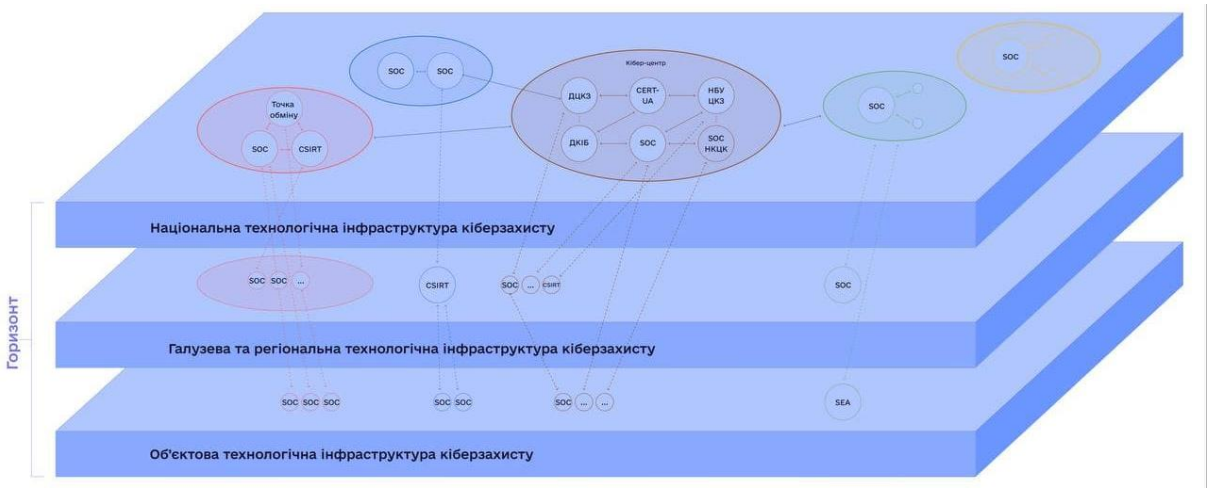


Рис. 1 - Технологічна інфраструктура кіберзахисту

Моделі культури кібербезпеки - це теоретичні та концептуальні рамки, які допомагають розуміти і практично впроваджувати підходи до забезпечення безпеки в інформаційних технологіях та цифровому середовищі. Основні моделі культури кібербезпеки включають

До основних принципів моделі культури кібербезпеки відноситься:

Модель *навчання та освіти*. Ця модель ставить акцент на навчанні співробітників та користувачів основам кібербезпеки, щоб вони могли розпізнавати загрози та вживати відповідні заходи захисту.

Модель *управління ризиками*. Ця модель спрямована на ідентифікацію, аналіз та управління ризиками в інформаційних системах та мережах для забезпечення їхньої надійності та стійкості.

Модель *внутрішньої безпеки*. Ця модель фокусується на внутрішніх загрозах, таких як необережне поводження персоналу, витоки інформації тощо, і включає в себе заходи контролю доступу та моніторингу діяльності користувачів.

Модель *захисту інформації*. Ця модель орієнтована на захист конфіденційної інформації шляхом застосування шифрування, аутентифікації, авторизації та інших технологічних заходів.

Модель *культури безпек*. Ця модель сприяє створенню безпечного інформаційного середовища шляхом формування свідомості про кібербезпеку серед персоналу, підтримки безпечної практики та створення позитивного ставлення до безпеки даних.

Ці моделі можуть використовуватись окремо або в поєднанні для покращення культури кібербезпеки в організаціях та суспільстві загалом.

Формується мережею взаємодіючих технічних підрозділів кіберзахисту (CSIRTів), засобів та сервісів (служб) кіберзахисту, інформаційних систем взаємодії та обміну інформацією про кіберінциденти, кібератаки та кіберзагрози, Операційних центрів кібербезпеки (Security Operations Centers) та інших організаційно-технічних об’єктів, що забезпечують реалізацію функцій та процесів кіберзахисту в межах політик (механізмів, процедур), визначених суб’єктами кіберзахисту. Наразі Держспецзв'язку розробляє типові вимоги до Операційних центрів кібербезпеки з урахуванням вимог, розроблених ENISA.

Зробимо висновки. Створення моделі культури кібербезпеки в організації є критичним для ефективного захисту від кіберзагроз та забезпечення безпеки даних і систем.

Перелік посилань:

1. Глобальна культура кібербезпеки в міжнародному дискурсі: цінності та принципи URL: https://journals.uran.ua/visnyknakkkim/article/view/175488 (дата звернення 11.04.2024)
2. Культура кібербезпеки: зведення основних правил та інструментів URL: https://ukeywaf.com/kultura-kiberbezpeky-zvedennya-osnovnyh-pravyl-ta-instrumentiv/ (дата звернення 11.04.2024)

3. Основи кібербезпеки та кібероборони URL: https://metod.suitt.edu.ua/download/686 (дата звернення 12.04.2024)

4. Культура кібербезпеки як складник цифрової компетентності URL: https://naurok.com.ua/kultura-kiberbezpeki-yak-skladnik-cifrovo-kompetentnosti-244767.html (дата звернення 12.04.2024)

5. Постановою Кабінету Міністрів України від 29 грудня 2021 р. № 1426 затверджено Положення про організаційно-технічну модель кіберзахисту. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=45109 (дата звернення 12.04.2024)

Івахненко Кирило Володимирович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

БЕЗПЕКА ХМАРНИХ ТЕХНОЛОГІЙ В КІБЕРБЕЗПЕЦІ

Стартапи розробляють хмарні платформи кібербезпеки, які дозволяють IT-командам керувати безпекою на хмарних платформах. Стартапи далі розвивають технології шифрування, такі як гомоморфне шифрування, які зменшують потребу в дешифруванні для обробки даних. Ці рішення значно покращують кібербезпеку хмарних сервісів.

Оскільки компанії продовжують перехід до повністю цифрового середовища, використання хмарних обчислень стає все більш популярним. Але хмарні обчислення пов’язані з проблемами кібербезпеки, тому розуміння важливості хмарної безпеки є важливим для забезпечення безпеки організації. [1]

З роками загрози безпеці стали неймовірно складними, і щороку з’являються нові вороги . У хмарі до всіх компонентів можна отримати віддалений доступ 24/7, тому відсутність належної стратегії безпеки ставить під загрозу зібрані дані відразу. Відповідно до звіту, кількість вторгнень у хмарне середовище зросла на 75% з 2022 по 2023 роки, причому кількість випадків, що свідомо користуються хмарою, зросла на 110% порівняно з минулим роком, а кількість випадків, пов’язаних із хмарою, зросла на 60% порівняно з минулим роком випадків. Крім того, звіт показав, що середній час прориву для інтерактивної активності вторгнення eCrime у 2023 році становив 62 хвилини, а один зловмисник зривався лише за 2 хвилини 7 секунд.

Одними з цих стартапів для захисту хмари є:

Lightspin пропонує хмарну безпеку на основі Graph

Lightspin — ізраїльський стартап, який забезпечує безпеку в хмарі на основі графіків. Багаторівнева платформа контекстної безпеки стартапу використовує аналіз шляху атаки та алгоритми теорії графів. Це допомагає візуалізувати, пріоритезувати та виправляти потенційні шляхи атак і прогалини в безпеці,

одночасно покращуючи видимість хмарних стеків. Це дозволяє групам безпеки виявляти ризики, які можна використовувати, і централізувати керування безпекою.

Cado Security допомагає Cloud Investigation

Cado Security – це британський стартап, який створює Cado Response, платформу для хмарних розслідувань. Він автоматизує збір і обробку даних для ефективного розслідування кіберінцидентів і реагування на них. Крім того, це дозволяє IT-командам покращити реагування на кіберризики в хмарних, контейнерних і безсерверних середовищах.

Хмарна безпека має бути невід'ємною частиною стратегії кібербезпеки організації незалежно від її розміру. [2]

Правильний захист хмарних технологій.

Хоча хмарні середовища можуть бути відкриті для вразливостей, існує багато передових методів захисту хмари, яких ви можете дотримуватися, щоб захистити хмару та запобігти зловмисникам від викрадення конфіденційних даних.

Деякі з найважливіших практик включають:

- Шифрування всіх даних в хмарі, щоб забезпечити безперебійний обмін додатками.
- Централізувати видимість приватних, гібридних і багатохмарних середовищ.
- Впроваджувати хмарні політики безпеки , які чітко визначають дозволи/обмеження для всієї організації.
- Забезпечити дотримання стандартів хмарної безпеки за допомогою рішення для керування безпекою в хмарі (CSPM).
- Захистити своє робоче навантаження та контейнери за допомогою хмарного рішення захисту робочого навантаження (CWP).
- Використовувати брандмауер веб-програм, щоб захистити свої хмарні програми.
- Використовувати можливості аналізу загроз, щоб передбачити майбутні загрози та ефективно визначити пріоритети, щоб запобігти їм.
- Розробити план реагування на інциденти в разі порушення, щоб виправити ситуацію, уникнути збоїв у роботі та відновити втрачені дані.
- Встановити нульову довіру , дозволяючи доступ лише тим користувачам, яким це дійсно потрібно, і лише до тих ресурсів, які їм потрібні. [1]

Зробимо висновки. Хмарні технології в сфері кібербезпеки представляють як безпечні переваги, так і ризики, які потребують уважного розгляду та управління. З одного боку, хмарні рішення можуть забезпечити значні переваги у вигляді масштабованості, доступності та ефективності в області захисту інформації. З іншого боку, існують потенційні загрози, пов'язані з конфіденційністю, цілісністю, доступністю та управлінням ризиками. Вирішення питань безпеки в хмарі вимагає поєднання технологічних засобів активного управління та стратегічного планування. Беручи це до уваги, хмарні технології можуть бути використані ефективно та безпечно для підтримки організацій з кібербезпеки.

Перелік посилань:

1. Що таке хмарна безпека? URL: https://www.crowdstrike.com/cybersecurity-101/cloud-security/ (дата звернення: 09.04.2024)
2. 10 найкращих тенденцій та інновацій у сфері кібербезпеки у 2023 році URL: https://www.startus-insights.com/innovators-guide/cybersecurity-trends-innovation/ (дата звернення: 09.04.2024)

Качний Ілля Сергійович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ПОБУДОВА SECURITY OPERATIONS CENTER

Операційний центр безпеки (SOC) є ефективним інструментом для моніторингу інформаційної безпеки організвції та кіберзагроз. Створення такого центру, однак, вимагає інвестицій часу, зусиль і ресурсів.

Найчастіше перед SOC стоїть завдання моніторингу безпеки. Це передбачає централізований збір і аналіз логів відповідних додатків і пристроїв у мережі з метою виявлення будь-яких аномалій, які могли виникнути. Зібрані дані логів можуть стосуватися широкого спектру додатків і пристроїв - від систем виявлення вторгнень (IDS), брандмауерів, веб-додатків, серверів Active Directory і антивірусного програмного забезпечення до промислових систем управління. Сюди можна віднести будь-яку систему, здатну надавати інформацію, необхідну для отримання уявлення про безпеку або стан мережі та підключених до неї систем. При визначенні того, який тип інформації збирати, з яких систем збирати інформацію та який метод кореляції використовувати, ключовим моментом є зосередження на інформації, що має відношення до організації, а не на тій, що вважається загальноприйнятою для збору.

Система управління інформацією та подіями безпеки (SIEM) - це

інструмент, який є невід'ємною частиною SOC. SIEM-системи - це програмне забезпечення, яке здатне інтерпретувати дані логів з різних джерел і співвідносити їх з кібератаками та іншими інцидентами безпеки, що відбуваються в мережі. Окрім інформації про системи та мережу, SOC також використовує так звану threat intelligence - інформацію із зовнішніх джерел про вразливості та інформацію про загрози у сфері кібербезпеки. Ця інформація може бути використана для оцінки подій, які стосуються системи та мережі.

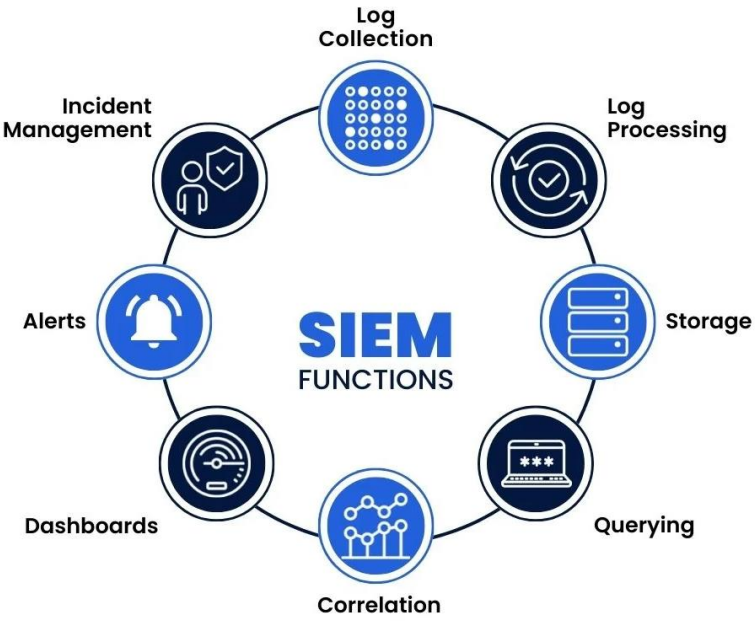


Рис.1. Функціональні можливості SIEM

Створення повноцінного SOC з нуля є серйозним викликом. Найпростіший підхід полягає в тому, щоб почати з малого, а потім повільно і контрольовано розвивати його до створення повноцінного SOC. Щоб досягти цього, слід почати з того, що команда спеціалістів повинна відстежувати дані логів певної кількості ключових компонентів інфраструктури або проміжного програмного забезпечення, таких як брандмауер, веб-сервер або антивірусне програмне забезпечення. Необхідно зосередитися на сповіщеннях, що вказують на конкретну проблему, або на індикаторах потенційних майбутніх проблем та повідомляти про будь-які знахідки в службу технічної підртимки.

Для того, щоб забезпечити належний моніторинг інформаційної безпеки, організаціям потрібно робити більше, ніж просто перевіряти файли журналів антивірусної програми, брандмауера або подібних засобів. Організація повинна здійснити низку заходів:

- Створення політики інформаційної безпеки. Політика інформаційної безпеки описує цілі інформаційної безпеки та спосіб управління інформацією в організації (хто за що відповідає). Цілі,

викладені в політиці інформаційної безпеки, можуть допомогти визначити сфери, на яких буде зосереджена діяльність SOC

- Аналіз середовища застосування програм. Огляд ландшафту програм дає уявлення про інформацію, якою володіє організація, і про те, як ця інформація обробляється. Такий огляд є ключовим для адекватного та ефективного моніторингу. Ця інформація також є важливою для аналізу ризиків.
- Результати останнього аналізу ризиків. Аналіз ризиків допомагає виявити можливі проблеми, пов'язані з порушенням доступності, цілісності або конфіденційності певної інформації. Крім того, аналіз ризиків також допомагає визначити, які загрози становлять неприйнятний ризик для обробки інформації. Ця інформація допомагає визначити пріоритетні напрямки для SOC.

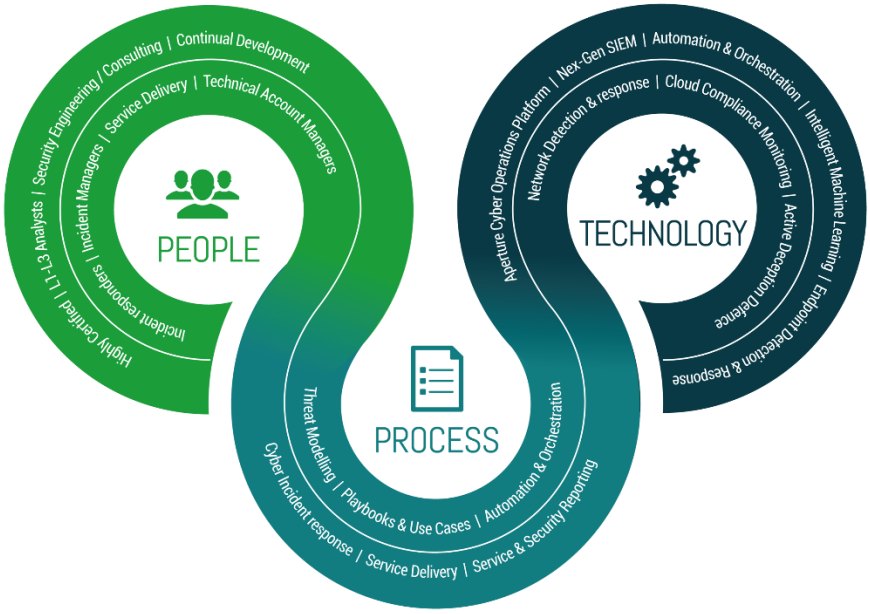


Рис.2. Складові частити SOC

Один з ризиків занадто швидкого зростання SOC полягає в тому, що обсяг зібраної інформації перевищує здатність SOC обробляти її. Крім того, відділ технічної підтримки повинен бути готовим до кількості повідомлень, яку йому надсилатиме SOC. Слід обмежити обсяг даних, які будуть збиратися, виходячи з пропускної спроможності SOC та технічної підтримки.

Розширення SOC, швидше за все, призведе до збільшення кількості аспектів, які потребують моніторингу. Інакше кажучи, збільшиться кількість правил кореляції, які використовуються для визначення того, чи відбулася небажана подія або порушення. Більша кількість правил означає збільшення

витрат на підтримку цих правил, оскільки кожна зміна, внесена в систему або мережу, може вимагати внесення змін до одного або декількох правил.

Перелік посилань:

1. How to Create a Next-Generation SOC. URL: https://www.paloaltonetworks.com/cybersecurity-perspectives/how-to-create-a-next-generation-soc (дата звернення: 9.04.2024).
2. Build an SOC. URL: https://english.ncsc.nl/get-to-work/build-an-soc (дата звернення: 09.04.2024).

Марченко Віталій Вікторович
д.ф.,доцент кафедри ІКБ, ННІЗІ ДУІКТ, Київ, Україна
Коліда Володимир Петрович
аспірант групи АІКБ-11, кафедри ІКБ, ННІЗІ ДУІКТ, Київ, Україна

Підвищення ефективності роботи SIEM системи

У світі інформаційних технологій, де цифрові дані стають все більш цінними, забезпечення безпеки інформації є пріоритетом для будь-якої компанії чи організації. SIEM (Security Information and Event Management) відіграє ключову роль у сучасній кібербезпеці і є невід'ємною частиною стратегії інформаційної безпеки для боротьби з загрозами та захистом від кіберінцидентів. Управління інформацією про безпеку та подіями (SIEM) — це область у сфері комп’ютерної безпеки, де програмні продукти та послуги поєднують керування інформацією про безпеку (SIM) і керування подіями безпеки (SEM).[1]

Одним із ключових завдань SIEM є виявлення та запобігання інцидентів безпеки. SIEM агрегує дані про події, створені рішеннями для моніторингу, оцінки, виявлення та реагування, розгорнутими в середовищі додатків, мереж, кінцевих точок і хмар. Можливості включають виявлення загроз за допомогою кореляції та аналітики поведінки користувачів і об’єктів (UEBA), а також інтеграцію реагування, якою зазвичай керують через координацію безпеки, автоматизацію та реагування (SOAR). Звіти про безпеку та постійно оновлюваний вміст загроз за допомогою функціональності платформи аналізу загроз (TIP) також є поширеними інтеграціями. Хоча SIEM в основному розгортається як хмарна служба, вона може підтримувати локальне розгортання.[2] За допомогою алгоритмів машинного навчання і аналітики даних SIEM може аналізувати великі обсяги інформації в реальному часі та виявляти аномальну поведінку, що вказує на можливі загрози. Наприклад, SIEM може автоматично виявляти підозрілі спроби входу в систему, незвичні мережеві запити або аномальний трафік, що дозволяє оперативно реагувати на потенційні атаки. Окрім того, SIEM допомагає у розслідуванні інцидентів безпеки. Вона зберігає та аналізує дані про події протягом тривалого часу, що дозволяє фахівцям проводити детальне розслідування інцидентів, виявляти їх

причини та наслідки, а також розробляти заходи щодо запобігання подібним інцидентам у майбутньому.

Для досягнення ефективного захисту система SIEM повинна мати ряд важливих характеристик. В першу чергу, це розширена інтеграція аналізу загроз, що означає, що платформа SIEM повинна мати інтеграцію зі всіма каналами аналізу загроз. Це гарантує, що організація має доступ до останньої інформації про нові загрози, дозволяючи завчасно оновлювати свої заходи безпеки. Співпраця між системами SIEM і джерелами аналізу загроз покращує загальний стан кібербезпеки, роблячи її більш стійкою проти нових загроз.

Більш глибока інтеграція штучного інтелекту (ШІ) та машинного навчання (ML) у рішення SIEM підвищує здатність виявляти складні кіберзагрози та реагувати на них шляхом вивчення шаблонів історичних даних і автоматизації аналізу загроз. Результатом є більш точне виявлення загроз і скорочення часу реагування, що дозволяє командам із кібербезпеки бути на крок попереду зловмисників.

Аналітика поведінки користувачів і суб’єктів (UEBA) має першочергове значення для визначення потенційних ризиків безпеці. Системи SIEM повинні розширювати свої можливості в аналізі поведінки користувачів і суб’єктів (UEBA). Використовуючи розширену аналітику, рішення SIEM зможуть виявляти аномальну поведінку та потенційні внутрішні загрози, забезпечуючи організаціям проактивний підхід до безпеки.

Також із зростанням поширення хмарних служб рішення SIEM розвиваються, щоб стати більш інтегрованими в хмару. SIEM повинні бути масштабовані, гнучкі і мати можливість бездоганної інтеграції з різними хмарними середовищами. Це дозволяє організаціям ефективно керувати безпекою в локальних і хмарних інфраструктурах, забезпечуючи комплексний захист від кіберзагроз.

Модель безпеки Zero Trust набуває все більшої популярності, підкреслюючи принцип «ніколи не довіряй, завжди перевіряй». Системи SIEM повинні узгоджуватися з цією структурою шляхом постійного моніторингу та автентифікації дій користувачів і пристроїв, незалежно від їх місцезнаходження чи мережі. Ця тенденція гарантує, що кожна сутність у мережі піддається постійному контролю, зменшуючи ризик несанкціонованого доступу та горизонтального переміщення зловмисників.

Також рішення SIEM повинні включати більше можливостей автоматизованого реагування на інциденти. Автоматизовані плейбуки та механізми реагування не тільки прискорюють процес реагування на інциденти, але й зменшують навантаження на команди з кібербезпеки. Ця тенденція

дозволяє організаціям швидко пом’якшувати загрози та мінімізувати вплив інцидентів безпеки.

Крім того, варто зазначити, що система SIEM є не лише інструментом для виявлення та запобігання інцидентів безпеки, але й цінним джерелом для аналізу та вдосконалення стратегій кібербезпеки в майбутньому. Вона повинна забезпечувати можливість аналізу великого обсягу даних, що дозволяє організаціям зрозуміти сучасні тренди в кіберзагрозах і адаптувати свої заходи безпеки відповідно до мінливих умов. Таким чином, SIEM виконує важливу роль у підвищенні загального рівня кібербезпеки та забезпеченні стійкості організацій проти потенційних загроз.

Отож, щоб забезпечити найвищий рівень захисту, система SIEM повинна мати перелічені характеристики, що допоможе організаціям забезпечити високий рівень безпеки та зменшити ризик виникнення кібератак.

Перелік посилань:

1. What is SIEM" | IBM URL: https://www.ibm.com/topics/siem
2. What is Security Information and Event Management (SIEM) | Gartner URL: https://www.gartner.com/reviews/market/security-information-event-management

Коровайченко Юрій Юрійович
аспірант групи АІКБ-11, ННІЗІ ДУІКТ, Київ, Україна

РОЗВИТОК NDR У ВІДПОВІДЬ НА ЕВОЛЮЦІЮ КІБЕРЗАГРОЗ: АДАПТИВНІ СТРАТЕГІЇ ТА ТЕХНОЛОГІЇ

У сучасному світі кібербезпеки, Network Detection and Response (NDR) відіграє ключову роль у захисті інформаційних систем від загроз що постійно еволюціонують. NDR – це підхід, що зосереджений на пошуку, розслідуванні та реагуванні на підозрілу активність у мережі, що дозволяє організаціям швидко виявляти та реагувати на потенційні кібератаки в мережі.

З розвитком технологій захисту - кіберзагрози стають все більш складними та витонченими, вимагаючи від систем безпеки невпинного розвитку та адаптації. Еволюція кіберзагроз свідчить про постійне вдосконалення методів атаки, включаючи використання Advanced Persistent Threat (APT), шкідливого програмного забезпечення, фішингу, інсайдерських загроз та інших тактик.

Мета цієї роботи - дослідити, як системи NDR адаптувались до постійних змін у ландшафті кіберзагроз, використовуючи адаптивні стратегії та передові технології виявлення загроз для підтримки безпеки в динамічному цифровому середовищі, та перспективи їх розвитку.

Від NBAD до NDR: еволюція у відповідь на кіберзагрози

Системи Network Behavior Anomaly Detection (NBAD) стали фундаментом для розвитку Network Detection and Response (NDR), і це відображає еволюцію в стратегіях боротьби з кіберзагрозами. NBAD, спочатку зосереджений на виявленні аномалій в мережеві, став одним з першоджерел NDR, що розширив функціонал до активного реагування на ідентифіковані загрози.

Зі збільшенням складності кіберзагроз, NDR виник як відповідь на необхідність не тільки виявляти аномалії, але й швидко реагувати на них. Це розвиток був природним кроком від простого спостереження до активного втручання, дозволяючи організаціям не тільки ідентифікувати потенційні інциденти безпеки, але й ефективно нейтралізувати загрози.

