ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИУТУ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ЦИФРОВА ТРАНСФОРМАЦІЯ КІБЕРБЕЗПЕКИ»»

Тези доповідей

27 квітня 2023

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.

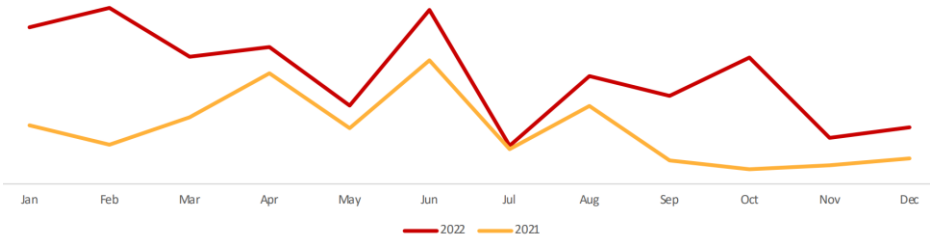


Figure 1 – Monitoring of DDoS attacks

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 телекомунікацій,,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.

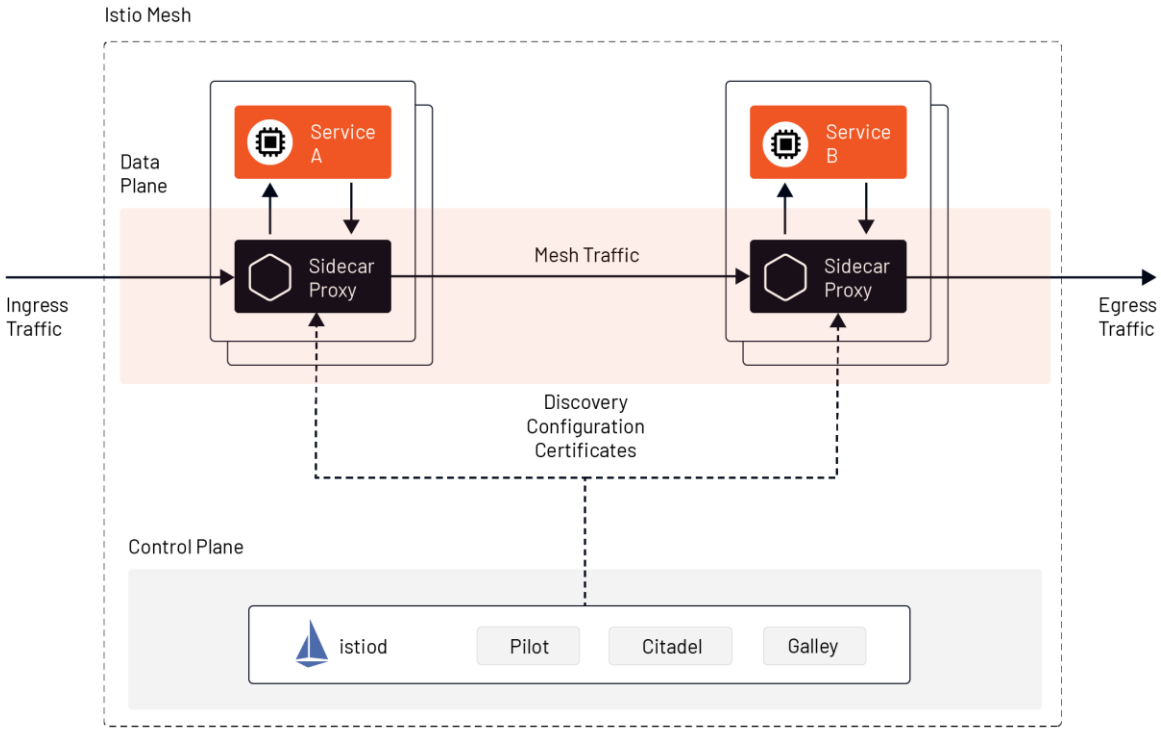


Рис.1 Архітектура Istio Service Mesh

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/

Бондарєв Ілля Дмитрович
студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

ВПЛИВ БОТІВ НА РОБОТУ СОЦІАЛЬНИХ МЕРЕЖ ТА КОРИСТУВАЧІВ

Платформи соціальних мереж зробили революцію у комунікації людей та отриманні інформації. Однак у той самий час, платформи, такі як Twitter, Facebook, Instagram та ін. швидко стали майданчиком для публічних маніпуляцій та поширення чи посилення дезінформації.

Хоча шкідливий контент може поширюватися певними особами, сьогодні існують мільйони окремих та скоординованих автоматизованих облікових записів, які поширюють ненависть, дезінформацію та маніпулюють громадською думкою без будь-якого втручання людини. Ще гіршим є те, що через високу складність таких автоматичних облікових записів, їх майже неможливо ідентифікувати людині, а для алгоритму це стає досить важким завданням.

Приклади впилву шкідливих ботів на користувачів соціальних мереж

Соціальні боти можуть бути об'єктами стрічки новин, які збирають новини з різних джерел та доставляють їх у стрічки підписників. Вони також можуть бути розважальними інструментами, які доставляють повідомлення певного типу або редагують зображення та повертають його. Їх можна використовувати для багатьох корисних цілей. Але також боти можуть бути шкідливими і завдавати проблем користувачам. Навіть такі боти, як, наприклад, ті, що доставляють новини, інформацію про погоду та боти, призначені виключно для розваги, можуть сприяти поширенню неперевіреної інформації.

Прикладом цього може бути новинний бот, який підбирає статтю з деякою новиною з ненадійного джерела. Неперевірена інформація або навмисно фейкові новини можуть бути перехоплені ботами та розміщені повторно.

Коли це робиться, неправдива інформація може швидко поширюватися серед багатьох людей за дуже короткий час. Це маніпулює людьми і може змусити їх повірити, в те, що не відповідає дійсності.

Найбільшу загрозу несуть боти, які навмисно були створені для досягнення зловмисних цілей. Дані боти були розроблені для заподіяння шкоди, поширення шкідливих програм, дезінформації, спаму та маніпулювання. Шкідливий тип соціальних ботів може, наприклад, використовуватись для впливу на громадську думку шляхом розміщення підроблених оглядів на сайтах продуктів або розповсюдження підроблених новин. Їх також можна використовувати для впливу на вибори, акції та різні події. Коли справа доходить до використання соціальних ботів для маніпулювання виборами, викликає велике занепокоєння, що це загрожує демократії.

У 2016 р. Бессі та ін. вивчали використання ботів на президентських виборах у США у 2016 році. Їхні результати показали, що боти відповідали за близько 20% розмов, пов'язаних з виборами. Хоча це й не доведено, широке використання ботів на виборах може вплинути на думку людей і, можливо, результат самих виборів [4].

Боти також можуть бути використані для впливу на фондовий ринок. Журналісти, аналітики та дослідники все частіше повідомляють про нові випадки потенційної небезпеки, яку несуть соціальні боти. До них відносяться необґрунтовані наслідки, які може спричинити широке поширення ботів

відносно стабільності ринків. За дослідженнями Еміліо Феррара, можна дійти висновку, що пости у Twitter можна використовувати для прогнозування фондового ринку і з'являється все більше свідчень того, що оператори ринку звертають увагу та оперативно реагують на інформацію із соціальних мереж. Так, наприклад, 23 квітня 2013 р. Сирійська електронна армія зламала твіттер-аккаунт Associated Press і опублікувала хибну чутку про теракт у Білому домі, внаслідок якого нібито було поранено президента Обаму. Це спричинило негайний обвал на фондовому ринку. 6 травня 2010 року на фондовому ринку США стався раптовий крах, коли індекс Доу-Джонса за кілька хвилин упав на понад 1000 пунктів (близько 9%) — найбільше одноденне падіння в історії. Після 5-місячного розслідування роль ботів стала очевидною, але досі залишається незрозуміло, чи мали ці боти доступ до інформації із соціальної мережі [1].

Ще одна проблема, яку викликають соціальні боти, — це репутація. В OSN користувачі, які отримують багато лайків або мають багато підписників, вважаються популярнішими. Але цю популярність можна придбати. Існує велика промисловість продажу лайків і підписників. Швидкий пошук у найпопулярнішому сервісі Google.com на запит «купити підписників» дає безліч сервісів, які дозволяють це зробити за декілька кліків, як показано на рисунку 1.2.

Прикладом сервісу, який продає лайки та підписників, є www.foxy-it.com.ua. За допомогою цього сервісу можна купити 100 підписників лише за 9 грн, інтерфейс даного сервісу показано на рисунку 1.3.

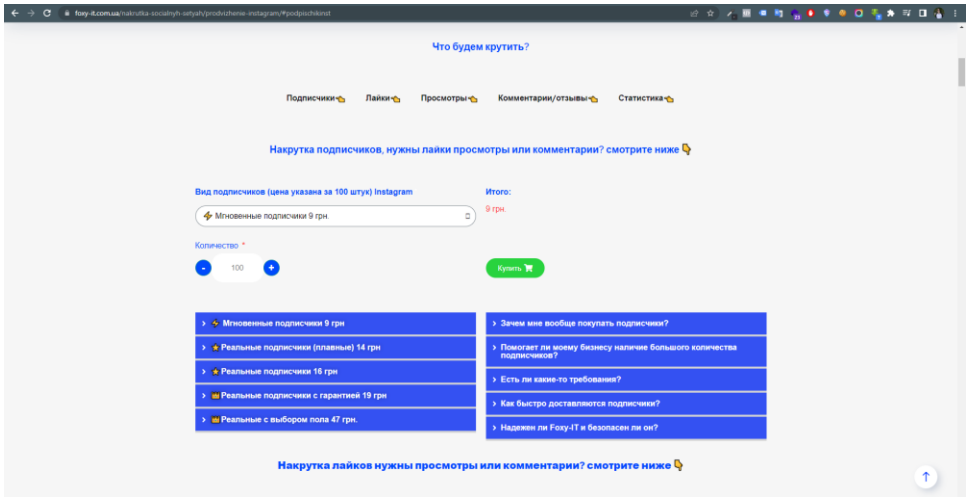


Рис. 1. – Інтерфейс веб-сайту для купівлі підписників та лайків

Лайки та підписники купуються з двох причин; щоб бути більш відомим і вимагати більше коштів за рекламу. Проблема, яку створюють ці сервіси, полягає в тому, що вони створюють штучну славу, яка обманює людей, думаючи, що вони є більш популярними або відомими, ніж вони є насправді. Вони також створюють штучну популярність продуктів, яка може маніпулювати думкою людей про продукт чи бренд.

У своєму дослідженні Yi Shen запропонував метод виявлення хибних

підписників на Sina Weibo, платформі мікроблогів, що дуже схожа на Twitter. Запропонований ними метод виявлення був сфокусований на таких характеристиках, як співвідношення числа підписників та числа підписок, відсоток двонаправлених друзів, середня частота публікації та частка нічних повідомлень. Аналізуючи ці особливості, дослідники змогли виявити підроблені акаунти з точністю понад 90%. Проаналізувавши більше 30 000 облікових записів, вони виявили, що у звичайних користувачів близько 14% хибних підписників. Крім того, вони виявили, що знаменитості мають близько 42% хибних підписників. Це означає, що майже половина підписників знаменитості – фейки. Але це не означає, що всі знаменитості займаються купівлею підписників та лайків. Соціальний етикет у Твіттері полягає у тому, щоб підписатися на людей, якщо вони підписуються на вас. Цим етикетом користуються соціальні роботи. Таким чином, більшість результатів Shen et al. можуть також включати соціальних роботів, а також підроблені облікові записи [2].

Перелік посилань:

1. A Decade of Social Bot Detection [Електронний ресурс] – Режим доступу: https://cacm.acm.org/magazines/2020/10/247598-a-decade-of-social-bot-detection/fulltext
2. Social Media Bot Detection [Електронний ресурс] – Режим доступу: http://ltu.diva-portal.org/smash/get/diva2:1601000/FULLTEXT01.pdf

Бригинець Анастасія Андріївна,
студентка групи БСД-31, ННІЗІ ДУТ, Київ, Україна

ТЕХНОЛОГІЯ РЕВЕРС-ІНЖИНІРИНГУ ДЛЯ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

Реверс-інжиніринг - це метод, який використовується для розуміння того, як працює програмне або апаратне забезпечення, шляхом аналізу його коду, дизайну та функціональності. У контексті кіберінцидентів реверс-інжиніринг часто використовується для аналізу шкідливого програмного забезпечення, щоб зрозуміти його поведінку, визначити його джерело і мету, а також розробити контрзаходи для запобігання або пом'якшення наслідків майбутніх атак. Цей процес включає вивчення коду та поведінки шкідливого програмного забезпечення, аналіз мережевого трафіку та використання різних інструментів і методів для розкриття основної структури та функціональності програмного забезпечення. Реверс-інжиніринг може бути критично важливим компонентом реагування на інциденти, дозволяючи аналітикам швидко виявляти кіберзагрози та реагувати на них.

Реверс-інжиніринг є важливою частиною розуміння шкідливого програмного забезпечення та боротьби з ним. Коли шкідливе програмне забезпечення виявлено, перше, що аналітики безпеки хочуть знати, це те, як воно працює.

Однак простого розуміння того, як працює шкідливе програмне забезпечення, недостатньо для захисту від нього. Щоб бути по-справжньому ефективними, аналітики безпеки повинні вміти не тільки розуміти, як працює шкідливе програмне забезпечення, а й передбачати, як воно буде діяти у системі.

Аналітики безпеки повинні добре розуміти мову асемблера та архітектуру

комп'ютера, щоб здійснювати реверс-інжиніринг шкідливого програмного забезпечення. Мова асемблера - це найнижчий рівень мови програмування, який використовується для написання програм, дуже близьких до апаратного забезпечення. Це робить її ідеальною для написання шкідливого програмного забезпечення, оскільки дає зловмиснику великий контроль над тим, що робить код.

До того ж, необхідно розбиратись у архітектурі комп’ютера. Розуміючи комп'ютерну архітектуру, дослідники безпеки можуть краще зрозуміти, як працює шкідливе програмне забезпечення і як його можна використовувати для атак на системи.

Існує два методи аналізу: статичний та динамічний. Статичний аналіз можна виконати, досліджуючи сам код або переглядаючи його метадані, такі як мітки часу або геші файлів. За допомогою статичного аналізу можна зрозуміти, що робить шкідливе програмне забезпечення, не турбуючись про те, що воно може завдати шкоди.

Динамічний аналіз - це процес виконання шкідливого програмного забезпечення для спостереження за його поведінкою. Це можна зробити, запустивши код у контрольованому середовищі, наприклад, у віртуальній машині або пісочниці. Динамічний аналіз можна використовувати для визначення поведінки шкідливого програмного забезпечення під час його запуску [1].

Як статичний, так і динамічний аналіз мають свої сильні та слабкі сторони. Статичний аналіз з меншою ймовірністю може завдати шкоди системі, але може бути складно зрозуміти, що робить шкідливе програмне забезпечення без його виконання. Динамічний аналіз з більшою ймовірністю може завдати шкоди системі, але він може надати більше інформації про те, як працює шкідливе програмне забезпечення.

Для успішного проведення реверс-інжинірингу, зазвичай, виконують шість кроків:

1. Отримання зразку шкідливого програмного забезпечення, шляхом його завантаження з інтернету або отримавши від когось іншого.

2. Отримання дизасемблера або декомпілятора. Для цього можна використовувати багато різних програм.

3. За допомогою дизасемблера або декомпілятора необхідно проаналізувати код шкідливого програмного забезпечення. Це допоможе зрозуміти, як працює шкідливе програмне забезпечення і що воно робить.

4. Створення середовища "пісочниці" - безпечного місце, де можна запустити шкідливе програмне забезпечення і подивитися, що воно робить, не ризикуючи заразити комп'ютер.

5. Запуск шкідливого програмне забезпечення в середовищі пісочниці та спостерігання за його поведінкою.

6. Створення звіту з висновками. Це допоможе поділитися результатами з іншими людьми, які можуть бути зацікавлені у реверс-інжинірингу шкідливого програмного забезпечення [2].

Отже, реверс-інжиніринг є цінним інструментом для цифрових криміналістичних розслідувань. Аналізуючи код і структуру шкідливого програмного забезпечення та інших цифрових артефактів, аналітики можуть отримати уявлення про методи і мотивацію кіберзлочинців, а також розробити ефективні контрзаходи для захисту від майбутніх атак. Реверс-інжиніринг також може бути використаний для розслідування та виявлення першопричин збоїв у роботі системи, витоку даних та інших інцидентів кібербезпеки. Однак зворотний інжиніринг - це складна технічна галузь, яка вимагає спеціальних знань і досвіду. Аналітики повинні бути навчені методам реверс-інжинірингу та бути в курсі новітніх інструментів і технологій, щоб ефективно використовувати цей підхід у своїх розслідуваннях. За умови належної підготовки та ресурсів, реверс-інжиніринг може стати потужним інструментом для фахівців з цифрової криміналістики, допомагаючи їм розплутувати навіть найскладніші кіберінциденти та зберігати цифрові системи в безпеці.

Перелік посилань:

1. Static Malware Analysis Vs Dynamic Malware Analysis | HackerCombat. HackerCombat. URL: https://hackercombat.com/static-malware-analysis-vs-dynamic-malware-analysis/.
2. What is reverse-engineering? how does it work?. *TechTarget*. URL: https://www.techtarget.com/searchsoftwarequality/definition/reverse-engineering.

Ветлицька О. С., аспірантка кафедри управління інформаційною та кібернетичною безпекою ДУТ, м. Київ

СОЦІОЛОГІЧНА КОНЦЕПТУАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У роботі проаналізовано сутність категорій концептуалізації, соціологічної концептуалізації. Встановлено, що соціологічна концептуалізація поняття «інформаційна безпека» передбачає виокремлення умов формування факторів впливу на забезпечення інформаційної безпеки; аналіз сутності й тенденцій розвитку інформаційного простору, а також ризиків і загроз, викликаних його функціонуванням; формування понятійного інструментарію для роботи з даною категорією. Досліджено стан захищеності молоді в інформаційному просторі, яка є найбільш вразливою категорією у контексті інформаційної безпеки. З'ясовано, що більшість молодих людей не усвідомлює всіх інформаційних ризиків та загроз, зокрема формування інформаційної залежності й споживацького ставлення до життя, маніпулювання свідомістю, подолати які в умовах неконтрольованості ЗМІ й Інтернет-ресурсів майже неможливо.

У світлі динамічного розвитку інформаційних процесів і технологій інформаційна безпека набуває все більш важливого наукового значення як чинник забезпечення сталого розвитку й захищеності суспільства.

Українське суспільство розвивається у межах світового інформаційного процесу, нарощуючи масштаб використання інформаційно-комп'ютерних технологій у всіх сферах життєдіяльності, впевнено рухаючись у напрямку всеосяжної інформатизації [1]. Глибокий соціологічний аналіз проблеми інформаційної безпеки надзвичайно важливий для сучасного інформаційного суспільства. Цим пояснюється актуальність соціологічної концептуалізації поняття «інформаційна безпека».

Концептуалізація – це створення мови, яка описує досліджуване явище, що

дозволить описати поняття інформаційна безпека за допомогою певних важливих ознак. Концепт дає змогу визначити теоретичний сенс певної категорії.

Соціологічна концептуалізація передбачає перетворення багатозначного поняття на щось прикладне, тобто таке, що можна практично виміряти, побачити. Також концептуалізації потребують поняття, які не можна назвати виключно абстрактними, з тих міркувань, що їм або вже присвячена велика кількість різних емпіричних досліджень або їм надано багато різних визначень.

Категорія інформаційної безпеки та характер її висвітлення у науковій літературі має надзвичайно дискусійний характер. У рамках даного дослідження розумітимемо під інформаційною безпекою стан захищеності особистості, суспільства, держави в інформаційному просторі, за якого соціальні суб'єкти ефективно функціонують в умовах наявності інформаційних ризиків та загроз [2].

Соціологічна концептуалізація поняття «інформаційна безпека» передбачає необхідність:

– виокремлення умов формування, факторів впливу на забезпечення інформаційної безпеки;

– аналізу сутності й тенденцій розвитку інформаційного простору, а також ризиків і загроз, викликаних його функціонуванням;

– формування понятійного інструментарію для роботи з даною категорією.

Оскільки не всі із зазначених моментів висвітлені в цій роботі, її характер носить узагальнюючий вигляд, окреслюючи межі соціологічного аналізу цього явища у подальших дослідженнях [3].

Говорячи про інформаційну безпеку у соціологічному аспекті, варто відзначити, що першою потрапляє під інформаційний вплив молодь як найбільш мобільна й активна група, що користується послугами мережі Інтернет і значний час проводить біля моніторів та екранів.

Як показують дослідження з цієї тематики [4], дозвілля молодих людей пов'язане, переважно, з мережею Інтернет (54,9 % опитаних обрали варіант відповіді «сиджу в Інтернеті»), де вони активно спілкуються. Водночас, справедливо буде відзначити, що молодь знаходить задоволення і в реальному спілкуванні (52,7% респондентів проводять свій вільний час, спілкуючись із друзями).

Оцінюючи стан інформаційної захищеності молоді, яка «сидить» в мережі Інтернет, не можна сказати, що вони перебувають у безпеці. Однак, молоді люди вважають, що саме тут вони знаходять справжню свободу, мають можливість вільно самовиражатися, розкривати себе. Лише деякі особи усвідомлюють, що постійно перебувають під впливом інформаційних загроз, які, перш за все, проявляються в формуванні інформаційної залежності [4].

Крім того, інформаційні загрози, що виходять з віртуального середовища, пов'язані з маніпулятивними впливами на свідомість і поведінку молоді, яка не завжди вміє протистояти цьому впливу. Молодь не здатна самостійно розібратися в істинності чи хибності тієї чи іншої інформації, у її змісті та ціннісному навантаженню. Внаслідок цього виникають загрози соціального

характеру, які подолати сьогодні, в умовах неконтрольованості засобів масової інформації й Інтернет-ресурсів практично неможливо.

Розвиток інформаційних технологій слід розглядати як позитивне явище, яке конструктивно впливає на економічний і технологічний розвиток суспільства, сприяє зростанню суспільного добробуту й комфортності життя. Але при цьому в сучасному суспільстві вже починають серйозно замислюватися про проблему дотримання прав людини в умовах високої динаміки інформаційно-комунікативних технологій, методи протистояння шкідливим інформаційним впливам.

При дослідженні сучасного інформаційного простору постає проблема його ціннісного та культурного змісту. Механізм трансляції підростаючому поколінню цінностей інформаційного суспільства і стратегій протистояння загрозам, які спричинені його розвитком, представлений, переважно, в мережі Інтернет і на телебаченні. Хоча з гуманістичних міркувань деякі канали й Інтернет-ресурси взагалі не мають права займати ефірний час і місце в системі суспільних комунікацій [5].

Добре відомо, що сучасний інформаційний простір наповнений елементами та змістом споживчої культури, що актуалізує іншу, не менш важливу проблему, – проблему розвитку інформаційної культури суспільства, яка відображає специфіку функціонування інформації у суспільстві й інформаційних якостей самого суспільства та його суб'єктів.

Отже, дослідження показало, що сучасні канали масової комунікації часто стають транслятором антикультурних цінностей, ідей, концепцій, які руйнують духовні цінності суспільства, сприяють формуванню інформаційної залежності й маніпулювання суспільною свідомістю. Основним об’єктом яких стають молоді люди. Це знищує у людині її духовний початок і формує замість нього споживацьке ставлення до життя, і навіть сім'я не здатна подолати загрози, які виходять з інформаційного простору [6].

Перелік посилань:

1. Дзьобань О. П. Національна безпека України: концептуальні засади та світоглядний сенс: монографія. Харків : Майдан, 2014. 284 с.
2. Дзьобань О. П. Сучасний віртуальний простір: конгеніальність віртуальності й міфу. Стратегічні пріоритети. 2017. № 3. С. 163-170.
3. Паламарчук С. А., Шемендюк О. В., Ляшенко Г. Т., Ткач В. О. Забезпечення захисту кіберпростору в провідних країнах світу. Збірник наукових праць Військового інституту телекомунікацій та інформатизації. 2020. Вип. 1. С. 58-64.
4. Гнатюк Р. Соціальні мережі: співвідношення позитиву і негативу. Дзеркало тижня. Україна. 2013. Випуск № 2. 18-25 січня. URL: https://zn.ua/ukr/family/socialni-merezhi-spivvidnoshennya-pozitivu-i-negativu.html
5. Samygin S.I., Vereshchagina V.A. Global challenges of the present and safety of a civilization of the third millennium. European Social Science Journal. 2014. № 6. V. 2. URL: http://mii-info.ru/data/documents/EZhSN-2014-6-2.pdf of Page 60–66
6. Samygin S.I., Vereshchagina V.A. Family and social safety. Humanities, Social-economic and Social Sciences. 2014. № 2. P. 116–120.

Владиченко Сергій Владиченко
Студент групи КІД-41, ННІЗ ДУТ, Київ, Україна

РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

Розслідування кіберінцидентів - це складний технічний процес, який вимагає високих знань у галузі кібербезпеки та знання технічних деталей комп'ютерних систем. У цьому матеріалі ми розглянемо деякі з тверджень та формул, які використовуються в розслідуванні кіберінцидентів.

1. Ідентифікація та аналіз інциденту У першу чергу розслідування кіберінциденту починається з ідентифікації та аналізу інциденту. Це включає в себе виявлення знаків порушення безпеки, таких як вимагання відкупу, підозрілі активності в мережі, незвичайний трафік та інше. Для аналізу використовуються різні інструменти, такі як системи виявлення вторгнень (IDS) та системи управління подіями безпеки (SIEM).
2. Відновлення даних Відновлення даних є однією з ключових складових розслідування кіберінциденту. Це включає в себе відновлення втраченої, пошкодженої або знищеної інформації. Для цього використовуються різні методи, такі як відновлення файлів з резервних копій, відновлення даних з віртуальної пам'яті та інше.
3. Використання криптоаналізу Криптоаналіз - це процес розшифрування криптографічних ключів та кодувань, які використовуються для захисту конфіденційної інформації. У розслідуванні кіберінцидентів криптоаналіз може допомогти знайти слабкі місця в системі захисту, які можуть бути використані злочинцями для отримання доступу до конфіденційної інформації. Криптоаналіз включає в себе використання аналітичних методів, таких як аналіз частоти літер, криптоаналіз зворотнього шифрування та інші методи.
4. Використання хеш-функцій Хеш-функції - це математичні алгоритми, які приймають на вхід довільну кількість даних і генерують фіксований хеш-код. У розслідуванні кіберінцидентів хеш-функції використовуються для ідентифікації та перевірки цілісності даних. Наприклад, якщо хеш-коди двох файлів співпадають, це означає, що файли ідентичні. Хеш-функції також використовуються для створення цифрових підписів, які дозволяють перевірити автентичність даних.
5. Використання техніки сіткарського аналізу Сіткарський аналіз - це техніка аналізу даних, яка використовується в розслідуванні кіберінцидентів для знаходження зв'язків між різними елементами системи. Наприклад, можна проаналізувати логи серверів та мережі, щоб визначити, які системи були скомпрометовані, які дані були викрадені та які злочинці були втягнуті в інцидент.

У розслідуванні кіберінцидентів використовуються різні техніки та інструменти, такі як системи виявлення вторгнень, відновлення даних, криптоаналіз, хеш-функції та сіткарський аналіз. Комбінація цих методів та інструментів дозволяє розслідувачам ефективно розслідувати кіберінциденти та ідентифікувати злочинців, які вчинили ці інциденти. Важливою частиною розслідування

кіберінцидентів є збір доказів, який може виконуватися за допомогою цих технік та інструментів.

Наприклад, системи виявлення вторгнень можуть допомогти виявити несанкціонований доступ до системи та ідентифікувати злочинців, які вчинили цей вторгнення. Відновлення даних може допомогти відновити втрачені дані та ідентифікувати джерело втрати даних. Криптоаналіз може допомогти розкрити зашифровану інформацію, таку як паролі та ключі шифрування, що може бути корисним для ідентифікації злочинців.

Хеш-функції дозволяють ідентифікувати та перевіряти цілісність даних, що може бути важливим при зборі доказів. Сіткарський аналіз може допомогти виявити зв'язки між різними елементами системи та ідентифікувати потенційних злочинців.

У розслідуванні кіберінцидентів також важливо використовувати етичні підходи, такі як збір та збереження доказів у відповідності зі стандартами безпеки та захисту приватності. Крім того, важливо розуміти, що деякі техніки та інструменти можуть бути незаконними у деяких країнах, тому важливо дотримуватися відповідних законодавчих актів та правил.

У підсумку, розслідування кіберінцидентів є складним та важливим процесом, який вимагає використання різних технік та інструментів. Ефективне розслідування кіберінцидентів потребує також спеціалізованих знань та навичок з області кібербезпеки та права. Розслідування може включати різноманітні методи та інструменти, такі як аналіз лог-файлів, електронна пошта, бази даних, мережі, веб-сайти та соціальні мережі.

Важливим кроком у розслідуванні кіберінцидентів є збір та аналіз інформації, яка може бути отримана з різних джерел. Це може включати аналіз лог-файлів, що містять інформацію про активність на комп'ютері або сервері, аналіз електронних листів та інших електронних повідомлень, аналіз мережевої активності, що включає в себе моніторинг мережевого трафіку та інші методи.

Під час збору та аналізу інформації важливо використовувати інструменти та техніки для збору та обробки даних. Наприклад, інструменти для збору інформації з веб-сайтів, такі як веб-сканери та веб-скрейпери, можуть допомогти зібрати інформацію про веб-сайти, які можуть бути пов'язані з кіберінцидентом.

Однією з ключових складових розслідування кіберінцидентів є аналіз доказів. Це може включати аналіз залишків вірусів, аналіз лог-файлів, аналіз схем баз даних та інші методи. Для аналізу доказів також використовуються спеціальні інструменти, такі як статичні та динамічні аналізатори вірусів, системи виявлення вторгнень та інші.

Крім того, у розслідуванні кіберінцидентів важливо використовувати методи та техніки для забезпечення безпеки. Наприклад, можуть використовуватися інструменти для виявлення та усунення вразливостей, щоб запобігти подальшим кібератакам.

Одним з ключових етапів розслідування кіберінцидентів є ідентифікація зловмисників. Для цього можуть використовуватися методи аналізу доказів та мережевої активності. Наприклад, можуть бути використані методи

відслідковування IP-адрес, виявлення шаблонів діяльності зловмисників та інші. У процесі розслідування кіберінцидентів важливо також забезпечити збереження та зберігання доказів. Це може включати зберігання копій даних, фіксацію мережевої активності, зберігання лог-файлів та інші методи.

Перелік посилань:

1. Birbaumer, N., & Cohen, L. G. (2007). Brain-computer interfaces: communication and restoration of movement in paralysis. The Journal of Physiology, 579(3), 621-636.
2. Choi, S., & Jo, S. (2020). The Future of Brain-Computer Interfaces (BCIs): Reviewing the Latest Trends in the Field. Journal of Korean Medical Science, 35(23), e210.
3. Farwell, L. A., & Donchin, E. (1988). Talking off the top of your head: Toward a mental prosthesis utilizing event-related brain potentials. Electroencephalography and Clinical Neurophysiology, 70(6), 510-523.
4. Fazel-Rezai, R., Allison, B. Z., & Guger, C. (2012). Brain computer interface: What neuroscience and robotics can learn from each other. Springer Science & Business Media.

Гайдур Ксенія Володимирівна
Студентка групи ТСД-41, ННІТ, ДУТ, Київ, Україна

МОНІТОРИНГ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІЗАЦІЙ

З кожним роком складність і кількість різних загроз інформаційної безпеки зростає, з'являються нові віруси і способи проникнення всередину IT інфраструктури. Проте разом з цим збільшується і число систем, покликаних захистити ваш бізнес від цих загроз.

