ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИУТУ ЗАХИСТУ ІНФОРМАЦІЇ

НАУКОВО-ПРАКТИЧНА ІНТЕРНЕТ-КОНФЕРЕНЦІЯ

«ЦИФРОВА ТРАНСФОРМАЦІЯ КІБЕРБЕЗПЕКИ»»

Тези доповідей

22 жовтня 2020

м. Київ

Зміст

ВИКОРИСТАННЯ СПЕЦІАЛІЗОВАНИХ ПЛАТФОРМ І РІШЕНЬ З БЕЗПЕКИ ІНФОРМАЦІЇ В СИСТЕМНОМУ АНАЛІЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЙ

Якименко Ю. М.
к. в. н., доцент кафедри управління інформаційною та кібернетичною безпекою
Державний університет телекомунікацій
м. Київ,Україна

Враховуючи сучасні можливості інформаційно-комунікаційних технологій та тенденції збільшення кількості загроз інформаційній та кібербезпеці, питання захисту інформації і використання методів її захисту набувають усе більшої актуальності. Ефективне використання новітніх досягнень в області інформаційних технологій (IT), програмних засобів підтримки інформаційно-аналітичної роботи та підготовки даних для прийняття рішень, з дотриманням правил та сучасних пристроїв від компаній-вендерів щодо забезпечення комп'ютерної безпеки дозволить забепечити високий рівень інформаційної безпеки будь-якої організації. Інформаційна аналітика формується як необхідна компонента управління підприємницької діяльності, як інструмент сучасного менеджменту. Інформаційна аналітика постійно затребувана як необхідний інструмент ефективної діяльності організації і цілком органічно вписується в її структуру, стаючи мозковим центром обгрунтування управлінських рішень і генератором появи новітних ідей в поліпшенні технологічних процесів .

До основних напрямів аналітичної роботи в сфері безпеки організації відносяться:

- аналіз інформаційного стану об'єктів захисту;
- аналіз інформаційних загроз;
- аналіз каналів несанкціонованого доступу до інформації;
- аналіз комплексної інформаційної безпеки і процесів її забезпечення;
- аналіз порушень режиму конфіденційності тощо;

- загальне обґрунтування прийнятого керівником рішення за результатами аналізу.

Серед інструментаріїв сучасних аналітичних служб організації, які виконують цей спектр робіт, є: Центри моніторингу, групи ситуаційного аналізу, засоби використання електронних ресурсів ЗМІ і Інтернету, неформальні джерела і соціологічні дані, засоби використання комп'ютерних технологій обробки інформаційних масивів даних і інтелектуалізованих режимів контекстного пошуку і т.п.

Робота аналітика інформаційної безпеки із аналітичних служб організації будується по отриманню кваліфікованого аналізу ситуації с захистом інформації і даних в реальному часі, по виявленню та пріоритизації загроз в сфері безпеки, прогнозу їх розвитку і прийняття рішень по їх недопущенню , аналізу виявлення аномальної поведінки користувачів і виробленню сценаріїв реагування на тактики, методи та процедури зловмисника.

Автоматизація управлінської праці аналітика інформаційної безпеки теж набуває усе більшої важливості.

Міжнародні компанії та провідні світові IT- виробникі, які займають лідируючі позиції в сфері поставок спеціалізованих комп'ютерних пристроїв, пропонують свою продукцію для реалізації, в тому числі і в процесах управління інформаційною та кібернетичною безпекою. Так, компанія FireEye (США), діє в Україні через офіційного дистриб'ютора, розробила спеціалізовані платформи і рішення безпеки, засновані на базі віртуальних машин, які забезпечують захист великих підприємств і державних установ від кібератак нового покоління та загроз нового покоління в режимі реального часу. Платформа безпеки FireEye гарантує забезпечити аналітиків інформаційної безпеки надійним інструментом для виявлення, аналізу та розслідування інцидентів в найкоротші терміни в порівнянні з традиційними підходами.

Такими спеціалізованими пристроями в сфері безпеки від компанії FireEye [1], після застосування методичних підходів і методів системного аналізу, є:

- **Системи для захисту файлової системи:**

FireEye FX – захист від загроз нового покоління знаходяться в файловій системі, це платформа для захисту від тематичних атак, що поширюються через файли різного формату, аналізує вміст мережевих файлових сховищ з метою виявлення і подальшого карантину загроз, які могли бути занесені вручну, за допомогою Web або поштою, тим самим перешкоджаючи їх подальшому поширенню; перешкоджає поширенню просунутих загроз, які пропускають традиційні засоби інформаційної безпеки, такі як NG Firewall, IPS, антивіруси і шлюзи.

- **Система аналізу загроз:**

FireEye AX - детальний аналіз загроз нового покоління, це платформа для повноцінного аналізу загроз і розслідування взаємозв'язку змішаних атак, це унікальна платформа для захисту бізнесу, що надає повноцінний аналіз загроз і розслідування взаємозв'язку змішаних атак та дає аналітикам безпеки контроль над потужним настроюваним тестової середовищем, де абсолютно безпечно можна виконати і досліджувати загрози нового покоління.

- **Системи для захисту інтернет трафіку:**

FireEye NX – захист від загроз нового покоління, які надходять по Web, це рішення по боротьбі з загрозами нового покоління.

FireEye EX – це захист від загроз нового покоління, які надходять по електронній пошті, це рішення для захисту організації від спрямованих фішинг поштових атак, які обходять традиційні репутаційні та антиспам технології.

- **Централізоване управління системою безпеки:**

FireEye CM – система централізованого управління, це платформа централізованого управління всіма рішеннями FireEye EX, FX, NX, AX, яка дозволяє об'єднати управління, звітність та поширення інформації про загрози.

- **Безпека кінцевих точок:**

FireEye HX – захист робочих станцій від сучасних кіберзагроз, це рішення, яке дозволяє швидко і точно приймати рішення щодо події безпеки на

кінцевій станції, та об'єднати активності, які виробляються на рівні мережі і на рівні робочих станцій, і дозволяє скоротити часові витрати на відновлення в зв'язку з інцидентом безпеки. FireEye HX використовує «індикатори ризику» (IOC) отримані з інших платформ FireEye (NX, EX, FX, AX) для оперативного підтвердження того, що кінцева станція була схильна до атаки.

FireEye Endpoint - це унікальне комплексне рішення по захисту кінцевих точок, Версія FireEye Endpoint 4.0 доступна з 28 вересня 2017 року і може працювати в хмарі, on-premise, віртуальної або гібридної інфраструктурі.

- **Безпека мобільних пристроїв:**

FireEye Mobile Threat Prevention - захист від шкідливих мобільних додатків**,** виявляє і зупиняє мобільні загрози.

Таким чином, розглянуті спеціалізовані пристрої в сфері безпеки від компанії FireEye, які забезпечують системний захист від загроз на різних етапах їх життєвого циклу в режимі реального часу, можуть бути реалізовані в роботі аналітичних служб будь-якої організації для підвищення своєї інформаційної безпеки.

Література:

1. *FireEye HX – защита рабочих станций от современных киберугроз. URL: https://bakotech.ua/product/200/.*

МАТЕМАТИЧНА МОДЕЛЬ ЗАХИСТУ ВІД ІНФОРМАЦІЙНОЇ АТАКИ

Касовська Ірина Валеріївна
студентка 4 курсу, групи БСД-44
(063)033 43 17
irakrasovakaja@gmail.com
Науковий керівник: Савченко Віталій Анатолійович
директор інституту захисту інформації
Державний університет телекомунікацій
м. Київ,Україна

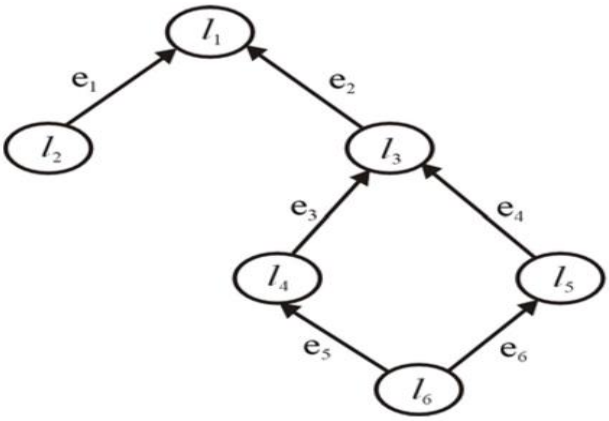
Математична модель інформаційної атаки базується на наступних трьох основних множинах: *V* - безліч вразливостей АС, *A* - безліч методів реалізації

атак і C - безліч наслідків атак. Для опису взаємозв'язку між елементами множин A, V і C визначено тернарне відношення W на безлічі $U = A \times V \times C$. Належність елемента (a, v, c) відношенню W, де $a \in A, v \in V, c \in C$, інтерпретується наступним чином: «Інформаційна атака, що реалізується порушником методом a шляхом активізації уразливості v, і яка веде до наслідку c».

Створена математична модель атаки представлена у вигляді графа $G = (L, E)$, де L - безліч вершин графа, а $E \subset L^2$- безліч дуг графа. Для графа G визначено відношення $T \in \{E \times W\}$, яке кожній дузі з безлічі E ставить в відповідність один або більше елементів відносини W. Використання відносини T дозволяє інтерпретувати кожну дугу графа G як один з етапів моделюється інформаційної атаки. При цьому відносно T однієї дузі $e \in E$ може відповідати одночасно кілька елементів безлічі W тільки за умови, що ці елементи позначають атаки, що призводять до одних і тих самих наслідків. У кожну вершину графа G може входити одночасно кілька дуг тільки за умови, що стосовно Т кожної такої дузі відповідають елементи безлічі W, що описують атаки, які призводять до однакових наслідків. Таким чином, вершини графа G може об'єднувати різні етапи атаки, що призводять до ідентичним наслідків. На Рис. 1 показаний приклад графа G, що описує довільну інформаційну атаку, а також ставлення T, яке визначає етапи атаки, що моделюються за допомогою дуг графа G.

Граф G, зображений на Рис. 1, являє собою модель інформаційної атаки, успішна реалізація якої призводить до наслідку $c_1 \in C$. Структура графа G дозволяє визначити всі можливі сценарії дій порушника в моделюючій атаці. Формально сценарії проведення атаки представлені безліччю можливих шляхів в графі G - Gp, де кожен шлях $gp \in Gp$ являє собою послідовність дуг $(e_{p_1}, e_{p_2}, \dots, e_{p_n})$ вигляду $e_{p_k} = (l_i, l_j), l_i, l_j \in L$, при цьому кінцева вершина дуги e_{p_k} одночасно є початковою вершиною дуги $e_{p_{k+1}}$. В якості початкової вершини шляху можуть виступати такі вершини $l \in L$ графа G, полустепені

заходу яких дорівнює 0. Кінцевою ж вершиною шляху може бути тільки така вершина l, полустепені результату якої дорівнює 0.



$$T = \{(e_1,(a_1, v_2, c_1)),\ (e_2,(a_2, v_2, c_1)),\ (e_3,(a_1, v_3, c_4)),\ (e_4,(a_3, v_3, c_4)),\ (e_5,(a_2, v_4, c_2)),\ (e_6,(a_2, v_5, c_3))\ \}$$

Рис. 1 - Приклад зваженого графа G, що описує довільну атаку

Безліч шляхів Gp для графа, зображеного на Рис. 1, має такий вигляд: $Gp = \{\{(l_2, l_1)\}, \{(l_6, l_4), (l_4, l_3), (l_3, l_1)\}, \{(l_6, l_5), (l_5, l_3), (l_3, l_1)\}\}$. Таким чином, до наслідків $c_1 \in C$ може привести один з трьох наступних сценаріїв реалізації атаки:

1) Реалізація атаки методом $a_1 \in A$, активізує вразливість $v_1 \in V$, що призводить до наслідку $c_1 \in C$ $(gp_1 = (e_1), (e_1, (a_1, v_2, c_1)) \in T)$;

2) Реалізація атак за допомогою методів $a_2, a_1, a_2 \in A$, які активізують уразливості $v_3, v_4, v_2 \in V$, і призводять до наслідків $c_2, c_1, c_4 \in C$, відповідно $(gp_2 = (e_5, e_3, e_2), \{(e_5, (a_2, v_4, c_2)), (e_3, (a_1, v_3, c_4)), (e_2, (a_2, v_2, c_1))\} \in T)$;

3) реалізація атак за допомогою методів $a_2, a_3, a_2 \in A$, які активізують уразливості $v_3, v_5, v_2 \in V$, і призводять до наслідків $c_3, c_1, c_4 \in C$, відповідно $(gp_3 = (e_6, e_4, e_2), \{(e_6, (a_2, v_5, c_3)), (e_4, (a_3, v_3, c_4)), (e_2, (a_2, v_2, c_1))\} \in T)$.

Розроблена математична модель інформаційної атаки має властивість універсальності, оскільки може бути використана для представлення різних типів атак, і може розширюватись за рахунок можливості додавання нових параметрів в модель атаки. Модель передбачає можливість як текстового, так і графічного зображення у вигляді графа. Модель може бути представлена у формалізованому вигляді за допомогою математичного апарату теорії графів.

На відміну від існуючих моделей інформаційних атак вона характеризується многофакторностью, що дозволяє враховувати три основних параметра атаки - вразливість, метод реалізації атаки і її можливі наслідки. Наявність всіх цих властивостей дозволяє зробити висновок про те, що використання розробленої моделі дозволяє більш продуктивно досліджувати особливості модельованих інформаційних атак і, отже, більш ефективно вибирати засоби захисту від цих атак.

Висновок: створена поведінкова модель процесу виявлення атак, на відміну від наявних, дозволяє виявляти як відомі, так і нові атаки, функціонуючи при цьому в режимі «білого ящика» і забезпечуючи можливість повністю простежувати процес прийняття рішення про виявленні атаки в АС. Розроблена модель може бути задана в формалізованому вигляді на основі апарату теорії графів. Модель виявлення атак розширювана, що дає можливість додавати нові параметри, необхідні для виявлення інформаційних атак.

Література:

1. *Сердюк В.А. Аналіз сучасних тенденцій побудови моделей інформаційних атак. //Інформаційні технології. 2004. №5. с. 20-26.*
2. *Баранова, Є.К. Методики та програмне забезпечення для оцінки ризиків у сфері інформаційної безпеки / Є.К. Баранова // Управління ризиком. - 2009. - № 1 (49). - С. 15-26.*
3. *Губарєва, О.Ю. Статистичний аналіз вразливостей інформаційної безпеки інформаційних систем / О.Ю. Губарєва, В.В. Пугин // Проблеми техніки і технологій телекомунікацій: Збірник праць XVI Міжнародній науково-технічній конференції - Уфа, 2015. - Т. 3. - С. 175-177.*

МЕТОД БЛОКУВАННЯ КАНАЛІВ АКТИВНИХ РАДІОЗАКЛАДНИХ ПРИСТРОЇВ З ШИРОТНО-ІМПУЛЬСНОЮ МОДУЛЯЦІЄЮ НЕСІЙНОГО СИГНАЛУ

Крючкова Л.П., Вовк М. О.,
аспірант АКБ-125,
Державний університет телекомунікацій
м. Київ, Україна

Одним з найбільш поширених технічних засобів, що використовуються для перехоплення конфіденційної інформації, є радіозакладні пристрої, які використовують радіоканал як середовище передачі небезпечних сигналів. Виявлення і вилучення цих пристроїв являє собою окрему і складну задачу в системі заходів щодо захисту інформації. В доповіді розглядається метод блокування технічних каналів витоку мовленнєвої інформації, утворюваних радіозакладними пристроями, розташованими на об'єктах інформаційної діяльності. Наводяться результати моделювання, спрямовані на визначення параметрів захисних сигналів, здатних забезпечити руйнування активних сигналів радіозакладних пристроїв. Сформульовано базові рекомендації, щодо виключення можливостей перехоплення інформації каналами радіозакладних пристроїв.

У сучасному світі в умовах інформатизації та швидкого зростання можливостей технічних засобів у сфері радіоелектроніки, відкривається можливість отримання доступу до конфіденційної інформації, шляхом впровадження широкого спектру радіопристроїв.

За статистикою переважна більшість інформації перехоплюється шляхом впровадження радіозакладних пристроїв (РЗП), виконаних у вигляді, як технічних модулів та закамуфльовані під технічні елементи пристрою, елементи одягу, побутові предмети тощо.

Передача інформації такими пристроями може здійснюватися [1]:

- в режимі реального часу;

- з накопиченням інформації;

- за дистанційним керуючим сигналом.

Мета наших досліджень полягала у знаходженні параметрів захисних сигналів, здатних забезпечити максимально можливу руйнацію інформативних параметрів небезпечного сигналу, і, як результат, створення протидії перехопленню конфіденційної інформації зацікавленими особами.

Для виконання досліджень використовувались методи математичного та імітаційного моделювання. В результаті теоретично розраховано та методами імітаційного моделювання практично визначено максимально ефективні параметри захисних сигналів, які в перспективі можна використовувати в системах автоматичної радіопротидії небезпечним сигналам різноманітного походження.

Сутність запропонованого методу полягає в застосуванні комбінованої активної завади (захисного сигналу), спрямованої на руйнування інформативних параметрів небезпечного сигналу радіозакладного пристрою [2].

Засобами радіомоніторингу визначається несійна частота РЗП (небезпечний сигнал). Після виявлення несійної (рис. 1, а) або несійних небезпечного сигналу для активної протидії використання створеного зловмисником каналу витоку інформації формуються захисні сигнали за наступними критеріями:

- перший сигнал – несійний сигнал, з частотою, віддаленою на 10% від частоти небезпечного сигналу (рис. 1, б). В результаті впливу першого захисного сигналу на небезпечний сигнал з’являється ефект биття (рис. 1, д)

- другий сигнал – сигнал коливальної частоти в межах від 5% до 20% частоти небезпечного сигналу (рис. 1, в).

В результаті комбінований вплив на небезпечний сигнал призводить до ефективної руйнації інформації, що передається сигналом РЗП (рис. 1, г).

Нами проведено дослідження щодо блокування запропонованим методом аналогових сигналів радіозакладних пристроїв з різними видами модуляції несійної частоти. Спираючись на результати досліджень, визначено параметри захисних сигналів, спрямованих на блокування сигналів радіозакладних пристроїв з широтно-імпульсною маніпуляцією несійної частоти.

В доповіді наводяться результати математичних розрахунків, виконаних з використанням мови програмування Python та імітаційного моделювання

впливу прицільних завадових сигналів на інформативні параметри небезпечних сигналів з використанням пакету LabVIEW версії 20.0.1.

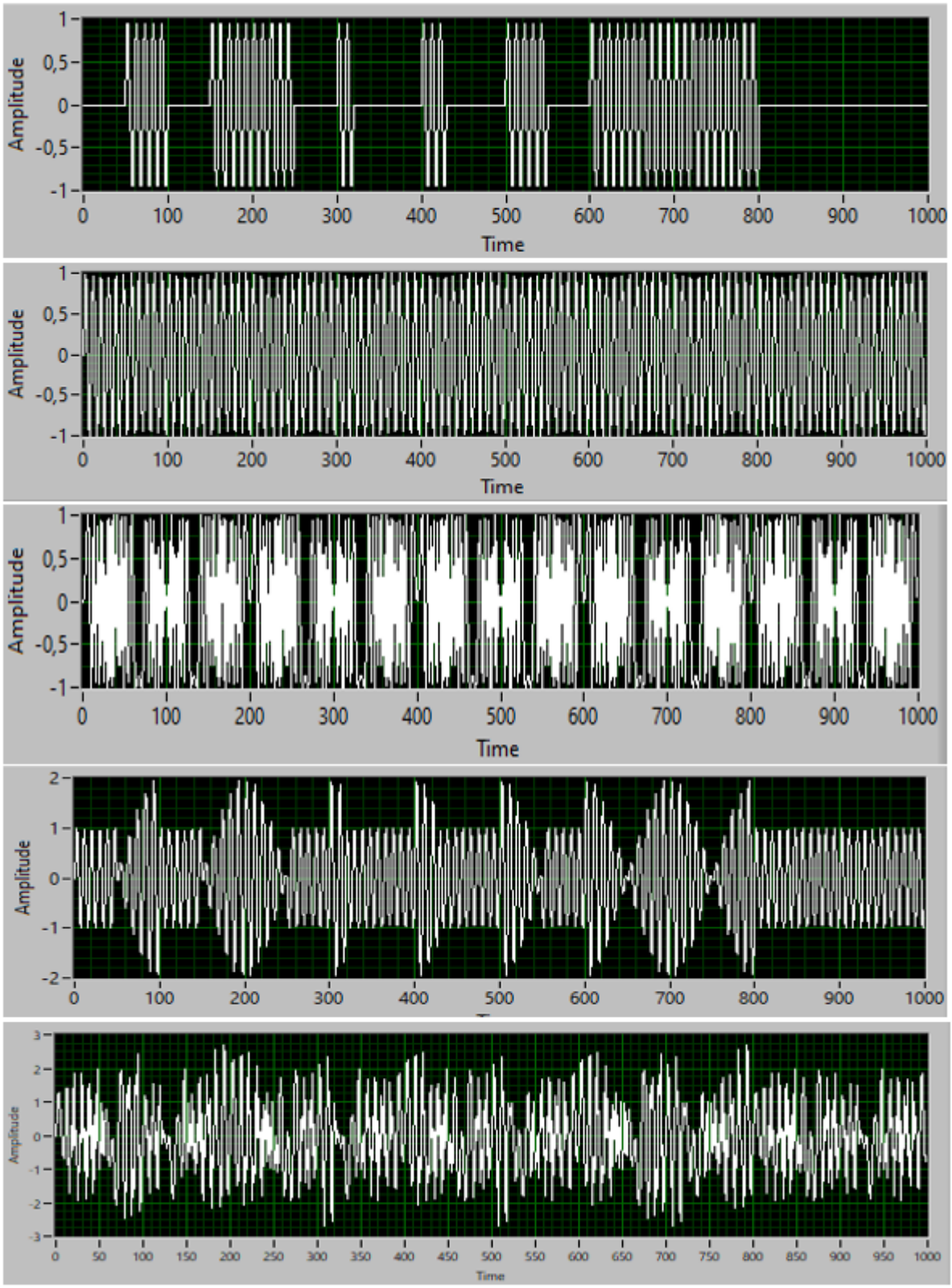


Рис. 1 . Зображення сигналів:
а) – небезпечний сигнал, б) – перший захисний сигнал, в) – сигнал коливальної частоти, г) – биття небезпечного та першого захисного сигналів, д) – результуючий небезпечний сигнал

В перспективі планується проведення досліджень з метою визначення параметрів захисних сигналів, які забезпечують блокування інших цифрових сигналів РЗП.

Література:

1. *Про критичну інфраструктуру та її захист. Проект закону України від 27.05.2019 №10328. [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/JH7YW00A.html*
2. *Ленков С.В., Рибальський О.В., Хорошко В.А., Крючкова Л.П. Принципы блокирования съема информации способами ВЧ-навязывания // Вісник Київського національного університету ім. Тараса Шевченка. Військово-спеціальні науки. К., Вип.22, 2009. – С.36 – 39.*

ROLE OF THREAT INTELLIGENCE IN CYBERSECURITY

Pavlo Pysarenko
Student at State University of Telecommunication

The increasing number of cyberattacks happening in cyberspace requires cybersecurity professionals to indicate, analyze and defend against the cyber threats in nearly real-time. In reality, timely coping with such a large quantity of attacks is practically impossible without deeply perusing the attack features and taking corresponding intelligent defensive actions — this defines the cyber threat intelligence notion. Nevertheless, such an intelligence would be impossible without the aid of machine learning and artificial intelligence techniques to gather, process, and interpret cyberattack evidence. This thesis aims to discuss the notion of cyber threat intelligence and its main challenges and opportunities.

Keywords: Cyber threat intelligence, Indicators of attack, Indicators of compromise, Artificial intelligence.

Ensuring the security and privacy of the individuals' and organizations' information is one of the most difficult issues to solve nowadays, as we live in a period of intense digital transformation of information technology. What makes it much more challenging for security analysts and forensic specialists to detect cyberattacks and protect against them is the recent drastic increase in their samples' quantity and variety.

The notion of "Therat Intelligence" was introduced in order to cope with this very problem. Threat Intelligence refers to "the set of data collected, assessed and applied regarding security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators". In fact, Cyber threat Intelligence (CTI) emerged in order to

help security practitioners in recognizing the indicators of cyberattacks, extracting information about the attack methods, and consequently responding to the attack accurately and in a timely manner.

Providing such an important challenge would be challenging. When large volume of data is collected from or generated by various security monitoring solutions, intelligent analytical methods related to big data are necessary to mine and extract new knowledge out of the gathered data. In this respect, several concerns come along and introduce new challenges to the filed.[1]

Thereby, cyberspace can be defined as an environment created and maintained for the purpose of facilitating data exploitation, human interaction and general communications. [2]

From a professional's perspective, intelligence is data that has been processed logically in an analytical way, which is most often a human-based process that evaluates the data in context and produces a usable output. In rare cases, there are options for that process to be entirely machine driven if the outcome allows an action, change in security or defensive posture, or decision that was not possible before the process. In any occasion, whether the data is transformed or distilled or otherwise turned into usable intelligence by a program or neurons, the output must meet at least the following three conditions to meet the definition of intelligence. The information must be:

1. Relevant: It must be relevant to the enterprise / industry / business objectives, or some other aspect of organizational life.

2. Actionable: The data must be concrete enough to either prompt, enable, or inform some response, action, decision, or change in security posture, configuration, level of sensitivity or other organizational network or human change to the environment; or provide sufficient information to support making an informed decision not to act.

3. Valuable: The information must have sufficient value, and at the organization (not department) level, value must translate to the business. [3]

Sources:

1. *Dehghantanha A. Cyber Threat Intelligence / A. Dehghantanha, C. Mauro, D. Tooska., 2018. – 334 c.*
2. *CBEST Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations 2.0, 2016. – 48 c.*
3. *Dalziel H. How to Define and Build an Effective Cyber Threat Intelligence Capability / Henry Dalziel., 2015. – 32 c.*

Толкачова А.Ю
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ, Україна

В сучасному світі існує велика кількість загроз. Ми зустрічаємо їх на кожному кроці нашого життя. З часом технології прогресують і загрози також. З розвитком кіберпростору , розвинулася і небезпека наших даних , тепер можна чекати несподіванки звідусіль.

Компанії намагаються не відставати від розвитку тезнологій і будують свої платформи, або перероблюють те мале, що в них було. Чим більша компанія та її продукт, тим більша вірогідність існування уразливості . Щоб запобігти витоку інформації, вони звертаються до пентестерів. Спеціалістів, що моделюють дії зловмисника, використовують вразливості і звітують як краще вирішити проблеми безпеки.

Тож, почнемо з початку. Існує певний алгоритм здійнестення пентесту. Перший крок це захистити себе та компанію від порушення закону. Підписання договору на юридичному рівні, де будуть прописанні такі нюанси як: що вам можна робити, які частини системи тестити, в які сроки і т.д. Потім настає стадія збирання інформації. Це одна з найважливіших частин, тому що на ній грунтуватися всі подальші кроки. Саме це далі буде розібрано більш детально. Після розвідки потрібно змоделювати можливі уразливості і експлотувати їх. Останній крок це складання звіту з деталями, якими інструментами ви зробили

свою роботу, скріншоти результатів, ризики, які несе знайдена уразливість та рекомендації щодо їх усунення.

Існує два типи розвідки. Пасивна та активна. Відрізняються вони тим, що активна безпосередньо взаємодіє з ціллю(наприклад,скан портів), а пасивна ні. При пошуку нас цікавить вся інформація , що є на ціль. Почати можна з браузеру . Знайти всі згадки про ціль, знайти її сторінки в соц. Мережах, проаналізувати їх. Далі можна почати сканування портів, сервісів , доменів, субдоменів і так далі. При цьому потрібно бути обережним, тому що за сканування навіть портів в деяких країнах є відповідальність. В Україні це статті 16 Розділу ККУ 361-363.

Існуює спеціальний синтаксис для розширеного пошуку в кожному браузері. За допомогою нього можна знайти документи, керовані сторінки, що вже недоступні і так далі. Також є відома «хакерська» пошукова система відрізняється вона тим , що може знайти погано сконфігуровані сервери, бази даних, директорії і тд , важливо вміти його використовувати.

Для того щоб мати уявлення про мережу є nmap,який сканує хости. Кожна машина, що підключена до Інтернету або локальної мережі має IP адресу.

Усю цю інформацію складно тримати в голові, тому раджу використовувати Maltego. За допомогою нього можна створювати графи або генерувати звіти. Також його можна використати для розвідки. За допомогою Maltego можна запустити сканування і знайдені результати приголомшлять. За декілька хвилин програма знайде інформацію про поштовий сервер, поштові адреси, номери телефонів, домени, субдоменів, геолокацію, IP адреса і так далі.

Література:

АНАЛІЗ МЕТОДІВ ЗЛОМУ ТА ВИКРАДЕННЯ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ПІДПРИЄМСТВІ ДЛЯ ЕФЕКТИВНОЇ ПРОТИДІЇ

Примаченко Богдан Олегович, БЗСМ-71
Державний університет телекомунікацій
м.Київ, Україна

В статті описана проблема соціальної інженерії для отриманння доступу до конфіденційної інформації користувачів, методи які використовують зловмисники, її напрями та приклад використання соціальної інженерії для злому акаунту Skype. Які психологічні прийоми використовують зловмисники, а також як можна їм протидіяти.

Вступ

Соціальна інженерія - це набір різних психологічних методик та шахрайських засобів ціллю яких є отримання конфіденційної інформації про людину, не чесним шляхом. Конфіденційна інформація - це логіни та паролі, інтимні дані, компромат, номера банківських карток, а також все що може принести матеріально чи репутаціяну шкоду людині.

Людський фактор це насправді слабка ланка у кібербезпеці. Безпека це не продукт це процесс. І це не техніна проблема, а проблема людей і управління. [1, с. 13-15]

Рис.1. Основна схема дій в соціальній інженерії [2, с. 13]

Напрями соціальної інженерії [3]

1. Кардинг - будь-які махінації з кредитними картками, для отримання вигоди.

2. Фішинг - це вид махінації ціллю якого є заволодіння вашими логінами і паролями від важливих сайтів. Назва йде від англійської, що перекладється як

«рибна ловля». Він отримав таку назву саме через те, що даний вид атаки не націлений на одну людину, розставляються так звані сітки. Як приклад, сумнівні листи на електронну пошту які просять вас перейти за посиланням, як тільки ви це зробите, можна вважати, що ваші данні уже у злочинця.

3. Фармінг - вид шахрайства, що пов'язаний з фішінгом, але є більш небезпечним. Зловмисиник за допомогою вірисних програм перенеправляє користувача на фішінгові сайти. Небезпечність полягає в тому, що користуач часто не бачить підміни і помічає її занадто пізно.

4. Злам соц мереж - дуже популярний вид шахрайства в наш час. Основною небезпекою зламу соц мереж є не злам саме вашого аккаунту, а наприклад акккаунту вашого знайомого, с якого вам потім прийде повідомлення про те, що терміново потрібні гроші чи допомога. Розумний хакер вивчить вашу переписку, щоб розумінити манеру спілкування і напише так, що відрізнити його від справжнього знайомого буде майже неможливо. Але так як у хакера обмаль часу на вивчення переписки, часто виявити злом достатньо просто.

5. СМС - атаки - механізмом їх дії є викликання жалості у людини. Вам приходить СМС з тексом про те що, треба допомога на збір дитині на лікування, чи сестрі, чи матері. Основною ціллю таких атак є люди 40+ та жінки з дітьми, які легко можуть повірити в таку історію і не будуть перевіряти надані реквізити перед відправкою грошей.

Злам за допомогою соціальної інженерії на прикладі зламу Skype до 2013 року [4]

Найбільшою проблемою Skype є його служба підтртримки, може виглядати дивним те, що служба метою якої є захист акаунтів, навпаки є його найбільшою загрозою. Але ось у чому справа, якщо ви не пам'ятаєте пароль, вам вишлють його на почту. Але ж ми не маємо доступу до почти жертви. На сайті Skype існувала форма подачі заявки на відновлення акаунта, для цього потрібна така інформація:

- Пошта, що прив'язана до акаунту

- Приблизна дата створення акаунту
- Дата останнього входу
- 3 і більше друзів в списку акаунту
- Країна, дата народження та ще декільна не дуже важливих пунктів

Якщо надати всі ці дані службі підтримки, то протягом 24 годин вам прийде відповідь про те чи вона підверджена, чи відхилена. І якщо відповідь позитивна, то нам будуть видані вся дані для відновлення доступу до акаунту.

Крок 1. Збір інформації.

На першому кроці проходить аналіз жертви. Додавши її в контаки ми вже можемо отримати країну та дату народження якщо вони не приховані, але у більшоссті користувачів вони в загальному доступі. Якщо ж вони закриті, то використовуючи логін можна пошукати вінформацю в пошукових системах, щоб знайти соц мережі чи форуми де можна подивитись цю інформацію.

Дату останнього входу легко дізнатись, бо Skype показує статуси ваших контактів. Невелика неручність якщо ви не можете застати жертву онлайн адже Skype не показує дату останнього входу. Для того, щоб дізнатись її можна відправити жертві файл, якщо через 2 дні файл так і не відправиться, то вказуємо останній візит більше 2 днів назад.

Дату створення акаунту дізнатись точно не можливо, але до цього пункту не дуже велика увага, тому підійде приблизний місяць і рік. Тут нам допомагає сбір інформації про жертву. Для чого використовується Skype, чим займається і тд.

Три контакти зі списку - це важче, але легким способом буде просто додатись в контакти трьома своїми акаунтами. Головне, щоб вони не були нові та не зареєстровані в один і той же час.

Отримання пошти проходило за допомогою Facebook, створюємо новий акаунт, натискаємо додати друзів, обираємо імпортувати з Skype і таким чином напроти кожного акаунту була його пошта. Після 2013 року цю інформацію

перестали передавати в цілях безпеки, а також саме через часті випадки злому акаунтів.

Крок 2. Заявка

При створенні заявки треба враховувати з якої країни жертва. Якщо жертва з Америки, а ви подаєте заявку з Китаю, то у служби підтримки виникне багато питань, і шанс відмови у відновленні доступу близиться до 100%. Тому важливо налаштувати проксі на ту саму країну, що й у жертви.

Вказавши всі дані, також треба придумати маленьку історію втрати доступу до акаунту. Наприклад:

«Я був на відпочинку і не користувався своїм акаунтом деякий час. Повернушись додому і зробивши спробу зайти я не зміг отримати дрступ до акаунту. Я впевнений, що пароль і логін вірний, тому припускаю, що моїм акаунтом могли заволодіти зловмисники, прошу допомогти»

Після цього вам протягом доби прийде відповідь на пошту. І в разі схвалення заявки, акаунт уже буду прив’язаний саме до цієї пошти. Тому ви зможете використати відновлення пароля і отримати доступ до акаунту.

Так розглянувши даний приклад, ми можемо впевнено сказати, що для отримання доступу не обов’язково знати мови програмування, та використовувати хитромудрі програми для підбору паролів, досить провести невеликий збір інформації і всі дані будут уже в нас.

Все, що було описано вище вже виправлено, саме через велику кількість зломів саме цим способом. Але з’явилось багато інших більш досконалих методів, хакери ніколи не зациклюються на одному засобі, саме тому дуже важливим є відношення до своєї безпеки в мережі.

Які психологічні методи вкиристовують соціальні інженери для злому

Механізми впливу

Найбільш важливий інструмент, який найбільше підходить для потреб зловминисників - психологія впливу і розуміння механізмів, які допомагають знаходити проріхи у переконаннях та цінностях людей.

Основним правилом психології впливу є: існують базові механізми і всі люди підвержені хочаб одному з них. Все залежить від розвітку людини і її інтелекту, чим він вищий тим важче буде на неї вплинути.

Психологи знайшли цілий ряд розумових стереотипів для прийняття щоденних рішень. Для цього було введено спеціальний термін - оціночна еврістика. Багато розумових стереотипів діють за моделлю «дороге = хороше». Схильність до спрощеного мислення часто буває корисною, але такоєж приводить до помилок. Чим і користуються зловмисники. [5, с. 12 - 13]

Вирішення: Раціональний підхід до прийняття рішень, а також відмова від прийняття швидких рішень під впливом емоцій.