Така еволюція NBAD до NDR забезпечила більш широкий функціонал рішень цих класів, дозволяючи комплексно аналізувати та реагувати на кіберзагрози.

Адаптивні стратегії NDR

NDR постійно адаптується до еволюції кіберзагроз, інтегруючи передові технології та розробляючи адаптивні стратегії. Використання автоматизованого аналізу мережевого трафіку, машинного навчання для прогнозування та виявлення складних атак, а також автоматичне реагування на інциденти безпеки, стали стандартними практиками. NDR забезпечує гнучкість у виявленні та реагуванні на новітні загрози, швидко адаптуючись до динаміки кіберландшафту.

Також, NDR використовує глибокий аналіз поведінки та передбачення для ідентифікації потенційних загроз ще до їх реалізації, покращуючи таким чином превентивні заходи безпеки. Ця адаптація не лише підвищує загальну ефективність систем безпеки, але й забезпечує більш широке розуміння мережевого середовища, допомагаючи у прийнятті обґрунтованих рішень щодо захисту інформаційних активів.

Технологічні інновації у NDR: AI та ML

Сучасні системи кібербезпеки інтенсивно впроваджують та використовують штучний інтелект (AI) та машинне навчання (ML) для підвищення своєї ефективності. Системи NDR не стали виключенням. AI та ML проводять революцію у способах виявлення та реагування на кіберзагрози, забезпечуючи автоматизацію складних процесів аналізу даних.

- **Штучний інтелект** сприяє розширенню можливостей NDR, надаючи системам здатність самостійного навчання та вдосконалення через взаємодію з мережевими даними. AI дозволяє системам NDR прогнозувати та ідентифікувати потенційні загрози, аналізуючи поведінкові патерни та використовуючи історичні дані для виявлення аномалій.
- **Машинне навчання** вносить вклад у покращення здатності NDR до автоматичного виявлення та класифікації загроз. Алгоритми ML обробляють великі масиви даних для виявлення зв'язків і тенденцій, які можуть бути неочевидними для людського аналізу. Це дозволяє системам NDR швидше і точніше виявляти атаки, зокрема, ті, які використовують новітні або складні методи.

Використання AI та ML в NDR значно покращує здатність систем виявляти та реагувати на кіберзагрози, роблячи процес більш швидким, точним та ефективним. Ці технології також допомагають зменшити кількість помилкових спрацьовувань, що дозволяє командам безпеки зосередитись на справжніх загрозах.

Виклики та перспективи NDR

Системи NDR мають подолати виклики, пов'язані з обробкою великих обсягів даних та їх аналізом в реальному часі, щоб ефективно виявляти складні кіберзагрози. Інтеграція з розширеними аналітичними інструментами та автоматизацією процесів допоможе збільшити швидкість та точність відповідей на інциденти. Технічні перспективи NDR включають вдосконалення алгоритмів машинного навчання для зниження кількості помилкових спрацьовувань і підвищення ефективності виявлення загроз. Крім того, розвиток квантових обчислень та штучного інтелекту може надати нові можливості для посилення систем NDR, зокрема, у виявленні та нейтралізації атак в автоматизованому режимі.

Завершуючи аналіз ролі та еволюції NDR у відповідь на кіберзагрози, можна підкреслити, що технічні інновації, зокрема в галузі штучного інтелекту та машинного навчання, значно посилили функціонал NDR систем. Ці технології не тільки покращили швидкість та точність виявлення загроз, але й сприяли розвитку адаптивних механізмів, які можуть ефективно протидіяти новітнім кібератакам що постійно еволюціонують. Технічна інтеграція з іншими інструментами безпеки та посилення автоматизації і аналітики даних дозволять NDR системам забезпечувати більш комплексний та ефективний захист в корпоративних інформаційних системах.

Перелік посилань:

1. Gartner - Network Behavior Analysis: Moving Beyond Signatures (02 March 2009)
2. Gartner - Market Guide for Network Detection and Response (14 December 2022)
3. Security Intelligence - What is Network Detection and Response and Why is it So Important? - URL: https://securityintelligence.com/posts/network-detection-and-response-network-security/
4. PaloAlto - What Is Network Detection and Response – URL: https://www.paloaltonetworks.com/cyberpedia/what-is-network-detection-and-response
5. Progress Flowmon - Resilient Cybersecurity with Network Detection and Response - URL: https://www.flowmon.com/en/resources/ebooks/resilient-cybersecurity-with-network-detection-and-response
6. ExtraHop - RevealX™ and the MITRE ATT&CK® Framework – URL: https://hop.extrahop.com/resources/papers/revealx-mitre-framework/

Корчук Дмитрій Вікторович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

SOC системи. Варіант чи необхідність?

Що таке SOC?

SOC (Операційний центр безпеки) - це фізичний або віртуальний об'єкт, призначений для захисту організації від кіберзагроз. Більшість SOC укомплектовані фахівцями з безпеки та аналітиками, які тісно співпрацюють з іншими технічними експертами в галузі IT-операцій та розробки.

Як працює SOC?

Команда SOC встановлює правила та здійснює постійний моніторинг мереж, серверів, пристроїв, операційних систем, додатків і баз даних на наявність ознак аномалій і винятків у системі безпеки або нових вразливостей. Дані про загрози збираються з брандмауерів, систем виявлення та запобігання вторгненням, а також систем управління інформацією та подіями безпеки (SIEM).

При виявленні підозрілої активності або порушень ці системи надсилають сповіщення команді SOC, яка розслідує та реагує на них у міру їх виникнення.

Команди SOC зазвичай працюють позмінно в режимі 24/7, щоб гарантувати швидке реагування на будь-які інциденти або загрози, що виникають.

Чому так важливо створити та впровадити SOC?

Окрім загальної підвищеної вразливості до кібератак та їхніх наслідків, відсутність ефективного робочого процесу Центру управління безпекою може

зробити майже неможливим зменшення ризиків та ефективне впровадження рішень.

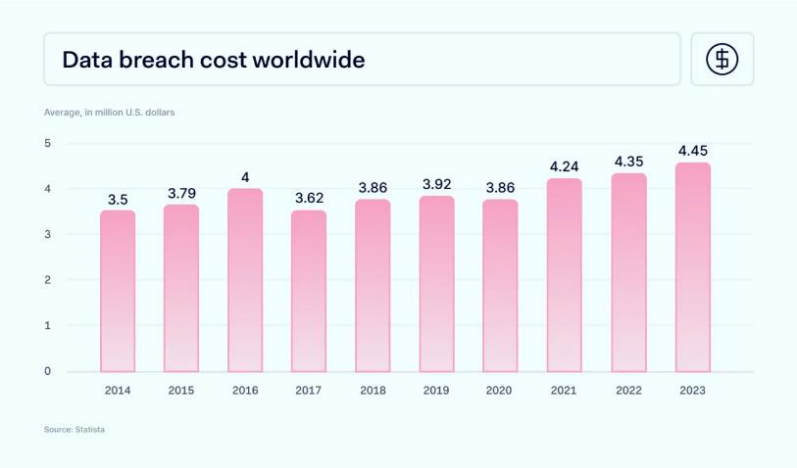


Рис. 1. Середня вартість витоку даних за 2014-2023 роки

Чи є створення власної SOC єдиним життєздатним способом для компаній створити можливості моніторингу безпеки?

Створення SOC - або взагалі створення певної форми внутрішньої системи моніторингу безпеки - це дорогий і трудомісткий процес, який вимагає постійної уваги для того, щоб бути ефективним. Велика кількість організацій вирішують не створювати SOC. Замість цього вони обирають інші варіанти моніторингу безпеки, такі як залучення керованого постачальника послуг безпеки Managed Security Service Providers (MSSP).

IT-директори та технологічні лідери, які планують створити власну SOC, повинні чітко усвідомлювати витрати та кадрові наслідки, пов'язані з таким підходом. Існує безліч альтернатив побудові та укомплектуванню штату власної SOC, і компаніям слід вивчити їх на додаток до різних типів моделей SOC.

Переваги операційного центру безпеки (SOC)

Захист активів: Проактивний моніторинг та можливості швидкого реагування SOC допомагають запобігти несанкціонованому доступу та мінімізувати ризик витоку даних. Це захистить критичні системи, конфіденційні дані та інтелектуальну власність від порушень безпеки та крадіжок.

Безперервність бізнесу: Зменшуючи кількість інцидентів безпеки та мінімізуючи їх вплив, SOC забезпечують безперервність бізнес-операцій. Це допомагає підтримувати продуктивність, потоки доходів і задоволеність клієнтів.

Відповідність нормативним вимогам: SOC допомагають організаціям

відповідати нормативним вимогам і галузевим стандартам кібербезпеки, впроваджуючи ефективні заходи безпеки та ведучи детальний облік інцидентів і реагування на них.

Економія витрат: Інвестиції в проактивні заходи безпеки через SOC можуть призвести до значної економії коштів за рахунок запобігання витоку даних і кібератак. Початкові інвестиції часто набагато менші, ніж фінансові збитки та ризики для репутації, спричинені кіберінцидентом, а в разі аутсорсингу вони замінюють необхідність утримувати фахівців з безпеки в штаті компанії.

Покращене реагування на інциденти: Можливості швидкого реагування SOC зменшують час простою та фінансові втрати, стримуючи загрози та швидко відновлюючи нормальну роботу, щоб мінімізувати збої в роботі.

Покращене управління ризиками: Аналізуючи події та тенденції у сфері безпеки, команди SOC можуть виявити потенційні вразливості організації. Потім вони можуть вжити проактивних заходів для їх усунення до того, як вони будуть використані.

Проактивне виявлення загроз: Завдяки постійному моніторингу мереж і систем, SOC можуть швидше виявляти та зменшувати загрози безпеці. Це мінімізує потенційні збитки та витоки даних, а також допомагає організаціям випереджати мінливий ландшафт загроз.

Перелік посилань:

1. What is a security operations center (SOC)? URL: https://www.ibm.com/topics/security-operations-center
2. Breakdown of the 12 most significant 2023 data breaches URL: https://nordlayer.com/blog/data-breaches-in2023/?gad_source=1&gclid=Cj0KCQjwztOwBhD7ARIsAPDKnkAl9IWkYCcLpfgGPohxXuJZCG6Mn8i0-qSqqm42fQR_QABA5jGSfoUaAqqoEALw_wcB
3. The Top 24 Security Predictions for 2024 (Part 2) URL: https://www.linkedin.com/pulse/top-24-security-predictions-2024-part-2-dan-lohrmann-ivqxe/
4. How to Build and Operate a Modern Security Operations Center URL: https://www.gartner.com/en/documents/4002259

Краєвський Владислав Юрійович
студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

ВИКЛИК СУЧАСНИМ ЗАГРОЗАМ

У епоху цифрової трансформації кібербезпека виросла у критичну проблему для організацій по всьому світу. Швидкий розвиток технологій не лише змінив підходи до ведення бізнесу, але й вніс нові вразливості, які можуть використовувати кіберзлочинці. Ця теза досліджує виклики, які сучасні загрози ставлять перед кібербезпекою, зосереджуючись на змінному пейзажі кіберзагроз і стратегіях

їх ефективного подолання.

Сучасні загрози кібербезпеці включають в себе широкий спектр високотехнологічних атак, таких як шифрувальники, фішинг, віруси та кібератаки з боку держав. Ці загрози характеризуються своєю зростаючою складністю, масштабом та впливом, що робить їх великим викликом для організацій. Зростання кількості пристроїв "Інтернет речей" (IoT), поширення хмарних технологій та збільшення залежності від цифрових платформ подальшим чином підвищили вразливість кібербезпеки (Рис. 1)

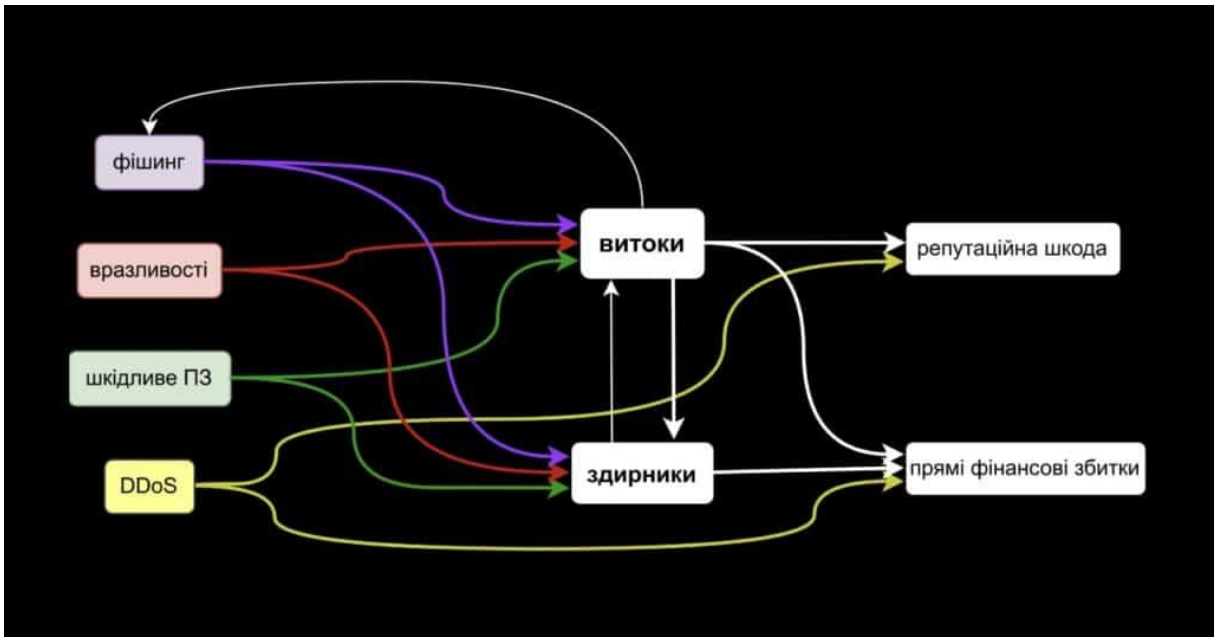


Рис.1. Основні типи атак, їх взаємодія та збитки від них.

Основні виклики, які ставлять перед сучасними загрозами кібербезпеці:

Збільшена складність атак: Кіберзлочинці використовують передові техніки, такі як машинне навчання та штучний інтелект, для створення більш складних та важкорозпізнаваних атак, що вимагає розвитку більш продвинутих механізмів виявлення та запобігання.

Масштаб та вплив атак: Масштаб та наслідки кібератак значно зросли, організації стикаються з потенційно великими витоками даних, фінансовими втратами та пошкодженням репутації. Це підкреслює потребу в надійних стратегіях кібербезпеки.

Змінний пейзаж загроз: Пейзаж кіберзагроз постійно змінюється, з'являються нові типи атак. Організаціям необхідно залишатися на крок попереду, постійно оновлюючи свої заходи кібербезпеки та впроваджуючи нові технології та практики.

Внутрішні загрози: Зростання використання дистанційної роботи та збільшення залежності від цифрових платформ призвело до зростання

внутрішніх загроз. Працівники, контрактники та сторонні постачальники, які мають доступ до конфіденційної інформації та систем, становлять значущий ризик.

Для подолання цих викликів організаціям необхідно вжити комплексного підходу до кібербезпеки:

Оцінка та управління ризиками: Регулярна оцінка та управління кіберризиками є важливими. Це включає виявлення потенційних вразливостей, оцінку впливу потенційних загроз та впровадження заходів для зниження цих ризиків.

Використання передових технологій безпеки: Організаціям необхідно використовувати передові технології безпеки, такі як штучний інтелект, машинне навчання та блокчейн, для виявлення та запобігання кіберзагрозам.

Постійна освіта та навчання: Працівників та інших учасників треба навчати найкращим практикам кібербезпеки, щоб зменшити ризик людських помилок та внутрішніх загроз.

Планування реагування на інциденти: У організацій повинен бути надійний план реагування на інциденти, щоб швидко виявляти, ізолювати та знижувати кіберзагрози.

Висновок: виклик сучасних загроз кібербезпеці є складною та змінною проблемою, яка вимагає комплексного підходу. За допомогою комплексної стратегії кібербезпеки, яка включає оцінку ризиків, передові технології безпеки, постійну освіту та ефективне планування реагування на інциденти, організації можуть краще захищати себе від непередбачуваного пейзажу кіберзагроз.

Перелік посилань:

U
(дата звернення 16.04.2024)
(дата звернення 16.04.2024)
5. Кібератаки 2022-2023: огляд найбільших інцидентів, та що нас чекає у 2024 році URL:
.
P
E
R
L
I
N
K

Клименко Ярослав Валерійович
студент групи БСД-43, ННІЗІ ДУІКТ, Київ, Україна

Аналіз використання Symantec DLP в контексті існуючих проблем

"
h
t
t
p
s
:

Сучасні організації стикаються з різноманітними загрозами безпеки даних, такими як витік

конфіденційної інформації, крадіжка даних та інші. Для забезпечення захисту даних використовуються різні технології, серед яких Symantec Data Loss Prevention (DLP) від Symantec Corporation відіграє ключову роль. У цьому рефераті ми розглянемо аналіз використання Symantec DLP в контексті існуючих проблем.

Проблеми безпеки даних:

- *Витік конфіденційної інформації*: З впровадженням хмарних технологій, мобільних пристроїв та роботи на відстані збільшується ризик витоку конфіденційних даних через несанкціонований доступ або недбалість користувачів;
- *Крадіжка даних*: Кіберзлочинці шукають способи для отримання доступу до цінної інформації організацій, такої як клієнтські дані, фінансова інформація тощо, щоб використовувати її у своїх цілях;
- *Корпоративні внутрішні загрози*: Іноді загрози для безпеки даних виникають зсередини самої організації, коли співробітники або інші внутрішні сторони намагаються недозволено отримати, змінити або пошкодити інформацію.

Роль Symantec DLP у вирішенні цих проблем:

1. *Виявлення та захист конфіденційної інформації*: Symantec DLP надає засоби для виявлення та моніторингу конфіденційних даних в різних джерелах, таких як файли, електронна пошта, веб-сайти тощо. Це допомагає уникнути витоку конфіденційної інформації;
2. *Запобігання крадіжки даних*: Широкі можливості налаштування політик безпеки дозволяють організаціям контролювати доступ до конфіденційної інформації та вчасно реагувати на спроби несанкціонованого доступу;
3. *Виявлення внутрішніх загроз*: Symantec DLP аналізує поведінку користувачів і виявляє незвичайні або підозрілі активності, що може вказувати на внутрішню загрозу безпеці даних.

Symantec DLP відіграє важливу роль у вирішенні проблем безпеки даних, забезпечуючи ефективний контроль за конфіденційною інформацією,

виявлення та запобігання витокам даних та внутрішнім загрозам. Проте важливо розуміти, що сама по собі Symantec DLP не є універсальним рішенням, і для досягнення повної безпеки даних потрібно комбінувати його з іншими технологіями та стратегіями безпеки.

Перелік посилань:

1. Symantec IT Analytics Solution for DLP. [Електронний ресурс] – режим доступу: https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/symantec-it-analytics-solution-for-dlp/2-9-1.html
2. Запобігання витокам інформації. [Електронний ресурс] – режим доступу: https://quadrosoft.by/images/pdf/baza_znanij/Symantec%20DLP%2012.0.pdf

Лазарєв Єгор Геннадійович
студент групи БСД-21, ННІЗІ, ДУІКТ, Київ, Україна

Важливість здійснення регулярних аудитів кібербезпеки для захисту організаційних даних

У сучасному цифровому світі, де кіберзлочинці стають все більш витонченими, захист даних організації є ключовим викликом для організацій будь-якого розміру. Одним із важливих інструментів забезпечення безпеки та виявлення слабких місць у захисті цифрових активів є проведення регулярних аудитів кібербезпеки.

Регулярний аудит кібербезпеки дозволяє організаціям систематично оцінювати стан своєї інформаційної безпеки та виявляти потенційні ризики і загрози. Однак аудит кібербезпеки не обмежується виявленням помилок і проблем. Він також може бути спрямований на пошук нових можливостей для підвищення безпеки та ефективності систем.

Під час аудиту експерти виявляють можливі слабкі місця в існуючих засобах захисту, оцінюють відповідність стандартам і рекомендаціям безпеки та розробляють плани вдосконалення. Крім того, аудитори можуть виявити нові технології та методи захисту, які можуть бути використані для запобігання майбутнім загрозам. Таким чином, аудит кібербезпеки може стати джерелом інновацій та новаторських рішень для покращення стану безпеки організації.

Регулярне проведення аудиту кібербезпеки має кілька важливих переваг. По-перше, організації можуть своєчасно виявляти та усувати вразливості до того, як ними скористаються зловмисники. По-друге, аудити допомагають підвищити рівень обізнаності та відповідальності працівників у сфері

кібербезпеки. Нарешті, аудит може допомогти оцінити ефективність існуючих заходів безпеки та впровадити нові стратегії для забезпечення високого рівня захисту.

Висновок

Регулярні аудити кібербезпеки є невід'ємною частиною ефективної стратегії захисту інформаційних активів організації. Аудити допомагають виявити та усунути потенційні ризики, а також забезпечити безпеку та надійність інформаційних систем. Регулярні аудити сприяють підвищенню обізнаності та навчанню персоналу з питань кібербезпеки, що має вирішальне значення для запобігання кібератакам та забезпечення стійкості інформаційної інфраструктури організації.

Перелік посилань:

1. Blue Light LLC «What is Cybersecurity?» URL: https://bluelightllc.com/what-is-cybersecurity/ (дата звернення 21.04.2024)
2. NIST Cybersecurity Framework 2.0 URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення 21.04.2024)

Лелюх Вадим Олександрович
Студент групи БСДМ-51 ННІЗІ ДУІКТ, Київ, Україна

ВРАЗЛИВІСТЬ SNMP ПРОТОКОЛУ ТА МЕТОДИ ДЛЯ ЙОГО ЗАХИСТУ

Актуальність: У сучасному світі, де мережеві технології відіграють ключову роль у практично будь-якій сфері, ефективне управління мережею стає важливим елементом для досягнення успіху. Протокол SNMP (Simple Network Management Protocol) виступає як важливий інструмент у цьому процесі, надаючи засоби моніторингу, керування та діагностики мережевих пристроїв. Ця теза спрямована на дослідження ролі та значення SNMP у сучасних мережевих середовищах, включаючи його архітектуру, принципи роботи, переваги та виклики.

Мета: Ця теза має на меті дослідити вразливості протоколу SNMP (Simple Network Management Protocol), зокрема ідентифікувати потенційні небезпеки та загрози, які виникають внаслідок цих вразливостей. Дослідження буде спрямоване на розкриття можливих наслідків вразливостей SNMP для мережевої безпеки, а також розглядатиме можливі стратегії та заходи захисту для зменшення ризиків та підвищення стійкості мережевого середовища. Ця теза має на меті поглиблене розуміння вразливостей SNMP та розробку

рекомендацій з мережевої безпеки для мінімізації потенційних загроз.

Перш за все, детально розглянемо, що таке SNMP і як він працює. SNMP є простим протоколом управління мережею, розробленим для моніторингу та керування мережевими пристроями, такими як маршрутизатори, комутатори, сервери тощо. Його основна мета полягає в забезпеченні стандартизованого механізму для взаємодії між управляючими станціями та агентами, що працюють на мережевих пристроях. У мережевому середовищі, агенти SNMP відповідають за збирання та надсилання інформації про стан пристроїв, таку як статуси, конфігурації та події. Управляючі станції, з свого боку, ініціюють запити до агентів та отримують відповіді, а також можуть виконувати дії керування на мережевих пристроях через SNMP.

Цей протокол базується на простому зразку взаємодії клієнт-сервер, де управляюча станція виступає як клієнт, який взаємодіє з сервером, що представляє агента на мережевому пристрої. Запити та відповіді обмінюються за допомогою стандартних PDU (Protocol Data Unit), таких як GET, SET та TRAP, що дозволяє взаємодіяти з різними аспектами мережевих пристроїв. Однак, разом зі своїми перевагами, SNMP також має вразливості, які можуть стати об'єктом атак з боку зловмисників.

На мою думку є декілька ризиків, які є наявні в SNMP протоколі, а саме:

- атака типу Man-in-the-Middle є серйозною вразливістю SNMP, особливо при використанні протоколу без відповідного захисту. В такому випадку, зловмисники можуть втручатися у комунікацію між управляючими станціями та агентами SNMP, перехоплюючи та змінюючи дані, які передаються між ними. Це може призвести до некоректного керування мережею, включаючи неправильну конфігурацію пристроїв або навіть виконання шкідливих команд на них. Щоб уникнути цієї вразливості, необхідно використовувати захищені версії SNMP (наприклад, SNMPv3) з шифруванням та аутентифікацією, а також застосовувати інші заходи безпеки, такі як використання внутрішньої мережі або використання VPN для захищеного з'єднання.