Моніторинг інформаційних систем необхідний компаніям, щоб бути впевненими, що певна система працює як потрібно. Але процес моніторингу IT інфраструктури буває досить клопітким й іноді викликає труднощі, якщо моніторинг не налаштований належним чином. У 99% великих компаній функціонує міжмережевий екран, антивірусне рішення і система виявлення вторгнення — на сьогодні це є необхідний мінімум щоб вберегти вашу систему принаймні від частини можливих загроз. Такого захисту потребують не тільки корпорації, а й малий бізнес, не можна ігнорувати необхідність моніторингу серверів, баз даних, мережі, безпеки, інфраструктури тощо, всі підсистеми генерують реєстраційні журнали і різні події. А якщо компанія має кілька філій або віддалених офісів, то потік даних від інформаційних підсистем збільшується в десятки разів.

Адміністратори, які спостерігають, виявляють та вирішують проблеми безпеки щодня отримують сотні тисяч повідомлень від безлічі різноманітних підсистем. При цьому функціонування кожної з підсистем окремо критично для бізнесу в цілому, тому фахівці просто змушені аналізувати весь цей потік інформації. Виділити важливі повідомлення серед нескінченного потоку стає все складніше, і в результаті цінність окремих рішень для забезпечення безпеки прямує до нуля, а час відновлення інформаційної системи після збоїв катастрофічно зростає.

Саме через це дуже важливо використовувати якісні інструменти моніторингу, оскільки вони мають вирішальне значення в різних галузях промисловості та сферах, включаючи охорону здоров'я, виробництво, транспорт, енергетику та фінанси, бо вони відіграють вирішальну роль у

забезпеченні безпеки, ефективності та продуктивності. Надають дані та інформацію в режимі реального часу, які допомагають у виявленні та вирішенні проблем, покращенні операційної ефективності та покращенні процесів прийняття рішень.

Так, наприклад, моніторинг інфраструктури дата-центру здійснюють на трьох рівнях:

- на рівні датчиків;
- обладнання;
- інженерної системи в цілому.

Тобто, щоб моніторинг був ефективним спеціалісту необхідно бачити повну картину роботи IT інфраструктури в візуалізацією отриманих даних. Найбільш ефективним варіантом візуалізації на сьогодні вважається виведення температурних карт, оскільки вони надають можливість побачити кольорову карту всього приміщення та оперативно визначити місця з підвищеними або зниженими температурними показниками, а карта вологості, наприклад, дозволяє контролювати показники вологості в машинних залах.

Будь яка система моніторингу має відповідати таким вимогам:

Раннє виявлення проблем. Системи моніторингу можуть виявляти проблеми на ранній стадії, дозволяючи своєчасно втручатися, перш ніж вони переростуть у серйозні проблеми. Наприклад, у галузі охорони здоров'я системи моніторингу пацієнтів можуть допомогти виявити зміни життєво важливих ознак, що вказує на потенційні проблеми зі здоров'ям.

Безпека. Системи моніторингу мають важливе значення для забезпечення безпеки в таких галузях, як хімічна промисловість, гірничодобувна промисловість, нафтогазова промисловість. Ці системи можуть контролювати небезпечні умови, виявляти витоки та потенційні небезпеки, а також сповіщати працівників про вжиття відповідних заходів.

Підвищення ефективності. Системи моніторингу можуть допомогти підвищити ефективність роботи, надаючи дані в реальному часі про показники продуктивності, такі як продуктивність, споживання енергії та рівень запасів. Ця інформація може бути використана для виявлення неефективності та областей для покращення.

Моніторинг навколишнього середовища. Системи моніторингу мають вирішальне значення для моніторингу та підтримки умов навколишнього середовища. Ці системи можуть виявляти зміни якості повітря, води та погодних умов, надаючи цінні дані для кліматичних досліджень і управління навколишнім середовищем.

Енергоефективність. Системи моніторингу також важливі для підвищення енергоефективності в будівлях і спорудах. Ці системи можуть контролювати споживання енергії, визначати зони відходів і допомагати підприємствам і окремим особам зменшувати споживання енергії та витрати.

Контроль якості. Системи моніторингу мають вирішальне значення для забезпечення контролю якості виробництва та виробничих процесів. Ці системи можуть контролювати виробничі лінії, виявляти дефекти чи невідповідності та

гарантувати, що продукти відповідають стандартам якості.

Топ систем моніторингу:

NetFlow Analyzer — це програмне забезпечення Cisco для моніторингу пропускної здатності, яке розширює підтримку багатьох інших великих постачальників. Це програмне забезпечення для моніторингу пропускної здатності мережі, яке допомагає вам визначати та уникати затримок пропускної здатності за допомогою налаштованих звітів, які можуть шукати конкретні дані про використання пропускної здатності, такі як програми, IP-адреса, ім'я хоста, протокол тощо.

Окрім цих звітів про пропускну здатність, монітор пропускної здатності NetFlow Analyzer також допомагає контролювати пропускну здатність, щоб обмежити використання неважливих для бізнесу програм. Незважаючи на те, що відстеження всіх дій у мережі та керування ними є складним завданням для будь-якої організації, NetFlow Analyzer, як розширений інструмент моніторингу використання пропускної здатності, полегшує це за допомогою ефективного моніторингу використання пропускної здатності.

AppDynamics — надає комплексне рішення для моніторингу інфраструктури, яке охоплює компоненти сервера, сховища та мережі як у хмарних, так і в гібридних середовищах. Така система може бути розгорнута локально або використовувати як хмарну службу SaaS.

Можливості повного стека моніторингу цього інструменту допомагають співвідносити проблеми продуктивності програми з вузькими місцями інфраструктури низького рівня, прискорюючи тим самим аналіз основних причин і усунення.

Icinga — спочатку це був форк Nagios. Але з часом їх шляхи сильно розійшлися, тож можна вважати Icinga самостійним продуктом. Причому якісним та повністю безплатним. У системі є все, що треба для повноцінного моніторингу. Дані може збирати як за допомогою агентів, так і без них. Бекенд написано на C++, вебінтерфейс на php. Як БД підтримує MySQL, Oracle Database, PostgreSQL.

Підсумовуючи, системи моніторингу відіграють вирішальну роль у забезпеченні надійності, безпеки та продуктивності сучасних IT-операцій, є актуальними для організацій будь-якого розміру та в різних галузях. Безперервно збираючи та аналізуючи дані з різних джерел, системи моніторингу можуть надавати інформацію про стан IT-інфраструктури в реальному часі, дозволяючи організаціям виявляти та запобігати проблемам до того, як вони стануть серйозними. Це не тільки допомагає мінімізувати час простою та втрати даних, але й дає змогу організаціям оптимізувати свої операції, підвищити відповідність нормативним вимогам і визначити можливості для економії коштів і підвищення ефективності. Крім того, системи моніторингу можуть відігравати вирішальну роль у забезпеченні безпеки IT-інфраструктури, відстежуючи підозрілу активність і сповіщаючи адміністраторів про потенційні порушення безпеки. У сучасному дедалі складнішому та взаємопов'язаному IT-ландшафті інвестиції у комплексну систему моніторингу стали важливими для організацій, які

покладаються на технології для підтримки своїх бізнес-процесів і цілей.

Перелік посилань:
1.Системи моніторингу та управління безпекою [Електронний ресурс] – Режим доступу:http://integritysys.com.ua/security/siem/.
2.Системи моніторингу IT-інфраструктури [Електронний ресурс] – Режим доступу https://valtek.com.ua/ua/system-integration/it-infrastructure/monitoring-system/monitoring-system.
3.ТОП 20 систем моніторингу IT інфраструктури [Електронний ресурс] – Режим доступу: https://blog.iteducenter.ua/ratings/monitoring_tools/ .

Головань Владислав Вікторович
студент групи БСД-41, ННІЗІ ДУТ, Київ, Україна

ВПРОВАДЖЕННЯ VPN ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНИХ МЕРЕЖ

Оскільки все більше компаній переходять на хмару, забезпечення безпеки корпоративних мереж стає головним пріоритетом. Завдяки рішенням VPN (віртуальна приватна мережа) організації можуть створювати безпечне зашифроване з'єднання між віддаленими співробітниками та корпоративними мережами. У цьому звіті було досліджено впровадження сучасних рішень для забезпечення безпеки хмарних технологій, зокрема використання рішень VPN.
Ключові слова: VPN, конфіденційна інформація, Інтернет, корпоративна мережа, контроль доступу

Рішення VPN є популярним варіантом для компаній, які прагнуть забезпечити безпеку своїх хмарних технологій. За допомогою VPN віддалені співробітники можуть підключатися до корпоративної мережі через зашифрований тунель, гарантуючи безпеку всіх даних, що передаються між працівником і мережею. Рішення VPN можна реалізувати кількома способами, включаючи локальні сервери VPN або хмарні служби VPN.

Локальні сервери VPN — це фізичні сервери, розташовані на території компанії, які забезпечують безпечний доступ до корпоративної мережі. Ці сервери можна налаштувати так, щоб віддалені співробітники могли підключатися через VPN, забезпечуючи доступ до мережевих ресурсів і файлів. Локальні VPN-сервери зазвичай безпечніші, ніж хмарні VPN-сервіси, оскільки компанія має повний контроль над параметрами безпеки та конфігураціями сервера.

Хмарні VPN-сервіси стають все більш популярними серед компаній будь-якого розміру. Ці служби розміщені в хмарі, і до них можна отримати доступ з будь-якого місця, де є підключення до Інтернету. Хмарні VPN-сервіси зазвичай легше налаштувати та керувати ними, ніж локальні VPN-сервери, оскільки постачальник послуг займається більшою частиною обслуговування та безпеки.

Використання рішень VPN може надати ряд переваг компаніям, які прагнуть забезпечити безпеку своїх хмарних технологій. Ці переваги включають:
• Зашифровані з'єднання: рішення VPN забезпечують зашифроване з'єднання між віддаленими працівниками та корпоративними мережами, забезпечуючи безпеку всіх даних, що передаються.

- Віддалений доступ: рішення VPN дозволяють віддаленим працівникам отримувати доступ до мережевих ресурсів і файлів з будь-якого місця, де є підключення до Інтернету.
- Централізоване управління: можна централізовано керувати рішеннями VPN, що дозволяє адміністраторам контролювати доступ до мережевих ресурсів і відстежувати діяльність користувачів.
- Масштабованість: Рішення VPN можна легко масштабувати відповідно до зростаючих компаній, що полегшує додавання нових віддалених працівників і пристроїв.

У міру того, як компанії продовжують переходити в хмару, забезпечення безпеки корпоративних мереж стало головним пріоритетом. Рішення VPN забезпечують безпечне зашифроване з'єднання між віддаленими працівниками та корпоративними мережами, забезпечуючи безпеку всіх даних, що передаються. За допомогою локальних серверів VPN або хмарних служб VPN, впровадження сучасних рішень для забезпечення безпеки хмарних технологій є важливим для будь-якого бізнесу, який прагне залишатися безпечним і конкурентоспроможним у сучасному цифровому середовищі.

Перелік посилань:
1. What is a VPN?, Journal of Internet URL: https://www.cloudflare.com/learning/accessmanagement/what-is-a-vpn/
2. Rama Bansode, Anup Girdhar, Common Vulnerabilities Exposed in VPN – A Survey, Journal of Physics: Conference Series URL: https://iopscience.iop.org/article/10.1088/1742-6596/1714/1/012045

Довгалюк Максим Олегович,
студент групи БСД-41, ННІЗІ ДУТ,Київ,Україна

ІНФОРМАЦІЙНА БЕЗПЕКА В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Інформаційна безпека є критично важливою проблемою в безпроводових сенсорних мережах. Оскільки БСМ продовжують ставати все більш поширеними в різних додатках, важливо забезпечити їх захист від атак і вразливостей. Для захисту конфіденційності, цілісності та доступності даних, а також для забезпечення автентичності комунікацій та ідентифікації учасників необхідно впроваджувати надійні механізми і протоколи безпеки

Завдяки значному прогресу в технологіях безпроводового і мобільного зв'язку та широкому розвитку потенційних застосувань, безпроводові сенсорні мережі (БСМ) привернули до себе велику увагу в останні роки. Проте, БСМ формуються динамічно з декількох сенсорних вузлів з обмеженою потужністю і вузла-менеджера з тривалим живленням. БСМ - це самоорганізовані та автономні системи, що складаються із загальних сенсорів, вузлів-менеджерів та внутрішнього центру обробки даних [1]. Загальні датчики відповідають за передачу даних датчиків в реальному часі з конкретного середовища моніторингу на проміжні вузли збору даних, які називаються вузлами-розпорядниками. Внутрішній центр обробки даних отримає дані від вузлів-менеджерів для подальшої обробки та аналізу. Весь зв'язок між вузлами

здійснюється за допомогою безпроводових технологій передачі даних. Крім того, завдяки властивості самоорганізації, без підтримки фіксованої інфраструктури, топологія мережі динамічно змінюється, тому широкомовлення є основним способом зв'язку в БСМ.

Безпроводові сенсорні мережі широко використовуються у практичних застосуваннях, таких як моніторинг лісових пожеж, виявлення об'єктів військового призначення, медицина, наука і навіть у повсякденному житті. Однак, БСМ легко піддаються зловмисникам через те, що безпроводовий зв'язок використовує широкомовне середовище передачі даних і не є стійким до несанкціонованого втручання. Тому зловмисник може підслуховувати весь трафік, впроваджувати шкідливі пакети, відтворювати старі повідомлення або скомпрометувати сенсорний вузол. Інформаційна безпека у БСМ [2] передбачає захист конфіденційності, цілісності та доступності даних, а також забезпечення автентичності комунікацій та ідентифікації учасників. Деякі ключові проблеми безпеки в глобальних мережах включають:

Обмеженість ресурсів: БСМ мають обмежену обчислювальну потужність, пам'ять і енергію, що ускладнює реалізацію надійних заходів безпеки.

Розподілена природа: Мережі БСМ є дуже розподіленими і децентралізованими, що ускладнює централізоване управління безпекою.

Безпроводовий зв'язок: Безпроводовий зв'язок в мережах БСМ вразливий до атак перехоплення, підслуховування та глушіння.

Ненадійний зв'язок: Мережі БСМ часто розгортаються в суворих умовах, де зв'язок може бути переривчастим, зашумленим і ненадійним.

Для вирішення цих проблем для мереж БСМ було запропоновано ряд механізмів і протоколів безпеки [2]. До них відносяться:

Шифрування: Шифрування можна використовувати для захисту конфіденційності даних, що передаються через мережу. Алгоритми шифрування з симетричним ключем, такі як Advanced Encryption Standard (AES), зазвичай використовуються через їх низькі обчислювальні витрати.

Керування ключами: Управління ключами має вирішальне значення для підтримки цілісності та автентичності даних в БСМ. Протоколи створення і розподілу ключів, такі як криптографія еліптичних кривих і обмін ключами Діффі-Хеллмана, можуть бути використані для безпечного розподілу ключів між вузлами.

Аутентифікація: Механізми автентифікації можуть бути використані для перевірки особи учасників БСМ. Цифрові сертифікати та інфраструктура відкритих ключів можуть бути використані для встановлення довіри між вузлами. Добре структурований механізм автентифікації може гарантувати, що жоден неавторизований вузол не зможе шахрайським шляхом взяти участь у роботі та отримати конфіденційну інформацію від БСМ.

Виявлення та запобігання вторгнень: Системи виявлення та запобігання вторгнень можуть бути використані для виявлення та пом'якшення наслідків атак на мережу. Ці системи можуть використовувати виявлення аномалій, виявлення на основі сигнатур або гібридні підходи для виявлення атак.

Таким чином, інформаційна безпека є дуже важливою проблемою у БСМ, і для забезпечення конфіденційності, цілісності та доступності даних, що передаються датчиками, можуть бути застосовані різні механізми.

Перелік посилань:
1. What is WSN. https://www.techtarget.com/searchdatacenter/definition/sensor-network
2. Security of WSN. https://arxiv.org/ftp/arxiv/papers/1301/1301.5065.pdf

Довженко Надія Михайлівна
к.т.н, доцент, доцент кафедри Інформаційної та кібернетичної безпеки,
ННІЗІ ДУТ, Київ, Україна

ПЕРЕДУМОВИ РОЗРОБКИ ЗАХИЩЕНОЇ ІОТ МЕРЕЖІ

Інтернет речей (IoT) — це об'єднана мережа, що складається із фізичних компонентів або «речей», у які вбудовано програмне забезпечення та сенсорні датчики, що підключенні до мережі Інтернет. У свою чергу, це дозволяє елементам мережі збирати, опрацьовувати та здійснювати обмін даними про стан навколишнього середовища та підпорядкованих об'єктів. Однак головною проблемою цього IT сектора, що швидко розвивається, можна назвати безпеку.

Швидке поширення технології Інтернету речей стимулює розробку та вдосконалення впровадження компонентів штучного інтелекту та й взагалі інтелектуальної складової до датчиків та сенсорів, які щодня використовуються користувачами вдома, на робочих місцях і в промисловості. Підключати можна всі можливі пристрої – камери, телефони, датчики руху та освітлення, холодильники, вітрові турбіни та складне промислове обладнання.
Більшість «розумних» пристроїв в мережі IoT досить прості в реалізації та обслуговуванні, але це зовсім не означає, що вони при цьому нешкідливі. Про це свідчить, наприклад, широкомасштабна DDoS-атака, яка залишила основні веб-сайти, такі як Twitter, Amazon, PayPal, недоступними через заливання ключів DNS-серверів. Для цієї атаки використовувався ботнет, який містив неправильно захищені пристрої IoT, часто з паролями за замовчуванням. В свою чергу, така ситуація підкреслює важливість належного захисту мереж IoT та їх складових компонентів.
Якщо окремо розглянути особливості розгортання звичайних мереж IoT, то можна виокремити цілу низку проблем безпеки. Ці проблеми можуть випливати із наступних факторів:

- технічний характер. Більшість систем IoT складається зі значної кількості необслуговуваних елементів з низькими обчислювальними можливостями. З цього можна зробити висновок, що якщо хоча б один із елементів мережі неналежним чином захищений, уся мережа може стати вразливою;
- особливості процесів проєктування мереж IoT. Пристрої та датчики, що використовуються, часто вироблені масово та з дешевих складових компонентів. Тому проблема ще більше ускладнюється від факту появи ненадійного вузла для відмовостійкості та надійності мережі в цілому;

- нехтування питанням конфіденційності. Це питання стосується використання багатьох систем та мереж IoT, які здатні скомпрометувати конфіденційність користувача, безпосередньо або опосередковано.

Ці фактори в сукупності вказують на те, що безпека повинна бути центром уваги розробки будь-якої системи IoT, навіть більше, ніж іншої мережі[1].

Якщо ж розглядається розгортання спеціалізованої мережі IoT, наприклад IIoT (промислова «розумна» мережа), або ж IoT мережа, призначена для виконання критично важливих завдань, то вимоги щодо алгоритмів та методології для забезпечення безпеки будуть жорсткішими. Тому всі питання, пов’язані з кібербезпекою, особливо атак, їх запобігання та пом'якшення є дуже важливими для створення безпечної та надійної мережі IoT[2].

В загальному розумінні, рішення для захисту від атак на мережі, складаються з трьох основних компонентів:

- *Запобігання*. Цей компонент спрямований на запобігання атакам до їх виникнення. У цьому випадку будь-який запропонований метод повинен мати можливість розробки заходів захисту від конкретного типу атаки[3]. Механізми запобігання вторгненням можуть протистояти зовнішнім зловмисникам IoT, але вони не призначені для протидії внутрішнім загрозам, наприклад;
- *Виявлення*. У випадку атаки, якщо зловмиснику вдається протидіяти заходам запобігання, це означає, що захист від атаки не вдався. В цьому випадку необхідно щоб елементи системи IoT оперативно реагували та виявляли ті вузли, які були скомпрометовані. Єдиним способом виявлення таких елементів прийнято вважати використання системи виявлення вторгнень (IDS). Після виявлення вторгнення запускається механізм пом’якшення, для мінімізації негативних наслідків атаки;
- *Пом’якшення.* Останній компонент спрямований на пом’якшення атак після їх виникнення [4]. Для здійснення ефективного захисту мережі, необхідно вжити заходів безпеки, таких як вимкнення постраждалих вузлів з впливу на інші елементи мережі або вимкнення портів мережевого обладнання, яке було використане під час атаки (шлюз, маршрутизатор тощо).

Таким чином, усі ці три компоненти здатні скласти цілісну структуру безпеки і не можуть розглядатися окремо при захисті мереж IoT та їх складових від різних видів атак.

Перелік посилань:

1. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao. «A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications». IEEE Internet of Things Journal. Vol.4. №5. Pp.1125–1142. 2017.
2. I.Butun, S. D. Morgera, R. Sankar. «A survey of intrusion detection systems in wireless sensor networks». IEEE communications surveys and tutorials. Vol.16. № 1. Pp.266–282. 2014.
3. Y. Liu, M. Dong, K. Ota, A. Liu. «Activetrust: secure and trustable routing in wireless sensor networks». IEEE Transactions on Information Forensics and Security. Vol.11. №9. Pp.2013–2027.2016.
4. S. Bhunia, M. Gurusamy. «Dynamic attack detection and mitigation in IoT using SDN». Telecommunication Networks and Applications Conference (ITNAC). Pp.1–6. 2017

Іваненко Поліна Олегівна
студентка групи БСД-43, ННІЗІ ДУТ, Київ, Україна

ПІДВИЩЕННЯ БЕЗПЕКИ В МЕРЕЖАХ IoT ЗА ДОПОМОГОЮ ВИКОРИСТАННЯ РОЗШИРЕНОГО КОНТРОЛЮ ДОСТУПУ ТА АВТЕНТИФІКАЦІЇ

Інтернет речей (IoT) — це мережа підключених пристроїв, у які вбудовано датчики, програмне забезпечення та інші технології, що дозволяє їм спілкуватися та обмінюватися даними один з одним та з іншими системами через Інтернет. IoT має потенціал змінити спосіб життя, роботи та взаємодії з навколишнім світом. Він уже відіграє значну роль у трансформації таких галузей, як охорона здоров'я, транспорт, виробництво та сільське господарство. Інтернет речей стає все більш важливим у нашому житті завдяки своїй здатності підвищувати ефективність, продуктивність і зручність, а також пропонувати нові можливості для інновацій і зростання.

Оскільки Інтернет речей (IoT) продовжує розвиватися та стає все більш поширеним, питання безпеки стають дедалі важливішими. Через величезну кількість взаємопов'язаних пристроїв і величезні обсяги даних, що передаються, існує багато можливостей для кібератак і витоку даних. Контроль доступу та автентифікація є двома важливими компонентами безпеки Інтернету речей, які можуть допомогти зменшити ці ризики.

Контроль доступу стосується процесу надання або заборони доступу до ресурсів на основі попередньо визначених політик. Існують різні типи моделей контролю доступу, включаючи дискреційний, обов'язковий і рольовий контроль доступу. У контексті IoT контроль доступу можна використовувати для обмеження доступу до пристроїв, мереж і даних, гарантуючи, що лише авторизовані користувачі та пристрої можуть отримати до них доступ. Однак впровадження контролю доступу в IoT представляє проблеми та обмеження. Однією з головних проблем є масштабованість. Зі збільшенням кількості пристроїв зростає і обсяг створюваних даних, що може швидко перевантажити існуючу мережеву інфраструктуру. Традиційний підхід централізації зберігання й обробки даних більше неможливий у масштабних розгортаннях IoT [1].

Іншою проблемою є різноманітність пристроїв і протоколів IoT. Існує багато виробників пристроїв Інтернету речей, кожен зі своїми власними протоколами та стандартами, через що може бути складно забезпечити взаємодію та безперебійну інтеграцію між пристроями. Це розмаїття також ускладнює розробку комплексної системи безпеки, яка може вирішувати унікальні виклики безпеки, створені різними пристроями.

На масштабованість також впливають обмеження основної комунікаційної інфраструктури. Багато пристроїв IoT працюють у віддалених або жорстких середовищах, де традиційне підключення до мережі може бути недоступним або надійним [2]. Це ускладнює створення надійної мережевої інфраструктури, яка може підтримувати потреби підключення всіх пристроїв.

Стандартизація протоколів і комунікаційних інтерфейсів також має вирішальне значення для забезпечення сумісності та бездоганної інтеграції між різними пристроями. Це вимагає співпраці між виробниками, галузевими органами та регуляторними органами для встановлення спільних стандартів для пристроїв IoT [1].

Забезпечення безпеки пристроїв і мереж Інтернету речей має важливе значення для запобігання кібератакам і витоку даних. Необхідно прийняти комплексну структуру безпеки, яка вирішує унікальні проблеми безпеки пристроїв Інтернету речей та інтегрує технології контролю доступу, автентифікації та шифрування.
Автентифікація є ще одним важливим компонентом безпеки IoT. Він передбачає перевірку ідентичності користувачів і пристроїв, які намагаються отримати доступ до мережі або даних. Автентифікацію можна здійснити за допомогою різних методів, включаючи паролі, біометричні дані та сертифікати. В IoT автентифікація особливо важлива, оскільки багато пристроїв розроблено для віддаленого доступу, що робить їх уразливими для несанкціонованого доступу.
Щоб підвищити безпеку в IoT за допомогою контролю доступу та автентифікації, можна реалізувати кілька методів. Одним із підходів є використання надійного шифрування для захисту даних під час передавання та зберігання. Цього можна досягти за допомогою безпечних протоколів зв'язку, таких як Transport Layer Security (TLS) і Secure Sockets Layer (SSL). Використання цифрових сертифікатів та інфраструктури відкритих ключів (PKI) також може покращити автентифікацію, надаючи надійний механізм для перевірки ідентичності пристроїв і користувачів.
Інший підхід полягає у використанні керування доступом на основі ролей (RBAC), який дозволяє отримати доступ до ресурсів на основі ролі користувача або пристрою. RBAC можна реалізувати в IoT шляхом визначення ролей на основі типів пристроїв, розташування або функцій. Наприклад, сенсорний пристрій на заводі може мати іншу роль і права доступу, ніж розумний термостат у домі [2].
Впровадження контролю доступу та автентифікації в IoT також вимагає співпраці між різними зацікавленими сторонами, включаючи виробників пристроїв, постачальників послуг і кінцевих користувачів. Виробники пристроїв повинні з самого початку вбудувати функції безпеки у свої пристрої, а постачальники послуг повинні гарантувати безпеку своїх мереж і послуг. Кінцеві користувачі також повинні знати про ризики безпеці та вживати відповідних заходів для захисту своїх пристроїв і даних [1].
Підводячи підсумки, контроль доступу та автентифікація є критично важливими компонентами безпеки IoT, які можуть допомогти зменшити ризики безпеки та захистити конфіденційні дані. Незважаючи на те, що впровадження контролю доступу та автентифікації в IoT викликає проблеми та обмеження, можна застосувати кілька методів для підвищення безпеки, включаючи надійне шифрування, RBAC та співпрацю між різними зацікавленими сторонами. Оскільки IoT продовжує розвиватися та стає все більш повсюдним, дуже важливо віддавати пріоритет безпеці, щоб гарантувати, що переваги IoT реалізуються при мінімізації ризиків для конфіденційності та безпеки.

Перелік посилань:

1. Access Control and Authentication in the Internet of Things Environment [Електронний ресурс] – Режим доступу: https://www.download-paper.com/wp-content/uploads/2016/09/2016-springer-Access-Control-and-Authentication-in-the-Internet-of-Things-Environment.pdf

2. Internet of Things Security, Device Authentication and Access Control: A Review [Електронний ресурс] – Режим доступу: https://arxiv.org/ftp/arxiv/papers/1901/1901.07309.pdf

Івахненко Кирило Володимирович
Студент групи БСД-41,ННІЗІ ДУТ, Київ, Україна

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ БЕЗПРОВОДОВОЇ МЕРЕЖІ ІЗ ВИКОРИСТАННЯ CISCO IDENTITY SERVICES ENGINE

Анотація. Комплексне рішення для планування та контролю політик безпеки як у дротових, так і в бездротових мережах. Варто відзначити той факт, що ISE стає ключовим елементом безпеки, збираючи інформацію про те, хто, де та за допомогою якого пристрою намагається підключитися до нашої мережі. У цьому контексті та з використанням сегментації мережі, визначеної програмним забезпеченням, ISE є правильною системою для впровадження Zero-Trust Security.

Cisco ISE — це універсальне рішення для оптимізації політики безпеки управління та зниження експлуатаційних витрат. За допомогою ISE можна бачити користувачів і пристрої, які контролюють доступ через проводові, безпроводові та VPN-підключення до корпоративної мережі. Cisco ISE дозволяє надавати високобезпечний мережевий доступ до користувачів і пристроїв. Це допомагає зрозуміти, що відбувається в мережі, наприклад, хто підключений, які програми встановлені та запущені та багато іншого. Це також ділиться життєво важливими контекстними даними, такими як ідентифікаційні дані користувачів і пристроїв, загрози та вразливості з інтегровані рішення від технологічних партнерів Cisco, щоб можна було виявляти, стримувати та усувати загрози швидше [2].

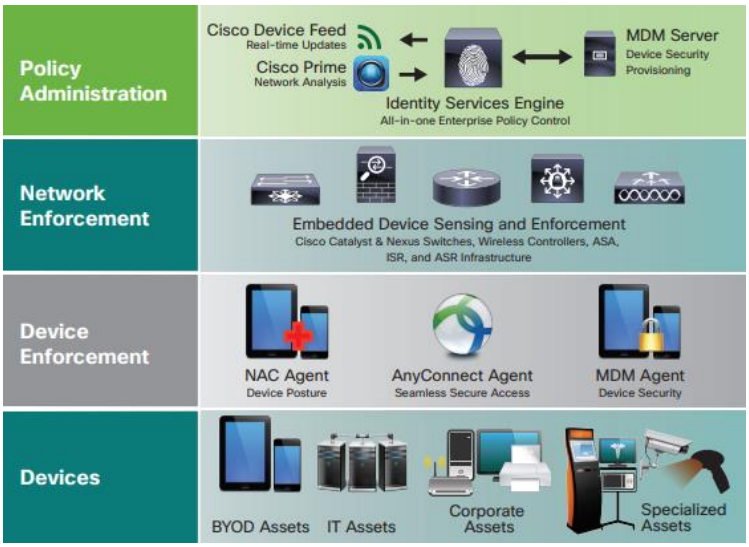


Рис.1 - Компоненти розгортання Cisco Identity Services Engine (ISE) [1, с. 1].