Керування емоційним станом людини

Одним з головних вмінь зловмисників, є вміння впливати на емоції людини. Золоте правило переговорів каже, що той хто може викликати будь які емоції у співрозмовника і буде керувати бесідою. І нажаль зловмисники постійно цим користуються, викликання жалю, співчття, злості, вини. За допомогою всих цих емоцій людину стає набато легче обманути.

Вирішення: при будь-яких суперечках чи розмовах завжди усвідомлювати свої слова та дії. Не піддаватися на провокації. Обмірковувати все спокійно та з холодною головою.

Психологія мас і соціологія

Дані знання дуже добре допомагають хакеру зрозуміти найбільш масові вразливості людей аж до конкретних регіонів. Використовуючі ці дані він буде знати як налаштовувати фішингові сайти та інші інструменти.

Вирішення: Використання тільки перевірених сайтів. Видаляти підозрілі листи з пошти. Оцінювати ситуацію.

Профілювання

Це навпаки навідміну від минулого пункту, зосередженість на вивченні конкретної людини з ціллю зламу. Найбільш дієвий метод для того щоб зламати когось конкретного, але потребує хороших навичок і знань, тому

більшість хакерів використовують інші методи знаходження вразливостей людини.

Яка сама велика небезбека ваших активів? Відповідь проста - соціальний інженер - нечесний фокусник, який змушує дивитись на його ліву руку, поки правою краде ваші секрети. І часто він такий дружній, що ви самі раді, що зустріли його - це і є профілювання. [1, с. 13 - 15]

Вирішення: не довіряти всім підряд свої секрети. Не розповідати про себе занадто багато незнайомцям чи малознайомим людям.

Висновок

На сьогоднішній день головною вразливість комп'ютерних систем є саме людина. Тому для протидії перерахованим вище методам викрадення інформації на підприємствах повинні проводитись заходи щодо навчання персоналу. Це навчання буде включати в себе огляд самих методів які існують. Проведення профілактичних бесід. Постійна робота по збільшенню обізнаності персоналу на тему кібербезпеки. Також в ідеальних умовах у відділі кібербезпеки повинен будти психолог який зможе розуміти хто з співробітників може буди найбільш врзаливою ціллю для зловмисників.

Завдяки не обережним людським діям відбуваються втрати даних, злами і помилки. Саме тому соціальна інженерія як метод злому є одним з найбільш поширених методів для отримання конфіденційної інформації. Для того щоб зберегти свої дані від викрадення треба в першу чергу подумати про свою безпеку в мережі. Використання однакових паролів, занадто багато загально доступної інформації, легкі паролі, переходи по сумнівним посиланням та ще багато іншого, що призводить до втрати акаунтів та інформації. Тому головним рішенням проблеми соціальної інженерії є самосвідомість користувачів мережі.

Література:

1. *Кевин Мітнік, «Исскуство обмана» - 2001 р.*
2. *Максим Кузнецов, Ігорь Сімдянов, «Социальная инжернерия и социальные хакеры» - 2007 р.*
3. *Социальная инженерия - технология «взлома» человека [Електронний ресурс] // - Режим доступу: https://medium.com/@Emisare/socialnaya-ingeneria-9f16e0ba7fa5*

4. *Социальная инженерия как метод атаки [Електронний ресурс] // - Режим доступу: https://habr.com/ru/post/348496/*
5. *Чалдіні Роберт, «Психология влияния» - 2009 р.*

ВИКОРИСТАННЯ СИТУАЦІЙНОГО ПІДХОДУ ДО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

Самко В. В.
студент УБД -41
Державний університет телекомунікацій
м. Київ, Україна

В умовах постійного розвитку сфери інформаційної безпеки керівництво організації здійснює вибір методології, що найкраще підходить для управління кібербезпекою організації. Так як кожний підхід має свої переваги та недоліки актуальним стає адаптація методів управління під конкретні ситуації.

Ситуаційний підхід до управління кібербезпекою базується на понятті ситуації.

Ситуація – сукупність стану підсистем, діючих процесів та подій, що відбулися [1].

Основним принципом ситуаційного управління є ідентифікація та аналіз ситуації в кожний момент часу, та прийняття управлінських рішень, щодо адаптації методів, алгоритмів управління. Основною перевагою ситуаційного підходу є сприйняття кожної ситуації в якості унікальної. Такий підхід дозволяє максимізувати ефективність вирішення задачі, хоч і займає більше часу. Отже, використання ситуаційного підходу найбільш ефективне для планування довгострокових рішень.

Основною особливістю підходу до управління кібербезпекою можна назвати його здатність до поєднання з іншими підходами. Як зазначає [2, с. 1-2] – ситуаційний підхід до управління не розглядається як заміна іншим підходам, а існує для розширення сфери їх використання.

Отже проведення аналізу ситуації зводиться до виконання наступних етапів:[3]

1. збір інформації про ситуацію;

2. прогнозування її розвитку;
3. адаптація методів, створення управлінських рішень;
4. імітація впливу таких рішень на об’єкт управління;
5. прийняття рішення;
6. застосування рішень до об’єкту управління.

Перший етап представляє собою типове завдання збору статистичних даних про стан кібербезпеки. На цьому етапі проводиться аналіз ризиків, політик безпеки, тестування на проникнення, пошук недоліків систем.

Другий етап є найбільш критичним так як його завданням є передбачити майбутню ситуацію відносно об’єкта управління. Для успішного здійснення цього етапу рекомендовано використовувати методи моделювання, що дозволяють більш точно розглянути майбутню ситуацію та оцінити ефективність розроблених управлінських рішень.

Після проведення аналізу існуючої ситуації та прогнозування її розвитку, отримуємо можливість провести адаптацію існуючих методів управління кібербезпекою відносно конкретної ситуації. Наприклад особливо ефективним використання такого методу може стати для управління інцидентами кібербезпеки. Використання ситуаційного управління дозволить не лише адаптувати прийняті процедури реагування на інциденти в залежності від особливостей ситуації(стану безпеки), але і знизити можливість їх повторення завдяки моделюванню та передбаченню потенційного розвитку ситуації.

У результаті використання методів моделювання та передбачення розвитку ситуації отримуємо можливість провести імітацію впливу розроблених рішень на об’єкт управління. У разі успішності показників управлінське рішення приймається та застосовується.

Отже найбільш ефективним способом використання ситуаційного підходу до управління кібербезпекою є його використання в якості інструменту адаптації та покращення існуючих методів управління. Використання такого методу передбачає вимоги до досвіду спеціалістів, що його застосовують, але

надає можливість максимізувати ефективність прийняти управлінських рішень на основі розгляду унікальності окремих ситуацій кібербезпеки.

Література:

1. *Визначення поняття ситуації URL:* http://itclaim.ru/wiki/index.php?n=CLAIM.%d0%a1%d0%b8%d1%82%d1%83%d0%b0%d1%86%d0%b8%d1%8f
2. *Про ситуаційний підхід до управління інформаційною безпекою С. 1-2, URL:* https://cyberleninka.ru/article/n/o-situatsionnom-podhode-k-upravleniyu informatsionnoy-bezopasnostyu/viewer
3. *Принципи ситуаційного управління URL:* http://itclaim.ru/wiki/index.php?n=CLAIM.%D0%A1%D0%B8%D1%82%D1%83%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B5%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5

ТЕХНОЛОГІЇ ТА ЗАСОБИ ПОБУДОВИ МОДЕЛІ БЕЗПЕКИ ДЛЯ КОРПОРАТИВНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ОБЛАДНАННЯ CISCO

Мадяр Г. Ф.
БСЗМ-71
Державний університет телекомунікацій,
м. Київ, Україна

Розглянуто зміст технологій та засобів побудови моделі безпеки для корпоративної мережі. Визначено мету і основні завдання щодо побудови моделі безпеки для корпоративної мережі. Розроблено рекомендації щодо застосування тахнологій та засобів побудови моделі безпеки для корпоративної мережі з іикористанням обладнання Cisco.

Питання забезпечення безпеки на сьогоднішній день як ніколи актуальні в організації будь-якого масштабу і області роботи. Все більш зростаюча кількість різних шкідливих програм (вірусів, хробаків та ін.) і залежність від інформації і її змісту вимагають підвищеної уваги до питань забезпечення безпеки. Для вирішення даних питань необхідний системний підхід і великий досвід створення систем подібного рівня з тим щоб врахувати всі можливі фактори, які впливають на безпеку.

Призначення систем мережевої безпеки:

захист сховищ даних, локальних і глобальних мереж від спроби несанкціонованого доступу і зовнішніх або внутрішніх атак з публічних мереж, наприклад, мережі Інтернет;

обмеження доступу несанкціонованих користувачів;

захист від вірусів, троянських програм, черв'яків і інших шкідливих програм;

шифрування критичного трафіку.

Система інформаційної безпеки мережі забезпечує:

аутентифікацію і авторизацію користувачів і мережевих пристроїв;

контроль доступу до ресурсів мережі;

контроль ресурсів мережі;

захист від відмов [1].

Реалізація вищеописаних завдань досягається наступними методами і засобами:

1) Система механізмів контролю доступу реалізована на основі наступних продуктів і рішень:

CiscoSecure ACS - продукт компанії Cisco Systems, використовується як засіб контролю доступу користувачів мережі до мережевих пристроїв і ресурсів мережі. Продукт реалізує наступні функціональні можливості:

аутентифікація, авторизація та облік використання ресурсів користувачами мережі (ААО);

повна інтеграція контролю доступу з використовуваним мережевим устаткуванням. Запит на авторизацію прав доступу користувача до ресурсу може виходити від мережевого обладнання, через яке здійснюється доступ;

можливість створення єдиного центру контролю доступу користувачів до мережевих пристроїв і ресурсів мережі;

гнучка схема контролю доступу на основі набору параметрів, що характеризують конкретного користувача інтранет;

можливість інтеграції з іншими засобами контролю доступу, в тому числі з протоколами RADIUS, TACACS +, LDAP, авторизацію в домені NT і NDS.

2) У якості механізмів обмінної аутентифікації в системі реалізовані і можуть бути застосовані наступні механізми:

Протокол PAP - ідентифікує абонента мережі на основі пари ідентифікатор/пароль. Пересилання пароля при цьому здійснюється у відкритому вигляді.

Протокол CHAP - ідентифікація відбувається із застосуванням хеш-функції (зазвичай MD5), одним з параметрів якої є «текстовий секрет», ніколи не передається по мережі.

3) Забезпечення безпечної маршрутизації грунтується на механізмах забезпечення її цілісності, і покликана протидіяти атакам на руйнування мережі шляхом застосування помилкових маршрутів в її центральній частині. Маршрутна ідентифікація гарантує, що оновлення маршрутизації виходить від перевіреного джерела і що ніякі дані не зіпсовані. Вона використовує шифрування, односторонню хеш-функцію для забезпечення ідентифікації робочого місця і цілісності змісту відновлення маршрутизації.

4) Відмовостійкість мережевих елементів мережі повинна розглядатися в двох аспектах: відмовостійкість самого обладнання і відмовостійкість обладнання під впливом зовнішніх мережевих впливів. Перше питання розглядається у відповідному розділі проектної документації, що описує технічні характеристики використовуваного обладнання. Другий аспект відноситься до питань забезпечення інформаційної безпеки і передбачає проведення комплексу організаційно-технічних заходів щодо захисту обладнання і елементів мережі від атак типу «відмова в обслуговуванні».

Для побудови корпоративної системи безпеки з урахуванням рекомендація SAFE компанії Cisco Systems. в центральному офісі рекомендується використовувати моделі «міжмережевих екранів» з функцією резервування серій Cisco PIX-515E, Cisco PIX-525 або Cisco PIX-535 з підтримкою декількох портів Fast Ethernet або Gigabit Ethernet. Міжмережеві екрани цієї серії дозволяють здійснювати гнучке налаштування політик безпеки, створення великої кількості нейтральних зон (DMZ), поряд з високою

продуктивністю і надійністю цього критичного вузла мережі. У нейтральних зонах традиційно розміщують важливі вузли корпоративної мережі, сегмент доступу до корпоративної мережі, сегмент віддаленого доступу клієнтів або користувачів мережі та ін [2].

Для забезпечення комплексності захисту рекомендується установка сенсорів виявлення атак («Система виявлення атак») серії Cisco IDS 4200 або систем запобігання вторгнень Cisco IPS 4200 які мають порти FastEthernet/Gigabit Ethernet і розраховані на різні швидкості аналізу трафіку. Слід зазначити, як уже зазначалося вище, що розміщувати рекомендується такі сенсори як на зовнішньому периметрі доступу в публічні мережі, так і на ділянках найбільш критичних ресурсів мережі компанії з метою запобігання несанкціонованому доступу до ресурсів, що захищаються і атак на ці ресурси. Перевагою установки IPS є можливість роботи даної системи в декількох режимах - режимі виявлення вторгнень (трафік аналізується, при цьому пристрій не бере участі в передачі трафіку; блокування трафіку можливе тільки при використанні зовнішніх пристроїв - брандмауера, маршрутизатора, комутатора рівня 3) і режимі запобігання вторгнень (трафік аналізується, при цьому пристрій бере участь в передачі трафіку і може здійснити блокування небажаного трафіку без додаткових зовнішніх пристроїв) і мішаному режимі - режимі виявлення вторгнень і запобігання вторгнень (система запобігання вторгнень працює для однієї ділянки мережі, система виявлення вторгнень для іншої ділянки мережі).

На наведеній схемі система запобігання атак служить в якості такої для інтерфейсу брандмауера, який підключений до корпоративної мережі, і в якості системи виявлення вторгнень на прикордонному маршрутизаторі. Також для підвищення безпеки на рівні серверів рекомендується установка «Host based IDS» (систем виявлення атак на рівні хоста) серії Cisco Security Agent на найбільш критичні сервера (в усі DMZ зони), для виявлення несанкціонованої активності на рівні сервера/робочої станції і встановленої операційної системи [3].

Для параметрів завершення зашифрованих VPN (Virtual Private Network) сесій від мобільних користувачів або віддалених локальних мереж можливе застосування окремого зовнішнього пристрою VPN концентратора, спеціально призначеного для таких цілей і дозволяє в залежності від моделі термінувати від 100 до 10 000 віддалених користувачів.

З метою забезпечення комплексного управління всіма елементами забезпечення безпеки рекомендується використання спеціалізованої системи управління Cisco VPN Management Solutions (VMS), що розміщується в зоні DMZ 1 «Сервери аутентифікації і управління».

Для забезпечення аутентифікації користувачів, мережевих пристроїв використовуються сервера аутентифікації, наприклад, Cisco ACS розміщується в зоні DMZ 1 «Сервери аутентифікації і управління».

Для підключення користувачів корпоративної мережі також рекомендується використовувати підключення в окрему демілітаризовану зону, що дозволить забезпечити необхідний рівень внутрішньої безпеки мережі («Маршрутизатор КС»).

Рекомендується винос зовнішніх серверів (SMTP, WWW, Proxy) та внутрішньокорпоративних серверів також в окремі DMZ зони, контрольовані міжмережевими екранами. Дане рішення дозволить забезпечити рівень безпеки для серверів і забезпечити безпеку доступу в і ззовні публічної мережі.

Так, наприклад, доступ в Інтернет через сервери Proxy і доступ до електронної пошти здійснюється через так звані Proxy або SMTP - relay агенти.

Загальний принцип функціонування полягає в тому, що всі запити від внутрішніх клієнтів перенаправляються на внутрішні сервера WWW і SMTP (зелена стрілка), потім вже внутрішні сервери WWW і SMTP взаємодіють через міжмережевий екран з зовнішніми серверами WWW і SMTP розміщеними в DMZ3 зоні (синя стрілка). І тільки зовнішні сервера WWW і SMTP взаємодіють безпосередньо з Інтернет серверами через міжмережевий екран (червона стрілка).

Таким чином здійснюється повний контроль над проходженням інформації, а також виключається безпосередня взаємодія користувачів локальної мережі з Інтернет мережею, що дозволяє значно збільшити загальну безпеку корпоративної мережі.

Для забезпечення захисту у віддалених офісах і для мобільних співробітників пропонується розглянути три типових варіанти побудови системи безпеки:

Рішення на базі інтегрованої в маршрутизатор функціональності міжмережевих екранів і систем виявлення атак, що дозволяє забезпечити більший рівень безпеки в порівнянні з базовими системами безпеки. Цей варіант рекомендується використовувати при обмежених коштах і для бюджетних рішень. В даному випадку в якості маршрутизаторів можуть встановлюватися серії Cisco 800, 1800, 2800 і вище. Для реалізації функцій систем виявлення атак можливе використання спеціалізованого модуля мережної системи виявлення атак NM-CIDS-K9 для серій Cisco 2800 і вище.

Рішення на базі окремих компонентів, володіє більшою надійністю і безпекою, оскільки функції маршрутизації і забезпечення безпеки реалізовані на різних пристроях. Дане рішення рекомендується для реалізації в разі необхідності забезпечення високого рівня безпеки корпоративної мережі. У якості маршрутизаторів можуть встановлюватися серії Cisco 800, 1800 і вище, а в якості міжмережевих екранів серії Cisco PIX-501, Cisco PIX-506E або вище. При необхідності можуть встановлюватися мережеві системи виявлення/запобігання атак (IDS / IPS) або host based IDS (Security Agent).

Для організації підключення віддалених мобільних користувачів, рекомендується використання зовнішнього VPN концентратора, Cisco PIX Firewall або маршрутизатора зі спеціалізованим ПЗ в центральному офісі та програмне забезпечення Cisco VPN клієнтів, на робочих місцях користувачів, що дозволяє забезпечити безпечне і захищене підключення, в тому числі і по публічним каналам зв'язку Інтернет, з організацією шифрованих IPSec тунелів.

Слід зазначити, що дане рішення є дійсно типовими і в реальних проектах можливе використання інших схем і методик забезпечення безпеки в залежності від бажаного результату, поставлених цілей і бюджету проекту.

Література:

1. *Курило А.П. Основы управления информационной безопасностью. Учебное пособие для вузов. / А.П.Курило, Н.Г.Милославская, М.Ю.Сенаторов, А.И.Толстой / – М.: Горячая линия-Телеком, 2012. – 244 с.*
2. *Садердинов А. А., Трайнев В. А., Федулов А. А. Информационная безопасность предприятия: Учебное пособие.2-е изд. – М.: Издательско-торговая корпорация «Дашков и К°». 2005. – 336 с.*
3. *Побудова мережевої та локальної системи безпеки (telesphera.net) .*

КАНАЛИ ВТРАТИ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Вдовиченко М. С.
студент БСД-42
Державний університет телекомунікацій
м.Київ, Україна

Стрімкий розвиток суспільства призвів до широкого використання в усіх сферах діяльності людини, швидкодіючих інформаційних систем та технологій, які надають можливість доступу до світового інформаційного простору. Зворотною стороною глобальної інформатизації стала поява комп'ютерної злочинності. На локальному рівні загроз інформаційної безпеки виділяють канали витоку інформації, під якими розуміють сукупність джерел інформації, матеріальних носіїв або середовища розповсюдження несучих цю інформацію сигналів і засобів виділення інформації з сигналів або носіїв. Об'єктивне існування даних каналів витоку передбачає їх можливе використання зловмисниками для несанкціонованого доступу до інформації, її модифікації, блокування та інших неправомірних маніпуляцій, тобто наявність каналів витоку інформації впливає на обрання способу вчинення злочину.

Втрата інформації припускає незаконний перехід конфіденційних відомостей до особи, яка не має права використовувати ці відомості у своїх цілях для одержання прибутку або передачі іншій особі. У тому випадку, коли втрата інформації відбувається з вини персоналу – втрата інформації позначається терміном розголошення або розголос інформації.

Розголошення інформації завжди здійснюється людиною усно, письмово, за допомогою жестів, міміки, умовних сигналів. Термін "витік інформації"

більшою мірою стосується втрати інформації за рахунок її перехоплення за допомогою технічних засобів розвідки.

Втрата інформації можлива за наявності каналів розголошення або витоку. Канал втрати інформації означає перехід цінних відомостей від закінченого джерела, по-перше, або безпосередньо до конкурента або зловмисника, по-друге, до третьої особи в несанкціонованому режимі. Під третьою особою розуміються будь-які особи, які одержали знання конфіденційної інформації через деякі обставини або в результаті безвідповідальності персоналу. Варто враховувати, що ці особи не зацікавлені в отриманій інформації. Перехід інформації до третьої особи утворить випадковий або стихійний канал втрати інформації в результаті:

- втрати документів або конфіденційних записів;

- незнання або ігнорування персоналу фірми вимог щодо захисту інформації;

- зайва балакучість співробітників з колегами по роботі, іншими особами в місцях загального користування, у транспорті й т. д.;

- роботи з конфіденційними документами при сторонніх особах за рахунок несанкціонованої передачі їх іншому співробітникові;

- у результаті наявності в документах зайвої конфіденційної інформації;

- у результаті самовільного копіювання співробітником документів у службових або колекційних цілях.

На відміну від третьої особи зловмисник цілеспрямовано намагається одержати конкретну інформацію й тому навмисно і таємно знаходить або формує канал розголошення або витоку інформації. Канали втрати конфіденційної інформації діляться на організаційні й технічні.

Організаційні канали розголошення інформації, засновані на встановленні різноманітних, у тому числі законних взаєминах з фірмою або співробітником фірми для наступного несанкціонованого доступу до інформації, що цікавить зловмисника. Основними видами організаційних каналів можуть бути:

- влаштування зловмисника на роботу у фірму, як правило на технічну, допоміжну або другорядну посаду;

- установлення зловмисником довірчих взаємин зі співробітником фірми або особами, що мають право вільного доступу в даній фірмі;

- кримінальний, силовий доступ до інформації, тобто крадіжка документів, справ, дискет, дисків, комп'ютерів, шантаж до співробітництва окремих працівників, підкуп працівників, інсценування екстремальних ситуацій;

- одержання інформації з випадкового каналу.

В свою чергу, теехнічний канал витоку інформації є сукупністю небезпечних фізичних сигналів, середовища їх розповсюдження та зберігання, об’єкту технічної розвідки й способів і засобів технічної розвідки, що можуть бути застосовані для зняття інформації з об’єкту, що охороняється.

Технічні канали прийнять поділяти за наступною класифікацією:

- акустичні канали витоку інформації, куди входять також канали з акустично-електричними перетвореннями;

- радіотехнічні канали витоку інформації, куди входять, по-перше, відкриті канали радіотехнічного зв’язку та, по-друге, канали, що утворюються за рахунок паразитних випромінювань та наводок;

- оптичні канали витоку інформації;

- речовий канал витоку інформації, який визначається людським фактором.

Наявність будь-якого з вище наведених каналів призводить до появи ризику, який в свою чергу може призвести до появи загрози, наслідком реалізації якої, будуть різні види прямих або непрямих втрат.

Статистика показує, що у всіх країнах збитки від зловмисних дій безупинно зростають. Причому основні причини збитків пов'язані не стільки з недостатністю засобів безпеки як таких, скільки з відсутністю взаємозв'язку між ними, тобто з нереалізованістю системного підходу. Тому необхідно випереджальними темпами вдосконалювати комплексні засоби захисту.

Література

1. *Хорошко В.О. Основи інформаційної безпеки /Хорошко В.О., Чередниченко В.С., Шелест М.Є./ За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 186 с.*
2. *Технічні канали витоку інформації. http://virt.ldubgd.edu.ua/pluginfile.php/42824/mod_resource/content/1/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%206.pdf*

REST АРХІТЕКТУРА ВЕБ-ДОДАТКІВ

Прус К. В.
Державний університет телекомунікацій
Навчально науковий інститут захисту інформації
м.Київ, Україна

З розвитком програмних засобів проектування та безпосередньої розробки як веб-додатків так і будь-яких інших ресурсів, що передбачають наявність користувацького інтерфейсу для взаємодії із користувачем, розвивались та вдосконалювались і підходи до розробки систем як таких. На відміну від звичайних веб-сайтів, що основним чином призначені для представлення тематичного контенту та за доцільністю являють собою більш інформаційний характер, веб-сервіси є більш ресурсномісткими майданчиками.

REST – це акронім, скорочення від англійського Representational State Transfer – передача стану уявлення.

Це архітектурний стиль взаємодії компонентів розподіленої системи в комп'ютерній мережі. Простіше кажучи, REST визначає стиль взаємодії (обміну даними) між різними компонентами системи, кожна з яких може фізично розташовуватися в різних місцях.

Даний архітектурний стиль являє собою узгоджений набір обмежень, що враховуються при проектуванні розподіленої системи. Ці обмеження іноді називають принципами REST. Їх небагато, всього 6 штук.

Як було сказано вище, REST визначає, як компоненти розподіленої системи повинні взаємодіяти один з одним. У загальному випадку цей відбувається за допомогою запитів-відповідей. Компоненту, яка відправляє запит називають клієнтом; компоненту, яка обробляє запит і відправляє клієнту відповідь, називають сервером. Запити та відповіді, найчастіше, відправляються

по протоколу HTTP (англ. HyperText Transfer Protocol - "протокол передачі гіпертексту").

Як правило сервер – це якийсь веб-додаток. Клієнтом ж може бути не те щоб що завгодно, але досить багато. Наприклад, мобільний додаток, яке запитує у сервера дані. Або браузер, який відправляє запити з веб-сторінки на сервер для завантаження даних.

Однозначно одне: компонента яка відсилає запит – це клієнт. Компонента, яка приймає, обробляє і відповідає на запит - сервер.

Однак не кожна система, чиї компоненти обмінюються даними за допомогою запитів-відповідей, є REST (або ж RESTful) системою. Щоб система вважалася RESTful, вона повинна "вписуватися" в шість REST обмежень:

1. Приведення архітектури до моделі клієнт-сервер;
2. Відсутність стану;
3. Кешування;
4. Единбурзі інтерфейсу;
5. Шари;
6. Код на вимогу (необов'язкове обмеження) [1].

Одна з найбільш тонких тим в REST - це моделювання ресурсів. Тут не існує якогось єдиного підходу або простого правила, яке вам допоможе точно підібрати межі ресурсу. Намагайтеся проектувати API так, щоб воно не могло привести додаток в непрацездатний вид.

Наприклад, ви пишете API для керування блогом. Якщо у вас є вимога, що до кожної статті обов'язково повинні бути вказані теги, то вам необхідно спроектувати API так, щоб клієнт не зміг порушити цієї властивості. Як варіант, при запиті на створення статті необхідно додатково передати список тегів.

А як би ви реалізували операцію зміни стану рахунку? Вірно, через транзакції. Транзакція на поповнення рахунку, транзакція на переказ коштів і т.д.

Моделювання ресурсів також не просто, як і моделювання предметної області.

Не існує якогось єдиного стандарту, який би повністю описував REST. Ми можемо брати за основу частина дисертації Роя Філдінга про REST.

Але існує безліч маленьких стандартів, які доповнюють даний стиль:

- URI і URI Template - про однакові ідентифікатори ресурсів;
- HTTP - як протокол передачі «гіпертексту»;
- HAL, Siren - для реалізація HATEOAS;
- JSON, XML і «сім'я» можуть використовуватися для вистав [1].

Так навіщо використовувати REST? Всесвітня павутина заснована на архітектурі REST.

Тому, якщо ви створюєте API-інтерфейс non-RESTful, який буде використовуватися в Інтернеті, то ви отримаєте неоптимальну сістему. Не оптимальний щодо оптимізованої архітектури.

Це важливо відзначити, оскільки non-RESTful API може бути неоптимальним в мережевій архітектурі, але оптимальним для інших проблем. Наприклад, сучасні додатки можуть мати дуже специфічні потреби, отже, зростає число бібліотек збору даних, таких як GraphQL або Falcor [3].

Література:

1. *REST архітектура – https://javarush.ru/groups/posts/2486-obzor-rest-chastjh-1-chto-takoe-rest*
2. *REST концепція – https://dou.ua/lenta/articles/rest-conception*
3. *REST – http://web.spt42.ru/index.php/chto-takoe-rest-api*

ОЦІНКА ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Хмелевський Р. М.
старший викладач
Державний університет телекомунікацій
м. Київ, Україна

В статті проведено дослідження оцінки основних загроз безпеці інформаційної системи та розглянута методика аналізу ризиків спричинених уразливостями системи. Запропоновані напрямки забезпечення кібербезпеки організації.

Ситуація у сучасному світі характеризуються високим ступенем невизначеності та непередбачуваності. У взятому Україною курсі на входження в європейський простір акцентується увага на посиленні значення кібербезпеки, як складової національної безпеки України. Одними із основних пріоритетів забезпечення кібербезпеки визначені: створення інтегрованої системи оцінки інформаційних загроз, оперативного реагування на них, моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам та їх нейтралізації [1; 2]. Стан кібербезпеки України істотно залежить від загроз, прояв яких може завдати непоправної шкоди національній економіці.

На безпеку роботи державних інформаційних систем (ІС) України постійно здійснюють вплив небезпечні загрози. Так наприклад, від нещодавніх масових кібератак шифрувальників Petya.A, WannaCry, XDATA постраждало більше 80 українських компаній в усіх галузях економіки. Вектор «шифрувальника» був стандартний: таргетований користувач отримує лист з вкладенням шкідливого файлу. Після відкриття якого відбувається експлуатація уразливості CVE-2017-0199, далі завантажувався файл hxxp://84.200.16.242/myguy.xls. [6].

Сьогодні з’являються нові технології та способи, за допомогою яких зловмисники інфікують пристрої. Зокрема, наприклад технологія ML (machine learning) застосовується кіберзлочинцями для удосконалення шкідливих програм і ускладнення виявлення загроз. Відомим прикладом є троян Emotet. Зловмисники також можуть використовувати ML різними способами: *створення та керування новими шкідливими програми з автоматизацією інфікування, націлюватися на конкретних жертв і викрадати їх особисті дані, шукати нові уразливості «0-дня», контролювати інфіковану мережу, створення нових шкідливих ботів, тощо* [7].

За даними центру кібербезпеки США одними з ключових ризиків найближчих років можуть стати: захист периметру безпеки, ідентифікація та автентифікація, управління ресурсами, управління обліковими записами [6].

В Україні в 2020 році на об’єктах моніторингу система кіберзахисту державних інформаційних ресурсів (ІР) зафіксувала 1 594 221 підозрілих подій. В основному – це мережеве сканування (92%), застосування нестандартних протоколів – (7%). Більшість інцидентів стосується недержавного сектору (99%). Основні інциденти стосуються розповсюдження шкідливого ПЗ (97%) [3].

Таким чином, дослідження основних загроз і оцінка інформаційної безпеки сучасних ІС, пошук нових відходів щодо розвитку побудови ефективних систем захисту інформації є актуальним завданням.

Вагомий внесок у розробку загальнотеоретичних та методологічних засад щодо проблем оцінювання загроз інформаційної безпеки зробили такі науковці: В.Л. Баранов, В.Л. Бурячок, П.О. Балашов, В.Б. Дудикевич, В.В. Домарев, С.В. Казмірчук, О.Г. Корченко, О.М. Ляшенко, В.О. Хорошко та інші.

На безпеку роботи ключових ІС впливає багато факторів: кібератаки, порушення інформаційної безпеки, вихід з ладу програмно-апаратного забезпечення, помилки персоналу. Для попередження доступу до інформації в організації потрібно проводити аналіз уразливостей системи по виявленню слабких місць, потенційних та актуальних загроз і їх походження.

У цьому напряму, якщо розглянути ймовірність реалізації кожної *i*-ої загрози по відношенню до *j*-го активу відповідно [4], визначатимемо, використовуючи наступне рівняння (1)**:**

$$d_{rj} = 1 - p_{ri} \times \prod_{i=1}^{m}(1 - p_{rji}) \qquad (1)$$

де: *n* – кількість загроз; *m* – кількість активів; p_{ri} – можливість здійснення *i*-ої загрози; d_{rj} – можливість реалізації хоча б однієї загрози *j*-му активу.

При цьому:

$$p_{ri} = p_{ti} \times p_{vi}\,, \qquad (2)$$

де: p_{ti} – можливість появлення *i*-ої загрози; p_{vi} – можливість появлення уразливості по реалізації *i*-ой загрози.

Виходячи з вищевказаного, та з урахуванням тверджень [5], розглянемо у нашому випадку аналіз ризиків інформаційної безпеки для ІС. Це в основному

включає ідентифікацію активів, ідентифікацію загроз та виявлення уразливостей. Після визначення взаємозв'язку між трьома елементами аналізу ризику можна точно оцінити ймовірність інцидентів із безпекою. Формула (3) – це математичний вираз збитків, спричинених настанням події безпеки.

$$R\ (A,T,V) = R\ (P\ (T,V), F(L_a\ , V_a\ )) \tag{3}$$

де: P – ймовірність подій безпеки, спричинених уразливостями системи; T – відноситься до ймовірності настання основних подій безпеки; V – стосується вразливості. $F(L_a\ , V_a\ )$ – втрата вартості активу, спричинена подією безпеки; L_a – втрата вартості активу; V_a – рівень вразливості. З цього можна визначити формулу розрахунку величини ризику.

Далі у рівнянні (4) L_v – втрата вартості активу, спричинена ціллю атаки, та P_G – це ймовірність наступ події цільового вузлу.

$$R = (L_v\ *\ P_G\ ) \tag{4}$$

Оцінка ризику зобов'язана відображати ймовірність потенційного ризику в ІС. Правопорушник бажатиме отримати повноваження управління ціллю, яка є кореневим вузлом дерева атаки. Спочатку аналізуються потенційні ризики цільової системи та встановлюється модель дерева атак. Потім оцінюється ймовірність впливу факторів на інші вузли. Нарешті розраховується ймовірність основних подій. Вищезазначений процес забезпечує велике значення для можливого опису шляху атаки, вивчення механізму атаки та застосування відповідних ефективних захисних заходів для ІС.

Таким чином, при забезпеченні кібербезпеки ІС увагу доцільно зосереджувати як на основних загрозах так і на ймовірності реалізації актуальних загроз. Це дозволить визначити ймовірність реалізації кожної загрози, отримати повне уявлення про варіанти її деструктивного впливу і їх наслідки для організації. На нашу думку, застосування аналізу ризиків в подальшому стане підґрунтям для наступних досліджень щодо формалізованої побудови загроз безпеки з позиції теорії множин з урахуванням складності, неоднозначності, невизначеності оцінки подій та послугує математичною основою побудови моделі важко формалізованих процесів в забезпечення кібербезпеки сучасних ІС.

Література:

1. *«Про Стратегію кібербезпеки України». Указ Президента України № 96/2016 от 27 січня 2016 року. – [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/962016-19836*
2. *«Про рішення Ради національної безпеки і оборони України» Указ Президента України №392/2020 від 14 вересня 2020 року «Про Стратегію національної безпеки України» . – [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/3922020-35037*
3. *Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест/відп. ред. О.Довгань; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І. Вернадського. – К., 2020– №11 (листопад) . – 281с.*
4. *Нурдинов Р.А., Батова Т.Н. Подходы и методы обоснования целесообразности выбора средств защиты информации // Современные проблемы науки и образования. – 2013. – № 2.*
5. *Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності / Р.М. Хмелевський // Сучасний захист інформації. – 2016. – № 4. – С. 65-70.*
6. *Хмелевський Р.М. Шляхи вдосконалення професійної підготовки кваліфікованих фахівців в області кібербезпеки / Р.М. Хмелевський // Сучасний захист інформації. – 2018. – № 2 (34). – С. 104 – 105.*
7. *Эра машинного обучения в кибербезопасности: шаг к прогрессу или угроза человечеству? – [Електронний ресурс]. – Режим доступу: https://eset.ua/ru/news/view/664/mashinnoye-obucheniye-v-kiberbezopasnosti-progress-ili-ugroza*

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВЕБ-РЕСУРСІВ ВІД DDOS-АТАК ЗА ДОПОМОГОЮ СЕРВІСІВ VOXILITY, CLOUDFLARE ТА ВБУДОВАНОЇ ФІЛЬТРАЦІЇ ТРАФІКУ

Довженко Н.М., Журавель В. О.
студент БСД-42
Державний університет телекомунікацій
м. Київ, Україна

В умовах карантину в 2020-2021 років, розповсюдження інформації та послуг стало більш актуальним, ніж у будь-який інший рік. В умовах ізоляції, значно збільшився попит на різноманітні сервіси, такі як кур'єрські послуги, інтернет-кінотеатри та IPTV, магазини секс-іграшок, послуги інтернет-провайдерів, ігрові послуги, тощо[1; 2]. Разом з цим, значно збільшилась кількість DDoS-атак на різноманітні сервіси, починаючи від постачальників програмного забезпечення чи товарів повсякденного використання, та продовжуючи різноманітними IPTV-сервісами. Якщо в першому випадку частіше використовується L3/L4 DDoS-атака, то в другому випадку частіше

використовується атака L7, базуючись на недоліках програмного забезпечення.