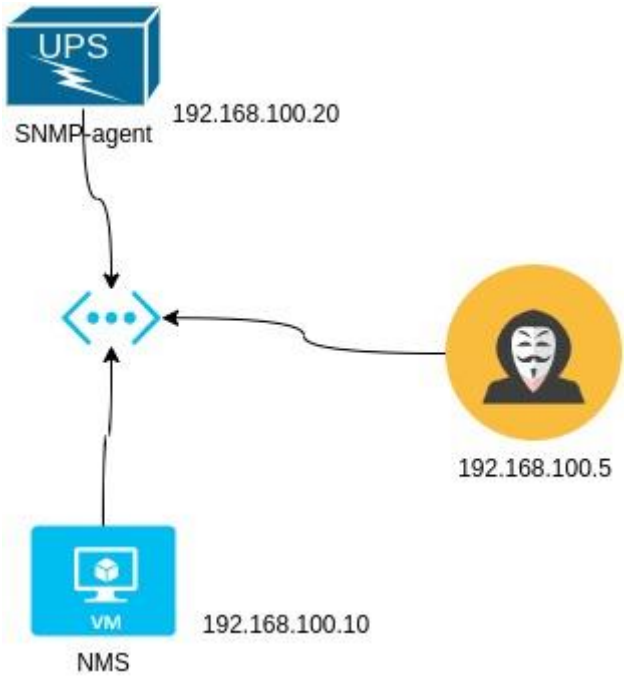


Рис. 1 – Приклад атаки Man-in-the-Middle

- також є проблема переповнення таблиць маршрутизації в SNMP, це справді серйозна проблема. Злоумисники можуть легко викликати переповнення, надсилаючи велику кількість запитів SNMP з великою кількістю даних. Якщо мережеві пристрої не в змозі ефективно обробляти цей потік запитів, це може призвести до серйозних проблем, включаючи втрату обробки легітимного трафіку та зниження доступності мережі. Щоб уникнути цього, важливо правильно налаштувати фільтрацію запитів SNMP та використовувати механізми контролю доступу, щоб обмежити кількість запитів, які можуть бути оброблені.

Тож, поговоримо про методи захисту, які забезпечать безпеку для даного протоколу та його можливостей. Один із них це поділення мережі на сегменти. Розділити її на окремі частини з різними рівнями доступу і застосувати різні політики безпеки до кожного з них. Наприклад, можна створити окремі сегменти для службових систем, технологічних пристроїв та SNMP-агентів, і заборонити доступ до цих сегментів з гостьових мереж WiFi або користувацьких сегментів. Такий підхід допомагає зменшити ризик компрометації систем через атаки на перехоплення або несанкціонований доступ.

Використання останньої версії протоколу - SNMPv3, може значно підвищити безпеку вашої мережі. Якщо ваше обладнання та системи управління мережею підтримують SNMPv3, рекомендується використовувати саме цю останню версію.

Також мною було проведено дослідження та виявлено, що коли SNMP-агент

працює в режимі "тільки для читання" (read-only), це означає, що можна тільки зчитувати інформацію з пристрою, але не можна вносити зміни до його конфігурації чи виконувати будь-які команди, які можуть вплинути на роботу мережі. Вимкнення режиму запису для SNMP-агентів створює додатковий шар захисту, оскільки зловмисники не зможуть змінювати конфігурацію пристроїв через SNMP, якщо вони намагаються отримати несанкціонований доступ до мережі. Це може запобігти потенційним атакам, таким як зміна IP-адреси, налаштування безпеки або зміна паролів.

Ще було помічено, що велику небезпеку несуть доступа до портів SNMP. Тому є сенс обмежити ці доступи. Цей підхід стосується захисту від атак спуфінгу в контексті міжмережевої взаємодії і може бути розглянутий як стратегія захисту мережі від потенційно небезпечних дій.

Перелік посилань:

1. Проблеми безпеки SNMP на практиці: імітація атак та запобіжні заходи. URL доступ: https://habr.com/ru/companies/selectel/articles/719402/

Ломовацький Олександр Вікторович
студент групи БСД-41, ННІЗІ ДУІКТ, Київ, Україна

РОЛЬ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЗАБЕЗПЕЧЕННІ СТІЙКОСТІ ТА НАДІЙНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

Сучасний світ безпеки інформації постійно зазнає викликів через швидкі технологічні зміни, динамічність кіберзагроз та поширення цифрових технологій у всіх сферах життя. В умовах цього невпинного еволюційного процесу, забезпечення стійкості та надійності інформаційних систем стає завданням критичного значення.

Аудит інформаційної безпеки відіграє ключову роль у цьому контексті, надаючи організаціям засоби для оцінки, контролю та вдосконалення рівня захищеності їх інформаційних ресурсів. Він не лише виявляє потенційні загрози та вразливості, але й допомагає виправляти їх та підвищувати рівень стійкості системи до майбутніх атак. У світлі неспокійних подій в галузі кібербезпеки, таких як масштабні кібератаки та витоки даних, розуміння ролі аудиту інформаційної безпеки набуває ще більшого значення. Він стає необхідним елементом стратегічного планування та управління ризиками, спрямованим на забезпечення безпеки, довіри та надійності інформаційних систем у будь-якому секторі.

Матеріали та методи

Для наукового обґрунтування результатів досліджень ролі аудиту інформаційної безпеки в забезпеченні стійкості та надійності інформаційних систем використаний статистичний метод, а саме досліджена статистика ДССЗІ щодо кіберінцидентів, які сталися протягом 2023 року[1].

Результати

Згідно звіту ДССЗІ, кількість зареєстрованих кіберінцидентів в порівнянні з 2022 роком, зросла на 62.5%. Згідно з Рис. - 1, події пов'язані з компрометацією системи(05.02), некоректною конфігурацією(09.02) та фішингом(03.03) мають більше ніж 100000 зафіксованих випадків.

Рис. 1 - Кількість зарєстрованих подій за типопом подій ІБ

Аудит інформаційної безпеки допомагає ідентифікувати потенційні загрози та вразливості в інформаційних системах. [2 - 125с.] Шляхом систематичного аналізу та оцінки рівня захисту, аудитори можуть виявляти слабкі місця, які потребують негайного вдосконалення, що дозволяє зменшити ризик виникнення кіберінцидентів. Проведення аудиту дозволяє оцінити ефективність та дієвість вжитих заходів безпеки. Шляхом перевірки відповідності практик безпеки стандартам та нормативам, аудитори можуть рекомендувати поліпшення в існуючих процедурах та політиках безпеки, щоб забезпечити більш ефективний захист інформації. Аудит інформаційної безпеки допомагає організаціям відповідати вимогам законодавства, стандартів та регуляторних вимог у сфері кібербезпеки. Проведення регулярного аудиту дозволяє підтримувати відповідність до встановлених нормативів та уникати потенційних штрафів та санкцій за порушення правил. Участь у процесі аудиту сприяє підвищенню рівня свідомості персоналу щодо важливості безпеки інформації та дотримання правил безпеки. Шляхом впровадження рекомендацій аудиторів та навчання персоналу з питань безпеки, організації

можуть підвищити культуру безпеки та знизити ризик внутрішніх та зовнішніх загроз.

Висновки

Результати підкреслюють важливу роль аудиту інформаційної безпеки у виявленні загроз та вразливостей в інформаційних системах, що сприяє зменшенню ризику кіберінцидентів та покращує загальний рівень безпеки. Крім того, аудит допомагає підтримувати відповідність до встановлених нормативів та стандартів у сфері кібербезпеки, а також сприяє підвищенню культури безпеки серед персоналу.

Перелік посилань:

1. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. *Державний центр кіберзахисту*. URL: https://scpc.gov.ua/uk/articles/334 (дата звернення: 04.04.2024).
2. АУДИТ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ / О. Корченко та ін. Київ : "Центр навч.-наук. та науково-практ. вид. Нац. акад. СБ України", 2014. 190 с.

Насонова Марія Сергіївна
Студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

Теперішні реалії російської військової агресії та фактично розв'язаної війни супроводжуються акціями кібернетичного впливу, в тому числі і кібератаками, що мають деструктивний характер, їх розслідування стає першочерговим завданням для розуміння тактик і технік, що використовують російські спецслужби.

Російські спецслужби та афілійовані з ними хакерські угруповання відповідальні за велику кількість кібератак по всьому світу, ці атаки мали різне значення та кінцеву мету, а розслідування та аналіз цих атак дають змогу визначити рівень обізнаності та кваліфікацію фізичних осіб, які за ними стоять.

Серед підконтрольних спецслужбам рф хакерських угруповань можна чітко виділити певну закономірність, що наштовхує на думку їх класифікації за різними ознаками.

Так, однією з характеристик може бути *публічність*. Серед публічних угруповань можна виділити такі, що ведуть свої сторінки у соціальних мережах та месенджерах, анонсують свої DDoS атаки та орієнтовані на внутрішнє населення рф, наприклад "Народная CyberАрмия" – веде свою сторінку в месенджері Telegram, де анонсує атаки на інфраструктури різних країн, до неї також можна віднести угруповання "NoName057(16)", що має 2 канали в

месенджері Telegram – 1 з описом атак російською мовою, інший з англійською мовою. З непублічних угруповань можна виділити угруповання "Turla", "Sandworm", APT28, APT29, які відповідальні за кампанії шпигунства та деструктивні атаки на різні країни світу включно з Україною.

Виходячи з вищесказаного, можна виділити наступний критерій – *міра проникнення.* Під поняттям міри проникнення слід розуміти наявність безпосереднього доступу до інфраструктури жертви, ексфільтрацію та\або знищення інформації. Таким чином публічне хакерське угруповання "Beregini", яке активно веде Telegram-канал, де публікує документи українських державних установ, проте безпосередньо до систем з яких ці документи було викрадено – не має. За таким самим принципом працює і угруповання "Джокер ДНР", яке проводить акції інформаційного впливу шляхом розповсюдження інформаційно-психологічних "вкидів", що дискредитують українську владу або державні органи, проте безпосереднього доступу до них вони не мають. На противагу до публічних угруповань, що мають на меті проведення спеціальних інформаційно-психологічних операцій діють і APT(Advanced persistent threat) угруповання, завданням яких є збір розвідувальної інформації про об'єкти суспільного, політичного, економічного та військового та інтересу.

Виходячи з усього вищесказаного можна зробити висновок, що розслідування кіберінцидентів тісно пов'язане з документуванням тактик, технік, а також мати стандартизований класифікатор, наприклад MITRE ATT&CK для відстеження тих чи інших угруповань.

Папуча Нікіта Віталійович
студент групи УБДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ДЛЯ ОПТИМІЗАЦІЇ ВИЯВЛЕННЯ ТА ВІДПОВІДІ НА КІБЕРЗАГРОЗИ В ОРГАНІЗАЦІЇ

Штучний інтелект дозволяє автоматизувати виявлення аномальних активностей, розробляти автоматизовані системи відгуку на кібератаки та проводити прогностичний аналіз для передбачення майбутніх загроз. Інтеграція ШІ підвищує ефективність управління кібербезпекою, допомагає організаціям швидше реагувати на кіберзагрози та забезпечує надійний захист їх цифрових активів. Ця стаття служить як огляд потенційних застосувань ШІ в кібербезпеці та рекомендацій для організацій, які прагнуть покращити свої заходи безпеки в цифровому середовищі.

На сьогодні кібербезпека стає все більш важливою для організацій будь-

якого розміру. Кібератаки стають все більш складними та розповсюдженими, вимагаючи від організацій постійної готовності та швидкого реагування. Штучний інтелект (ШІ) відіграє ключову роль у підвищенні ефективності управління кібербезпекою, надаючи можливості для автоматизації, аналізу та прогнозування.

Однією з основних переваг ШІ в кібербезпеці є його здатність автоматично виявляти аномальну активність в мережах і системах. За допомогою машинного навчання та алгоритмів аналізу великих даних, ШІ може виявляти зміни в поведінці користувачів та мережевому трафіку, що вказує на потенційні загрози.

Штучний інтелект також може бути використаний для розробки автоматизованих систем відгуку на кібератаки. Системи з ШІ можуть швидко реагувати на загрози, блокуючи атакуючі джерела, ізолюючи заражені системи та відновлюючи нормальну роботу мережі[1].

Інтеграція ШІ в системи управління кібербезпекою дозволяє організаціям не тільки реагувати на поточні загрози, але й прогнозувати майбутні ризики. За допомогою аналітичних моделей та прогностичного аналізу, ШІ може ідентифікувати слабкі місця у системах безпеки та рекомендувати стратегії для їх вдосконалення.

Інтеграція штучного інтелекту також може сприяти ефективному використанню ресурсів організації, зокрема людських ресурсів, часу та бюджету. Автоматизація процесів виявлення та аналізу кіберзагроз зменшує необхідність в ручній роботі, дозволяючи спеціалістам зосередитися на стратегічних завданнях та вдосконаленні систем безпеки. Крім того, раннє виявлення та блокування загроз може значно знизити витрати на відновлення після кібератак і мінімізувати потенційні фінансові втрати в результаті кіберінцидентів[2].

Впровадження штучного інтелекту в сферу кібербезпеки також підкреслює важливість постійної освіти та навчання персоналу. ШІ може використовуватися як інструмент для створення симуляцій кібератак, тренування співробітників на випадок реальних загроз та аналізу реакції команди на інциденти. Забезпечення належного рівня обізнаності та підготовки персоналу є ключовим для успішної інтеграції штучного інтелекту в системи управління кібербезпекою та підвищення загальної рівня безпеки в організації[3].

Штучний інтелект відкриває нові горизонти для управління кібербезпекою в організаціях. Автоматизація виявлення аномальних активностей, розробка автоматизованих систем відгуку та прогностичний

аналіз дозволяють організаціям бути краще підготовленими до кіберзагроз, ефективно реагувати на них та попереджувати майбутні ризики. З інтеграцією ШІ в системи управління кібербезпекою організації можуть забезпечити надійний захист своїх цифрових активів та зберегти репутацію в епоху постійних кіберзагроз. Інтеграція штучного інтелекту в системи управління кібербезпекою не лише підвищує ефективність захисту організацій від кіберзагроз, але й сприяє оптимізації використання ресурсів, зменшенню витрат та покращенню підготовки персоналу. Штучний інтелект відкриває нові можливості для підвищення безпеки в цифровому світі, стаючи невід'ємною частиною сучасних стратегій управління кібербезпекою в організаціях.

Перелік посилань:

1. Пацула В. І. Штучний інтелект 2006. URL: http://essuir.sumdu.edu.ua/handle/123456789/60273 (дата звернення: 09.04.2024).
2. Таранич А., Пелехацький Д. Використання штучного інтелекту в процесах стратегічного управління підприємствами. *Economy of ukraine*. 2024. Т. 67, № 1(746). С. 54–65. URL: https://doi.org/10.15407/economyukr.2024.01.054 (дата звернення: 09.04.2024).
3. Інтеграція штучного інтелекту в процес онлайн-навчання. А. Кім та ін. *Молодь і ринок*. 2024. № 10/218. С. 32–37. URL: https://doi.org/10.24919/2308-4634.2023.292867 (дата звернення: 10.04.2024).

Парфенюк Тетяна Миколаївна
Студентка групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ЗАСТОСУВАННЯ ПРИНЦИПУ ZERO TRUST ДЛЯ ПОПЕРЕДЖЕННЯ ІНСАЙДЕРСЬКИХ ЗАГРОЗ

В контексті цифрової трансформації, коли компанії все більше покладаються на цифрові технології, значення захисту від внутрішніх загроз зростає. Інсайдерські загрози представляють складний і динамічний ризик, що впливає на державні та приватні домени всіх секторів критичної інфраструктури. Визначення цих загроз є критично важливим кроком у розумінні та створенні програми пом’якшення внутрішніх загроз.

Агентство з кібербезпеки та безпеки інфраструктури (CISA) визначає внутрішню загрозу як загрозу того, що інсайдер використовує свій авторизований доступ, навмисно чи ненавмисно, щоб завдати шкоди місії, ресурсам, персоналу, об’єктам, інформації, обладнанню, мережам або системам департаменту. . Внутрішні загрози проявляються різними способами: насильство, шпигунство, диверсії, крадіжки та кіберактивності.

Інсайдер — це будь-яка особа, яка має або мала авторизований доступ або знання ресурсів організації, включаючи персонал, приміщення, інформацію, обладнання, мережі та системи.

Авторизовані акаунти інсайдерів є основними загрозами, які необхідно перевіряти у випадку витоку даних. Авторизовані користувачі можуть виконувати багато операцій з даними компанії залежно від своїх привілейованих прав доступу, і можуть піддавати вашу компанію кібератакам, якщо не застосовувати різні передові протоколи безпеки. Успішне впровадження таких протоколів і відсутність прогалин, які можуть призвести до порушень безпеки доступу, має прямий вплив як на довгостроковий успіх, так і на фінансову звітність компаній. Це пов'язано з тим, що втрати, пов'язані з витоком даних внаслідок інсайдерської загрози, призводять до серйозних негативних фінансових наслідків для компаній.

IT-відділи та команди кібербезпеки, відповідальні за забезпечення інформаційної безпеки, повинні захищати авторизовані облікові записи та відстежувати всі кроки, які вони здійснюють у процесі привілейованого доступу. Методології нульової довіри та найменших привілеїв є одними з найбільш функціональних варіантів для команд, які можуть впроваджувати та перевіряти привілейований доступ і забезпечувати високий рівень безпеки даних.

Всупереч поширеній думці, Zero Trust не є програмою безпеки або додатком для захисту даних. Простіше кажучи, Zero Trust - це стратегічний підхід до безпеки даних, який був розроблений на основі принципу "Ніколи не довіряй, завжди перевіряй" і базується на тому, що компанії не повинні довіряти жодному цифровому активу всередині або поза мережею. Ця політика безпеки базується на принципі, що всі цифрові об'єкти, які намагаються підключитися до мережі компанії, повинні бути перевірені перед тим, як їм буде надано доступ до даних.

Найважливішою перевагою методології нульової довіри є її здатність протистояти внутрішнім загрозам. Містячи багато процесів, які вимагають перевірки та затвердження авторизації, політика нульової довіри значно зменшує потенційні витоки даних, спричинені внутрішніми загрозами. Zero Trust тримає доступ під контролем за допомогою таких функцій, як централізоване управління паролями, управління авторизованими сеансами та багатофакторна автентифікація (MFA).

Отже, інсайдерські загрози є безперечно актуальною проблемою, яка вимагає вирішення. Одним із методів попередження є застосування принципу нульової довіри, оскільки від полягає у наданні доступу лише до необхідних для роботі ресурсів. Цей принцип дозволяє пом’якшити наслідки від потенційних інсайдерських атак.

Перелік посилань

1. Defining Insider Threats URL: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats
2. Ways to Mitigate Insider Threats Using Privileged Access Management URL: https://krontech.com/ways-to-mitigate-insider-threats-using-privileged-access-management

Пелюх Володимир Ігорович
студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

НАСЛІДКИ ДЛЯ БЕЗПЕКИ ВІД СИСТЕМ З ВРАЗЛИВОСТЯМИ

Короткий огляд можливостей використання незакритих вразливостей та потенційних наслідків для організацій. Аналіз реальних кейсів атак за останній час.

Складність цифрового ландшафту. Він стає дедалі складнішим, а організації для ведення бізнесу значною мірою покладаються на взаємопов'язані системи та програмні додатки. Така залежність від технологій вимагає надійних заходів кібербезпеки для захисту від кіберзагроз, що постійно змінюються. Важливим елементом кібербезпеки є управління вразливостями, що передбачає виявлення, визначення пріоритетів та усунення слабких місць у системах. Постачальники програмного забезпечення постійно випускають патчі для усунення цих вразливостей, проте багато організацій намагаються підтримувати процес своєчасного встановлення патчів, залишаючи свої системи вразливими.

Невиправлені вразливості створюють значні загрози безпеці, відкриваючи двері для зловмисників, якими вони можуть скористатися. У цій тезі буде розглянуто вплив невиправлених систем на безпеку, зосереджуючись на потенційних наслідках для організацій. У наступних розділах розглядається природа вразливостей та управління виправленнями, а потім детально описуються конкретні ризики безпеки, пов'язані з невиправленими системами, такі як витік даних, зараження шкідливим програмним забезпеченням та збої в роботі системи. Щоб ще більше проілюструвати серйозність цих наслідків, буде розглянуто реальний приклад масштабної кібератаки з використанням невиправлених вразливостей. Насамкінець тези буде підсумовано ключові ризики безпеки та підкреслено важливість своєчасного управління вразливостями та виправленнями[1].

Вразливості та управління виправленнями. Природа програмних додатків передбачає, що вони можуть містити недосконалості або слабкі місця в коді, спочатку баги, котрі можуть перерости у вразливості. Ці вразливості можуть

бути використані зловмисниками для отримання несанкціонованого доступу до систем, викрадення даних або порушення роботи. Вразливості класифікуються за ступенем їхньої серйозності: "критичний", "високий", "середній" і "низький" вказують на потенційний вплив, який вони можуть мати, якщо ними скористатися.

Управління виправленнями - це безперервний процес виявлення, одержання, тестування та розгортання оновлень програмного забезпечення (патчів), які усувають ці вразливості. Зазвичай ці патчі випускаються постачальниками програмного забезпечення і призначені для усунення вразливостей і покращення загального стану безпеки системи.

Однак підтримка процесу своєчасного встановлення виправлень може бути складним завданням для організацій. Тестування патчів перед розгортанням може зайняти багато часу, а занепокоєння щодо потенційних простоїв або проблем стабільності з існуючим програмним забезпеченням може призвести до затримок. Це підкреслює важливість дотримання балансу між безпекою та операційною ефективністю при впровадженні системи управління виправленнями[2].

Наслідки невиправлених систем для безпеки. Невиправлені системи створюють сприятливий ґрунт для кібератак, роблячи організації вразливими до низки загроз безпеці. У цій частині ми розглянемо деякі з найпоширеніших та найнебезпечніших наслідків:

Витоки даних: Невиправлені вразливості можуть стати для зловмисників воротами для проникнення в системи та викрадення конфіденційних даних. У 2024 році кібератака "невідомих" хакерів на одного з найбільших інтернет-провайдерів у Москві використовувала невиправлену вразливість, що скомпрометувала особисту інформацію мільйонів абонентів і призвела до повного знищення систем. Цей інцидент підкреслює величезну кількість конфіденційних даних, якими володіють телекомунікаційні компанії, і серйозні наслідки, до яких може призвести нездатність усунути вразливості. [3]

Ще ближче до нас — нещодавній інцидент, що стався наприкінці 2023 року з Київстаром, відомим українським оператором мобільного зв'язку, слугує суворим нагадуванням про ризики, пов'язані з невиправленими системами. Хоча деталі все ще з'ясовуються, перші звіти свідчать про те, що зловмисники отримали доступ до системи завдяки невиправленій вразливості, потенційно скомпрометувавши дані клієнтів і порушивши роботу критично важливих сервісів. Ці реальні випадки демонструють, як нехтування управлінням виправленнями може мати значний вплив на конфіденційність клієнтів і довіру до організації. [4]

Зараження шкідливим програмним забезпеченням: Невиправлені вразливості можуть бути використані зловмисниками для розгортання шкідливого програмного забезпечення на скомпрометованих системах. Шкідливе програмне забезпечення охоплює цілу низку шкідливих програм, включаючи програми-вимагачі, які шифрують файли та вимагають плату за розшифрування, шпигунські програми, які викрадають конфіденційну інформацію, та ботнети, які використовують скомпрометовані системи для проведення масштабних атак. Атака вірусу-здирника WannaCry 2017 року, який використовував не виправлену вразливість у Microsoft Windows, слугує жахливим прикладом того, до яких масштабних порушень роботи та фінансових втрат може призвести шкідливе програмне забезпечення.

Порушення роботи системи та простої: Невиправлені системи більш вразливі до атак, які можуть дестабілізувати або вивести з ладу критично важливі системи. Це може призвести до тривалих періодів простою, вплинути на основні бізнес-операції та спричинити значні фінансові втрати. Наприклад, нещодавня кібератака, спрямована на мережу лікарень, використовувала незахищену вразливість, що призвело до переривання надання критично важливих медичних послуг і потенційної затримки важливих процедур. Ці інциденти підкреслюють важливість управління виправленнями для забезпечення стабільності та безперервності роботи системи. [5]

У цій тезі розглянуті критичні наслідки для безпеки неоновлених систем, підкреслюючи потенційні наслідки для організацій у сучасному цифровому ландшафті. Нехтуючи своєчасним встановленням виправлень, організації наражають себе на низку кіберзагроз, включаючи витік даних, зараження шкідливим програмним забезпеченням та збоїв в роботі системи. Реальні приклади, такі як злам мобільного оператора у 2023 році, атака вірусу-здирника WannaCry у 2017 році, та безліч інших прикладів, ілюструють масштабність збоїв та фінансових втрат, які можуть статися внаслідок використання вразливостей зловмисниками. [5]

Зміцнення системи безпеки організації вимагає проактивного підходу до управління вразливостями та управління виправленнями. Це передбачає систематичну ідентифікацію, визначення пріоритетів і розгортання патчів безпеки для усунення вразливостей у системах. Ефективні програми управління виправленнями враховують такі фактори, як серйозність, можливість експлуатації та потенційний час простою, щоб забезпечити своєчасне усунення вразливостей, мінімізуючи при цьому перебої в роботі. Крім того, інтеграція автоматизації виявлення та виправлення загроз може покращити визначення пріоритетів безпеки, зосередивши увагу на

вразливостях, які активно використовуються зловмисниками.

Надаючи пріоритет управлінню виправленнями та прийнявши комплексну стратегію кібербезпеки, організації можуть значно зменшити поверхню атак і підвищити загальну стійкість. Майбутні напрямки досліджень можуть вивчати потенціал автоматизації для оптимізації процесів розгортання патчів та інтеграції управління вразливостями з ширшими системами безпеки. Насамкінець, оскільки ландшафт кіберзагроз постійно розвивається, пріоритетне управління виправленнями залишається важливим елементом захисту конфіденційних даних, забезпечення стабільності системи та підтримки безперервності бізнесу в цифрову епоху.