Функціональні можливості. Будучи сервером Radius, Cisco ISE підтримує функції, які підтримують класичні сервери Radius (такі як добре відома Cisco

ACS – система контролю доступу). Отже, розгорнувши Cisco ISE, можна запустити:

- Механізм 802.1x у мережі Wi-Fi
- Механізм 802.1x у проводовій мережі
- Аутентифікація та налаштування атрибутів для користувачів, підключених через VPN
- MAC Authentication Bypass (MAB), що означає автентифікацію пристрою за допомогою MAC-адрес

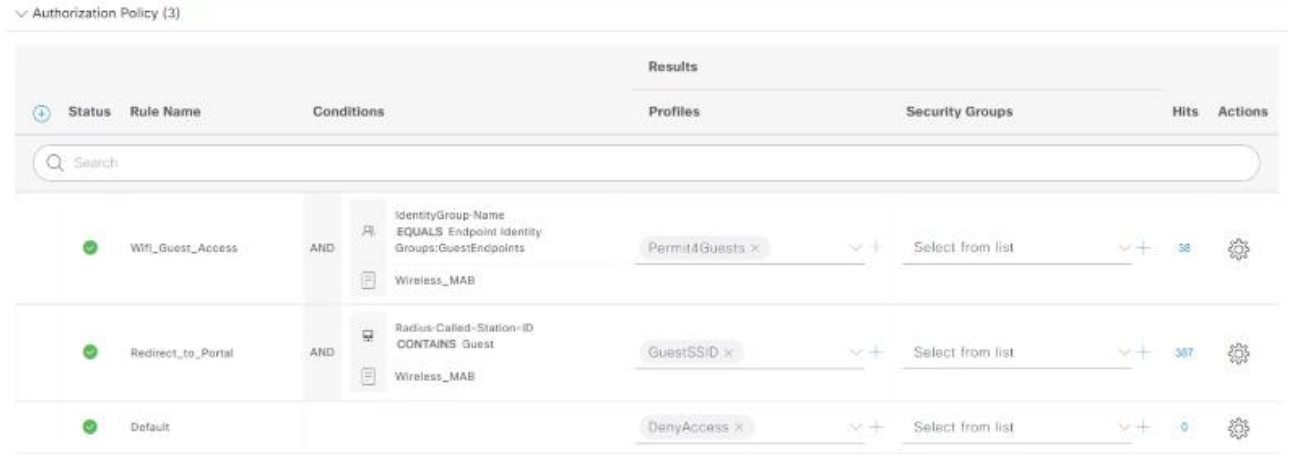


Рис. 2 – Процес авторизації гостя в ISE

Механізми. Identity Services Engine використовує так звані розширені зв'язки Radius CoA (Change of Authorization), які роблять можливою динамічну взаємодію між вузлом ISE (Policy Service Node) і мережевими пристроями, такими як комутатори, маршрутизатори, мережеві контролери Wi-Fi та брандмауери.

Профілювання. Здатність ISE розуміти тип пристрою, браузер, виробника, тип пристрою, як-от телефон чи ноутбук, і ОС, дозволяє реагувати, наприклад, під час передачі пакету з налаштованим запитувачем 802.1x, тобто частиною програмного забезпечення відповідає за підключення клієнтів до захищеної мережі 802.1x для користувача.

За допомогою профілювання Cisco ISE надсилає потрібний пакет на потрібний пристрій, наприклад, інший на MacBook з OSX і інший на пристрій Lenovo з Windows 10 [2].

Переваги:

• Неперевершена видимість у мережі з великими можливостями профілювання точно ідентифікувати та оцінювати всіх користувачів і пристрої, які підключаються до мережі.

• Надзвичайно надійний контроль для надання, обмеження та карантинного доступу до мережі узгодження з відповідною бізнес-політикою компанії або дотримання вимог безпеки вимоги та рекомендації.

• Широке, послідовне застосування політики за допомогою засобів контролю доступу до мережі, пристрою MDM безпеку та пом'якшення загроз SIEM/TD, щоб виявити загрози безпеці та пом'якшити поширення атак у мережі.

• Зменшення операційних витрат завдяки ефективності за рахунок використання вбудованого датчика і забезпечення виконання в існуючій мережі в поєднанні з централізованою політикою контроль і видимість мережі для оптимізації зусиль щодо безпечного доступу [1, с. 2].

Оцінка стану. Механізм, відомий із таких рішень, як Мережевий доступ/Контроль доступу (NAC), який використовується для перевірки кінцевої системи, яка підключається до мережі, на відповідність умовам, які застосовуються політикою безпеки. Такими умовами є, наприклад, наявність антивірусного програмного забезпечення, виправлень ОС або інших ключових програм для певної організації. Під час перевірки Posture може перенаправити перевірену систему для завершення будь-яких відсутніх елементів [2].

Перелік посилань:

1. Glance A. A. Cisco Identity Services Engine (ISE) / A. Glance // Cisco. – 2013. URL: https://www.infranetgroup.com/wp-content/uploads/2014/07/ise.pdf
2. Osmałek K. Cisco Identity Service Engine. Secure Network Access / Krzysztof Osmałek // Grandmetric. – 2022. URL: https://www.grandmetric.com/cisco-ise-what-is-identity-services-engine/

Качний Кирило Сергійович
студент групи БСДМ-53, ННІЗІ ДУТ, Київ, Україна

ЗАГРОЗИ БЕЗПЕКИ IoT

Інтернет речей (IoT) - це технологія, яка стає все більш популярною в сучасному світі. Її використання охоплює багато різних сфер життя, від побутових пристроїв до промислових систем. Однак, як і будь-яка технологія, IoT має свої ризики та виклики, особливо в питаннях безпеки.

Існують різні загрози для безпеки IoT, які можуть стати причиною витоку конфіденційної інформації, злому системи або зниженню її ефективності. Серед них можна виділити наступні:

1. Недостатня захищеність пристроїв. Часто IoT-пристрої розробляються з пріоритетом на швидкість та економію ресурсів, а не на безпеку. Це може призвести до недостатньої захищеності пристроїв та їх вразливості перед зловмисниками.
2. Недостатня захищеність мережі. IoT-пристрої часто підключаються до мережі без будь-якого контролю або захисту. Це може дозволити зловмисникам здійснювати атаки на мережу або отримувати конфіденційну інформацію.
3. Відсутність оновлень. Багато виробників IoT-пристроїв не забезпечують оновлення безпеки для своїх пристроїв. Це означає, що вони залишаються вразливими до нових загроз.

Для захисту IoT від різноманітних загроз можна вжити такі заходи:

4. Встановлення захисних механізмів на рівні пристроїв. IoT-пристрої повинні мати вбудовані захисні механізми, такі як шифрування, аутентифікація

та авторизація, що дозволить запобігти несанкціонованому доступу до даних та забезпечить безпеку пристроїв в цілому.

5. Захист мережі. Важливо забезпечити безпеку мережі, до якої підключені IoT-пристрої. Для цього можна використовувати фаєрволи, віртуальні приватні мережі та інші засоби захисту, які дозволять заблокувати небажані підключення до мережі.

6. Підтримка безпеки. Виробники IoT-пристроїв повинні забезпечувати оновлення безпеки для своїх пристроїв. Це означає, що вони повинні виправляти виявлені вразливості та випускати патчі для своїх пристроїв. Також важливо забезпечити належний захист та шифрування даних, які передаються між пристроями та серверами.

7. Використання сильних паролів та двофакторної аутентифікації. Важливо використовувати складні паролі для доступу до IoT-пристроїв та регулярно їх змінювати. Для додаткової захисту можна використовувати двофакторну аутентифікацію, що дозволить забезпечити безпеку підключення до пристроїв.

8. Моніторинг даних та аналіз поведінки. Важливо моніторити дані, які передаються між пристроями та серверами, а також поведінку користувачів та пристроїв.

Кліменченко Владислав Сергійович
студент групи БСД-42, ННІЗІ ДУТ, Київ, Україна

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИКОРИСТАННЯ OPENVPN ДЛЯ ЗАХИСТУ ПЕРЕДАЧІ ІНФОРМАЦІЇ В ЛОКАЛЬНІЙ МЕРЕЖІ

Вивчення способів і розробка рекомендацій щодо використання OpenVPN для захисту передачі даних у локальній мережі передбачає вивчення переваг і недоліків використання OpenVPN як безпечного методу передачі даних. OpenVPN — це широко розповсюджене рішення віртуальної приватної мережі (VPN) із відкритим кодом, яке забезпечує безпечну та зашифровану передачу даних через Інтернет.

Щоб розпочати дослідження, слід оцінити мережну інфраструктуру та вимоги користувачів. Потім дослідження має бути зосереджено на визначенні найкращої конфігурації та налаштування OpenVPN для мережі. Рекомендована настройка повинна враховувати кількість користувачів, тип даних, що передаються, і необхідний рівень безпеки. На Рис.1 який показаний нижче можна побачити як працює тунелювання для багатьох клієнтів [1].

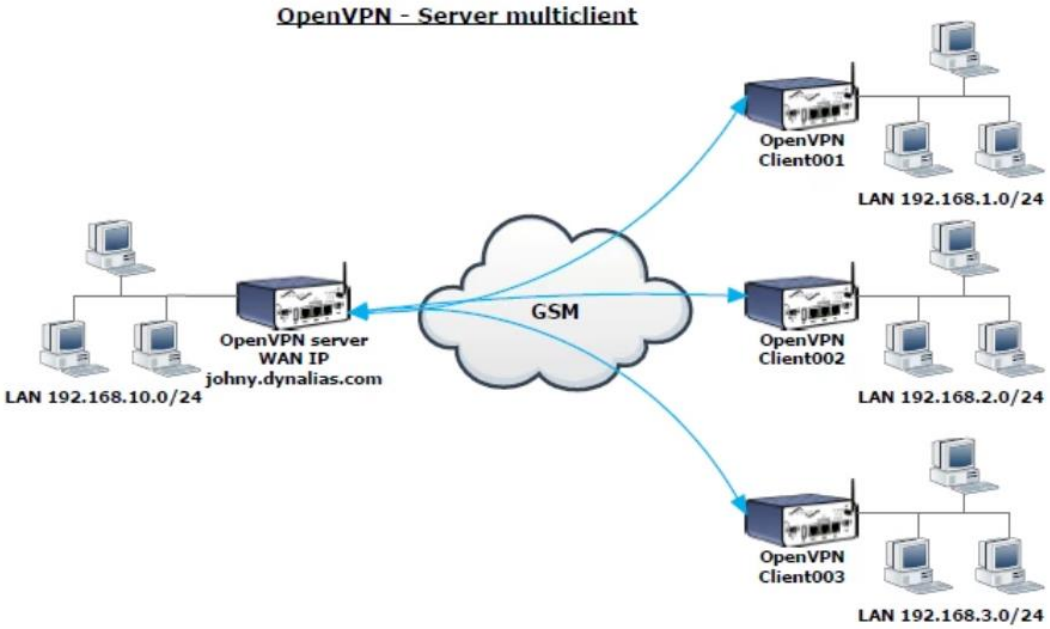


Рис.1 - Сервер мультиклієнт OpenVPN

Ось короткий огляд того, як працює OpenVPN у мультиклієнтній конфігурації сервера [2]:

1. Встановіть та настройте OpenVPN на сервері. Перший крок – налаштувати OpenVPN на сервері. Це включає встановлення програмного забезпечення OpenVPN, налаштування сервера для роботи в якості кінцевої точки VPN і створення необхідних криптографічних ключів і сертифікатів.
2. Створення файлів конфігурації клієнта: після налаштування сервера необхідно створити файли конфігурації для кожного клієнта, який буде підключатися до сервера. Ці файли містять таку інформацію, як криптографічні ключі та сертифікати клієнта, а також IP-адресу та порт сервера.
3. Розповсюдження файлів конфігурації клієнта. Файли конфігурації клієнта повинні бути розповсюджені на кожен клієнтський пристрій або користувача. Це можна зробити вручну або за допомогою автоматизованого процесу, залежно від кількості клієнтів та складності мережі.
4. Підключення клієнтів до сервера. Маючи конфігураційні файли клієнта, клієнти можуть підключатися до сервера за допомогою клієнтського програмного забезпечення OpenVPN. Програмне забезпечення клієнта ініціює підключення до сервера та узгоджує параметри VPN-підключення, включаючи криптографічні ключі та алгоритми шифрування.
5. Безпечна передача даних: після встановлення VPN-підключення клієнти можуть безпечно передавати дані між своїм пристроєм та сервером. Ці дані зашифровані та захищені від прослуховування та інших видів атак.

Таким чином, OpenVPN у багатоклієнтській конфігурації сервера дозволяє кільком клієнтам безпечно підключатися до одного сервера через Інтернет. Сервер діє як кінцева точка VPN і шифрує всі дані, що передаються між клієнтами та сервером, забезпечуючи конфіденційність та безпеку мережного

трафіку [2].

На Рис.2 ми можемо побачити пропускну здатність та затримку нашого рішення OpenVPN server [2].

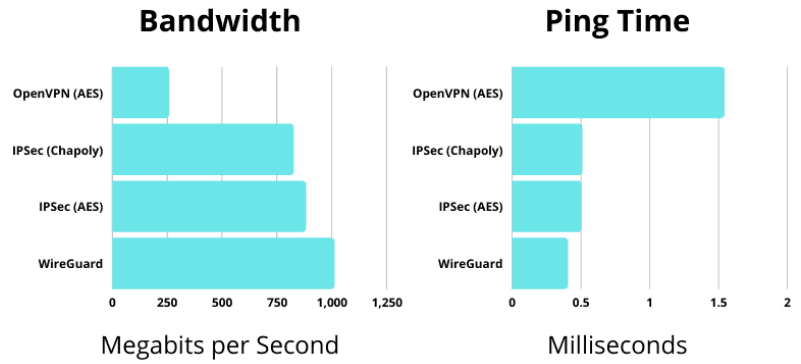


Рис.2 – Затримка та пропускна здатність OpenVPN server

Ця теза спрямована на оцінку продуктивності та безпеки OpenVPN в захищеній мережі у порівнянні з іншими протоколами VPN. Оцінка буде проводитись за допомогою серії експериментів та симуляцій, які перевіряють протоколи в різних умовах, таких як затримка в мережі, обмеження пропускної спроможності та надійність шифрування. В ході експериментів також буде вивчено вплив різних конфігурацій та оптимізації на продуктивність та безпеку за допомогою OpenVPN [2, 3].

Важливо зазначити, що підхід до побудови захищеної мережі на основі побудови мультиклієнтського серверу на прикладі OpenVPN, буде ефективним надійним рішенням яке зможе забезпечити надійне шифрування, автентифікацію та цілісніть даних. Його гнучкість, сумісність із брандмауером та функція екстреного відключення від мережі роблять його популярним вибором серед користувачів, які віддають пріоритет конфіденційності та безпеки [3].

Перелік посилань:

1. «ADVANTECH: OpenVPN server» [Електронний ресурс] – https://icr.advantech.cz/support/faq/detail/how-to-create-an-openvpn-server-multiclient-on-a-router
2. «Freecodecamp – How to Secure your Network Connections Using OpenVPN» [Електронний ресурс] – https://www.freecodecamp.org/news/securing-your-network-connections-using-openvpn/
3. «Geeksforgeeks – Threats to Information Security» [Електронний ресурс] – https://www.geeksforgeeks.org/threats-to-information-security/

Козерема Вікторія Андріївна
студентка групи УФЕ-31с, ЛНУ імені Івана Франка, Львів, Україна

ПРОБЛЕМИ БЕЗПЕКИ ХМАРНИХ ТЕХНОЛОГІЙ ТА ТИПИ ІНСТРУМЕНТІВ ДЛЯ БЕЗПЕКИ В ХМАРІ

Хмарні технології — це спосіб надання обчислювальних потужностей як послугу через мережу.

Завдяки використанню хмарних технологій користувачі отримують більше місця для зберігання даних, адже сховище не обмежується місткістю будь-якого фізичного пристрою. Також хмара дозволяє за потреби гнучко збільшувати та зменшувати кількість оперативної пам’яті, віртуальних машин, дисків тощо. Працівники підключаються до сервісів із будь-якої точки світу та з будь-якого гаджета, що сприяє кращій взаємодії між віддаленими командами. Також завдяки хмарним технологіям можна відновити втрачені дані у випадку їх видалення [1].

У випадку використання хмарних обчислювальних служб без належних заходів безпеки, зловмисники мають можливості викрадення даних, знищення конфіденційних файлів, несанкціонованого віддаленого входу у хмарну систему.

Захистом хмарних даних та хмарної інфраструктури від внутрішніх та зовнішніх загроз займається хмарна безпека, інструменти якої дбають про безпеку інформації, не обмежуючи можливості користувача легко отримувати до неї доступ [2].

Взаємопов’язаність хмар дає змогу з легкістю працювати та взаємодіяти у віртуальному середовищі, але водночас сприяє виникненню ризиків для безпеки. Користувачам хмарних технологій потрібні рішення, які допомагають вирішувати наведені нижче ключові проблеми безпеки в хмарі.

- Недостатня видимість даних;

Щоб організації працювали максимально продуктивно, IT-відділам потрібно надавати працівникам, бізнес-партнерам і підрядникам доступ до корпоративних ресурсів та даних. Оскільки багато людей використовують свої пристрої для доступу до корпоративних ресурсів у різних загальнодоступних і приватних хмарах, дуже важко відстежувати, які служби використовуються та як дані переміщуються в хмарі. Командам технічних спеціалістів потрібно стежити за тим, щоб дані не переміщувалися до менш захищених розташувань, а також запобігати несанкціонованому доступу до делікатної інформації.

- Комплексні середовища;

Завдяки хмарі значно простіше розгортати інфраструктури та програми. Завдяки тому, що існує велика кількість різних постачальників, IT-відділи можуть вибрати середовище, яке найкраще відповідає вимогам продукту та служби. Такий підхід призводить до появи комплексних середовищ, що охоплюють локальні ресурси, а також загальнодоступні й приватні хмари. Для роботи в гібридному багатохмарному середовищі потрібні рішення для безпеки, які охоплюють усю екосистему та захищають користувачів, які отримують доступ до різних ресурсів із різних розташувань. У таких комплексних середовищах часто виникають помилки конфігурації.

- Швидке впровадження інновацій;

Сукупність різних факторів сприяє швидкому впровадженню інновацій і розгортанню нових продуктів в організаціях. Технології штучного інтелекту, машинного навчання й Інтернету речей дають компаніям змогу ефективніше збирати та використовувати дані. Постачальники хмарних служб пропонують малокодові та безкодові рішення, які спрощують використання новітніх

технологій у компаніях. Процеси DevOps скорочують цикл розробки. Оскільки все більше корпоративної інфраструктури зберігається в хмарі, багато організацій перерозподіляють ресурси для досліджень і розробок. Недолік швидкого впровадження інновацій полягає в тому, що через стрімкий розвиток технологій стандарти безпеки часто ігнорують.

- Відповідність вимогам і керування;

Попри те, що більшість основних постачальників хмарних служб дотримуються кількох відомих програм акредитації, саме їхні клієнти відповідають за забезпечення відповідності своїх робочих процесів урядовим і внутрішнім стандартам.

- Внутрішні загрози.

Людський фактор часто стає причиною виникнення ризиків для безпеки компанії. Багато порушень безпеки виникають тоді, коли працівник переходить за посиланням і таким чином завантажує шкідливе програмне забезпечення. На жаль, самі працівники організацій іноді навмисно розголошують дані.

Для зменшення вразливості в хмарі та ризику несанкціонованого доступу користувачів до делікатних даних використовують наступні інструменти для безпеки в хмарі:

- Керування захищеністю хмари;

Рішення для керування захищеністю хмари допомагає зменшувати ризики, постійно скануючи середовище на наявність помилок конфігурації, які можуть призвести до порушення безпеки. Ці автоматизовані рішення зменшують ризик виникнення помилок у рутинних процесах і покращують видимість середовищ із тисячами служб та облікових записів. Після виявлення вразливостей розробники можуть усунути їх за допомогою покрокових рекомендацій. Крім того, рішення для керування захищеністю хмари постійно сканує середовище на наявність зловмисних дій або несанкціонованого доступу.

- Платформа захисту хмарної інфраструктури;

Платформа захисту хмарної інфраструктури допомагає захищати обчислювальні, накопичувальні та мережеві можливості програм у хмарі. Вона виявляє робочі процеси в загальнодоступних, приватних і гібридних хмарних середовищах та сканує їх на наявність уразливостей.

- Посередники, які забезпечують захищений доступ до хмари;

Посередники, які забезпечують захищений доступ до хмари (CASB), допомагають IT-відділам стежити за використанням хмарних програм і оцінювати ризики кожної з них. Ці рішення також допомагають захищати дані та забезпечувати відповідність вимогам за допомогою інструментів, які показують, як дані переміщуються в хмарі. Організації також використовують ці інструменти, щоб виявляти підозрілу поведінку користувачів і усувати загрози.

- Керування ідентичностями та доступом;

Організації використовують рішення для керування ідентичностями та доступом, щоб перевіряти ідентифікаційні дані, обмежувати доступ до

делікатних ресурсів, застосовувати багатофакторну автентифікацію й політики доступу з мінімальними правами.

- Керування правами на використання хмарної інфраструктури.

Рішення для керування правами на використання хмарної інфраструктури дає компаніям змогу визначати, до яких ресурсів надається доступ, хто його отримує та з якої хмарної платформи. ІТ-команди також використовують ці продукти для застосування різних політик безпеки, зокрема політик доступу з мінімальними правами[3].

Використання хмарних технологій забезпечує надають нам безліч переваг при користуванні ними, проте не варто забувати про безпеку даних, конфіденційних файлів та самої хмарної системи, яка може зазнати внутрішніх та зовнішніх загроз при необізнаності щодо проблем безпеки хмарних технологій та не використанні інструментів безпеки в хмарі.

Перелік посилань:
1. Хмарні технології: що це та які переваги надають людям для бізнес [Електронний ресурс] – Режим доступу: https://gigacloud.ua/blog/navchannja/scho-take-hmarni-tehnologii
2. Що таке хмарна безпека? Захист у хмарі [Електронний ресурс] – Режим доступу: https://nordvpn.com/uk/cybersecurity/cloud-security/
3. Що таке безпека в хмарі? [Електронний ресурс] – Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cloud-security

Козерема Вікторія Андріївна
студентка групи УФЕ-31с, ЛНУ імені Івана Франка, Львів, Україна

ПОШИРЕНІ АТАКИ НА ІОТ ПІДПРИЄМСТВ ТА ЗАХИСТ ВІД НИХ

Інтернет речей – це мережа фізичних об’єктів із вбудованими технологіями, які дозволяють взаємодіяти із зовнішнім середовищем, передавати інформацію про їхній стан та отримувати дані ззовні [1]. Тобто, по суті, це екосистема підключених до Інтернету пристроїв і технологій, які постійно збирають і передають дані. Пристрої Інтернету речей (IoT) значно спрощують повсякденне життя людей і роботу організацій.

На жаль, ідеальних технологій просто не існує. Попри популярність і зручність IoT-пристроїв, вони також мають недоліки. Оскільки людського втручання в IoT мало, стає складніше відстежити підозрілу активність або наявність вірусів. Кожен пристрій IoT є потенційно вразливою точкою входу в мережі та бізнес-процеси [3].

З розвитком технологій кібербезпека пристроїв стає все більш критичною проблемою. Це особливо очевидно в контексті Інтернету речей, оскільки кількість пристроїв, які можуть отримувати та надсилати конфіденційні дані, зростає щодня.

Впровадження та оновлення заходів безпеки пристроїв має бути пріоритетом для технологій IoT, оскільки вони вразливі до:

- DDoS-атак: виникають, коли ботнет (мережа заражених комп'ютерів) постійно заповнює систему запитами. Незвично висока активність може спричинити значні затримки або навіть призупинити роботу системи. Добре налаштована та налаштована DDoS-атака може спричинити збій компонентів безпеки, маскуючи фактичну шкідливу активність. Крім того, заражені пристрої IoT також можуть стати частиною ботнетів і допомогти зловмисникам здійснювати більш деструктивні атаки з локальних мереж, які зазвичай мають вищий рівень довіри до систем інформаційної безпеки.
- Експлуатації програмного забезпечення: багато кіберзлочинців використовують відомі вразливості в програмній частині пристрою для здійснення своїх атак. Розробники зазвичай закривають виявлені «діри» в безпеці в оновленнях. Однак нові версії програмного забезпечення не завжди завантажуються на пристрої вчасно. Саме це робить їх уразливими до атак. Ще одна загроза полягає в тому, що не всі виробники пристроїв будуть інформувати користувачів про справжній технологічний стек програмного забезпечення пристрою, це пов'язано з ринковими стимулами використовувати його.
- Атак MITM (атака «людина посередині»): хакери можуть перехоплювати мережевий трафік і отримувати облікові дані або конфіденційну інформацію, яку пристрої IoT передають через корпоративну мережу. Оскільки багато інтелектуальних пристроїв часто не зашифровані, зловмиснику легко використовувати отримані дані для отримання несанкціонованого доступу до системи.
- Фізичне втручання: простого вставлення флешпам'яті USB зі зловмисним кодом у зовнішній пристрій Інтернету речей достатньо, щоб кіберзлочинці поширювали зловмисне програмне забезпечення в мережі та контролювали його зв'язок.
- Атаки «грубою силою» (брут-форс атаки): компанії часто не приділяють достатньої уваги безпеці паролів пристроїв Інтернету речей, що робить їх уразливими до потенційних атак грубої сили. Як правило, паролі пристроїв IoT залишаються незмінними після інсталяції з використанням лише головного пароля, що полегшує їх отримання для зловмисників.
- Викрадення прошивки: якщо оновлення мікропрограми пристрою не підписано криптографічно або якщо мікропрограма передається по незахищеному каналу зв'язку, це дозволяє зловмиснику перехопити її та завантажити шкідливе програмне забезпечення на пристрій під виглядом оновлення. Також за допомогою вкраденої прошивки кіберзлочинці мають можливість отримати облікові дані пристрою. Використовуючи облікові дані, вони можуть отримати доступ до корпоративних мереж або інших систем, які зберігають конфіденційну інформацію. Таким чином, атака на, здавалося б, нешкідливий пристрій може перетворитися на повномасштабного витоку даних.

З наведених вище векторів атак для IoT можна зробити висновок, що основні компоненти систем IoT дуже вразливі для зловмисників. Незалежно від розміру та типу середовища, у якому вбудована система IoT, на етапі проектування необхідно враховувати безпеку, щоб покращити її інтеграцію. Також варто дотримуватися наступних рекомендацій щодо запобігання кібератакам на IoT:

- Керування поверхнею атаки, інвентаризація та моніторинг усіх пристроїв;

Під час планування безпеки IoT одним із головних завдань має бути створення карти підключених пристроїв для їх інвентаризації. Команди безпеки повинні знати точну кількість використовуваних пристроїв, а також ідентифікатори виробників, серійні номери, версії обладнання та мікропрограми. Моніторинг, аналіз і звітність у режимі реального часу є критично важливими для організацій для управління ризиками Інтернету речей. Рішення для моніторингу поверхні атак без агентів забезпечують оцінку ризиків у реальному часі шляхом постійного аналізу поведінки та справності всіх підключених пристроїв IoT.

- Сегментація мережі;

У разі успішної кібератаки зловмисник отримує доступ до всієї мережі організації. Сегментація запобігає цьому, обмежуючи поверхню атаки та мінімізуючи пошкодження. Сегментація мережі — це процес поділу внутрішньої мережі на кілька незалежних підмереж. Хоча сегменти можуть час від часу спілкуватися один з одним, зазвичай вони незалежні та ізольовані один від одного. Такий підхід дозволяє зосередити більше уваги на окремих ділянках мережі, які містять найбільш критичні дані, підвищуючи їх захист.

- Встановлення надійних паролів для IoT;

Багато пристроїв IoT постачаються зі слабкими попередньо встановленими паролями, які можна легко вгадати. Коли IoT-пристрій вперше зареєструється у вашій мережі, найкраще змінити його пароль за замовчуванням на більш складний. Нові паролі мають бути складними для вгадування, унікальними для кожного захищеного пристрою та відповідати політиці керування паролями групи IT-безпеки.

- Фізичний захист всіх пристроїв IoT;

Фізичний захист пристроїв дуже важливий, оскільки зловмисники можуть фізично втручатися в зовнішні пристрої, щоб отримати несанкціонований доступ або завантажити шкідливе програмне забезпечення в систему. Тому необхідно забезпечити надійне місцеперебування пристрою, щоб запобігти його публічному доступу.

- Своєчасне оновлення прошивки;

Нові версії мікропрограми можуть виправляти наявні вразливості програмного забезпечення пристрою. Ось чому їх регулярні оновлення значно покращать загальну безпеку IoT. Однак вам також слід перевірити, чи оновлення не є підробленим, оскільки зловмисники можуть

використати вигляд оновлення для завантаження зловмисного програмного забезпечення на пристрій. Зворотною стороною оновлень є помилки в офіційних оновленнях. Необхідно контролювати контроль версій і підтримувати останню безпечну версію прошивки, в цьому допоможе система автоматичного аналізу прошивки пристрою [2].

Розуміння типів атак IoT і впровадження заходів безпеки допоможуть мінімізувати ризики використання IoT. Однак варто пам'ятати, що кібератаки постійно розвиваються та оновлюються, тому необхідно відстежувати події в кіберпросторі та регулярно оновлювати заходи безпеки, використовуючи сучасні передові рішення для забезпечення моніторингу пристроїв та аналізу поверхні атаки.

Перелік посилань:

4. Захист інтернет речей IOT – це те що потрібно захищати, як впровадження в інноваційний зміст навчання [Електронний ресурс] – Режим доступу: https://dut.edu.ua/ua/news-1-569-8709-zahist-internet-rechey-iot-%E2%80%93-ce-te-scho-potribno-zahischati-yak-vprovadzhennya-v-innovaciyniy-zmist-navchannya_kafedra-cistem-tehnichnogo-zahistu-informacii
5. Поширені атаки на IoT та захист від них [Електронний ресурс] – Режим доступу: https://corewin.ua/blog/attacks-on-iot-how-protect/
6. Як посилити захист Інтернету речей – базові кроки [Електронний ресурс] – Режим доступу: https://eset.ua/ua/blog/view/94/kak-usilit-zashchitu-internet-veshchey-bazovyye-shagi

Матвєєв Олександр Андрійович
студент групи БСД-41, ННІЗІ ДУТ, Київ, Україна

ПРОЦЕС РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Кібератаки стали звичним явищем у всьому світі, становлячи реальну і серйозну загрозу для організацій. Зросла не тільки кількість атак, а і їхня складність, масштабність та летальність. Велика кількість загроз створена, щоб бути непоміченими, водночас як компаніям часто доводиться стикатися з економічними наслідками втраченої інформації та довіри клієнтів.

Традиційні механізми захисту не можуть протистояти силі сучасних кіберзагроз. Багато організацій не мають достатнього рівня обізнаності та необхідну кількість ресурсів, щоб захистити себе від внутрішніх і зовнішніх кіберзагроз. Саме тому впровадження практики розслідування кіберінцидентів є необхідним кроком для забезпечення стабільності бізнесу компаній, збереження клієнтів та постійного розвитку.

Кіберінциденти це зафіксовані факти надзвичайних подій в кіберпросторі, які частіше за все спрямовані на дестабілізацію бізнесу компаній тощо.

Практика розслідування кіберінцидентів дозволяє розв'язати низку проблем та ліквідувати або звести до мінімуму наслідки, на які наражається компанія у разі кібератаки, а саме:

1. Ризик порушення цілісності даних, що може призвести до компрометації даних та втрати значних сум коштів на клієнтських рахунках;
2. Ризик репутаційних втрат, коли розголос інформації про можливий злам чи компрометацію інформаційної системи може призвести до зниження іміджу компанії на ринку;

3. Ризик відтоку клієнтів у разі втрати коштів та підвищення занепокоєності захищеністю систем;
4. Вплив на фінансові показники, коли порушення конфіденційності та цілісності даних може призводити до прямих та непрямих фінансових втрат компанії.

Практика розслідування кіберінцидентів містить декілька етапів, основними завданнями яких є:

1. Діагностуваня кіберінциденту;
2. Локалізація та мінімізування наслідків і втрат;
3. Виявлення основних причин;
4. Відновлення скомпрометованих інформаційних систем;
5. Впровадження заходів захисту для унеможливлення подібних інцидентів.

До основних етапів Практики розслідування кіберінцидентів належать:

1. Дослідження

Основне завдання під час дослідження кіберінциденту – підтвердити зазначений проспект події та визначити мережеву активність після події стосовно інфільтрації систем та ексфільтрації даних, а також визначити додаткові зламані комп'ютери та облікові записи користувачів.