Розглядаючи випадок захисту невеликого інтернет-магазину настільних ігор, слід проаналізувати можливі варіанти нападів. Наприклад, для розміщення сайту може використовуватись невеликий віртуальний сервер (VPS) з використанням програмного забезпечення WHM/cPanel та встановленим WordPress. В даному випадку, найбільш вірогідний напад з використанням L3/L4 DDoS-атаки, так як в даному випадку, ймовірніше за все буде відсутнє програмне забезпечення що буде найбільш підходити для проведення атак на програмному рівні (L7 DDoS-атака). В даному випадку слід розглядати декілька варіантів захисту:

- Захист за допомогою проксінгу трафіку через доменне ім’я;
- Захист з використанням захищеного аплінку з фільтруванням трафіку;
- Заборона певних різновидів трафіку.

У випадку використання методу з забороною певних різновидів трафіку, виникає ймовірність того що деяке програмне забезпечення почне некоректно працювати. Наприклад, якщо заборонити ICMP-трафік, то використовувати сервіси Nagios (або аналогічні) з перевіркою серверу на працездатність за допомогою відправки періодичних ICMP запросів, може виникнути ситуація, коли сервіс буде помічено як непрацюючий.

У випадку блокування UDP трафіку з метою захисту від UDP-flood атак, можуть виникнути проблеми з DNS, так як він все ще працює через UDP. Прикладом подібних проблем можуть бути недоступність реєстрації/відновлення SSL-сертифікатів за допомогою сервісу AutoSSL, що входить в комплект до WHM/cPanel. Аналогічні проблеми можуть повторитися і у випадку використання CertBot для отримання аналогічного SSL-сертифікату. З першого погляду може здатися що для подібного магазину SSL сертифікат може бути не обов’язковим, у випадку коли сайт виступає як каталог товарів, але багато клієнтів можуть покинути сервіс, побачивши у себе на екрані мітку “незахищеного підключення”. Також, у випадку HTTP-сайтів, деякі недобросовістні провайдери можуть модифікувати пакети, проводячи MITM-

атаку, наприклад, підмінивши сторінку с кодом помилки 404 на свою, в яку може входити реклама, чи інші дані[3; 4] .

За допомогою nginx, можна заборонити трафік із певних країн, але в такому випадку, користувачі, що використовують VPN для захисту в мережі, можуть опинитися в ситуації, коли для них сайт буде недоступний, а тому вони перейдуть на сервіси конкурентів.

Інші два випадки можуть бути платними, але мати меньше мінусів, ніж радикальна заборона певного трафіку. Для розгляду захищених аплінків, можна розглядати послуги компанії Voxility. Приклад послуг даної компанії зображено на рисунку 1:

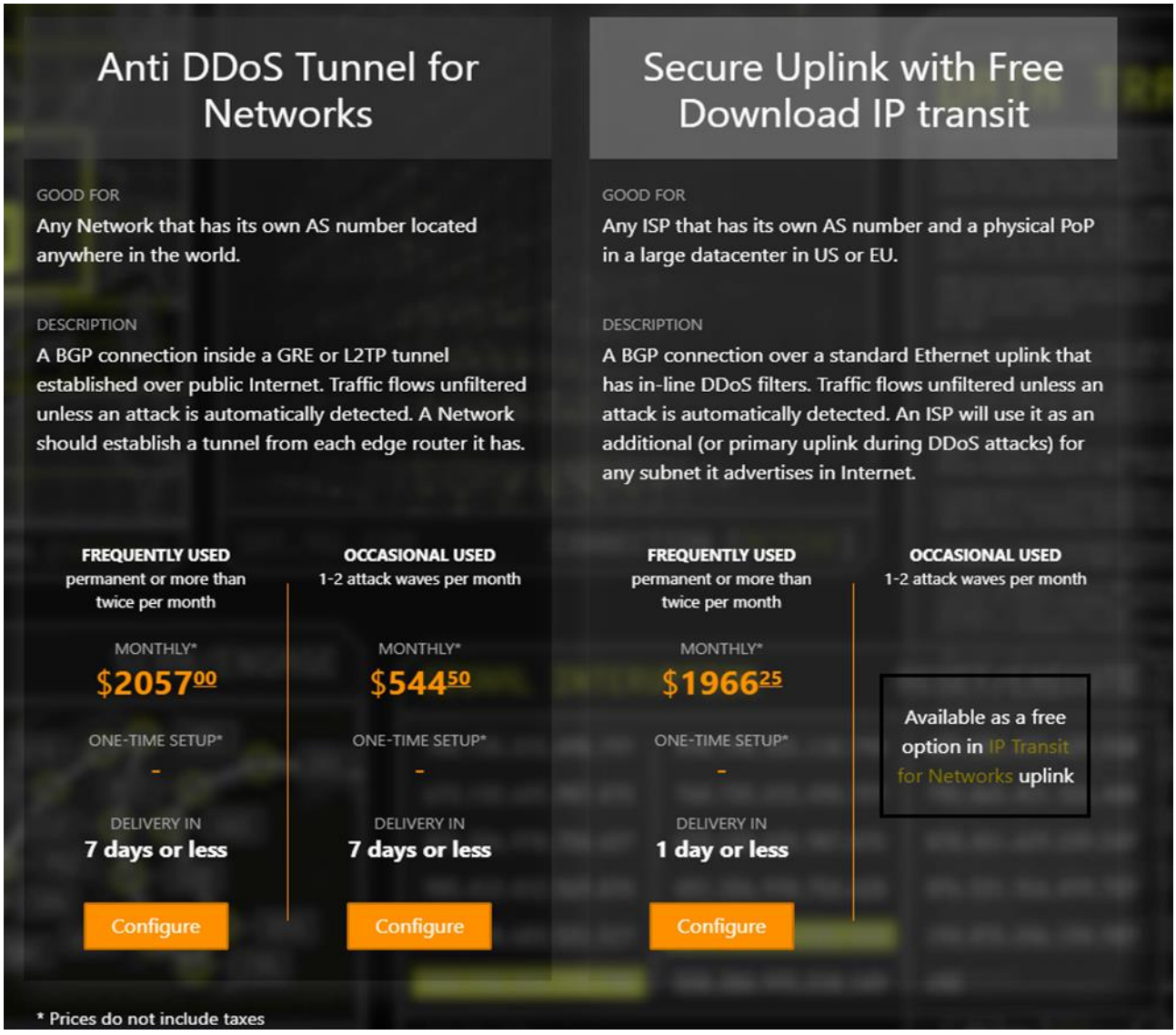


Рис. 1. Послуги захищеного аплінку від Voxility

Використання даного типу захисту допомагає в більшості випадків L3/L4

захисту, але воно занадто дороге для використання для окремого сайту. Даний захист може бути куплений у хостинг-провайдера, а вже далі розділяти захищені IP-адреси між клієнтами за певну плату.

Третім способом є використання проксі-захисту через доменні імена. Прикладом подібного сервісу може бути CloudFlare, що представляє свій захист у декількох тарифних планах, серед яких є і безкоштовний, що підходить для даного випадку. Для використання безкоштовного захисту від CloudFlare достатньо лише зареєструватися на їх сервісі та змінити свої NS-сервери на NS-сервери CloudFlare. Після цього хід трафіку зміниться та буде проходити через фільтри сервісу.

Також даний сервіс пропонує платні тарифи з більшим рівнем захисту, але в даному випадку вони дорожчі[5], ніж у конкурентів та підійдуть в першу чергу тим, хто захоче щоб їх захищала велика компанія з багатолітнім досвідом.

Література:

1. *Коронавирус и бизнес: кто выиграл и кто проиграл в условиях карантина - BBC News Русская служба - www.bbc.com/russian/features-52647490*
2. *Какие сервисы и компании выиграли от перехода на удаленную работу (rg.ru) – rg.ru/2020/04/03/kakie-servisy-i-kompanii-vyigrali-ot-perehoda-na-udalennuiu-rabotu.html*
3. *sevo-shmevo on Twitter: "А вот так Киевстар через мобильный трафик подменяет 404 страницы https://t.co/q4qDRqlXs7" / Twitter - twitter.com/seo_shmeo/status/767659445753155584*
4. *«Мегафон» перехватил мою «404» — Приёмная на vc.ru - vc.ru/claim/202065-megafon-perehvatil-moyu-404*
5. *Что есть что и кто есть кто на рынке защиты от DDoS / Блог компании Southbridge / Хабр (habr.com) - habr.com/ru/company/southbridge/blog/450092/*

ТИПОВІ РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ WEB-СЕРВЕРУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ.

Хмелевський Р. М., Маницький В. Є.
студент БСД-44
Державний університет телекомунікацій
м. Київ, Україна

В роботі розглянуто типові рекомендації щодо підвищення безпеки Web-сервера. Дуже часто простого встановлення Firewall або WAF замало, необхідно також правильно налаштувати компоненти сервера і тільки після цього вже встановити Firewall "перед" ним. Такими компонентами можуть бути nginx, mysql та php.

В сучасних умовах Web-сервери атакуються все частіше, та чому це відбувається? Якщо в цьому розібратися, то відразу стає зрозуміло навіщо їх захищати і чому до цього треба підходити відповідально.

Зараз у кожної організації є власний Web-сайт. Вони розташовані або як спеціальний хостинг (GoDaddy, BlueHost), або як Web-сервер в мережі компанії. В першому варіанті сервер на якому буде розташований сайт компанії знаходиться в дата-центрі хостинг провайдера і компанія буде мати доступ лише до конфігурації самих компонентів Web-сервера. Відомі випадки, коли до сайту, що знаходиться на сервері хостинг-провайдера був отриманий несанкціонований доступ (НСД), а після цього і до всього сервера, інших сайтів на ньому. Отже, захисту Web-сервера треба приділити особливу увагу. При нехтуванні безпекою цього ресурсу, зловмисник може отримати НСД до всієї підмережі.

То ж як підвищити безпеку Web-серверу? Є основні рекомендації які в цьому допоможуть. Починати потрібно з деталей. Розглянемо на прикладі таких компонентів: nginx, mysql, php. А також роль Firewall та WAF, що займають важливе місце у захисті Web-серверу.

Nginx – це саме і є HTTP-server який оброблює запити клієнтів. Саме він і надає доступ до файлів, сторінок, що лежать на сервері. Перше, що потрібно пам’ятати – оновлення. Дослідники завжди знаходять нові вразливості, які розробник закриває виходами “патчів” – завжди потрібно слідкувати за версією ПЗ. А ось що до самої конфігурації nginx, тут треба поглянути більш детально. По-перше – рекомендується відключити директиву server_tokens. За замовчуванням вона відображає версію nginx на всіх http відповідях у заголовку сервера, та при отриманні помилок. Якщо зловмисник дізнається версію Web-серверу, йому буде простіше дізнатися які вразливості на ньому присутні так знайти експлойт. Друге – налаштування SSL/TLS. Nginx підтримує шифрування даних за допомогою SSL/TLS, що передаються між клієнтом і сервером і зробить атаку MITM складнішою, бо вони будуть у шифрованому вигляді. І

важливий пункт – вказати точну адресу на якому сервер буде слухати підключення, бо якщо цього не зробити, при додаванні нового інтерфейсу на сервер, nginx автоматично почне приймати підключення і з нього, і якщо Firewall на цьому інтерфейсі не налаштований, це може стати великою небезпекою для Web-серверу.

MySql – база даних в якій можуть зберігатись будь-які дані. З основних порад тут – це переведення mysql на localhost, щоб вона могла приймати підключення лише з цього серверу і до неї неможливо було отримати доступ з іншої точки. Далі – пароль, тому що зловмисник може отримати доступ до серверу через вразливість у Web-додатку. Звісно також потрібно перевіряти версію ПЗ.

Щодо php – в ньому знаходять вразливості досить часто, ці вразливості дозволяють віддалено виконати код, або отримати НСД. Та не дивлячись на це, розробники дуже часто випускають патчі і активно досліджують нові вразливості, що призвело до підвищення рівня безпеки php. Щодо параметрів конфігурації php, один з найважливіших і найчастіше ігноруючих – opendir. Цей параметр прямо вказує до яких файлів має доступ php. Цей доступ має бути обмеженим директорією Web-сайту, та директорією з тимчасовими файлами.

І декілька слів про Firewall. Він безумовно відіграє дуже важливу роль. Блокування портів, що не використовуються в роботі Web-серверу, IDP/IPS, сегментація мережі та введення Web-серверу у DMZ, що не дасть зловмиснику отримати доступ до мережі, навіть якщо він проникне на Web-сервер. Розглянемо сучасний NGFW, як приклад, Fortigate від Fortinet, які посідають чільне місце серед лідерів мережевої безпеки у списку Gartner (рис 1).

Він включає в себе функції WAF – який захистить саме Web-додаток. Надає захист від sql, xss-ін’єкцій, захист від брут-форсу, DDoS-атак, логування подій. Але основна функція Fortigate – захист периметру мережі, тому функції WAF містить в собі механізми захисту лише від найвідоміших загроз. FortiWeb WAF від Fortinet має більш широку базу вразливостей та більш гнучке налаштування в залежності від Web-додатку.

Рис.1 – Fortinet у списку Gartner.

Найкраще рішення – поєднання їх для захисту самої мережі і блокування атак на Web-сервер, які не будуть використовувати Web-додаток, та захисту безпосередньо Web-ресурсу (рис 2).

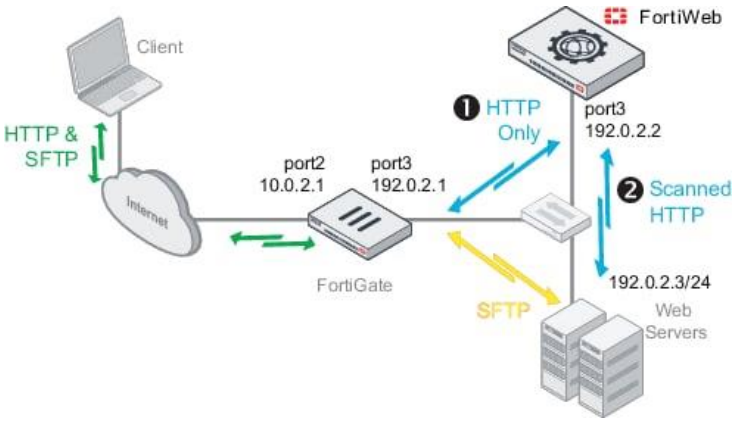


Рис 2. – Робота Foritgate у парі з FortiWeb.

Та через те, зловмисники знаходять нові способи реалізації вразливостей, іноді фаєрволи можуть не помітити спробу атаки, саме тут правильна конфігурація компонентів Web-серверу може і врятувати.

Для попередження доступу до інформації потрібно проводити аналіз вразливостей системи, опис потенційних кіберзагроз та їх походження. У нашому випадку ми проводимо опис кіберзагрози, яка може виступати одним з каналів НСД *(реалізація мережевої атаки на Web-сервер, впливу шкідливих*

програм), вказуємо суб'єкт НСД, шлях поширення загрози і інформаційний об'єкт, до якого здійснюється НСД і описуємо цю кіберзагрозу кортежем:

$$U = \langle S, R, SR_n, SR_{h,} P, \text{IO(C)} \rangle, \quad (1)$$

де S *– джерело загрози (користувач (інсайдер), зовнішній зловмисник); R – обладнання в каналі зв'язку (комутатори, маршрутизатори та ін.);* SR_n, $\text{Б}_{\text{Х}}$ *– сервіси інформаційної безпеки на шляху поширення загрози, мережеві і хостові (міжмережеві екрани, системи виявлення аномалій, журнали реєстрації аномальних мережевих з'єднань, журнали реєстрації операційних систем і ін.); P – протоколи і пакети; IO – інформаційний об'єкт доступу (в конкретному мережевому сегменті обмеження C).*

Основну увагу слід приділяти безлічі актуальних внутрішніх і навмисних кіберзагроз та ймовірності їх реалізації. Для ідентифікації зовнішнього НСД потрібно додатково використовувати індикатори, що відображають аномальні події на периметрі мережі підприємства.

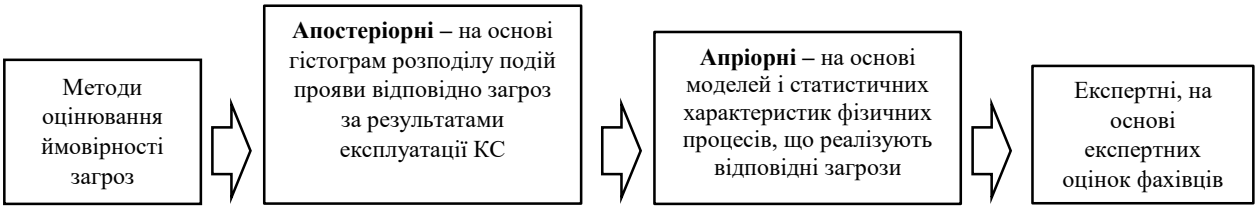


Рис. 3. Методи визначення ймовірності реалізації загроз.

Оцінювання ймовірної реалізації загроз доцільно починати з актуальних загроз. Одним із найважливіших етапів процесу аналізу факторів, які можуть вплинути на реалізацію певної загрози системи для КС є проведення якісно-кількісної оцінки можливості реалізації кожної загрози (рис.3).

Література:

1. *Базові рекомендації для підвищення безпеки *піх веб-сервера: веб-сайт. URL: https://habr.com/ru/post/112908/ (дата звернення: 18.03.2021).*
2. *Богуш В. М., Юдін О. К.Б74 Інформаційна безпека держави. – К.: "МК-Прес", 2005.*
3. *Як захистити веб-сервер: веб-сайт. URL: https://tproger.ru/articles/protecting-web-servers/ (дата звернення: 18.03.2021).*
4. *Хмелевський Р.М. «Кібербезпека як одна з основ забезпечення ефективної роботи об'єктів інформаційної діяльності та органів державного управління» // Матеріали регіональної конференції МСЕ для країн Європи і СНД «Цифрове майбутнє на основі 4G/5G» 14-16 травня 2018 року., Київ. Збірник тез. – К.: ДУТ, 2018. – С. 92-94.*

5. *Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності / Р.М. Хмелевський // Сучасний захист інформації. – 2016. – № 4. – С. 65-70.*

СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА ЇЇ МЕТОДИ

Тітаренко А. П.
студент Державного університету уелекомунікацій
м. Київ, Україна

Соціальна інженерія - це мистецтво використання людської психології, а не технічних методів злому, щоб отримати доступ до будівель, систем або даних.

Наприклад, замість того, щоб намагатися знайти вразливість програмного забезпечення, соціальний інженер може зателефонувати співробітникові та видати себе за службу IT-служби, намагаючись обдурити працівника, щоб розголосити його пароль.

Методи несанкціонованого доступу до інформації можна умовно поділити на дві категорії: з використанням методів соціальної інженерії та без них. На відміну від другого випадку, коли зловмисник повинен володіти знаннями у галузі IT, у першому для отримання конфіденційних даних він спирається на знання з соціології та психології.

Ключові слова: Фішинг, Претекстинг, «Дорожнє яблуко», інформація

Психологічною передумовою застосування методів соціальної інженерії є така особливість людської психіки, як когнітивні упередження. Через це надійність комп'ютерної системи є не вищою, ніж надійність її оператора. Зловмисники проникають навіть у добре спроектовані, захищені комп'ютерні системи, скориставшись неуважністю довірених користувачів або умисно вводячи їх в оману (наприклад, відрекомендувавшись системним адміністратором або амбасадором комерційного бренду, надсилають повідомлення із запитом паролів).

Існують різні типи кібератак, наприклад, уведення шкідливого коду у код веб-сайту або застосування шкідливих програм (вірусів, троянів тощо). Атаки такого виду перешкоджають керуванню пошкодженим продуктом або його налагодженню. Що ж стосується соціальної інженерії, то цей тип атак спрямований не безпосередньо на комп'ютерну систему, а на її користувачів — «найслабшу ланку», і шляхом обходу інфраструктури, призначеної для захисту від шкідливих програм, він дозволяє досягти тих же результатів, що й інші види

кібератак. Оскільки такі прийоми значно складніше виявити чи запобігти їм, цей напрям атак є набагато ефективнішим за інші.

Основна тактика соціальної інженерії - за допомогою психологічних методів, наприклад, спілкуючись начебто від імені сервісної компанії чи банку або переконати користувача розкрити інформацію особистого характеру такі як паролі, номери кредитних карток тощо.

Претекстинг. У Великій Британії також використовується термін blagging чи bohoing, полягає у застосуванні заздалегідь розробленого сценарію (приводу, чи претексту), щоб спонукати вибрану жертву до розголошення інформації чи виконання дій, до яких у звичайних обставинах вона не вдалася б. Оскільки цей метод ґрунтується на спланованій схемі обману, то атакуванню передує збір інформації, необхідної шахраєві для того, аби видати себе за іншу особу (з'ясування дати народження, паспортних та інших ідентифікуючих даних, суми останнього рахунку тощо), щоб у жертви не виникло сумнівів у законності дій шахрая[1].

Фішинг - це метод заволодіння інформацією приватного характеру обманним шляхом. Зазвичай фішер надсилає електронний лист начебто від імені офіційної установи — банку чи платіжної системи — із запитом про «верифікацію» інформації та попередженням про настання певних негативних наслідків у разі невиконання зазначених вимог. Такий лист, як правило, містить посилання на підробну веб-сторінку, схожу на справжню (із логотипами компанії, аналогічним контентом та ін.), де від користувача вимагається ввести у форму особисті дані, від домашньої адреси до PIN-коду банківської платіжної картки.[1]

Телефонний фішинг - це один з найстаріших методів соціальної інженерії. Телефонний зв'язок забезпечує унікальні можливості для проведення соціотехнічних атак і є звичним і знеособленим засобом спілкування, оскільки жертва не може бачити зловмисника. Основні цілі таких атак:

- Запит інформації, яка забезпечує доступ до самої телефонної системи або дозволяє отримати віддалений доступ до комп'ютерних систем.

- Отримання можливості здійснювати безкоштовні дзвінки.
- Отримання доступу до комунікаційної мережі.

Запит інформації чи доступу по телефону є порівняно безпечним видом атаки для зловмисника. Якщо жертва починає підозрювати щось чи відмовляється виконувати запит, зловмисник завжди може покласти трубку. [1]

Дорожнє яблуко. Метод атаки «Дорожнє яблуко» схожий на дію троянської програми. Зміст атаки в тому, щоб підкинути співробітнику компанії фальшивий фізичний носій інформації (флеш-накопичувач, тощо). Носій має виглядати як офіційний, мати логотип чи надпис, що зацікавить співробітника, наприклад флеш-накопичувач з надписом «заробітна плата 2017—2018». Якщо співробітник вставить такий носій до комп'ютеру, що має зв'язок з корпоративною мережею підприємства, запускається шкідливий код і зловмисник отримує доступ до одного комп'ютера чи до усієї мережі. [2]

Література:

1. *В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа (2015). У В. Б. Толубко (загальна редакція). Інформаційна кіберберзпека: соціотехнічний аспект. Київ: Державний університет телекомунікацій. ISBN 978-966-2970-86-9.*
2. *Markus Jakobsson, ред. (2016). Understanding social engineering based scams. New York, NY: Springer Science+Business Media. ISBN 978-1-4939-6455-0.*

ПРОГНОЗ РИНКУ МІЖМЕРЕЖЕВИХ ЕКРАНІВ ДО 2026

Корнецький Д. С.
Студент Державного університету телекомунікацій
м.Київ, Україна

Сьогодні зростаюча кількість проблем з мережею і конфіденційністю сприяє збільшенню кількості загроз. Крім цього в зв'язку з пандемією COVID-19 все більше людей стало використовувати цифрові методи ведення бізнесу через, що виріс відсоток атак на корпоративну пошту. Отже, щоб уникнути компрометації корпоративних мереж, важливо добре пов'язане поєднання мережевих брандмауерів, захисту електронної пошти і передових методів роботи персоналу. Це, в поєднанні з доступністю декількох виробників брандмауерів мережевої безпеки, призвело до збільшення розміру ринку брандмауерів мережевої безпеки.

Ключові слова: міжмережевий екран, брандмауер, фаервол, ринок, прогноз.

За прогнозами, обсяг світового ринку міжмережевих екранів для мережевої безпеки досягне 5138,1 мільйона доларів США до 2026 року в порівнянні з 3364 мільйонами доларів США в 2020 році при середньорічному темпі зростання 7,3% протягом 2021-2026 років.

Основними факторами, що визначають розмір ринку міжмережевих екранів мережевої безпеки, є збільшення числа центрів обробки даних, зростання використання IP-відео та віртуалізації, а також оптимізація мережі як хмарної послуги.

У зв'язку з пандемією COVID-19 різні уряди і регулюючі органи вимагають, щоб як державні, так і приватні організації застосовували нові методи і підтримували соціальну дистанцію. З тих пір цифрові способи ведення бізнесу стали новим планом забезпечення безперервності бізнесу для різних організацій. Організації стикаються зі зростанням атак на корпоративну електронну пошту, коли злочинці видають себе за офіційні особи, намагаючись обманом змусити людей поділитися обліковими даними для доступу до свого облікового запису або відкрити шкідливі вкладення електронної пошти. Отже, щоб уникнути компрометації корпоративних мереж, важливо добре пов'язане поєднання мережевих брандмауерів, захисту електронної пошти і кращих практик серед персоналу. Очікується, що це, в свою чергу, збільшить зростання ринку міжмережевих екранів для мережевої безпеки.

Прогнозується більш широке поширення хмарних сервісів, що в свою чергу, збільшить зростання ринку міжмережевих екранів для мережевої безпеки. Бізнес-організації постійно мають потребу в захисті своїх даних, що зберігаються на хмарній платформі. У центрах обробки даних такі дані у більшій безпеці, ніж у віртуальній хмарній мережі. Тому захист даних розглядається як одна з основних проблем для організацій при впровадженні хмарних технологій. Таким чином, хмарні міжмережеві екрани відіграють вирішальну роль в реалізації захисту даних. Серед іншого, ці рішення пропонують різні функції, такі як веб-фільтрація, безпеку електронної пошти та управління мережевим трафіком.

Очікується, що протягом прогнозованого періоду найбільша частка ринку міжмережевих екранів мережевої безпеки буде належати Північній Америці. У Північній Америці країни переживають поступове зростання кібератак, тому інвестиції у зміцнення захисту допомогли регіону зайняти найбільшу частку ринку міжмережевих екранів мережевої безпеки.

Протягом прогнозованого періоду найбільша частка ринку буде належати сегменту рішень брандмауера SMS. Це пов'язано зі зростаючим числом телекомунікаційних компаній, які впроваджують рішення для обміну повідомленнями A2P. Крім того, рішення брандмауера SMS використовуються для виявлення шкідливих програм в мережі оператора в додатках брандмауера мережевої безпеки.

В Азіатсько-Тихоокеанському регіоні буде спостерігатися найвище зростання ринку міжмережевих екранів для мережевої безпеки. В Азіатсько-Тихоокеанському регіоні спостерігається складне і динамічне прийняття нових технологій, і він завжди був прибутковим ринком для постачальників телекомунікаційних послуг. У зв'язку з постійною зміною мережевих операторів телекомунікаційний сектор в Азіатсько-Тихоокеанському регіоні значно розширився. У країнах регіону є велика кількість операторів мобільного зв'язку, які використовують звичайні мережеві екрани або міжмережеві екрани першого покоління, які не можуть забезпечити повний захист мережі від шахрайських механізмів SS7 і протоколу діаметра.[1]

Література:

1. *Network Security Firewall Market Size is Projected to Reach USD 5138.1 Million by 2026 - Valuates Reports [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.prnewswire.com/news-releases/network-security-firewall-market-size-is-projected-to-reach-usd-5138-1-million-by-2026---valuates-reports-301158803.html.*

ЗАГАЛЬНА ХАРАКТЕРИСТИКА МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Семенова І. Д.
студентка БСДМ-51
Державний університет телекомунікацій
м. Київ, Україна

В умовах форсованого формування глобального інформаційного простору і розвитку інформаційного суспільства, широкого використання інноваційних технологій в телекомунікаційних системах та мережах, а так само при впровадженні та реалізації високорівневих інформаційних послуг особливого значення набувають проблеми інформаційної та кібернетичної безпеки держави. Найбільш важливими напрямками діяльності в цій галузі є: всебічна оцінка загроз і небезпек, ідентифікація критичної інфраструктури, як в рамках держави, так і в рамках окремої інфо-системи.

Діяльність із забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які в сукупності і складають методи. Метод передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування.

1. Класифікація методів аналізу захищеності системи

Важливими методами аналізу стану забезпечення інформаційної безпеки (ІБ) є методи опису і класифікації. Для здійснення ефективного захисту тієї чи іншої системи слід описати, а тільки потім класифікувати різні види загроз і небезпек, ризиків і викликів, і, відповідно, сформулювати систему заходів управління ними.

Як поширені методи аналізу рівня захищеності використовуються методи дослідження при діючих зв'язках. За допомогою даних методів виявляються причинні зв'язки між погрозами і небезпеками; здійснюється пошук причин, які стали джерелом і викликали актуалізацію тих чи інших факторів небезпеки, а також розробляються заходи по їх нейтралізації. У числі методів причинних зв'язків можна назвати наступні: метод подібності, метод відмінності, метод повідомлення подібності та відмінності, метод супутніх змін, метод залишків.

Вибір методів аналізу стану захищеності залежить від конкретного рівня і сфери організації захисту. Залежно від загрози стає можливим рішення задачі по диференціації, як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери ІБ, то в ній зазвичай виділяють сім рівнів. Фізичний (організація і фізичний захист), програмно-технічний (управління доступом, аудит, криптографія), управлінський (координація та контроль організаційних, технологічних і технічних заходів), технологічний (реалізація політики інформаційної безпеки (ПІБ)), призначений для користувача (реалізація ПІБ спрямована на зменшення рефлексивного впливу на об'єкти ІБ, запобігання інформаційного впливу з боку соціального середовища), мережевий (політика реалізується в форматі координації дій компонентів системи управління) і процедурний (вжиття заходів реалізуються людьми: управління персоналом, підтримання працездатності і т.д.).

2. Класифікація методів забезпечення інформаційної безпеки

• Однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою;

• Багаторівневі методи будуються на підставі декількох, кожен з яких служить рішенням власної завдання, при цьому приватні технології не пов'язані між собою і спрямовані тільки на конкретні чинники інформаційних загроз;

• Комплексні методи - багаторівневі технології, об'єднані в єдину систему координуючими функціями на організаційному рівні з метою забезпечення ІБ, виходячи з аналізу сукупності факторів небезпеки, які мають семантичну зв'язок або генеруються з єдиного інформаційного простору;

• Інтегровані високоінтелектуальні методи - багаторівневі, багатокомпонентні технології, побудовані на підставі потужних автоматизованих інтелектуальних засобів з організаційним управлінням.

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якій стадії управління погрозами. До таких стадій відносяться: прийняття рішення щодо визначення області і контексту

інформаційної загрози і складу учасників процесу протидії; прийняття загальної стратегії і схеми дій; управління інцидентами і т.д.

3. Методи забезпечення інформаційної безпеки

Специфіка використовуються методів значною мірою залежить від суб'єкта діяльності, об'єкта впливу, а також переслідуваних цілей.

Дуже важливим є *застосування аналітичних методів пізнання і дослідження стану суспільної свідомості* в сфері ІБ. Необхідно донести, що зараз важливою умовою забезпечення ІБ є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність і захищеність від різних загроз - система повинна адекватно реагувати і гарантувати ефективну діяльність.

Одним з методів забезпечення ІБ є *метод розвитку* . Оскільки, загроза і небезпека є атрибутивними компонентами системи ІБ, то їх реалізація і неминучі негативні наслідки служать імпульсом і керівництвом до вдосконалення системи і підвищення рівня її захищеності.

Основним методом аналізу інформаційних ризиків є кількісний і якісний аналіз, факторний аналіз і ін .; мета якісної оцінки ризиків - ранжувати інформаційні загрози і небезпеки за різними критеріями, система яких дозволить сформувати ефективну систему впливу на них.

Важливим методом забезпечення ІБ є також *метод критичних сценаріїв* . У зазначених сценаріях аналізуються ситуації, коли уявний противник паралізує систему управління і відповідно знижує здатність підтримувати систему в межах оптимальних параметрів.

Також можна вказати на *метод моделювання* , за допомогою якого доцільно навчати майбутніх фахівців в сфері інформаційної безпеки розвиваючи практичні навички захисту систем шляхом моделювання форм інформаційних атак властивих інформаційній війні.

Серед методів забезпечення ІБ важливу роль відіграє *метод дихотомії* : для протидії загрозам інформаційної безпеки приймаються необхідні заходи як в напрямку надання певного впливу на джерело загрози, так і в напрямку

зміцнення об'єкта безпеки. Відповідно, виділяють дві предметні області протидії: одна - сукупність джерел загроз, а інша - сукупність заходів щодо забезпечення інформаційної безпеки об'єкта.

Захист інформації не обмежується технічними методами, для ефективного забезпечення ІБ важливо різноманітність моделей і методів оцінки загроз. Для успішного проектування, реалізації та підтримки захищеної системи важливо розуміти характер, природу, сутність і зміст загроз і небезпек; вміти вчасно ідентифікувати їх джерела і знаходити засоби протидії; знати способи мінімізації негативних наслідків реалізації загрози; володіти навичками управління наслідками інцидентів для відновлення коректного функціонування системи, а так само для подальшого розвитку і вдосконалення, функціональних можливостей захисту системи.

Література:

1. *Ліпкан В.А. Національна безпека України: навчальний посібник. Київ: КНТ, 2009 – 576 с.*
2. *Доктрина інформаційної безпеки України від 1.05.2014*
3. *Кавун С.В. Інформаційна безпека. Навчальний посібник. Харків: ХНЕУ, 2008. - 352 с.*

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

Бойко А. О.
студентка БСД-42
Державний університет телекомунікацій
м. Київ, Україна

Хмарні сервіси — новітній вид мережевих послуг, які дозволяють інформаційними засобами віртуального середовища розширити програмно-технічні ресурси комп'ютерного пристрою користувача. Поява хмарних сервісів стала можливою у процесі розвитку технологій хмарних обчислень (англ. Cloud Computing), які реалізуються за умов динамічного масштабного доступу до розподілених зовнішніх мережевих ресурсів. Надання такого доступу, як відокремлена послуга, залишається різновидом хмарних технологій.

Для реалізації використовують віртуальні машини, що функціонують у великих дата-центрах і замінюють собою фізичні персональні комп'ютери (ПК) та сервери. Головна відмінність від звичайного використання програмного

забезпечення в хмарних сервісах полягає в тому, що користувач може поєднувати внутрішні ресурси свого комп'ютерного пристрою та програмні ресурси, які надаються йому як інтернет-сервіс. При цьому він має повний доступ до управління власними даними, але не може управляти операційною системою чи програмною базою, за допомогою яких ця робота відбувається.

Хмарні технології мають цілу низку переваг: користувач може задіяти віртуальний комп'ютер практично будь-якої конфігурації для виконання ресурсоємних завдань; може працювати в будь-якому місці за умов використання комп'ютерного пристрою, що має підключення до інтернету; користувач застрахований від збоїв у роботі пристрою і може за потреби ділитися результатами роботи з іншими користувачами. Для організацій перевагою використання є зниження витрат на обслуговування, підтримку, модернізацію та адміністрування комп'ютерного обладнання і програмного забезпечення.