Перелік посилань:

1. What are the risks of unpatched software vulnerabilities [Електронний ресурс] – Режим доступу до ресурсу: https://www.pdq.com/blog/risks-of-unpatched-software-vulnerabilities/
2. A comparative breakdown of Patch and Vulnerability Management [Електронний ресурс] – Режим доступу до ресурсу: https://www.syxsense.com/a-comparative-breakdown-of-patch-and-vulnerability-management
3. Blackjack hackers target Moscow ISP in retaliation for Kyivstar cyberattack [Електронний ресурс] – Режим доступу до ресурсу: https://siliconangle.com/2024/01/09/blackjack-hackers-target-moscow-isp-retaliation-kyivstar-cyberattack/
4. Cyberattack Cripples Ukraine's Largest Telecom Operator [Електронний ресурс] – Режим доступу до ресурсу: https://www.securityweek.com/cyberattack-cripples-ukraines-largest-telcom-operator/
5. Vulnerability Management / Malicious Code [Електронний ресурс] – Режим доступу до ресурсу: https://www.aquasec.com/cloud-native-academy/vulnerability-management/malicious-code/

Поліщук Артем Сергійович,
Студент групи БСД-51 ,ННІЗІ ДУІКТ, Київ, Україна

Технологія забезпечення безпеки на основі ELK Stack

Аннотація: Системи SIEM (Security Information and Event Management) є важливим елементом інфраструктури безпеки для багатьох організацій. SIEM поєднує в собі функціональність системи виявлення вторгнень (IDS) та системи управління журналами подій (Log Management), що дозволяє забезпечувати безпеку даних у реальному часі.

Основні функції SIEM включають збір, агрегацію та аналіз журналів подій з різних джерел у мережі, виявлення аномальних патернів у поведінці користувачів та сутностей, а також сповіщення та реагування на потенційні загрози.

У цій тезі розглянуто ELK стек який використовується як SIEM система.

Огляд ELK Stack

ELK Stack - це набір програмних продуктів, який включає три основні компоненти: Elasticsearch, Logstash і Kibana.

Elasticsearch - це потужний та розподілений пошуковий движок, який дозволяє здійснювати швидкий пошук та аналіз структурованих даних в реальному часі. Основні можливості Elasticsearch включають:

- Індексація даних: Elasticsearch забезпечує швидку та ефективну індексацію даних, що дозволяє швидко отримувати результати пошуку навіть у великих обсягах даних.
- Пошук та аналіз даних: Elasticsearch надає потужні можливості пошуку та аналізу даних, включаючи підтримку різних типів запитів, агрегацію даних та функції ранжування.
- Розподіленість та масштабованість: Elasticsearch розроблений для роботи у розподіленому середовищі, що дозволяє масштабувати його до дуже великих обсягів даних та високих навантажень.
- Реалізація в ELK Stack: Elasticsearch використовується для зберігання та індексації даних, зібраних Logstash, і для подальшого відображення та аналізу даних у Kibana.

Logstash - це інструмент для обробки та інтеграції різноманітних даних з різних джерел перед їхнім індексуванням у Elasticsearch. Основні можливості Logstash включають:

- Збір логів: Logstash може збирати логи з різних джерел, таких як журнали подій, веб-сервери, бази даних тощо, для подальшої обробки та аналізу.
- Обробка даних: Logstash надає можливості для обробки даних, включаючи фільтрацію, перетворення та структурування даних перед їхнім індексуванням у Elasticsearch.
- Інтеграція з різними джерелами: Logstash підтримує різноманітні вихідні та вхідні джерела даних, що дозволяє легко інтегрувати його з різними системами та джерелами даних.
- Реалізація в ELK Stack: Logstash використовується для збору, обробки та пересилання даних до Elasticsearch для подальшого аналізу та візуалізації у Kibana.

Logstash допомагає структурувати та підготувати дані для подальшого аналізу в Elasticsearch, що робить його важливою частиною ELK Stack для забезпечення безпеки даних.

Kibana - це візуалізаційний інтерфейс, який дозволяє створювати інтерактивні графіки, діаграми та таблиці для аналізу даних, збережених у Elasticsearch. Основні можливості Kibana включають:

- Візуалізація даних: Kibana дозволяє візуалізувати дані з Elasticsearch у вигляді різноманітних графіків, діаграм та таблиць, що допомагає аналізувати дані та виявляти закономірності.
- Створення віджетів: Крім графіків та діаграм, Kibana дозволяє створювати віджети для відображення конкретних аспектів даних, таких як таблиці з даними або фільтри для вибору певних даних.
- Розгортання та керування панелями: Kibana надає можливість створювати та керувати різними панелями для організації візуалізацій та дашбордів.
- Інтеграція з Elasticsearch: Kibana безпосередньо інтегрується з Elasticsearch, що дозволяє легко візуалізувати та аналізувати дані, збережені у Elasticsearch.

Kibana допомагає візуалізувати дані з Elasticsearch у зручному та зрозумілому форматі, що дозволяє аналізувати дані та виявляти важливі відомості для забезпечення безпеки даних.

ELK Stack дозволяє збирати, зберігати, аналізувати та візуалізувати дані з різних джерел, що робить його потужним інструментом для аналізу даних та моніторингу безпеки.

ELK Stack є потужним інструментом для аналізу поведінки користувачів і сутностей у мережі з метою забезпечення безпеки даних. Використання Elasticsearch для зберігання та індексації даних, Logstash для збору та обробки даних та Kibana для візуалізації даних дозволяє ефективно виявляти аномалії та потенційні загрози.

Основні переваги ELK Stack полягають у його відкритому вихідному коді, гнучкості та ефективності аналізу даних. Використання ELK Stack може значно підвищити ефективність заходів забезпечення безпеки та допомогти виявляти та реагувати на потенційні загрози швидше та ефективніше.

Перелік посилань:

1. Elasticsearch [Електронний ресурс] – Режим доступу до ресурсу: https://www.elastic.co/elasticsearch/

2. Logstash [Електронний ресурс] – Режим доступу до ресурсу: https://www.elastic.co/logstash/
3. Kibana [Електронний ресурс] – Режим доступу до ресурсу: https://www.elastic.co/kibana/

Розгон Денис Анатоілйович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

Блокчейн як інструмент для забезпечення приватності ідентифікаційних даних

Технологія Blockchain, спочатку розроблена для біткойнів, тепер використовується в багатьох сферах, оскільки вона добре забезпечує безпеку, чіткість і незмінність даних. Основні ідеї, такі як відсутність єдиного контролю, домовленості щодо даних і коду для збереження даних, роблять його ідеальним для змішування та збереження надійності даних у сучасних інформаційних системах. У цьому матеріалі розповідається про те, як блокчейн використовується для цих цілей, і розглядаються реальні приклади.

Основи блокчейна можна Описати трьома принципами:

- Децентралізація: відсутність єдиного місця контролю означає, що його важче атакувати або зламати.

- Незмінність даних: після додавання блоку його інформацію неможливо змінити без зміни всіх блоків після нього, що майже неможливо без згоди багатьох людей.

- Безпечний код: використання хеш-функцій і нерівномірне кодування захищає дані від небажаного доступу.

Блокчейн може створити одну надійну базу даних, яка об’єднує інформацію з різних місць. Це корисно в:

- Ланцюгах поставок: відстеження кожного товару від виробника до покупця.

- Охороні здоров'я: одне місце для медичних записів, відкритих з різних місць здоров'я.

- Фінансах: полегшення транзакцій і скорочення посередників.

Блокчейн надає можливості прослідковувати потоки даних, що додає можливість довести правдивість даних і їх походження, що є важливою і ключовою характеристикою для:

- Документів: збереження юридичної сили онлайн-документів.

- Голосування: створення систем голосування, де кожен голос можна перевірити, але не змінити.

- Юридичних питань: запис угод, контрактів та інших юридичних речей у фіксованій формі.

Далі буде наведено два приклади реального використання блокчейну, та дослідження цієї теми:

1. Естонія є лідером у світі за використанням блокчейну в урядовій роботі. Часто досліджується їхній успіх у додаванні нових технологій у громадські місця. Нижче наведено ключові моменти про те, як Естонія використовує блокчейн для онлайн-голосування, медичних записів і дій уряду.

Естонія першою з 2005 року запровадила онлайн-голосування по всій країні за допомогою блокчейну. Ця система голосування дозволяє громадянам голосувати з будь-якого місця, де є Інтернет, що полегшує участь у виборах. Блокчейн зберігає голоси в безпеці та незмінності, зупиняючи будь-які зміни чи видалення після голосування.

Естонія використовує блокчейн для збереження медичних записів у безпеці та конфіденційності. Ця система дозволяє пацієнтам і лікарям переглядати історію хвороби, рецепти та результати аналізів онлайн. Blockchain гарантує, що кожна зміна (як лікар, який оновлює запис) залишає безпечний слід, який запобігає фальшивим записам або небажаному доступу.

Блокчейн допомагає зробити урядові рішення більш чіткими та ефективними. Це включає в себе ведення обліку власності, податкової інформації та державних закупівель. Кожна дія фіксується в блокчейні, що полегшує перевірку державних даних і довіру до них, а також знижує ймовірність корупції.

Незважаючи на великі переваги, використання блокчейну в уряді в Естонії також стикається з проблемами. До них належать проблеми з масштабуванням, вартість налаштування та збереження конфіденційності. Тим не менш, Естонія продовжує лідирувати в цій галузі, постійно вдосконалюючи свої технологічні рішення.

Цей приклад може стати посібником для інших країн, які планують використовувати блокчейн, щоб зробити державне управління більш прозорим, безпечним і ефективним.

2. Maersk, провідна світова компанія з транспортування речей у великих ящиках, і IBM, велика технологічна фірма, об’єдналися, щоб створити систему під назвою TradeLens, використовуючи технологію блокчейн. Цей проект стартував у 2018 році, щоб покращити роботу ланцюгів доставки та постачання. TradeLens дозволяє людям і компаніям, які займаються торгівлею, наприклад тим, хто відправляє товари, транспортним компаніям, портовим обробникам і митним агентам, швидко й легко обмінюватися інформацією та документами.

Завдяки блокчейну TradeLens пропонує чіткий і безпечний спосіб обробки даних, знижуючи ризики та витрати, пов’язані з паперовою роботою та затримками. Це також допомагає швидше робити вибір завдяки автоматизації та кращому доступу до свіжої інформації. TradeLens об’єднав понад 100 груп, у тому числі багато портів по всьому світу, демонструючи величезний інтерес до цієї технології в сучасному судноплавстві.

Незважаючи на багато хороших моментів, є великі проблеми:

- Обмежена здатність обробляти багато транзакцій.

- Важко влитися в існуючі IT-системи.

- Немає загальних правових правил використання блокчейну.

Блокчейн пропонує унікальні можливості для змішування та збереження даних. Його прийняття може значно змінити багато галузей, запропонувавши більше безпеки, ефективності та чіткості операцій. Проте, щоб повністю використати його потенціал, необхідно подолати технічні та юридичні проблеми. Навчання та спільна робота ключових гравців мають вирішальне значення для вирішення цих проблем і забезпечення широкого поширення технології блокчейн.

Перелік посилань:

1. TradeLens Solution brief edition two URL: https://www.maersk.com/~/media_sc9/maersk/local-information/files/west-central-asia/india/tradelens-solution-brief.pdf (дата звернення: 30.03.2024).

2. Estonia – the Digital Republic Secured by Blockchain URL: https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf (дата звернення: 03.04.2022).

Савельєв Олександр Андрійович
Студент групи УБДМ-51, ННІЗІ ДУІКТ, Київ, Україна

Аналіз та оцінка методів тестування безпеки SCADA у критичній інфраструктурі

Робота присвячена аналізу та оцінці методів тестування безпеки систем управління супутньою технічною інфраструктурою (SCADA) у критичній інфраструктурі. З урахуванням зростаючих загроз кібербезпеці та важливості забезпечення стійкості та безпеки критичних інфраструктурних систем, дослідження ефективності та захищеності методів тестування є актуальною задачею.

Аналіз та оцінка ефективності методів тестування безпеки систем управління супутньою технічною інфраструктурою (SCADA) є критичним аспектом забезпечення кібербезпеки критичної інфраструктури. У зв'язку з постійним розвитком технологій та зростаючими загрозами кібератак, необхідно постійно аналізувати та оцінювати наявні методи тестування на їхню ефективність та рівень захищеності.

До основних принципів аналізу та оцінки методів тестування безпеки SCADA у критичній інфраструктурі відноситься:

Огляд існуючих методів тестування безпеки SCADA. У розділі буде проведений огляд та аналіз існуючих методів тестування безпеки SCADA, включаючи пентестінг, вразливості та уразливість додатків, та аналіз згідно стандартів безпеки.

Визначення критеріїв оцінки ефективності методів тестування. В цьому розділі будуть визначені критерії, за якими буде проведена оцінка ефективності та захищеності методів тестування безпеки SCADA.

Аналіз та порівняння методів тестування. В даному розділі будуть проведені аналіз та порівняння різних методів тестування безпеки SCADA з використанням раніше визначених критеріїв.

Зробимо висновки. У заключному розділі будуть сформульовані висновки щодо ефективності та захищеності існуючих методів тестування безпеки SCADA та рекомендації щодо їхнього використання.

Сайчук Вадим Дмитрович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

Технології захисту корпоративних інформаційних систем.

Корпоративні інформаційні системи - сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів у корпоративних мережах. Інформаційні системи – сучасний вид зв’язку, без якого не можлива наша комунікація з зовнішнім світом. За допомогою мереж кожну секунду передаються сотні Гігабіт даних та інформації. Відбувається спілкування людей між собою на великих відстанях та у різних країнах. За допомогою мереж ми маємо доступ до усієї інформації, яка нам необхідна для роботи та життя. В той же час кіберзлочинці постійно намагаються отримати доступ до корпоративних мереж для того, щоб заволодіти конфіденційною інформацією великих компаній та особистою інформацією користувача, для подальшого її використання у незаконних цілях.

До організаційних засобів захисту інформації відноситься комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач фізичного захисту шляхом надання доступу персоналу до інформаційних систем та порядку функціювання засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення контролю доступу.

Для захисту мереж від кіберзлочинців, найчастіше користуються технічними системами та засобами захисту інформації в корпоративних інформаційних системах. Як основний засіб захисту від атак через мережу Інтернет на локальну мережу - використовують Брандмауер (firewall). Ці пристрої використовуються, як для захисту мережі в цілому, так і для захисту окремих комп’ютерів у даній мережі.

У інформаційних системах брандмауер може бути на основі як програмного так і апаратного забезпечення, який забезпечує зв’язок між локальними (безпечними) та небезпечними (Інтернет) мережами.

Головна задача брандмауера – це перевірка трафіку, який проходить по усім каналам зв’язку, як захищених (SSH, SSL, TLS та ін.) так і незахищених (Telnet, http, SMTP на ін.). За допомогою відстеження мережевого трафіку він виявляє шкідливі програми (віруси, шпигунські програми і так далі) та блокує їх ще на вході у мережу.

Для захисту комп’ютера у мережі за часту використовуються антивірусні програми, які безпосередньо встановлюються на комп’ютер клієнта. Вони захищають інформацію людини від вірусів які проникають з мережі.

В даний час все частіше зустрічаються приклади використання цілих комплексів захисту інформації в мережі. Вони об’єднують як брандмауери, антивіруси так і постійний моніторинг трафіку в середині мережі та сповіщення про підозрілий контент.

З вище сказаного, можна зробити висновок, що технології захисту корпоративних інформаційних систем є необхідною мірою захисту в сучасному цифровому світі. Вони повинні постійно розвиватись та удосконалюватись, тому що кіберзлочинці все частіше знаходять нові і нові методи доступу до даних в мережі, з метою подальшого їх заволодіння.

Перелік посилань:

1. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013ю — 256 с.
2. Буров Є. В. Комп'ютерні мережі: підручник / Євген Вікторович Буров. — Львів: «Магнолія 2006», 2010. — 262 с.
3. Комп'ютерні мережі та телекомунікації : навч. посібник / В. А. Ткаченко, О. В. Касілов, В. А. Рябик. – Харків: НТУ "ХПІ", 2011. – 224 с.
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.

Самойленко Владислав Олексійович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

БЕЗПЕКА БАЗ ДАНИХ

Робота розкриває стратегії та практики захисту інформації в базах даних, включаючи аутентифікацію, шифрування та моніторинг. Вона підкреслює необхідність адаптації до змінюваних загроз для забезпечення цілісності, конфіденційності та доступності даних.

Безпека баз даних є критично важливою складовою стратегії інформаційної безпеки організації. Оскільки бази даних часто містять конфіденційну інформацію, таку як персональні дані, фінансові записи та інтелектуальну власність. Це робить бази даних привабливими цілями для кіберзлочинців. У зв'язку з цим, захист цих цінних ресурсів є пріоритетом для забезпечення конфіденційності, цілісності та доступності інформації.

До основних аспектів безпеки баз даних відносяться:

Аутентифікація та управління доступом. Це забезпечить те, що користувачі є тими, за кого вони себе видають, а також впевненість у тому, що вони мають доступ лише до тих даних, до яких вони мають права доступу. Це може включати механізми, такі як двофакторна аутентифікація та мінімізація прав доступу.

Шифрування даних. Шифрування бази даних і з'єднання, що передається між клієнтом та сервером, запобігає несанкціонованому доступу до даних, навіть якщо зловмисник отримує фізичний доступ до бази даних.

Резервне копіювання та відновлення. Регулярне резервне копіювання даних та розробка надійних планів відновлення після збоїв забезпечують відновлення баз даних без втрати даних у разі фізичних або технічних неполадок.

Аудит та моніторинг. Постійний моніторинг та аудит дій користувачів та системних подій в базі даних допомагають виявляти та реагувати на підозрілу поведінку, помилки конфігурації та спроби несанкціонованого доступу.

Оновлення та управління патчами. Регулярне оновлення баз даних та разом з цим програмного забезпечення для усунення відомих.

Роз'єднання обов'язків. Розділення обов'язків і функцій між різними особами або групами зменшує ризик зловмисних дій та помилок, оскільки вимагає більше ніж однієї особи для здійснення критичних дій.

Зробимо висновки. Ефективне застосування цих принципів та методів може значно зменшити ризики, пов'язані з безпекою баз даних, та забезпечити захист конфіденційних даних. Однак, у світі, де кіберзагрози постійно еволюціонують, важливо постійно оцінювати та оновлювати заходи безпеки, щоб вони відповідали сучасним викликам.

Перелік посилань:

1. Important aspects of database security URL: https://www.geopits.com/blog/important-aspects-of-database-security.html (дата звернення 04.04.2024)
2. Top 10 Database Security Best Practices URL: https://satoricyber.com/database-security/top-10-database-security-best-practices/ (дата звернення 05.04.2024)

Кубрак Володимир Олександрович
викладач, ІСЗЗІ КПІ ім. Ігоря Сікорського, Київ, Україна
Семерич Олена Сергіївна
студент, БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

АНАЛІЗ СУЧАСНИХ IDS ТА IPS ПРИ ПОБУДОВІ SOC

Вибір системи виявлення вторгнень - IDS та системи запобігання вторгненням - IPS відіграє ключову роль при побудові Security Operation Center. Вдалий вибір цих систем сприяє вчасному виявленню та блокуванню атак на мережевому рівні. Вони допомагають виявити аномальну активність в мережі та відреагувати на неї.

Сучасні системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) є ключовими компонентами в інфраструктурі кібербезпеки для виявлення та реагування на кіберзагрози. Ці системи використовуються для моніторингу та аналізу трафіку з метою ідентифікації активностей, а також для прийняття заходів щодо їх блокування.

Однак, IDS та IPS використовують різноманітні методи для виявлення потенційних загроз, включаючи аналіз сигнатур, евристичний аналіз, аналіз змісту пакетів та машинне навчання. Вони можуть виявляти не лише відомі атаки за відомими сигнатурами, але й аномальні патерни поведінки, що можуть вказувати на нові атаки або раніше невідомі загрози. Це дозволяє їм ефективно захищати мережеву інфраструктуру в реальному часі. [1]

Однією з ключових характеристик сучасних IDS/IPS є їх гнучкість і налаштовуваність. Адміністратори можуть налаштовувати правила та пороги виявлення відповідно до конкретних потреб та характеристик мережі організації. Це дозволяє максимально адаптувати систему до специфічних вимог безпеки організації та забезпечити ефективний захист від різноманітних загроз.

Більшість сучасних IDS/IPS також підтримують інтеграцію з іншими компонентами інфраструктури кібербезпеки, такими як системи управління інцидентами та безпеки (SIEM).

Не зважаючи на переваги, сучасні IDS/IPS також стикаються з викликами, такими як хибнопозитивні спрацьовування [2], завантаження мережі та необхідність постійного оновлення сигнатур та алгоритмів аналізу. Вирішення цих проблем вимагає ретельного налаштування та підтримки з боку кваліфікованих спеціалістів з кібербезпеки.

Отже, сучасні IDS та IPS відіграють важливу роль у забезпеченні безпеки мережі та інфраструктури організації, пропонуючи широкий спектр функціональності та гнучкість налаштування для ефективного виявлення та запобігання кіберзагрозам, а раціональний вибір таких систем дозволить збільшити якість та швидкість роботи Security Operation Center в умовах сучасних загроз та війни в кіберпросторі.

Перелік посилань:

1. A. Zhylin, M. Khudyncev, M. Litvinov, Functional model of cybersecurity situation center, Information Technology and Security. July-December 2018. Vol. 6. Iss. 2 (11), DOI: 10.20535/2411-1031.2018.6.2.153490.

2. I. Subach, V. Kubrak, and A. Mykytiuk, Methodology of rational choice of security incident management system for building operational security center, CEUR Workshop Proceedings, 2019, 2577, pp. 11–20.

Сидоренко Володимир Дмитрович
студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЇ ЗАХИСТУ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

В сучасних умовах значення захисту кінцевих точок у корпоративних системах зросло відносно до того, що було раніше, оскільки дедалі більше організацій працюють в онлайн середовищі та мають значні кількості конфіденційних даних, які необхідно захистити від небажаних атак зловмисників.

У контексті забезпечення кібербезпеки в організаціях кінцеві точки є потенційними місцями, через які зловмисники можуть проникнути до систем організацій та здійснити крадіжку конфіденційної інформації, вірусну атаку або інші злочинні дії.

Захист кінцевих точок організацій має велике значення в сучасному цифровому світі. Кінцеві точки, є потенційними вразливими місцями, через які зловмисники можуть отримати несанкціонований доступ до конфіденційної інформації, поширити шкідливі програми або завдати іншої шкоди організації. Зловмисники стають все винахідливішими та спритнішими в своїх атаках. Вони використовують різні методи, такі як шкідливі програми, фішинг, розповсюдження шкідливого програмного забезпечення та інші, щоб зламати безпеку кінцевих точок. Захист кінцевих точок допомагає запобігти таким загрозам і забезпечити безпеку організації.

У річному дослідженні, що проводила компанія Adaptive спільно з Ponemon Institute, було відзначено, що для більшості корпоративних IT-організацій управління пристроями стає проблемою, проте вони успішно вирішують її. Проте, до середини 2022 року через розподілену робочу силу IT-спеціалісти втратили значну кількість видимості пристроїв, які підключаються до їхніх мереж, і більшість з них (48%) залишається невідомою для спеціалістів. Це сталося переважно через те, що працівники стали менш передбачуваними, і IT-спеціалісти не можуть передбачити, де і коли працівники з'являться на роботі, на яких пристроях і т.д.

Сучасні технології ставлять IT-спеціалістів перед складним вибором: дозволити працівникам бути продуктивними в будь-якому місці, збільшуючи при цьому ризики для безпеки компанії, або змусити їх працювати в офісі, що може стати менш популярним у 2022 році та в майбутньому. Незважаючи на те, що 49% респондентів у дослідженні відмітили, що віддалена робоча сила ускладнює керування оновленнями безпеки та виправленнями, вони передбачають, що все більше компаній будуть користуватися розподіленою робочою силою. Якщо компанії бажають зберегти контроль над своїми децентралізованими кінцевими точками, то їм доведеться змінити свій підхід.

Фахівці з IT-операцій та IT-безпеки мають різні підходи до управління, що ускладнює спільну роботу. Наприклад, лише 40% фахівців з безпеки IT відзначили проблеми з віддаленою робочою силою, у порівнянні з 57% з IT-операцій. Команди IT-операцій зазвичай займаються профілактичними заходами, такими як управління кінцевими точками та встановлення виправлень, тоді як групи IT-безпеки сконцентровані на антивірусних заходах та виявленні та реагуванні на загрози.

У мережах організацій кінцеві точки (пристрої, такі як комп’ютери, мобільні телефони, ноутбуки і планшети) поширюються, що ускладнює боротьбу з кіберзагрозами, такими як вірусні атаки і фішинг. Середня організація, що взяла участь у дослідженні, має близько 135 000 кінцевих точок, з яких у середньому 48% (64 800) є під загрозою через невиявлення їх IT або застарілу операційну систему. Щорічно на захист кінцевих точок витрачається у середньому 4 252 500 доларів США, причому більшість витрат пов’язані з проблемами сумісності програмного забезпечення.

Використовуючи сучасне рішення для захисту кінцевих точок корпоративних систем можна досягти максимальної захищеності інформації.