2) Оцінка збитку

Оцінка збитку фокусується на з'ясуванні скомпрометованих файлів і даних. Спроба представити загальну картину скомпрометованих або ексфільтрованих даних в інциденті, щоб визначити загальний збиток і основні проблеми, які повинні бути розглянуті в майбутніх діях. Оцінка збитку може дати додаткові вказівки щодо впливу ексфільтрації даних на компанію загалом.

3) Відновлення

Визначити короткострокові потреби та дії для усунення кіберзагрози на основі показників інциденту та рівня захищеності інформаційних систем. А також визначити довгострокові проекти для подальшого зміцнення інформаційної безпеки компанії.

Практика розслідування кіберінцидентів спрямована на миттєве реагування та інформування компанії. Завдяки комплексному поєднанню людей, методології та технологій можна забезпечити швидку звітність, розуміння вже атакованих систем та даних, що перебувають під загрозою атаки. Чітке розуміння ключових ризиків та потреб компанії робить обізнаність працівників унікальним інструментом, а компанія отримає низку конкурентних переваг:

1.Скорочення ризиків втрати даних;
2.Скорочення витрат на відновлення даних;
3.Проактивного, а не реактивного реагування на інциденти;
4.Інтелектуальне розслідування
5.Управління в умовах кризових ситуацій.

Для успішного реагування на кіберінциденти компанії потрібні сертифіковані спеціалісти в галузі інформаційної безпеки (CISM) та кібербезпеки (CSX) як часткового напряму. Вони повинні володіти знаннями найкращих практик

(Cobit), стандартів інформаційної безпеки та практичним досвідом впровадження (ISO/IEC 27001, ISO/IEC 27002, NIST). Також ця команда повинна володіти низкою технік для збору та аналізу даних з багатьох операційних систем та IT-архітектур, поєднуючи широко прийняті інструменти і власне розроблене ПЗ; Команда повинна мати можливість ефективно збирати дані з безлічі середовищ, зокрема Windows, Mac OS X, Linux і мобільних платформ, таких, як Android та iOS. Також, працівники повинні використовувати загальноприйняті інструменти і методи для збору і вивчення даних з цих операційних систем. Ці інструменти містять як комерційні (EnCase, Forensic Toolkit (FTK), HB Gary, Paraben, Mandiant, Bit9, NetWitness, Internet Evidence Finder, Hardware Write Block/Disk Duplicator), так і безкоштовні рішення (SANS Investigative Forensic Toolkit (SIFT), SANS Network Investigative Forensic Toolkit (SNIFT), Sleuthkit, Log2timeline, Autopsy, Registry Ripper, Sysinternals, Network Miner).

Перелік посилань:

1. У 2022 році в Україні зареєстрували 2194 кіберінциденти — Держспецзв'язку [Електронний ресурс] – Режим доступу: https://suspilne.media/397220-u-2022-roci-v-ukraini-zareestruvali-2194-kiberincidenti-derzspeczvazku/
2. Реагування на інциденти [Електронний ресурс] – Режим доступу: https://www2.deloitte.com/ua/uk/pages/risk/solutions/incident-response.html

Мельников Антон Анатолійович
студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

СПЕЦИФІКА КІБЕРКУЛЬТУРИ ЯК ТЕОРЕТИЧНОГО КОНЦЕПТУ

Актуальність. Кіберкультура є складним та багатогранним явищем, що виникає в зв'язку з використанням інформаційних технологій та мережі Інтернет. Це поняття виникло на початку 1990-х років, коли Інтернет став доступним для широкої публіки. Кіберкультура охоплює різноманітні аспекти, включаючи кіберспорт, соціальні мережі, віртуальну реальність, інтернет-меми тощо. Емпіричним підґрунтям появи такого концепту є те, що людина не мислить свого існування без телебачення, кіно, соціальних мереж, мобільного та Інтернет зв'язку [1].

Постановка задачі. У вказаній роботі прагнемо розглянути історію розвитку кіберкультури та визначити основні її етапи та характеристики, визначити ключові поняття та теоретичні концепти, які використовуються для аналізу кіберкультури, проаналізувати вплив кіберкультури на сучасне суспільство, включаючи вплив на культуру споживання, комунікації та взаємодії між людьми.

Метою є визначення основних характеристик та ключових понять, пов'язаних з кіберкультурою, її соціальної, культурної та технологічної природи, а також впливу кіберкультури на сучасне суспільство.

Основні положення. Основоположником розуміння «кіберкультура» є

дослідник, який стояв біля витоків дослідження цієї теорії – Мануель Кастельс зазначає, що культура Інтернету це «культура творців Інтернету» [2, с. 52].

Специфіка кіберкультури полягає в тому, що вона є теоретичним концептом, який поєднує в собі елементи культури та технології. Це означає, що кіберкультура не може бути розглянута окремо від технологій, які використовуються для її створення та поширення. Водночас, кіберкультура має свої власні культурні особливості, які роблять її відмінною від інших культурних явищ.

І.В. Девтеров визначає дане явище у декількох значеннях. Дослідник вказує, що з одного боку, люди вживали (і досі вживають) префікс «кібер» у визначеннях дій або соціальних проектів, що здійснювалися за допомогою Інтернет, як наприклад «кіберактивність», «кіберкафе» «кібермистецтво» тощо. Складається враження, що термін «кіберкультура» виник як нове поняття для об’єднання всього вищезгаданого. З іншого боку, він використовувався деякими вченими як поняття для розуміння впливу Інтернет на суспільство. Згодом, «кіберкультура» постає як нова міждисциплінарна область дослідження, що визначається культурним аналізом комунікативних та інформаційних технологій [3, с. 220].

Кіберкультура – це теоретичний концепт, який визначається як сукупність культурних явищ та процесів, що виникають в результаті використання інформаційних технологій та мережі Інтернет. Специфіка кіберкультури полягає у тому, що вона є відкритою, глобальною та безмежною, здатною забезпечувати комунікацію та взаємодію людей з усього світу.

Кіберкультура змінює спосіб, яким ми сприймаємо світ та взаємодіємо між собою. Вона дозволяє нам створювати та споживати контент, спілкуватися та взаємодіяти з іншими людьми, без необхідності фізичного знаходження в одному місці. Дане явище змінює наші цінності та інтереси, створює нові форми самовираження та співпраці.

Аналізуючи кіберкультуру як сучасний феномен, сучасні дослідники пропонують осмислювати Інтернет саме крізь призму розвитку культури: кіберкультура як нова культурна модель, основана на інтернет-технологіях; кіберкультура як спонтанна інтернет-культура; кіберкультура як культурний продукт розвитку інтернету; кіберкультура як медіаформа [4, с. 73].

Специфіка кіберкультури також полягає у тому, що вона постійно змінюється та розвивається. Нові технології та інтернет-сервіси надають нові можливості для створення та взаємодії з кіберкультурою. Також виникають нові проблеми та виклики, пов'язані з кібербезпекою, цифровою приватністю, віртуальною реальністю та іншими аспектами.

Отже, специфіка кіберкультури полягає в її безмежності, глобальності, здатності змінюватися та розвиватися, а також в тому, що вона впливає на наш спосіб життя та взаємодії між людьми.

Специфіка кіберкультури також полягає у тому, що вона може бути розглянута як самостійний культурний феномен, який відрізняється від традиційних культурних форм. Кіберкультура включає в себе елементи

інформаційних технологій, які використовуються для створення, споживання та обміну культурними продуктами.

Крім того, кіберкультура має свої власні цінності та норми поведінки, які відрізняються від традиційних культурних форм. Наприклад, в кіберкультурі існує тенденція до анонімності та свободи виразу, а також до підтримки та співпраці між спільнотами. Також, полягає в її відкритості та доступності. Кіберкультура не має меж та кордонів, що дозволяє людям з усього світу взаємодіяти та співпрацювати. З розвитком технологій кіберкультура стає все більш доступною та зрозумілою для людей, навіть для тих, хто не має технічної освіти або досвіду використання Інтернету.

Специфіка кіберкультури також пов'язана з тим, що вона створює нові форми культурного взаємодії та самовираження. Завдяки кіберкультурі з'являються нові способи викладання та вивчення матеріалу, нові форми творчості та мистецтва. Крім того, кіберкультура дозволяє людям з різних країн та культур спілкуватися та взаємодіяти, сприяє розвитку міжкультурного діалогу та розуміння.

Однак, кіберкультура також має свої недоліки та виклики. Зокрема, це пов'язано з проблемами кібербулінгу, онлайн-злочинів, дезінформації, залежності від інтернету та інших проблемами. Тому, дослідження та аналіз кіберкультури є важливим завданням, що дозволяє розуміти як позитивні, так і негативні наслідки її впливу.

Додамо, що специфіка кіберкультури полягає у її мультикультурності та різноманітності. Завдяки мережі Інтернет та інформаційним технологіям, люди з різних країн та культур можуть легко спілкуватися та обмінюватися ідеями та знаннями. Кіберкультура створює умови для розвитку культурної плюралістичності та культурного діалогу, що сприяє збагаченню культурного досвіду та взаєморозумінню між різними національностями та культурами.

Ще однією важливою специфікою кіберкультури є її взаємозв'язок з технологіями. Кіберкультура формується та розвивається завдяки використанню різних інформаційних технологій, таких як програмне забезпечення, комп'ютерна техніка, мережі Інтернет тощо. Кіберкультура стає важливою складовою сучасного інформаційного суспільства, яке все більше стає залежним від технологій.

У кіберкультурі також існує поняття віртуальності та цифрової реальності. Вона дає можливість створювати віртуальні світи, де люди можуть взаємодіяти між собою, створювати та споживати контент, ігри, мультимедійні продукти тощо. Віртуальна реальність є важливим елементом кіберкультури, що дозволяє змінювати сприйняття світу та розвивати нові форми самовираження.

Висновок. Отже, специфіка кіберкультури полягає в безмежності, глобальності, здатності змінюватися та розвиватися, мультикультурності та взаємозв'язку з технологіями, а також у віртуальності та цифровій реальності. Кіберкультура є важливим явищем для сучасного суспільства, оскільки вона не тільки формує культурні практики та традиції, але й впливає на розвиток науково-технічного прогресу, змінює соціальні та економічні відносини, впливає

на політичні та геополітичні процеси.

Перелік використаних джерел:

1. Кастельс М., Хіманен П. Інтернет-галактика. Міркування щодо Інтернету, бізнесу і суспільства. К.: Ера, 2007. 304 с.
2. Девтеров І.В. Роль та місце кіберкультури в інформаційному суспільстві. Науковий вісник кафедри ЮНЕСКО Київського національного лінгвістичного університету. 2010. Вип. 21. С. 218-223.
3. Дзьобань О.П. Формування інформаційної картини світу як результат відображення генезису базових форм буття / О.П. Дзьобань // Проблема інформаційного суспільства: соціально-правовий аналіз : наук. ст. та тези наук. повідом. за матеріалами «Круглого столу», 28 лют. 2013 р. – Полтава : ТОВ «Фірма “Техсервіс”», 2013. – С. 26–36.
4. Власенко Ф.П., Левченюк Є.В., Товмаш Д.А. ПОСТКУЛЬТУРА В КОНТЕКСТІ ТРАНСГУМАНІЗМУ. Вісник Національної академії керівних кадрів культури і мистецтв. № 2 (2019). URL: https://doi.org/10.32461/2226-3209.2.2019.177399.

Негода Вадим Андрійович
студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

НАЙКРАЩІ ПРАКТИКИ І МЕТОДИ ЗАХИСТУ МОБІЛЬНИХ ПРИСТРОЇВ У КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ ЗА ДОПОМОГОЮ MOBILEIRON

Мобільні пристрої стали необхідністю у сучасному корпоративному середовищі, де працівники використовують смартфони та планшети, щоб залишатися на зв’язку та бути продуктивними. Хоча ці пристрої можуть поліпшити ефективність та продуктивність, вони також становлять значний ризик для безпеки, викладаючи корпоративні дані на ризик від зловмисних програм, витоку даних та несанкціонованого доступу. Для зменшення цих ризиків організації повинні використовувати ефективні засоби управління мобільними пристроями, такі як MobileIron, для захисту своїх мобільних пристроїв та захисту конфіденційної інформації.

MobileIron — це провідне рішення для управління мобільністю підприємства (EMM – enterprise mobility management), яке допомагає організаціям безпечно керувати своїми мобільними пристроями та програмами. За допомогою MobileIron організації можуть застосовувати політики, шифрувати дані та контролювати активність пристрою, щоб запобігти порушенням безпеки та захистити корпоративні дані. Деякі з ключових функцій і можливостей MobileIron включають[1]:

- Управління мобільними пристроями (MDM): MobileIron забезпечує IT-командам повну видимість і контроль над мобільними пристроями, включаючи налаштування параметрів пристрою, моніторинг активності пристрою та віддалене видалення даних у разі втрати або викрадення пристроїв.
- Управління мобільними додатками (MAM): MobileIron дозволяє організаціям керувати та захищати мобільні додатки, зокрема надсилати запити на оновлення додатків, блокувати невідомі додатки та вмикати систему єдиного входу (SSO) для корпоративних додатків.
- Управління мобільним вмістом (MCM): MobileIron забезпечує безпечний доступ до корпоративних даних, дозволяючи користувачам безпечно

отримувати доступ, редагувати та ділитися корпоративним вмістом без ризику витоку даних.

- Захист від загроз: MobileIron використовує машинне навчання для виявлення та запобігання зловмисному програмному забезпеченню та іншим кіберзагрозам, гарантуючи безпеку корпоративних даних.
- Керування ідентифікаційним доступом (IAM): MobileIron дозволяє організаціям керувати ідентифікаційними даними користувачів і контролем доступу, гарантуючи, що лише авторизовані користувачі мають доступ до конфіденційних корпоративних даних.

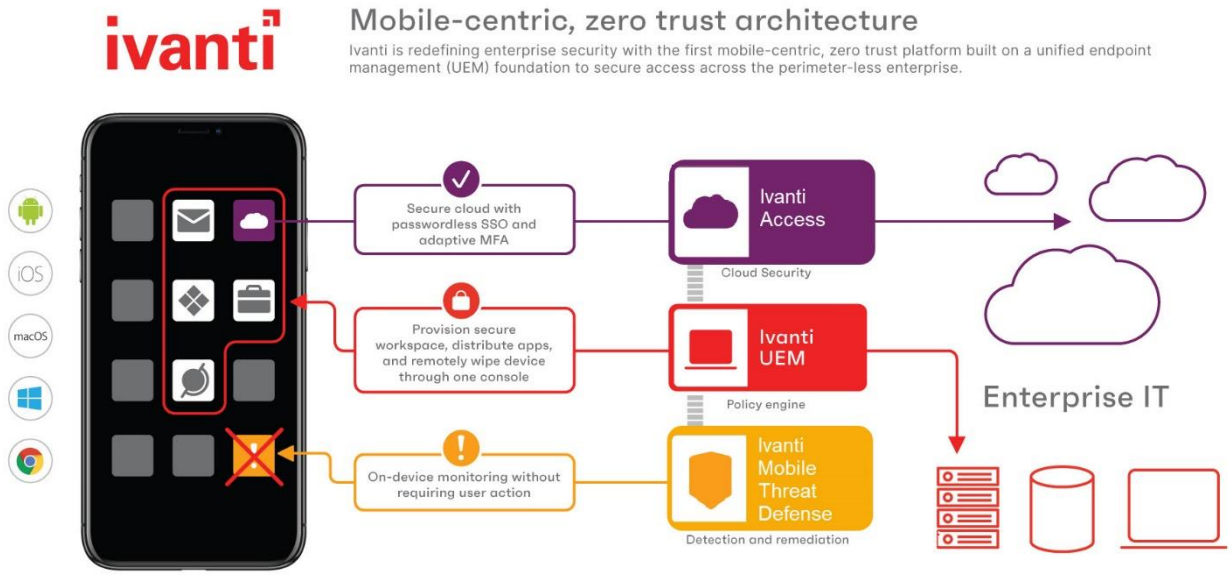


Рис.1 – Схема захисту конфіденційних даних за допомогою MobileIron

Однією з найважливіших переваг використання MobileIron є те, що він надає організаціям наскрізну безпеку для їхніх мобільних пристроїв, гарантуючи, що вони захищені від уразливостей, таких як зловмисне програмне забезпечення, витік даних або несанкціонований доступ. Наприклад, можливості захисту від загроз MobileIron використовують машинне навчання для виявлення та запобігання зловмисному програмному забезпеченню, гарантуючи безпеку корпоративних даних. Подібним чином можливості MobileIron MAM дозволяють IT-командам блокувати невідомі програми, запобігаючи завантаженню зловмисних програм, які можуть поставити під загрозу безпеку пристрою.

Щоб використовувати MobileIron ефективно та результативно, компанії повинні дотримуватися передових практик, таких як:

1. Запровадження комплексної політики щодо мобільних пристроїв: чітка та лаконічна політика щодо мобільних пристроїв може допомогти організаціям створити протоколи безпеки та переконатися, що працівники розуміють свої обов’язки під час використання мобільних пристроїв.

2. Проведення регулярних перевірок безпеки. Регулярні перевірки безпеки можуть допомогти організаціям виявити вразливі місця та області, які потрібно вдосконалити, дозволяючи їм вживати активних заходів для захисту своїх мобільних пристроїв і даних.
3. Увімкнення багатофакторної автентифікації (MFA): увімкнення MFA може допомогти організаціям запобігти несанкціонованому доступу до корпоративних даних, забезпечивши доступ до конфіденційної інформації лише авторизованим користувачам.
4. Проведення регулярних тренінгів із безпеки: регулярне навчання з питань безпеки може допомогти співробітникам зрозуміти важливість безпеки мобільних пристроїв і навчитися ефективно використовувати MobileIron для захисту своїх пристроїв і даних.

Підсумовуючи, MobileIron є важливим інструментом для захисту мобільних пристроїв у корпоративній інформаційній системі. Його можливості, такі як керування мобільними пристроями, керування мобільними додатками, керування мобільним контентом, захист від загроз та керування доступом до конфіденційних даних, роблять його комплексним рішенням для безпечного керування мобільними пристроями та додатками. Дотримуючись найкращих практик і рекомендацій, організації можуть використовувати MobileIron ефективно для захисту своїх мобільних пристроїв і конфіденційної інформації.

Перелік посилань:
1. Getting Started with Ivanti EPMM. URL: https://help.ivanti.com/mi/help/en_us/core/11.x/gsg/CoreGettingStarted/Core_overview.htm

Оладько Ярослав Олександрович
студент групи БСДМ-52, ІКБ ДУТ, Київ, Україна

ТЕХНОЛОГІЇ ЗАХИСТУ ВІД НЕСАНКЦІЙОВАНОГО ВИТОКУ ІНФОРМАЦІЇ З ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

Технології захисту від несанкційованого витоку інформації є важливим елементом безпеки будь-якої організації. У світі, де кіберзлочинці стають все поширенішими, необхідно дбати про захист конфіденційної інформації та персональних даних клієнтів. У цьому тексті я розгляну різноманітні технології, які допомагають організаціям захиститися від несанкційованого витоку інформації з їх інформаційних систем.

Першою технологією, яку слід розглянути, є шифрування. Шифрування є процесом перетворення звичайного тексту в кодовий таким чином, що його можна розшифрувати тільки з використанням відповідного ключа. Шифрування допомагає захистити дані від несанкційованого доступу, оскільки лише особа, яка має правильний ключ, зможе прочитати інформацію. Доповнивши шифрування реалізацією мультифакторної автентифікації дає високу ступінь захисту інформації. Можна використовувати різноманітні програмні рішення,

такі як Authy, Duo, Google Authenticator, LastPass і багато інших. Ці програми забезпечують генерацію додаткового пін-коду для кожної автентифікації або відправку SMS повідомлення з кодом на телефон користувача. Крім того, деякі сервіси та платформи, такі як Microsoft Azure та Amazon Web Services, мають вбудовану підтримку мультифакторної автентифікації. Це дозволяє забезпечити захист доступу до важливих ресурсів та даних в облікових записах, що зменшує ризик несанкційованого витоку інформації.

Другою технологією є використання системи контролю доступу на основі ролей (Role-Based Access Control, RBAC). Ця технологія полягає в тому, що користувачам надається доступ до інформації на основі їхніх ролей в організації. Наприклад, адміністратор системи має повний доступ до всієї інформації, тоді як звичайні користувачі можуть мати доступ лише до тієї інформації, яка необхідна для виконання їхніх робочих обов'язків. Для реалізації системи контролю доступу на основі ролей можна використовувати спеціальні програмні продукти, такі як IBM Security Access Manager, Oracle Identity Manager, Microsoft Identity Manager, CyberArk Privileged Access Security і багато інших. Ці програми дозволяють встановлювати права доступу до різних ресурсів та інформації на основі ролей користувачів. Крім того, для забезпечення безпеки можна використовувати технології аудиту доступу до інформації, які дозволяють відстежувати, хто, коли і яку інформацію переглядав або змінював. Це дозволяє вчасно виявляти та реагувати на можливі загрози безпеці інформації, зменшуючи ризик несанкційованого витоку. У разі виявлення порушення безпеки можна використовувати інші рішення, такі як системи захисту від DDoS-атак, системи виявлення та запобігання інцидентам безпеки, системи моніторингу та інші. Застосування цих технологій забезпечує комплексний підхід до захисту інформації та зменшує ризик несанкційованого доступу до неї.

Третьою технологією захисту від несанкційованого витоку інформації є використання антивірусного програмного забезпечення. Антивірусне програмне забезпечення дозволяє організаціям захистити свої інформаційні системи від різноманітних загроз, таких як віруси, троянські програми, черви та інші шкідливі програми. Зважаючи на те, що безпека інформації є ключовою проблемою для будь-якої організації, використання комплексних рішень забезпечення безпеки може стати оптимальним рішенням. Eset Safetica One є одним з таких комплексних рішень, яке забезпечує захист від несанкційованого витоку інформації з інформаційної системи організації. Eset Safetica One - це комплексна система захисту, яка включає в себе різноманітні функції для забезпечення безпеки інформації. Програмний продукт має інтелектуальну систему виявлення загроз, яка забезпечує ефективний захист від вірусів, шпигунського програмного забезпечення, хакерських атак та інших загроз, які можуть призвести до несанкційованого витоку інформації. Eset Safetica One забезпечує комплексний захист інформації з використанням різноманітних технологій, таких як антивірусний захист, захист від шкідливих сайтів, функція контролю за документами та ін. Продукт також забезпечує контроль за використанням USB-накопичувачів, підключенням до мережі та іншими

функціями, які можуть бути потенційними загрозами для безпеки інформації. Одним із ключових елементів Eset Safetica One є його можливості забезпечення контролю за документами. За допомогою цієї функції ви можете стежити за всіма документами, що створюються та зберігаються в інформаційній системі організації. Ви можете контролювати доступ до документів, а також встановлювати обмеження на їх копіювання та відправлення.

Четвертою технологією, яку можна використовувати для захисту від несанкційованого витоку інформації, є виявлення та відновлення даних. Ця технологія дозволяє організації виявляти витоки інформації та відновлювати втрачені дані. Для цього можуть використовуватися спеціальні програми, які зберігають копії даних на зовнішніх носіях або в хмарних сховищах. Якщо відбувається витік даних, організація може використовувати ці копії для відновлення втраченої інформації та запобігання наслідкам витоку. Загалом, технології захисту від несанкційованого витоку інформації є важливим елементом безпеки будь-якої організації.

Крім технологій захисту, важливо також забезпечувати свідомість та кваліфікацію співробітників організації щодо захисту інформації та відповідальності за її збереження. Зокрема, необхідно проводити навчання з питань кібербезпеки, встановлювати політики та процедури з контролю доступу до інформації, розробляти та використовувати сильні паролі та шифрування, регулярно оновлювати програмне забезпечення та антивірусні бази даних, проводити аудит безпеки інформації та інші заходи, які можуть допомогти забезпечити найвищий рівень захисту інформації.

Отже, використання технологій захисту від несанкційованого витоку інформації є необхідним для забезпечення безпеки та надійності інформаційної системи організації. Варто звернути увагу на існуючі технології та методи захисту, забезпечити їх постійне оновлення та вдосконалення, а також забезпечити належний рівень свідомості та кваліфікації співробітників організації щодо захисту інформації. Ці заходи допоможуть забезпечити ефективний захист від несанкційованого витоку інформації та запобігти негативним наслідкам, які можуть виникнути внаслідок таких витоків.

Перелік посилань:

1. Sterling, B. (2012). The Complete Cybersecurity Guide for Small Businesses. PCWorld. [Електронний ресурс] – Режим доступу: https://www.pcworld.com/article/2022380/the-complete-cybersecurity-guide-for-small-businesses.html
2. What is Malware? (2022). Malwarebytes. [Електронний ресурс] – Режим доступу: https://www.malwarebytes.com/malware/
3. Schwartz, M. J. (2016). Ransomware: How to defend against it. InformationWeek. [Електронний ресурс] – Режим доступу: https://www.darkreading.com/risk/ransomware-how-to-defend-against-it-/a/d-id/1325613
4. 12 Types of Cyber Crime. (2022). NortonLifeLock. [Електронний ресурс] – Режим доступу: https://us.norton.com/internetsecurity-emerging-threats-12-types-of-cybercrime.html
5. Gupta, R. K. (2017). Understanding network security concepts and policies. CRC Press.
6. Al-Ali, A. R., & Yusoff, Y. M. (2017). Cybersecurity Framework for Cloud Computing: A Review. Journal of Information Security, 8(1), 32-44.

7. Gajawada, N., & Chaturvedi, V. (2017). Analysis of network security attacks and mitigation techniques: A review. International Journal of Computer Applications, 168(1), 8-12.
8. Yaraghi, N., & Du, A. Y. (2016). The impact of information security breaches on financial performance of firms: An empirical investigation. Journal of Management Information Systems,.
9. Canavan, J. E., Pollack, M. E., & Winkler, V. J. (2018). Principled cybersecurity: Realigning your cyber efforts with your mission. Routledge.
10. Andress, J., & Winterfeld, S. (2014). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Syngress.

Павленко Марина Юріївна
студентка групи ІСД-42, ННІІТ ДУТ, Київ. Україна

ХМАРНІ ТЕХНОЛІГІЇ: БІЗНЕС-ІНСТРУМЕНТ ЧИ РИЗИК ДЛЯ БЕЗПЕКИ ДАНИХ?

З поширенням хмарних обчислень та зберігання даних в хмарі, безпека стала однією з найбільш важливих проблем, які ми повинні вирішувати. Хмарні технології є необхідними для сучасного бізнесу, оскільки вони надають безкоштовні і доступні інструменти для зберігання і обробки даних, зокрема, даних клієнтів і підприємств. Однак, зростання популярності хмарних технологій також призводить до зростання ризику зламу безпеки.

Виклики конфіденційності та безпеки в хмарних обчисленнях.

Оскільки все більше організацій переходять на хмару як ефективний засіб зберігання даних, їм потрібно ділитися, швидко обробляти та поширювати великий обсяг конфіденційної інформації для покращення ефективного прийняття рішень [1]. Однак значним недоліком є відсутність безпеки та гнучкості конфіденційності. Поточний механізм безпеки та конфіденційності не має достатньої гнучкості для реагування на зміну зовнішнього середовища, що призвело до неконтрольованого ризику витоку даних. Організації стурбовані стабілізацією хмарних інфраструктур безпеки без зменшення витоку даних та інформації користувачів. На жаль, служби зберігання даних постійно змінюються, і сьогодні конфіденційність може бути визначена індивідуально — те, що може бути конфіденційним для особи, може бути розголошене деякими без занепокоєння. Таким чином, існує потреба в описі неспецифічних вимог при створенні протоколів конфіденційності та безпеки для хмарних обчислень. Суворі протоколи конфіденційності чи безпеки залишаться на місці лише в довгостроковій перспективі, оскільки технології та їхні ресурси переходять у відкритий світ, де кожен може вирішувати, що він вибере для приватного, особливо в хмарному середовищі.

Різноманітність додатків хмарних обчислень привернула увагу до безпеки, коли йдеться про зберігання, керування та обробку даних. Хмарні обчислення створюють відкриті питання щодо безпеки та конфіденційності даних, переданих стороннім виконавцям. Завдяки своїй динамічній абстракції та масштабованості програми та дані, передані в хмару, мають необмежені межі безпеки та інфраструктуру. Ще однією основною проблемою безпеки, пов’язаною з впровадженням хмарних обчислень, є їх багатокористувацький характер і

спільне використання віртуалізованих ресурсів. Хмарні провайдери, такі як Google, Microsoft і Amazon, нещодавно прискорили свою інфраструктуру та послуги хмарних обчислень для підтримки значної кількості користувачів [2]. Тим не менш, проблема конфіденційності та безпеки продовжуватиме зростати, оскільки хмарні бази даних зазвичай містять важливу конфіденційну інформацію.

Однією з найбільш поширених загроз є злам хмарного сервера, який містить конфіденційну інформацію. Це може призвести до витоку даних та порушення прав на приватність. Також можливо атакувати самі хмарні сервіси, що призведе до втрати доступу до важливої інформації.

Одним з ключових рішень для запобігання цих загроз є шифрування даних. Шифрування дозволяє зберігати дані в зашифрованому вигляді, тому зламати сервер та отримати доступ до конфіденційної інформації буде неможливо без знання ключа розшифрування. Крім того, можна використовувати багаторівневі заходи захисту, щоб знизити ризик витоку даних.

Однак шифрування не є панацеєю інколи, навіть зашифровані дані можуть бути скомпрометовані. Тому, регулярні аудити безпеки хмарних серверів є необхідністю. Такі аудити дозволяють виявляти можливі проблеми та вразливості, щоб їх можна було вчасно виправити та запобігти можливим атакам.

У кінці кінців, безпека хмарних технологій має бути поставлена на однаковий рівень з розробкою та використанням цих технологій.

Перелік посилань:

1. Sun, X.; Liu, P.; Singhal, A. Toward Cyberresiliency in the Context of Cloud Computing . IEEE Secur. Priv. 2018, 16, 71–75.
2. Визначення безпеки в хмарі [Електронний ресурс] Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cloud-security
3. Security and Privacy in Cloud Computing [Електронний ресурс] Режим доступу: https://encyclopedia.pub/entry/17992

Парфенюк Тетяна Миколаївна
студентка групи БСД-41, ННІЗІ ДУТ, Київ, Україна

КОНТРОЛЬ ПРІВЕЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ ЗА ДОПОМОГОЮ РІШЕНЬ PAM

Управління доступом привілейованих користувачів (Privileged Access Management або PAM) є важливим завданням для забезпечення інформаційної безпеки підприємств. Для великих організацій це питання може бути серйозним викликом. Адже на відміну від невеликих компаній, у великих організаціях велика кількість співробітників з високим рівнем доступу і в ручному режимі керувати їх обліковими записами досить проблематично. Саме для вирішення цієї проблеми існують платформи Privileged Access Management.

Визначення привілейованих користувачів

Привілейованими користувачами є ті, хто має доступ до критичних систем із правами адміністратора.[1] Наприклад, людину, яка має можливість створювати нові облікові записи в корпоративній мережі, можна назвати привілейованим

користувачем. Те саме стосується і співробітників, які можуть змінювати налаштування систем, встановлювати та видаляти ПЗ, мати доступ до конфіденційних даних тощо. Такий високий рівень доступу до корпоративної IT-системи відкриває можливості для зловживань і навіть саботажу. І не варто забувати — що більше організація, то більше в ній привілейованих акаунтів. Ось чому за такими обліковими записами також потрібний контроль, який забезпечують PAM-системи.