Хмарні сервіси за формою поданн можуть бути розділені на такі категорії: додатки, платформи та інфраструктури, серед яких виділяють більш деталізовані типи: 1) як сервіс зберігання даних (Storage-as-a-Service), дисковий простір на вимогу. Ця послуга дає можливість зберігати дані в зовнішньому сховищі у «хмарі»; 2) сервіс баз даних (Database-as-a-Service), який надає можливості працювати з базами даних так, ніби система управління базами даних була встановлена на локальному ресурсі; 3) інформаційний сервіс (Information-as-a-Service), дає можливість віддалено використовувати будь-які види та архіви інформації, яка може змінюватися в часі; 4) сервіс управління процесами (Process-as-a-Service) є віддаленим ресурсом, який може зв'язати воєдино кілька ресурсів, таких як послуги або дані, що містяться в межах однієї хмари або інших доступних хмарах, для створення єдиного бізнес-процесу; 5) додаток як сервіс (Application-as-a-Service) може мати назву «програмне забезпечення як сервіс» (Software as a Service), тобто будь-який додаток або програма, які користувач може запускати через інтернет; 6) сервіс-платформа (Platform-as-a-Service) — це повна платформа, що містить додатки, інтерфейси,

бази даних, їх зберігання і тестування; 7) сервіс-інтеграція програм (Integration-as-a-Service) — можливість отримувати з хмари повний інтеграційний пакет, у тому числі програмні інтерфейси між додатками, семантичну медіацію, управління алгоритмом і дизайн інтегрованого пакета; 8) сервіс-безпека (Security-as-a-Service) — забезпечує безпечний доступ до корпоративної інформації, у тому числі ідентифікацію користувача, розпізнавання прав доступу тощо, які надаються з хмари; 9) сервіс адміністрування та управління (Management/Governace-as-a-Ser-vice) дає можливість керувати і задавати параметри роботи одного або багатьох Х.с.: топологія, використання ресурсів, віртуалізація, тимчасові параметри роботи сервісів; 10) сервіс інфраструктур (Infrastructureas a Service) надає клієнту комп'ютерні інфраструктури: сервери, системи зберігання даних, мережеве устаткування, а також програми для управління цими ресурсами; 11) сервіс-дані (Desktopas a Service) клієнти отримують повністю готове до роботи стандартизоване віртуальне робоче місце, яке кожен користувач може додатково налаштовувати під свої завдання; 12) сервіс робоче місце (Workspaceas a Service) — на відміну від попереднього сервісу дозволяє користувачеві отримувати доступ лише до програмного забезпечення, а всі обчислення відбуваються безпосередньо на ПК користувача.

За способом використання (з урахуванням прав власності) хмарні сервіси поділяють на: 1) *публічні хмари*, що використовуються безліччю компаній та сервісів. Користувачі в публічній хмарі не мають можливості управляти й обслуговувати ці хмари, вся відповідальність з цих питань покладена на власника хмари. Абонентом такого сервісу може стати будь-яка компанія чи індивідуальний користувач; 2) *приватні хмари*, що контролюються та експлуатуються в інтересах єдиної організації. Організація може керувати приватною хмарою самостійно чи доручити це завдання зовнішньому підряднику; 3) *гібридні хмари*, що використовують особливості публічної та приватної хмари при вирішенні поставленого завдання. Такий тип хмар часто використовують, якщо організація має сезонні періоди активності; якщо внутрішня інфраструктура не справляється з поточними завданнями, частина

потужностей перекидається на публічну хмару, а також для надання доступу користувачам до ресурсів підприємства (до приватної хмари) через публічну хмару.

Таблиця 1. Основні принципи безпеки для хмарних сервісів

№ з/п	Принципи	Коротка характеристика принципів
1.	Прозорість	Компанії-провайдери розкривають внутрішні правила обробки інформації, а також відомості про діяльність
2.	Обмеження за сферами використаня	Компанії не претендують на володіння даними замовників і можуть використовувати їх лише в тих цілях, для яких вони були отримані від замовників
3.	Розкриття	Компанії розкривають дані замовників лише у випадку, якщо це потрібно самим замовникам або передбачено законом, і повинні в такому разі попередньо повідомляти замовників про розкриття даних на вимогу правоохоронних органів у тій частині, наскільки це дозволяє законодавство
4.	Система управління безпекою	Компанії володіють потужною системою захисту даних, що відповідає міжнародним стандартам (таким, як ISO 27002)
5.	Додаткові можливості у сфері безпеки	Компанії зобов'язуються пропонувати замовникам додаткові можливості щодо захисту їх даних
6.	Розміщення даних	Компанії надають замовникам список країн, в яких розміщуються пов'язані з ними дані
7.	Повідомлення про витоки інформації	Компанії оперативно повідомляють замовників про всі відомі витоки, які ставлять під загрозу конфіденційність або цілісність даних
8.	Аудит	Компанії звертаються до послуг сторонніх аудиторів з метою перевірки того, наскільки їх система управління безпекою відповідає вимогам відповідних стандартів
9.	Переносимість даних	Компанії надають замовникам можливість вивантаження даних у стандартному форматі, придатному для передавання через Інтернет
10.	Звітність	Компанії співпрацюють із замовниками в адекватному розподілі обов'язків під час складання звітності «Про приватність і безпеку»

Література:

1. *Softwareon-demand, Platform as a service, Infrastructure as a service, Google Apps Education Edition. — Режим доступу: World Wide Web. – URL: http://www.google.com/a/help/intl/en/edu/index.html*

МІЖМЕРЕЖЕВІ ЕКРАНИ НАСТУПНОГО ПОКОЛІННЯ

Герніченко Г. Д.
студент БСД-42
Державний університет телекомунікацій
м. Київ, Україна

Міжмережеві екрани наступного покоління (NGFW) є частиною технології брандмауера третього покоління, що реалізована в програмному забезпеченні і здатна виявляти і блокувати складні атаки, застосовуючи політики безпеки на рівні додатків, портів і протоколів.

NGFW зазвичай мають додаткові функції:

- розпізнавання додатків;
- вбудовані системи попередження вторгнень (IPS);
- контроль користувачів та груп користувачів;
- мостовий та маршрутизований режими;
- здатність застосування зовнішніх джерел інформації.

Таким чином, більшість брандмауерів наступного покоління мають в собі наступні функції: можливості міжмережевого екрану, систему попередження вторгнень і контролю додатків.

Подібно введенню перевірки з відстеженням стану в традиційних брандмауерах, новітні функції вносять додатковий контекст в процес прийняття рішень брандмауером наступного покоління, надаючи йому можливість розуміти деталі трафіку веб-додатків, що проходить через нього, і вживати заходів з блокування трафіку, що може бути потенційно небезпечним.

Різноманітні функції брандмауерів наступного покоління створюють різноманітні переваги, які можливо індивідуалізувати для кожного користувача. NGFW часто можуть блокувати небезпечне ПЗ до того, як воно опиниться в мережі, що недоступно для стандартних міжмережевих екранів. Брандмауери наступного покоління краще пристосовані до протидії розвиненим постійним загрозам (APT), оскільки вони можуть бути оснащені службами розіедки загроз, також вони можуть являти собою недорогий варіант базового захисту пристроїв, за рахунок використання обізнаності про додатки, інспекційних служб, систем захисту та засобів інформування.

Існує три основних критерії при виборі міжмережевого екрану наступного покоління: якість захисту, ціна, швидкодія. Якість захисту визначається набором вбудованого функціоналу, та якістю кожного окремого елемента, бо в NGFW кожний елемент безпеки доповнює інший (наприклад, сендбокс допомагає URL фільтрації). Наразі більшість виробників NGFW встановлюють приблизно однакову ціну, тому варто шукати оптимальний продукт від різних компаній-виробників. Швидкодія більше залежить саме від елементів мережі, тому варто постійно оновлювати обладнання і обирати саме той продукт, що підходить під вашу мережу. Трійка лідерів серед виробників Брандмауерів наступного покоління: Palo Alto NWs, Check Point, WatchGuard.

Література:

1. *What is next-generation firewalls — Режим доступу: World Wide Web. – URL: https://searchsecurity.techtarget.com/definition/next-generation-firewall-NGFW*
2. *Межсетевой экран следующего поколения (NGFW): критерии выбора firewalls — Режим доступу: World Wide Web. – URL: https://www.securitylab.ru/analytics/511475.php*

МЕТОДИ ВИЯВЛЕННЯ ТА ОБХОДУ ІЗОЛЬОВАНИХ ВІРТУАЛЬНИХ СЕРЕДОВИЩ

Каленський Ю. М.
студент БСД-42
Державний університет телекомунікацій
м. Київ, Україна

Ізольоване віртуальне середовище (або пісочниця) – механізм безпечного виконання програм. Пісочниці використовуються для запуску неперевіреного коду з невідомих джерел та виявлення вірусів чи закладок. Пісочниця не заміняє міжмережевий екран чи антивірусне ПЗ, а є наступною лінією оборони проти 0-day, цільових атак та інших загроз.

Найчастіше техніки обходу пісочниць та виявлення засобів аналізу впроваджують в шкідливе програмне забезпечення (далі ШПЗ) для віддаленого доступу і завантажувачі. Це пояснюється тим, що подібні програми використовуються як раз у розвідці та зборі інформації про цільову систему. Якщо зловмисники виявлять, що ШПЗ почало виконання у віртуальному середовищі, то вони не стануть розвивати цей вектор атаки і завантажувати шкідливе навантаження, а постараються приховати свою присутність, припинивши роботу.

Найпопулярнішими методами виявлення то обходу засобів віртуалізації (пісочниць) є [1]:

- Перевірка запущених процесів

Перед завантаженням шкідливого навантаження ШКЗ перевіряє список запущених процесів. Критерії можуть бути різними – від кількості запущених процесів до пошуку визначених процесів, наприклад «vmtoolsd», «vbox.exe» та інші.

- WMI-запити

При створенні ШПЗ зловмисники з 2016 року активно використовують запити Windows Management Instrumentation (WMI) – технологія для централізованого управління різними частинами комп'ютерної

інфраструктури під управлінням Windows для звернення до пристроїв, облікових записів, сервісів, процесів, мережних інтерфейсів та інших програм. Найбільш часто зустрічаються перевірки використовуваних моделей жорсткого диска, материнської плати, версій ОС, BIOS. Також можна виділити перевірку температури процесора і стан та статистику роботи кулера процесора.

- Перевірка значень ключів реєстру

Частина ШКЗ зчитує значення ключів реєстру і шукає в них підрядки, що вказують на використання засобів віртуалізації. Наприклад: зчитуються значення ключів реєстру System\CurrentControlSet\Enum\IDE та проводиться пошук підрядків продуктів віртуалізації QEMU, VirtualBox, VMware і Xen.

- Інші перевірки середовища

Крім перегляду запущених процесів, перевірки значень ключів реєстру і використання WMI-запитів, зловмисники використовують і інші способи перевірки оточення. Наприклад, проводиться пошук папок чи файлів з певною назвою на диску C; перевіряється наявність специфічних бібліотек; перевірка дати й часу; визначається розмір жорсткого диску (частіше всього, віртуальні середовища мають обмежену кількість простору жорсткого диску).

Отже, зловмисники в своєму арсеналі мають значну кількість методів виявлення засобів віртуалізації, і їх кількість та складність буде тільки зростати. Проте, спеціалісти з кібербезпеки також не стоять на місці та продовжують впроваджувати нові варіанти приховування віртуалізації.

Література:

1. *Обнаружение и обход песочниц. Как изменилось вредоносное ПО за 10 лет [Електронний ресурс]. Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/antisandbox-technics/?sphrase_id=84297.*

БЕЗПЕКА ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

Алексеєнко О. А.
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ, Україна

Актуальність інформаційної безпеки за останні роки почала особливо стрімко зростати. Проте головними темами розмов стають хмарні, веб, мережеві та інші технології, які розглядаються в контексті безпеки. Нажаль ці дискусії не розглядають питання вбудованих застосувань, систем, особливо, якщо вони мають обмежені ресурси. Отже, хотілось би розглянути деякі тенденції та їх особливості в області інтернету речей.

Вбудована система – система, що буде працювати, будучи вбудованої безпосередньо в сам пристрій, яким вона призначена керувати. Важливо розуміти, що навіть, якщо пристрій створений на одному чіпі з мінімальною обв'язкою, він буде працювати як кінцевий пристрій (можливо одноплатний все ж буде потребувати мінімальної периферії проте суть залишається одною).

Зазвичай, компанія-виробник випускає кінцевий пристрій, що одразу включає в себе, по-перше, «залізо», по-друге, як обов'язковий додаток, сам софт. Очевидно. Що купуючи смартфон, йде розрахунок на наявність на ньому відповідного ПЗ з усіма необхідними додатками. Тому розробники виконують увесь спектр проектувальних робіт, щодо своїх пристроїв, будь то програмні або апаратні.

Ще однією особливість розробки вбудованих систем є те, що вони майже усі мають обмежені ресурси. Тобто на цих системах не завжди присутня ОС, не кажучи вже й про більшість типових для більшості технологій. Через це виникає необхідність економити, в тому числі це впливає і на безпеку – більшість стандартів або не підтримуються, або працюють з обмеженнями. Значну кількість технологій реалізувати своїми силами або майже не можливо, або занадто дорого. Через це важливо, щоб розробник цих чіпів слідкував за тенденціями, підтримував сучасні технології. Наприклад, апаратний AES з'явився досить давно майже у всіх, то підтримку TLS/DTLS багато хто наразі не вміє забезпечувати.

Окрім цього, основною мовою розробки вбудованих систем виступає *C*, який відомий своїми недоліками відносно до роботи з пам'яттю, що напряму впливає на безпеку.

В рамках розгляду питання безпеки вбудованих систем важливо і розуміти групу застосувань, які підпадають під вимоги стандартів функціональної безпеки: промислова, медична, автомобільна, залізнична автоматизація. Тобто області, що мають безпосередній вплив на здоров'я людини, або на системи, які не можливо просто взяти та зупинити. В таких сферах все чітко регламентовано на кожному етапі розробки. Апарати, на

яких відбувається розробка, спеціалізовані та потребують сертифікації. Отже, на виході це виходить дуже дорого і займає багато часу. Тому ті, хто починають розробку, зазвичай, не замислюються про ці питання, якщо одразу не були визначенні обов'язкові до виконання стандарти.

Існують загалом 4 етапа захисту пристроїв інтернет речей:

1. **Безпечне завантаження(Security Boot)** – перевіряється, чи є прошивка справжньою, чи не була вона змінена, а також не може бути знижена у версії.
2. **Безпечне оновлення прошивки через повітря(Secure FOTA)** – можуть бути завантажені лише аутентифіковані і перевірені оновлення; майбутні загрози безпеки можуть бути усунені(збереження контролю над оновленням).
3. **Безпечні фізичні інтерфейси та API** – тільки авторизовані користувачі можуть отримувати доступ «отладки» до пристрою, де кожний доступ є унікальним; блокує «розробку» закладок та забезпечує авторизоване використання API; дані автентифіковані та захищені цілісністю в обох направленнях – ззовні та всередині модулю.
4. **Захищений транспортний рівень –** пристрій може бути автентифіковувати та підписувати або шифрувати повідомлення з сервером; нема атак посередника (Man-in-The-Middle) на шляху між пристроєм та сервером.

Для захисту пристрою пропонується идентифікувати/верифікувати дані що приходять на кожному етапі. В основі даної концепції закладена ідея кореня довіри Root-of-Trust, RoT. Її суть полягає у тому, що в пристрій вшивається деякий ідентифікатор, ключ та відбувається апаратна процедура перевірки співвідношення унікальності ключа даної платформи та коду, що виконується. Надалі всі важливі бібліотеки використовують RoT для власної роботи. Найбільш розповсюдженим рішенням на ринку являється TrustZone від ARM.

Як правило, виконуються наступні 3 етапи:

1. **Надання довіри**: включення RoT на етапі виробництва в структуру чіпа.
2. **Використання довіри:** отримання довірених ключів
3. **Гарантія довіри:** ключі використовуються для захисту будь-якої функції.

Література:

1. *«Безпека та Інтернет речей – пов'язані разом» / [Електронний ресурс] – Режим доступу: https://worldvision.com.ua/ua/articles/bezopasnost-i-internet-veshchey-svyazani-vmeste*
2. *«Безпека IoT починається з ідентифікації» / [Електронний ресурс] – Режим доступу: https://iot-ssl.com.ua/iot_secure.html*

3. *«Root-of-Trust для IoT и другие тенденции безопасности устройств интернета вещей» / [Електронний ресурс] – Режим доступу: https://habr.com/ru/post/499662/*
4. *«Trusted Platform Module» / [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Trusted_Platform_Module*

РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ НА ЕТАПАХ ПРОЕКТУВАННЯ WEB-ДОДАТКУ. WEB 2.0

Хмелевський Р.М, Кисельов О. В.
студент БСД-44
Державний університет телекомунікацій
м. Київ, Україна

В роботі проаналізовано методи написання захищеного коду під час проектування Web-додатку із використанням мови програмування JavaScript. JS вже на протязі довгих років входить в п'ятірку мов програмування, які користуються попитом. Після того як JS підкорив увесь фронтенд, він не зупинився і перейшов на сторону серверу - NodeJS, і, навіть, складає конкуренцію Python і Java в Machine Learning. Із розвитком нових технологій, розвиваються і можливості зловмисників. Використання JavaScript в зловмисних цілях може являти собою небезпеку витоку інформації, що спричинить фінансові та репутаційні втрати бізнесу, а, можливо - і повну ліквідацію. Але і ненавмисне використання мови програмування може до цього призвести. Наприклад, халатність або необізнаність розробника стосовно "best practices" по написанню захищеного коду.

Зараз, у 2021-ому році написані тисячі "готових рішень" в якості бібліотек та фреймворків для написання сучасного веб-додатку з великою кількістю нових можливостей, чого не було раніше. Одним із таких відомих і актуальних фреймворків є React - розробка компанії Facebook, яку вони спочатку створили для використання всередині компанії, а потім представили світу.

Більшість сучасних веб-сайтів створені за принципом SPA(Single Page Application) - це, по суті, остання революція в розробці Web-додатків. SPA мається на увазі, що браузер не робить велику кількість запитів на сервер для отримання інформації, як раніше. Натомість - браузер завантажує одну HTML-сторінку, розбиту на розділи, а JavaScript код в свою чергу, що працює у Web-браузері, викликає різні API(Application Programming Interface) на сервері, які повертають дані. Потім, бібліотеки JavaScript беруть ці дані та оновлюють HTML на сторінці відповідно до логіки презентації контенту в

коді. Чим більше інтерактивності відбувається на стороні клієнта, тим більше потрібно коду JavaScript, щоб ці інтерактивні елементи функціонували належним чином. І чим більше написано коду, тим важливіше мати чисту та добре спроектовану кодову базу. І саме в цьому полягає проблема, яку допомагають вирішити фреймворки JavaScript - кожна зі своїм підходом. Існує багато фреймворків з відкритим кодом JavaScript, які допомагають створювати SPA, такі як Angular, React, Ember, Aurelia, Vue.js, Cycle.js та Backbone.

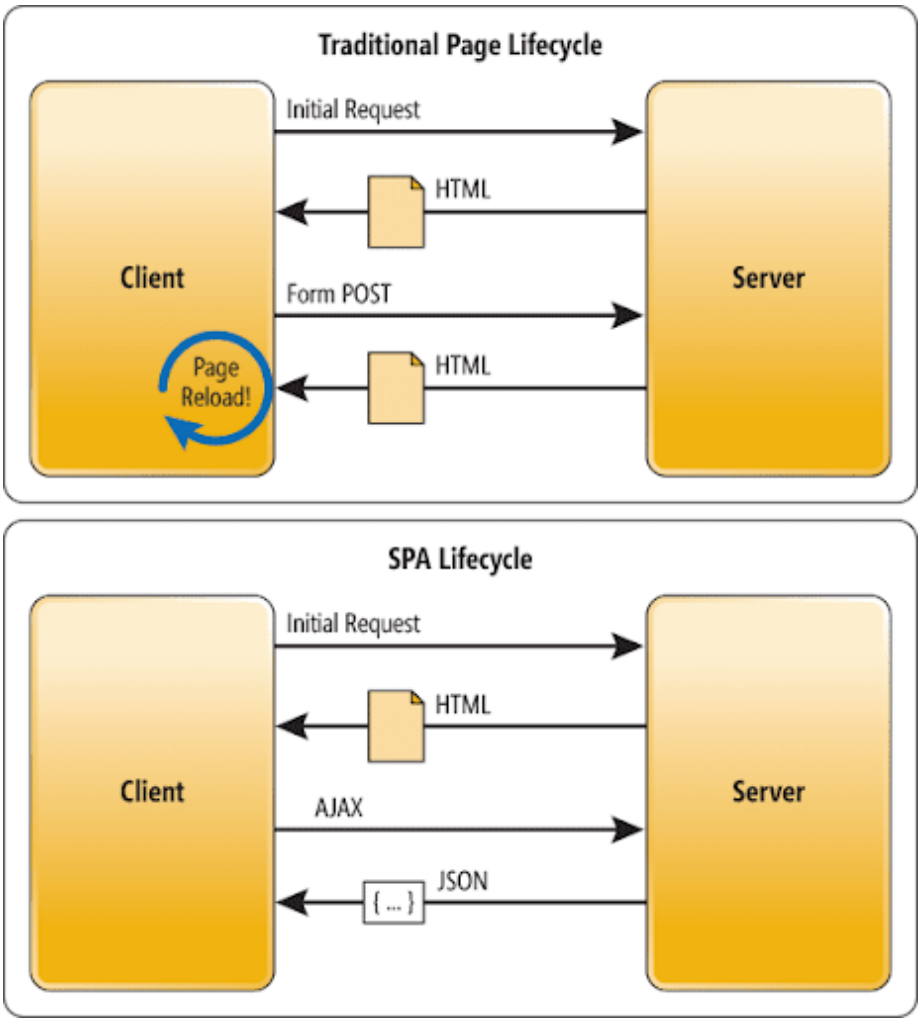


Рис.1. Принцип роботи SPA

Проте ті ж проблеми безпеки властиві і в SPA. Якщо ви використовуєте традиційний Web-сайт, вам потрібно захистити окремі сторінки на сервері, тоді як в SPA-додатку, ви повинні захистити кінцеві точки даних.

Найпоширенішими проблемами захисту інформації,з якими стикаються Single Page Application є:

● Cross Site Scripting(XSS) - виникають, коли вразливий додаток дозволяє вводити та виконувати довільний код JavaScript на сторінці. Це часто відбувається через поля форми на сторінці.

● Cross Site Request Forgery (CSRF) - відбувається, коли шкідливий Web-додаток змушує веб-браузер користувача виконувати небажані дії на надійному веб-сайті, на якому користувач вже автинтифікувася і сесія є активною. CSRF виникає, коли шкідливий веб-сайт має посилання або форму, яка підключається до іншого веб-сайту, на який ви вже увійшли.

Створюючи додатки у стилі SPA, використовуючи такі фреймворки, як Angular, Ember, React тощо, люди вважають, що це найкращі практики аутентифікації та управління сеансами. Ось декілька пропозицій, які рекомендують як найкращі методи захисту односторінкових додатків:

● SSL - шифрування

● Використання токенів із обмеженим терміном дії - користувач надсилає ім’я користувача та пароль, а натомість отримує маркер, який можна використовувати для автентифікації запитів

● Відокремлення конфіденційних даних до окремої зони

SPA повинні використовувати параметр "state", щоб захиститися від атаки CSRF та атак обміну кодами авторизації і ПОВИННІ використовувати унікальне значення для кожного запиту авторизації. У веб-браузері є кілька варіантів зберігання токенів. Ви можете зберегти їх у файлах cookie, або зберегти у сховищі HTML5 (sessionStorage або localStorage), або зберегти в пам'яті браузера. Тож який найбезпечніший варіант? Файли cookie будуть найменш безпечним варіантом серед трьох, оскільки вони вразливі як до атак між сайтами (XSS), так і до атак із фальсифікацією запитів (CSRF). Сховище HTML5, до якого можна отримати доступ через JavaScript вразливе до атак XSS. Нарешті, у нас є опція пам’яті браузера, яка є рішенням, побудованим за допомогою Web Workers, і вважається найбільш безпечним варіантом.

Рішення на основі Web Workers є більш безпечним, оскільки Web Workers працюють в іншому глобальному контексті, який відрізняється від поточного вікна. Отже, неможливо отримати доступ до маркерів, що зберігаються у Web Worker, використовуючи JavaScript, запущений у браузері.

Із покращенням технологій, пропорційно потрібно покращувати їх системи захисту. Це стосується новітніх технологій, таких, як Web 2.0.

Web 2.0 — друге покоління мережних сервісів, що останнім часом стали основою розвитку мережі Інтернет. Принциповою відмінністю технології Web 2.0 від технологій Web 1.0 (першого покоління сервісів мережі Інтернет), є те, що її використання дає змогу не лише переглядати веб-ресурси мережі, а й завантажувати власні, здійснювати обмін цими ресурсами з іншими користувачами, діяти спільно з метою їхнього накопичення, брати участь в обговореннях та ін.

Сьогодні термін Web 2.0 швидше означає не стільки сукупність певних конкретних технологій, а філософію представлення інформації у веб-орієнтованому середовищі та побудову інформаційних відношень.

Технології Web 2.0 справедливо називають соціальними сервісами мережі Інтернет, оскільки їх використання зазвичай здійснюється спільно в межах відповідної групи користувачів. Найпопулярніші ресурси, які генерують найбільшу кількість трафіку і найактивніше використовують динамічний контент Веб 2.0, є найбільш вразливими для атак. Так, згідно з дослідженням Websense, більш 60% сайтів, що входять в список 100 найбільш відвідуваних ресурсів, містили шкідливий контент або приховані механізми перенаправлення на сайти підвищеного ризику. Динамічний контент Веб 2.0 не може відслідковуватися існуючими технологіями безпеки, такими як бази даних репутацій і системи URL-фільтрації. Це ставить перед відділами інформаційної безпеки складну задачу: надати співробітникам можливість використання потужного потенціалу другого покоління Інтернету і, в той же час, забезпечити безпеку мережі, робочих місць і корпоративних даних.

Для поліпшення інформаційної безпеки та захисту даних в форматі технології Web 2.0 рекомендується аналізувати загрози безпеці перед шкідливими атаками, під час атак та після атак:

1) До атак: все обладнання та все програмне забезпечення , додатки та системи повинні бути сертифіковані, особливо це стосується всіх систем з відкритим кодом та власних продуктів; Все критичне програмне забезпечення повинно регулярно виправлятися та оновлюватися або якомога швидше після того, як вразливість була виявлен. Впроваджувати комплекс інформаційної безпеки та управління подіями (SIEM). Рішення віртуальної приватної мережі (VPN); Контроль доступу до мережі (IAM / NAC); Application Control.

2) Під час атак: Система запобігання вторгненню (IPS), яка є технікою, що поєднує належним чином технології брандмауера з технологією IDS. IDS - це захисна система, яка виявляє ворожу діяльність у мережі: для виявлення та, можливо, запобігання діяльності, яка може порушити безпеку системи, або триває спроба злому, включаючи етапи розвідки / збору даних, які включають, наприклад, сканування портів. Однією з ключових особливостей систем виявлення вторгнень є їх здатність надавати огляд незвичної активності та видавати сповіщення, що сповіщають адміністраторів та / або блокувати підозрюване з'єднання

3) Після атак: Системи виявлення вторгнень (IDS); Система із криміналістики; Комплекс безпеки інформації та управління подіями (SIEM).

Література:

1. *Богуш В. М., Юдін О. К.Б74 Інформаційна безпека держави. — К.: "МК-Прес", 2005.*
2. *INFORMATION SECURITY AND DEVELOPMENT PROBLEMS eGOVERNMENTSYSTEMSINUKRAINE - KhmelevskoyR., Khmelevskoy Y., Kozachok V., Semko V., Ilin O. [p.74]*
3. *https://blog.risingstack.com/node-js-security-checklist/*
4. *https://wso2.com/blogs/thesource/securing-spas-best-practices/*

ЗАХИСТ ВІД RANSOMWARE (ПРОГРАМИ-ВИМАГАЧА) ЯК ЗОВНІШНЬОЇ ЗАГРОЗИ

Вакуленко О. С.
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ, Україна

Стаття присвячена розробленню та створення короткого повідомлення про що таке Ransomware або програма-вимогач, як запобігти зараженням та як протидіяти наслідкам, якщо зараження відбулося.

Ключові слова: Ransomware, програма-виимогач, шкідливе програмне забезпечення, загроза.

Постановка проблеми: Ransomware є неперервно зростаючою та актуальною загрозою, що може приносити збитків на мільярди доларів. Основним способом розповсюдження даного типу загрози є електронна пошта.

Ransomware – це шкідливе програмне забезпечення, яке використовує шифрування для зберігання інформації жертви під викуп. Важливі дані користувача чи організації зашифровані, щоб вони не мали доступу до файлів, баз даних або програм. Потім вимагається викуп для надання доступу. Вимагаючі програми часто розроблені для розповсюдження по мережі та цільових серверів баз даних та файлів, і таким чином можуть швидко паралізувати всю організацію. *Це зростаюча загроза, яка приносить мільярди доларів виплат кіберзлочинцям та завдає значної шкоди та витрат бізнесу та урядовим організаціям.*

Ймовірність реалізації Ransomware (*i*) загрози по відношенню до j-го активу може визначатися за допомогою рівняння (1):

$$d_{rj} = \overline{1 - p_{ri}} \times \prod_{i=1}^{m} (1 - p_{rji}), \quad (1)$$

де n – кількість загроз; m – кількість активів; p_{ri} – можливість здійснення і-ої загрози; d_{rj} – можливість реалізації хоча б однієї загрози j-му активу.

У випадку загрози програми-вимагача, n може залежати від тенденцій безпеки (обізнаність користувачів, готовність вендорів безпеки до такого типу загрози).

Загальними рекомендаціями щодо захисту від програм-вимагачів є:

- Освіта: навчання користувачів способам визначення та уникнення потенційних атак програм-вимагачів має вирішальне значення. Оскільки багато з сучасних кібератак починаються з цільового електронного листа, який навіть не містить шкідливих програм, а тільки повідомлення, засноване на використанні психології, яке спонукає користувача перейти по шкідливої посиланням, навчання користувачів часто вважається одним з найбільш важливих способів захисту, який може застосовувати організація .
- Впровадити програму підвищення обізнаності щодо безпеки. Проводити регулярні тренінги з підвищення рівня безпеки для кожного члена вашої організації, щоб вони могли уникнути фішингу та інших атак соціальної інженерії. Проводити регулярні тренування та випробування, щоб переконатися, що процес навчання відбувся успішно.
- Постійне резервне копіювання даних: регулярне резервне копіювання даних в якості рутинного процесу є дуже важливою практикою для запобігання втрати даних і можливості їх відновлення в разі пошкодження або несправності дискового обладнання. Функціональні резервні копії також можуть допомогти організаціям відновитися після атак програм-вимагачів.
- Захист резервних копій: переконатися, що дані резервної копії недоступні для модифікації або видалення із систем, де містяться дані. Вимагальники шукатимуть резервні копії даних і шифруватимуть або видалятимуть їх, щоб їх не можна було відновити, тому використовуйте системи резервного копіювання, які не дозволяють прямого доступу до файлів резервних копій.

- Установка оновлень: установка оновлень є важливим компонентом захисту від атак програм-вимагачів, оскільки кіберзлочинці часто шукають свіжі розкриті експлойти в доступних оновленнях, а потім вибирають системи, що ще не були оновлені до останньої версії використовуваних програм або систем. Таким чином, дуже важливо, щоб організації забезпечували установку останніх оновлень для всіх систем, оскільки це знижує кількість потенційних вразливостей в системах компанії, які зловмисник може використовувати.

- Переконатися, що оновлення програмного забезпечення пристроїв відбувається рано і часто, оскільки виправлення для дир безпеки зазвичай містяться в кожному оновленні.

Рекомендації щодо забезпечення безпеки:

- Захист робочих станцій: звичайний сигнатурний антивірус є високоефективним рішенням для запобігання відомих атак і обов'язково повинен використовуватися в будь-якій організації, оскільки він захищає від більшості атак шкідливих програм, з якими стикається організація.

- Мережева захист: вдосконалені засоби захисту в корпоративній мережі, такі як IPS, мережевий антивірус і анти-бот, також мають вирішальне значення і ефективні для запобігання відомих атак. Передові технології, такі як «пісочниця», дозволяють аналізувати нові, невідомі шкідливі програми, запускати їх в режимі реального часу, шукати ознаки того, що це шкідливий код, і, як результат, блокувати його і запобігати зараженню робочих станцій і поширення в інших місцях організації. Таким чином, пісочниця є важливим механізмом запобігання загрозам, який може захистити від ухильних шкідливих програм або шкідливих програм нульового дня, а також від багатьох типів невідомих атак на організацію.

Рекомендації щодо пом’якшення репутаційних втрат:

- Повідомлення правоохоронних органів про напад та масштаби порушення даних.

• Своєчасне розкриття інформації та повідомлення про атаку, що відбулась.

Висновки: Загальними рекомендаціями щодо захисту від програм-вимогачів, що можуть розповсюджуватися електронною поштою, є: освіта користувачів корпоративної системи правилам безпеки, створення захищених бекапів, своєчасне оновлення програмного забезпечення.

Література:

1. *McAfee. What Is Ransomware? / Режим доступу: [https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html/]*
2. *Check Point. How to Prevent Ransomware Attacks / Режим доступу: [https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/how-to-prevent-ransomware/]*
3. *Trend Micro. Ransomware / Режим доступу: [https://www.trendmicro.com/vinfo/us/security/definition/ransomware]*
4. *Bitdefender. Что такое программы-вымогатели и что нужно знать, чтобы оставаться в безопасности? Ransomware / Режим доступу: [https://bitdefender.ru/stati/programmy-vymogateli-i-kak-but-v-bezopasnosti/]*
5. *Хмелевський Р.М. Тези. «Інформаційна безпека, як одна з основ забезпечення ефективності роботи державного управління». Матеріали міжнародної науково-технічної конференції «Сучасні інформаційнотелекомунікаційні технології» Том IV «Сучасні технології інформаційної безпеки» Київ, ДУТ. 17–20 листопада 2015 р. – С.155–158*

ТИПОВІ РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ANDROID ДЕВАЙСУ ВІД ЗАГРОЗ

Хмелевський Р.М, Бурлін М. О.
студент БСД-44
Державний університет телекомунікацій
м. Київ, Україна

Анотація. У статті розглядаються, порівнюються та аналізуються основні вектори атак на смартфони під управлінням ОС Android в якості клієнтських інтерфейсів. Даний аналіз проводиться з метою отримання базового матеріалу для розробки практичних принципів забезпечення безпеки на рівні архітектури таких систем. Виконано категоріювання можливих атак та вразливостей, що полягають в їхній основі в контексті безпеки Android додатків та з урахуванням моделі безпеки самої операційної системи і середовища. Для виконання поставлених дослідницьких завдань було проведено аналіз компонентів Android-додатку та типової інформаційної інфраструктури досліджуваних систем. що так чи інакше впливають на їхню захищеність. Проведено аналіз наявної інформації щодо розповсюджених вразливостей цих компонентів та атак, що передбачають експлуатацію даних проблем. Досліджено декілька можливих моделей порушника, що можуть виконувати атаки на інформаційну систему. В результаті

проведеного дослідження отримано аналітичні дані щодо векторів порушення цілісності та конфіденційності інформації з обмеженим доступом в інформаційних системах, що надають доступ до неї через мобільні додатки. В рамках порівняльної характеристики надається аналіз можливого впливу порушника на інформаційну систему зважаючи на його технічні можливості та поверхні атаки на кожному з визначених напрямків. Отримані теоретичні висновки щодо модифікації архітектури інформаційних систем, побудованих на базі мобільних додатків з метою підвищення їх захищеності від розповсюджених загроз інформації. Результати можуть бути використані для формування моделі загроз та порушника для додатку, що надає доступ до інформації з обмеженим доступом, розробки рекомендацій щодо реалізації тих чи інших етапів життєвого циклу інформаційної системи з метою зменшення ризиків компрометації даних, розробки технічних вимог до етапів тестування та розробки тощо.

В сучасний час гаджети є невід'ємною частиною нашого життя. Мільйони людей у всьому світі використовують смартфони для онлайн-замовлень, перевірки пошти або спілкування в соціальних мережах. Через збільшення використання мобільних пристроїв зростає кількість атак зловмисників з метою зараження і викрадення даних. У зв'язку з цим мобільну безпеку і захист телефону набувають все більшого значення. За результатами останніх досліджень було виявлено, що мобільний трафік складає 52% використання Інтернету в світі. Незважаючи на цей показник, для користувачів більш пріоритетною залишається захист ноутбука або комп'ютера ніж захист телефону.

На сьогоднішній день велика кількість компаній має робочі мобільні пристрої, які використовуються співробітниками в особистих цілях, що часто призводить до витоку конфіденційних даних підприємства. Тому мобільні девайси бізнес-організацій є найбільш привабливими для кіберзлочинців і потребують захисту в першу чергу.

У зв'язку з потенційними небезпеками фахівці ESET підготували основні рекомендації для захисту телефону від зараження шкідливими програмами.