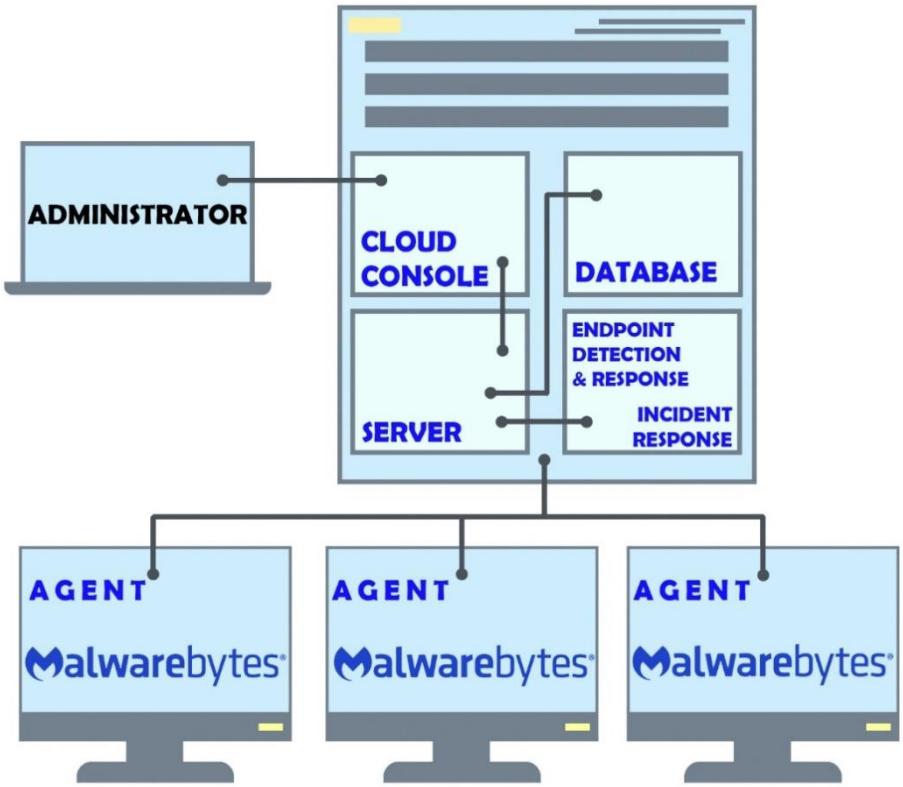


Рис. 1 – Архітектура корпоративної інформаційної системи на прикладі рішення Malwarebytes Endpoint Protection

Агент захисту кінцевих точок – це легкий програмний компонент, який встановлюється на кінцевих точках, включаючи настільні комп'ютери, ноутбуки та сервери. Він забезпечує захист від шкідливих програм та інших кіберзагроз у режимі реального часу. Агент використовує сканування на основі сигнатур, поведінковий аналіз та алгоритми машинного навчання для виявлення та блокування шкідливого програмного забезпечення.

Таким чином з наведених вище тез можна зробити наступні висновки:

Захист кінцевих точок у корпоративних системах є важливою складовою

сучасних стратегій кібербезпеки, оскільки організації все більше працюють в онлайн середовищі та зберігають значні обсяги конфіденційних даних. Кінцеві точки можуть стати вразливими місцями для атак зловмисників, що може призвести до крадіжки даних або поширення шкідливих програм.

Управління кінцевими точками стає складнішим через розподілену робочу силу, що може знизити видимість пристроїв, підключених до мережі організації. Це може збільшити ризики безпеки, оскільки працівники працюють з різних місць та пристроїв.

Незважаючи на це, сучасні технології захисту кінцевих точок, які використовують сканування на основі сигнатур, поведінковий аналіз та алгоритми машинного навчання, допомагають запобігти кіберзагрозам.

Таким чином, інвестування в сучасні технології захисту кінцевих точок є важливою складовою стратегії кібербезпеки для організацій у сучасному цифровому світі.

Перелік посилань:

1. Preyproject. «What is Endpoint Security?». June 15, 2021[Електронний ресурс] – Режим доступу: https://preyproject.com/blog/what-is-endpoint-security
2. Guidelines on Firewalls and Firewall Policy. Recommendations of the National Institute of Standards and Technology. Available online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

Силко С.С.
студент групи УБД-42 ННІЗІ ДУІКТ, Київ, Україна

МЕТОДИ УПРАВЛІННЯ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ НА ПІДПРИЄМСТВІ ВІДПОВІДНО ДО КОНЦЕПЦІЇ NIST

Мобільні пристрої відіграють важливу роль не лише у спрощенні робочих процесів, але й стають основними засобами доступу до корпоративної інформації. Однак це також збільшує ймовірність втрати або крадіжки пристроїв, атак з використанням шкідливого ПЗ і витоку конфіденційних даних.

Проблеми, пов'язані з безпекою мобільних пристроїв на підприємствах, включають недостатню контрольованість пристроїв, яка може виникати через дозвіл персоналу використовувати власні мобільні пристрої. Це ускладнює централізований контроль і може призвести до різних проблем, включаючи

втрату пристроїв або незаконний доступ до корпоративних даних. Друга проблема полягає у наявності вразливостей ПЗ мобільних пристроїв, які можуть бути використані зловмисниками для атак. Третя проблема - це втрата або крадіжка пристроїв, що може призвести до несанкціонованого доступу до конфіденційної інформації. Відсутність ефективного механізму реагування на інциденти безпеки також становить серйозну загрозу для підприємства [1].

Застосування концепції NIST до управління безпекою мобільних пристроїв на підприємстві є важливим етапом для забезпечення захисту конфіденційної інформації та запобігання потенційним загрозам безпеки. Ця концепція передбачає реалізацію комплексного підходу до управління безпекою, що включає кілька методів, серед яких: ідентифікація - вимагає ретельного аналізу та класифікації всіх мобільних пристроїв, які використовуються на підприємстві; захист - передбачає використання технічних та організаційних заходів для захисту пристроїв від несанкціонованого доступу й атак; виявлення - вимагає постійного моніторингу й виявлення можливих загроз і вразливостей; відповідь - передбачає швидку реакцію на виявлені загрози та вжиття необхідних заходів для їх ліквідації; відновлення - охоплює відновлення пошкоджених даних і функціональності системи після інциденту. Загальна мета полягає в забезпеченні ефективного управління безпекою мобільних пристроїв з метою забезпечення захисту важливих даних та мінімізації ризиків порушень безпеки [2].

Також фахівці NIST виділяють шість основних кроків, які повинні зробити підприємства, щоб керувати мобільними пристроями в безпечному середовищі:

1. Створення політики безпеки мобільних пристроїв, що визначає, які ресурси доступні через них і як керувати доступом.
2. Розробка моделей загроз для мобільних пристроїв і їх ресурсів з урахуванням їх особливостей.
3. Вибір послуг безпеки, що відповідають потребам компанії, інтеграція рішень.

4. Тестування рішень перед впровадженням з урахуванням різних типів пристроїв і їх функціональності.

5. Забезпечення повного захисту виданих пристроїв перед наданням доступу.

6. Регулярне оновлення та підтримка безпеки мобільних пристроїв, зокрема перевірка оновлень, синхронізація годинника і виявлення аномалій [3].

Мобільні технології на підприємствах надають доступ до даних, але вимагають управління безпекою. Застосування концепції NIST допомагає ідентифікувати ризики, розробляти політики безпеки та захищати дані. Такий підхід знижує загрози порушення безпеки та забезпечує цілісність і конфіденційність даних.

Перелік посилань:

1. 6 Steps to Secure Mobile Devices. URL: https://www.bankinfosecurity.com/6-steps-to-secure-mobile-devices-in-enterprise-a-5857

2. Guidelines for Managing the Security of Mobile Devices in the Enterprise. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2.pdf

3. Mobile Device Security: Corporate-Owned Personally-Enabled (COPE). URL: https://www.nccoe.nist.gov/sites/default/files/legacy-files/mdse-nist-sp1800-21a-final.pdf

Ситайло Родіон Романович
Студент групи УБДМ-51, ННІЗІ ДУІКТ, Київ, Україна

СТРАТЕГІЇ ПОДОЛАННЯ ПОВЕДІНКОВИХ ОБМЕЖЕНЬ У ПРОГРАМАХ НАВЧАННЯ ТА ПІДВИЩЕННЯ ОБІЗНАНОСТІ З СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ПІДПРИЄМСТВАХ

Дослідження ролі симуляційного навчання у свідомому реагуванні персоналу на соціальні інженерні загрози.

У контексті інформаційної безпеки соціальна інженерія це психологічне маніпулювання людьми з метою спонукання їх до виконання певних дій або розголошення конфіденційної інформації. Будучи різновидом обману з метою збору інформації, шахрайства або доступу до системи, вона відрізняється від традиційної "афери" тим, що часто є одним з багатьох кроків у більш складній схемі шахрайства.

Оскільки соціальна інженерія пов'язана з людськими можливостями, поведінкові обмеження працівників становлять виклик для ефективності програм навчання та підвищення обізнаності. Серед усіх працівників специфічні поведінкові обмеження включають упередження та культурний вплив. Дослідження виділяють поведінкові обмеження серед основних причин, що підвищують ймовірність соціально-інженерних атак в організаціях. Перш за все, невідповідна поведінка, що спостерігається серед працівників у процесі навчання та інформаційних програм, вважається однією з проблем, яку необхідно подолати для створення безпечної культури. У випадку витоку інформації про інформаційну безпеку, витрати компаній на його локалізацію можуть бути набагато вищими, ніж якби навчання розглядалося в першу чергу. Щоб протистояти таким поведінковим обмеженням і упередженням, організаціям необхідно встановити чіткі правила безпеки та ознайомити з ними весь персонал. Одна з ключових стратегій протидії таким викликам у програмах навчання та підвищенні обізнаності полягає в тому, що працівники повинні навчитися уникати переоцінки своїх можливостей щодо зменшення ризиків для безпеки. Натомість, за допомогою інформаційних програм слід навчити працівників, що вони можуть використовувати свої знання з безпеки для досягнення позитивного комплексного результату для загальної безпеки. Кампанії з підвищення обізнаності працівників повинні витіснити індивідуальну упередженість і усунути думки про те, що такі атаки "не трапляться зі мною".

Координація між членами команди є складним завданням у процесі навчання та в інформаційних програмах. Оскільки атаки соціальної інженерії динамічні та еволюціонують, організації прагнуть стримувати хакерські загрози, використовуючи сучасні методи навчання. Ці методи включають серйозні ігри, віртуальні лабораторії та тематичні інформаційні відео та модулі. Тим не менш, наявність спеціалізованих координаторів навчання з інформаційної безпеки, які обізнані з новітніми методами, є важливим превентивним заходом для зменшення вразливостей, спричинених недостатньою обізнаністю в питаннях безпеки. Координатори та інструктори повинні наголошувати на важливості розробки блок-схем стримування загроз, щоб конкретно інформувати всіх співробітників про те, хто і за який аспект відповідає контролю загроз. Стратегії стримування соціально-інженерних загроз включають проведення навчань з готовності, заснованих на спільних процесах реагування на інциденти. Дуже важливо скласти детальний опис взаємозалежності між різними командами організації. Вони повинні конкретно включати всі необхідні заходи в послідовності для сприяння програмам

навчання та підвищення обізнаності на базі фірми. Коротко кажучи, програми навчання та підвищення обізнаності сприяють розвитку здібностей персоналу, який, як очікується, бачитиме ширшу картину щодо стримування вразливостей організації. Також, для кращої координації дій у боротьбі з динамічними соціально інженерними атаками координатори та інструктори тренінгів повинні бути в курсі подій і регулярно відвідувати останні конференції, щоб краще знати, як розвивати внутрішні тренінги.

Зробимо висновки. Загрози соціальної інженерії використовують довіру та вразливість людської природи, що робить їх серйозним викликом для фахівців з кібербезпеки. Однак за допомогою правильних технологічних рішень організації можуть значно посилити свій захист від цієї оманливої тактики. Вдосконалені фільтри електронної пошти, багатофакторна автентифікація, поведінкова аналітика та інструменти безпеки на основі штучного інтелекту відіграють вирішальну роль у виявленні та запобіганні атакам соціальної інженерії.

Крім того, навчальні платформи з підвищення обізнаності про безпеку надають працівникам знання та навички, необхідні для розпізнавання та реагування на прояви соціальної інженерії. Оскільки тактика соціальної інженерії продовжує розвиватися, комплексний підхід, що поєднує технології, навчання співробітників та розвідку загроз, є важливим для боротьби з цими загрозами та захисту конфіденційної інформації. Інтегруючи технології як ключовий компонент своєї стратегії кібербезпеки, організації можуть створити потужний захист від загроз соціальної інженерії та захистити свої цифрові активи у все більш складному та взаємопов'язаному світі.

Перелік посилань:

1. Anderson, Ross J. (2008). Security engineering: a guide to building dependable distributed systems (2 ed.). Indianapolis, IN: Wiley. p. 1040. ISBN 978-0-470-06852-6.
2. Parsons, K.; McCormac, A.; Butavicius, M.; Pattinson, M.; Jerram, C. Determining employee awareness using the human aspects of information security questionnaire (hais-q). Comput. Secur. 2014, 42, 165–176. URL: https://doi.org/10.1016/j.cose.2013.12.003

Сич Микола Валентинович
Старший викладач, ННІЗІ ДУІКТ, Київ, Україна

КОНТЕЙНЕРИЗАЦІЯ ЯК ІНСТРУМЕНТ ОРГАНІЗАЦІЇ КІБЕРБЕЗПЕКИ СИСТЕМИ

З розвитком цифровізації кібербезпека продовжує бути критично важливою для організацій, які зіштовхуються з постійно розвиваючимися загрозами. Традиційні заходи безпеки забезпечують певний рівень захисту, вони часто виявляються недостатніми для

вирішення сучасних викликів безпеці та кіберзагроз. Технологія контейнеризації багатообіцяючий напрямок для забезпечення безпеки, що має певні переваги порівняно з традиційними віртуальними машинами (ВМ). Інкапсулюючи програми та їхні залежності в ізольованих середовищах, контейнери забезпечують надійний механізм захисту від несанкціонованого доступу та потенційних порушень безпеки.

Контейнери забезпечують мають певну перевагу над віртуальними машинами (ВМ Рис. 1) щодо організуції безпеки. На відміну від віртуальних машин, які вимагають окремої операційної системи для кожного працюючого екземпляра, контейнери використовують ядро (хост операційної системи), таким чином звужуючи поверхню атаки та пом'якшуючи наслідки порушення безпеки системи. У разі злому контейнера обмежується доступ до скомпрометованої програми чи служби, перешкоджаючи проникненню зловмисників у всю систему. Ця властивість - ізолювання контейнерів робить їх застосування обґрунтованим, особливо для захисту хмарних обчислень і великих об'ємів даних, де швидкість розгортання додатків має критичне значення.

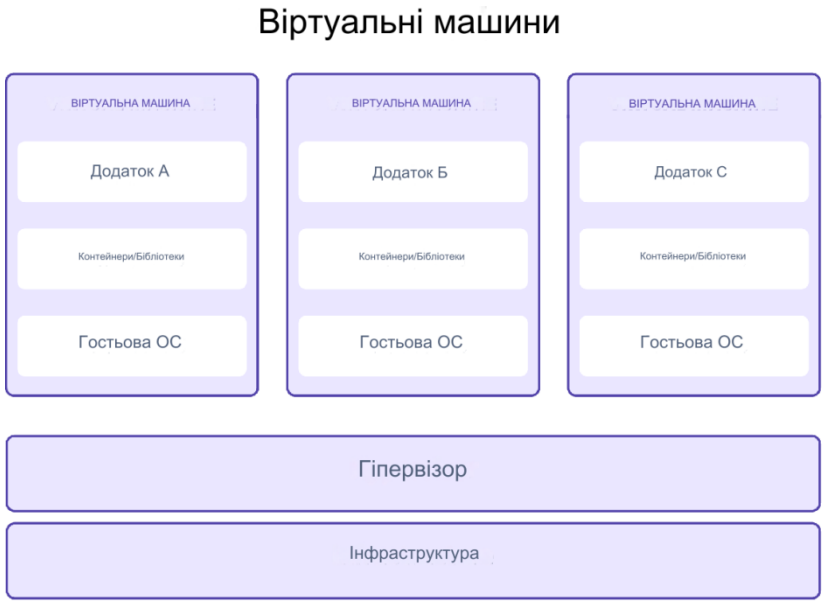


Рис. 1 - Віртуальні машини

Поверхня атаки описує потенційні шляхи, за допомогою яких зловмисник може скомпрометувати систему чи певну її службу. У контексті віртуалізації менша поверхня атаки передбачає менше точок входу для використання зловмисниками, що підвищує рівень безпеки всієї системи.

Ізоляція означає процес відокремлення компонентів або процесів у системі для запобігання втручанню або неавторизованому доступу у випадку, коли інша служба цієї системи була скомпрометована. У контексті контейнерів

ізоляція гарантує, що кожна програма або служба працює незалежно у своєму обмеженому середовищі, захищаючи їх від зовнішніх загроз.

Хмарні обчислення передбачають надання обчислювальних послуг, включаючи сервери, сховища, бази даних, віддалену мережеву інфраструктуру, програмне забезпечення тощо, клієнту через Інтернет, забезпечуючи масштабований віддалений доступ до ресурсі.

Великі дані (big data) передбачають обробку й аналіз величезних обсягів даних, які зазвичай характеризуються такими параметрами як обсяг, швидкість і різноманітність. Технології що використовуються для обробки великих даних спрощують зберігання, керування та аналіз масивних наборів даних, потребуючи відповідної швидкості роботи від програмного та апаратного забезбечення.

За останні роки технологія контейнеризації зазнала значних змін, у відповідь на потребу в гнучких і масштабованих системах. Такі платформи, як Kubernetes, стали еталонами в галузі, забезпечуючи розгортання та адміністрування контейнерів. Крім того, удосконалення цієї технології позитивно вплинуло на розвуток підходів з організації кібербезпеки, дозволивши ефективніше виявляти загрози та протидіяти їм.

Технології контейнеризації - це інструменти або фреймворки, призначені для автоматизації розгортання, масштабування та керування контейнерними програмами. Kubernetes є одним з прикладів, який забезпечує ефективну роботу контейнерів.

Організація кібербезпеки включає ряд методів і технологій, спрямованих на захист цифрових даних, систем і мереж від зловмисних дій, таких як несанкціонований доступ, витік даних внаслідок кібератак.

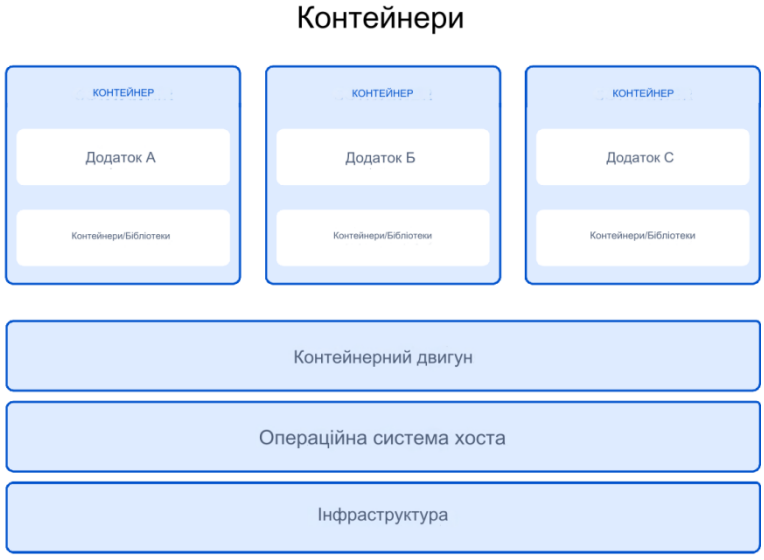


Рис. 2 - Віртуальні машини

Контейнери створюють нові можливості для досліджень у сфері кібербезпеки, створюючи середовище для експериментів і досліджень. Розгортаючи контейнери дослідники можуть відтворювати кіберзагрози, ретельно вивчати вектори атак і розробляти нову тактику захисту. Крім того, контейнери створюють відтворюване та контрольоване середовище для проведення експериментів, сприяючи спрощеній співпраці між дослідниками та поширенню ідей у сфері кібербезпеки. Завдяки використанню можливостей технології контейнеризації дослідники розвивають сферу кібербезпеки, сприяючи створенню більш надійних механізмів захисту.

Дослідження кібербезпеки - це включає вивчення та дослідження методів, методологій і технологій, спрямованих на підвищення безпеки цифрових систем і мереж від кіберзагроз.

Вектори атак - це шляхи або методи, за допомогою яких кібер-зловмисники отримують несанкціонований доступ до систем або мереж. Розуміння векторів атак має вирішальне значення для розробки ефективних стратегій захисту.

Механізми захисту охоплюють стратегії, інструменти та протоколи, які використовуються для захисту систем і мереж від кіберзагроз, наприклад системи виявлення вторгнень, брандмауери та протоколи шифрування.

У підсумку технології контейнеризації сприяють організації безпеки систем, забезпечуючи можливість швидкого розгортання систем та ізолювання їх окремих компонентів на відміну від звичайних віртуальних машин. Швидкий розвиток контейнерних технологій за останні роки сприяв розвитку технологій кібербезпеки, надавши фахівцям потужні ресурси для протидії загрозам, що розвиваються. Крім того, контейнеризація пропонує нові перспективи для дослідження аспектів кібербезпеки, надаючи можливість дослідникам впроваджувати інновації та поглиблювати співпрацю. З розвитком технологій контейнеризації відкриватимуться нові можливості для покращення та формуванні нових технології кібербезпеки.

Перелік посилань:

1. A. Celesti, D. Mulfari, M. Fazio, M. Villari, and A. Puliafito. "Exploring container virtualization in IoT clouds." In Smart Computing (SMARTCOMP), 2016 IEEE International Conference on, pages 1–6. IEEE, 2016.Привілейований доступ Delinea URL: https://channel4it.com/publications/ostann-onovlennya-delinea-server-suite-znizhu-rizik-zagroz-bekdoru-na-serverah.html (дата звернення 03.10.2023)

2. T. Bui. "Analysis of Docker Security." arXiv preprint arXiv:1501.02967, 2015.

3. Bernstein, D. "Containers and cloud: from LXC to Docker to Kubernetes." IEEE Cloud Computing, 1(3), 81–84 (2014).

Терно Ярослав Анатолійович
студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

БЕЗПЕКА ХМАРНИХ ТЕХНОЛОГІЙ

Безпека хмарних технологій (Cloud Security) - це сукупність заходів, процедур, політик та технологій, спрямованих на захист інформації, даних, інфраструктури та послуг, що знаходяться в хмарному середовищі. Оскільки хмарні технології передбачають збереження, обробку та передачу даних через інтернет і сторонні сервери, вони потребують особливої уваги до безпеки.

Якими хмарними сховищами ми найчастіше користуємося? Одними з найпопулярніших є Dropbox, Google Drive (Google Диск), Microsoft OneDrive та ICloud для користувачів технікою Apple. Існують також інші, маловідомі, хмарні сховища даних, та технологія роботи у них приблизно однакова. Важливо переконатися, що дані вашого Dropbox, Google Диска чи Microsoft OneDrive захищені, а доступ до них при цьому, як і раніше, простий та зрозумілий [1, 1].

Захищеність хмари проти безпеки в хмарі (Рис.1).

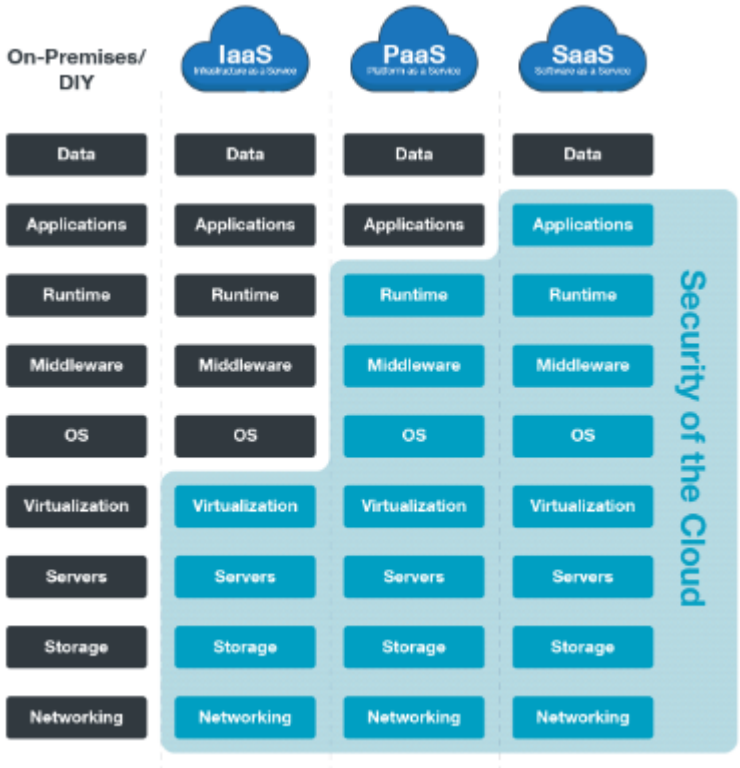


Рис.1.Безпеки в хмарі

Основні аспекти безпеки хмарних технологій включають:

Конфіденційність даних: Захист від несанкціонованого доступу до конфіденційної інформації, яка зберігається або передається через хмарне

середовище.

Цілісність даних: Забезпечення того, що дані не будуть змінені або псуватися без дозволу.

Доступність послуг: Гарантування доступності хмарних послуг для користувачів у всі часи, відвертаючи атаки на надійність мережі та інфраструктури.

Аутентифікація і авторизація: Забезпечення того, що лише авторизовані користувачі мають доступ до ресурсів хмарної платформи, і вони мають доступ лише до тих даних і функцій, які відповідають їх ролям і правам.

Мережева безпека: Захист від мережевих атак, таких як перехоплення даних, атаки з використанням зловмисних програм (малвари), атаки типу "человік-у-середині", і т.д.

Захист від DDoS-атак: Захист від атак типу "розподілене відмова в обслуговуванні", які можуть призвести до недоступності хмарних послуг.

Захист від іншими загрозами безпеки: Включаючи в себе заходи з протидії витокам даних, зловживанням привілеями, внутрішніми загрозами та іншими потенційними загрозами безпеки.

Управління ідентифікацією та ключами: Забезпечення безпеки процесів автентифікації та управління ключами шифрування для забезпечення конфіденційності та цілісності даних.