Функціональність рішень PAM

Звернімо увагу, що багато присутніх на ринку вендорів таких платформ представляють комплексні рішення, що складаються з безлічі окремих інструментів.

Якщо говорити глобально, то інструментарій PAM-платформ можна поділити на три категорії. Перша - це керування доступом. Через продукти цієї категорії визначаються політики доступу користувачів до тих чи інших систем та регулюються їхні можливості. За допомогою засобів управління доступом можна створювати, редагувати та видаляти права доступу конкретних облікових записів або їх груп до сегментів корпоративної IT-інфраструктури.[2]

Друга – управління сесіями. Інструменти цієї категорії дозволяють відстежувати дії користувачів у системах, куди вони мають доступ. Це також допомагає при проведенні розслідувань інцидентів, адже вони чітко показують, хто та які дії вчинив у певний час у конкретній системі.

Третя — керування паролями та процедурами входу в систему. Сюди відноситься їх зберігання, скидання та відновлення. Просунуті системи можуть надавати доступ привілейованим обліковим записам, не повідомляючи користувачам пароль. Це запобігає витоку паролів та несанкціонованого доступу третіх осіб. Крім того, PAM-рішення підтримують засоби мультифакторної аутентифікації.[2]

Вибір інструментів PAM повністю залежить від потреб компанії, а саме масштабу інфраструктури та наявних засобів контролю. На ринку є чимало пропозицій, перелік яких наведено у рейтинговій таблиці Gartner за 2022 рік.[3]

Рис.1 – Gartner Magic Quadrant для рішень PAM

Перелік посилань:

1. Priveleged Access Management Solutions Reviews and Ratings [Електронний ресурс] – Режим доступу: https://www.gartner.com/reviews/market/privileged-access-management
2. Огляд рішень з управління привілейованим доступом (Privileged Access Management) [Електронний ресурс] – Режим доступу: http://blog.roi4cio.com/2021/06/privileged-access-management.html
3. ManageEngine positioned in the Gartner® Magic Quadrant™ for Privileged Access Management [Електронний ресурс] – Режим доступу: https://www.manageengine.com/privileged-access-management/analyst-opinion/gartner-magic-quadrant-pam-2022.html

Приблудюк Юрій Олександрович
студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

ОСНОВНІ РИЗИКИ ВПЛИВУ DDOS-АТАК НА БЕЗПЕКУ КОМП'ЮТЕРНИХ МЕРЕЖ

Дослідження особливостей реалізації DDoS атак є важливим напрямом вивчення кібербезпеки, оскільки дозволяє зрозуміти методи та засоби, які використовуються для здійснення таких атак, що забезпечує можливість розробки ефективних засобів захисту від них. DDoS-атаки є найскладнішими для захисту, і, на жаль, не існує стандартних механізмів захисту, які організації можуть використовувати для захисту від DDoS-атак. Багато в чому це пов'язано з тим, що DDoS-атаки намагаються імітувати звичайний трафік, але їхня кількість збільшується в геометричній прогресії.

Мотиви та специфіка DDOS-атак

Частота кібератак різко зросла останніми роками, оскільки кількість осіб та організацій, які вирішили розпочати такі атаки на своїх конкурентів або

ворогів, також збільшилася, так само як і використання потенційно вразливих комп'ютерів та комп'ютерних мереж. У той час як велика кількість атак мають фінансову мотивацію, від заподіяння шкоди бізнес-конкуренту до кримінального мотиву, багато інших мають політичні мотиви або навіть просто для розваги.

Зловмисники часто проводять DDoS-атаки, у яких для підвищення ефективності використовується кілька машин. У цьому сценарії часто буває складніше виявити та заблокувати зловмисників вручну, тому потрібні спеціальні засоби захисту для виявлення та захисту від таких великомасштабних атак. Крім того, зловмисники майже ніколи не контролюють атакуючі машини на законних підставах; швидше, вони заражають спеціалізованими шкідливими програмами тисячі комп'ютерів по всьому світу, щоб отримати несанкціонований доступ до таких машин. Сукупність сотень або тисяч скомпрометованих машин, що діють як армія під контролем одного зловмисника, називається «ботнетом» (рис.1),, і часто фактичні власники машин, що є частиною ботнета, не підозрюють, що їхні комп'ютери були атаковані та використовуються для запуску DDoS-атак [1]. За винятком створення ботнета, запуск DDoS-атаки не є складним завданням навіть для нетехнічного спеціаліста. Користувачам не потрібно створювати власні ботнети для запуску великомасштабних атак, оскільки кожен може користуватися різними платними DDoS-сервісами. Будь-хто, хто використовує такий сервіс, може запустити потужну DDoS-атаку на обрану ним мету за 5-200 доларів на годину, залежно від розміру та тривалості атаки. Коли зловмисник готовий, йому потрібно виявити вразливі сайти чи хости, а можливо, і всю мережу.

Щоб зловмисники могли створювати великі ботнети з комп'ютерів, що знаходяться під їх контролем, у них є два варіанти: більш поширений варіант використання спеціалізованого шкідливого програмного забезпечення для зараження машин користувачів, які не знають, що їх машини скомпрометовані, або відносно новий варіант збору великої кількості добровольців, які бажають спільно використовувати програми DoS.

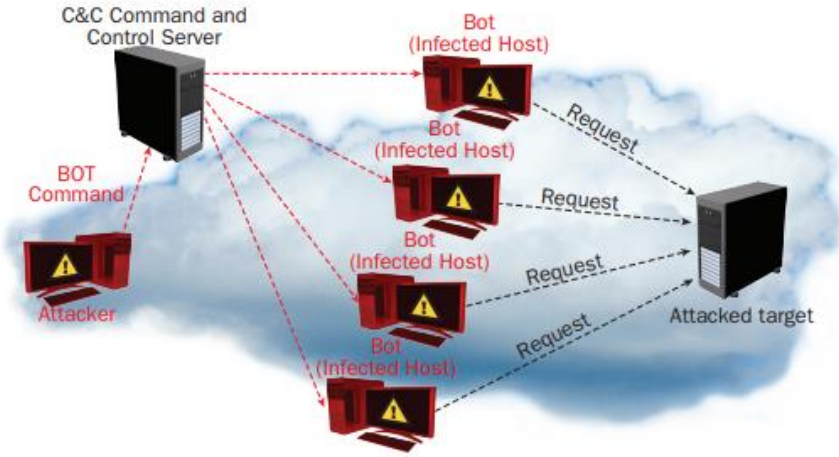


Рис. 1 – Реалізація «ботнету»

Атаки DDoS класифікуються за: ступенем автоматизації, використаною

вразливістю, перевіркою адреси джерела, можливістю характеристики, динамікою частоти атак, впливом на жертву, типом жертви та збереженням набору агентів.

Багато сучасних атак зазвичай використовують кілька векторів в рамках однієї кампанії атаки, націленої на кілька компонентів мережевої інфраструктури організації та її додатків. Атаки не призначені для крадіжки будь-якої інформації та не вплинуть на безпеку. Швидше, вони призначені для зниження продуктивності сайту або його відключення. Атаки намагатимуться споживати не тільки мережеві ресурси, але в деяких випадках також ресурси сервера (та інших сучасних пристроїв) або програми. Надзвичайно складно класифікувати різні типи DoS та DDoS-атак лише за одним параметром. Кожен тип атаки має різні характеристики, що може свідчити, що він належить до кількох категорій. Взагалі кажучи, типи атак включають ті, що орієнтовані на мережеві ресурси, ті, які орієнтовані на ресурси сервера, і ті, які орієнтовані на програмні ресурси [2].

Перелік посилань:

1. Introduction to Network Security [Електронний ресурс] – Режим доступу: https://handoutset.com/wp-content/uploads/2022/02/Introduction-to-Network-Security-by-Neal-Krawetz.pdf
2. What Is the Cyber Kill Chain and How It Can Protect Against Attacks [Електронний ресурс] – Режим доступу: https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can-protect-against-attacks

Скибун Олександр Жоржович
студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

КІБЕРБЕЗПЕКА КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Сучасний етап розвитку суспільства відзначається подальшим зростанням рівнів цифровізації, комп’ютеризації та віртуалізації усіх сфер суспільства (економічної, політичної, соціальної та гуманітарної) та суспільних відносин. Також разом із розвитком ІКТ, інформаційних та комунікативних процесів широко впроваджується у комерційне використання елементів штучного інтелекту, Інтернету речей, робототехніки та автоматизації процесів управління, технологічних процесів та процесів ведення бізнесу. Важливими елементами яких виступають електронні комунікації та інформаційно-комунікаційні системи. Крім того зростає кількість компаній, основою бізнес процесів яких є Інтернет, веб-ресурси та відкриті дані. Водночас разом із зростанням цифрової складової відбувається збільшення кіберзагроз та кіберінцидентів, що потребує швидкого та дієвого реагування.

На сьогодні стрімкий розвиток цифрової економіки разом із впровадженням широкого спектру програм та проєктів з інформатизації багатьох аспектів життєдіяльності суспільства, бізнесу та влади відбувається новими методами ведення бізнесу, управління та взаємовідносин на рівні суспільство-влада-бізнес. Перш за все це перехід на цифрові віртуальні інструменти комунікацій та ведення бізнесу, інтегровані у відповідні інформаційно-комунікаційні мережі, робота в яких та доступ інформації відбувається за допомогою відповідного технологічного комунікаційного обладнання та програмованих кінцевих пристроїв (комп’ютери, ноутбуки,

смартфони тощо). Вказане вимагає/потребує створення відповідних комп'ютерних мереж та інформаційно-комунікаційних систем. При цьому зростає часка компаній різних форм власності та державних установ, які працюють з відкритими даними через веб-ресурси, веб-сайти та електронною поштою. Так, «у сучасному світі досить складно уявити собі підприємство, яке успішно розвивається і керується без участі такої системи» [3, с.61]. Завдяки цьому зростає питання безпеки та захисту адже «в корпоративних інформаційних системах зберігається інформація, порушення цілісності або конфіденційності якої може привести до краху цілого підприємства гостро стоїть питання про захист інформації в корпоративних інформаційних системах» [3, с.61]. Так, разом із цифровим сектором економіки з'явилися цифрові правопорушення – кіберзлочини, кіберініциденти, рівень яких постійно зростає. Це пов'язано з тим, що «сучасні корпоративні інформаційні системи мають велику кількість вразливостей з боку зовнішніх і внутрішніх зловмисників, а реалізація їх атак не вимагає серйозної кваліфікації» а також «досить низьким є рівень захищеності бездротових мереж і рівень обізнаності користувачів в питаннях інформаційної безпеки» [3, с.64]. А тому «однією із важливих складових сучасної практики забезпечення корпоративної безпеки в державних та приватних структурах є кібербезпека», яка серед іншого «включає заходи із захисту інформації з обмеженим доступом та відкритої інформації від загроз її несанкціонованої модифікації, блокування та знищення; протидії розповсюдженню неповної, невчасної та неправдивої інформації у кіберпросторі» тощо [1, с.51].

Так, за даними компаній, які проводять аналіз інформаційної безпеки компаній «до найбільш поширених вразливостей захисту внутрішніх ресурсів належать: недоліки захисту протоколів мережевого і канального рівнів, … використання словникових паролів … та недостатній рівень захисту привілейованих облікових записів» [3, с.64]. В цілому перелік найбільш поширених уразливостей на мережевому периметрі представлено на рисунку 1.

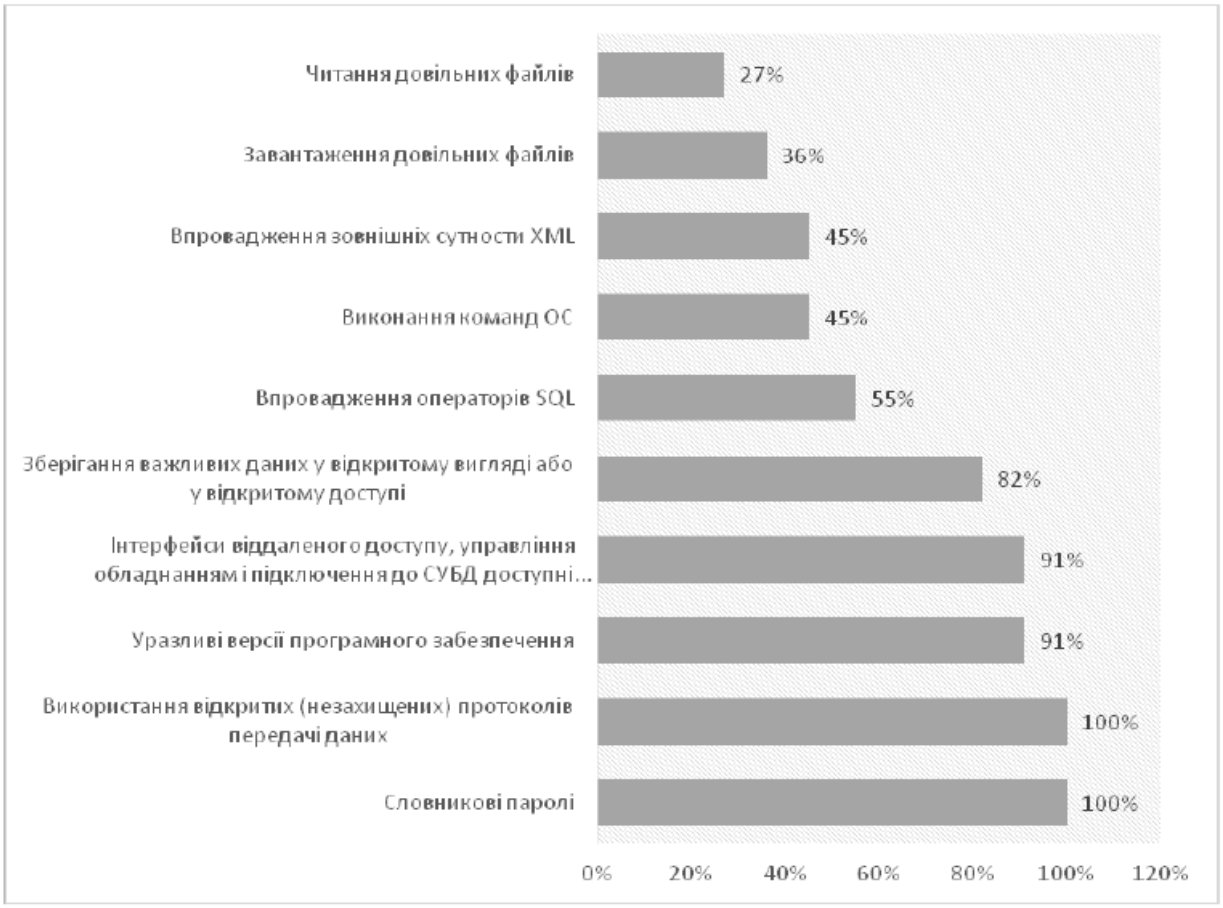


Рис. 1. Найбільш поширені уразливості на мережевому периметрі (частка систем) [3].

Для забезпечення рівня кібербезпеки в корпоративних інформаційних системах групою науковців запропоновано наступні «принципи забезпечення інформаційної безпеки», які необхідно застосовувати у комплексі, а саме: «використовувати сувору парольний політику; захищати привілейовані облікові записи; не зберігати конфіденційну інформацію у відкритому вигляді або у відкритому доступі; обмежити число доступних для підключення на мережевому периметрі інтерфейсів мережевих служб; захищати або відключати в локальної обчислювальної мережі протоколи канального або мережевого рівня, які не використовуються та розділяти мережу на сегменти; мінімізувати привілеї користувачів і служб; регулярно оновлювати ПО і встановлювати оновлення безпеки ОС; для своєчасного виявлення атак використовувати SIEM-системи; для захисту веб-додатків використовувати web application firewalls; проводити регулярні тренінги, спрямовані на підвищення обізнаності користувачів в питаннях інформаційної безпеки (при цьому важливо проводити і оцінку ефективності таких тренінгів); для захисту від поширення шкідливого програмного забезпечення із застосуванням соціальної інженерії використовувати спеціалізовані антивірусні рішення; регулярно проводити тестування на проникнення для своєчасного виявлення нових векторів атак і перевірки вжитих заходів захисту на практиці.» [3, с.64].

В той же час компанія «АМ Інтегратор» запропонувала наступний концепт кіберзахисту, що складається з таких складових: «**виявлення загроз (п**латформа **Fidelis Elevate** складається з трьох основних компонентів: Network module, Endpoint module та Deception module, – які відповідно забезпечують безпеку внутрішньої мережі, безпеку кінцевих точок (серверів та робочих станцій), та пошук загроз, які не були помічені рештою існуючих засобів забезпечення безпеки у корпоративній мережі**); контроль персоналу (р**озумна система контролю активності співробітників **Mirobase** – це програма, яка моніторить всі дії співробітників на комп'ютері та надає данні про ефективність загрузки персоналу, загрози та витоки інформації, використання ресурсів компанії**); кіберполігон** (**CyberBit Range** – платформа з двох навчальних класів, яка дозволяє моделювати атаки і тренувати навички персоналу в захисті від цих різноманітних атак).» [2].

Таким чином питання кіберзахисту набуває все більшого значення та актуальності з огляду на подальше збільшення можливостей корпоративних інформаційно-комунікаційних та інформаційних систем підприємств, установ, організацій та відомств усіх форм власності та розмірів (від малого бізнесу до транснаціональних корпорацій), у контексті збільшення переліку програмних продуктів, які використовуються та послуг, що надаються. При цьому необхідно зважати на комплексний підхід, а саме: використання та постійне оновлення відповідного програмного забезпечення; наявність окремої команди фахівців з кібербербезпеки та їх взаємодія із кіберсередовищем (вендорами програмного забезпечення); безперевна робота з персоналом в частині дотримання кібербезпеки та формування відповідної кіберетики серед працівників компанії; підвищення загального рівня кібергігієни.

Перелік посилань:

1. Довгань О.Д., Тарасюк А.В. Корпоративна культура кібербезпеки суб'єктів наукової та науково-технічної діяльності. Інформація і право № 2(25)/2018. С.51-61.
2. Кібербезпека як запорука корпоративної стабільності. [Електронний ресурс]. – Режим доступу: https://amintegrator.com/ua/kiberbezpeka-yak-zaporuka-korporativnoyi-stabilnosti/. (дата звернення – 09.04.2023).
3. Мехед Д, Ткач Ю, Базилевич, Гур'єв В, Усов Я Аналіз вразливостей корпоративних інформаційних систем. Захист інформації, ТОМ 20, №1, січень-березень 2018, С.61-66. [Електронний ресурс]. – Режим доступу: https://jrnl.nau.edu.ua/index.php/ZI/article/view/12453. (дата звернення – 08.04.2023).

Скрипка Олександр Володимирович
студент групи УБД-21, ННІЗІ ДУТ, Київ, Україна

ЗАХОДИ ЩОДО ПОБУДОВИ КІБЕРБЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Для багатьох команд розробників ідея вбудувати кібербезпеку в свій дизайн IoT може здатися страшною. Встановлення балансу між додаванням функціональності та мінімізацією витрат на впровадження кібербезпеки може швидко призвести до плутанини та розчарування без систематичного підходу до вирішення проблеми. В тезі розглянуто заходи щодо побудови кібербезпеки Інтернету речей, запропоновані урядом США для підтримки розробників з метою забезпечення зрозумілої основи щодо можливостей безпеки своїх пристроїв.

Ключові слова: IoT, Інтернет речей, кібербезпека.

У своєму документі NISTIR 8259 «Основна діяльність у сфері кібербезпеки для виробників пристроїв Інтернету речей» [1] Національний інститут стандартів і

технологій Міністерства торгівлі США (NIST) визначив шість основоположних заходів, які, на його думку, мають бути важливими для команд розробників, розглядаючи питання кібербезпеки в дизайні своїх пристроїв Інтернету речей. Ці базові заходи можна згрупувати в дві часові групи.

Перша група – це дії, які відбуваються ще до початку детальної розробки. Вони допоможуть командам розробників визначити, які функціональні можливості безпеки мають забезпечувати їхні проекти, і часто можуть розкрити вказівки щодо реалізації цієї функції.

Друга група заходів вступає в дію після появи готового продукту на ринок, хоча їх слід планувати до початку розробки. Ця пост-маркетингова діяльність стосується питання про те, як підтримати клієнтів, які придбали продукт і включили його у свої системи. Процеси кібератак постійно розвиваються, тому пристрої IoT також повинні мати можливість розвиватися. Більшість клієнтів очікують, що постачальник IoT систем зможе підтримувати постійних захист їхніх пристроїв. На рис. 1 [1, ст. 3] наведена відповідна схема.

Рис. 1 – Заходи щодо побудови кібербезпеки Інтернету речей

На етапі підготовки до виходу на ринок є чотири ключові види діяльності, призначені для доповнення або паралельності з іншими традиційними заходами команди розробників перед виходом на ринок, які допомагають визначити ринкову можливість, яку проект прагне реалізувати. Розглянемо кожен пункт:

1. Визначити потенційних користувачів та їх використання продукту

Ця діяльність має важливе значення для визначення того, які функції кібербезпеки будуть потрібні клієнтам, і часто може вказати, як ці функції потрібно буде впровадити. Запитання можуть включати, як і де буде використовуватися пристрій, як довго пристрій використовуватиметься, з якими іншими клієнтськими системами пристрій буде взаємодіяти, а також як зловмисники можуть скомпрометувати або зловживати пристроєм.

2. Дослідіть потреби та цілі клієнтів щодо кібербезпеки

Розробникам доведеться принаймні частково розуміти, як клієнту потрібно буде зменшити унікальні ризики кібербезпеки. Розуміння того, чим ризикує клієнт, і засобів, за допомогою яких клієнт контролюватиме свій ризик,

значною мірою допоможе визначити вимоги до функціональних можливостей кібербезпеки пристрою. Загрози включають в себе злам пристрою, спотворення його функціональних можливостей, інформацію, яку обробляє пристрій і в свою чергу вона потребує захисту від крадіжки чи маніпуляцій. Для деяких клієнтів і варіантів використання також може виникнути потреба в кібербезпеці, яка пов'язана з нормативними актами чи програмою. У таких випадках дизайн виграє від реалізації функцій, які спрощують і підтримують клієнта в задоволенні цих потреб. Таким чином, ця діяльність може включати вивчення відповідних нормативних стандартів для вказівок щодо вимог до функцій, а також опитування потенційних клієнтів, щоб зрозуміти їхні потреби та очікування.

3. Визначте, як задовольнити потреби та цілі клієнтів

Для кожної цілі кібербезпеки, визначеної в попередньому заході, команди розробників повинні поставити запитання: який засіб або комбінація засобів є придатним для досягнення цієї мети? Засоби можуть включати можливості, вбудовані в сам пристрій, надаватися іншим пристроєм користувача, наприклад концентратором або шлюзом, або надаватися третіми сторонами, наприклад хмарною службою. Нетехнічні засоби також потребують розгляду, наприклад, готовність клієнта прийняти ризик недосягнення мети. Команди також повинні розглянути, наскільки надійними повинні бути засоби.

4. Сплануйте адекватну підтримку потреб і цілей клієнтів

Розробники можуть зробити свої проекти більш придатними для досягнення цілей клієнтів, забезпечивши наявність механізмів і вибір дизайну, зроблений з урахуванням ідеї довгострокової підтримки пристрою. Наприклад, якщо встановлений пристрій має термін служби протягом десятиліть, може бути доцільно включити можливість оновлення алгоритмів шифрування або зміни ключів після встановлення. Інші запитання, які можна поставити, включають те, як клієнти можуть перевірити цілісність апаратного та програмного забезпечення, як забезпечити безпеку стороннього програмного забезпечення та як захистити код від втручання та несанкціонованого доступу.

На додаток до цих заходів, які можуть допомогти у виборі та впровадженні функцій кібербезпеки пристрою, є дві пост-ринкові дії, які слід планувати командам розробників.

5. Визначте підходи до комунікації з клієнтами

Клієнти, які оцінюють пристрій для покупки, швидше за все, повинні будуть знати, які можливості безпеки може надати пристрій. Після встановлення їм може знадобитися знати, як активувати, змінювати чи оновлювати такі функції. Таким чином, командам розробників необхідно спланувати, як донести цю інформацію до клієнтів. Питання, які слід розглянути, включають те, яку термінологію зрозуміє клієнт (виходячи з його технічної складності), скільки інформації йому знадобиться, як ця інформація має бути доступною та як клієнти можуть перевірити цілісність інформації.

6. Вирішіть, що і як повідомляти клієнтам

Багато факторів можуть брати участь у визначенні того, яку інформацію

передати та як це зробити. Одне, що слід враховувати, це те, як довго підтримувати пристрій після продажу та що станеться після закінчення терміну служби. Ще одне міркування полягає в тому, щоб визначити, що клієнти повинні знати про пристрій і його дизайн, щоб інтегрувати його в свої системи та обслуговувати його. Запитання також включають, як клієнти отримають оновлення програмного забезпечення, що вони повинні зробити, щоб вимкнути пристрій, і як вони можуть передати право власності іншій стороні. Документ NIST NISTIR 8259 містить численні додаткові, більш детальні пропозиції для команд розробників, які прагнуть брати участь у цій діяльності. Кібербезпека може здатися складною, але ці вказівки забезпечать командам розробників надійну основу для початку вирішення цієї проблеми.

Перелік посилань:

1. NISTIR 8259 Foundational Cybersecurity Activitiesfor IoT Device Manufacturers [Електронний ресурс] – Режим доступу: https://doi.org/10.6028/NIST.IR.8259

Соколянський Костянтин Анатолійович
студент групи БСДМ-53, ННІЗІ ДУТ, Київ, Україна

МЕТОДИ ПОБУДОВИ ЕФЕКТИВНОЇ SOC-МОДЕЛІ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ

Вступ

Зараз, в умовах зростаючих загроз кібербезпеці, все більша кількість компаній звертається до створення або залучення SOC - Security Operations Center, який має за мету забезпечення безпеки та захисту інформаційних систем від потенційних кібератак. Побудова ефективної SOC-моделі є важливою задачею для будь-якої компанії, яка зберігає важливу інформацію та прагне захистити її від кіберзагроз. У цій тезі будуть розглянуті методи побудови ефективної SOC-моделі у корпоративному середовищі, що дозволить компаніям відповідати на сучасні виклики кібербезпеки та забезпечувати надійний захист своєї інформації.

SOC - це центр забезпечення безпеки, створений з метою моніторингу, виявлення та реагування на потенційні загрози безпеці інформації компанії. Від побудови ефективної SOC-моделі залежить можливість реагувати на нові кібератаки та забезпечення надійного захисту інформації.

Побудова ефективної SOC-моделі у корпоративному середовищі потребує визначення конкретних потреб і викликів, що стоять перед компанією. Зазвичай, побудова SOC-моделі включає такі етапи як аудит існуючих систем безпеки, розробка стратегії та архітектури, вибір потрібного обладнання, встановлення необхідного програмного забезпечення, організація персоналу та тренінги для роботи зі створеною системою.

Для ефективної роботи SOC необхідні не тільки технічні засоби, а й професійний персонал, здатний швидко та правильно реагувати на загрози та вести розслідування кібератак. Крім того, необхідно враховувати специфіку діяльності компанії та можливість використання новітніх технологій та методів для забезпечення безпеки.

Для побудови ефективної SOC-моделі у корпоративному середовищі можна використовувати наступні методи:

1. **Визначення потенційних загроз та їхній аналіз** - цей метод полягає у визначенні можливих загроз та їхньому ретельному аналізі з метою виявлення потенційно небезпечних ситуацій. Для цього можна використовувати підписки на медіа-ресурси, які розміщують на своїх сторінках новини про останні загрози та вразливості, що дозволяє команді SOC оперативно реагувати та протидіяти актуальним загрозам.
2. **Встановлення системи моніторингу** - цей метод передбачає встановлення спеціальних систем моніторингу, що дозволяють відслідковувати потенційні загрози та вчасно реагувати на них (наприклад, DLP, WAF, тощо).
3. **Розробка плану реагування** - цей метод передбачає розробку детального плану дій, що дозволить ефективно реагувати на потенційні загрози та забезпечити максимальний рівень

захисту інформаційних ресурсів (наприклад, створення відповідних плейбуків з покроковим описом плану дій при певній категорії інциденту).

4. **Впровадження системи управління інцидентами** - цей метод полягає у впровадженні спеціальних систем управління інцидентами, що дозволяють ефективно координувати дії підрозділів SOC та швидко реагувати на потенційні загрози (наприклад, SIEM).
5. **Підвищення кваліфікації персоналу** - цей метод передбачає постійне підвищення кваліфікації персоналу SOC з метою забезпечення максимального рівня компетентності у сфері інформаційної безпеки (наприклад, проходження курсів від вендора, воркшопи, Threat Emulation, Red & Blue Teaming, тощо).

З яких елементів складається зразкова SOC-команда?

Зразкова SOC-команда повинна складатися з кваліфікованих фахівців, які мають різні компетенції та досвід у різних областях інформаційної безпеки. Така команда повинна мати наступний склад:

Аналітик загроз (Threat Analyst) - фахівець з аналізу та ідентифікації потенційних загроз для систем безпеки, включаючи виявлення нових атак та вразливостей.

Аналітик інцидентів (Incident Analyst) - фахівець з виявлення та розслідування інцидентів, який відповідає за вчасну ідентифікацію та вирішення проблем.

Адміністратор систем безпеки (Security Administrator) - фахівець з настройки та підтримки систем безпеки, включаючи моніторинг та управління доступом.

Інженер зі збереження даних (Data Retention Engineer) - фахівець зі збереження та відновлення даних, який відповідає за забезпечення належного збереження та доступу до даних в разі потреби.

Інженер зі збереження мережі (Network Retention Engineer) - фахівець зі збереження та аналізу мережі, який відповідає за збереження та аналіз мережевих даних.

Керівник SOC (SOC Manager) - відповідальний за керуванням всією командою SOC та забезпеченням високої рівня безпеки корпоративної інформації.

Крім того, зразкова SOC-команда повинна мати належні інструменти та технології для виявлення, аналізу та реагування на загрози.

Які інструменти та технології може потенційно використовувати SOC-команда?

SOC-команда повинна мати доступ до різних інструментів та технологій для ефективного виявлення, аналізу та реагування на загрози. Деякі з них включають:

1. **SIEM (Security Information and Event Management)** - це система, яка збирає та аналізує дані з різних джерел, виявляє потенційні загрози та надсилає сповіщення.
2. **IDS/IPS (Intrusion Detection and Prevention Systems)** - ці системи дозволяють виявляти та запобігати несанкціонованому доступу до мережі.
3. **Антивірусні програми та системи захисту від злочинної активності** - дозволяють виявляти та блокувати шкідливі програми та код.
4. **Firewall** - забезпечує захист мережі шляхом блокування небезпечного трафіку та фільтрації вхідних та вихідних даних.
5. **Моніторинг вхідних та вихідних даних** - дозволяє виявляти та запобігати несанкціонованому доступу до даних.
6. **Технології інтерналізації** - дозволяють відстежувати дії користувачів в мережі та ідентифікувати небезпечні патерни поведінки.
7. **Аналітичні інструменти** - дозволяють проводити детальний аналіз даних та виявляти складні шаблони поведінки атакувачів.
8. **Інструменти реагування на інциденти** - дозволяють вчасно реагувати на виявлені загрози та запобігати їх подальшій експлуатації.

Залежно від розміру та складності мережі, SOC-команда може використовувати різні комбінації інструментів та технологій для забезпечення ефективного захисту від загроз.