- здійснюйте регулярне оновлення операційної системи та іншого програмного забезпечення для зменшення кількості вразливостей, через які зловмисники можуть заражати пристрої.

- використовуйте складні і унікальні паролі, а також двухфакторную аутентифікацію для захисту облікових записів Інтернет-банкінгу, пошти і соціальних мереж від несанкціонованого доступу.

- авантажуйте програми перевірених розробників. В Інтернеті Ви можете знайти більш детальну інформацію про розробника або окремий додаток, відшукати сайт або контактні дані.

- будьте обізнані з можливими функціями пристрою. Неуважне використання функції Touch ID може привести до викрадення Ваших особистих даних або навіть коштів з банківської карти.

- не відкривайте підозрілі файли і посилання в листах Вашої електронної пошти від невідомих користувачів. Зловмисники часто використовують заражені електронні листи або SMS-повідомлення для здійснення фішингових атак. Особливо велика кількість різних листів і повідомлень приходить в сезон знижок і акцій.

- будьте уважні при здійсненні онлайн-покупок. Остерігайтеся занадто спокусливих пропозицій здійснити покупку по гарячій ціні - це поширена схема викрадення грошових коштів або зараження Вашого смартфона. За статистикою, майже кожен третій відчував тиск від пропозицій «встигни придбати тільки сьогодні».

Оскільки в повсякденному житті ми все частіше користуємося смартфонами, важливим кроком до забезпечення захисту телефону є використання антивіруса. Якщо раніше телефон був пристроєм для підтримки зв'язку, то зараз це повноцінний комп'ютер, який зберігає і використовує особисту інформацію користувача у відкритому вигляді.

Дуже важливим є методи блокування смартфона, в основному за допомогою біометричних сенсорів. Сьогодні багато компаній і людей використовує смартфон як спосіб зберігання різної конфіденційної інформації від банківських рахунків до данних про співробітників. На віддаленій роботі використовують як доступ до коорпоративної мережі. Тому безпека девайсу є вкрай важлива.

Є наступні види захисту Вашого смартфону від фізичного доступу:

- Графічний ключ - такий метод блокування екрана на телефоні передбачає введення певного шаблону малюнка. Чим простіший графічний ключ, наприклад, у формі літери L, тим легше буде його відгадати або повторити.
- Pin-код або пароль - блокування телефона за допомогою пароля залишається одним з найпопулярніших методів. Якщо ви використовуєте пароль, важливо аби він складався принаймні з 8 символів та містив літери, цифри та спеціальні символи.
- Біометричний відбиток пальців - варто зазначити, що блокування телефона за допомогою відбитка пальця є одним з найшвидших та найбезпечніших методів.
- Сканування обличчя - цей метод захисту передбачає сканування обличчя користувача. І хоча на перший погляд здається, що процес є досить складним і тягне за собою велику кількість технологічних процесів;

Існує велика кількість варіантів блокування телефона, тому кожен користувач може обрати найбільш зручний для нього. Але ми рекомендуємо використовувати комбінацію з різних типів захисту. Найбільш безпечними варіантами і надалі вважаються надійний PIN-код та складний унікальний пароль, а також сканування відбитків пальців.

Література:

1. *Базові рекомендації для підвищення безпеки смартфону: веб-сайт. URL: https://eset.ua/ru/blog/view/24/bezopasnost-smartfona-rekomendatsii-po-obespecheniyu-zashchity-telefona (дата звернення: 19.03.2021).*
2. *Як надійно захистити смартфон на бахі Андроїд URL: http://www.dut.edu.ua/ua/news-1-569-8525-yak-nadiyno-zahistiti-smartfon-na-bazi-android--v-innovaciynomu-zmisti-navchannya_kafedra-cistem-tehnichnogo-zahistu-informacii (дата звернення: 19.03.2021).*
3. *Бржевська З.М, Рабчун Д.І., Драгунцов Р.І. «Принципи забезпечення безпеки архітектури операційної системи на базі клієнтських додатків на базі ОС Андроїд» - журнал «Кібербезпека» випуск №4 від 2020 р*

PHISHING

Мальгіна К.
Державний університет телекомунікацій
м. Київ, Україна

Фішингові атаки - це спроби шахраїв обманом змусити вас видати особисту інформацію, таку як номери ваших банківських рахунків, паролі і номери кредитних карт.

Шахрай зв'язується з вами, видаючи себе за представника законного підприємства, такого як банк, телефон або інтернет-провайдер. З вами можуть зв'язатися по електронній пошті, в соціальних мережах, по телефону або за допомогою текстового повідомлення.

Шахрай просить вас надати або підтвердити ваші особисті дані. Наприклад, мошенник може сказати, що банк або організація перевіряє записи про клієнтів з-за технічної помилки, яка видаляє дані про клієнтів. Або вони можуть попросити вас поповнити приватні клієнти та запропонувати приз за участь.

Крім того, шахрай може попередити вас про «несанкціонованої або підозрілої активності в ваш профіль». Вам можуть сказати, що в іншій країні була здійснена велика покупка, і запитають, чи дозволили ви оплату. Якщо ви відповісте, що немає, шахрай попросить вас підтвердити вашу кредитну карту або банківські реквізити, щоб «банк» міг провести розслідування. У деяких випадках шахрай може вже мати номер вашої кредитної картки і попросити вас підтвердити свою особу, вказавши трьох-або чотиризначний код безпеки, надрукований на карті.

Фішингові повідомлення виглядають справжніми і часто копіюють формат, який використовується організацією, яку нібито представляє шахрай, включаючи їх бренд і логотип. Вони перенаправляють вас на підроблений веб-сайт, який виглядає як справжній, але має трохи іншу адресу. Наприклад, якщо легітимний сайт - «www.realbank.com.au», шахрай може використовувати таку адресу, як «www.reallbank.com».

Якщо ви надасте шахраєві свої дані в Інтернеті або по телефону, він буде використовувати їх для здійснення шахрайських дій, таких як використання ваших кредитних карт і крадіжка ваших грошей.

Інші види фішинг-шахрайства

Китобійний промисел і цільової фішинг - шахрай націлений на бізнес, намагаючись отримати конфіденційну інформацію в шахрайських цілях. Щоб їх запит виглядав законним, вони використовують деталі та інформацію, які стосуються бізнесу, які вони отримали в іншому місці.

Фішингг - шахрай перенаправляє вас на підроблену версію законного веб-сайту, який ви намагаєтеся відвідати. Це робиться шляхом зараження вашого комп'ютера шкідливим ПЗ, яке призводить до перенаправлення на підроблений сайт, навіть якщо ви вводите реальну адресу або клацаєте посилання, додану в закладки.

Попереджувальні знаки

Ви отримуєте електронного листа, текстове повідомлення або телефонний дзвінок від банку, забезпечення сервісу оператором або іншого підприємства, з яким ви регулярно працюєте, з проханням оновити або підтвердити свої дані.

Електронне або текстове повідомлення не вдається до вам за вашим ім'ям і може містити помилки і граматичні помилки.

Адреса веб-сайту не схожий на адресу, яку ви зазвичай використовуєте, і запитує деталі, які законний сайт зазвичай не запитує.

Ви помічаєте нові значки на екрані комп'ютера або ваш комп'ютер працює не так швидко, як зазвичай.

Захистіться

Не натискайте жодних посилань та не відкривайте вкладення з електронних листів, де стверджується, що вони надійшли від вашого банку або іншої довіреної організації та просять вас оновити або підтвердити свої дані - просто натисніть видалити.

Зробіть пошук в Інтернеті, використовуючи імена або точні формулювання електронного листа чи повідомлення, щоб перевірити наявність посилань на шахрайство - багато шахраїв можна визначити таким чином.

Шукайте захищений символ. Безпечні веб-сайти можна визначити за допомогою "https:", а не "http:" на початку Інтернет-адреси, або закритого замка або значка клавіші в нижньому правому куті вікна вашого браузера. Законні веб-сайти, які просять вас ввести конфіденційну інформацію, зазвичай шифруються для захисту ваших даних.

Ніколи не повідомляйте дані своєї особистої, кредитної картки або рахунку в Інтернеті, якщо вам надходить дзвінок, який стверджує, що надійшов від вашого банку або будь-якої іншої організації. Натомість запитуйте їх ім’я та контактний номер і перед передзвоненням проведіть незалежну перевірку у відповідної організації.

Література:

1. *https://phishinsight.trendmicro.com/en/?gclid=Cj0KCQjwutaCBhDfARIsAJHWnHsxioEYX5U1tYOPSZuej0fDAqz30iY8iwvq-r7R3l-YcJd9xSaUVKAaAmkqEALw_wcB*
2. *https://www.webroot.com/us/en/resources/tips-articles/what-is-phishing*
3. *https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/*

ПРОГРАМНІ ВРАЗЛИВОСТІ, ЯК ЗАГРОЗА МЕРЕЖЕВІЙ БЕЗПЕЦІ

Марченко В. В.
асистент кафедри інформаційної та кібернетичної безпеки,

Макеєв М. В.
студент БСД-42

Навчально-науковий інститут захисту інформації
Державний університет телекомунікацій
м.Київ, Україна

В наш час інтернет та мобільні додатки посідають важливе місце у нашому житті. У цій роботі буде розглянутий вплив уразливостей у програмному забезпечені на безпеку мережі вцілому та способи протидії або мінімізації збитків.

На сьогоднішній день, інформаційна безпека є важливим компонентом сучасного життя. Інформатизація все більше проникає у всі сфери нашого життя. В свою чергу, наше оточення все активніше переходить у мережу. Усі соціальні мережі, воласники мобільних додатків та провайдери інтернет послуг стикаються з проблемою інформаційної безпеки, зокрема – мережевої безпеки. При організації роботи свого продукту, його власники так чи інакше стикаються з проблемою мережевої безпеки.

При організації безпеки мережі використовують програмно-апаратні комплекси (фаєрволи, розподільники навантаження, маршрутизатори, та ін.). Однією з важливих частин безпеки є програмне забезпечення. Для реалізації атаки на мережу потрібна уразливість яка буде використовуватися зловмисниками.

У багатьох випадках уразливості в програмах зводили нанівець усі зусилля при налаштуванні обладнання для забезпечення безпеки.

Так наприклад, для використання програмних вразливостей, може використовуватися фішинг. Він відбувається за наступним алгоритмом:

-отримання користувачем листа з експлойтом

-активація експлойту користувачем

-зараження системи шкідливим ПЗ, та/або експлуатація ним уразливості.

- отримання зловмисником доступу до системи.

У даній схемі атаки, у залежності від типу уразливості у ПЗ користувачеві в деяких випадках навіть не потрібно власноруч активовувати код або програму зловмисника. Так, наприклад, у мобільному додатку Instagram була уразливість, яка дозволяла отримати доступ до пристроїв та персональної інформації користувачів за допомогою одного зображення. Уразливість отримала кодову назву CVE-2020-1895[1]. Суть цієї уразливості полягала в тому, що клієнт на телефоні жертви намагався відобразити зображення, яке переповнювало пам’ять і в цей момент виконувався

шкідливий код, за допомогою якого зловмисник отримував доступ до пристрою жертви[2].

Таким чином, для того, щоб отримати персональні дані користувача,

зловмиснику не було потрібно проникати на захищені сервери компанії для отримання доступу до персональних даних кінцевих користувачів.

У схожих випадках ефект може посилюватися в залежності від персональних налаштувань та/або ставлення користувача/адміністратора до безпеки своїх пристроїв. Подібні випадки відкривають поле діяльності для подальших дій зловмисника. В залежності від пристрою та налаштування мережі у якій він знаходиться – під загрозою може бути ціла мережа та пристрої у ній.

Мінімізувати наслідки від подібних загроз можливо – виконуючи наступні прості кроки:

1) Своєчасно оновлювати програмне забезпечення на своїх пристроях.

2) Не нехтувати налаштуванням своїх пристроїв – а саме:

- встановлювати відповідні паролі;
- змінювати стандартні налаштування.

3) Правильне розподілення доступу.

4) Резервне копіювання даних.

5) Не передавати чутливу, конфіденційну, таємну інформацію.

Отже, беручи до уваги все вищесказане. Для того, щоб забезпечити безпеку мережі , потрібен комплекс дій. Регулярні оновлення, аудит і правильне налаштування систем та програм сприяють посиленню загальної безпеки всієї мережі та зменшують збитки від атак всіх типів, а в особливості від уразливостей, які проявляють та знахлодяться в процесі експлуатації програмного забезпечення.

Література:

1. *Instagram-аккаунты пользователей можно было взломать с помощью картинки. Р е ж и м*

2. *CVE-2020-1895. Режим доступу: [https://cve.mitre.org/cgi-*

ОСНОВНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

Атаманчук І. В.
Навчально-науковий інститут захисту інформації
Державний університет телекомунікацій
м. Київ, Україна

Однією з важливих проблем безпеки мережевого середовища є зловмисні або, принаймні, небажані спроби вторгнення в мережу, що виконуються деякими користувачами або програмним забезпеченням. Такого роду порушення з боку користувачів можуть мати форму спроб несанкціонованого доступу до комп'ютера або спроб легального користувача одержати привілеї або виконати операції, які виходять за рамки наданих йому повноважень. Під порушеннями з боку програмного забезпечення мають на увазі роботу вірусу, "черв'яка" або "троянського коня".

Усі ці порушення належать до питань захисту мереж, оскільки вхід до системи може здійснюватися за допомогою мережі. Проте ці порушення не можна віднести до чисто мережевих. Користувач, що має доступ до локального терміналу, може спробувати проникнути до системи, не використовуючи мережевих засобів. Вірус або "троянський кінь" можуть потрапити до системи з дискети. У цьому сенсі тільки "черв'як" може вважатися чисто мережевим засобом вторгнення в систему. Таким чином, питання вторгнення до системи знаходяться на перетині галузей, що належать до захисту мереж і захисту комп'ютерних систем.

Однією з двох найпоширеніших загроз безпеки є порушники (другою загрозою є віруси), яких називають хакерами (hacker) або зломщиками (cracker). Дамо класифікацію порушників[1, с.46].

- Імітатор (masquerader) – це особа, що не має права користуватися комп'ютером, але подолала механізм керування доступом і використовує

права доступу деякого легального користувача.

- Правопорушник (misfeasor) – це легальний користувач, що намагається дістати доступ до даних, програм або ресурсів, до яких він не має відповідних прав доступу, або користувач, який має в своєму розпорядженні відповідні права доступу, але використовує їх в зловмисних цілях.

- Таємний користувач (clandestine user) – це особа, що заволоділа правами керування системою і використовує ці права для обходу засобів аудиту і керування доступом або для створення перешкод у реєстрації системних подій.

Нині високотехнологічна злочинність набуває високих темпів. Загалом об'єктами зазіхань можуть бути як технічні засоби (комп'ютери і периферія), так і програмне забезпечення та бази даних, для яких комп'ютер є середовищем. У першому випадку правопорушення можна кваліфікувати за звичайними нормами права (крадіжка, грабіж, розбій і т. ін.). В інших випадках, коли комп'ютер виступає і як інструмент, і як об'єкт, злочин відносять до окремої категорії (див. розділ XVI Кримінального кодексу України).

Найбільш поширені види комп'ютерних злочинів[2]:

1. ***Підробка комп'ютерної інформації.*** Цей злочин можна вважати різновидом несанкціонованого доступу з тією різницею, що скоїти його може і стороння особа, і законний користувач, і розробник ІС. В останньому випадку може підроблятись вихідна інформація з метою імітування роботоздатності ІС і здачі замовнику свідомо несправної продукції. До цього самого виду злочинів можна віднести підтасування результатів виборів, голосувань і т. ін.

2. **Уведення у програмне забезпечення «логічних бомб»** — невеликих програм, які спрацьовують з настанням певних умов і можуть призвести до часткового або повного виведення системи з ладу. Різновидом логічної бомби є «часова бомба», яка спрацьовує в певний момент часу. Ще

одним способом модифікації програмного забезпечення є таємне введення у програму (чужу або свою) «троянського коня» — команд, які дають можливість зі збереженням роботоздатності програми виконати додаткові, не задокументовані функції, наприклад переслати інформацію (зокрема паролі), що зберігається на комп'ютері. В останньому випадку «троянській кінь» є засобом реалізації «прихованого каналу». Виявити «троянського коня» дуже важко, оскільки сучасні програми складаються з тисяч і навіть мільйонів команд і мають складну структуру. Завдання ускладнюється, коли у програму вставляється не власне «троянській кінь» (див. вище визначення), а команди, які його формують і після досягнення поставленої мети — знищують. Також можна зазначити, що «троянські коні» можуть перебувати не тільки у програмах, а й в інших файлах, наприклад в електронних листах.

3. ***Розробка і поширення комп'ютерних вірусів.*** Напевне, сьогодні не має жодного користува а ІС, який у своїй роботі не стикався б із комп'ютерними вірусами. Прояви вірусів можуть бути різноманітними — від появи на екрані точки, що світиться (так званий «італійський стрибунець»), до стирання файлів з жорсткого диска. У будь-якому разі це означає порушення цілісності ІС. Сьогодні фахівці очікують появи вірусів для програмованих мікросхем і мобільних телефонів.

4. ***Злочинна недбалість у розробці, виготовленні й експлуатації комп'ютерної техніки та програмного забезпечення.*** Необережне використання комп'ютерної техніки аналогічне недбалому поводженню з будь-яким іншим видом техніки, транспорту і т. ін. Його особливістю є те, що безпомилкових програм не буває у принципі.

Окремим випадком недбалості програмістів є створення і залишення без контролю «люків» («чорних ходів») — прихованих, не задокументованих точок входу у програмний модуль, які часто використовуються для відлагодження програми та її підтримання у процесі використання. Але «люк» може бути використаний і для зламування системи сторонньою особою, і для таємного доступу до програми самим розробником. Для

виявлення «люків» слід проводити ретельний аналіз початкових текстів програм.

Література:

1. *Захист інформації в комп'ютерних системах та мережах: Навчальний посібник. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Харків: НТУ «ХПІ», 2014*
2. *Основні види комп'ютерних злочинів. [Електронний ресурс] Режим доступу: https://studopedia.su/9_84000_osnovni-vidi-kompyuternih-zlochiniv.html*

АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЯК МЕТОД ПРОТИДІЇ КІБЕРАТАКАМ

Киричок Р. В.
ст. викладач
Ахтьоров В. Ю.
студент БСД-42
Державний університет телекомунікацій
м. Київ, Україна

На сьогодні, через активну інтеграцію інформаційних технологій в роботу приватних організацій та державних установ, стрімкого зростання кількості шкідливого програмного забезпечення та реалізації за його допомогою кібернетичних атак, гостро постає питання забезпечення швидкого виявлення та нейтралізації негативного кібернетичного впливу.

Аналіз шкідливого програмного забезпечення є одним з превентивних методів протидії кібератакам, який використовується фахівцями в галузі інформаційної та кібернетичної безпеки. Дослідження даного питання дозволяє підвищити загальну ефективність систем захисту інформації, зокрема, що стосується оцінки, прогнозування збитків від кібератак та проведення розслідувань кіберінцидентів.

Аналіз шкідливого програмного забезпечення (ШПЗ) – це дослідження або процес визначення функціоналу, походження та потенційні наслідки його функціонування в системі певного шкідливого програмного забезпечення. Аналіз ШПЗ виконує декілька функцій при протидії кібератакам: визначення точних збитків та вектору атаки в інформаційній системі, розробка методів протидії на основі інформації зібраної під час аналізу, визначення вразливостей інформаційної системи до реалізації атак певного типу.

Можна виділити два основні напрямки використання даних отриманих

при аналізі шкідливого ПЗ. Першим є формування сигнатурної бази. Сигнатура шкідливого ПЗ – це послідовність байтових даних, які характерні для даного ШПЗ. Під час аналізу файлів шкідливого ПЗ генерується сигнатура, яку можуть використовувати антивірусні ПЗ, детектори та монітори. Це допоможе в майбутньому запобігти реалізації атак на інформаційну систему.

Існують хешові (hash signature) та рядкові (string signature) сигнатури. Хешові – генерується при процесі хешування, тобто при перетворенні даних програмного забезпечення в рядок даних встановленої довжини за допомогою певного алгоритму [1]. Рядкові сигнатури являють собою короткий байтовий рядок з шкідливого програмного забезпечення. На відміну від хешових сигнатур вони можуть використовуватись для виявлення великої кількості ШПЗ. Рядкові сигнатури створюються вручну фахівцем з кібернетичної безпеки, адже потрібно виділити конкретну частину ШПЗ для формування ефективної сигнатури [2].

Другим напрямком є використання даних аналізу для визначення наслідків кібератаки та можливе зменшення збитків. Для цього аналізується структура ПЗ, принципи його роботи. Перш за все проводиться статичний аналіз, тобто проводиться робота з файлами без запуску шкідливого ПЗ. В результаті такого аналізу можна вивести первинну інформацію про об’єкт дослідження, перевірити наявність інформації про нього в відповідних джерелах, якщо робота проводиться над відомим шкідливим ПЗ. Корисним є метод пошуку рядків за допомогою якого можна знайти звернення до певних файлів, переходи по URL, IP-адреси. Щоб отримати більш детальну інформацію необхідно провести зворотну розробку (reverse engineering), яка дозволить отримати детальну інформацію про принципи роботи ШПЗ.

Наступним етапом буде динамічний аналіз, який надасть інформацію про поведінку ПЗ та дозволить вивести повну картину щодо кібератаки. При динамічному аналізі звертається увага на процеси в системі, використання її ресурсів. Також аналізується мережева активність ШПЗ – DNS-звернення,

використані порти тощо.

В результаті проведення статичного та динамічного аналізів можна вивести класифікацію шкідливого ПЗ, що дасть змогу зручно описати його функціонал. Зазвичай класифікація включає в себе наступні типи шкідливого ПЗ: шпигунські програми, вимагачі, кейлогери, троянські програми, мережеві хробаки, бекдори [3]. В більшості випадків ШПЗ відноситься зразу до кількох згаданих типів. При детальному аналізі структури ШПЗ можна визначити:

- залежності від операційних систем (чи може ШПЗ функціонувати на декількох ОС) або інших факторів;
- мережеву активність ШПЗ;
- наявність корисного навантаження;
- принципи пакування ШПЗ, якщо вони використовуються;
- точний функціонал ШПЗ;
- іншу інформацію.

Після надання класифікації та детального аналізу структури та принципів дії ШПЗ можна підрахувати збитки, які принесла кібератака, визначити заражені частини інформаційної системи та знайти уразливості в системі захисту, які були використані для реалізації кібератаки. До таких вразливостей можна віднести в тому числі людський фактор, якщо шкідливе ПЗ потрапило в інформаційну систему за допомогою методів соціальної інженерії використаних зловмисником.

Інколи на основі отриманих даних можна створити певні механізми відновлення системи від ураження шкідливим ПЗ. Як приклад проаналізувавши оперативну пам’ять пристрою на якому файли були зашифровані програмою-вимагачем можна віднайти ключі шифрування, які були використані цією програмою. Також при аналізу ШПЗ можна знайти інформацію, яка може вивести на зловмисника, яким була проведена кібератака.

Отже аналізуючи шкідливе програмне забезпечення можна створити

сигнатури для подальшого попередження реалізацій атак з використанням даного ШПЗ, точно визначити наслідки кібератаки, зменшити збитки які принесла кібератака. На даний момент статичний та динамічний аналізи ШПЗ є невід'ємною частиною розслідувань кіберінцидентів та мають виконуватись фахівцями з інформаційної та кібернетичної безпеки для ефективної протидії кібератакам.

Література:

1. *Michael S. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software / S. Michael, H. Andrew. – San Francisco: No Starch Press, 2012. – p.32*
2. *Szor P. THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE / Piter Szor., 2005. – p.36*
3. *Automatic Generation of String Signatures for Malware Detection / K.Griffin, S. Schneider, X. Hu, T. Chiueh. // RAID '09: Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection. – 2009. – №1. – p. 102–103.*

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Кравчук В.В.
студентка БСД-44
Державний університет телекомунікацій
м. Київ, Україна

Хакерська активність підвищується щодня, а, з огляду на кількість кінцевих пристроїв, яка зросла в рази, включаючи мобільні, ризики проникнення зловмисників у внутрішню мережу безперервно підвищуються.

Тому безпека кінцевих точок стає все більш поширеною функцією безпеки, оскільки все більше співробітників залучають до роботи мобільні пристрої споживачів, а компанії дозволяють своїм співробітникам використовувати ці пристрої в корпоративній мережі.

Шкідливим вважається будь-яке програмне забезпечення, яке намагається заразити комп'ютер або мобільний пристрій. Зловмисники використовують його для самих різних цілей, включаючи отримання особистих даних і паролів, викрадення грошових коштів, блокування доступу до пристрою для його власника.

Разом з розвитком технологій, з'являються нові загрози та вектори атак, протистояти яким може не кожен встановлений антивірус на пристрої.

Тому еволюція векторів кібератак і розвиток шкідливого програмного забезпечення пояснює необхідність передового рішення захисту кінцевих точок мереж.

Розглянемо декілька типів атак, які можуть бути реалізовані за допомогою використання даного ПЗ:

1. Безфайлові шкідливі програми і атаки нульового дня.

Саме шкідливе ПО розвивається у відповідь на посилення захисту від кіберзагроз, також збільшується кількість шкідливих програм. Наприклад, за даними Інституту Ponemon, 41% атак здійснюються за допомогою «безфайлового шкідливого ПЗ», яке використовує процеси операційних систем замість завантаження файлу, подібного до класичної шкідливої програми. Тому, коли негативний процес активується, звичайні антивірусні рішення не запускають моніторинг, а вбудований шкідливий код запускається і зникає без сліду.

Підприємства також повинні боротися з атаками нульового дня. Вони характерні тим, що не мають сигнатури або можуть використовувати уразливість, виявлену до виходу патча. Тому будь-яке сучасне рішення для захисту кінцевих точок повинно мати можливість захисту як від шкідливих програм, так і від атак нульового дня.

2. Загрози для хмари

В недавній статті для Dark Reading головний технічний директор WatchGuard Technologies Корі Нахрейнер передбачив, що програми-вимагачі скоро націляться на хмару. Він представив кілька причин для цього:

- по-перше, рутинні робочі процеси підприємств стають все більш залежними від хмари.
- по-друге, Нахрейнер зазначає, що багато компаній помилково вважають, що їх хмарні провайдери управляють своєю кібербезпекою.

Таким чином, хмара являє собою один з нових уразливих векторів атак на кінцеві точки підприємства, який не можуть захистити ні застарілі платформи захисту кінцевих точок, ні антивірус.

Сучасне рішення для захисту кінцевих точок повинно включати поведінковий моніторинг і машинне навчання, а також конфігураційну безпеку і деяку форму управління ідентифікацією.

3. Інтернет речей

Інтернет речей рідко поставляється з елементами кібербезпеки; вони можуть мати жорстко запрограмовані основні паролі адміністратора.

Традиційні методи безпеки рідко мають можливості, необхідні для моніторингу пристроїв IoT. Навіть рішення виявлення і реагування (EDR) для кінцевих точок можуть не бачити пристрої IoT, що дозволяє їм непомітно увійти в мережу і вийти з неї. Тому IoT дає можливість хакерам створювати загрози або переміщатися по всій мережі без виявлення.

Згідно наведеної інформації вище можна зробити висновок, що хакери відходять від традиційних типів атак, а одним з головних векторів все частіше стають не тільки пристрої і ПЗ, але і користувачі, які порушують елементарні принципи інформаційної безпеки.

Тому для захисту корпоративного периметра потрібні нові інструменти, які здатні не тільки блокувати стандартні атаки, але і розпізнавати нові їх види, аналізувати інформацію і відслідковувати стан інфраструктури безпеки в комплексі.

Платформи для захисту кінцевих пристроїв типу EPP (Endpoint Protection Platform) - це класичні антивіруси, ПЗ для захисту від шкідливих програм, системи шифрування д.аних, файрволи та рішення для захисту від вторгнень і втрати даних. Вони можуть виявити відомі загрози, але нові і незвичайні вектори атак інколи здатні їх обійти.

Зокрема, вони не мають ефективних інструментів для аналізу атак і не можуть визначити, що окремі зафіксовані в логах інциденти - це частина комплексної кібератаки на інфраструктуру, а безфайлові віруси можуть просто не помітити.

Більш сучасні рішення відносяться до класу EDR (Endpoint Detection and Response), і їх головна перевага - це поєднання класичних інструментів з

арсеналу EPP і ефективної системи аналізу, виявлення та попередження атак. Завдяки застосуванню нових технологій, а також інтелектуального відстеження та фіксації всієї активності системи і її компонентів, рішення EDR набагато частіше виявляють і знешкоджують комплексні кіберзагрози і атаки без використання «прямих» методів, наприклад, безфайлові атаки.

Розгорнуте рішення класу EDR може бути доповнено службою MDR (Managed Detection & Response), тобто послугою управління знаходження загроз і реагуванням на них.

Такі служби найчастіше працюють «по підписці» і займаються моніторингом безпеки замовника в цілодобовому режимі. Вони дозволяють знизити навантаження на IT-спеціалістів компаній, взявши на себе аналіз подій, відсіювання помилкових спрацьовувань і розстановку пріоритетів при отриманні нових даних, виявлення потенційних загроз і автоматичний підбір інструментів для захисту від них. Ці ж служби допомагають сформувати плани заходів щодо усунення загроз і запобігання повторних атак, що особливо важливо для компаній з мінімальним штатом фахівців з інформаційної безпеки.

В ідеалі всі перераховані вище інструменти повинні використовуватись в одному програмному комплексі, який зможе працювати з будь-якими платформами, реагувати на виявлені вразливості і без участі користувачів, виявляти нові типи векторів атак та по можливості обмінюватись отриманою інформацією з централізованою базою даних.

Якщо кожен вендор у реалізації своїх рішень буде використовувати даний комплекс, то це дозволить створити багаторівневий захист як від класичного шкідливого ПЗ, так і від нових, більш розвинутих атак. Також даний комплекс значно допоможе у роботі спеціалістам з кібербезпеки та набагато краще захистить корпоративну мережу від самих користувачів, які не завжди замислюються на якій сайти вони заходять, та які саме файли завантажують на свої пристрої.

Література:

1. *«Защита конечных точек в современных условиях: инструменты и основные проблемы»/[Електронний ресурс] – Режим доступу: https://ko.com.ua/zashhita_konechnyh_tochek_v_sovremennyh_usloviyah_instrumenty_i_osnovnye_problemy_129548*
2. *«Эволюция векторов атак на конечные точки предприятия»/[Електронний ресурс] – Режим доступу: https://cis.bakotech.com/news/evolyuciya-vektorov-atak-na-konechnie-tochki-predpriyatiya/*
3. *«Защита конечных точек»/[Електронний ресурс] – Режим доступу: https://softline.ru/solutions/security/zaschita-prilozheniy/zaschita-konechnyih-tochek*

ДОСЛІДЖЕННЯ МЕТОДІВ ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ

Крук Д. М.
Навчально-науковий інститут захисту інформації
Державний університет телекомунікацій
м. Київ, Україна

Атаки соціальної інженерії не тільки стають все більш поширеними проти малих та середніх підприємств, але вони також розвивають у більш складні. Вони, як правило, передбачають певні форми психологічних маніпуляцій, обдурюючи користувачів або співробітників щодо передачі конфіденційної та «чутливої» інформації.

Зазвичай соціальна інженерія включає вплив та атаки на електронну пошту або інші способи взаємодії, що викликає сильні емоції у жертви, такі як страх, азарт або зацікавленість, змушуючи її негайно розкривати конфіденційну інформацію шляхом натискання на шкідливе посилання або відкриття шкідливого файлу. Оскільки соціальна інженерія включає людський фактор, запобігання цим атакам може бути складним для підприємств.

Недавнє дослідження Webroot [1] показує, що компанії серйозно ставляться до кібербезпеки, але хоч і майже 100 відсотків підприємств навчають працівників найкращим практикам кібербезпеки , ця цифра падає до половини чи третини, коли запитують про «безперервне» навчання, що життєво важливо для ефективності. Це призводить до наступної статистики,

79 відсотків не можуть сказати, що "повністю готові керувати IT-безпекою та захищати від загроз".

Нажаль, повністю захиститись від атак соціальної інженерії неможливо. Згідно дослідження компанії Tessian Limited [2], збиток, який нанесли компаніям лише фішингові атаки протягом 2020 року становить близько 3,92 мільйони доларів.

Керівні методи протидії соціальній інженерії:

- Постійно навчайте персонал. Компанії повинні підходити до безпеки за допомогою активного контролю безпеки, що враховує людський фактор. Навчальні програми з підвищення рівня обізнаності дійсно корисні для зменшення ризику скомпрометування та витоку конфіденційної інформації організації.
- Фільтрування спаму позбавляє певної частини фішингових листів, жодна автоматизація не буде ефективною на 100 відсотків. Навіть якщо відправник виглядає знайомим, потрібно переконатися, що адреса електронної пошти відправника є достовірною. Регулярне моделювання фішингових атак максимізує обізнаність про різні методи фішингу та мінімізує багато наслідків.
- Сегментуйте рівень доступу. Переконайтеся, що лише люди, які мають доступ до конфіденційних даних, можуть взаємодіяти з цими даними.
- Дуже важливо постійно оновлювати все програмне забезпечення. Така практика може допомогти вам пом’якшити безліч атак, тому що зловмисники намагатимуться знайти будь-які лазівки у вашій інфраструктурі.

З наведеної інформації видно, що соціальна інженерія є, мабуть, найефективнішою кіберзброєю в арсеналі кіберзлочинців. Техніки соціального інжинірингу еволюціонували до свого максимального рівня, опираючись на сучаний спосіб життя, поширеність соціальних мереж, простоти пошуку інформації про осіб та необізнаність населення і працівників. Проте недавні дослідження показують, що разом ростом рівня

ознайомлення людей у галузі кібербезпеки, з кожним роком методи соціальної інженерії приносять все менше збитків та втрачають свою ефективність.

Література:

1. Confidence wavers in face of evolving cybersecurity threats: https://www.helpnetsecurity.com/2018/06/27/confidence-cybersecurity-threats/
2. Must-Know Phishing Statistics: Updated 2021 : https://www.tessian.com/blog/phishing-statistics-2020/

УДОСКОНАЛЕНА МЕТОДИКА ДОСЛІДЖЕННЯ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ВІДЕОТРАКТУ ПЕОМ У БЛИЖНІЙ ЗОНІ

Крючкова Л.П., Українець Є. О.
аспірант
Державний університет телекомунікацій
м. Київ, Україна

Однією з найнебезпечніших загроз для інформації, що обробляється технічними засобами в складі автоматизованих інформаційних, телекомунікаційних та інформаційно-комунікаційних систем, є витік інформації каналами побічних електромагнітних випромінювань і наведень. Методи захисту окремих систем та персональних електронних комп'ютерів від витоку такими каналами добре розроблені і регламентуються відповідними нормативними актами. Завдяки стрімкому впровадженню інформаційно-комунікаційних систем в державні органи України широко застосовуються розвідувальні засоби, спрямовані на перехоплення інформації, що обробляється (передається, зберігається) такими системами.

В загальному комплексі заходів щодо забезпечення національної безпеки України в інформаційній сфері важливе місце займає технічний захист інформації, який безпосередньо призначений для забезпечення організаційними, інженерними та технічними заходами, методами і засобами конфіденційності, цілісності та доступності інформації, яка обробляється в інформаційно-телекомунікаційних системах, циркулює на об'єктах інформаційної діяльності.

Небезпечним каналом витоку конфіденційної інформації, яка циркулює в інформаційно-телекомунікаційних системах, є канал, утворений шляхом перехоплення побічних електромагнітних випромінювань (ПЕМВ) технічних

засобів розвідувальними технічними засобами. При цьому найбільш небезпечним джерелом ПЕМВ є відеосистеми, оскільки сигнал статичної картинки відеозображення багаторазово повторюється і теоретично його можна накопичувати.

Ряд питань, пов'язаних з перехопленням ПЕМВ, що виникають при виведенні зображення на екран монітора для аналогового інтерфейсу VGA неодноразово розглядались у відкритих публікаціях.

Слід зазначити, що окрім ПЕМВ самого монітора присутні і сигнали, випромінювані сполучними лініями. Протоколи відеосигналів, які проходять цими сполучними лініями, стандартизовані для ряду типів відео-інтерфейсів (VGA, DVI, DisplayPort і HDMI тощо). Параметри цих сигналів можуть дещо змінюватися в залежності від режимів роботи засобів відображення: роздільна здатність екрана, частоти розгорток тощо.