Відповідність з правовими нормами і регуляціями. Забезпечення відповідності з різноманітними законодавчими, регуляторними та стандартними вимогами щодо захисту даних та приватності.

Масштабування: На мережевому шлюзі розміщуються спеціальне обладнання для моніторингу передбачуваного трафіку і пристроїв. Однак сьогодні цього вже недостатньо. Щоб усунути прогалини в безпеці, організаціям потрібна єдина панель управління, яка забезпечує наочність і дозволяє сформувати узгоджені політики безпеки у всій інфраструктурі для ефективного управління ризиками. Рішення безпеки повинні обмінюватися і зіставляти відомості про загрози, отримувати і впроваджувати централізовано узгоджені політики і зміни в конфігураціях і координувати всі ресурси для своєчасного реагування на виявлені загрози. Окрім того, вони мають охоплювати всю розподілену інфраструктуру, динамічно масштабуватися при збільшенні ресурсів додатків і автоматично адаптуватися в міру пристосування інфраструктури до мінливих вимог. І, що не менш важливо, ці рішення повинні забезпечувати узгоджену функціональність і застосування політик незалежно від свого форм-фактору й місця розгортання.

Безпека під навантаженням: Захист робочих навантажень від

експлуатації, зловмисного програмного забезпечення та несанкціонованих змін — це складне завдання для адміністраторів хмар, оскільки навантаження постійно змінюється. Однак кожен елемент має бути видимим адміністратору хмари та керуватися політикою безпеки.

DevOps (Безпека контейнерів): Розробка додатків у хмарі стає все більш поширеною. Це означає, що контейнери повинні бути відскановані на предмет наявності шкідливих програм, вразливостей і порушень відповідності. Чим раніше ці перевірки безпеки робляться під час збирання системи, тим краще.

Додатки (Serverless, APIs, Web Apps): Традиційна безпека не може бути розгорнута на певних серверних або контейнерних платформах, але самі програми потрібно захищати так само надійно, як і інші частини інформаційної системи. Для багатьох компаній швидке та ефективне програмування та розгортання нових додатків є головними рушіями переходу до хмари. Але ці програми є потужними точками входу для загроз виконання веб-додатків, таких як введення коду, автоматизовані атаки та віддалені виконання команд.

Зберігання файлів: Компанії розглядають хмару, головним чином або частково, як спосіб вивантажити сховище з локальних серверів. Хмарне зберігання файлів чи об’єктів може стати джерелом зараження, якщо з будь-якої причини на нього було завантажено шкідливий файл. Сканування має бути доступним для будь-якого типу файлів, незалежно від розміру [2, 2].

Зробимо висновки. Ефективні аспекти безпеки хмарних технологій варіюються в залежності від конкретного хмарного середовища та типу послуг, які використовуються. Важливо, щоб організації, що використовують хмарні технології, розуміли ці аспекти та вживали відповідні заходи для забезпечення безпеки своїх даних та інфраструктури..

Перелік посилань:

1. Безпека хмарних сховищ і технологій. Основні правила.URL: https://datami.ua/bezpeka-hmarnih-shovishh-i-tehnologij-osnovni-pravila/ (дата звернення 25.08.2020)
2. **Хмарна безпека: ключові поняття, загрози та рішення** URL: https://sgs4business.com/news/khmarna-bezpeka-kliuchovi-poniattia-zahrozy-ta-rishennia.html (дата звернення 04.06.2020)

Хавер Анюта Вячеславівна
аспірантка групи АІКБ-11, Кафедри ІКБ ДУІКТ, Київ, Україна

ПРАКТИЧНЕ ВИКОРИСТАННЯ МОДЕЛІ PURDUE В АРХІТЕКТУРІ

ОБ’ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Стале функціонування об'єктів критичної інформаційної інфраструктури (ОКІІ) є особливо важливим і актуальним завданням, зважаючи на збройну агресію РФ, нестабільну геополітичну обстановку в світі та активне використання кіберпростору для відстоювання політичних інтересів держав з потужним кіберпотенціалом. Ряд причин робить ОКІІ пріоритетними цілями хакерських груп спонсорованих державами. Про це свідчить і аналіз наймасштабніших та найдеструктивніших кібератак більш ніж як за останнє дисятиліття. Це кібератаки спрямовані на операційні технологічні системи (ОТС) з застосуванням спеціального шкідливого програмного забезпечення: Stuxnet - 2010 рік, Industroyer - 2016 рік; Triton - 2017 рік. Дві останні з вищезгаданих кібератак спеціалісти з кібербезпеки пов'язують з діяльністю російських хакерських груп.

Враховуючи поточну кон'юнктуру в кіберпросторі важливо здійснювати ефективні заходи по забезпеченню кіберстійкості вже функціонуючих ОКІІ та при плануванні безпечної архітектури систем, що лише плануються до введення в експлуатацію.

Ключові слова: кібербезпека, кіберстійкість, об'єкти критичної інформаційної інфраструктури, модель Purdue, операційні технологічні системи, Industrial Control System (ICS), Supervisory Control and Data Acquisition (SCADA).

Все частіше корпоративні (IT) та промислові (ОТС) інформаційні системи ОКІІ стають конвергентними, що як додає зручності до управління бізнес процесами так і збільшує ризики пов’язані з кібератаками на критичні ОТС, кібератака на які може призвести до успішних деструктивних дій з боку суб’єктів кіберзагроз та значних фінансових збитків, а іноді і потенційно техногенних катастроф.

Найпоширенішими векторами кібератак на промислові інформаційні системи (ОТС) є:

кібератаки з Інтернет на безпосередньо підключені до нього пристрої промислової системи;

використання суб’єктами кіберзагроз викрадених облікових даних для віддаленого доступу у авторизованих користувачів;

кібератаки спрямовані на промислову інформаційну систему через зовнішній вебресурс з використанням експлойтів і вразливостей;

підключення зараженого мобільного пристрою до елементів (пристроїв) промислової інформаційної системи;

таргетовані фішингові надсилання спрямовані на встановлення присутності на автоматизованих робочих місцях корпоративних користувачів з подальшим переміщенням (leteral movement) вглиб до промислової інформаційної системи [1].

Одним із заходів спрямованих на підвищення рівня кібербезпеки підприємства є коректна сегментація корпоративної та промислової мереж. Концептуальною основою для сегментації корпоративних та промислових мереж є шестирівнева еталонна модель Purdue (Purdue Enterprise Reference Architecture (“PERA”)/“ISA-99”) (далі — модель, Рис.1), яка розроблена в 90-х роках в університеті Пердью (Purdue University). Модель враховують при побудові архітектури ОКІІ та використовують як складову глобальної концепції Defense-in-depth підприємства. Верхні рівні моделі (від 5 рівня до рівня 3.5) стосуються корпоративної зони та включають здебільшого типову IT-інфраструктуру. До рівнів промислової зони належать 3 — 0 рівні [2].

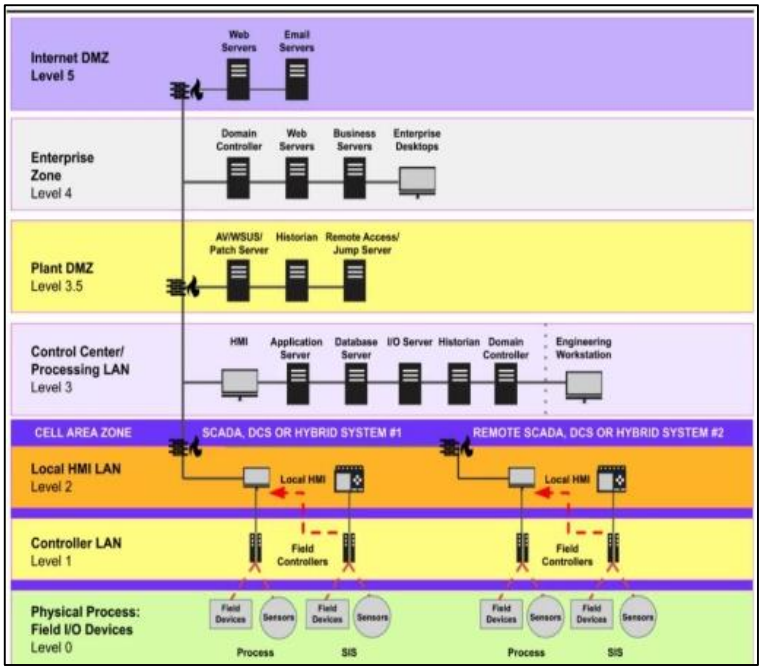


Рис.1 Приклад практичної реалізації Моделі Purdue

Варто відзначити, що існує декілька варіацій побудови та реалізації верхніх рівнів моделі, що залежить від специфіки та потреб для роботи самої корпоративної мережі підприємства. Розглянемо класичну модель, яка описана у виданні 2021 року “Industrial Cybersecurity Second Edition” Паскаля Акермана (Pascal Ackerman).

5 та 4 рівні моделі прийнято об'єднувати під назвою — Enterprice Security Zone.

На 5 рівні (Enterprise Network) прийнято розгортати бізнес-системи такі як Enterprice Resource Planning (ERP), Systems Applications and Products (SAP). Такі системи на п’ятому рівні можуть охоплювати декілька об’єктів підприємства чи підприємств та отримувати від них дані для звітування про загальний стан виробництва, запаси та попит для управління бізнес-рішеннями.

На 4 рівні (Site Business Planning and Logistics) зазвичай розгортаються IT-

системи, що підтримують виробничі процеси. На цьому рівні можуть бути розгорнуті: сервери баз даних, сервери додатків, сервери звітів, Manufacturing Execution System (MES), рішення Artificial intelligence/Machine learning (з подальшим застосуванням на рівні 3 моделі для оптимізації процесів виробництва), файлові сервери, клієнти електронної пошти, робочі столи супервізора і так далі.

Еволюційно, у ході виникнення необхідності об'єднання корпоративної та промислової зон, а також врахування стандартів таких як NIST Cybersecurity Framework, North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) до моделі було додано підрівень 3.5 (IDMZ), який представляє собою Industrial Demilitarized Zone і фактично розділяє IT та OTC інформаційні інфраструктури (інформаційні потоки), зазвичай з використанням двох фаєрволів різних виробників (Рис.3). Проте все частіше зустрічається використання діодів даних або їх поєднання з фаєрволами. Крім того, для підвищення рівня кіберстійкості на рівні 3.5 розгортаються IDS/IPS рішення. За фаєрволом цього рівня через комутатор може бути розгорнуто сервери віддаленого доступу, сервери реплікації баз даних, Network Time Protocol сервери (NTP), сервери передачі даних, Windows Server Update Service (WSUS) та інші сервери сервісів компанії. Однією з важливих функцій рівня 3.5 є обмін необхідною інформацією між OTC та бізнес (5-й рівень) чи IT-системами (4-й рівень) з рівня 3 та нижче.

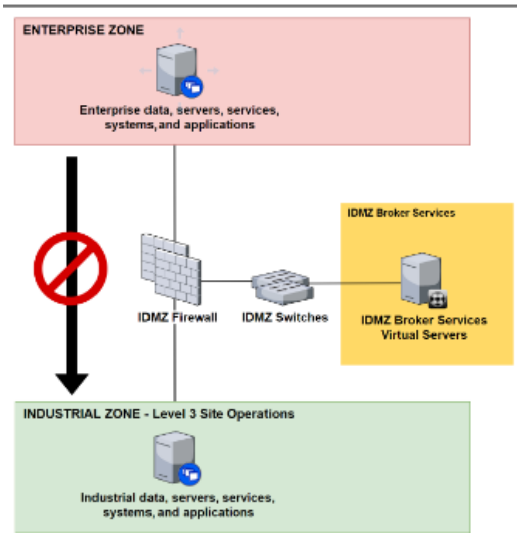


Рис. 3 Місце рівня 3.5 (IDMZ) у моделі Purdue

Від рівня 3 моделі — рівня операцій (Site Operation) розпочинається промислова інформаційна зона. Зазвичай рівень 3 взаємодіє з вищестоящими рівнями завдяки маршрутизатору. На цьому рівні знаходяться системи, які підтримують функції управління та моніторингу в масштабах підприємства. Розгорнуто взаємодію з загальними виробничими системами через централізовані

диспетчерські з Human-machine interface (HMI) та операторськими терміналами, які дають огляд усіх систем, що керують процесами на підприємстві. Оператор використовує HMI для виконання перевірки якості, керування часом безвідмовної роботи, моніторингу сигналів тривоги, подій і тенденцій. На 3 рівні також знаходяться пристрої, які надають інформацію IT-системам рівня 4. На цьому ж рівні розгортаються сервери збору та агрегації даних (Historian) які зберігають дані за певний тривалий проміжок часу зі SCADA-сервера (зазвичай за протоколом OPC — Open Platform Communications), сервери HMI, інженерні робочі станції, тощо [3].

На рівні 2 моделі — зона систем управління (Control Systems Zone) розгортаються програмні рішення SCADA (Distributed Control Systems — DCS), які контролюють фізичні процеси в промисловій зоні, агрегують дані та надсилають їх на Historian сервер рівня 3 моделі. HMI рівня 2 моделі підключаються до Programmable Logic Controller (PLC) щоб забезпечити базове керування та моніторинг технологічних процесів.

Рівень 1 моделі — базового керування (Basic controls) включає до свого складу пристрої (PLC) та системи для керування дискретними та аналоговими сигналами для забезпечення автоматизованого керування промисловим процесом (наприклад виробничою лінією) через пристрої які фізично знаходяться на 0 рівні моделі.

Рівень 0 моделі — фізичного процесу (Physical Processes) включає пристрої, які беруть участь у виробничому процесі такі як сенсори, датчики, приводи, двигуни та інш. Зазвичай ці елементи не мають вбудованих механізмів безпеки, але передають свої дані по ієрархії вище на інші рівні моделі, де їхня інформація враховується різними системами безпеки.

Враховуючи еталонну модель Purdue при побудові архітектури ОКІІ можна виконати ефективну та безпечну сегментацію корпоративної та промислової мереж, спроєктувати та впровадити ефективні механізми захисту від суб'єктів кіберзагрози на кожному з шести рівнів моделі, оптимізувати інформаційні потоки між підсистемами рівнів моделі та впровадити гнучкі і захищені бізнес-системи, які дозволять отримувати інформацію безпосередньо з технологічної зони для аналітики та покращення виробничих спроможностей (показників).

Перелік посилань:

1. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies – [Електрон.Ресурс] – Режим доступу: https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf;

2. What Is the Purdue Model for ICS Security (bxc-consulting.com) – [Електрон.Ресурс] – Режим доступу: https://www.bxc-consulting.com/blog/what-is-the-purdue-model-for-ics-security-2;

3."Industrial Cybersecurity Second Edition" – Pascal Ackerman, 2021. – 800 p.

Часовський Сергій Анатолійович
студент групи БСДМ-52, ДУІКТ, Київ, Україна

DATABASE SECURITY CHALLENGES AND SOLUTIONS

The modern infrastructures are dynamic and flexible, readily expanding resources in response to demand. This variability presents challenges in maintaining a solid security posture. Traditional security measures frequently face difficulties in adjusting to these changes, however when it comes to databases, the challenges extend beyond operational concerns, and dive into deeper complexities.

Databases store vast amounts of sensitive information ranging from personal data to financial records, making them demanded targets for cybercriminals. With the increasing complexity of cyber threats, modern database security faces numerous challenges. This essay explores the key issues of modern database security and discusses potential solutions to mitigate these risks.

Рис. 1 - Top database security threats

1. Cyber attacks

Cyber attacks pose a significant threat to the security of modern databases. These attacks include a wide range of malicious activities aimed at exploiting vulnerabilities in database systems to gain unauthorized access, steal sensitive information, or disrupt operations. Some of the most prevalent cyber attacks targeting databases include:

- SQL injection. These attacks remain one of the most common and damaging threats to databases. Attackers exploit vulnerabilities in web applications to inject malicious SQL queries into database servers, allowing them to retrieve, modify, or delete data stored in the database

- Malware. Malware, such as viruses, worms and trojans can infect database systems through various vectors, including email attachments, malicious websites, or compromised software. Once installed, malware can steal credentials, monitor user activity, or facilitate unauthorized access to sensitive data
- Ransomware. Ransomware attacks have become increasingly prevalent, targeting databases and encrypting critical data to extort ransom payments from victims. These attacks can disrupt business operations, cause financial losses, and damage the reputation of affected organizations
- DDoS attacks. Distributed Denial of Service (DDoS) attacks aim to overwhelm database servers with a flood of malicious traffic, rendering them inaccessible to legitimate users. By disrupting database services, DDoS attacks can disrupt business continuity and cause significant financial losses
- Zero-day exploits. Zero-day exploits target previously unknown vulnerabilities in database software, allowing attackers to bypass traditional security measures and compromise systems before patches or updates are available. Zero-day exploits pose a significant risk to databases, as organizations may be unaware of the vulnerability until it is actively exploited by attackers.

2. Insider threats

Insider threats present a significant challenge to the security of databases, as they involve individuals who have authorized access to sensitive information but misuse or abuse their privileges for malicious purposes or inadvertently compromise security due to negligence. Insider threats can appear in various forms, including:

- Malicious insiders. Malicious insiders are individuals within an organization who intentionally exploit their access to databases for personal gain, financial profit, or sabotage. These insiders may have privileged access to sensitive data and systems, allowing them to steal confidential information, manipulate data, or disrupt operations without being detected
- Negligent employees. Negligent employees pose a significant risk to database security, as they may inadvertently compromise sensitive information through careless actions or disregard for security protocols. Common examples of negligence include storing passwords in plaintext,

falling victim to phishing attacks, or improperly handling confidential data

- Compromised accounts. Insider threats can also originate from compromised user accounts, where attackers gain unauthorized access to databases using stolen credentials or exploiting vulnerabilities in authentication mechanisms. Once compromised, these accounts can be used to exfiltrate data, introduce malware, or escalate privileges within the database environment
- Third-party vendors and contractors. Third-party vendors and contractors with access to database systems can also pose insider threats if their credentials are compromised or if they misuse their access privileges. Organizations must carefully manage and monitor the activities of third-party entities to prevent unauthorized access and protect sensitive data from exploitation.

3. Compliance requirements

In the realm of modern database security, adherence to regulatory compliance standards is paramount. Various regulations and industry standards provide strict guidelines for protecting sensitive data stored in databases. Non-compliance with these requirements can result in severe penalties, legal ramifications, reputational damage, and loss of trust among customers and stakeholders. Some of the prominent compliance frameworks that organizations need to consider in database security include:

- GDPR (General Data Protection Regulation): GDPR is a comprehensive data protection law that governs the processing and handling of personal data of individuals within the European Union (EU) and the European Economic Area (EEA). Organizations that collect, store, or process personal data of EU/EEA residents must comply with GDPR's principles, which include obtaining explicit consent for data processing, implementing measures to ensure data security and privacy
- HIPAA (Health Insurance Portability and Accountability Act): HIPAA sets forth standards for protecting the privacy and security of protected health information (PHI) in the healthcare industry. Covered entities, including healthcare providers, health plans, and healthcare clearinghouses, must implement administrative, physical, and technical safeguards to safeguard PHI against unauthorized access, use, or disclosure

- PCI-DSS (Payment Card Industry Data Security Standard): PCI-DSS is a set of security standards designed to ensure the secure handling of credit cardholder data by merchants and service providers

4. Cloud security

With the adoption of cloud-based database solutions, organizations face unique security challenges related to data protection, access control, and secure integration with other cloud services. Ensuring the security of data stored in the cloud requires robust encryption, authentication mechanisms, and continuous monitoring.

5. Solutions to enhance database security

- Encryption. Encrypting data at rest and in transit helps protecting sensitive information from unauthorized access. Implementing strong encryption algorithms and key management practices ensures that data remains secure even if the database is compromised
- Access controls. Implementing strict access controls and role-based permissions limits the exposure of sensitive data to authorized users only. By enforcing the principle of least privilege, organizations can reduce the risk of insider threats and unauthorized access
- Patch management. Regularly updating database software and applying security patches is crucial for addressing vulnerabilities and preventing their exploitation. Automated patch management systems streamline the process of identifying and remedying security flaws in databases
- Database activity monitoring. Monitoring database activity in real-time allows organizations to detect suspicious behavior, unauthorized access attempts, and data exfiltration. Advanced monitoring solutions provide alerts and forensic capabilities to investigate security incidents promptly
- Regular audits and penetration testing. Conducting regular security audits and penetration testing helps identify vulnerabilities and weaknesses in database systems. By simulating real-world cyber attacks, organizations can proactively address security issues and fortify their defenses against complex modern threats.

Conclusion

Modern database security is a versatile challenge that requires a proactive and

layered approach to mitigation. By addressing issues such as cyber attacks, insider threats, data breaches, compliance requirements, and cloud security, organizations can strengthen the security state of their databases. By implementing robust security measures such as encryption, access control, patch management, monitoring, and regular audits, organizations can safeguard sensitive data and preserve the trust of their customers and stakeholders.

Перелік посилань:

1. ResearchGate. Security problems and solutions in databases article: https://www.researchgate.net/publication/369378336_SECURITY_PROBLEMS_AND_SOLUTIONS_IN_DATABASES
2. Free Learning Platform's. Challenges of database security article: https://www.javatpoint.com/challenges-of-database-security
3. Imperva Learning Center. Database Security article: https://www.imperva.com/learn/data-security/database-security/

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/.

Шайкова Анастасія Олегівна
Студентка групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ЕЛЕКТРОННОЇ ПОШТИ

У сучасному цифровому світі, де інтернет-злочинці постійно шукають способи доступу до особистої інформації, забезпечення захисту електронної пошти є надзвичайно актуальним. Це стає невід'ємною частиною, оскільки допомагає убезпечити дані від несанкціонованого доступу та атак з боку хакерів. Завдяки постійному розвитку та вдосконаленню технологій захисту, користувачі можуть бути впевнені у безпеці своєї електронної переписки та конфіденційності своєї інформації.

Безпека електронної пошти – це термін, що описує різні процедури та методи захисту облікових записів та комунікації електронної пошти від несанкціонованого доступу, втрати або компрометації.

Деякі з найпоширеніших типів атак на електронну пошту включають в себе наступні [1]:

Шахрайство: ці атаки через електронну пошту можуть набувати різних форм: від класичних шахрайських схем з передоплатою, спрямованих на звичайних людей, до повідомлень про компрометацію електронної пошти бізнесу, які мають на меті обдурити бухгалтерію великих підприємств і змусити їх переказати гроші на нелегальні рахунки. Часто зловмисник використовує підміну домену, щоб запит на переказ коштів виглядав так, ніби він надходить із законного джерела.

Фішинг: зловмисник намагається змусити жертву надати конфіденційну інформацію. Фішингові атаки можуть перенаправляти користувачів на фальшиву веб-сторінку, яка збирає облікові дані, або просто вимагати від користувача надіслати інформацію на електронну адресу, яку таємно контролює зловмисник. Підробка доменів також часто зустрічається в подібних атаках.

Шкідливе програмне забезпечення: типи шкідливих програм, що

надсилаються електронною поштою, включають шпигунські програми, рекламні програми, програми-вимагачі та інші. Зловмисники можуть доставляти шкідливе програмне забезпечення електронною поштою кількома різними способами. Один з найпоширеніших – включення в електронний лист вкладення, яке містить шкідливий код.

Захоплення облікового запису: зловмисники захоплюють поштові скриньки законних користувачів з різними цілями, наприклад, для моніторингу їхніх повідомлень, крадіжки інформації або використання законних адрес електронної пошти для перенаправлення атак шкідливого програмного забезпечення та спаму своїм контактам.

Існують спеціальні типи записів DNS, які допомагають гарантувати, що електронні листи надходять з легітимного джерела, а не від підставних осіб: SPF-записи, DKIM-записи та DMARC-записи. Постачальники послуг електронної пошти перевіряють електронні листи за всіма трьома цими записами, щоб переконатися, що вони надійшли саме з того місця, звідки, як вони стверджують, і не були змінені під час транспортування [1].

SPF (Sender Policy Framework). Запис SPF – це запис DNS, що містить IP-адреси офіційних поштових серверів і доменів організації, які можуть надсилати електронні листи від імені бізнесу [2].

SPF перешкоджає кіберзлочинцям підробляти домен, а спам-фільтри з меншою ймовірністю будуть вносити його до чорного списку. Якщо використовується стороння поштова система для керування електронною поштою, потрібен SPF-запис, який повідомляє поштові сервери одержувачів, що відправник уповноважений надсилати повідомлення від імені компанії.

DKIM (Domain Keys Identified Mail). Це система автентифікації електронної пошти, яка забезпечує цілісність і безвідмовність за допомогою криптографічних підписів [2].

Протокол DKIM створює криптографічний підпис для кожного повідомлення, що надсилається одержувачам, а також підпис домену, який додають у заголовок повідомлення. Цей підпис використовується одержувачем для перевірки того, що повідомлення дійсно було надіслано власником домену, а не кимось іншим. Він також підтверджує, що повідомлення не було підроблено на шляху від відправника до одержувача.

Якщо вони не збігаються, то: а) повідомлення було змінено під час передачі, або б) повідомлення відправляється від імені іншої людини, яка має доступ до закритого ключа сервера-відправника.

У таких випадках розбіжності підписів DKIM не дозволить доставити ці листи адресатам, оскільки вони не зможуть підтвердити їх як легітимні

повідомлення.

DMARC (Domain-based Message Authentication, Reporting & Conformance). Перевірка автентичності відправника електронного листа, заснована на протоколах DKIM і SPF [2].

SPF, DKIM і DMARC – це важливі технології для захисту електронної пошти від шахраїв та спамерів. Їх використання допомагає у підвищенні безпеки та довіри до електронної пошти.