Отже, можна зробити висновок, що методи побудови ефективної SOC-моделі в корпоративному середовищі є важливим елементом в захисті інформаційної безпеки. При створенні SOC-команди необхідно враховувати фаховість, досвід та знання кожного члена команди. Також не менш важливою є правильна побудова процесів виявлення, аналізу та реагування на загрози, а також використання сучасних інструментів та технологій для цих цілей. Необхідність виявлення та реагування на загрози у реальному часі стає все більш актуальною, і SOC-команда є ключовим фактором для забезпечення безпеки в інформаційному просторі корпорації.

Степанов Михайло Григорович
Студент групи БСДМ-53, ННІЗІ ДУТ, Київ, Україна

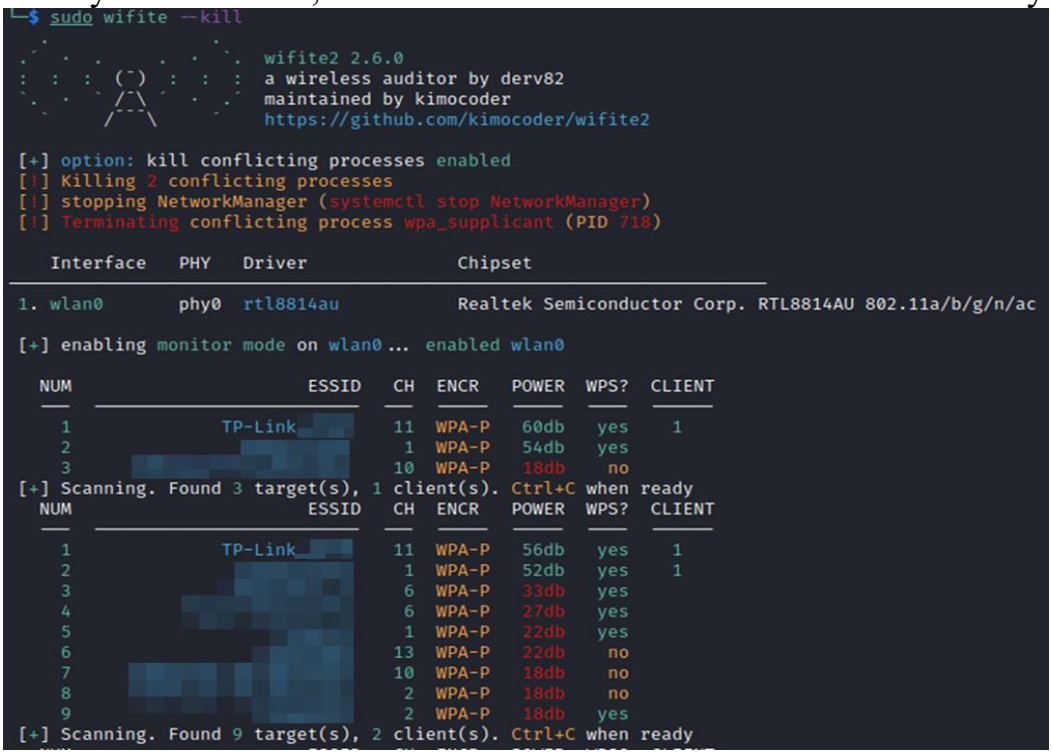
HOW TO PROTECT WIRELESS ACCESS POINTS FROM “PIXIE DUST” ATTACK

Nowadays, cybersecurity become a part of our daily routine. We should store passwords in a safe place, avoid phishing resources, and many other activities just to keep the private data in secret and not to lose the finances. Some of the responsibility for our security on the Internet lies on the services which process the personal data, such as online banking, e-commerce, exchanges, etc. That’s why we are providing penetration tests, audits, and many other security services. But all of this is useless if your own local area network is compromised. As soon as the malicious user connects to your Wi-Fi access point, he can capture the traffic and extract the passwords and credit cards data or navigate you to the fake resources instead of the legitimate one. That’s why we decided to prepare a three-part article where we will describe common attacks on the Wi-Fi routers in details and how to secure yourself from them.

“Pixie dust” attack

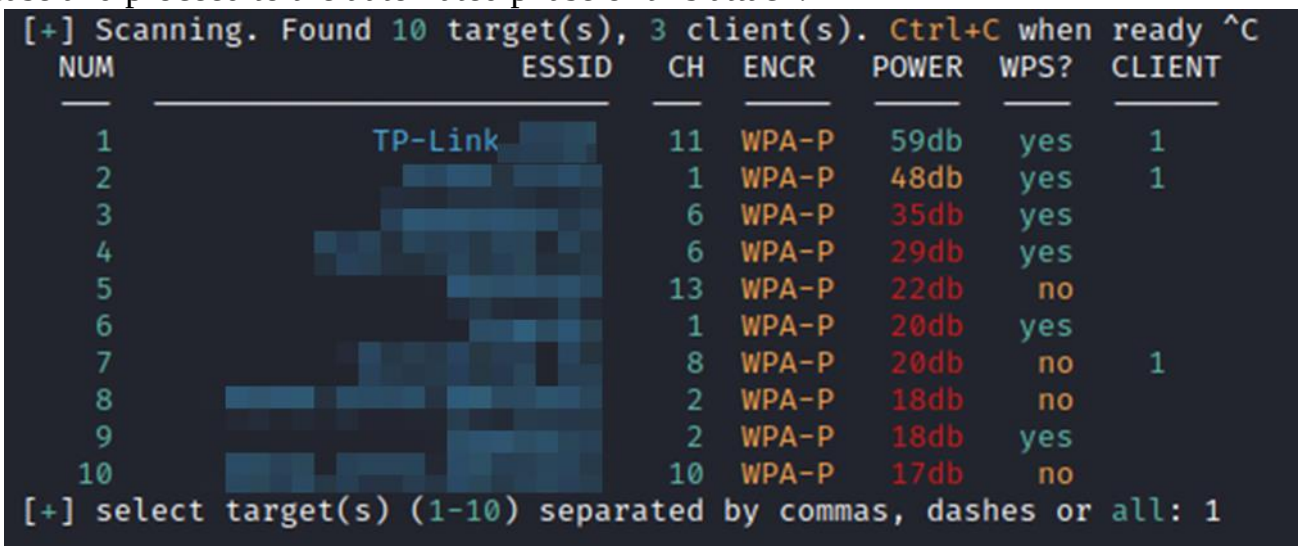
Cracking the WPS PINs is one of the easiest attacks. Everything you need is switch your network card to monitor mode, select the target and start the attack. All of this can be automated with built-in Kali Linux tool named wifite2.

To start with, run wifite2 as a sudo with –kill flag, which will kill all the conflicting processes: sudo wifite –kill. This tool will automatically enable monitor mode and start recon phase, which will help you to enumerate ESSID, channel, encryption type, power of the signal, is WPS enabled and number of clients of the access point. After the tool launched, you will the list of the wireless access points, which will be periodically updating. Wait until you will your target and then just “Ctrl + C” which will stop the recon phase. After that, everything you need to do is type the target's number, which is shown on the left side of the result table and hit enter. That’s all you need to do, all the other actions wifite will do automatically.



Pic.1 – “wifite” output

As it was mentioned before, after we enumerated the target, we need to make sure that WPS is enabled and then just enter target's number, which is number 1 in our case and proceed to the automated phase of this attack.



Pic.2 – Identified targets

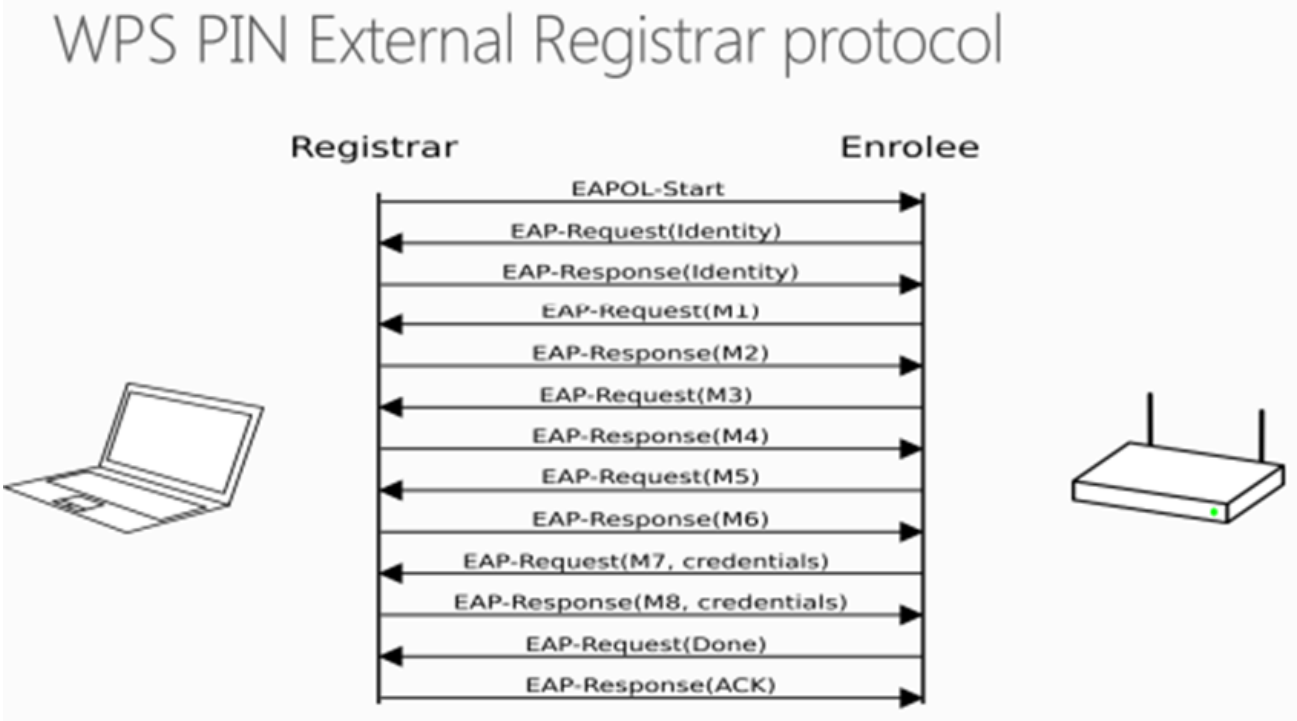
After a few seconds, we will see the result, in case the attack was successful. The output contains a cracked WPS PIN and a password which was retrieved from the router with the WPS PIN.

Pic.3 – Attacks result

As you can see, even the strongest password can be received in a second. So, let’s dive into some theory and try to get why it’s even possible and how to protect yourself.

Pic.4 – Attacks result

Back in 2013, the researcher whose name is Dominique Bongard, discovered that some of the wireless access points have weak algorithm of generating nonces, also known as E-S1 and E-S2, which supposed to be secret. In case we are able to find that numbers, we can easily get the WPS PIN of the access point, which is usually transmitted as a hash.



Pic.3 – WPS protocol

The picture above describes how the WPS works in depth, but as for attack, the most interesting actions are executed during the M1 and M3 messaging. With M1 message, the access point sends N1, a 128-bit random nonce generated by Enrollee, as well as PKE, Diffie-Hellman public key of the Enrollee. The M3 message is the most important part of this attack, as it contains E-Hash1 = $HMAC_{AuthKey}$(E-S1 || PSK1 || PKE || PKR) and E-Hash2 = $HMAC_{AuthKey}$(E-S2 || PSK2 || PKE || PKR) which will be used in further calculations. Finding E-S1 and E-S2, is a key to our win with PSK1 and PSK2 as a price. So how to get them? E-S1 and E-S2 is calculated right after the N1 nonce, with the same function and everything we need to do is brute force the state of that function with N1 and then just calculate the E-S1 and E-S2 values based on the function's state. After that we need to brute force PSK1 from E-Hash1 and PSK2 from E-Hash2. As a result, we will receive PSK1 value, which is first four numbers of the WPS PIN and PSK2 – the last four number of the WPS PIN.

Pic.3 – WPS protocol exmaple

Finally, do the full WPS protocol to get the credentials of the wireless access point. Looks too complex, doesn’t it. Thankfully for the security researchers from all around the world, all these actions were automated and packed to the great tools, and one of them was cowered by our article.

How to secure yourself from this attack? There are several methods: disable WPS, disable WPS, disable WPS, and finally, make sure, that WPS is not enabled on your router.

Тальченко Дмитро Олександрович, студент групи КБм-22-1
Державний університет «Житомирська політехніка», м. Житомир, Україна

АНАЛІЗ ВРАЗЛИВОСТЕЙ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Охорона територій та об'єктів за допомогою систем відеоспостереження є актуальним завданням для багатьох підприємств та установ. Однак, такі системи можуть стати об'єктом кібератак, оскільки вони можуть містити різноманітні вразливості. Розуміння і вчасне виявлення цих вразливостей надають адміністраторам безпеки можливість повноцінно захистити систему від отримання несанкціонованого доступу та викрадення конфіденційної інформації організації.

Які вразливості систем відеоспостереження можуть використовувати зловмисники.

Недостатній захист від несанкціонованого доступу та слабкі паролі. Багато систем відеоспостереження встановлюються з дуже слабкими паролями, або зовсім без них. Це дозволяє хакерам легко проникнути до системи та отримати доступ до відеозаписів. Для захисту систем відеоспостереження важливо встановлювати складні паролі та змінювати їх регулярно.

Відсутність шифрування. Багато систем відеоспостереження не використовують шифрування для захисту передачі даних між камерами та сервером, що може призвести до зловживань та викрадення даних. Шифрування даних є важливим кроком у забезпеченні безпеки системи відеоспостереження.

Несанкціонований доступ до записів. Відеозаписи можуть бути дуже цінними доказами в розслідуванні злочинів, тому вони мають бути доступні лише відповідним службам. Відсутність контролю доступу до відеозаписів може призвести до їх викрадення або маніпулювання ними.

Застарілі версії програмного забезпечення. Системи відеоспостереження можуть містити старі версії програмного забезпечення, які мають відомі вразливості. Наявність таких вразливостей може дозволити зловмисникам використовувати різні методи атак на систему. Щоб уникнути цього, важливо встановлювати оновлення програмного забезпечення та регулярно перевіряти систему на наявність вразливостей.

Недостатній захист під час передачі інформації. Крім шифрування даних, важливо забезпечити захист інформації під час її передачі через мережу. Це можна зробити за допомогою використання протоколів безпеки, таких як SSL або TLS.

Недостатній контроль захисту даних. Важливо встановити необхідний контроль захисту даних, які зберігаються на сервері системи відеоспостереження. Це включає у себе захист від вірусів, шкідливих програм та зловмисного програмного забезпечення.
Відсутність або недостатність фізичної безпеки. Система відеоспостереження може бути піддана фізичним атакам, таким як крадіжка камер або їх руйнування. Щоб забезпечити фізичну безпеку системи відеоспостереження, важливо встановити її на надійних місцях та використовувати високоякісні пристрої.
Недостатнє управління доступом. Деякі системи відеоспостереження можуть дозволяти доступ до камер та збереженого матеріалу навіть без авторизації. Це може стати проблемою, оскільки зловмисники можуть мати доступ до цієї інформації та використовувати її для своїх злочинних цілей. Важливо забезпечити авторизацію та аутентифікацію користувачів, щоб забезпечити високий рівень захисту.
Відсутність аудиту. Для того, щоб забезпечити високий рівень безпеки системи відеоспостереження, важливо мати можливість аналізувати журнали дій користувачів, які мають доступ до системи. Це дозволяє виявляти незвичну активність та несанкціонований доступ до системи.
Використання застарілих протоколів та технологій. Системи відеоспостереження можуть використовувати застарілі протоколи та технології, які мають відомі вразливості. Це може дозволити зловмисникам використовувати різні методи атак на систему. Щоб уникнути цього, важливо встановлювати оновлення програмного забезпечення та регулярно перевіряти наявність вразливостей.
Недостатній захист від внутрішніх загроз. Це включає в себе загрози, які походять від власних співробітників, які мають доступ до системи відеоспостереження. Важливо забезпечити контроль за діяльністю співробітників та встановити для них необхідні правила безпеки.
Недостатня кількість камер. Недостатня кількість камер може призвести до того, що система відеоспостереження не покриває всіх потрібних ділянок, які потрібно відслідковувати. Наприклад, якщо певна ділянка залишається без нагляду, це може стати вразливістю системи. Важливо ретельно спланувати розташування камер та встановити необхідну їх кількість.
Недостатня якість зображення. Низька якість зображення може призвести до того, що система відеоспостереження не зможе відслідкувати деталі, які можуть бути важливими для розслідування подій. Важливо встановити камери з достатньою роздільною здатністю та забезпечити правильне освітлення для кожної ділянки.
Незахищені мережеві протоколи. Коли система відеоспостереження підключена до мережі, важливо забезпечити захист мережевих протоколів. Недостатній захист може призвести до того, що зловмисники зможуть перехоплювати дані, які передаються по мережі. Важливо встановити шифрування трафіку та забезпечити захист мережевих протоколів.
Використання несумісних камер та обладнання. Якщо система

відеоспостереження використовує різноманітне обладнання від різних виробників, це може призвести до проблем із сумісністю та несправності обладнання. Важливо вибирати обладнання, яке підтримується системою відеоспостереження та є сумісним з іншим обладнанням.

Недостатня захищеність пристроїв зберігання даних. Проблема відноситься до використання звичайних дисків або flash-носіїв, що можуть бути просто викрадені. Вони повинні бути захищені від фізичного доступу, а також повинні бути захищені паролем і шифруванням. Якщо диск або flash-носій не захищені, це може призвести до витоку конфіденційної інформації.

Незабезпеченість системних патчів. Як і будь-яка інша система, система відеоспостереження потребує регулярних оновлень та системних патчів для забезпечення захисту від нових загроз. Недостатнє оновлення може призвести до вразливостей системи та може бути використане зловмисниками для атак.

Недостатня кількість обмежень доступу. Для запобігання несанкціонованого доступу до системи відеоспостереження важливо встановити необхідні обмеження доступу для користувачів системи. Це допоможе запобігти несанкціонованому доступу до відеозаписів та іншої конфіденційної інформації.

Недостатня освіта користувачів. Користувачі системи відеоспостереження можуть бути вразливі до атак, якщо вони не мають достатньої освіти про безпеку та правильне використання системи. Важливо проводити регулярне навчання користувачів системи відеоспостереження щодо правильного використання та забезпечення її безпеки [1, 2].

Таким чином, відеоспостереження є важливим інструментом для забезпечення безпеки в різних сферах, від охорони приватної власності до забезпечення безпеки вулиць та міст. Однак, як і будь-яка інша система, вона має свої вразливості, які можуть бути використані зловмисниками для атак на систему та витоку конфіденційної інформації. Для забезпечення безпеки системи відеоспостереження важливо встановлювати правильні налаштування, які зменшать ризик вразливостей та забезпечать безпеку системи відеоспостереження. До заходів безпеки систем відеоспостереження можна віднести наступні: регулярне оновлення системи відеоспостереження та її компонентів, що забезпечує усунення виявлених вразливостей та запобігання новим; використання сильних паролів та захищених мереж для забезпечення захисту від несанкціонованого доступу до системи; шифрування даних, що передаються та зберігаються в системі відеоспостереження; встановлення обмежень доступу до системи відеоспостереження для забезпечення захисту від несанкціонованого доступу до відеозаписів та іншої конфіденційної інформації; проведення регулярного навчання користувачів системи відеоспостереження щодо правильного використання та забезпечення безпеки.

У світі, де кібербезпека є одним з головних завдань, важливо приділяти належну увагу захисту систем відеоспостереження та підвищувати свідомість користувачів щодо правильного використання цих систем. Відповідальне ставлення до безпеки систем відеоспостереження може зменшити ризик вразливостей та забезпечити захист від можливих кібератак.

Перелік посилань:

1. Vennam, P., Pramod T. C., Thippeswamy B. M., Yong-Guk Kim, Pavan Kumar B. N. Attacks and Preventive Measures on Video Surveillance Systems: Review. Appl. Sci. 2021, 11, 5571.
2. Tanner LaRocque. Security Vulnerabilities in Networked Video Surveillance Systems. [Електронний ресурс] – Режим доступу: https://blog.razberi.net/security-vulnerabilities-in-networked-video-surveillance-systems

Поліщук Артем Сергійович,
Студент группи БСД-41 ,ННІЗІ ДУТ, Київ, Україна

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ВІД ІНСАЙДЕРСЬКИХ АТАК ЗА ДОПОМОГОЮ DEVICE LOCK DLP

Аннотація: інсайдерська атака є однією з найбільш складних викликів, з якими зіштовхуються організації у забезпеченні безпеки своєї інформації. Інсайдерська атака відбувається, коли працівник організації, який має легальний доступ до конфіденційної інформації, використовує цей доступ для зловживання чи збирання інформації зі своїх власних особистих мотивів. Інсайдерські атаки можуть призвести до втрати конфіденційної інформації, фінансових втрат, втрати довіри клієнтів та інших наслідків.

Програмний комплекс DeviceLock DLP складається з функціональних взаємодоповнюючих модулів - DeviceLock, NetworkLock, ContentLock, DeviceLock Search Server (DLSS) та DeviceLock Discovery, що ліцензуються опціонально в будь-яких комбінаціях для задоволення завдань служб інформаційної безпеки.

Базисний компонент DeviceLock є інфраструктурною платформою та ядром для іншихкомпонентів комплексу та реалізує всі функції його централізованого управління та адміністрування. DeviceLock підтримує повний набір механізмів контекстного контролю доступу користувачів, а також забезпечує подійне протоколювання (аудит) і тіньове копіювання даних для всіх локальних каналів введення-виведення на захищених комп'ютерах, включаючи периферійні пристрої та інтерфейси, системний буфер обміну, локально під'єднані смартфони та КПК, Media Transfer Protocol (MTP), а також канал друку документів на локальні та мережеві принтери. Крім того, компонент DeviceLock включає всі консолі централізованого управління.

Компонент NetworkLock™ забезпечує контекстний контроль каналів мережевих комунікацій на робочих комп'ютерах, включаючи розпізнавання мережевих протоколів незалежно від використовуваних портів, детектування комунікаційних додатків та їх селективну блокування, реконструкцію сесій з відновленням файлів, даних та параметрів, а також подієве протоколювання і тіньове копіювання даних, що передаються.

NetworkLock контролює більшість популярних мережевих протоколів та додатків, включаючи прості та SSL-захищені SMTP-сесії електронної пошти (з роздільним контролем повідомлень та вкладень), взаємодія між клієнтом Microsoft Outlook та сервером Microsoft Exchange (протокол MAPI), IBM Notes,

веб-доступ та інші HTTP програми, включаючи HTTPS сесії, веб-служби електронної пошти та соціальні мережі (AOL Mail, freenet.de, Gmail, GMX Mail, Hotmail (Outlook.com), Mail.ru, NAVER, Outlook Web App (OWA), Rambler Mail, T-online.de, Web.de, Yahoo! Mail, Yandex Mail, Zimbra; Facebook, Google+, Instagram, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, Pinterest, StudiVZ, Tumblr, Twitter, Vkontakte, XING, Disqus, LiveInternet.ru), служби миттєвих повідомлень (Skype, Telegram, Viber, WhatsApp, ICQ Messenger, Jabber, IRC, Mail.ru Агент), хмарні сховища (Amazon S3, Dropbox, Box, Google Drive, Microsoft OneDrive та ін), передачу файлів по протоколів FTP та FTP-SSL, передачу файлів у локальній мережі за SMB, а також сеанси Telnet та Торент.

Компонент ContentLock™ реалізує механізми контентного моніторингу та фільтрації файлів та даних, що передаються з/на змінні носії та в каналах мережевих комунікацій - веб-пошті та соціальних мережах, службах миттєвих повідомлень, файловому обміні протоколів FTP та FTP-SSL та ін. Крім того, технології контентної фільтрації в модулі ContentLock дозволяють встановити фільтрацію для даних тіньового копіювання, щоб зберігати лише ті файли та дані, які інформаційно значущі для завдань аудиту інформаційної безпеки, розслідувань позаштатних ситуацій та їх криміналістичного аналізу.

Компонент DeviceLock Search Server (DLSS) забезпечує повнотекстовий пошук по централізованих баз даних тіньового копіювання та подійного протоколювання.

Сервер DLSS дозволяє значно знизити трудомісткість та підвищити ефективність процесів аудиту та розслідування інцидентів інформаційної безпеки, пов'язаних з витоками інформації, їх криміналістичного аналізу та збору доказової бази.

DeviceLock Search Server може автоматично розпізнавати, індексувати, знаходити та відображати документи багатьох форматів, таких як: Adobe Acrobat (включаючи зашифровані файли, якщо шифрування файлу виконано одним із наступних алгоритмів: 40-bit RC4, 128-bit RC4, 128-bit AES та 256-bit AES, і при цьому дозволи, встановлені на файл, не забороняють вилучення тексту) (PDF), Ami Pro, AutoCAD (DWG, DXF), Архіви (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Visio, Microsoft Word, Microsoft Works, OpenOffice (документи, таблиці та презентації), Quattro Pro, WordPerfect, WordStar та багато інших.

Компонент DeviceLock Discovery виконує сканування робочих станцій та корпоративних мережевих ресурсів, і на підставі заданих політик здатний виявляти документи та файли з критичним вмістом, здійснювати різні дії з виявленими документами, а також може ініціювати процедури керування інцидентами, спрямовуючи тривожні оповіщення у реальному режимі часу. Детальну інформацію про DeviceLock Discovery можна знайти у документі “Посібник користувача DeviceLock Discovery”.

Перелік посилань:

1. Acronis DeviceLock DLP 9.0 Manual. – 2022. URL: https://dl.acronis.com/u/pdf/Acronis-DeviceLock-DLP-9.0-Man_en-US.pdf

2. Федеральне агентство з кібербезпеки (Federal Cybersecurity Agency). (2020). Інсайдерські атаки: розуміння,

виявлення та запобігання [Insider Attacks: Understanding, Detection, and Prevention]. – 2020. URL: https://www.cisa.gov/sites/default/files/publications/Insider_Attacks_508.pdf
3. Методи і технології захисту інформації в сучасних умовах / О. О. Шаталін, С. М. Коваленко, В. І. Чередніченко та ін. ; за заг. ред. О. О. Шаталіна. - Харків : Факт, 2018. - 438 с.

Васецька Поліна Олександрівна,
студентка групи БСД-41
ННІЗІ ДУТ, Київ, Україна

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ХМАРНИХ СЕРВІСІВ ІЗ ВИКОРИСТАННЯМ CISCO STEALTHWATCH CLOUD

В роботі розглядається хмарний інструмент безпеки мережі Cisco Stealthwatch Cloud з метою розробки рекомендації щодо збереження безпеки від вразливостей. Виток даних, отримання доступу до інформаційної системи можуть поставити під загрозу організацію, завдаючи величезної фінансової та репутаційної шкоди. Тому дослідження методів захисту та рекомендацій є актуальними.

Ключові слова: Cisco StealthWatch, SaaS, хмарне середовище, ПЗ

Cisco Stealthwatch Cloud — це хмарний інструмент безпеки мережі, який допомагає організаціям виявляти загрози та реагувати на них у реальному часі. Stealthwatch Cloud - це хмарне, ПЗ як послуга (SaaS), що надається на основі хмарних технологій і складається з двох основних пропозицій: Моніторинг публічної хмари та Моніторинг приватної мережі[2].

Моніторинг публічної хмари можна використовувати в поєднанні з моніторингом приватної мережі або Cisco Stealthwatch Enterprise, щоб забезпечити видимість і виявлення загроз у всій мережі, таких як Інфраструктури AWS, GCP і Microsoft Azure. Це хмарне рішення на основі SaaS(Software-as-a-Service), яке можна легко і швидко розгортати. Ця хмарна модель - найпоширеніша. Програми та сервіси розробляє і обслуговує провайдер, розміщує їх в хмарі і пропонує кінцевому користувачеві через браузер або додаток на його ПК, технічною підтримкою програм займається також провайдер[2].

Пропонованй продукт має всі можливості і засоби та ресурси для ефективного виявлення та реагування на загрози. Інтеграція з іншими рішеннями Cisco для забезпечення безпеки: Cisco Stealthwatch Cloud можна інтегрувати з іншими рішеннями безпеки Cisco, такими як Cisco Umbrella і Cisco Firepower, забезпечуючи комплексне рішення безпеки для організацій [1].

Головні переваги Cisco Stealthwatch Cloud:

- Видимість у реальному часі: що дозволяє командам безпеки швидко виявляти загрози та реагувати на них[3];
- Виявлення та реагування на загрози: Використовуються методи машинного навчання і поведінкового аналізу для виявлення і реагування на загрози в режимі реального часу;
- Хмарна архітектура[1];
- Простота розгортання та управління;

- Висока масштабованість;
- Відповідність вимогам: Рішення відповідає нормативним вимогам, таким як GDPR і PCI-DSS, надаючи детальну інформацію про мережевий трафік.

Головні недоліки Cisco Stealthwatch Cloud:

- Обмежена видимість: Cisco Stealthwatch Cloud покладається на аналіз мережевого трафіку для виявлення загроз. Як наслідок, він може бути не в змозі виявити загрози, які не видно в мережевому трафіку;
- Висока вартість: Вартість Cisco Stealthwatch Cloud може бути високою, особливо для малого та середнього бізнесу. Це може ускладнити для таких організацій виправдання витрат на розгортання рішення;
- Складність використання: Розгортання та конфігурація Cisco Stealthwatch Cloud може бути складним процесом, що вимагає значної кількості часу і досвіду для правильного налаштування. Це може бути складним завданням для організацій, які не мають спеціального IT-персоналу;
- Хибні спрацьовування;
- Залежність від мережевого трафіку.

Найкраші практики в організації безпеки передбачають деякі рекомендації та шляхи щодо захисту хмарних служб за допомогою Cisco Stealthwatch Cloud:

- Відстеження всього мережевого трафіку
- Налаштування попереджень і сповіщень
- Поведінкова аналітика: Stealthwatch Cloud використовує вдосконалену поведінкову аналітику для виявлення загроз і реагування на них
- Машинне навчання: Stealthwatch Cloud використовує алгоритми машинного навчання, щоб вивчати шаблони мережевого трафіку та виявляти аномалії.
- Інтеграція з іншими інструментами безпеки: Stealthwatch Cloud може інтегруватися з іншими інструментами безпеки, такими як брандмауери та системи запобігання вторгненням.
- Перегляд та оновлення політики

Використані джерела:

1. https://www.cisco.com/c/ru_ua/products/security/stealthwatch/index.html
2. https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf
3. https://habr.com/ru/company/tssolution/blog/509812/

Хоменко Анна Олегівна,
студентка групи БСДМ-43, ННІЗІ ДУТ, Київ, Україна

КОНЦЕПЦІЯ IOT ТА ЇЇ СКЛАДОВІ

Найбільш популярною та доступною мережею являється Internet of Things (IoT). IoT набуває поширення в сучасному світі, дану технологію ми зустрічаємо кожного дня. Оскільки, системи

Інтернету речей все більше, то питання безпеки залишається актуальним. Найчастішими проблемами являються: автентифікація, авторизація, витік інформації, конфіденційність, доступність, цілісність. Основними причинами безпеки є їх незахищене підключення до Інтернету та відсутність безпечного підключення.

IoT - це система взаємопов'язаних обчислювальних пристроїв, які в свою чергу забезпечені унікальними ідентифікаторами та можливістю передачі даних через мережу, яка не вимагає зв'язку «людина-людина» або «людина-комп'ютер». Дана система має вплив на багато сфер та застосовується кожним з нас. IoT представимо далі, як систему, яка:

- IoT являється сучасною інновацією в сфері технологій;
- IoT є однією з важливих технологією на сучасному ринку;

Вплив IoT з кожним роком підвищується та стає більш затребуваний. Розглянемо, що являє собою інформаційно-комунікаційні технології (IT), це засіб надійності та безпеки, та забезпечення систем для критичних та комерційних доменів.