В доповіді розглянуто дві основні методики оцінки захищеності технічного засобу (ТЗ) від витоку по каналу ПЕМВ [1,2]:

- методика спеціальних досліджень, заснована на визначенні значень радіуса зони R2 навколо технічного засобу, на межі і за межами якої напруженість електромагнітного поля інформативного сигналу не перевищує нормованого значення, радіусу зони r1 навколо ТЗ, в межах якого не допускається розміщення зосереджених антен і радіусу зони r1' навколо ТЗ, в межах якого не допускається розміщення випадкових антен;
- методика вимірювання наведень і реального загасання, що враховує реальне загасання сигналів від досліджуваного ТЗ до межі КЗ. Однак в її рамках не визначаються значення r1 і r1' і сама вона є помітно спрощеною. У зв'язку з цим для об'єктових досліджень найбільш об'єктивною слід визнати методику спеціальних досліджень (визначення R2, r1 і r1'), доповнену методом реальних зон.

Нами вирішується актуальна науково-прикладна задача удосконалення методики виявлення побічних електромагнітних випромінювань і наведень відеотракту ПЕОМ в ближній зоні шляхом розвитку технології вимірювання.

Запропоновано використовувати непрямий метод виявлення побічних електромагнітних випромінювань відеотракту ПЕОМ.

Цей метод не використовує проведення фактичного виявлення сигналу і ґрунтується на застосуванні в інформаційних випромінюючих колах ПЕОМ тестових сигналів у вигляді періодичної послідовності інформаційних імпульсів. Структурну схему вимірювання ПЕМВ відеотракту у ближній зоні точковою антеною наведено на Рис.1.

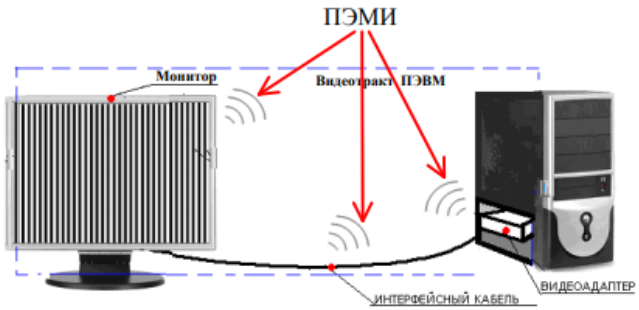


Рис. 1. Структурна схема вимірювання ПЕМВ відеотракту у ближній зоні точковою антеною

Дослідження відеотракту здійснювалось на моніторі Samsung SyncMaster 940T, відеорежим 1280 x 1024 x 64 Гц. Перша гармоніка спектра інформативного сигналу складає близько 54MHz.

Вимірювання для виявлення електричної і електромагнітної складової ПЕОМ у ближній зоні здійснювалось аналізатором спектра ROHDE&SCHWARZFSW 13 (Signal&Spectrum Analyzer) з використанням комплекта антен R&S до аналізатора ROHDE&SCHWARZ FSW 13.

Пошук сигналів, що випромінюються усіма блоками відеотракту при включеному тестовому сигналі в діапазоні частот 30 ... 1000 МГц, здійснювався за допомогою точкової антени - R&S MAGNETICNEAR-FIELDPROBEHZ-14.

Дослідження ПЕМВ окремих блоків відеотракту ПЕОМ здійснювались за наступною методикою:

1. Вимірюється рівень сигналу відеоадаптера (відеокарта ПЕОМ) з якого йде випромінювання ПЕМВ відеотракту;

2. Вимірюється рівень сигналу інтерфейсного кабелю, який з’єднує монітор і ПЕОМ;

3. Вимірюється рівень сигналу з монітору (відеопідсилювач).

Фрагменти спектрограм сигналів відеотракту ПЕОМ у ближній зоні наведено на Рис.2.

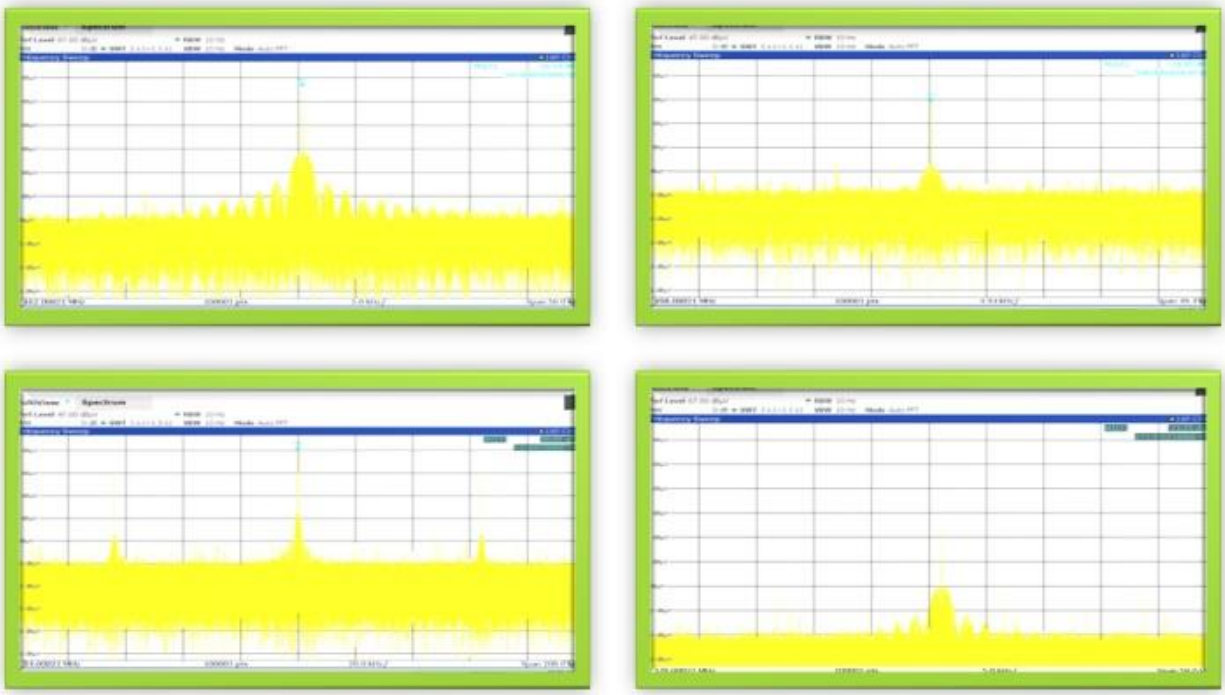


Рис. 2. Фотографії спектрограм сигналів відеотракту ПЕОМ у ближній зоні при дослідженні побічних електромагнітних випромінювань

Виходячи з практичних вимірювань виявлених ПЕМВ за удосконаленою методикою, можна більш детально виявити найбільш найбільш небезпечний елемент відеосистеми, що ми і показали в своїх дослідженнях. Процедура вимірювання побічних електромагнітних випромінювань в ближній зоні електронних засобів з наступною ідентифікацією параметрів джерел випромінювання дозволить забезпечити підвищення достовірності і точності їх локалізації та прогнозування найбільш небезпечних просторових напрямків формування каналів витоку інформації в широкій смузі частот.

Література:

1. *А. А. Хорев "Оценка возможности по перехвату побочнях электромагнитных злучений видеосистемы компьютера. Ч. 2" // Специальная техника. – 2011. – № 4. – С. 51–62.*

2. *Голев Д.В., Кононович В.Г., Хомич С.В. Методики оцінки інформаційної захищеності телекомунікацій: навч. посіб. Одеса, 2013. 220 с.*

Технології підвищення захисту веб-ресурсів на базі рішення F5 Networks

Ткачук А. О.
БСЗМ-71
Державний університет телекомунікацій
м. Київ, Україна

Описано удосконалення захисту веб-ресурсів на базі рішення F5 Networks. Розроблено рекомендації щодо застосування технологій балансувальник F5 BIG-IP та його модулів ASM(WAF), LTM, APM на ОІД.

Захист веб-ресурсів залишається одним із найважливіших напрямків інформаційної безпеки. Щороку їх кількість стрімко зростає, що в свою чергу збільшує кількість важливої(зокрема конфіденційної) інформації, яка зберігається на серверах.

Останнім часом більшість компаній переходять в онлайн. Це пов'язано не тільки з мінімізацією витрат на обладнення та його обслуговування, але й у зв'язку з глобальною пандемією. У результаті цього більшість зовнішніх атак націлюються на корпоративні інформаційні системи, а саме на вразливості веб-додатків. А поширення онлайн-платежів тільки підсилює цю тенденцію. Тому удосконалення захисту веб-ресурсів від атак є необхідно важливим внаслідок зростання економічних, соціальних та політичних наслідків від зловмисних атак.

Проблемам захисту веб-ресурсів приділяють велику увагу. Щороку їх види змінюються. Яскравим прикладом для розгляду видів найпопулярніх атак є QWASP TOP 10. На малюнку наведена порівняльна характеристика щодо топ 10 вразливостей в 2017 та 2021 році(мал.1). Отож ми бачимо що в лідерах залишається саме атаки типу "Ін'єкції" та "Зламана аутентифікаця". Всі інші атаки час від часу змінюються. Тому важливим аспектом є захист не тільки від відомих загроз, але й від атак нульового дня.

OWASP Top 10 2017		change	OWASP Top 10 2021 proposal	
A1	Injections	as is	A1	Injections
A2	Broken Authentication	as is	A2	Broken Authentication
A3	Sensitive Data Exposure	down 1	A3	Cross-Site Scripting (XSS)
A4	XML eXternal Entities (XXE)	down 1 + A8	A4	Sensitive Data Exposure
A5	Broken Access Control	down 1	A5	Insecure Deserialization (merged with XXE)
A6	Security Misconfiguration	down 4	A6	Broken Access Control
A7	Cross-Site Scripting (XSS)	up 4	A7	Insufficient Logging & Monitoring
A8	Insecure Deserialization	up 3 + A4	A8	NEW: Server Side Request Forgery (SSRF)
A9	Known Vulnerabilities	as is	A9	Known Vulnerabilities
A10	Insufficient Logging & Monitoring	up 3	A10	Security Misconfiguration

Рис. 1.Порівняльна таблиця QWASP 2017 і QWASP 2021

Виходячи з аналізу проблеми, один з основних методівзахистів веб-ресурсів є — WAF (Web Application Firewall). Суть якого полягає в захисті WEB ресурсів компанії, що виставлені назовні.

Рішення BIG-IP F5(балансувальник) є чудовим інструментом для повноціного захисту веб-ресурсів компанії. До його складу входять рішення, які дозволяють повністю контролювати трафік, зокрема це модулі:

•- ASM. Менеджер безпеки додатків F5 BIG-IP Application Security Manager (ASM) є високопродуктивним фаєрволом рівня додатків (Web Application Firewall, WAF), який забезпечує високий рівень безпеки веб-додатків. Глибокий аналіз трафіку додатків дозволяє відобразити найскладніші DoS і DDoS атаки.BIG-IP ASM з IP Intelligence дозволяє класифікувати джерело запитів до додатків і на цій підставі застосовувати політики безпеки до цього трафіку. IP Intelligence - це сервіс F5, який дозволяє класифікувати IP-адреси і IP-мережі відправників запитів з додатком і заблокувати трафік від цих джерел, якщо вони визначені як небезпечні. BIG-IP ASM щодня завантажує з сервісу F5 сигнатури атак на додатки. До категорій класифікаці загроз ASM входить:

•- Windows exploits - активні IP-адреси джерел шкідливого ПО, вірусів,

руткітів і т. д.

●- Web attaks - джерела, які беруть участь в експлуатації вразливостей веб ресурсів (iFrame injection, SQL injection, domain password brute force)

●- Botnets - джерела, які є частиною бот мережі (як заражені пристрої, так і джерела управління ними)

●- Scanners - джерела, з яких виробляється сканування портів, сканування доменних зон, грубий підбір паролів (brute force)

●- Denial of Service - джерела, з яких зафіксовані прецеденти DoS і DDoS атак

●- Reputation - джерела, які відомі, як заражені шкідливим ПЗ

●- Phishing - різні фішингові сервіси

●- Proxy - IP-адреси анонімних проксі серверів і TOR.

●- LTM. Менеджер локального трафіку BIG-IP Local Traffic Manager (LTM) який може перетвоювати мережу в динамічну інфраструктуру для представлення додатків. Він виконує роль повного посередника між користувачами і сервером веб-додатків, створюючи рівень абстракції для захисту, оптимізації та балансування навантаження трафіку.

●- APM.Менеджер політик додатків F5 BIG-IP Access Policy Manager (APM) - це рішення від F5, яке дозволяє забезпечити безпечний доступ і роботу з додатками, незалежно від того, де знаходяться користувачі (в межах корпоративної мережі, або за її межами). Також за допомогою APM є можливість спростити підхід до визначення політик безпеки (без шкоди для останньої).

Основними перевагами комплексу F5 BIG-IP є:

- Простота розгортання додатків і гарантована доступність.

- Безпека веб додатків, що не вимагає зміни їх коду.

- Комплексне рішення відображення DDoS атак.

- Повна звітність про події, логування.

- Висока продуктивність і гнучкість.

- Забезпечення безпеки додатків, мережі і даних: Приховування ресурсів і помилок сервісів, вибіркове шифрування, шифрування cookies, аналіз аномалій по протоколам, можливості брандмауера(визначення джерела, які беруть участь в експлуатації вразливостей веб ресурсів.

- Ефективне і просте розгортування політик захисту та самих додатків за шаблонами, можливість сегментації архітектури підприємства.

- Зниження навантаження на сервера: перетворення контенту, OneConnect, швидке кешування, прискорення роботи і розвантаження SSL, формування черги з'єднань TCP та інші техології.

- Можливість інтеграції з різними SIEM(IBM QRadar, Splunk і т.д).

Таким чином, технології підвищення захисту веб-ресурсів є важливим напрямком у інформаційній безпеці у сучасному світі. Стрімкий ріст інформаційних технологій, поширення конфіденційних даних та багатократне збільшення кількості та видів атак змушують компанії шукати рішення для захисту своїх веб-ресурсів, мінімізації шкоди від атак та збереження своєї репутації. Тому технології на базі F5 Networks підходить для вирішення таких проблем. Адже дозволяє взяти під контроль архітектуру підприємства без втручання в роботу самих веб-ресурсів, контролювати тарфік на усіх рівнях; налаштувати безпеку додатків, даних та мережі; дає можливість інтеграції з різними рішеннями для аналізу логів та виявлення проблем; забезпечує відмовостійкість та контроль навантаження веб-ресурсів.

Література:

1. *Sen J. A Robust Mechanism for Defending Distributed Denial OF Service Attacks on Web Servers / J. Sen // International Journal of Network Security & Its Applications (IJNSA). — 2011, March. — Vol. 3, N 2. — Ç. 162–179.*
2. *BIG-IP Local Traffic Manager & BIG-IP Global Traffic Manager Operations Guide: https://bakotech.ua/uploads/ckeditor/files/f5-ltm-gtm-operations-guide-1-0(1).pdf*
3. *BIG-IP® Application Security Manager®: Getting Started: https://techdocs.f5.com/content/kb/en-us/products/big-ip_asm/manuals/product/asm-getting-started-13-0-0/_jcr_content/pdfAttach/download/file.res/BIG-IP_Application_Security_Manager__Getting_Started.pdf*

4. *Knowledge centers: https://support.f5.com/csp/knowledge-center/software/BIG-IP?module=BIG-IP%20LTM&version=14.0.0*

ФРЕЙМВОРКИ УПРАВЛІННЯ ЗАГРОЗАМИ КІБЕРБЕЗПЕКИ

Фесенко О. М.
Навчально-науковий інститут захисту інформації
Державний університет телекомунікацій,
м. Київ, Україна

Розглянуті переваги використання фреймворків управління загрозами кібербезпеки в компаніях та що відбувається протягом життєвого шляху процесу реалізації фреймворку. Проаналізувавши статті, стало зрозуміло, що використання таких фреймворків спрощує роботу з ризиками кібербезпеки, так як надаються застереження, кращі практики тощо. Також було наведено, для прикладу, на надано коротку характеристику декількох фреймворків, стандартів, які можуть бути використані у наш час.

Інформаційна безпека – це, як відомо, «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій». Основу ІБ становлять політика ІБ, законодавча, нормативно-правова та наукова база ІБ, структура органів, які здійснюють захист інформації, а також методи, способи і засоби, які вони для цього застосовують [1, с. 65].

Роль фреймворків управління загрозами кібербезпеки в цьому – це спростити задачу, надати рекомендації та кращі практики для забезпечення гнучкого за дисциплінованого процесу управління ризиками безпеки. Перечислене у тому числі забезпечує категоризацію інформаційної безпеки, відбір контролю, оцінку та впровадження, а також авторизацію системи та контролю та постійний моніторинг тощо.

В основному існує шість етапів процесу управління ризикам. Кожен крок включає оцінку ризику кібербезпеки, яка має відбуватися протягом усього процесу життєвого циклу після початку впровадження управління ризиками кібербезпеки.

Хоча конкретні методології різняться, процес управління ризиками зазвичай виконує такі дії [2]:

1) Визначає ризики, які можуть порушити кібербезпеку. Зазвичай це передбачає виявлення вразливостей у системі та загроз, які можуть їх використати.
2) Аналіз ступеня тяжкості кожного ризику, оцінивши, ймовірність того, що він може виникнути, і наскільки значним може бути вплив, якщо він з’явиться.
3) Оцінка, як кожен ризик відповідає приоритетам (заздалегідь визначений рівень прийнятного ризику).
4) Призначення певного пріоритету кожному ризику.
5) Як реагувати на кожен ризик. Зазвичай існує чотири варіанти: зменшити вірогідність того, що ризик буде використаний; прийняти ризик; повністю усунути ризик; передати ризик підряднику.
6) Моніторинг існуючих ризиків, та знаходження нових.

Відомі стандарти та фреймворки що визначають підхід до управління кібер-ризиками на сьогодні:

1) CIS (Center for Internet Security) Controls - це набір із 20 дій, також відомих як CSC (критичний контроль безпеки), для кіберзахисту, які забезпечують конкретні та ефективні способи зупинити найпоширеніші та найнебезпечніші атаки сьогодні.
2) ISO / IEC 27001: 2013 - міжнародний стандарт управління інформаційною безпекою.
3) NIST Risk Management Framework забезпечує комплексний, гнучкий 7-етапний процес, який будь-яка організація може використовувати для управління інформаційною безпекою та ризиком конфіденційності для організацій та систем [3].
4) Факторний аналіз інформаційного ризику (The Factor Analysis of Information Risk, FAIRTM) - це система кібер-ризиків, розроблена The Open Group з метою допомогти підприємствам зрозуміти, виміряти та проаналізувати інформаційний ризик, щоб допомогти бізнес-лідерам,

експертам з кібербезпеки та фахівцям з ризиків приймати обґрунтовані рішення щодо їх практики кібербезпеки [4].

Фреймворки управління ризиками кібербезпеки (RMF) є критично важливою як для організацій. Метою використання RMF є боротьба з ризиками кібербезпеки та прийняття рішень щодо бізнес-ризиків. Управління ризиками спричиняє великі зміни в галузі, і важливо мати можливість спочатку виявляти та перешкоджати погрозам, на відміну від спроб відшкодувати шкоду, яку вони завдають. Майбутнє галузі виглядає неймовірно багатообіцяючим, особливо з тим, як технології продовжують прогресувати.

Література:

1. *Хмелевський Р. М. ДОСЛІДЖЕННЯ ОЦІНКИ ЗАГРОЗ ІНФОРМАЦІЙНЇЇ БЕЗПЕЦІ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ / Ростислав Миколайович Хмелевський. – 2016.*
2. *Cyber Risk Management Service [Електронний ресурс] – Режим доступу до ресурсу: https://www.itgovernance.co.uk/cyber-security-risk-management.*
3. *NIST Risk Management Framework [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://csrc.nist.gov/projects/risk-management.*
4. *Chickowski E. Cybersecurity risk management explained [Електронний ресурс] / Ericka Chickowski. – 2020. – Режим доступу до ресурсу: https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-risk-management-explained.*

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ПРОТИДІЇ СУЧАСНИМ ВНУТРІШНІМ ЗАГРОЗАМ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Хмелевський Р.М., Клецько О. М.
студентка БСД-42
Державний університет Телекомунікацій
м. Київ, Україна

Постановка проблеми

В умовах сьогодення, коли розвиток технологічного прогресу підвищує свої темпи до рекордних значень, коли інформаційні технології стають базисом для побудови соціальних взаємодій, роботи компаній і державних установ, інформаційна безпека і захист від внутрішніх загроз стає життєвою необхідністю для підтримки нормальної життєдіяльності соціуму і окремих його частин.

Стан інформаційної безпеки України напряму спирається на різноманітні загрози, необачне відношення до яких може призвести до подій, що нанесуть неоправну школу як державному, так і комерційному секторам національної економіки[1].Спираючись на вищесказане, можна зробити висновок про високу актуальність дослідження шляхів та розроблення рекомендацій щодо протидії сучасним внутрішнім загрозам корпоративної інформаційної системи.

Аналіз останніх досліджень і публікацій

Інформаційна безпека, як механізм передбачення, запобігання та боротьби з наслідками різного роду загроз, як внутрішніх, так і зовнішніх, в останній стрімко завойовує популярність і має високу доцільність не тільки в сфері корпоративної безпеки, а й виходить на державний рівень (Указ Президента України про Стратегію кібербезпеки Україні [2]). Дослідженню цих питань присвячені роботи таких авторів:

- В.Л. Бурячок,
- Ю.В. Богданович,
- П.О. Балашов,

- С.В. Кавун,
- С.В. Казмірчук,
- О.Г. Корченко,
- В.О. Хорошко

Викладення основного матеріалу

Інформаційна безпека — це, за загально прийнятим поняттям, «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій»[3].

Зазвичай, під внутрішніми загрозами інформаційної безпеки розуміють загрозу з боку співробітників компанії як умисних (шахрайство, крадіжка, зміна або видалення конфіденційної інформації, промисловий шпіонаж, тощо), так і неумисні (зміна або знищення інформації через низьку кваліфікацію співробітника), а також порушення режиму роботи апаратних і програмних засобів обробки і зберігання інформації.

Основні блоки дій в боротьбі з внутрішніми загрозами

Захист від витоків конфіденційної інформації (Data Leakage Prevention)

Даний механізм являє собою побудову комплексної системи контролю та протидії внутрішнім загрозам безпеці (умисним діям інсайдерів щодо порушення цілісності, доступності або конфіденційності інформації). Впровадження даного комплексу дозволяє забезпечити захист ділової інформації від несанкціонованого доступу, копіювання, спотворення:

- в каналах передачі даних - застосовуються системи контентної фільтрації трафіку користувачів (WEB, E-mail, ICQ, P2P);
- на робочих місцях співробітників - контроль знімних носіїв (USB пристрої - флешки, зовнішні HDD), черг друку, доступу до мережевих ресурсів.

Дана система дозволяє централізовано керувати контролем і ефективно застосовувати заходи з протидії, а також створювати необхідну доказову базу

по інцидентах безпеки. При цьому сама система залишається абсолютно «прозорою» для користувачів.

Забезпечення конфіденційності інформації при зберіганні і передачі

Являє собою комплекс організаційно-технічних заходів щодо недопущення компрометації, крадіжки, модифікації або знищення конфіденційної інформації як внутрішніми порушниками безпеки, так і третіми особами. В рамках даних методів боротьби з загрозами пропонується:

- шифрування каналів зв'язку (організація VPN, SSL, ЕЦП, PKI);
- шифрування носіїв інформації (створення захищених контйнеров, побудова корпоративної системи шифрування і зберігання даних).

Висновки

У зв’язку із зростаючою роллю спроб промислового шпіонажу, саботажу, умисного знищення і передачі третім особам конфіденційної інформації, дослідження шляхів та розроблення рекомендацій щодо протидії сучасним внутрішнім загрозам корпоративної інформаційної системи вимагає великої уваги з боку сучасних компаній.

Література:

1. *Хмелевський Р.М. Тези. «Інформаційна безпека, як одна з основ забезпечення ефективності роботи державного управління». Матеріали міжнародної науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології» Том IV «Сучасні технології інформаційної безпеки» Київ, ДУТ. 17–20 листопада 2015 р. – С.155–158.*
2. *«Про Стратегію кібербезпеки України». Указ Президента України №96 / 2016 від 27 січня 2016 року. – [Електроний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/287/2015*
3. *Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1 / С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.*

БЕЗПЕКА КІНЦЕВИХ ПРИСТРОЇВ КОРИСТУВАЧІВ ВІД ЗЛОЯКІСНОГО WEB КОНТЕНТУ

Поліщук Д.В.
БСД-42
Державний університет телекомунікацій
м. Київ, Україна

Інтернет - це нова форма розповсюдження та спілкування. Як і будь-які інші комунікаційні технології, особливо на початкових стадіях їх розвитку, Інтернет несе в собі потенційно шкідливий або незаконний вміст або використовується як засіб злочинної діяльності. Як і будь-яка інша комунікаційна технологія, така як телефон або GSM, зловмисники можуть використовувати Інтернет для полегшення своєї діяльності. З точки зору незаконного та шкідливого вмісту, важливо розрізняти вміст що є незаконним та іншим шкідливим вмістом. Ці різні категорії вмісту ставлять принципово різні принципові питання і вимагають дуже різних юридичних та технологічних реакцій.

- Незаконний вміст

Це стосується, наприклад, дитячої порнографії, торгівлі людьми, розповсюдження расистських матеріалів або підбурювання до расової ненависті, тероризму або всіх видів шахрайства (наприклад, шахрайство з кредитними картками , вірусні посилання)

- Шкідливий вміст

Різні типи матеріалів можуть ображати цінності та почуття інших людей: вміст, що виражає політичні думки, релігійні переконання чи погляди на расові питання тощо.

Визначення та боротьба з незаконним змістом в інтернеті.

Держава повинна визначити, що заборонено законом, і забезпечити його застосування шляхом виявлення незаконної діяльності та покарання правопорушників. Однак особливі характеристики Інтернету означають, що

правоохоронні органи є більш складними, ніж там, де використовуються більш традиційні засоби.

Хоча виявити порушення закону в публічних додатках Інтернету просто, це стає складніше в приватних програмах (наприклад, електронна пошта). Подібним чином, хоча застосування закону порівняно легко в національних межах, набагато складніше в міжнародному контексті.

- Технічні обмеження для правоохоронних органів

Технічні особливості Інтернету роблять певні види контролю неефективними. Через те що можна перенаправляти Інтернет-повідомлення, управління дійсно може відбуватися лише у точках входу та виходу в Мережу (сервері, через який користувач отримує доступ, або на терміналі, який використовується для зчитування або завантаження інформації та сервер, на якому опублікований документ). Навіть якщо опублікований документ буде видалено з одного сервера в результаті втручання влади, його можна легко і швидко скопіювати на інші сервери в інших юрисдикціях, щоб він продовжував бути доступним, доки такі сайти також не будуть заблоковані.

- Роль постачальників доступу до Інтернету та постачальників послуг хостингу

Провайдери доступу до Інтернету та провайдери хост-послуг відіграють ключову роль у наданні користувачам доступу до Інтернет-контенту. Однак не слід забувати, що основна відповідальність за контент лежить на авторах та постачальниках контенту.

- Анонімне використання Інтернету

Користувачів Інтернету, як правило, ідентифікують, вказуючи автора домашньої сторінки в Інтернеті, або ідентифікуючи адресу сторінки ("URL"), або згадуючи адресу електронної пошти для електронної пошти або повідомлення групи новин. Це бажано відповідно до демократичного принципу, згідно з яким люди, хоча і можуть вільно висловлювати свої думки та переконання, повинні нести відповідальність за свої дії.

Література:

1. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1996:0487:FIN:en:PDF
2. https://www.herbertsmithfreehills.com/latest-thinking/online-harmful-content

ТЕХНОЛОГІЯ ЕКСТРЕННОГО АПАРАТНОГО ЗНИЩЕННЯ ТА ШИФРУВАННЯ ДАНИХ НА ОСНОВНИХ НОСІЯХ ІНФОРМАЦІЇ

Рухлядко М. А.
БСЗМ-71
Державний університет телекомунікацій,
м. Київ, Україна

Аннотація: У даній статі розглянута практична можливість захисту носіїв інформації, типу SSD та HDD, апаратними методами шифрування за перевіреними стандартами та методиками National Institute of Standards and Technology для покращення захищеності робочих місць та уникненню отримання доступу до інформації на носіях

Ключові слова: захист інформації, алгоритм, зловмисник, інформація, апаратний захист, пристрій, інформаційна безпека, NIST.

1. ВСТУП

Ми живемо в епоху інформаційного суспільства, коли інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, держави. Сьогодні ми все більше й більше використовуємо їх у своїй діяльності. Не є винятком і Збройні Сили. Але взявши на службу телекомунікації і глобальні комп’ютерні мережі, слід знати й розуміти, які можливості для зловживання створюють ці технології. Сьогодні жертвами хакерів можуть стати не лише люди, але й цілі держави. За ефективністю та наслідками застосування кіберзброю, а саме такий термін все частіше використовують вчені, можна прирівняти до зброї масового ураження. Тому кібербезпека – одна з основних проблем, що викликає занепокоєння.

І чим швидше людство розвиває інформаційні технології, тим більшою є потреба в захисті інформаційно-телекомунікаційних систем. Оскільки критичні вразливості в програмному забезпеченні та автоматизованих

системах викликають небезпідставні побоювання, то не дивно, що уряди та суспільство в усьому світі шукають кращих заходів і методів для захисту особистих даних Інтернет-ресурсів від кіберзагроз.

В теперішній час накопичувачі на жорстких магнітних дисках (НЖМД, або HDD – Hard disk drive), твердотілі накопичувачі (SSD – Solid-state drive) лягають в основу пристроїв зовнішньої пам'яті сучасних комп'ютерів. За останні роки місткість носіїв збільшується а отже і збільшується як і кількість носіїв так й інформації, що потребує захисту.

Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Технічний захист інформації – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та (або) програмних і технічних засобів конфіденційності, цілісності та доступності інформації, а також унеможливлення її блокування.

2. ТЕОРЕТИЧНА ЧАСТИНА

Шифрація інформації

Advanced Encryption Standard (AES), також відомий як Rijndael – симетричний алгоритм блочного шифрування (розмір блоку 128 біт, ключ 128/192/256 біт), прийнятий в якості стандарту шифрування урядом США за результатами конкурсу AES. Цей алгоритм добре проаналізований і зараз широко використовується.

Розширений стандарт шифрування (AES) вказує криптографічний алгоритм, затверджений FIPS-код, який можна використовувати для захисту електронних даних. Алгоритм AES – це симетричний блок-шифр, який може шифрувати (шифрувати) та дешифрувати (розшифровувати) інформацію. Шифрування перетворює дані у нерозбірливу форму, що називається шифротекст; дешифрування шифротексту перетворює дані назад у початковий вигляд, який називається простим текстом. Алгоритм AES здатний використовувати криптографічні ключі 128, 192 та 256 біт для шифрування та дешифрування даних у блоках із 128 біт.

Види AES

Алгоритм AES перетворює блок довжиною 128 бітів в інший блок тієї ж довжини. Для перетворення застосовується розклад ключів w отримується з ключа. 128-бітний блок в AES представляється у вигляді матриці 4 × Nb. Стандарт допускає тільки одне значення Nb = 4, тому довжина блоку завжди 128 біт, хоча алгоритм може працювати з будь-яким Nb. Довжина ключа дорівнює 4Nk байт. Алгоритм шифрування блоку складається з Nr раундів - застосувань однієї і тієї ж групи перетворень до 128-бітного блоку даних. Стандарт допускає такі комбінації цих трьох параметрів:

	Nk	Nb	Nr
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Технології запису даних

Принцип роботи жорстких дисків схожий на роботу магнітофонів. Робоча поверхня диска рухається щодо голівки, що зчитує (наприклад, у вигляді котушки індуктивності з зазором в магнітопроводі). При подачі змінного електричного струму (при записі) на котушку головки виникає змінне магнітне поле з зазору головки впливає на феромагнетик поверхні диска і змінює напрямок вектора намагніченості доменів в залежності від величини сигналу. При зчитуванні переміщення доменів у зазору головки приводить до зміни магнітного потоку в муздрамтеатрі головки, що

призводить до виникнення змінного електричного сигналу в котушці за рахунок електромагнітної індукції.

З кінця 1990-х на ринку пристроїв зберігання інформації почали застосовуватися головки на основі ефекту гігантського магнітоопору (ГМО).

З початку 2000-х головки на основі ефекту ГМО стали замінюватися на головки на основі тунельного магніторезистивного ефекту (в них зміна магнітного поля призводить до зміни опору в залежності від зміни напруженості магнітного поля; подібні головки дозволяють збільшити вірогідність достовірності зчитування інформації, особливо при великій щільності запису інформації). У 2007 році пристрою на основі тунельного магніторезистивного ефекту з оксидом магнію (ефект відкритий в 2005 році) повністю замінили пристрої на основі ефекту ГМО.

3. АПАРАТНА ЧАСТИНА

Знищення інформації

Часто, коли необхідна підвищена надійність знищення інформації, до НЖМД застосовують методи знищення, при яких руйнується сам носій інформації.

Вартість НЖМД значно знизилася за останні роки. Тому, як і в випадку гнучких магнітних дисків, для багатьох компаній економічно може бути більш доцільно знищувати їх, а не видаляти інформацію. Але тут виникає проблема високої вартості обладнання для механічного знищення і процесом контролю знищення в разі наявності цього обладнання в інших компаніях.

Гарантоване екстрене знищення інформації

Гарантоване екстрене знищення інформації – одна з важливіших аспектів захисту інформації від несанкціонованого доступу. Проте на шляху гарантованого знищення постає дуже багато проблем, оскільки в деяких випадках знищення інформації повинно відбуватись моментально. У випадку екстреної потреби знищення інформації найкраще підходять HDD носії.

Накопичувач на жорстких магнітних дисках, або НЖМД - накопичувач (пристрій зберігання інформації) довільного доступу, засноване на принципі

магнітного запису. Є основним накопичувачем даних в більшості комп'ютерів.

На відміну від гнучкого диска (дискети), інформація в НЖМД записується на жорсткі (алюмінієві або скляні) пластини, покриті шаром феромагнітного матеріалу, найчастіше діоксиду хрому - магнітні диски. У НЖМД використовується одна або кілька пластин на одній осі. Зчитувальні головки в робочому режимі не торкаються поверхні пластин завдяки прошарку набігаючого потоку повітря, що утворюється у поверхні при швидкому обертанні. Відстань між головкою і диском складає декілька нанометрів (у сучасних дисках близько 10 нм), а відсутність механічного контакту забезпечує довгий термін служби пристрою. При відсутності обертання дисків головки знаходяться у шпінделя або за межами диска в безпечній («паркувальної») зоні, де виключений їх нештатний контакт з поверхнею дисків.

Також, на відміну від гнучкого диска, носій інформації зазвичай поєднують з накопичувачем, приводом і блоком електроніки. Такі жорсткі диски часто використовуються в якості незнімного носія інформації.

Внаслідок наявності терміна логічний диск, магнітні диски (пластини) жорстких дисків, щоб уникнути плутанини, називаються фізичний диск, сленгове - млинець. З цієї ж причини твердотільні накопичувачі іноді називаються жорсткий диск SSD, хоча магнітні диски і рухливі пристрої в них відсутні.

Представлені основні показники механічних методів знищення інформації на НЖМД. При всіх зазначених методах знищення інформації на НЖМД, можливість повторного використання НЖМД відсутня.

Механічний	Знищення носія механічною дією	Можливе гарантоване знищення
Термічний	Нагрівання носія до температури знищення його основи(або ж до точки Кюрі)	Гарантоване знищення
Піротехнічний	Знищення носія підривом	Можливе гарантоване знищення. Проблеми

		забезпечення безпеки виконавця.
Металотермічний	Знищення основи носія високою температурою самопоширюючимся високотемпературним синтезом	Гарантоване знищення
Хімічний	Знищення робочого слою або основи носія хімічно агресивним середовищем	Можливе гарантоване знищення. Проблеми забезпечення безпеки виконавця.
Радіаційний	Знищення носія іонізуючими променями	Загроза зараження

Інший метод – розмагнічення феромагнетика в НЖМД

Розмагнітити феромагнетик можна, помістивши його в повільно убуває змінне магнітне поле.