Перелік посилань:

1. What is email security? [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudflare.com/learning/email-security/what-is-email-security/.
2. Thobson Technologies. (2020, 5 листопада). How DKIM SPF & DMARC Work to Prevent Email Spoofing [Відео]. YouTube. https://www.youtube.com/watch?v=c9fLp5uIxp8&t=87s&ab_channel=ThobsonTechnologies.

Шандровський Ярослав Ігорович
студент групи БСД-41, ННІЗІ ДУІКТ, Київ, Україна

Впровадження PAM для захисту корпоративних інформаційних систем від несанкціонованого доступу

Сучасні організації стикаються зі складними викликами у сфері кібербезпеки, що вимагають негайних та ефективних заходів для захисту інформаційних ресурсів.

Першим із цих викликів є складність IT-середовища, де кожен користувач має певний рівень привілеїв, а процеси автоматизації зробили системи ще вразливішими.

По-друге, зловмисники використовують нові технології, атакуючи системи інноваційними методами для здійснення більш ефективних атак.

По-третє, різноманіття технологічних постачальників рішень захисту може створювати додаткові проблеми.

Такий ландшафт створює різноманітні точки вразливості для несанкціонованого доступу, що становить серйозну загрозу безпеці даних та систем, тому усі ці виклики вимагають цілеспрямованих та комплексних рішень.

Несприятливі наслідки кібератак продовжують ставати серйозною загрозою для сучасних організацій, незважаючи на величезні зусилля, які вони вкладають у забезпечення безпеки своєї інфраструктури. Зловмисникам все ще вдається отримати несанкціонований доступ до корпоративних інформаційних систем, що часто призводить до крадіжки конфіденційних даних та інших важливих ресурсів.

Крім того, як це свідчить звіт компанії Apple, спостерігається тенденція зростання кількості таких інцидентів з кожним роком (у глобальному масштабі кількість жертв у 2023 році зросла вдвічі порівняно з 2022 роком), що свідчить про недостатню ефективність захисних заходів та потребу в удосконаленні

підходів до кібербезпеки [1].

Проте, чому не вдається повністю захистити інформаційні системи від кіберзагроз? Що саме перешкоджає всім цим колосальним зусиллям у досягненні мети? Ці запитання є на чолі досліджень та обговорень у галузі кібербезпеки. Нерідко вони ведуть до відкриття ключових причин, які лежать в основі зростання інцидентів несанкціонованого доступу до інформаційних систем організацій, що веде до витоків даних.

Таким чином, зважаючи на стан розвитку сучасної IT-індустрії, основними факторами, що спричиняють такі інциденти, можна виділити:

Складність IT-інфраструктури. Складність IT-інфраструктури сьогодні стає однією з найбільш актуальних проблем у сфері кібербезпеки. Розвиток технологій призводить до зростання кількості систем, сервісів та пристроїв, що використовуються в організаціях. За світовими дослідженнями, проведеними компанією CrowdStrike, більшість витоків даних (до 80%) відбуваються через використання викрадених або скомпрометованих облікових даних [2].

Проте, як саме складність IT-інфраструктури призводить до таких проблем?

- Надмірний доступ: Перевантажені адміністратори можуть намагатися підвищити продуктивність та зменшити рівень стресу серед користувачів, надаючи надмірний доступ. Аккаунти з надлишковими привілеями потім можуть бути забуті або не контролюватися.
- Поступове наростання привілеїв: Коли працівники отримують підвищення або змінюють ролі в компанії, вони часто зберігають доступ до систем, які вже не потрібні. Без моніторингу такі системи залишаються без управління та можуть забуватися з часом.
- Zombie-аккаунти: Також відомі як залишені або відкинуті аккаунти, вони з'являються, коли працівник покидає компанію, а привілеї доступу не утилізуються.

Розширення ландшафту загроз. Загрози кібербезпеки постійно зростають, а хакери постійно вдосконалюють свої методи атак. Отримання несанкціонованого доступу, є одним із найбільш актуальних і небезпечних аспектів цього росту. За допомогою автоматизації інформаційні атаки стають широко поширеними і ефективними. Так, у своїй підборці “top ten”, OWASP виділяє два ризики, пов'язані з несанкціонованим доступом з використанням облікових даних (один з яких займає перше місце) [3].

Зловмисники використовують різноманітні методи для злому привілейованих облікових записів, підвищення своїх привілеїв та отримання несанкціонованого доступу до чутливих систем та даних. Деякі поширені вектори загроз привілеїв включають в себе наступні:

- Атаки на паролі. Атаки грубої сили, підбір паролів або крадіжка облікових даних для отримання доступу до привілейованих облікових записів.
- Підвищення привілеїв. Використання вразливостей або неправильних конфігурацій для підвищення привілеїв від звичайного користувача до привілейованого облікового запису.
- Крадіжка облікових даних. Викрадення привілейованих облікових даних за допомогою фішингу, соціальної інженерії або шкідливого програмного забезпечення.

Різноманітність рішень у сфері захисту інформації. Існує велика кількість постачальників рішень захисту, кожен з яких пропонує свої технології для вирішення окремих аспектів проблеми несанкціонованого доступу. Проте небезпека полягає в тому, що жоден з цих постачальників не бере цілісного погляду на інфраструктуру IT компанії.

Недоліки такого підходу можуть бути серйозними і призвести до ризиків та викликів при впровадженні:

- Складність. Деякі рішення захисту складні у розгортанні та управлінні, що вимагає ретельного планування та інтеграції з існуючими системами.
- Опір користувачів. Користувачі з привілейованим доступом можуть чинити опір впровадженню захисних рішень через зміни в їхніх робочих процесах.
- Неправильні конфігурації. Неправильно налаштовані системи захисту можуть призвести до збоїв у критично важливих процесах або ненавмисного підвищення привілеїв.

Таким чином, на основі поставлених викликів у сфері захисту інформаційних систем можна зробити висновок, що впровадження захисних рішень управління привілейованим доступом (PAM) виявляється найбільш ефективним рішенням для боротьби з цими проблемами. PAM дозволяє ефективно керувати доступом до критичних ресурсів, обмежувати ризики несанкціонованого доступу та підвищувати загальний рівень безпеки.

Деякі найкращі практики впровадження PAM в організації включають в

себе наступні:

- Впровадження принципу найменших привілеїв. Цей принцип передбачає, що користувачам повинні надаватись тільки ті привілеї, які є необхідними для виконання їх робочих обов'язків, без надання зайвих прав доступу. Це допомагає обмежити потенційний шкідливий вплив користувачів та зменшити ризики витоку даних чи несанкціонованого доступу.
- Централізоване керування обліковими записами. Функція єдиного входу (SSO) для корпоративних ресурсів забезпечує централізовану видимість і керування корпоративними обліковими записами.
- Використання багатофакторної автентифікацію (MFA). Ефективний метод забезпечення безпеки облікових записів шляхом вимоги введення двох або більше форм ідентифікації перед наданням доступу. Це може включати щось, що користувач знає (наприклад, пароль), щось, що він має (такий як фізичний пристрій або ключ), або щось, що він є (наприклад, біометричні дані).
- Політика безпеки з нульовою довірою (ZT). Політика безпеки з нульовою довірою вимагає, щоб усі запити на доступ до корпоративних даних або ресурсів розглядалися в індивідуальному порядку. Це допомагає гарантувати, що всі запити є санкціонованими, і забезпечує видимість того, як використовуються привілейовані облікові записи.

Перелік посилань:

1. Professor Stuart E. (2023) The Continued Threat to Personal Data, United States.
2. Kurtz G. (2024) CrowdStrike 2024 GlobalThreat Report, United States.
3. OWASP Top Ten URL: https://owasp.org/www-project-top-ten/ (дата звернення 10.04.2024)

Швиденко Богдан Геннадійович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

ВАЖЛИВІСТЬ ПРОТИДІЇ СПАМУ У КОРПОРАТИВНІЙ МЕРЕЖІ

Електронна пошта є найпоширенішим методом і відправною точкою атак, спрямованих на організації. Антиспам виявляє та фільтрує електронні листи зі спамом за допомогою комплексного багаторівневого захисту.

Антиспам — це програмне забезпечення, метою якого є виявлення та блокування потенційно небезпечних електронних листів із скриньок вхідних

повідомлень користувачів. Протоколи захисту від спаму визначають, що таке небажане та небажане повідомлення (спам); у багатьох випадках спам - це рекламований продукт, який багато з яких є законним (хоча все ще небажаним) або шкідливим. Програмне забезпечення для захисту від спаму використовує фільтри, які дозволяють лише відомим і схваленим адресам електронної пошти отримувати доступ до папок "Вхідні" користувачів. Програмне забезпечення для захисту від спаму зазвичай дозволяє переглядати електронну пошту, класифіковану як спам, у випадку, якщо вона неправильно визначила законну електронну пошту.

Загалом кажучи, програмне забезпечення для захисту від спаму використовує три методи боротьби зі спамом:

- Ініційоване користувачем визначення спам-адрес електронної пошти.
- Автоматична ідентифікація спаму адміністраторами та/або користувачами.
- Спам, виявлений дослідниками та представниками правоохоронних органів.

Кіберзлочинці сприймають спам, тому що він дешевий, ефективний і успішний, часто достатньо прибутковий – про це свідчать 300 мільярдів спам-повідомлень, які надсилаються щороку. Хоча деякі електронні листи зі спамом можуть просто підірвати продуктивність співробітників, увесь спам може стати причиною фішингу, програм-вимагачів, вірусів та інших шкідливих дій.

Спам став критичним вектором мережевих атак і, отже, головною проблемою мережевих адміністраторів. Співробітник, який взаємодіє зі спамом, може призвести до захоплення одного або кількох облікових записів, викрадання даних або іншого подібного серйозного результату. Крім того, як і інші розробники зловмисного програмного забезпечення, спамери постійно адаптуються та розвиваються, щоб уникнути виявлення та підвищити ефективність.

Вихідний спам викликає ще одне занепокоєння. Спамери часто використовують ботнети для своєї роботи, і корпоративний комп’ютер може стати скомпрометованим і почати викидати спам через корпоративний домен. Це може завдати шкоди репутації домену організації, що може призвести до серйозних наслідків, наприклад блокування електронної пошти з домену організації, що призведе до видалення законної електронної пошти. Крім того, вихідний спам може порушувати нормативні вимоги, вилучати конфіденційні дані тощо.

Сервери електронної пошти, як на місці, так і в хмарі, пропонують низку засобів захисту від спаму, як-от фільтрування вмісту, чорні списки, спам-пастки та інші. Кожна з цих технік має свої сильні та слабкі сторони. Незважаючи на те, що антиспам на основі сервера може використовувати кілька різних методів, однак функціонально це все одно єдиний рівень захисту від спаму.

Зловмисники використовують спам, щоб заманити користувача на шкідливі сайти або залучити до фінансових шахрайств.

Рішення для захисту від спаму також включає класифікацію в реальному часі з унікальною архітектурою оновлення «витягування» (на відміну від «виштовхування»). Це безперервне оновлення дозволяє обробляти близько 75% класифікації спаму через локальний кеш, прискорюючи пропускну здатність і загальну продуктивність.

Програмне забезпечення для боротьби зі спамом зазвичай поєднує різні методи виявлення та блокування спам-повідомлень. Ці техніки включають:

- Фільтрування вмісту

Фільтрування вмісту дозволяє програмному забезпеченню для захисту від спаму сканувати вміст повідомлення, щоб визначити конкретні ключові слова чи фрази, які зазвичай використовуються в електронних листах зі спамом і спливаючих повідомленнях. Потім програмне забезпечення блокує або поміщає ці типи вмісту в окремі папки для перегляду.

- Чорні та білі списки

Чорний список передбачає ведення списку відомих відправників спаму або доменів і блокування повідомлень від них. Білий список, з іншого боку, передбачає дозвіл на повідомлення лише від схвалених відправників або доменів.

Програмне забезпечення для захисту від спаму підтримує список відомих відправників спаму, які можуть бути автоматично заблоковані. Подібним чином він може підтримувати білий список довірених відправників, чиї повідомлення завжди пропускаються. Додавання до сірого списку тимчасово відхиляє вхідні повідомлення та вимагає від відправника повторити спробу пізніше, оскільки законні відправники зазвичай повторюють спробу, тоді як спамери часто цього не роблять.

- Аналіз репутації

Аналіз репутації аналізує репутацію IP-адреси, імені домену та інших характеристик відправника, щоб визначити ймовірність того, що повідомлення надійшло з підозрілих джерел. Якщо відправник має погану репутацію, його повідомлення може бути заблоковано або відфільтровано.

- Евристичний аналіз

Евристичний аналіз використовує алгоритми машинного навчання для аналізу вмісту та характеристик повідомлень, щоб визначити шаблони, які зазвичай зустрічаються в спамі. Якщо повідомлення містить ці шаблони, воно може бути заблоковано або відфільтровано.

У сучасному цифровому світі заходи боротьби зі спамом мають вирішальне значення для захисту від ризиків електронної пошти зі спамом, включаючи зловмисне програмне забезпечення, фішинг та інше шахрайство. Для особистого чи бізнес-користування технологія захисту від спаму є важливим інструментом кібербезпеки для забезпечення безпечного та ефективного спілкування електронною поштою. Переваги програмного забезпечення для боротьби зі спамом роблять його безпрограшним для організацій у всіх галузях, тому воно має бути обов'язковим.

Перелік посилань:

1. Why You Need Anti-Spam in Your NGFW | Hillstone Networks. *Hillstone Networks*. URL: https://www.hillstonenet.com/blog/why-you-need-anti-spam-in-your-ngfw/ (дата звернення: 02.04.2024).

2. Anti-Spam 101: A Complete Cybersecurity Safety Guide. *Business Software Reviews at Wheelhouse | 2024*. URL: https://www.wheelhouse.com/resources/anti-spam-101-a-complete-cybersecurity-safety-guide-a11428 (дата звернення: 03.04.2024).

3. What is Anti-Spam? | Anti-Spam Software. *Mimecast*. URL: https://www.mimecast.com/content/anti-spam-software/ (дата звернення: 03.04.2024).

Шевчук Владислав Ігорович
Студент групи БСДМ-53, ННІЗІ, ДУІКТ, Київ, Україна

РОЗСЛІДУВАННЯ КІБЕРІЦИДЕНТІВ ЧЕРЕЗ ПРИЗМУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

За останні десятиліття кількість користувачів Інтернету швидко зростає, а разом з цим і кількість кіберінцидентів по всьому світу. Щодня мільйони людей та організацій стають жертвами кібератак, що призводить до значних втрат даних, фінансових втрат та порушень приватності. За таких умов важливо розробляти та вдосконалювати методи розслідування кіберінцидентів, щоб забезпечити ефективний захист користувачів та мережі в цілому.

Протягом останнього десятиріччя збільшення користувачів Інтернету спричинило нестримні тенденції, що породжують нові виклики у сфері кібербезпеки. Цей експоненціальний приріст викликає великий потік кіберінцидентів, які атакують як окремих користувачів, так і корпоративні та

державні системи. Щодня мільйони людей і компаній стають жертвами хакерських атак, зловмисники використовують широкий спектр методів для отримання доступу до конфіденційної інформації, викрадення особистих даних, а також вчинення шкоди фінансовим ресурсам.

Така ситуація потребує постійного удосконалення та вдосконалення методів розслідування кіберінцидентів, щоб забезпечити ефективний захист в цифровому просторі. Відповідно, індустрія кібербезпеки активно працює над розвитком та впровадженням технологій штучного інтелекту для розпізнавання, виявлення та відповіді на загрози, що дозволяє більш швидко та ефективно реагувати на кібератаки та мінімізувати їхні наслідки.

Розслідування кіберінцидентів за допомогою технологій штучного інтелекту складається з різноманітних аспектів, оскільки цей процес включає в себе широкий спектр методів та підходів. Використання штучного інтелекту у розслідуванні кіберінцидентів дозволяє аналізувати великі обсяги даних та виявляти складні зв'язки, які можуть залишитися непоміченими за допомогою традиційних методів. Завдяки вдосконаленій технологічній оснащеності та алгоритмам машинного навчання, розслідувачі можуть ефективно реагувати на загрози та вчасно приймати заходи для захисту від кібератак.

Ефективність штучного інтелекту в розслідуванні кіберінцидентів полягає у його здатності аналізувати великі обсяги даних з високою швидкістю та точністю. Штучний інтелект може автоматизувати процеси виявлення аномального поведінки, виявлення загроз та прогнозування майбутніх атак на основі аналізу попередніх інцидентів. Додатково, штучний інтелект може використовувати машинне навчання для постійного вдосконалення своїх алгоритмів та адаптації до нових видів загроз, що робить його надзвичайно потужним інструментом у сфері кібербезпеки.

Штучний інтелект здатний адаптуватися до тенденцій зростання кіберінцидентів та розвитку нових загроз шляхом постійного навчання та аналізу даних. Це означає, що системи штучного інтелекту можуть ефективно виявляти та реагувати на нові типи атак навіть без значного втручання людини. Крім того, завдяки автоматизованим алгоритмам та інтелектуальним системам, які працюють у реальному часі, ШІ може надавати захист навіть менш кваліфікованим користувачам, забезпечуючи безпеку їхніх цифрових пристроїв та мережі. Це дозволяє зменшити ризик кібератак та забезпечити більшу безпеку в Інтернеті для всіх користувачів.

У підсумку, використання штучного інтелекту в розслідуванні кіберінцидентів виявляється ключовим фактором у забезпеченні безпеки в Інтернеті. Його ефективність полягає у здатності забезпечити високий рівень

захисту користувачів та організацій, навіть у складних та змінних цифрових середовищах. Інтелектуальні системи і алгоритми машинного навчання дозволяють швидко і точно виявляти загрози, забезпечуючи навіть менш кваліфікованим користувачам надійний захист. Такий підхід відкриває нові перспективи для забезпечення цифрової безпеки та захисту приватності в онлайн-середовищі.

Шпортко Дмитро Вікторович
студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

Кіберінцидент – це одна або кілька подій безпеки, які поставили під загрозу безпеку інформації або послуг інформаційної системи.

Кібератака – це навмисна дія особи чи групи, мета якої – порушити доступність, конфіденційність або цілісність даних за допомогою інформаційно–комунікаційних технологій.

Актуальність дослідження випливає з того, що інформаційні технології стають все більш інтегрованими та взаємозалежними у сучасних організаціях і відіграють ключову роль у їх ефективному функціонуванні. Одночасно з цим розвиток технологій відкриває нові можливості для кіберзлочинців, що призводить до ускладнення кібератак. Традиційні методи захисту периметра, такі як брандмауери та системи виявлення вторгнень, вже не вистачають для забезпечення безпеки бізнесу. Зі зростанням кількості та різноманітності послуг IT стає неможливим для фахівців з кібербезпеки контролювати та відстежувати їхню діяльність вручну, щоб забезпечити безпеку бізнесу. Тут виникає необхідність в системах безпеки та керування подіями як основного інструменту для цього.

Комп’ютерні мережі створюються з високим рівнем складності, і мережі структуровані з різними рівнями, функціональність яких включає підтримку безпеки даних. Сучасні мережі та їх відповідна вразливість можуть дозволити зловмиснику вплинути на безпеку інформації. Відповідна система управління системною інформацією та подіями може надати всі засоби для керування інформаційною безпекою, допомагаючи в ефективному аналізі трафіку та ідентифікації та дослідженні кіберінцидентів за допомогою програмного забезпечення. Це програмне забезпечення призначене для сповіщення про

незвичайні події після аналізу та кореляції вхідних журналів з різних систем і пристроїв.

У звичайній практиці брандмауери, IPS та IDS розроблені для виявлення конкретних сигнатур атак у мережевому трафіку. Вони контролюють певні аспекти мережевого периметру, а також обробку мережевого трафіку, такого як TCP/IP пакети, VPN трафік, і т.д. Однак, традиційні методи не враховують нові форми атак, такі як IoT пристрої, і не ефективні у виявленні змін в мережевій активності.

Зокрема, попередні покоління IDS/IPS-брандмауерів спрощують виявлення аномалій шляхом порівняння з відомими атаками та новими IP-адресами, проте цей підхід обмежений. Зловмисники постійно адаптуються, використовуючи легітимні дані та інструменти, що вже є в мережах, що створює серйозні загрози. Відповідно, розроблено продукти аналізу мережевого трафіку, які ефективно виявляють нові форми атак. З впровадженням хмарних обчислень, DevOps та IoT, підтримка прозорості мережі стала складнішою.

Спираючись на минулий досвід було виявлено, що більш сучасні підходи допомагають комплексно реагувати на кіберінциденти

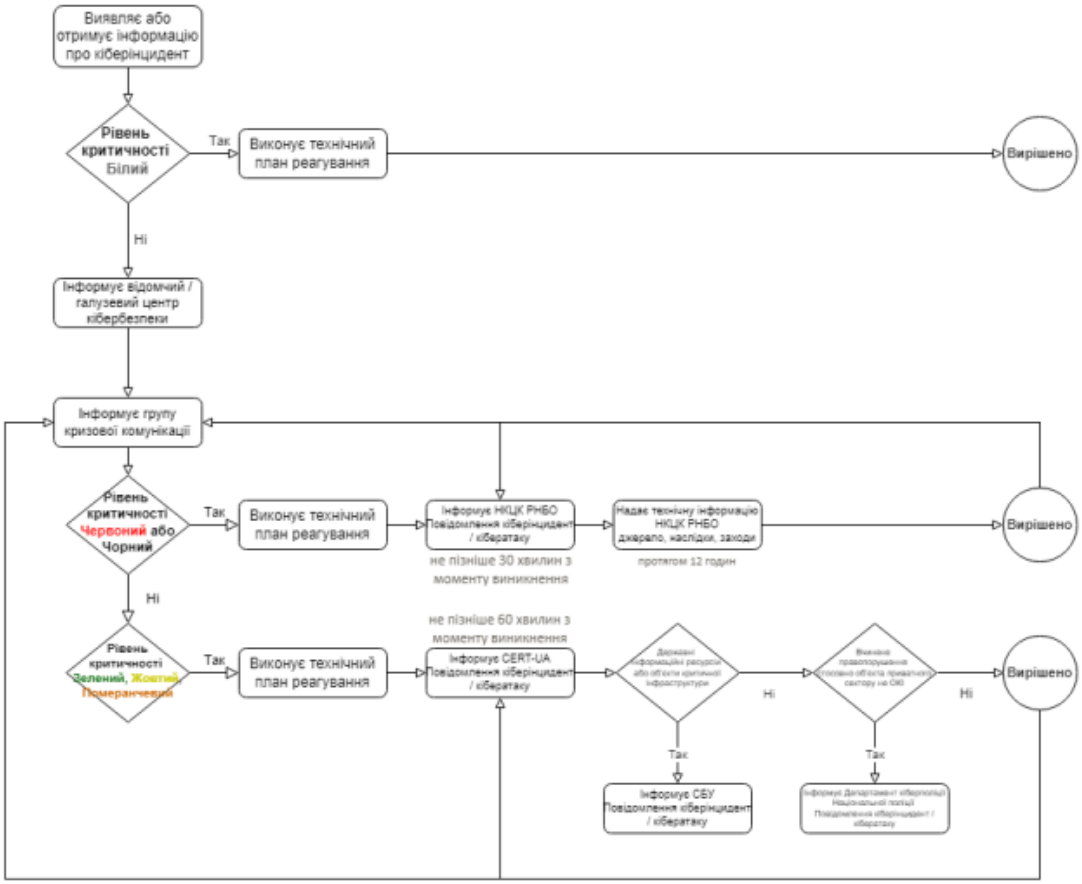


Рис. 1 – Порядок реагування на кіберінциденти та кібератаки

Згідно з наведеними тезами, можна зробити наступні висновки:

Актуальність дослідження кіберінцидентів: З розвитком інформаційних технологій зростає необхідність вивчення кіберінцидентів, оскільки вони стають складнішими та загрожують безпеці інформації та функціонуванню організацій.

Необхідність нових підходів у кібербезпеці: Традиційні методи захисту, такі як брандмауери та системи виявлення вторгнень, виявляються недостатніми для ефективного захисту від сучасних кіберзагроз. Потрібні нові технології та підходи, які здатні адаптуватися до змінних умов.

Роль систем безпеки та керування подіями: SIEM системи виявляються ключовими інструментами у виявленні та реагуванні на кіберінциденти, оскільки вони надають засоби для аналізу трафіку та ідентифікації аномалій.

Сучасні тенденції та їх вплив: З впровадженням хмарних обчислень, DevOps та IoT, управління безпекою стає складнішим. Це вимагає розробки нових стратегій та технологій для забезпечення безпеки мережі.

Потреба в комплексному підході: Дослідження кіберінцидентів виявляється більш ефективним за умови використання комплексного підходу, який охоплює як технічні, так і стратегічні аспекти управління кібербезпекою.

Отже, для ефективного реагування на сучасні кіберзагрози необхідно поєднати нові технології, стратегії та процеси управління безпекою, щоб забезпечити високий рівень захисту інформації та функціонування організацій.

Перелік посилань:

1. Привілейований доступ. Чому це важливо і як його контролювати URL: https://ko.com.ua/privilejovanij_dostup_chomu_ce_vazhlivo_i_yak_jogo_kontrolyuvati_129976 (дата звернення 02.10.2023)
2. Muakhori, I., Sunardi, S.T, M.T, Phd, D., & Abdul Fadlil, M. . (2018). Membangun Web Server Menggunakan Dynamic Domain Name System (Dns) Berbasis Berkeley Internet Name Domain (Bind9) Pada Ip Dinamis. Jurnal Sistem Informasi (JSI) Universitas Dirgantara Marsekal Suryadarma, 5(2), 1–8.