За допомогою технології IoT можна створювати динамічні мережі, які складаються з кількох міліардів елементів, які в свою чергу взаємодіють між собою.

Існує багато факторів, за допомогою яких виник IoT, основні з них:

- Збільшення пропускної здібності інтернету;
- Здійснення доступу для користувачів і пристроїв до мережі із великої кількості місць;
- Збільшення кількості пристроїв, які мають доступ до інтернету;
- Збільшення потреб, які пов'язані з взаємодіями в Інтернеті;
- Розвиток інфраструктури інтернету речей.

Рис. 1 — Взаємодія IoT

До перших представників Інтернету речей можна віднести Machine-to-Machine, M2M). Дана технологія дозволяє машинам обмінюватися інформацією один з одним. Наприклад, банкомати можуть автоматично передавати інформацію по GSM-мережах, про те що в них закінчилися кошти або навпаки, що коштів багато і потрібно, щоб прийшли інкасатори. Застосування даної технології широко

поширене та застосовується у багатьох сферах, таких як: медицина, логістика, енергетика та багато інших. Один з найбільш популярних методів M2M являється дистанційний моніторинг і управління процесами за допомогою різних датчиків, міток. Цей метод називається Radio frequency identification (RFID). Мітки допомагають детального відслідковувати процеси виготовлення продукції. А також, допомагають оптимізувати логістичні ряди, мінімізувати витрати на транспорт, та найголовніше знизити людський фактор на всіх етапах виготовлення продукції та продажу товару. Саме, за допомогою даних міток, можна в будь-який момент відслідковувати стан товару, а також вони можуть повідомити про неполадки в роботі.

Отже, дана технологія надзвичайно поширена та вимагає надійного захисту. Заходи безпеки, які необхідно вжити слід розглядати на кожному рівні IoT. Якщо враховувати, відповідні правила, то ризик від атак, який спрямований на мережу буде мінімальний.

Перелік посилань:

1. F. Alaba, M. Othman, I. Hashem and F. Alotaibi, “Internet of Things security: A survey”, Journal of Network and Computer Applications, 88, pp.10-28, 2017.
2. H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," in IT Professional, vol. 19, no. 5, pp. 27-33, 2017.

Чорній Олександр Сергійович
студент групи БСД-42, ННІЗІ ДУТ, Київ, Україна

УПРАВЛІННЯ ТА ОБ'ЄДНАННЯ АВТОМАТИЗОВАНИХ СИСТЕМ «РОЗУМНОГО» БУДИНКУ

Визначено актуальність процесу об'єднання різних систем у єдину інтегровану систему керування. включаючи в себе протоколи зв'язку, які використовуються для комунікації між системами, методи інтеграції систем, технології моніторингу та управління системами. Розглянуто переваги та недоліки використання інтегрованих систем "розумного" будинку, а також способи вирішення можливих проблем, які можуть виникати в процесі їх розгортання та експлуатації.

Однією з ключових технологій, що використовується в розумних будинках, є Інтернет речей (IoT). IoT дозволяє підключати до мережі Інтернет різноманітні пристрої, такі як датчики, електроприлади, системи безпеки, системи опалення та кондиціонування повітря.

Це дозволяє дистанційно керувати всіма цими пристроями через Інтернет, що забезпечує високу рівень комфорту та енергоефективності [1].

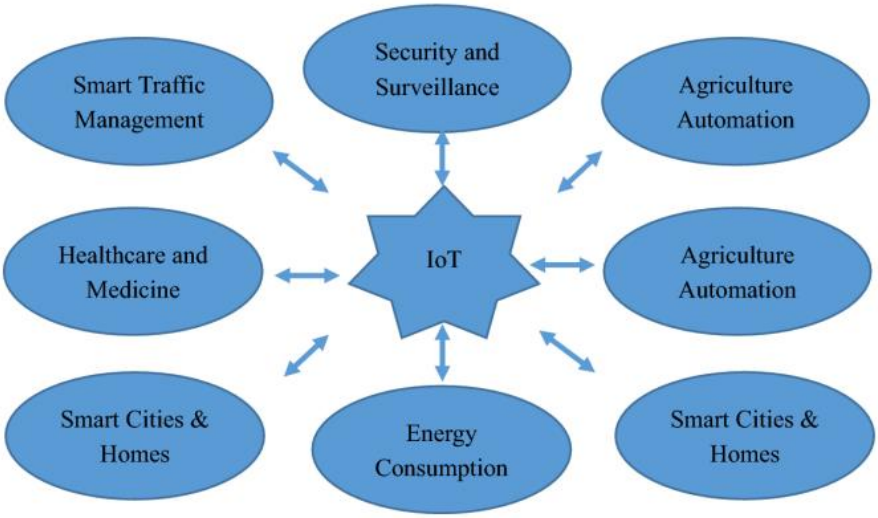


Рис.1 – Потенційні області застосування Інтернет речей

Крім того, в розумних будинках можуть використовуватися системи штучного інтелекту, що дозволяють аналізувати інформацію, зібрану датчиками та іншими пристроями, та приймати рішення щодо управління будинком. Блокчейн також може допомогти забезпечити безпеку даних, збережених у системі управління будинком, оскільки він дозволяє зберігати дані в зашифрованому вигляді та контролювати доступ до них.

Важливим елементом розумного будинку є також системи зберігання енергії, які можуть забезпечувати енергонезалежність та допомагати економити на витратах на електроенергію. Серед технологій, що використовуються для зберігання енергії, можна виділити сонячні батареї, батареї зарядки на основі вітроенергії та гідроенергії, а також системи зберігання енергії на основі різних хімічних речовин [2].

Зокрема, що стосується систем автоматизації, то вони базуються на інтернеті речей (IoT), який дозволяє розумним пристроям спілкуватись між собою та зі спеціальними платформами керування. Наприклад, система освітлення може виконувати різні функції, такі як включення світла відповідно до розкладу, адаптування яскравості до зміни освітленості в приміщенні, включення світла відповідно до наявності людей у кімнаті тощо. Аналогічні функції реалізуються у системах опалення, кондиціювання повітря та інших [3].

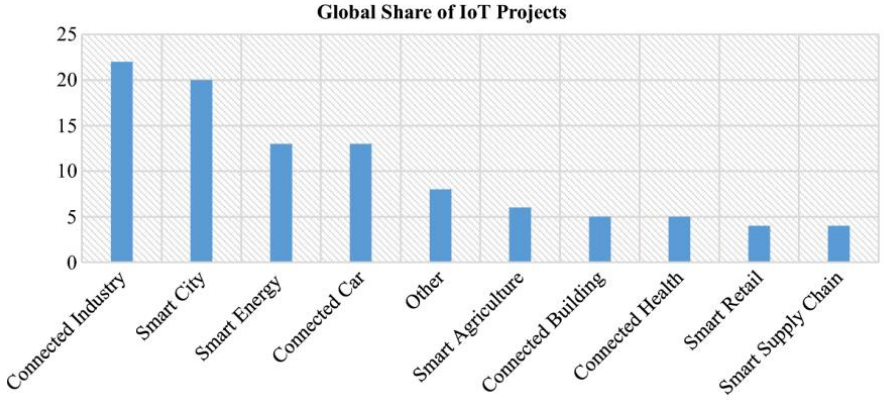


Рис.2 – Глобальна частка проектів Інтернет речей у світі

Остаточно, важливо зазначити, що розумні будинки – це дуже комплексна система, яка поєднує в собі різноманітні технології та пристрої. Ці технології дозволяють забезпечити високий рівень комфорту, енергоефективності та безпеки у будинку, що робить їх дуже привабливими для власників житла та інших користувачів.

Перелік посилань:

1. "Smart Home Automation: A Literature Review" [Електронний ресурс] – Режим доступу: https://www.mdpi.com/1424-8220/19/20/4325
2. "A Survey of Smart Homes: Past, Present, and Future" [Електронний ресурс] – Режим доступу: https://ieeexplore.ieee.org/abstract/document/6682373
3. "A Comprehensive Review on Smart Home Technology: State-of-the-Art and Future Directions" [Електронний ресурс] – Режим доступу: https://www.mdpi.com/1424-8220/21/3/1089

Шайкова Анастасія Олегівна
Студентка групи БСД-41, ННІЗІ ДУТ, Київ, Україна

ЗАХИСТ ДИСТАНЦІЙНИХ ПРАЦІВНИКІВ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ CISCO UMBRELLA

Визначено актуальність захисту дистанційних працівників. Розглянуто можливості нанесення шкоди організаціям через дистанційних працівників. Досліджено можливості вирішення загроз з рішенням Cisco Umbrella. Розкрито зміст технології захисту дистанційних працівників на базі рішення Cisco Umbrella.

Останніми роками дистанційна робота стала більш поширеною через низку причин. Доступність інструментів для спільної роботи та широке використання високошвидкісного інтернету спростили людям роботу на відстані як ніколи раніше. Багато працівників прагнуть покращити баланс між роботою та особистим життям і отримати більшу гнучкість у плануванні робочого часу. Люди, які працюють віддалено, мають можливість робити це з будь-якого місця, що дає їм більше контролю над своїм часом і покращує їхню здатність балансувати між особистими та професійними обов’язками. Компанії все більше усвідомлюють переваги віддаленої роботи, зокрема вищу продуктивність та нижчі накладні витрати. Більше того, віддалена зайнятість може гарантувати безперервність бізнесу в надзвичайних ситуаціях, таких як пандемія чи стихійне лихо.

Хоча віддалена робота може мати багато переваг, вона також несе в собі загрози та виклики, які організації повинні враховувати. Збільшується ризик кібератак і витоку даних, оскільки працівники, які працюють дистанційно, можуть отримувати доступ до конфіденційної інформації з незахищених мереж або пристроїв. Організаціям важливо забезпечити працівникам доступ до захищених мереж і пристроїв, а також навчити їх найкращим практикам кібербезпеки. Деякі загрози, пов’язані з віддаленою роботою, включають наступні: фішинг, шкідливе програмне забезпечення, DoS, сканування портів.

Cisco Umbrella – хмарна платформа, що забезпечує захист від загроз в інтернеті. Функції безпеки Cisco Umbrella [1]:

1. Захист на рівні DNS від Umbrella – це найшвидший і найпростіший спосіб підвищити рівень безпеки. Він допомагає поліпшити видимість безпеки, виявити скомпрометовані системи та захистити ваших користувачів у мережі та поза нею, зупиняючи загрози через будь-який порт або протокол ще до того, як вони потраплять у вашу мережу або на кінцеві точки.

2. Безпечний веб-шлюз Umbrella. Реєструє та перевіряє веб-трафік, забезпечуючи повну видимість, контроль URL-адрес і додатків, а також захист від шкідливого програмного забезпечення. Використовуйте тунелі IPsec, PAC-файли для перенаправлення трафіку на наш хмарний проксі-сервер, щоб забезпечити дотримання прийнятних політик використання та блокувати сучасні загрози.

3. Мережевий екран. Реєструє всю активність і блокує небажаний трафік, використовуючи правила для IP-адрес, портів і протоколів. Щоб переадресувати трафік, просто налаштуйте IPsec-тунель з будь-якого мережевого пристрою. При створенні нових тунелів політики автоматично застосовуються для простого налаштування та послідовного застосування скрізь.

4. Cloud access security broker. Щоб безпечно й організовано керувати переходом на хмарні технології, потрібна повна інформація про ризики та їхню видимість. Після прийняття рішень щодо конкретних програм необхідно блокувати можливий доступ до несанкціонованих додатків, щоб зменшити ризик втрати конфіденційних даних, компрометації облікових записів і зараження шкідливим програмним забезпеченням.

5. Інтерактивна розвідка загроз. Надає інформацію про шкідливі домени, IP-адреси та URL-адреси. Доступний через консоль та API, Umbrella Investigate в режимі реального часу сповіщає про шкідливе програмне забезпечення, фішинг, ботнети, трояни та інші загрози, що дозволяє швидше розслідувати інциденти та реагувати на них [1].

6. Інтеграція з SD-WAN. Інтеграція Umbrella та Cisco SD-WAN легко розгортається у вашій мережі для потужного захисту від хмарних загроз та інтернет-загроз. Наш інтегрований підхід забезпечує доступ до хмарних сервісів і ефективно захищає користувачів філій, підключені пристрої та програми від будь-яких прямих атак на доступ до Інтернету.

SASE – це гнучка архітектура, створена спеціально для гібридних робочих місць, розподілених мереж та компаній з віддаленими працівниками. Рішення SASE забезпечує мережеві та безпекові можливості в хмарі, пропонуючи компаніям можливість безперешкодно масштабуватися відповідно до зростаючої кількості працівників, незалежно від їхнього місцезнаходження [2].

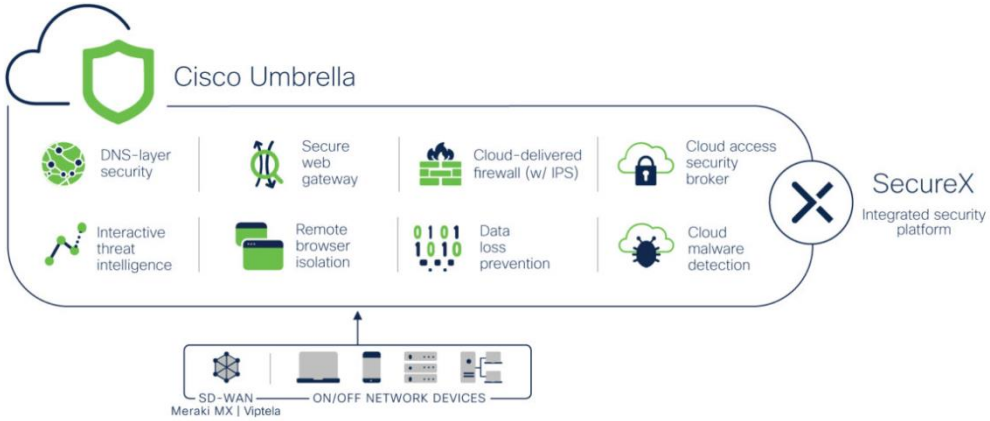


Рис. 1 – Модель безпеки SASE в Cisco Umbrella

Завдяки Cisco Umbrella віддалені співробітники отримують повний захист, який допомагає забезпечити безпеку їхніх мереж, пристроїв і даних. Розгорнувши Cisco Umbrella, організації можуть захиститися від різноманітних кіберзагроз і забезпечити своїм працівникам, які працюють дистанційно, безпечне та ефективне робоче середовище.

Перелік посилань:
1. Cloud Security Service. Cisco Umbrella. URL: https://umbrella.cisco.com/products/cloud-security-service.
2. Our SASE Solution – Secure Access Service Edge. Cisco Umbrella. URL: https://umbrella.cisco.com/secure-access-service-edge-sase/cisco-umbrella-sase.

Шиповський Володимир Володимирович,
Ад'юнкт кафедри ІАТ, ІІКТК,НУОУ

ЗАСТОСУВАННЯ ЛУКОВИЦІ БЕЗПЕКИ В МУЛЬТИШАРОВІЙ МОДЕЛІ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Термін "луковиця безпеки" (англ. security onion) в кібербезпеці використовується для опису архітектурного підходу до забезпечення безпеки мережі. Цей підхід полягає у розгляді мережі як багатошарової структури, подібної до луковиці. Кожен шар мережі захищений своїми власними заходами безпеки, що дозволяє забезпечити більш високий рівень захисту в порівнянні зі звичайним підходом до захисту мережі.

Зазвичай, луковиця безпеки складається з таких шарів:

1. Шар користувачів: захист від соціальної інженерії та фішингу.
2. Шар антивірусного програмного забезпечення та вогнепальних стін: захист від шкідливих програм та інших видів зловмисних атак.
3. Шар моніторингу мережі: забезпечує відслідковування активності в мережі та виявлення потенційно небезпечних дій.
4. Шар захисту від DDoS-атак: забезпечує захист від розподілених атак на відмову в обслуговуванні.
5. Шар захисту від витоку даних: забезпечує захист від незаконного виведення конфіденційної інформації з мережі [1].

Для опису луковиці безпеки за допомогою математики можна використовувати поняття теорії множин та логічних операцій.

уковиця безпеки є багаторівневою моделлю захисту, яка складається з кількох шарів. Можна описати луковицю безпеки за допомогою наступної математичної формули:

$$L = (S1, S2, ..., Sn)$$

де *L* - луковиця безпеки, *S1-Sn* - окремі шари захисту, які включають різні заходи для забезпечення безпеки інформаційної системи.

Кожен шар має власну функцію захисту, що може бути описана як:

$$Si = f(Xi, Yi)$$

де *Si* - *i*-й шар, *Xi* - вхідні дані в шар, *Yi* - вихідні дані з шару, *f* - функція захисту, яка забезпечує захист вхідних даних та надсилає оброблені дані на наступний шар.

Також можна описати внутрішній процес функціонування луковиці безпеки за допомогою наступної математичної формули:

$$Yn = f(Sn, f(Sn-1, ... f(S2, f(S1, X)) ...))$$

де *Yn* - вихідні дані з останнього шару, *X* - вхідні дані, *f* - функція захисту, що застосовується до кожного шару послідовно [2].

Отже, луковиця безпеки може бути описана за допомогою математичних формул, що допомагає розуміти, як вона працює та які заходи захисту включаються в кожен шар.Кожен наступний шар луковиці безпеки містить доповнення до попереднього шару, що дозволяє захистити мережу від більш широкого спектру загроз. Оскільки кожен шар містить доповнення до попереднього, то зростає загальний рівень захисту мережі.

Хоча луковиця безпеки є корисним інструментом для захисту мережі від різних загроз, вона не є універсальним рішенням і не може покрити всі можливі проблеми, які можуть виникнути в області кібербезпеки. Деякі з проблем, які не можуть бути вирішені за допомогою луковиці безпеки, включають:

Недосконалість програмного забезпечення: незалежно від застосовуваних заходів захисту, програмне забезпечення може містити вразливості, які можуть бути використані зловмисниками для здійснення атак.

Соціальна інженерія: зловмисники можуть використовувати соціальну інженерію для отримання доступу до системи або інформації, обхідуючи технічні засоби захисту.

Недосконалість алгоритмів машинного навчання: системи захисту, які використовують алгоритми машинного навчання, можуть бути обмануті зловмисниками, які знають, які дані використовуються для навчання.

Внутрішні загрози: луковиця безпеки зазвичай орієнтована на зовнішні

загрози, але існують внутрішні загрози, такі як зловживання довірою, які можуть бути важко виявити за допомогою технічних засобів захисту.

Отже, хоча луковиця безпеки є корисним інструментом для захисту мережі, важливо розуміти, що вона не є універсальним рішенням і потребує постійного оновлення та доповнення для врахування нових типів загроз. Застосування луковиці безпеки в мультишаровій моделі може значно збільшити ефективність захисту інформаційних систем об'єктів критичної інфраструктури від кіберзагроз. Використання цієї моделі дозволяє створити багаторівневий захист, що забезпечує надійну оборону від різноманітних кібератак та зменшує ризик порушення безпеки даних. Застосування мультишарової моделі з луковицею безпеки є актуальною задачею для організацій, що працюють з об'єктами критичної інфраструктури, оскільки це допоможе зберегти інформацію від кіберзагроз та зберігати функціональність об'єктів.

Перелік посилань:
1. THE ONION OF CYBER SECURITY: 6 LAYERS OF DIGITAL SECURITY. [Електронний ресурс] – Режим доступу: https://dut.edu.ua/ua/news-1-574-10778-vseukrainska-naukova-konferenciya--cifrova-transformaciya-kiberbezpeki_kafedra-informaciynoi-ta-kibernetichnoi-bezpeki
2. Data Security Defense in Depth: The Onion Approach to IT Security. [Електронний ресурс] – Режим доступу: httpshttps://securityintelligence.com/data-security-defense-in-depth-the-onion-approach-to-it-security/

Щур Наталія Олександрівна
старший викладач кафедри комп'ютерної інженерії та кібербезпеки,
Державний університет «Житомирська політехніка», Житомир, Україна

ПЕРЕВАГИ ТА НЕДОЛІКИ ВПРОВАДЖЕННЯ ЛЕГКОВАГОВОЇ КРИПТОГРАФІЇ В ПРИСТРОЯХ IOT

Пристрої Інтернету речей (IoT) стають все більш поширеними в нашому повсякденному житті, і потреба в безпечному та ефективному зв'язку між ними є надзвичайно важливою. Одним із способів досягти цього є використання криптографічних рішень, які забезпечать надійний захист, будуть ефективними з обчислювальної точки зору та використовуватимуть менше ресурсів. Метою даної роботи є дослідження переваг та недоліків впровадження легковагових криптографічних алгоритмів для захисту IoT пристроїв.

IoT являє собою мережу взаємозв'язаних фізичних пристроїв, які здатні збирати, обробляти та передавати дані через Інтернет з метою автоматизації та оптимізації процесів в різних сферах життя. Ці дані можуть включати інформацію про стан пристроїв, їхнє місцезнаходження, взаємодію з іншими пристроями тощо. Зловмисники можуть використовувати IoT-пристрої для атак на комп'ютерні системи або мережі, що часто призводить до крадіжки конфіденційної інформації, шахрайства або розповсюдження шкідливого програмного забезпечення. Таким чином, дуже важливо зберегти та захистити інформацію та дані, що використовуються в IoT.

Захист пристроїв та мереж IoT криптографічними методами є складним завданням з кількох причин. По-перше, процесори в пристроях IoT мають невелику фізичну площу та низьку обчислювальну потужність для обробки

даних. По-друге, більшість алгоритмів криптографічного захисту споживають багато енергії під час роботи, а пристрої IoT зазвичай живляться від батареї, що має обмежений заряд. Тому звичайні криптографічні методи можуть бути непрактичними або неефективними для захисту IoT. Це визначає необхідність розробки та застосування алгоритмів малоресурсної (low resource) або легковагової криптографії (lightweight cryptography, LWC), яка призначена для ефективної роботи на пристроях з обмеженими обчислювальними ресурсами [1]. Існує багато «полегшених» криптографічних алгоритмів, вибір яких залежить від конкретних потреб мережі IoT та вимог до безпеки даних. Деякі з них є звичайними алгоритмами шифрування, в той час як інші також забезпечують автентифіковане шифрування з приєднаними даними (Authenticated Encryption with Associated Data, AEAD) або хешування.

Розглянемо деякі з переваг впровадження легковагової криптографії в пристроях IoT.

Енергоефективність. Алгоритми легковагової криптографії оптимізовані для пристроїв з обмеженими ресурсами, що означає, що вони вимагають менше потужності та енергії, ніж традиційні криптографічні алгоритми. Таким чином, IoT-пристрої можуть бути захищені без шкоди для їх продуктивності або часу роботи батареї.

Компактність. Пристрої IoT часто мають обмежений фізичний простір, тому «полегшені» криптографічні алгоритми мають менший обсяг коду та забезпечують ефективне використання пам’яті, що є критичним для вбудованих пристроїв та інших IoT-систем.

Швидкість. Легковагова криптографія вимагає меншої кількості обчислень та використання обчислювальних ресурсів, що дозволяє забезпечити швидше шифрування та дешифрування даних.

Безпека. Незважаючи на те, що LWC-алгоритми розроблені для пристроїв з обмеженими ресурсами, вони є досить крипостійкими та забезпечують ефективний захист від різних типів атак. Вони також пропонують надійні інструменти для перевірки автентифікації та цілісності даних.

Гнучкість. Малоресурсні криптоалгоритми прості в налаштуванні, що означає, що їх можна адаптувати відповідно до конкретних потреб різних пристроїв IoT. Це дозволяє виробникам вибирати відповідний рівень безпеки для своїх пристроїв залежно від даних, які потребують захисту.

Водночас впровадження легковагової криптографії в пристроях Інтернету речей може також бути складним через низку недоліків описаних нижче.

Невеликі розміри ключів. Одним із основних недоліків LWC-алгоритмів є те, що вони зазвичай використовують менші розміри ключів, ніж традиційні криптографічні алгоритми. Це може зробити їх більш вразливим до атак методом грубої сили, що включає спробу перебору всіх можливих комбінацій ключів, доки не буде знайдено правильну.

Проблеми сумісності. «Полегшені» криптографічні алгоритми можуть бути несумісними з усіма пристроями IoT, особливо з тими, які використовують традиційні алгоритми, що може ускладнити їх інтеграцію в існуючі екосистеми

Інтернету речей.

Відсутність стандартизації. Пристрої IoT бувають різних форм та розмірів, і не існує стандартного протоколу для їхнього зв'язку один з одним. Це може збільшити складність і вартість реалізації заходів безпеки для пристроїв IoT. Варто зазначити, що Національний інститут стандартів і технологій (NIST) ініціював процес стандартизації легковагових криптографічних алгоритмів [2].

Схильність до атак сторонніми каналами. «Полегшені» алгоритми криптографії можуть бути вразливішими до атак сторонніми каналами, які використовують слабкі місця в реалізації алгоритму.

Додаткові витрати. Впровадження полегшеної криптографії в пристроях IoT може вимагати додаткових витрат на апаратне та програмне забезпечення, що може стати проблемою для деяких виробників, які працюють з обмеженим бюджетом.

Незважаючи на певні недоліки, легковагова криптографія здатна забезпечити ефективний захист даних IoT-пристроїв за мінімального використання обчислювальних ресурсів. Розробники повинні ретельно враховувати компроміси між безпекою та продуктивністю під час вибору криптографічних методів для пристроїв IoT і переконатися, що вибрані алгоритми відповідають вимогам безпеки конкретної реалізації IoT.

Перелік посилань:

1. Lightweight Cryptography to Secure Internet of Things (IoT) [Електронний ресурс] – Режим доступу: https://www.irjet.net/archives/V7/i5/IRJET-V7I51179.pdf
2. Lightweight Cryptography [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/projects/lightweight-cryptography

Васьків Оксана Миколаївна
ст. викл. кафедри цифрової економіки та бізнес-аналітики
факультет управління фінансами та бізнесу
ЛНУ імені Івана Франка, Львів, Україна
Яковець Ірина Вікторівна
студентка групи УФЕ-31с, ЛНУ імені Івана Франка, Львів, Україна

ПЕРЕОСМИСЛЕННЯ КІБЕРБЕЗПЕКИ ПІД ЧАС ВОЄННОГО СТАНУ

Від початку повномасштабного вторгнення росії Україна стала ціллю чисельних кібератак, які охопили державні установи, приватні організації, громадян, які ведуть комунікацію за допомогою електронних засобів зв'язку, що несе загрозу їхньому інформаційному простору не менше, аніж війна на полі бою.

Розуміючи це, у перший місяць війни парламент оперативно оптимізував кримінальне та кримінально-процесуальне законодавство, удосконаливши підстави та процесуальні механізми притягнення до кримінальної відповідальності кіберзлочинців. Зміни зосереджено відповідних законах [1, 2].

В умовах сьогодення викликами для України у сфері кібербезпеки є [3, 4]:

1) активне використання кіберзасобів у міжнародній конкуренції;

2) конкурентний характер розвитку інструментів кібербезпеки в контексті інформаційно-комунікаційних технологій, що швидко розвивається та змінюється, особливо хмарних і квантових обчислень, мереж 5G, великих даних, Інтернету речей, штучного інтелекту тощо;

3) мілітаризація кіберпростору та розробка кіберзброї для здійснення таємних кібератак у кіберпросторі для підтримки військових дій та діяльності знищення інформації;

4) вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинило швидку зміну та організацію значної частини суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем;

5) впровадження нових технологій, цифрових сервісів та електронних механізмів взаємодії між громадянами та державами, які здійснюються поетапно без належної оцінки ризиків з точки зору заходів кібербезпеки.

Розглядаючи виклики кібербезпеки у сьогоденні, перед компаніями постало питання готовності до кіберінцидентів і шляхи вирішення наявних атак.

Експертами KPMG було підготували рекомендації, що можуть допомогти оцінити рівень готовності кібербезпеки тієї чи іншої компанії, а саме (рис. 1.) [5].

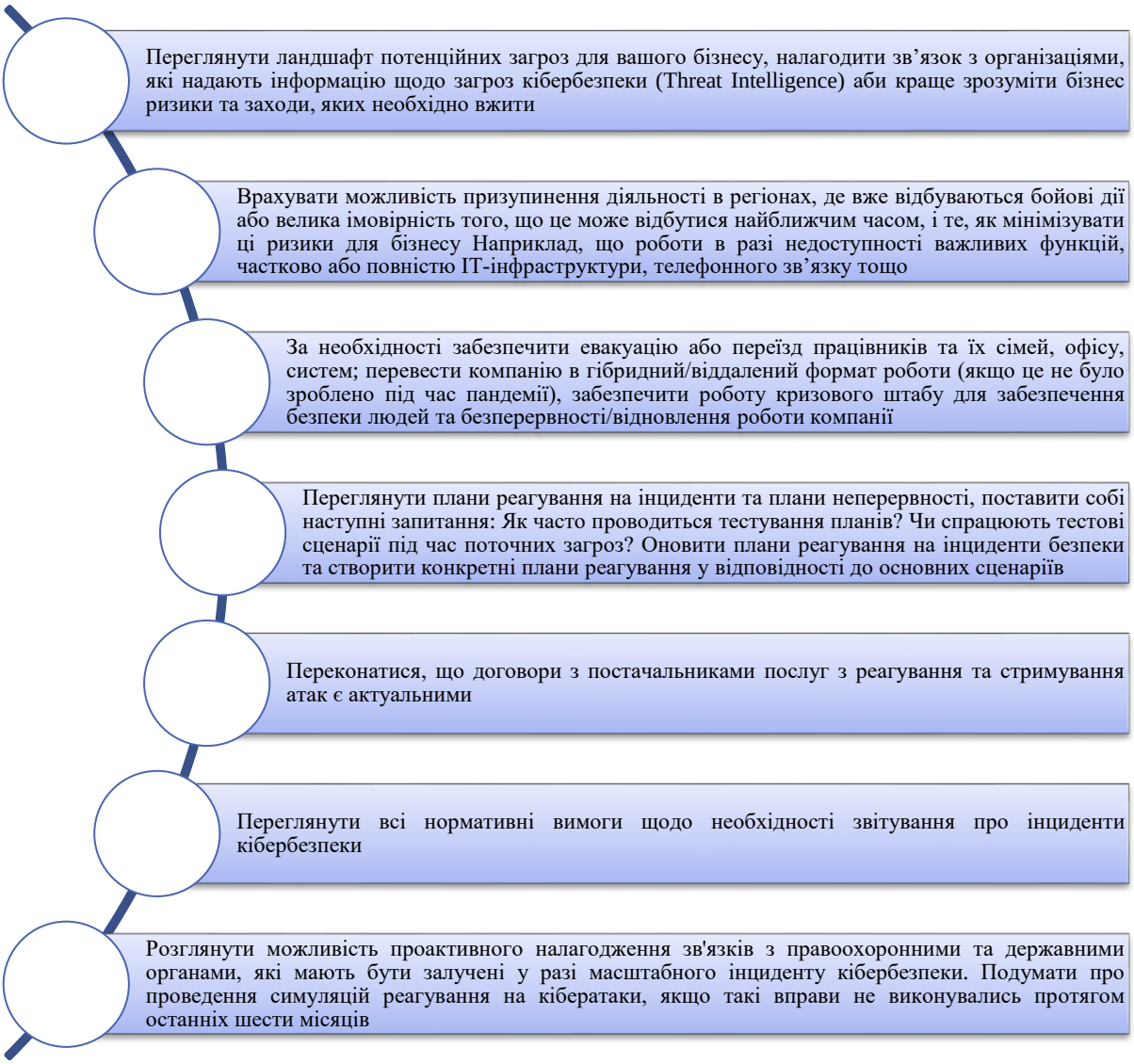


Рис. 1 – Рекомендації, що можуть допомогти оцінити рівень готовності кібербезпеки компанії
Джерело: розроблено автором за [5]

Кібербезпека повинна не лише реагувати на інциденти, а й запобігати атакам до початку їх здійснення. Проблема ефективного забезпечення інформаційної безпеки потребує комплексного вирішення і вимагає скоординованих дії на національному та міжнародному рівні для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади [6].