У випадку з НЖМД виникають труднощі, пов'язані з великою коерцитивної силою (залишкової намагніченістю) феромагнітного покриття диска.

Більш продуктивним є підхід, пов'язаний з намагнічуванням робочих поверхонь носія до максимально можливих значень (насичення) носія.

Спосіб заснований на положенні, що в разі НЖМД зовнішнє магнітне поле розглядається як аналог поля, створюваного магнітними головками під час запису.

Якщо характеристики зовнішнього поля будуть перевищувати напруженість поля, створюваного головками на таку величину, при якій відбудеться магнітне насичення матеріалу поверхні диска, то все магнітні домени будуть переорієнтовані у напрямку цього зовнішнього поля і вся інформація на жорсткому диску буде знищена.

З огляду на те, що характеристика матеріалу, з якого виготовляються покриття поверхонь сучасних НЖМД, як правило, фірмами-виробниками не розголошується, оцінку величини напруженості намагнічує поле доводиться розраховувати з деяким запасом.

Запропоновано розрахунок напруженості магнітного поля для знищення інформації на НЖМД приводах виробляти по аналогії з розрахунком стираючого поля для магнітних стрічок.

4. ВИСНОВКИ

Одна з проблем захищеності інформації на робочих місцях – легкий фізичний доступ до носіїв інформації. Соціальна інженерія в наш час дуже розвинута і тому отримати доступ до робочого місця не так вже й важко, тому потрібно обов'язково створювати такі або схожі і навіть покращені комплексні системи для захисту як носіїв інформації так і інформації на них. За допомогою шифраторів та спеціалізованих перевірених інформаційних сейфів, спеціалізованих корпусів робочих станцій та серверів можливо і необхідно створювати підвищений рівень захищеності. Інколи краще втратити частину інформації, але зберегти її від несанкціонованого доступу недозволеним лицям, ніж втратити інформацію, помітити витік інформації. Для забезпечення роботи систем кожен день, або, хоча б раз на тиждень – потрібно робити резервне копіювання на окремий захищений носій чи сховище.

Література:

1. *Патент 66512 Україна G11B 5/024 Пристрій для стирання записів на магнітному носії жорсткого магнітного диска / Товариство з обмеженою відповідальністю «ЕПОС» 25 квітня 2007 рік, бюл. №5*
2. *Advanced Encryption Standard (AES) [Електронний ресурс] // - Режим доступу: https://csrc.nist.gov/publications/detail/fips/197/final#pubs-abstract-header*
3. *Public Comments on the Draft Federal Information Processing Standard (FIPS) for the Advanced Encryption Standard (AES) [Електронний ресурс] // - Режим доступу: https://csrc.nist.gov/CSRC/media/Publications/fips/197/final/documents/fips197-draft-comments-received.pdf*
4. *Advanced Encryption Standard [Електронний ресурс] // - Режим доступу: wikipedia.org/wiki/Advanced_Encryption_Standard*
5. *Как устроен AES [Електронний ресурс] // - Режим доступу: https://habr.com/ru/post/112733/*
6. *Ломаем модифицированный AES-256 [Електронний ресурс] // - Режим доступу: https://habr.com/ru/post/339910/*
7. *Методы стирания информации, хранимой на жёстких магнитных дисках [Електронний ресурс] // - Режим доступу: https://www.epos.ua/view.php/about_pubs_archive?subaction=showfull&id=1013378400&archive=&start_from=&ucat=2&*
8. *Разрушающие методы уничтожения информации на НЖМД [Електронний ресурс] // - Режим доступу: https://www.epos.ua/view.php/about_research_datakill*
9. *ЗАКОН УКРАЇНИ Про основні засади забезпечення кібербезпеки України [Електронний ресурс] // - Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19*

10. *20 лютого 2003 року на засіданні Верховної Ради України прийнято за основу законопроект "Про внесення змін до Закону України "Про захист інформації в автоматизованих системах" [Електронний ресурс] // - Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=85BF300F8B9D19738131E3F63C5D663A?art_id=40629&cat_id=38710*
11. *Устройство жесткого диска, принцип работы HDD. [Електронний ресурс] // - Режим доступу: http://hdd.co.ua/blog/2013/05/03/ustrojstvo-zhestkogo-diska/*
12. *Жёсткий диск [Електронний ресурс] // - Режим доступу: https://ru.wikipedia.org/wiki/Жёсткий_диск*
13. *Algebraic Aspects of the Advanced Encryption Standard by Carlos Cid, Sean Murphy, Matthew Robshaw*
14. *Advances in Cryptology — CRYPTO 2015 – 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part 1*

ВИКОРИСТАННЯ PYTHON В СУЧАСНИХ МЕТОДАХ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ WEB-ДОДАТКІВ

Рибаков А. Ю.
Студент БСД-42
Державний університет телекомунікацій
м. Київ, Україна

За останні роки спостерігається зріст кіберзагроз в усіх областях кіберпростору – ця проблема не оминула і WEB-додатки. Для забезпечення їх безпеки потрібно визначитися з інструментами для цього, зокрема – з мовою програмування.

Для реалізації бекенда WEB-додатків використовується багато мов програмування, із яких на сьогоднішній день можна виділити PHP, Ruby, Java, JS, .NET, C, C++, і, звісно, Python. У кожної мови свої технічні особливості, переваги та недоліки, але зараз акцентуємо увагу на аспекті кібербезпеки.

Відносно дослідженню від WhiteSource [1] Python розділяє останні три місця з C++ та Ruby по кількості зафіксованих вразливостей на мову програмування, коли C займає перше місце та охоплює майже половину усіх випадків.

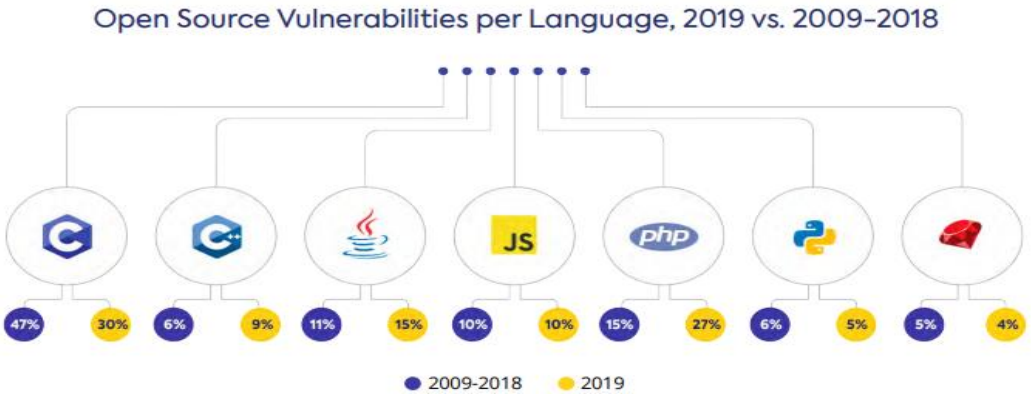


Рис. 1. Відсоток зафіксованих вразливостей на мову програмування.

Основні вразливості у Python – CWE-20 (неправильна перевірка вводу), CWE-264 (Дозволи, привілеї та засоби контролю доступу), CWE-79 (Міжсайтовий скриптинг) та CWE-200 (витік/розкриття інформації).

Крім високого рівня захисту від вразливостей відносно інших мов програмування при використанні в написанні бекенду, Python, за допомогою влаштованих інструментів та зовнішніх бібліотек, дозволяє провести ефективне тестування системи на проникнення (penetration testing).

Penetration testing, або тестування на проникання - це випробування, метою яких є здійснення спроби обминути або відключити механізми захисту [2].

Приклади інструментів, які можуть бути використані для проведення пентестування:

- Scapy – бібліотека, яка дозволяє працювати з мережевими пакетами – створювати їх, модифікувати, відправляти та приймати. За допомогою Scapy можливо комбінувати атаки різних типів, а варіації того, як конкретно буде створений той чи інший пакет, не обмежені стандартними рамками, що приводить к можливості виконувати задачі, які неможливі в інших інструментаріях з подібним функціоналом.
- Vulners – ця бібліотека основана на базі даних Vulners, яку називають «гуглом для хакерів». Вона містить в собі величезний перечень вразливостей, патчей, експлойтов, багов, який постійно оновлюється. Усю

інформацію з Vulners можливо аналізувати та використовувати, що може бути дуже корисно і для розуміння того, як реалізовуються ті чи інші атаки, і для створення свого сканеру безпеки WEB-додатків.

- Sqlmap – вузьконаправлена бібліотека, основна мета якої – пошук та виявлення можливостей для проведення усіх п’яти основних видів SQL-ін’єкцій. Крім цього, Sqlmap вміє зламувати хеші, завантажувати або вивантажувати файли з серверу, та, використовуючи команди відповідної операційної системи, орієнтуватись по внутрішній мережі.

Кількість інструментів для тестування на проникання в Python дуже велике, а використовувати їх просто. Ця мова програмування легка для вивчення, код пишеться швидко та зручно читається. Навіть початківець в області кібербезпеки може знайти для себе можливість покращувати свою спеціалізацію за допомогою Python, бо написання скриптів та праця безпосередньо з вразливостями та експлойтами дає безцінний досвід.

Література:

1. *The state of open source vulnerabilties 2020 [Електронний ресурс]. – Режим доступу до ресурсу: https://resources.whitesourcesoftware.com/research-reports/the-state-of-open-source-vulnerabilties-2020.*
2. *НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.*

МЕТОДИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У WEB-ДОДАТКАХ ЗА ДОПОМОГОЮ СУЧАСНИХ ТЕХНОЛОГІЙ

Мельничук А. П.
студент БСД-42
Державний університет телекомунікацій
м. Київ, Україна

Сьогодні перелік сервісів і ресурсів, які виросли в Інтернеті дуже велика кількість. Інтернет перетворився з подібних між собою статичних сторінок документів в серйозний інструмент інтерактивності і взаємодії з кінцевими користувачами. В зв’язку з таким розвитком, шалену популярність набуло застосування Web-додатків, які пропонують безліч переваг у даному секторі: від простоти у використанні до міжплатформенності, від автоматичності оновлень до швидкості і відносно невисокої вартості розробки.

Інтернет-сервіси надають великий обсяг можливостей, але в той же час, зі збільшенням кількості додатків пропорційно зростає і кількість кіберзагроз. Актуальною

являться проблема забезпечення інформаційної безпеки web-додатків, особливо через ускладненення їх функціоналу і підтримки нових протоколів. Веб-сервери додатків зберігають велику кількість конфіденційної інформації користувачів, що також посилює необхідність використання сучасних технологій для виявлення загроз безпеки у веб-додатках.

Природою походження загроз інформаційної безпеки можуть бути як випадкові чинники (збої, помилки, побічні впливи тощо), так і навмисні злочинні дії соціуму. Основним джерелом загроз безпеки Web-додатків являються зовнішні порушники. Зовнішній порушник – особа, яка найчастіше вмотивована комерційними цілями, має доступ до додатку та висококваліфікована з питань мережевої безпеки та реалізації мережевих атак на різні типи інформаційних систем. Як правило, засобами реалізації загроз у Web-додатках є інтернет-шахрайство (phishing, carding, pharming тощо), міжсайтовий скриптинг (XSS), різного роду ін'єкції (SQL-injection, PHP-injection), DoS та DDoS-атаки тощо [1; 2].

Оскільки більшість загроз безпеці інтернет-ресурсів надходить з зовнішнього простору, потрібно правильно розгорнути та покращувати системи, які будуть виявляти та відповідним чином реагувати на вторгнення.

Найпоширенішими технологіями, які використовуються для поставленої вище мети, являються системи виявлення та запобігання вторгненням (IDS/IPS, Intrusion Detection System/Intrusion Prevention System). Головною відмінністю між ними є те, що IDS – це система моніторингу, а IPS – система управління. Основне завдання подібних систем – виявлення факторів неавторизованого доступу в мережу і прийняття відповідних заходів протидії: інформування спеціалістів ІБ про факт вторгнення, вимкнення з'єднання і переналаштування міжмережевого екрану для блокування наступних дій зловмисника [3].

Існують різні методи виявлення інцидентів за допомогою технологій IDS/IPS:

- виявлення вторгнень за допомогою сигнатур – процес порівняння сигнатури (шаблон, який визначає відповідну атаку) з можливим інцидентом. Цей метод дуже ефективний при виявленні загально відомих загроз, але втрачає свої переваги проти атак, які не мають відповідних сигнатур в базі.

- виявлення вторгнень по аномальній поведінці – метод, який базується на порівнянні нормальної активності подій з активністю, яка виходить за рамки допустимого рівня. В подальшому IDS/IPS використовує статичні методи для порівняння різних характеристик реальної активності із заданим пороговим значенням, при перевищенні якого відправляється відповідне повідомлення про небезпеку до спецілістів ІБ.

Більшість сучасних систем виявлення вторгнень використовують поєднання даних методів, що значно підвищує ступінь виявлення та зменшує кількість помилкових спрацювань.

Отже, сучасні IDS/IPS критично важливі для захисту web-додатків, особливо, якщо звернути увагу на PIDS/APIDS. Protocol-based intrusion detection system – це система виявлення вторгнень, що встановлюється, на веб-

сервері і виконує моніторинг та аналіз протоколу, який використовується обчислювальними машинами. Зазвичай PIDS використовується як інтерфейс веб-сервера, який відслідковує HTTP/HTTPS потік. Application protocol-based intrusion detection system – це система виявлення вторгнень, яка фокусує свій моніторинг і аналіз на конкретному прикладному протоколі web-додатку. Типове місце для використання APIDS знаходиться між веб-сервером і системою управління базою даних, відслідковуючи протокол SQL, специфічний для проміжного програмного забезпечення чи бізнес-логіки, коли він взаємодіє з базою даних.

Література:

1. *Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності / Р.М. Хмелевський // Сучасний захист інформації. – 2016. – № 4. – С. 65-70.*
2. *Основные угрозы безопасности сайта [Електронний ресурс] – Режим доступу: https://habr.com/ru/post/279787/*
3. *IDS/IPS - системы обнаружения и предотвращения вторжений и хакерских атак [Електронний ресурс] – Режим доступу: http://www.altell.ru/solutions/by_technologies/ids/*

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Капітанець Є.Л.
студент БСД-43
Державний університет телекомунікацій
м. Київ, Україна

Загрози для системи електронного документообігу досить стандартні і можуть бути класифіковані наступним чином:

- загроза цілісності - пошкодження і знищення інформації, перекручення інформації - як не навмисне в разі помилок і збоїв, так і зловмисне.

- загроза конфіденційності - це будь-яке порушення конфіденційності, у тому числі крадіжка, перехоплення інформації, зміни маршрутів.

- загроза працездатності системи - всілякі загрози, реалізація яких призведе до порушення або припинення роботи системи; сюди входять як умисні атаки, так і помилки користувачів, а також збої в устаткуванні і програмному забезпеченні.

Захист саме від цих загроз в тій чи іншій мірі повинна реалізовувати будь-яка система електронного документообігу. При цьому, з одного боку, впроваджуючи СЕД, впорядковуючи і консолідуючи інформацію, збільшуються ризики реалізації загроз, але з іншого боку, як це не парадоксально, упорядкування документообігу дозволяє вибудувати більш якісну систему захисту. Джерел загроз в нашому небезпечному світі не мало: це і "криві руки" деяких системних адміністраторів, техніка, яка має властивість ламатися в самий невідповідний момент, і форс-мажорні обставини, які рідко, але все ж відбуваються. І навіть якщо сервери не постраждають від пожежі, що сталася в будівлі, будьте впевнені - їх неодмінно заллють водою пожежники, які приїхали. В цілому ж, можна виділити декілька основних груп: легальні користувачі системи, адміністративний IT-персонал, зовнішні зловмисники. Спектр можливих злочинів легальних користувачів досить широкий - від скрепок в апаратних частинах системи до навмисної крадіжки інформації з корисливою метою. Можлива реалізація загроз в різних класах: загрози конфіденційності, загрози цілісності. Користувач системи - це потенційний зловмисник, він може свідомо чи не свідомо порушити конфіденційність інформації. Особлива група - це адміністративний IT-персонал або персонал служби іт-безпеки. Ця група, як правило, має необмежені повноваження і доступ до сховищ даних, тому до неї треба поставитися з особливою увагою. Вони не тільки мають великі повноваження, але і найбільш кваліфіковані в питаннях безпеки та інформаційних можливостей. Не так важливий мотив цих злочинів, чи був це корисливий намір або помилка, від якої ніхто не застрахований, результат один - інформація або загубилася, або отримала розголос. Відповідно до численних досліджень, від 70 до 80% втрат від злочинів припадають на атаки зсередини. Набір зовнішніх зловмисників суто індивідуальний. Це можуть бути і конкуренти, і партнери, і навіть клієнти.

Не зупиняючись на засобах захисту комп'ютерних мереж, мережевих пристроїв та операційних систем з їх файловими система, що представляють

окрему тему для розмови, розглянемо більш докладно кошти, інтегровані в самі СЕД. Будь-яка СЕД, що претендує на звання "захищеної", має як мінімум передбачити механізм захисту від основних її загроз: забезпечення збереженості документів, забезпечення безпечного доступу, забезпечення достовірності документів, протоколювання дії користувачів. СЕД повинна забезпечити збереження документів від втрати і псування і мати можливість їх швидкого відновлення. Статистика невблаганна, в 45% випадків втрати важливої інформації припадають на фізичні причини (відмова апаратури, стихійні лиха тощо), 35% обумовлені помилками користувачів і менше 20% - дією шкідливих програм і зловмисників. Опитування аналітичної компанії Deloitte Touche, проведений на початку 2006 р., показав, що більше половини всіх компаній стикалися з втратою даних протягом останніх 12 місяців. 33% таких втрат призвели до серйозного фінансового збитку. Представники половини компаній, що пережили втрату даних, заявляють, що причиною інциденту став саботаж або недбале ставлення до правил інформаційної політики компанії, і тільки 20% респондентів повідомили, що інтелектуальна власність їхніх компаній захищена належним чином. Лише 4% опитаних заявили, що їхні роботодавці звертають особливу увагу на інформаційну політику компанії. Що стосується СЕД, то в ефективності її захисту впевнено тільки 24% учасників опитування. Так, наприклад, СЕД, в основі своєї використовують бази даних Microsoft SQL Server або Oracle, воліють користуватися коштами резервного копіювання від розробника СУБД (в даному випадку Microsoft або Oracle). Інші ж системи мають власні підсистеми резервного копіювання, розроблені безпосередньо виробником СЕД. Сюди слід також віднести можливість відновлення не тільки даних, але і самої системи в разі пошкодження.

Підхід до захисту електронного документообігу має бути комплексним. Необхідно тверезо оцінювати можливі загрози і ризики СЕД і величину можливих втрат від реалізованих загроз. Захист СЕД не зводиться лише до захисту документів і розмежування доступу до них. Залишаються

питання захисту апаратних засобів системи, персональних комп'ютерів, принтерів та інших пристроїв; захисту мережного середовища, в якій функціонує система, захист каналів передачі даних і мережевого устаткування, можливе виділення СЕД в особливий сегмент мережі. Комплекс організаційних заходів грають роль на кожному рівні захисту, але їм, на жаль, часто нехтують. Адже тут і інструктаж, і підготовка звичайного персоналу до роботи з конфіденційною інформацією. Погана організація може звести нанівець усі технічні заходи, як досконалі вони б не були.

5 НАЙБІЛЬШИХ ТЕНДЕНЦІЙ В ІНТЕРНЕТІ РЕЧЕЙ У 2021 РОЦІ

Починок М. О.
Виконав студент Державного Університету Телекомунікацій
м. Київ, Україна

Інтернет речей (IoT) - одна з найвизначніших технологічних тенденцій, яка з'явилася за останні роки. Простіше кажучи, це стосується того факту, що хоча слово «Інтернет» спочатку означало широкомасштабну мережу комп'ютерів, сьогодні пристрої будь-якого розміру та форми - від автомобілів до кухонних приладів до промислових машин - з'єднані та обмінюються інформацією у цифровому, глобальному масштабі.

Як і в кожному аспекті нашого життя, глобальна пандемія коронавірусу, безсумнівно, вплинула на те, як ця тенденція розвивається та впливає на наше життя. У світі, де на сьогодні контакт між людьми є більш обмеженим, контакт між пристроями, інструментами та іграшками може допомогти нам залишатися на зв'язку.

У цій статті буде освітлено погляд всесвітньо відомого футуролога, інфлюенсера та лідера думок у галузі бізнесу та технологій Бернарда Марра на розвиток ринку інтернету речей впродовж 2021 року.

Ключові слова: прогноз, тенденції розвитку ринку, діджиталізація, розумне місто, інтернет речей

Різкий ріст інвестицій охорони здоров'я в IoT

Від телемедицини до автоматизованої допомоги по дому для літніх людей та інвалідів - інтелектуальні переносні пристрої, датчики і пов'язані мережею пристрої будуть продовжувати змінювати способи надання медичної допомоги. Вони також буде використовуватися для зведення до мінімуму непотрібних контактів в ситуаціях, коли ризик вірусного зараження

особливо високий, наприклад, в будинках для людей похилого віку та інфекційних палатах в лікарнях.

Як чудова демонстрація того, як триваюча пандемія прискорила прийняття технологічної трансформації охорони здоров'я, оригінальні оцінки кількості "віртуальних візитів" або зустрічей в Інтернеті з постачальниками медичних послуг у США становили 36 мільйонів. Насправді ця цифра зараз має стати ближчою до одного мільярда, і ця тенденція, безсумнівно, буде продовжуватись зростати протягом 2021 року, коли вже існує інфраструктура та обізнаність пацієнтів про переваги.

Сильний ріст спостерігається також на ринку пристроїв, які дозволять людям похилого віку довше залишатися незалежними у власних будинках. Це включатиме інструменти, що використовують штучний інтелект для виявлення падінь або змін до звичайних розпорядків дня, які можуть попередити родичів або медичних працівників про необхідність втручання. Пристосовуючись до викликів, поставлених Covid-19, за цією ж технологією можна визначити, чи спостерігається швидке погіршення здоров'я людей, які можуть захищати або ізолювати вдома, оскільки хвороба часто може привести людей до стану, в якому вони не можуть самостійно звернутися за допомогою вчасно.

IoT зробить роботу з дому більш продуктивною

Робота вдома - це нове звичне явище для багатьох з нас в інформаційній економіці, через проблеми безпеки навколо великої кількості людей, які збираються в офісах та центрах міст. Оскільки персональні помічники на базі штучного інтелекту є зараз у багатьох наших будинках, ми можемо розраховувати на додатки, розроблені для того, щоб допомогти нам управляти своїм днем, працюючи віддалено. Це означатиме розумніші автоматизовані інструменти планування та календаря, а також кращу якість, більш інтерактивні відеоконференції та технологію віртуальних зустрічей. Наприклад, платформа Microsoft Virtual Stage використовує свої датчики

Azure Kinect, щоб забезпечити захоплюючі презентації на основі штучного інтелекту, які допоможуть нам краще взаємодіяти.

Коли компанії все ще потребують фізичної присутності - як це відбувається у більшості виробничих, промислових та логістичних операцій - IoT означає, що активи можна ефективніше відстежувати віддалено, забезпечуючи спокій, що автоматизовані машини продовжать свою роботу, а інженери або технічний персонал можуть бути попереджені про необхідність втручання.

IoT у роздрібній торгівлі - безпечніші та ефективніші магазини та супермаркети

Роздрібна торгівля - це сектор, який, безсумнівно, сильно постраждав від коронавірусу. Як ми переконалися в перші дні цієї пандемії, багато несуттєвих торгових точок можна тимчасово закрити, мінімально змінюючи наше життя - багато в чому завдяки появі роздрібної торгівлі в Інтернеті. Однак магазини, що постачають товари першої необхідності, такі як їжа та ліки, повинні залишатися відкритими для задоволення основних потреб місцевого населення.

Протягом наступного року ми можемо розраховувати побачити нову мету для таких інноваційних моделей, як повністю автоматизовані супермаркети, які скорочують необхідність нежиттєвої людської взаємодії, оскільки ми забезпечуємо свої будинки продуктами харчування та іншими необхідними предметами. Автоматизація через пристрої з підтримкою IoT також буде продовжувати рости у масивних виконавчих центрах, які відправляють запаси в магазини. Безконтактні способи оплати також стануть дедалі поширенішими, оскільки ми будемо рухатись далі до “безготівкового суспільства”, яке, як передбачається, з’явиться вже через певний час - і несе із собою власні проблеми.

Інші розробки в роздрібній торгівлі включатимуть використання RFID-міток для відстеження пересування покупців по магазинах. Як і раніше, це буде використовуватися для прийняття рішень щодо розміщення продуктів,

запам'ятовуючи, як і коли клієнти взаємодіють з дисплеями та продуктами на полицях. У світлі цьогорічних змін у суспільстві, тепер він також буде все частіше використовуватися для моніторингу соціальних дистанцій та захисту від небезпеки перенаселення в особливо людних районах магазинів, супермаркетів та торгових центрів.

IoT у масштабі міста

Концепція "розумного міста" набирає популярності протягом останніх років, використовуючи технологію IoT, яка використовується для моніторингу руху в дорожніх мережах, використання громадського транспорту, руху навколо пішохідних районів та використання таких громадських зручностей, як центри утилізації та збору відходів. Розумні лічильники фіксують використання енергії в будинках та на підприємствах, тому постачання може бути збалансованим, щоб задовольнити потреби під час піків та уникнути марнотратства там, де це не потрібно.

Протягом наступного року ми можемо очікувати припливу ресурсів, спрямованих на створення цифрових можливостей у муніципальних владах, щоб вони могли краще використовувати нові технології, які стають доступними. Це буде вкрай важливо для вирішення проблем мінливого суспільства. Враховуючи проблеми безпеки навколо громадського транспорту, офісів у центрі міста та рекреаційних закладів, таких як центри дозвілля та парки, технологія IoT дозволить владі та бізнесу краще зрозуміти схеми використання, а також ефективніше планувати заходи безпеки та стратегії реагування на надзвичайні ситуації.

IoT на периферії

Нарешті, периферійні обчислення - ще одна потужна тенденція, яка не зникне завдяки Covid. Як і у випадку інших згаданих тут тенденцій, зміна, яку він дає, стане актуальною як ніколи, швидше за все, призведе до збільшення швидкості прийняття та темпів інновацій.

Завдяки периферійним обчисленням, а не пристроям IoT, які надсилають всі дані, які вони збирають, у хмару для аналізу та вилучення

статистичних даних, ця робота виконується безпосередньо на самих пристроях. Однією з явних переваг є значна економія у використанні пропускної здатності та зменшення витрат, як фінансових, так і екологічних. Однак настільки ж життєво важливими у світі після коронавірусу будуть переваги для конфіденційності та управління даними. Багато ініціативних та реактивних ініціатив, таких як виявлення спалаху та відстеження контактів, покладаються на дуже особисті дані, такі як дані про стан здоров'я та місцезнаходження. Нові способи обробки та вжиття заходів з цією інформацією використовуватимуть сучасні обчислювальні технології для зменшення ризику, спричиненому надсиланням цією інформації між персональними пристроями та хмарними серверами. Це може виявитись надзвичайно важливим, коли мова йде про зміцнення довіри громадськості до цих заходів - те, що потрібно зробити для успішного їх масштабного розгортання.

Література:

1. *Marr B. The 5 Biggest Internet Of Things (IoT) Trends In 2021 Everyone Must Get Ready For Now [Електронний ресурс] / Bernard Marr. – 2020. – Режим доступу до ресурсу: https://www.bernardmarr.com/default.asp?contentID=2125.*

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ ПЛАТІЖНИХ СИСТЕМ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ СЕРТИФІКАЦІЇ PCI DSS

Потужна А. О.
БСДМ-71
Державний університет телекомунікацій
м. Київ, Україна

Розглянуто стандарт безпеки PCI DSS для організацій, що мають справу з платіжними картками та систем що обробляють чи зберігають карткові данні. Визначено призначення та мету проходження сертифікації і отримання сертифікату відповідності. А також розглянуто усі 12 вимог стандарту PCI DSS.

Успішність бізнесу напряму залежить від ефективності розвитку та відповідності сучасним тенденціям в світі інформаційних технологій.

Нещодавно в зв’язку з пандемією, однією з таких тенденцій стало переводження бізнесу до он-лайну. Компанії почали налагоджувати свої процеси, обмін даними та документами через Інтернет. Також це спровокувало великий інтерес власників бізнесу до впровадження систем сплати послуг чи товару. Бізнес зробив вибір на користь ефективності, але тепер під загрозу потрапила безпека.

Досвід минулих літ звернув увагу бізнесу також і на впровадження та контроль безпеки свого підприємства. Ігнорування вразливостей які потенційно можуть бути експлуатованими зловмисниками можуть бути причиною втрат як фінансових так і репутаційних. Тому наразі сертифікація безпеки платіжних систем знаходиться на піку своєї популярності.

Звичайно причиною тому стало те, що останнім часом у всьому світі почастішали випадки злому саме банківських інформаційних систем. Тому компанії що мають справу з платіжними картками та їх даними вимушені звертати підвищену увагу на інформаційну безпеки систем та операцій.

Для безпечного використання даних карт прийнятий комплекс заходів, сформульованих у вигляді спеціального стандарту з інформаційної безпеки (Payment Card Industry Data Security Standard, PCI DSS). Стандарт був розроблений у 2004 році, він об’єднав у собі набір вимог до безпеки платіжних карток Visa, MasterCard, American Express, Discover Card і JCB. Згодом у 2006 році була створена спеціальна Рада з безпеки - PCI Security Standards Council. Основними функціями якої є розробка та публікація стандартів PCI та супутньої документації.

Дія PCI DSS поширюється на торгово-сервісні підприємства і постачальників послуг, які працюють з міжнародними платіжними системами, тобто на всіх, хто передає, обробляє і зберігає дані власників карт. Це стосується як загальних даних - номер карти (Primary Account Number, PAN), ім'я власника картки, код обслуговування, дата видачі та закінчення терміну дії, так і критичних даних авторизації (sensitive authentication data) - повне утримання магнітної смуги, коди CVC2 / CVV2 /

CID та PIN-блок. Елементи даних необхідно захищати, якщо вони зберігаються разом з номером картки, а по завершенні процедури авторизації критичні дані не повинні зберігатися навіть в зашифрованому вигляді. Вимоги стандарту PCI DSS не застосовуються, якщо не виконується зберігання, обробка або передача номера картки (PAN).

Вимоги стандарту PCI DSS розповсюджуються на всі системні компоненти, в тому числі на мережеве обладнання, сервери і програми, що входять до складу середовища даних платіжних карт (частина мережі, в якій обробляються дані платіжних карт або критичні дані авторизації) або безпосередньо до неї підключені. До мережевих компонентів відносяться (але не обмежуються ними) міжмережеві екрани, комутатори, маршрутизатори, бездротові точки доступу, пристрої захисту інформації та інше мережеве обладнання. Серед типів серверів - сервери Web, сервери баз даних, аутентифікаційні і поштові сервери, proxy-, NTP-, DNS- і інші сервери. У перелік додатків входять всі придбані і розроблені додатки, як внутрішні, так і зовнішні.[1]

Залежно від числа оброблюваних за рік транзакцій (до 120 тис., До 600 тис., До 6 млн., Більше 6 млн.) Компанії присвоюється певний рівень з обов'язковим набором вимог з безпеки. Процедури підтвердження відповідності стандарту включають щорічний аудит, щоквартальне сканування мережі на наявність вразливостей і, в деяких випадках, заповнення аркуша самооцінки (Self Assessment Questionauire). Для виконання аудиту та сканування мереж компанії повинні залучати сторонню організацію, що має статус Qualified Security Assessor (QSA, для аудиту) та Approved Scanning Vendor (ASV, для сканування мережі). Згадані статуси присвоюються радою PCI Security Standards Council, і їх список розміщений на сайті.

Стандарт PCI DSS складається з 6-ти цілей та 12-ти вимог яким потенційна компанія повинна відповідати.[2] Коротко розглянемо нижче.

Ціль 1. Побудова та підтримка захищеної мережі.

Вимога 1: З метою захисту даних платіжних карт необхідно забезпечити розробку міжмережевих екранів і управління їх конфігурацією.

Вимога 2: Параметри безпеки і системні паролі, встановлені виробником за замовчуванням, використовувати забороняється.

Ціль 2. Захист даних платіжних карт.

Вимога 3: При зберіганні дані платіжних карт слід надійно захистити.

Вимога 4: Дані платіжних карт, що передаються по мережах загального користування, необхідно шифрувати.

Ціль 3. Реалізація програми управління уразливими.

Вимога 5: Обов'язкове використання і регулярне оновлення антивірусного ПЗ.

Вимога 6: Забезпечення безпеки при розробці і підтримці систем і додатків.

Ціль 4. Реалізація заходів по строгому контролю доступу.

Вимога 7: Доступ до даних платіжних карт повинен бути обмежений відповідно зі службовою необхідністю.

Вимога 8: Кожному особі, яка має доступ до обчислювальних ресурсів, призначається унікальний ідентифікатор.

Вимога 9: Фізичний доступ до даних платіжних карт слід обмежити.

Ціль 5. Регулярний моніторинг і тестування мереж.

Вимога 10: Доступ до мережевих ресурсів і даних платіжних карт слід контролювати.

Вимога 11: Системи і процеси забезпечення безпеки необхідно регулярно тестувати.

Ціль 6. Підтримка політики інформаційної безпеки.

Вимога 12: Діяльність співробітників і контрагентів регламентується в рамках політики інформаційної безпеки.

Таким чином, якщо компанії необхідно пройти сертифікацію на відповідність PCI DSS і самостійно обробляти дані банківських карт на сайті, до неї застосовуються всі вимоги стандарту PCI DSS. Вони охоплюють

безпеку на рівні мереж, обладнання, додатків, баз даних, фізичних сховищ, документування та управління процесами. Для компаній, які працюють тільки з платіжним шлюзом і не приймають на своєму даних банківських карт клієнтів, відносяться тільки вимоги департаменту ризиків платіжного шлюзу.[3]

В результаті проведеного аналізу вимог стандарту PCI DSS, практичного досвіду, набутого під час проходження технологічної та переддипломної практик в організації, яка займається обробкою платежів на міжнародному рівні, працює з тисячами мерчантів та сервіс-провайдерами, стало зрозумілим, що для забезпечення подальшого підвищення рівня безпеки даних даних тримачів карт необхідно постійно вдосконалювати систему захисту, враховуючи при цьому всі вимоги стандарту PCI DSS.

Висновки

PCI Data Security Standard був розроблений для визначення рівня захищеності систем які передають, обробляють або зберігають дані платіжних карток. Стандарт був введений для того, щоб допомогти власникам платіжних карток, а також організаціям, які володіють інформацією про платіжні картки, уберегтися від щорічної втрати коштів через шахрайство. Він допомагає організаціям, що працюють з картами, підвищити рівень безпеки, але не є єдиною причиною для реалізації відповідних рішень безпеки.

Література:

1. *Official PCI Security Standards Council Site. Available: https://www.pcisecuritystandards.org/.*
2. *MAINTAINING PAYMENT SECURITY. Available: https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security*
3. *PCI SECURITY STANDARDS OVERVIEW. Available: https://www.pcisecuritystandards.org/pci_security/standards_overview*

МЕТОДИ ЗАХИЩЕНОСТІ WEB ДОДАТКІВ

Боднар К.С.

БСД-42
Державний університет телекомунікацій
м. Київ, Україна

З кожним роком число компаній які використовують веб-технології для залучення нових клієнтів та збільшення продуктивності роботи стрімко росте. Особливо зараз, під час карантину, число сервісів та послуг, які доступні у мережі, вражає. Наприклад, за останній рік, більшість ресторанів стрімко розвивають свої веб-додатки, у яких клієнти можуть замовляти доставку їжі на дім, у зв'язку з неможливістю обслужити клієнта особисто і подобні тенденції відбуваються в багатьох сферах. Таким чином, веб-вразливості перевершують по кількості і можливій шкоді майже будь-які інші проблеми інформаційної безпеки.

Вразливості веб-додатків, як правило, є наслідком відсутності фільтрації вводу та виводу даних, що часто використовуються для маніпулювання вихідним кодом або отримання несанкціонованого доступу. Такі уразливості дозволяють використовувати різні вектори атак, включаючи: SQL та PHP ін’єкції, Cross-site Scripting (XSS), Remote File Inclusion та Cross-site Request Forgery (CSRF).