Щибун Євген Юрійович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

БЕЗПЕКА БАЗ ДАНИХ: ШИФРУВАННЯ В БАЗАХ ДАНИХ

Більшість підприємств, корпорацій, державних установ не можуть обійтися без використання інформаційної бази (клієнтів, нормативних актів, продуктів, фінансової звітності). Такі масиви майже завжди містять персональну, корпоративну та конфіденційну інформацію. Її викрадення може призводити до катастрофічних наслідків як фінансового, так і репутаційного характеру. Через це безпека даних стає все важливішою.

Існує два основних мотиви для приватних компаній та державних установ збільшувати захист своїх баз даних:

Перший мотив — це кіберзлочинність. Зростаюча кількість інструментів зловмисників, нові вимагачі програм, методи проникнення без файлів, а також ризик того, що співробітник може вчинити дії, які загрожують конфіденційності інформації.

Другий мотив — це посилення міжнародного законодавства щодо захисту особистої інформації. Відповідальність за збереження конфіденційних даних покладається на організації, що збирають ці дані в процесі своєї діяльності.

Що таке шифрування даних:

Шифрування даних — це процес перетворення чіткого тексту (відкритий текст) в нечитабельний формат (шифротекст) за допомогою криптографічних алгоритмів. Цей процес забезпечує конфіденційність інформації, роблячи її нерозбірливою для неавторизованих осіб.

Основні принципи шифрування даних в СУБД:

Шифрування на рівні стовпців (Column-level encryption):

Опис: Шифрування конкретних стовпців в базі даних, що дозволяє зберігати конфіденційні дані в зашифрованому вигляді навіть внутрішнім адміністраторам бази даних.

Застосування: Ідеально підходить для зберігання особистої інформації, фінансових даних, медичних записів та інших чутливих даних, які вимагають високого рівня конфіденційності.

Шифрування на рівні файлів (File-level encryption):

Опис: Шифрування всієї бази даних або окремих файлів бази даних на рівні файлової системи, що забезпечує додатковий рівень захисту.

Застосування: Використовується для захисту великих об'ємів даних, зокрема, для забезпечення безпеки при зберіганні резервних копій та переміщенні даних між різними системами.

Шифрування на рівні каналу (SSL/TLS encryption):

Опис: Захист даних під час їх передачі між клієнтом і сервером за допомогою протоколів SSL/TLS.

Застосування: Використовується для захисту даних під час транзакцій, авторизації та інших мережевих операцій, що вимагають надійного захисту даних.

Алгоритми шифрування:

Симетричні алгоритми використовують один і той самий ключ для шифрування та розшифрування даних. Ці алгоритми є швидшими і зазвичай менш складними для виконання порівняно з асиметричними алгоритмами.

AES (Advanced Encryption Standard):

Опис: AES є одним з найбільш популярних симетричних алгоритмів шифрування. Він використовує ключі різної довжини (128, 192 або 256 біт) для шифрування даних.

Застосування: AES часто використовується в різних сферах, включаючи захист даних в мережах, зберігання інформації на дисках та комунікацію через Інтернет.

DES (Data Encryption Standard):

Опис: DES був одним з перших стандартів шифрування і використовує 56-бітні ключі для шифрування даних.

Застосування: Хоча DES вважається застарілим і менш безпечним, він все ще може використовуватися в специфічних випадках або як компонент більш складних шифрувальних систем.

Асиметричні алгоритми використовують пару ключів: публічний і приватний. Публічний ключ використовується для шифрування даних, тоді як приватний ключ — для розшифрування.

RSA (Rivest–Shamir–Adleman):

Опис: RSA є одним з найбільш відомих асиметричних алгоритмів шифрування. Він базується на проблемах факторизації цілих чисел і використовується для шифрування даних та цифрового підпису.

Застосування: RSA широко використовується в криптографічних протоколах, таких як TLS/SSL, для захисту комунікації в мережах.

ECC (Elliptic Curve Cryptography):

Опис: ECC є сучасним алгоритмом шифрування, який базується на математичних властивостях еліптичних кривих. Він забезпечує високий рівень безпеки при використанні коротших ключів порівняно з традиційними асиметричними алгоритмами.

Застосування: ECC знаходить застосування в сучасних криптографічних системах, таких як TLS/SSL, де важливо оптимізувати швидкість та ефективність захисту.

Шифрування даних в системах управління базами даних (СУБД) відіграє вирішальну роль у забезпеченні конфіденційності, цілісності та доступності інформації. Вибір відповідних алгоритмів та методів шифрування є критично важливим для створення надійної системи безпеки. Ефективне шифрування дозволяє організаціям знизити ризики витоку даних, захистити важливу

інформацію від несанкціонованого доступу та забезпечити дотримання регулятивних стандартів. Тому розуміння і правильне впровадження шифрування стає невід'ємною частиною комплексної стратегії кібербезпеки організацій у сучасному цифровому світі.

Перелік посилань:

1. Stallings, William. "Cryptography and Network Security: Principles and Practice." Pearson, 2017 (дата звернення 15.04.2024)
2. Ferguson, Niels, and Bruce Schneier. "Practical Cryptography." Wiley, 2003 (дата звернення 16.04.2024)
3. Paar, Christof, and Jan Pelzl. "Understanding Cryptography: A Textbook for Students and Practitioners." Springer, 2010 (дата звернення 16.04.2024)
4. NIST Special Publication 800-57 Part 1 Revision 5. "Recommendation for Key Management: Part 1 - General." URL: https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final (дата звернення 17.04.2024)

Юхимович Анатолій
Васильович
студент групи БСДМ-53, ННІЗІ ДУІКТ, Київ, Україна

БЕЗПЕКА БАЗ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Безпека баз даних є фундаментальною складовою загальної інформаційної безпеки організації, яка забезпечує захист даних від несанкціонованого доступу, модифікації, втрати або крадіжки.

Захист конфіденційності даних передбачає впровадження політик та процедур, які регулюють доступ до чутливої інформації та її використання. Це включає в себе:

Контроль доступу. Встановлення правил, які визначають, хто може переглядати або змінювати дані.

Аудит та моніторинг. Реєстрація та аналіз активності користувачів для виявлення підозрілих дій.

Маскування даних. Застосування методів, які приховують чутливу інформацію від користувачів, яким вона не призначена.

Інтеграція безпеки на всіх рівнях вимагає вбудовування заходів безпеки безпосередньо в архітектуру баз даних та пов’язаних з ними додатків. Це включає:

Захищене програмування. Розробка додатків з урахуванням безпеки для запобігання SQL-ін’єкціям та іншим вразливостям.

Шифрування. Використання сильних алгоритмів шифрування для захисту

даних під час передачі та зберігання.
Регулярне оновлення. Підтримка актуальності всіх системних компонентів для захисту від відомих уразливостей.

Відновлення після інцидентів є критично важливим для забезпечення неперервності бізнесу та збереження довіри клієнтів. Для цього необхідно:
Резервне копіювання. Створення та зберігання копій даних для їх відновлення у випадку втрати.
План відновлення. Розробка детального плану дій для швидкого відновлення системи після інциденту.
Тестування планів. Регулярне перевіряння та оновлення планів відновлення для забезпечення їх ефективності.

Висновок: Ефективна безпека баз даних вимагає комплексного підходу, який включає в себе різноманітні технічні та організаційні заходи. Від контролю доступу до резервного копіювання та відновлення, кожен аспект відіграє важливу роль у захисті цінної інформації організації. Забезпечення безпеки даних є невід'ємною частиною загальної стратегії інформаційної безпеки, яка допомагає зменшити ризики та забезпечити довіру клієнтів та партнерів.

Перелік посилань:

1. Основні методи безпеки баз даних URL: https://datalabsua.com/ua/the-main-database-security-practices/ (дата звернення 08.04.2024)
2. Основні складові процесу забезпечення безпеки даних URL: https://datalabsua.com/ua/the-main-data-security-aspects/ (дата звернення 08.04.2024)

Якимено Юрій Михайлович
викладач, доцент кфедри УІКБ, ННІЗІ ДУІКТ, Київ, Україна

РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК СКЛАДНИЙ І КОМПЛЕКСНИЙ ПРОЦЕС В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

В сучасних умовах виникає кілька завдань, без вирішення яких неможливо створення умов для успішного розслідування інцидентів інформаційної безпеки. Розслідування інцидентів інформаційної безпеки - складний і комплексний процес, що вимагає участі багатьох підрозділів організації. Розслідування включає перевірку і збір доказів з серверів, мережевих пристроїв, а також традиційні заходи нетехнічного характеру. Показано програмне забезпечення як допоміжний засіб

розслідування інцидентів. Приведені наслідки неправильних розслідувань інцидентів в інформаційних системах. Визначено грамотне розслідування інцидентів, представлені основні етапи розслідування інцидентів інформаційної безпеки. Вказані напрями приймання рішення керівництвом організації по продовженню розслідування.

Інциденти, пов'язані з порушенням інформаційної безпеки у організаціях, можуть привести до прямих фінансових втрат. Згідно зі статистикою, на першому місці інциденти трапляються в банках, на другому місці телекомунікаційні компанії, а потім державні підприємства. По даним журналу з кібербезпеки «**Cyberthreat Defense Report**» тільки в одному 2020 році 71% комерційних організацій були піддані кібератакам, а інциденти інформаційної безпеки збільшилися на 66% (Найчастіші інциденти – це Ddos-атаки (23%). Серед джерел основних інцидентів перше місце займає кримінал та кіберзлочинність (31%).Тому співробітники відділу інформаційної безпеки організації повинні мати можливість виявляти і розслідувати будь які спроби звершення незаконних дій.

Навіть при зростанні рівня безпеки, уникнути інцидентів не можливо.

В разі виникнення інцидентів для проведення розслідувань у складі департаменту інформаційної безпеки бажано мати *експерта відповідного рівня*.

Розслідування інцидентів інформаційної безпеки - складний і комплексний процес, що вимагає участі багатьох підрозділів організації: співробітників відділу кадрів, юристів, технічних експертів IT-системи, зовнішніх консультантів з інформаційної безпеки, бізнес-менеджерів, кінцевих користувачів інформаційної системи, співробітників служб технічної підтримки, співробітників служби безпеки та інших.

Розслідування включає перевірку і збір доказів з серверів, мережевих пристроїв, а також традиційні заходи нетехнічного характеру.

Аналіз зібраних даних включає аналіз файлів протоколів роботи, конфігураційних файлів, історії Інтернет-провідників (включаючи соокіез), повідомлень електронної пошти та прикріплених файлів, інстальованих додатків, графічних файлів і іншого. Необхідно провести аналіз ПЗ, пошук за ключовими словами, перевірити дату і час інциденту. **Криміналістичний аналіз** може також включати аналіз на рівні - пошуку видалених файлів і областей, втрачених кластерів, вільного місця, а також аналіз відновлених даних з зруйнованих носіїв (наприклад, по залишкової намагніченості).

При розслідуванні інциденту збір даних може бути виконаний за допомогою програмного забезпечення "**Disk Duplicate**". Воно дозволяє зробити точні копії жорстких дисків ("сектор в сектор") автоматизованих робочих місць користувачів (співробітників компанії) і серверів. Для аналізу отриманих даних

можуть також використовуватися спеціальні засоби емуляції робочих машин користувачів, наприклад, "**VMware VirtuaI Machine**". У ряді випадків для виявлення слідів комп'ютерних інцидентів можуть бути використані різноманітні програмно-апаратні комплекси. Спланована послідовність дій з використанням наведеного програмного забезпечення є досить важкою без додаткових знань, що може приводить до неправильних результатів у розслідуванні [1, 2].

До наслідків неправильних розслідувань інцидентів в інформаційних системах можно віднести:

- втрата можливості відновити документи, що було втрачено;
- нанесення додаткових збитків через не обізнаність або невизначеність в діях;
- випадкова втрата, знищення доказів злочину, через не знання плану дій;
- зупинка бізнес процесів та важливих систем;
- простої системи через довге розслідування;
- неможливість визначити винних у злочинах;
- несвоечасне інформування правоохоронних органів про злочин.

В той же час, якщо інцидент інформаційної безпеки все-таки відбувся, організації необхідно провести його **грамотне розслідування** - виявити вразливості, припинити їхнє подальше використання, визначити «джерело» загрози, її виконавця, грамотно зібрати докази злочину й надати матеріали в правоохоронні органі для порушення справи про адміністративний і (або) кримінальне правопорушення. Послуга розслідування інцидентів інформаційної безпеки з боку окремих компаній полягає в розкритті кіберзлочинів (запобігання, виявлення, реагування й розслідування інцидентів) і законодавчому переслідуванні зловмисників у сфері комп'ютерних технологій. Базуючись на практичному досвіді [2, 3], на рис.1 представлені основні етапи розслідування інцидентів інформаційної безпеки.

Керівництво організації повинно **приймати рішення по продовженню розслідування**:

- залучати співробітників правоохоронних органів для проведення розслідування (якщо немає команди експертів по комп'ютерній криміналістиці - forensics team),
- звергатися до зовнішніх експертів у випадку підозри про здійснення злочину,
- продовжувати збирати докази з метою передачі їх до судового переслідування, або досить просто закрити відповідну вразливість.

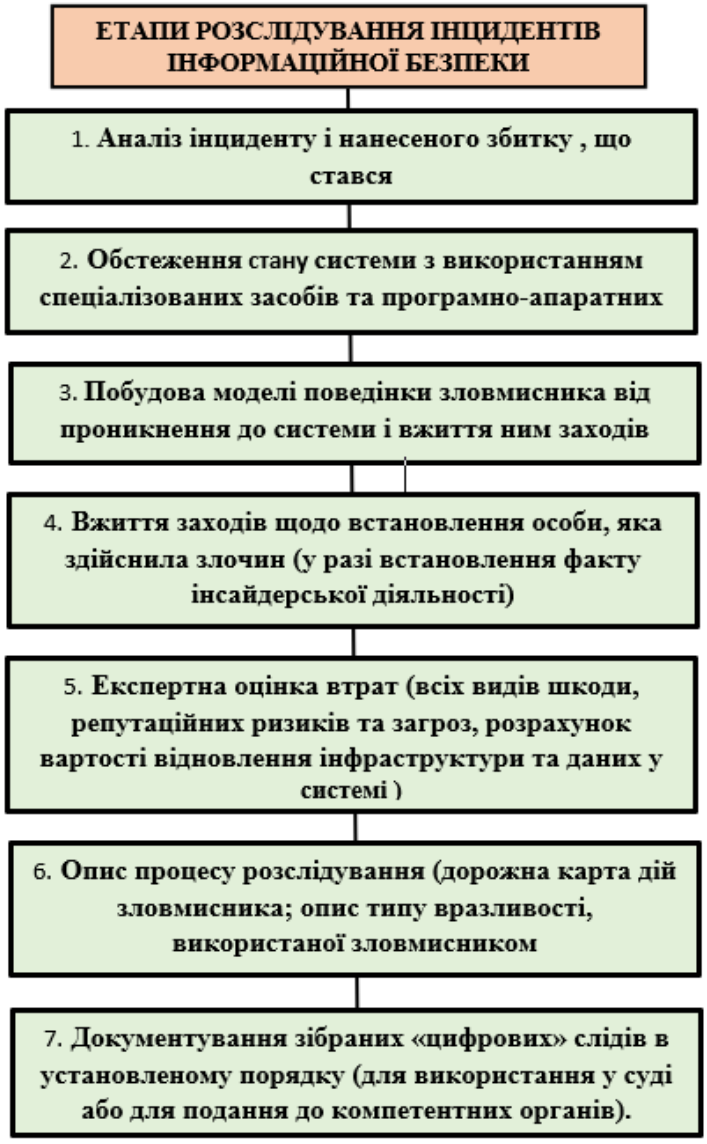


Рис.1- Основні етапи розслідування інцидентів інформаційної безпеки

Перелік посилань:

1. В. Безмалий. Реагування на інциденти інформаційної безпеки . URL: https://www.it-community.in.ua/2014/07/reagirovanie-na-intsidenty-informatsionnoj-bezopasnosti.hlml/

2. Інформаційні технології та послуги. URL: http://www.ucop.edu/information-technology-services/initiatives/resources-and-tools/security-incidcnt-handling.html

3. Якименко Ю.М., Легомінова С.В., Щавінський Ю.В., Рабчун Д.І. Управління інцидентами інформаційної безпеки. Сучасні методи і засоби: навчальний посібник. Київ: Державний університет телекомунікацій, 2023. 241с.

Яловик Денис Володимирович
студент групи БСДМ-53,
ННІЗІ ДУІКТ, Київ, Україна

БЕЗПЕКА БАЗ ДАНИХ

Безпека баз даних - це заходи, спрямовані на захист бази даних від несанкціонованого доступу, недобросовісного використання, пошкодження та втрати даних. Він охоплює широкий спектр технік, політик та технологій, спрямованих на забезпечення конфіденційності, цілісності та доступності даних, збережених у базі даних.

Багато вразливостей програмного забезпечення, неправильних налаштувань або випадків недбалості можуть призвести до порушень безпеки (Рис.1).

Рис.1. Види загроз безпеки баз даних

До ключових аспектів безпеки баз даних відноситься:

Аутентифікація та авторизація: До бази даних повинні мати доступ лише авторизовані користувачі. Аутентифікація перевіряє ідентифікацію користувачів, зазвичай за допомогою імен користувачів та паролів, тоді як авторизація визначає, які дії користувачі мають право виконувати у базі даних.

Шифрування: Шифрування полягає у перетворенні даних у кодовану форму, яку можна розкодувати лише за допомогою вірного ключа дешифрування. Шифрування чутливих даних, збережених у базі даних, допомагає запобігти несанкціонованому доступу, навіть якщо дані буде викрадено.

Контроль доступу: Механізми контролю доступу обмежують, хто може отримати доступ до конкретних даних у базі даних та які дії вони можуть

виконувати з ними. Це включає контроль доступу на основі ролей (RBAC), який надає дозволи на основі ролей окремих користувачів.

Аудит та ведення журналів: Аудит передбачає моніторинг та реєстрацію дій у межах бази даних, таких як спроби входу, модифікації даних та спроби доступу. Журнали можна проаналізувати для виявлення підозрілої поведінки та інцидентів безпеки.

Маскування та редакція даних: Техніки маскування та редакції даних приховують чутливу інформацію від користувачів, які не повинні бачити її. Це може включати заміну чутливих даних фіктивними або маскованими значеннями збереженням формату та структури даних.

Резервне копіювання та відновлення: Регулярні резервні копії бази даних повинні створюватися для того, щоб забезпечити можливість відновлення даних у разі втрати або пошкодження. Резервні дані повинні зберігатися та шифруватися для запобігання несанкціонованому доступу.

Управління патчами: Регулярне оновлення та застосування патчів до системи управління базами даних (СУБД) та інших компонентів програмного забезпечення допомагає вирішувати відомі уразливості безпеки та зменшує ризик їх використання зловмисниками.

Мережева безпека: Захист інфраструктури мережі, яка з'єднує сервери баз даних з клієнтами та іншими системами, є важливим для безпеки баз даних. Це включає впровадження брандмауерів, систем виявлення/запобігання вторгнень та безпечних мережевих протоколів.

Фізична безпека: Фізичні заходи безпеки, такі як контроль доступу, спостереження та середовищні контролі, є важливими для захисту серверів та пристроїв зберігання, які містять базу даних, від фізичних загроз, таких як крадіжка, вандалізм та стихійні лиха.

Тренування та освіта з питань безпеки: Навчання адміністраторів баз даних, розробників та користувачів щодо найкращих практик безпеки та потенційних загроз допомагає створити культуру, свідому безпеки та зменшити ймовірність порушень безпеки через людську помилку чи недбалість.

Зробимо висновки. Впровадження комплексної стратегії безпеки баз даних потребує поєднання технічних контролів, політик та процедур, адаптованих до конкретних вимог та ризиків, з якими стикається організація. Регулярні оцінки безпеки та аудити можуть допомогти виявити слабкі місця та забезпечити ефективність заходів безпеки протягом часу.

Перелік посилань

1. " Database Security: An Essential Guide | IBM " URL: https://www.ibm.com/topics/database-security (дата звернення 08.04.2024)
2. " What is database security?" URL: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-database-security#:~:text=Database%20security%20is%20the%20processes,and%20integrity%20of%20the%20database. (дата звернення 10.04.2024)

Яровий Олексій Юрійович
Курсант 1 курсу Навчально-наукового
інституту права та підготовки фахівців
для підрозділів Національної поліції
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Турчанікова Ганна Олександрівна
капітан поліції
викладач кафедри
Тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ

ПРІОРИТЕТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

В умовах гібридної війни, яка ведеться наразі, питання кібербезпеки є досить актуальним. Сучасні технологічні виклики, такі як кібератаки, кібершпигунство, кібертероризм, потребують комплексного підходу для захисту важливих інформаційних систем. Україна, як і багато інших країн, стикається з ростом кіберзагроз у всіх сферах життєдіяльності. Зокрема, організовані кібергрупи та поодинокі хакери використовують різноманітні методи для викрадення важливої для державного захисту інформації та впливу на інформаційні системи. Безпека критично важливих об’єктів під час війні: енергетичних систем, транспортної інфраструктури та комунікаційних мереж є найбільш привабливою ціллю для їх ураження. Тому для України є необхідним розробка національної стратегії забезпечення кібербезпеки.

Такі положення були затвердженні Указом Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". Основними пріоритетами забезпечення кібербезпеки є забезпечення безпеки кіберпростору для захисту державної цілісності України та розвитку суспільства, захист законних прав, свобод та

інтересів громадян України, а також європейська та євроатлантична інтеграція у сфері кібербезпеки [1]. Інформаційна грамотність населення є ключовим фактором для запобігання успішним кібератакам. Треба здійснювати постійну роботу з підвищення кіберграмотності громадян.

Також слід пам'ятати про основні принципи кібербезпеки України. Це верховенство права та законності, поваги до прав людини, забезпечення національних інтересів держави та захищеності кіберпростору, розвитку мережі Інтернет. Держава повинна широко співпрацювати з громадськістю та іншими державами задля зміцнення взаємної довіри у сфері кібербезпеки та виробленню спільних підходів для протидії кіберзагрозам. Органи, що забезпечують захист кіберсистем, повинні пропорційно вживати заходів щодо потенційних та реальних ризиків і загроз, а також призначати невідворотне покарання за вчинення кіберзлочинів. [2, ст 7]

Отже, забезпечення кібербезпеки України є важливим завданням, яке лежить в основі напрямків діяльності державної безпеки. Розробка ефективних стратегій та заходів, які будуть базуватися на пріоритетах забезпечення кібербезпеки держави, дозволить підвищити рівень розвитку систем кіберзахисту та зменшити можливість впливу різноманітних кібератак.

Перелік посилань:

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" Указ Президента України; Стратегія від 26.08.2021 № 447/2021
https://zakon.rada.gov.ua/laws/show/447/2021#Text
2. Про основні засади забезпечення кібербезпеки України
Закон України від 05.10.2017 № 2163-VIII
https://zakon.rada.gov.ua/laws/show/2163-19#Text

Яценко Денис Дмитрович
студент групи БСДМ-52, ННІЗІ ДУІКТ, Київ, Україна

СУЧАСНІ СПОСОБИ ЗАХИСТУ ВІД ШКІДЛИВИХ ПРОГРАМ НА ПІДПРИЄМСТВАХ

Захист від шкідливих програм на підприємствах - це важлива складова інформаційної безпеки підприємств, яка допомагає вберегти компанії від серйозні проблеми, включаючи втрату конфіденційної інформації, пошкодження даних, а також витрати часу і ресурсів на відновлення систем.

Хоча способів захисту від шкідливих програм і багато але усі вони спрямовані або на запобігання потрапляння програми у захищене середовище

або на скоріше їх виявлення у системі та знешкодження.

Для того щоб розібратися в системах захисту від шкідливих програм нам спочатку потрібно дізнатися від чого ми захищаємося(Рис.1).

Рис.1. Основні види шкідливих програм

До основних способів захисту від шкідливих програм відноситься:

Комплексні антивірусні платформи: Це програми, які включають в себе не лише антивіруси, але й антишпіонське програмне забезпечення, міжмережеві файрволи, заходи контролю за вмістом та інші заходи захисту. Прикладами можуть бути платформи від Symantec, McAfee, Kaspersky, Trend Micro тощо.

Системи моніторингу інтрузій: Ці системи виявляють та реагують на надзвичайні події або аномальну активність в мережі або на комп'ютерах. Наприклад, Snort або Suricata.

Системи управління відомостями та аналізу подій безпеки (SIEM): Вони використовуються для агрегування, аналізу та кореляції журналів подій з різних джерел в мережі. Це допомагає виявляти атаки та незвичайну активність. Приклади SIEM-систем включають Splunk, IBM QRadar, ArcSight.

Безпека електронної пошти: Програми для фільтрації спаму, виявлення і блокування вірусів та інших шкідливих вкладень в електронній пошті. Прикладами можуть бути Microsoft Exchange Online Protection, Proofpoint,

Управління мобільною безпекою: Пристрої мобільних працівників можуть бути потенційною точкою входу для загроз, тому використання програм для мобільної безпеки, таких як MobileIron, VMware Workspace ONE, BlackBerry UEM, допомагає захистити корпоративні дані на мобільних пристроях.

Системи контролю за доступом і ідентифікацією користувачів: Ці

системи вимагають аутентифікацію користувачів та надають доступ лише до необхідних ресурсів. Прикладами можуть бути системи одноразових паролів, двофакторної аутентифікації та системи управління доступом, такі як Okta, Duo

Перелік посилань:

1. «Безпека в обчисленнях» Charles P. Pfleeger Shari Lawrence Pfleeger Jonathan Margulies URL: звернення 16.04.2024)

2. « З в і д з н а н ь з к і б е р б е з п е к и H Y P E R L I N K " h t t p s : /