В контексті актуального питання варто наголосити на варіантах захисту конфіденційної інформації від кібератак (рис. 2) [5, 6].

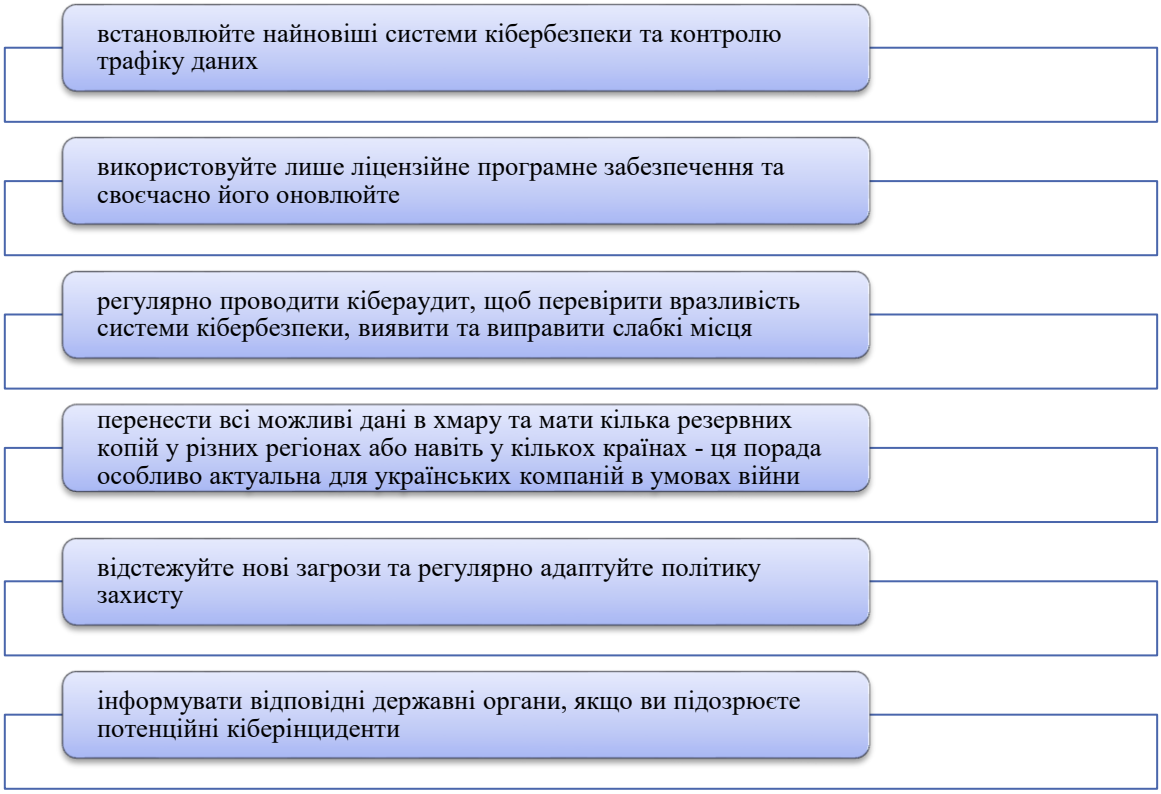


Рис. 2 – Варіанти захисту конфіденційної інформації
Джерело: розроблено автором за [6]

Кібербезпека є безперервним та вкрай актуальним процесом в сучасних українських реаліях. Доцільно впроваджувати відповідні заходи, особливе значення серед яких належить налагодженню потужного кіберзахисту інформаційних систем. Також варто приймати до уваги, що ворог постійно працює над удосконалення кібератак, тому стратегічно важливо як для державних установ, так і для приватного бізнесу, так і для звичайних людей, працювати над покращенням кібербезпеки, що створює непереможну стратегію, яка забезпечує Україні потужний інформаційний тил.

Перелік посилань:

1. Інформаційні злочини. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96_%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%B8
2. Боротьба з кіберзлочинністю в умовах дії воєнного стану. Закон 2149-IX. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix
3. 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. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12.
4. Кузьменко О., Маклюк О., Чернишова О. Кібербезпека бізнесу під час війни. Економіка та суспільство. – Випуск №44. – 2022. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1790
5. Янковський О. Питання кібербезпеки в умовах воєнного часу. URL: https://kpmg.com/ua/uk/blogs/home/posts/2022/4/pytannya-kiberbezpeky-v-umovakh-voyennoho-chasu.html
6. Кібербезпека бізнесу під час війни. URL: https://mklegalservice.com/tpost/k123zz39h1-kberbezpeka-bznesu-pd-chas-vini

Якименка Юрія Михайловича
доцента кафедри УІКБ,ННІЗІ ДУТ, Київ, Україна

ПІДВИЩЕННЯ РОЛІ DLP - СИСТЕМ У РОЗСЛІДУВАННІ ІНЦИДЕНТІВ (КІБЕРІНЦИДЕНТІВ) ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Головною проблемою з кібербезпеки на сьогодні залишається створення ефективної системи менеджмента (управління) у області інформаційної безпеки (ІБ) – СМІБ (СУІБ). Для вирішення задач контролю всіх інформаційних потоків, що відбуваються в організаціях існує система DLP (Data Leak Protection). розробники нових DLP стали впроваджувати у свої додатки до систем питання розслідування інцидентів, що допоможе службі безпеки виявляти факт порушення правил обігу із секретною інформацією. Першочерговими завданнями становлять питання автоматизації процесів управління інцидентами інформаційної безпеки у сучасних DLP – Системах в напрямках виявлення, реагування і розслідування інцидентів . Тому при роботі із системою DLP пропонується орієнтуватись на послідовність кроків в управлінні інцидентами ІБ (кіберінцидентами).

Розвиток сучасних DLP-Систем іде в напрямку автоматизації процесів не тільки в засобах реєстрації подій і інцидентів інформаційної безпеки (ІБ), в тому числі і кіберінцидентів, а ще і в управлінні ними. У системі DLP створено безліч перехоплювачів, агентів і пошукових роботів, які збирають відомості про інформаційні системи організації й активності її окремих співробітників. Але всі ці зібрані дані не захищають, а лише допомагають службі безпеки виявити факт порушення правил обігу із секретною інформацією.

В той же час зараз вже багато систем уміють збирати, зберігати й категорувати події ІБ, виявляти критичні інциденти, повідомляти про них усіх необхідних осіб, надають зручний інструмент збору додаткової інформації й розслідування інцидентів (тому числі і кіберінцидентів), дозволяють будувати різні звіти (по конкретній події, по конкретному працівникові або групі працівників) надавати зведену інформацію про всі інциденти й багато чого іншого [1,2,4]. Але ще недостатньо зроблено з повною автоматизацією цих процесів. Окремо варто відзначити, що сучасні системи DLP вже можуть зберігати архіви всіх переданих повідомлень, що дозволяє проводити більш результативні розслідування й будувати кореляції між різними подіями безпеки.

Слід ще відзначити, що єдиної методики розслідування інцидентів не існує, кожна організація повинна пристосовувати під себе загальні рекомендації в цьому питанні. Тому що процес виявлення й реагування залежить від багатьох факторів, наприклад, від загальної культури й політики ІБ у організації, ролі й місця підрозділу ІБ у системі безпеки організації, найменування, версії й настроювань використовуваної системи DLP, припустимого рівня ризиків, критичності оброблюваної інформації й багато чого іншого.

Однак, проаналізувавши багато «кращі практики» по побудові процесу управління інцидентами (наприклад, ДСТУ ISO/IEC 27002:2015 [1,3], ДСТУ ISO/IEC 27035:2018 [4], NIST SP 800-61 Rev. 2 процеси, що відповідають іншим стандартам - в ITIL і COBIT5), пропонується орієнтуватися на наступну послідовність кроків при роботі із системою DLP:

1. Виявлення й реєстрація подій ІБ.

2. Категорування подій, збір додаткової інформації й виявлення інцидентів ІБ.
3. Оперативне реагування на інцидент (запобігання або усунення наслідків інциденту).
4. Розбір (розслідування) інциденту ІБ.
5. Реагування на інцидент (дисциплінарні стягнення, карне переслідування порушників, управлінські рішення й інше),
6. Аналіз причин інциденту й «отриманих уроків», підготовка рекомендацій з підвищення загального рівня ІБ (при необхідності).

Таким чином, в сучасних умовах розвиток інформаційних технологій дозволяє охоплювати усе більше каналів цифрових комунікацій співробітників і зберігати значні масиви інформації, що значно розширює можливості розслідування порушень, пошуку непрямих ознак шахрайства, виявлення закономірностей і аномалій.

Зворотною стороною цих можливостей стає збільшення потоку подій ІБ (в тому числі і кіберінцидентів), що вимагають додаткової уваги фахівців з безпеки, тому сучасні DLP повинні мати розвинені засоби автоматизації управління життєвим циклом інциденту (для скорочення працезатрат), елементи кейс-менеджменту, інструменти пошуку й аналізу інформації на достатньому рівні для проведення поглибленого і якісного розслідування інцидентів (в тому числі і кіберінцидентів) безпеки .

Перелік посилань:

1. Гладиш С. В. Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в ор ганізаційно-технічних системах / Реєстрація, зберігання і обробка даних.- Одеса: Одеська національна академія зв'язку, 2008-С.116-19.
2. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с.
3. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки
4. ДСТУ ISO/IEC 27035-1:2018 (ISO/IEC 27035-1:2016, IDT) Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки.

Мужанова Т.М., к.держ.упр, доцент, доцент кафедри управління інформаційною та кібернетичною безпекою ННІЗІ ДУТ, м.Київ
Легомінова С.В., д.е.н., професор, завідувач кафедри управління інформаційною та кібернетичною безпекою ННІЗІ ДУТ, м.Київ

КОНЦЕПЦІЯ МЕРЕЖЕВОЇ БЕЗПЕКИ CISCO

Встановлено, що відповідно до концепції CISCO для захисту основної мережевої інфраструктури доцільно забезпечувати кілька рівнів захисту по периметру та всередині мережі, кожен з яких реалізує політики й заходи управління безпекою. У рамках забезпечення мережевої безпеки доцільно використовувати комплекс різноманітних засобів і заходів, зокрема брандмауери, мережі VPN, системи IPS, DLP, UBA/UEBA і SIEM, засоби управління доступом, сегментації мережі, безпеки робочих навантажень, антивірусне ПЗ, інструменти захисту додатків, електронної пошти і мобільних пристроїв, а також рішення з безпеки використання Інтернет, хмарних обчислень і бездротових мереж.
Ключові слова: мережева безпека, концепція мережевої безпеки CISCO.

Як свідчать реалії, ландшафт кібербезпеки постійно змінюється, а за останні кілька років змінилися підходи до розуміння ризиків кібербезпеки та з'явилися

нові типи кіберзагроз.

Це викликано насамперед впливом пандемії COVID-19, внаслідок чого суттєво зріс відсоток віддаленої зайнятості: у 2022 році понад третини працівників по всьому світу працювали віддалено. З огляду на такі зміни зросла кількість пристроїв, які використовуються для дистанційної роботи, а, отже, потребують захисту. Крім цього значно зросла кількість кібератак: 61% організацій стали жертвами кібернападів, число яких з початку пандемії COVID-19 збільшилося на чверть і більше.

Аналітики загроз CISCO виявили, що окрім збільшення обсягу, нові кібератаки також демонструють підвищену складність, частіше мають кілька етапів, що наражає компанії на різні види ризиків. На сьогодні найбільшу загрозу становлять фішингові атаки, несанкціонований криптомайнінг, програми-вимагачі, використання зловмисного ПЗ для крадіжки інформації [1].

З огляду на еволюцію найпопулярніших кібератак, які становлять реальну загрозу для мереж компанії, перед сучасними командами безпеки стоїть завдання пошуку надійних і ефективних рішень кібербезпеки.

На думку фахівців CISCO, для захисту основної мережевої інфраструктури від несанкціонованого доступу, неправомірного використання або крадіжки інформації має бути створена інфраструктура для безпечної роботи пристроїв, програм, користувачів і програм. Безпека мережі має забезпечувати кілька рівнів захисту по периметру та всередині мережі, кожен з яких реалізує політики й заходи управління безпекою. Відповідно до бачення CISCO, у рамках мережевої безпеки використовують комплекс різноманітних засобів і заходів (Рис.1).

Брандмауер виконує функції відстеження вхідного й вихідного мережевого трафіку та вирішує, дозволяти чи блокувати певний трафік на основі визначеного набору правил безпеки.

Віртуальна приватна мережа (VPN) створює приватне мережеве підключення між пристроями за допомогою Інтернету. Мережі VPN використовуються для безпечної й анонімної передачі даних у публічних мережах.

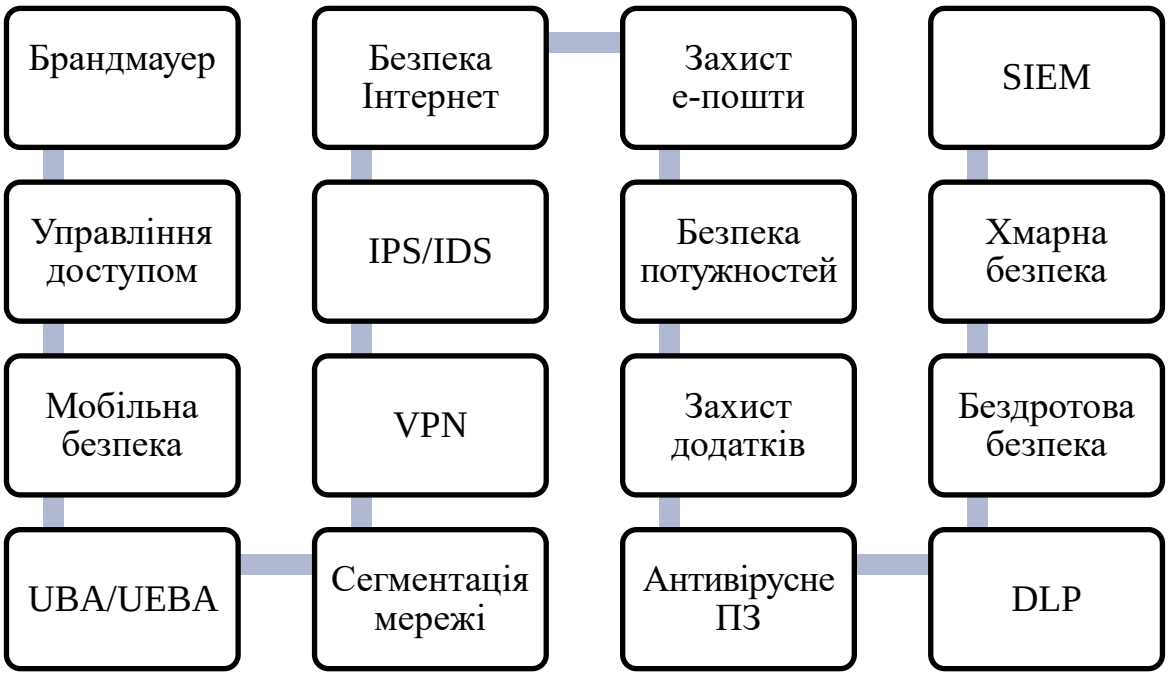


Рис. 1. Засоби й заходи мережевої безпеки CISCO

Система запобігання вторгненням (IPS) сканує мережевий трафік, щоб активно блокувати атаки. Пристрої IPS роблять це шляхом кореляції величезних обсягів глобальної інформації про загрози, щоб не тільки блокувати зловмисну діяльність, але й відстежувати розвиток підозрілих файлів і зловмисного ПЗ в мережі з метою запобігання спалахам і повторному зараженню.

Безпека робочих навантажень передбачає захист робочих навантажень, які переміщуються між різними хмарними та гібридними середовищами, а, отже, мають більші поверхні атаки, які мають бути захищені, щоб не шкодити гнучкості бізнесу.

Сегментація мережі розміщує мережевий трафік у різні сегменти та полегшує застосування політик безпеки. Організація може призначати права доступу на основі ролі, локації тощо, щоб певний рівень доступу надавався відповідним особам, а підозрілі пристрої локалізувалися та виправлялися.

Управління доступом необхідне для того, щоб уникнути потенційних зловмисників шляхом розпізнавання кожного користувача та кожного пристрою. Організація може заблокувати несумісні кінцеві пристрої або надати їм лише обмежений доступ. Цей процес є контролем доступу до мережі (NAC).

Антивірусний захист має не тільки сканувати на наявність зловмисного ПЗ під час входу, але й постійно відстежувати файли, щоб знайти аномалії, видалити зловмисне ПЗ й усунути пошкодження.

Безпека додатків охоплює апаратне і програмне забезпечення, а також процеси, які використовуються для того, щоб закрити вразливості, які зловмисники можуть використати для проникнення у мережу.

Поведінкова аналітика. Системи UBA/UEBA є інструментом виявлення аномальної поведінки користувачів та IT-об’єктів у мережі, що дозволяє встановити випадки перевищення привілеїв, крадіжки даних, зловмисної поведінки, компрометації облікових даних тощо і швидко усувати загрози.

Хмарна безпека включає широкий набір технологій, політик і програм, які застосовуються для захисту онлайн-IP, служб, програм та інших важливих даних. Це допомагає організації краще захищати користувачів, корпоративні дані та програми в хмарі.

Запобігання втраті даних. DLP-системи виявляють і запобігають витоку даних, викраденню або небажаному знищенню конфіденційних даних. DLP перешкоджають працівникам компанії завантажувати, пересилати чи навіть друкувати критичну інформацію небезпечним способом.

Безпека електронної пошти. Програма захисту електронної пошти блокує вхідні атаки й контролює вихідні повідомлення, щоб перешкодити зловмисникам обманним шляхом виманити у працівників конфіденційні дані компанії й запобігти їх втраті.

Безпека мобільних пристроїв має на меті забезпечити контроль над усіма пристроями, які мають доступ до корпоративної мережі, налаштувати безпечне з'єднання, щоб зберегти конфіденційність мережевого трафіку.

Управління інформацією і подіями безпеки. Рішення SIEM поєднують функції агрегації й кореляції даних безпеки, оповіщення про виявлені проблеми, формування звітів для зібраних даних, їх зберігання і застосування з метою управління безпекою та проведення аудиту.

Веб-безпека контролює використання Інтернету персоналом організації, блокує веб-загрози і забороняє доступ до шкідливих веб-сайтів, захищаючи таким чином корпоративний веб-шлюз на сайті або в хмарі. Також рішення веб-безпеки забезпечують захист веб-сайту компанії.

Бездротова безпека. З огляду на те, що бездротові мережі не такі безпечні, як дротові, вони потребують застосування суворіших заходів безпеки. Щоб запобігти поширенню експлойтів, використовують продукти, спеціально розроблені для захисту бездротової мережі.

Отже, в умовах поширення віддаленої роботи, стрімкого зростання кількості кіберзагроз та їхнього постійного ускладнення експерти CISCO рекомендують для захисту основної мережевої інфраструктури від несанкціонованого доступу, неправомірного використання або крадіжки забезпечувати кілька рівнів захисту по периметру та всередині мережі, кожен з яких реалізує політики й заходи управління безпекою.

У рамках забезпечення мережевої безпеки доцільно використовувати комплекс різноманітних засобів і заходів, зокрема брандмауери, мережі VPN, системи IPS, UBA/UEBA, DLP і SIEM, засоби управління доступом, сегментації мережі, забезпечення безпеки робочих навантажень, антивірусне ПЗ, інструменти захисту додатків, е-пошти і мобільних пристроїв, а також рішення з безпеки використання мережі Інтернет, хмарних обчислень і бездротових мереж.

Список використаних джерел

1. The Top Cybersecurity Threats in 2022. URL: https://umbrella.cisco.com/blog/top-cybersecurity-threats-2022
2. What Is Network Security? URL: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html
3. How Modern Security Teams Fight Today's Cyber Threats. URL: https://umbrella.cisco.com/info/ebook-how-modern-security-teams-fight-todays-cyber-threats

Калабухов Ілля Ігорович
студент групи БСД-41, ННІЗІ ДУТ, Київ, Україна

ТЕХНОЛОГІЇ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

Побудова безпечної корпоративної мережі потребує комплексного підходу, що включає реалізацію багаторівневої системи захисту, управління доступом, моніторинг активності користувачів та оновлення програмного забезпечення, що забезпечує надійний захист корпоративних даних від зовнішніх і внутрішніх загроз. Конструкція безпеки корпоративної мережі є ключовим елементом інфраструктури будь-якої компанії. Вона забезпечує необхідний зв'язок між різними співробітниками, відділами та офісами, забезпечує швидкий обмін інформацією та покращує продуктивність усієї компанії в цілому.

Мережва безпка є головною проблемою при побудові корпоративної мережі. Незважаючи на всі переваги, неправильно побудована або недостатньо захищена мережа може стати легкою здобиччю для хакерів, що призведе до витоку конфіденційних даних, втрати репутації та фінансових втрат.

Перш ніж розпочати побудову корпоративної мережі, компанія має розробити план безпеки. У ньому повинні бути вказані уразливості, які можуть бути використані хакерами, а також описані всі можливі загрози, пов'язані з безпекою. У цьому випадку можна розробити відповідні заходи безпеки, які захистять корпоративну мережу від будь-яких загроз.

Види атак і основні вразливості корпоративних мереж

Корпоративна мережа, як і будь-яка інша мережа, схильна до багатьох загроз безпеці. У своїй основі методи зловмисників залишилися практично незмінними і спрямовані на наступні уразливості:

- Віруси та інше шкідливе програмне забезпечення;
- Фішинг;
- DDoS;
- Порушення доступу;
- Несанкціоноване використання ресурсів;
- Недоліки безпеки пристроїв;
- Порушення політики безпеки.

Якщо при побудові корпоративної мережі не було виявлено вразливостей, це не означає, що мережа повністю захищена від можливих атак. Нові вразливості можуть з'являтися у будь-який момент часу, і якщо не відбувається постійний моніторинг мережі, то компанія може виявитися вразливою до нових видів атак.

Тому важливо розуміти, що забезпечення безпеки корпоративної мережі – це безперервний процес, який потребує постійного моніторингу та аналізу вразливостей. Це включає регулярне оновлення програмного забезпечення та операційних систем на всіх пристроях, які підключені до мережі, використання сучасних методів захисту від атак, моніторинг мережевого трафіку.

Крім того, важливо навчати персонал компанії основ кібербезпеки, щоб знизити ризик виникнення загроз зсередини. Співробітники повинні знати, які дії можуть призвести до порушення безпеки мережі, які паролі використовувати та як їх зберігати, як виявити атаки фішинга тощо.

В ідеалі, забезпечення безпеки корпоративної мережі має бути інтегроване в культуру компанії та бути настільки важливим, що кожен співробітник розуміє свою роль у захисті мережі. Якщо компанія постійно працює над удосконаленням своєї стратегії безпеки, це допоможе мінімізувати ризики виникнення загроз і забезпечити надійний захист корпоративної мережі.

Тестування мереж на вразливості є важливою частиною стратегії безпеки корпоративної мережі. Цей процес дозволяє виявити слабкі місця в мережі та вжити заходів щодо їх усунення.

Penetration Testing

Існують різні методи тестування мереж на вразливості, які можуть використовуватись компаніями для забезпечення безпеки своїх мережевих ресурсів. Це може включати сканування портів, тестування на проникнення та інші методи.

Сканування портів дозволяє виявити відкриті порти на пристроях, підключених до мережі. Це може допомогти виявити несанкціоновані послуги або служби, які можуть бути використані зловмисниками для атаки на мережу.

Тестування на проникнення полягає у спробі імітувати атаку на мережу та виявити вразливості, які можуть бути використані зловмисниками. Це дозволяє оцінити рівень безпеки мережі та виявити слабкі місця, які потребують додаткового захисту.

Однак важливо розуміти, що тестування на вразливості не є єдиним способом забезпечення безпеки корпоративної мережі. Це лише один із багатьох інструментів, які можуть бути використані у рамках комплексної стратегії забезпечення безпеки.

Крім того, при проведенні тестування на вразливості необхідно дотримуватись етичних та законних принципів. Не можна використовувати цей інструмент для незаконного отримання доступу до чужої мережі або порушення будь-яких прав. Важливо проводити тестування лише з дозволу власника мережі та дотримуватись усіх відповідних норм та правил, щоб запобігти будь-яким негативним наслідкам.

Шляхи забезпчення захисту корпоративної мрежі

Існує безліч шляхів захисту корпоративних мереж від кіберзагроз, і найефективніша стратегія захисту має містити кілька рівнів. Ось деякі з них:

- Захист периметра: Це перший рівень захисту, який обмежує доступ до корпоративної мережі із зовнішнього середовища. Цей рівень включає

використання брандмауера, аутентифікації користувачів, VPN-підключень, контролю доступу.

- Захист програм і даних: Цей рівень включає захист програм і даних всередині мережі. Для цього використовуються різні методи, такі як шифрування, контроль доступу, моніторинг трафіку та виявлення вторгнень.
- Управління вразливістю: Цей рівень включає постійний моніторинг мережі та пошук вразливостей, які можуть бути використані зловмисниками для атаки на мережу. Цей процес включає регулярне оновлення програмного забезпечення та операційних систем на всіх пристроях в мережі, а також тестування мережі на вразливості.
- Навчання персоналу: Співробітники компанії можуть бути слабкою ланкою в ланцюжку безпеки, тому навчання персоналу основам кібербезпеки є важливим кроком у захисті корпоративної мережі. Це включає організацію тренінгів і навчання співробітників тому, як убезпечити свої паролі та дані, як виявити фішингові атаки.
- Моніторинг та аналіз: Постійний моніторинг мережі та аналіз мережевого трафіку можуть допомогти у швидкому виявленні та реагуванні на кібератаки. Використання спеціалізованого програмного забезпечення для моніторингу мережної активності, аналізу подій та виявлення вторгнень може значно покращити безпеку корпоративної мережі.

Комплексне застосування цих та інших заходів захисту може суттєво підвищити безпеку корпоративної мережі. Крім того, важливо регулярно проводити аудит та перевірку мережі на наявність нових вразливостей, щоб зберігати високий рівень захисту протягом часу.

Однак не варто забувати, що захист корпоративної мережі – це безперервний процес, і кіберзагрози можуть з'являтися щодня у нових формах та варіантах. Тому важливо мати гнучку та адаптивну систему захисту, яка може швидко реагувати на нові загрози та вживати відповідних заходів для їх запобігання.

Загалом, захист корпоративної мережі є складним та багатогранним процесом, який потребує постійної уваги та зусиль з боку адміністраторів та співробітників компанії. Однак, за умови правильного підходу, це може значно знизити ймовірність успішної кібератаки на корпоративну мережу та забезпечити високий рівень безпеки даних та інформації компанії.

Перелік посилань:

1. Як забезпечити захист корпоративної мережі: поширені помилки компаній та рекомендації, як їх уникнути [Електронний ресурс] — https://eset.ua/ua/blog/view/40/kak-obespechit-zashchitu-korporativnoy-seti-rasprostranennyye-oshibki-kompaniy-i-rekomendatsii-kak-ikh-izbezhat.
2. 11 рішень SASE для захисту корпоративних мереж для малого та середнього бізнесу [Електронний ресурс] — https://techukraine.net/

Кондратенко Іван Сергійович,
студент групи БСД-31, ННІЗІ ДУТ, Київ, Україна

СУТНІСТЬ ХХЕ АТАКИ ЇЇ НАСЛІДКІВ ТА ЯК ЦЬОМУ ЗАПОБІГТИ

XXE (XML External Entity) атака - це тип атаки на веб-додатки, що дає змогу зловмиснику виконати довільний код на сервері, використовуючи XML-обробник веб-додатка. XXE атака становить серйозні ризики для безпеки системи, оскільки вона може призвести до виконання довільного коду на сервері та отримання несанкціонованого доступу до конфіденційної інформації.

Стандарт XML передбачає можливість використання DTD (document type definition). DTD дає можливість визначати та використовувати XML-сутності. Сутності можуть як посилатися на якийсь зовнішній ресурс, так і бути повністю визначені всередині документа. В останньому випадку вони можуть бути представлені якимось рядком або, наприклад, іншими сутностями.
Принцип роботи атаки полягає в тому, що зловмисник вводить у поле введення веб-форми спеціально сформований XML-документ, що містить посилання на зовнішні сутності (external entities). Під час обробки документа XML-обробник веб-додатка завантажує ці зовнішні сутності, що може призвести до виконання довільного коду на сервері.[1]
За подібним принципом, шляхом збільшення кількості вкладених сутностей, створюються так звані XML-бомби. Вони являють собою невеликі за розміром файли, які під час розкриття сутностей розростаються до величезних розмірів. Звідси ж походять різні назви такого типу атак: XEE (XML Entity Expansion); billion laughs (через багаторазове повторення 'lol'). Таким чином, DoS-атака на додаток із використанням XML-бомб можлива, якщо: зловмисник може передати додатку XML-бомбу; XML-парсер, який оброблятиме цей файл, має небезпечну конфігурацію. [2]
Для захисту від XXE атак необхідно:

1. Використовувати останні версії XML-обробників, які підтримують захист від XXE атак.
2. Обмежувати доступ до зовнішніх сутностей або відключати підтримку зовнішніх сутностей, якщо це можливо.
3. Фільтрувати дані, що вводяться користувачем, щоб унеможливити впровадження шкідливого коду.
4. Використовувати підпис XML-документів і перевірку цілісності даних.
5. Забезпечувати захист файлової системи сервера, щоб запобігти читанню або запису на нього з боку зловмисників.

У результаті XXE атаки зловмисник може:

1. Отримати доступ до файлів на сервері та виконати довільний код на стороні сервера, що може призвести до крадіжки конфіденційної інформації.
2. Відмовити в обслуговуванні (DoS-атака) серверу, використовуючи спеціально сформований XML-документ, що може призвести до недоступності програми для звичайних користувачів.

3. Здійснити атаку впровадження команд (Command Injection), використовуючи XXE атаку як один із векторів атаки.
4. Використовувати вразливість для обходу механізмів аутентифікації та авторизації.
5. Використовувати вразливість для проведення інших видів атак на сервер або на мережу, в якій він працює.

Тому необхідно вживати заходів для захисту від XXE атак, включно з використанням останніх версій XML-обробників і фільтрацією користувацького введення, щоб запобігти можливості впровадження шкідливого коду.

Для захисту від XXE атак необхідно:

1. Використовувати останні версії XML-обробників, які підтримують захист від XXE атак.
2. Обмежувати доступ до зовнішніх сутностей або відключати підтримку зовнішніх сутностей, якщо це можливо.
3. Фільтрувати дані, що вводяться користувачем, щоб унеможливити впровадження шкідливого коду.
4. Використовувати підпис XML-документів і перевірку цілісності даних.
5. Забезпечувати захист файлової системи сервера, щоб запобігти читанню або запису на нього з боку зловмисників.[3]

Перелік посилань:

1. XML external entity (XXE) injection

URL: https://portswigger.net/web-security/xxe

2. XXE: XML bomb

URL: https://habr.com/ru/articles/170333/

3. XXE: XML external entity

URL: https://habr.com/ru/companies/vds/articles/454614/