Серед основних загроз з використанням веб-вразивостей, зловмисники також активно використовують і фішингові інструменти, які є результатом помилок людей. Від цього ніхто не застрахований, тому навчання персоналу і перевірка компетентності робітників теж є важливою частиною кібербезпеки.

Одне з кращих рішень для захисту веб-додатків на сьогодні виступає Web application firewall (WAF). Ця технологія, наприклад, широко використовується на такому популярному веб сервісі як “Amazon”. Це апаратні та програмні рішення, що використовуються для захисту від загроз безпеки додатків. Ці рішення призначені для вивчення вхідного трафіку та блокування спроб атаки, тим самим компенсуючи будь-які недоліки коду.

Захищаючи дані від крадіжок та маніпуляцій, розгортання WAF відповідає ключовим критеріям для сертифікації PCI DSS.

Майже всі брандмауери можуть бути налаштовані спеціально для конкретних випадків використання та політики безпеки, а також для боротьби з новими загрозами. Також, більшість сучасних рішень використовують дані про поведінку програми, щоб отримати додаткові уявлення про вхідний трафік.

WAF, як правило, інтегровані з іншими програмними рішеннями для формування периметра безпеки. Сюди можуть входити, наприклад, рішення захисту від DDoS атак, що забезпечують додаткову масштабованість, необхідну для блокування великих обсягів атак.

На ряду з WAF, існує безліч важливих нюансів захисту веб-додатків. Одним з найважливіших є:

- Перевірка додатку вручну для ідентифікації вхідних точок та коду на стороні клієнта.
- Криптографічний захист передачі даних.
- Підвищення стійкості програми до загрози DDoS шляхом тестування на анти-автоматизацію, блокування облікового запису, DoS протоколу HTTP та DoS підстановки SQL ресурсів.
- Тест на проникнення. Цей метод дає можливість оцінити захист інформаційної системи зі сторони порушника безпеки, використовуючи різні сценарії кібератак.

Тендеція така, що веб-додатки зараз охоплюють велику частину інтернет трафіку та стрімко розвиваються, що призводить до великої кількості загроз у цьому сегменті, які постійно розвиваються. Ось чому важливо надавати увагу до захисту у цій сфері та моніторити новітні засоби для забезпечення безпеки.

Література:

1. https://octavacapital.ua/zahyst-web-dodatkiv-chomu-ce-aktualno/
2. https://www.imperva.com/learn/application-security/application-security/
3. https://itbiz.ua/ua/zashhita-veb-prilozheniy-pochemu-yeto-vazhn

МЕТОДИ ПРОТИДІЇ ВПЛИВУ СПАМУ

Супрунов В.С.
БСД - 41
Державний університет телекомунікацій
м. Київ, Україна

Питанням протидії спаму присвячено багато досліджень. В основному, це фільтри, побудовані на байєсівському підході, що, як відомо, не дозволяє враховувати семантику електронних повідомлень. При розробці систем фільтрації вхідних повідомлень недостатньо повно використовується системний підхід і сучасні технології штучного інтелекту для вирішення задачі класифікації.

Ключові слова: спам, спам-фільтр, фільтрація спаму, криптографічна аутентифікація.

Спам - повідомлення діляться залежно від цілей, що переслідуються спамером. Одні спамери роблять масові розсилки з метою отримання прибутку, наприклад, в повідомленні може міститися реклама товару або послуги або заклик брати участь в політичних кампаніях. Інші розсилають повідомлення шахрайського характеру або поширюють шкідливі програми (віруси і троянські коні) [1].

Шкідливі програми розробляються з метою нанесення шкоди комп'ютерній системі і розсилаються під виглядом нешкідливого додатку до повідомлення. Віруси, "черв'яки", "троянські коні", програми-шпигуни і рекламні програми вкладаються в листи і запускаються при відкритті вкладеного файлу. Між спамом і шкідливими програмами існує взаємозалежність: через спам розсилаються шкідливі програми, вони завдають шкоди комп’ютеру, щоб контролювати його на відстані і розсилати ще більше спаму. Такі комп'ютери називаються "зомбі". Таким чином, електронні листи з шкідливими програмами порушують не тільки доступність зовнішніх ресурсів і конфіденційність секретних даних (за рахунок можливості деяких вірусів знаходити і відправляти господареві номера банківських карт і паролів доступу), але і цілісність всієї інформації, збереженої на комп'ютері.

Методи боротьби із спамом можна розділити на коротко-, середньо- і довгострокові. Механізми фільтрації і блокування розглядаються як короткострокові методи, оскільки їх застосування може бути обмежене інфраструктурою місцевої поштової організації з незначними модифікаціями. Деякі методи, засновані на DNS, які впливають на структуру і вміст в записах DNS можуть запускатися місяцями або навіть роками. Методи, засновані на Інфраструктурі відкритих ключів і методи, засновані на ресурсах, можуть виявитися довгостроковими зважаючи на значні зміни і розширення інфраструктури.

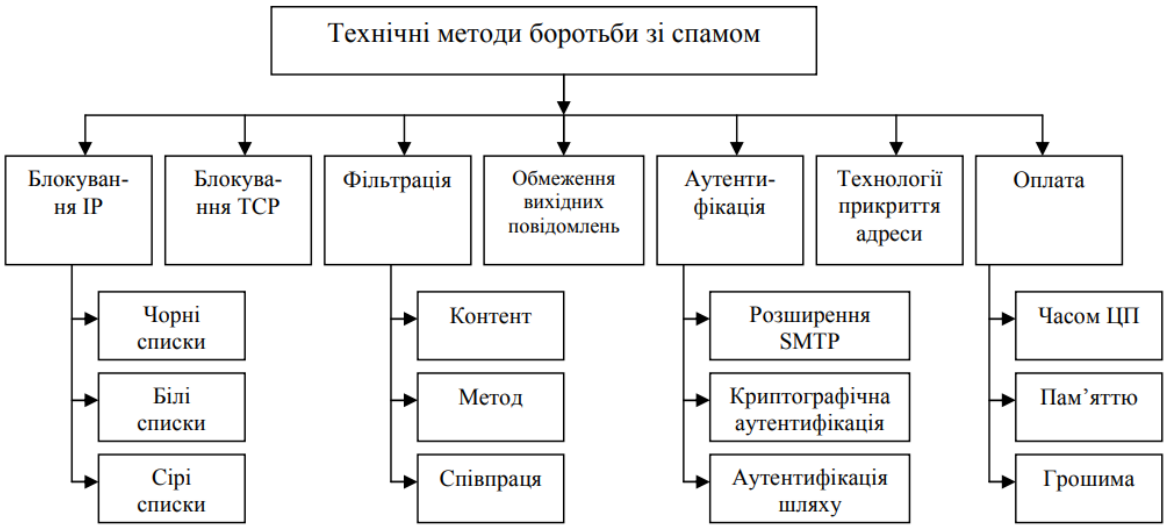


Рис. 1. Технічні методи боротьби зі спамом

Оскільки спамери розсилають мільйони повідомлень, вони ігнорують повідомлення про неможливість доставки листів, що використовують механізми верифікації для блокування спаму. У схемі верифікації, жодне повідомлення не посилається поки відправник, або організація-відправник не буде занесена в білий список. Якщо відправник намагається доставити повідомлення в захищений ящик, дане повідомлення ставиться в чергу на карантин і повертається запит. Щоб користувач міг надалі відправляти листи, йому пропонується відповісти на повідомлення, виконати математичні обчислення або розпізнати текст з картинки.

Механізми аутентифікації діляться на 3 категорії. До першої відносяться розширення SMTP, друга категорія заснована на криптографічній аутентифікації і відноситься до захисту шляху передачі повідомлень. Третя категорія направлена розпізнавання шляху передачі повідомлень, який визначає домен останнього мережевого сегменту або останнього MTA. Ця категорія включає протоколи, які називаються LMAP – Lightweight MTA Authentication Protocols.

Метод, коли клієнт ініціює з'єднання SMTP, на мережевому або транспортному рівні встановлюється TCP/IP зв'язок з SMTP [2] сервером. IP-адрес хоста відправника може бути легко визначений і він же буде першою інформацією про клієнта, яку отримає сервер. Якщо IP-адрес схожий на адрес клієнта, який розсилав спам у минулому, в з'єднанні може бути відмовлено ("чорний список"). Іноді, в чорний список заноситься цілий діапазон IP адрес, наприклад адреси певного домена або ISP. Якщо IP–адрес належить надійному клієнтові, з'єднання буде встановлено ("білий список"). Термін "сірий список" описує такий спосіб, коли IP–адрес – це частина інформації, яка використовується для ухвалення або відхилення з'єднання. Кожна поштова транзакція спочатку відхиляється, а дані (адреса відправника, адреса одержувача і тема повідомлення) про цю первинну невдалу спробу зберігаються. Якщо в спеціальному тимчасовому вікні SMTP клієнт намагається знову виконати невдалу поштову транзакцію, сервер приймає цю транзакцію як таку, що підходить під збережені параметри. Занесення в сірі списки грунтується на припущенні, що більшість джерел спаму в цілях економії часу не пересилають повідомлення наново, вважаючи, що поштовий сервер став недоступним.

Методи криптографічної аутентифікації направлені на боротьбу із спуфінгом в загальному сенсі. Цифровий підпис додається в повідомлення і підтверджує особу відправника. Підписи розрізняються по мірі достовірності: деякі засновані на імені користувача або його адресі

підписується зазвичай MUA, інші вимагають підтвердження домена або ESP підписується MTA [3].

Ґрунтуючись на навединих методах аналізу та використаних джерел, можна зробити висновок що застосування різних механізмів фільтрації спаму дозволяє знаходити та ліквідовувати велику кількість шахрайських і фішингових листів, усіх спроб їх порушення доступності зовнішніх ресурсів і конфеденційності.

Література:

1. *OECD: 2004a, Background Paper for the OECD Workshop on Spam, p. 40–41.*
2. *Myers, J.: 1999, SMTP Service Extension for Authentication, RFC 2554, IETF Network Working Group, p. 92.*
3. *Ramsdell, B.: 2004, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification, RFC 3851, IETF Network Working Group, p. 52.*

ВИЯВЛЕННЯ ЗОВНІШНІХ ЗАГРОЗ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Хмелевський Р.М., Олексійчук М. І.
студент БСЗ-51
Державний університет телекомунікацій
м. Київ, Україна

Стаття присвячена дослідженню зовнішніх загроз інформаційної безпеці об'єктів інформаційної діяльності, а також засадам забезпечення інформаційної безпеки організації. В статті узагальнено існуючі наукові підходи до визначення сутності загроз та джерел, вразливостей, розглянуто класифікації можливих загроз та напрями забезпечення інформаційної безпеки організації. Розглядаються актуальні шляхи виявлення зовнішніх загроз сучасними засобами захисту інформації.

Постановка проблеми

В останні роки в Україні досить стрімко на великих підприємствах почались впроваджуватися корпоративні інформаційні системи (КІС), що базуються на клієнт-серверній архітектурі. Цими системами почались витіснятися традиційні АСУП і цей процес набирає оберти. Стан інформаційної безпеки КІС істотно залежить від зовнішніх загроз прояв яких

може завдати непоправну шкоду комерційній діяльності КІС. Саме тому виявлення зовнішніх загроз в КІС є актуальним.

Аналіз останніх досліджень і публікацій у яких розглянуто перелік найбільш розповсюджених вразливостей та методів їх експлуатуванні на основі даних, зібраних NGFW і системою запобігання вторгненню (IPS) сенсорної мережі та деталізує деякі найпопулярніші та найцікавіші техніки атаки спостерігається дослідниками Check Point у першій половині 2020 року. [1]

Метою статі є дослідження сучасних шляхів щодо виявлення зовнішніх загроз в КІС на основі NGFW і вбудованими IPS/IDS.

Викладення основного матеріалу

Усі шкідливі дії можуть бути здійснені тільки при наявності вразливостей (рис. 1). А якщо є дії, то є найвища загроза їх здійснення, а також наявні джерела, з яких ці загрози можуть виходити.

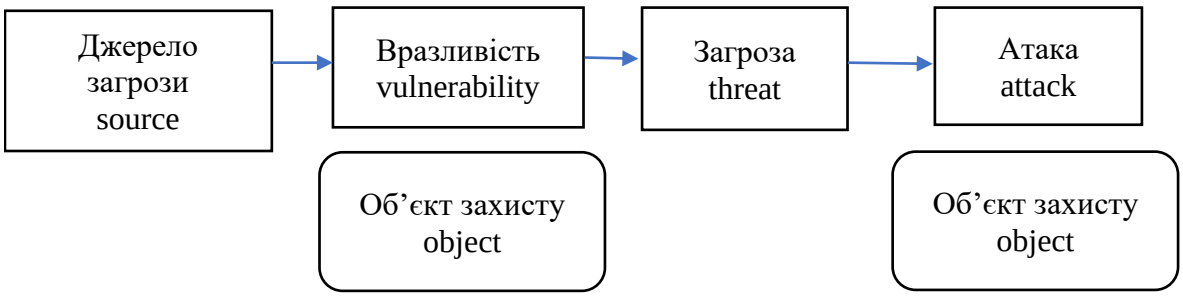


Рис. 1. Механізм формування атаки

Виникає наступний ланцюжок: джерело загрози – уразливість – загроза – атака. Джерело загрози – це потенційні антропогенні, техногенні або стихійні носії загрози безпеці. Вразливість – це властиві об’єкту інформатизації причини, які призводять до порушення безпеки інформації на конкретному об’єкті та зумовлені вадами процесу функціонування об’єкта інформатизації. Загроза – це можлива небезпека(потенційна або така, що існує реально) вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об’єкта захисту (інформаційних ресурсів), яке наносить

збиток власнику або користувачу. Атака – це завжди пара “джерело-уразливість”, що реалізує загрозу та приводить до збитків.[2]

Найбільший інтерес з точки зору організації захисту представляє штучні зовнішні загрози (рис.2), так як дії суб'єкта завжди можна оцінити, спрогнозувати і вжити адекватних заходів.

В якості штучних джерел загроз можна розглядати суб'єкта, що має доступ до роботи зі штатними засобами захисту об’єкта. Розглянемо суб'єктів дії яких можуть призвести до порушення безпеки інформації. Зовнішні джерела можуть бути випадковими або навмисними і мати різний рівень кваліфікації. До них відносяться, наприклад: 1) кримінальні структури; 2) потенційні правопорушники; 3) правопорушники з конкретних організацій; 4) хакери, шахраї; 5) крадії; 6) особи, що навмисно порушили пропускний режим.

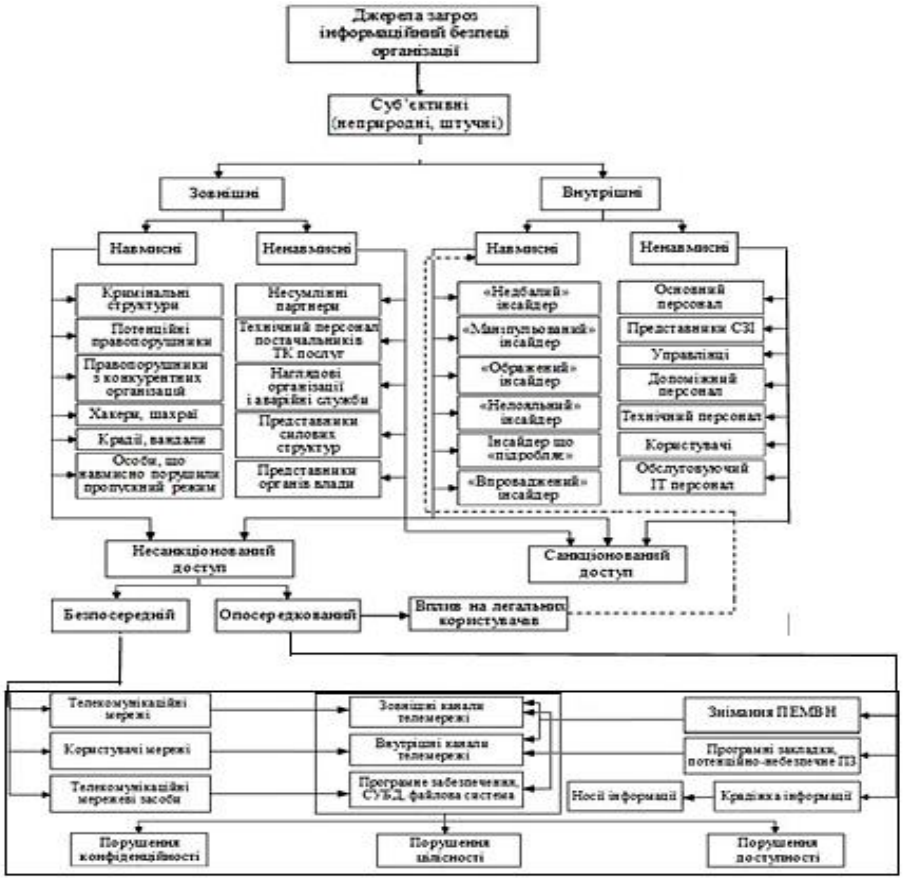


Рис. 2. Класифікація загроз за видами ознак та можливі цілі їх прояву[3]

Враховуючи таке та з урахуванням пропозицій науковців ймовірність реалізації кожної *i*-ої загрози по відношенню до *j*-го активу визначатимемо, використовуючи рівняння (1):

$$d_{rj} = 1 - p_{ri} \times \prod_{i=1}^{m}(1 - p_{rji}), \quad (1)$$

де n – кількість загроз; m – кількість активів; p_{ri} – можливість здійснення і-ої загрози; d_{rj} – можливість реалізації хоча б однієї загрози j-му активу.

При цьому: $$p_{ri} = p_{ti} \times p_{vi}$$

де p_{ti} – можливість появи і-ої загрози; p_{vi} – можливість появи уразливості щодо реалізації і-ої загрози.

Наступним етапом буде обчислювання ціни ризику *Rj* для кожного *j*-го активу:

$$R_j = d_{rj} \times p_j, \quad (2)$$

Ціна повного ризику дорівнює сумі цін ризику для всіх активів за формулою:

$$R_{\text{ПОВН}} = \sum_{j=1}^{n} R_j, \quad (3)$$

Для захисту від зовнішніх загроз традиційно використовувався *мережевий екран*. Традиційні *мережеві екрани* контролюють вхідний та вихідний трафік на пристрої. Вони використовують як статичну, так і динамічну фільтрацію пакетів та підтримку VPN. Це забезпечує дійсне та безпечне з'єднання з мережею та Інтернетом. Традиційні *мережеві екрани* також відображають IP-адреси, перекладаючи адреси - як мережеві, так і портові.

Традиційні *мережеві екрани* та їх наступники мають спільні функції, включаючи фільтрування пакетів та перевірку стану. Розглянемо продукт PfSense це дистрибутив для створення мережевого екрану наступного покоління(NGFW)/ роутера, заснований на FreeBSD. Однак NGFW може робити все, що робить традиційний *мережевий екран*, але краще та пропонує додаткові функції безпеки. Наприклад, NGFW покращують фільтрацію пакетів за допомогою глибокої перевірки пакетів (DPI).

У попередніх поколіннях *мережевий екран використовував* SPI (Stateful Packet Inspection) що запам'ятовував інформацію про поточний стан сесії і проводився аналіз всіх вхідних пакетів для перевірки їх коректності і дозволяти проходити лише пакетам з відомими активними з'єднаннями. У NGFW функція DPI збільшує фільтрацію пакетів для обробки розширених загроз шкідливого програмного забезпечення. Традиційна фільтрація пакетів просто читає заголовок пакета. DPI потрапляє у вміст пакета і порівнює деталі вмісту з базою даних підписів атак. Підписи – це шаблони байтів, які є унікальними для шкідливого програмного забезпечення.

Системи запобігання проникненню (IPS) – це еволюція систем виявлення вторгнень (IDS) і важлива для виявлення загроз, запобігання доступу загрози до мережі та інформування адміністраторів про загрозу. Інструмент IPS Suricata вбудований в pfSense контролює мережу та виявляє загрози в режимі реального часу. Існує кілька різних способів, які IPS може виявити загрози:

Виявлення на основі підпису – порівнює підписи байтів у пакеті з тими, що відомі загрози, часто на основі даних сторонніх розвідувальних даних.

Виявлення статистичних аномалій – порівнює відстежуваний трафік із базовим рівнем, створеним адміністратором для прийнятної поведінки трафіку в мережі. Коли трафік починає поводитися таким чином, що не відповідає очікуваній поведінці, трафік може бути заблокований або позначений для перевірки.

Виявлення аналізу протоколів з використанням стану – також використовує профіль прийнятної поведінки для виявлення статистичної аномалії. Попередні покоління мережевих екранів використовували лише інформацію з четвертого рівня моделі OSI для інформування своїх дій. З іншого боку, NGFW можуть перевіряти трафік з рівнів 2-7. Це означає, що ці мережеві екрани можуть перевіряти сьомий рівень, прикладний рівень. Це

важливо, тому що прикладний рівень – це місце, де дані взаємодіють із користувачем і все частіше використовуються як вектор атаки.

NGFW перевіряє трафік рівня 7 та визначає, з яких портів повинні підключатися пакети додатків, і якщо вони не збігаються, NGFW може блокувати пакети. Наприклад, пакет HTTP був надісланий через порт FTP; NGFW може визнати на основі політики це потенційно підозрілим і запобігти проходженню пакета.

Висновки

Отже, правильно налаштований NGFW з вбудованим IPS дає дуже високий рівень безпеки від зовнішніх загроз. Корпоративна інформаційна система отримує захист периметра від більшості типів шкідливого ПО, значно ускладнює роботу правопорушника, який вирішив атакувати КІС.

Література

1. *Checkpoint cyber-attack 2020 trends* https://pages.checkpoint.com/cyber-attack-2020-trends.html, *2020. –27 с.*
2. *Богуш В. М. Інформаційна безпека держави: [навч. посіб.] / В. М. Богуш, О. К. Юдін. – К.: МК-Прес, 2005. – 432 с.*
3. *Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об’єктів інформаційної діяльності / Р.М. Хмелевський // Сучасний захист інформації. – 2016. – № 4. – С. 65-70.*

УДОСКОНАЛЕНИЙ МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ ВІД ПЕРЕХОПЛЕННЯ МЕТОДОМ ВИСОКОЧАСТОТНОГО НАВ’ЯЗУВАННЯ

Крючкова Л. П., Цмоканич І. В.
Державний університет телекомунікацій
м. Київ, Україна

Розглянуто актуальність проблеми захисту інформації на об'єктах критичної інфраструктури. Висвітлено сутність перехоплення конфіденційної інформації методом високочастотного нав'язування. Описано і запропоновано удосконалений метод захисту інформації від витоку, який досягається генерацією високочастотного сигналу для формування ефекту "биття" частот.

Зараз у світі прослідковується процес глобальної інформатизації суспільства. Реальна безпека держави багато в чому залежить від безпеки її

інформаційних ресурсів і технологій, а забезпечення безпеки інформації залежить від захисту конфіденційної інформації. Саме тому захист національної конфіденційної інформації є одним з головних пріоритетів державної політики.

Одним з ефективних методів перехоплення конфіденційної інформації є метод високочастотного нав'язування. Можливість витоку інформації при використанні високочастотного нав'язування пов'язана з наявністю в колах технічних засобів нелінійних або параметричних елементів [1]. Нав'язувані високочастотні коливання впливають на ці елементи одночасно з низькочастотними сигналами, що виникають при роботі технічних засобів. В результаті цієї взаємодії високочастотні нав'язувані коливання виявляються модульованими низькочастотними (інформаційними) сигналами. Поширення таких модульованих інформаційними сигналами високочастотних коливань струмоведучими колами або шляхом електромагнітного випромінювання у вільний простір створює реальну можливість витоку конфіденційної інформації та подальшого перехоплення.

В даний час застосовуються два методи високочастотного нав'язування:

- за допомогою контактного або індукційного введення високочастотного сигналу в електричні кола, які мають функціональні або паразитні зв'язки з основним технічним засобом;

- шляхом опромінення високочастотним електромагнітним сигналом джерела інформації і прийняття відбитого модульованого сигналу.

Серед загальновідомих методів захисту інформації від перехоплення за допомогою високочатотного «нав’язування» можна вказати наступні: встановлення додаткових конструкцій екранування на початкових етапах розробки апаратури, яка буде використовуватись; встановлення додаткового екранування конструкції; встановлення фільтрації високочастотних зондуючих сигналів в усіх підключених до апаратури електричних колах і

лініях зв’язку. Однак вказані пасивні методи не забезпечують повноцінного захисту інформації.

Нами пропонується застосування активних методів захисту інформації від витоку каналами високочастотного нав’язування. Сутність методу полягає в наступному:

1. Методом радіомоніторингу на об’єкті інформаційної діяльності виявляється частота небезпечного сигналу.

2. У випадку виявлення небезпечного сигналу, високочастотним генератором формується сигнал, спрямований на руйнування інформативних параметрів небезпечного сигналу [2], що унеможливлює перехоплення інформації.

Удосконаленням і новизною запропонованого нами методу є те, що захисні сигнали формуються не тільки на основній частоті небезпечного сигналу, а й на його гармоніках. При цьому частоти сформованих захисних сигналів вибираються таким чином, щоб забезпечити явище «биття» і на основній частоті, і на гармоніках небезпечного сигналу. Це забезпечує більш ефективний захист від перехоплення інформації методами високочастотного нав’язування.

Спираючись на результати досліджень, нами визначено параметри захисних сигналів, спрямованих на забезпечення явища «биття» з небезпечними сигналами високочастотного нав’язування. Нами також встановлено, що ефективність руйнування інформативних параметрів небезпечного сигналу високочастотного нав’язування зростає при формуванні додаткових захисних сигналів, сформованих генераторами коливальної частоти.

В подальшому планується виконання досліджень щодо визначення параметрів захисних сигналів, здатних забезпечити найбільш ефективну захищеність інформації від витоку каналами високочастотного нав’язування.

Література:

1. *Крючкова Л.П., Провозін О.П. Перехоплення мовленнєвої інформації методами високочастотного "нав'язування" // Сучасний захист інформації – 2017. – №3(31), С.74-80.*
2. *Патент 95365 Україна, МПК (2011.01) H04K 3/00. Спосіб захисту інформації / Рибальський О.В., Хорошко В.О., Крючкова Л.П., Джужа О.М., Орлов Ю.Ю.; заявник і патентовласник Національна академія внутрішніх справ. - № a200913327; заявл. 22.12.2009; 55 опубл. 25.07.2011, Бюл. № 14.*

ЗАХИСТ SPA ДОДАТКІВ В МЕРЕЖІ ІНТЕРНЕТ

Покрасьон А. М.
Державний університет телекомунікацій
Навчально науковий інститут захисту інформації
м. Київ, Україна

З розвитком програмних засобів проектування та безпосередньої розробки як веб-додатків так і будь-яких інших ресурсів, що передбачають наявність користувацького інтерфейсу для взаємодії із користувачем, розвивались та вдосконалювались і підходи до розробки систем як таких. На даний момент конфіденційність користувача є важливим етапом на стадії розробки будь якого програмного продукту в цілому.

SPA – це акронім, скорочення від англійського Single-Page Application односторінковий інтерфейс. Ця технологія з'явилась досить недавно, але використовується і застосовується досить активно на даний момент. SPA – це web-додаток розміщений на одній web-сторінці, яка для забезпечення роботи завантажує весь необхідний код разом із завантаженням самої сторінки. Якщо додаток досить складний і містить багатий функціонал, як наприклад, система електронного документообігу, то кількість файлів зі скриптами може досягати декількох сотень, а то і тисяч. А завантаження всіх скриптів жодним чином не означає, що при завантаженні сайту будуть завантажені відразу всі сотні і тисячі файлів з скриптами. Для вирішення проблеми завантаження великої кількості скриптів в SPA використовуюсь API під назвою AMD. AMD реалізує можливість завантаження скриптів на вимогу. Тобто, якщо для "головної сторінки" односторінкового порталу знадобилося 3 скрипта, вони будуть завантажені зразу перед стартом програми. А якщо користувач клікнув на іншу сторінку односторінкового порталу, наприклад, "Про

програму", то принцип AMD завантажить модуль скрипт + розмітка тільки перед тим як перейти на цю сторінку.

То яким чином при розробці SPA-додатку ми можемо забезпечити конфіденційність нашим клієнтам. Перш за все, хочу зазначити, що дані користувача зберігаються на сервері. Користувач, який ввійшов до системи отримує так званий ідентифікаційний ключ за допомогою якого, сервер може ідентифікувати дану особу. Даний ключ ми повинні зберегти у нашому браузері для того, щоб передавати його при кожному запиті на сервер від клієнта. Таким чином у нас є три варіанта де зберігати даний ключ, це може бути Local Storage, Session Storage та Cookie. Який з цих варіантів більш для нас підходить та є більш безпечним?

Короткий огляд Access token і Refresh token

Токени доступу (Access token) зазвичай є недовговічними токенами JWT, підписаними сервером і включеними в кожен HTTP-запит до сервера для авторизації запиту.

Токени оновлення (Refresh token) зазвичай являють собою довговічні зашифровані токенами JWT, що зберігаються в базі даних, які використовуються для отримання нового токена доступу після закінчення терміну його дії.

Де краще зберігати свої токени?

Існує два найпоширеніші способи зберігання токенів: в localStorage і в cookie. Є багато суперечок про те, який з них краще, але більшість людей схиляються до cookie через більшу безпеку.

Давайте розглянемо це порівняння трохи більш докладніше.

Local Storage

Плюси: Це зручно.

- Це чистий JavaScript і з ним зручніше працювати. Якщо у вас немає бекенда і ви покладаєтеся на стороннє API, ви не завжди зможете встановити певні cookie для вашого застосування.

- Працює з API-інтерфейсами, які вимагають, щоб ви помістили свій токен доступу в заголовок запиту, типу такого Authorization Bearer $ {access_token}.

Мінуси: Такий спосіб вразливий до XSS атак.

Атака XSS відбувається, коли зловмисник може запустити свій скрипт JavaScript на вашому сайті під час використання його іншим користувачем. Це означає, що зловмисник зможе отримає доступ до токенів доступу, який ви зберегли в localStorage.

Cookies

Плюси: Файл cookie може бути недоступний через JavaScript, тому він не так вразливий для атак XSS, як localStorage.

- Якщо ви використовуєте прапори httpOnly, то cookie будуть не доступні з JavaScript. Це означає, що навіть якщо зловмисник зможе запустити JS на сайті, він не зможе прочитати ваш токен доступу.
- Cookie автоматично відправляється в кожному HTTP-запиті на ваш сервер.

Мінуси: Залежно від варіанту використання іноді ви не зможете зберігати свої маркери в файлах cookie ..

Розмір файлів cookie обмежений 4 КБ, тому, якщо ви використовуєте великі токени JWT, збереження в файлі cookie стане не можливим.

Існують сценарії, коли ви не можете використовувати cookie безпосередньо для доступу до серверного API. Наприклад коли потрібна наявність токена в заголовку запиту.

Коротко про XSS атаки

Отже ми вже сказали що local storage вразливий, так як він легко доступний за допомогою JavaScript, і зловмисник може отримати access token і використовувати його. Однак, хоча cookie з httpOnly недоступні з JavaScript, це не означає, що за допомогою cookie ви повністю захищені від XSS атак.

Якщо зловмисник може запустити JavaScript у вашому додатку, він все одно зможе відправити HTTP-запит на ваш сервер отримавши таким чином

всі токени. Але для зловмисника це менш зручно, тому що він не зможе прочитати вміст токена, хоча це і не завжди потрібно.

Cookies та CSRF Атаки

CSRF Attack - це атака, яка дозволяє зробити запит від імені користувача але без його відома. Наприклад, якщо веб-сайт приймає запит на зміну електронної пошти через такий запит:

```
POST /email/change HTTP/1.1
Host: site.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
Cookie: session=abcdefghijklmnopqrstu

email=myemail.example.com
```

Рис. 1.1 Приклад запиту

То зловмисник може легко створити форму на шкідливому веб-сайті, яка відправить POST запит на https://site.com/email/change з прихованим полем електронної пошти, і cookie з токенами будуть автоматично включені в цей запит.

Однак це можна легко виправити, використовуючи прапор cookie sameSite і додавши anti-CSRF token.

Тож, хоча куки все ще мають деякі уразливості, вони кращі в порівнянні з localStorage, коли їх застосування можливо. І ось чому?

Як localStorage, так і cookie уразливі для атак XSS, але зловмисникові складніше виконати цю атаку, коли ви використовуєте cookie з httpOnly.

Cookie уразливі для атак CSRF, але їх ймовірність можна зменшити за допомогою прапора sameSite і токенів захисту від CSRF (anti-CSRF tokens).

Ви все ще можете використовувати cookie, навіть якщо вам потрібно використовувати заголовок Authorization: Bearer або ваш JWT більше 4 КБ. Це також узгоджується з рекомендацією спільноти OWASP.

Література:

1. *LocalStorage vs Cookies – https://webdevblog.ru/localstorage-vs-cookies-vse-chto-nuzhno-znat-o-bezopasnom-hranenii-tokenov-jwt-vo-front-end/*
2. *Що таке SPA – http://www.codenet.ru/webmast/js/spa/*
3. *Local Storage vs. Session Storage vs. Cookie – https://ru.hexlet.io/blog/posts/lokalnoe-hranilische-vs-sessionnoe-hranilische-vs-cookie*

УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ІНФОРМАЦІЙНИХ СИСТЕМ МЕТОДАМИ МАШИННОГО НАВЧАННЯ

Гайдур Г.І.,
Найман Г.Г.
аспірант АКБ-125
Державний університет телекомунікацій
м. Київ, Україна

Як не буває абсолютно здорових людей, так і не буває абсолютно захищених інформаційних систем. Компоненти IT-інфраструктури завжди мають вразливості в захисті. Важливо навчитися вчасно виявляти потенційні загрози та реагувати на них до моменту нанесення збитку. Як показує статистика, налагодженість в цьому процесі дозволяє уникнути до 97% всіх інцидентів інформаційної безпеки, пов'язаних з використанням зловмисниками проломів в компонентах інфраструктури. Хоча компанії та установи постійно працюють над захистом та посиленням заходів безпеки, це відбувається не так ефективно. Таким чином, управління вразливостями в інформаційних системах методами машинного навчання може стати плацдармом для виправлення даної ситуації.

Ключові слова: *машинне навчання, управління вразливостями, кібербезпека, методи управління вразливостями, інформаційні системи.*

Управління вразливостями в інформаційних системах - це сукупність процесів виявлення вразливостей в корпоративній мережі, оцінки ризику та вжиття відповідних заходів щодо їх усунення. [1]

Управління вразливістю передбачає роботу над тим, щоб проактивно знайти і виправити потенційні недоліки в архітектурі кібербезпеки. Це виконується з метою застосування виправлень, раніше, аніж зловмисники зможуть використати будь-які недоліки системи. Створення ж системи управління вразливостями, яка регулярно перевіряє наявність нових вразливих ситуацій, є надзвичайно важливою для запобігання порушенням кібербезпеки. Без системи виправлення вразливостей недоліки в безпеці можуть залишатися в мережі протягом тривалого часу, шо надає

зловмисникам більше можливостей використовувати вразливості та проводити атаки. [2]

Тому найперспективнішим засобом управління вразливостями в інформаційних системах є управління вразливостями методами машинного навчання.

Машинне навчання - це «розділ штучного інтелекту, який досліджує методи, що дозволяють комп'ютерам покращувати свої характеристики на основі отриманого досвіду».

Розрізняють два типи машинного навчання: навчання по прецедентах, або індуктивне навчання, і дедуктивне навчання. Навчання по прецедентах, в свою чергу, поділяють на три основних типи: контрольоване навчання, або навчання з учителем, неконтрольоване навчання або навчання без учителя, і навчання з підкріпленням. [3]

Контрольоване навчання - цей метод навчання застосовується у випадках, коли є великі обсяги даних, база вразливостей з маркерами. Необхідно створити алгоритм, за допомогою якого машина могла б визначити, вразливість. У ролі «вчителя» в даному випадку виступає людина, яка заздалегідь проставила маркери. Машина сама обирає ознаки, за якими вона розрізняє вразливості.

Хоча маркованих, розмічених даних накопичилося вже досить багато, даних без маркерів (міток) все ж набагато більше. Це зображення без підписів, аудіозаписи без коментарів, тексти без анотацій. Завдання машини при неконтрольованому навчанні - знайти зв'язку між окремими даними, виявити закономірності, підібрати шаблони, упорядкувати дані або описати їх структуру, виконати класифікацію даних.

Навчання з підкріпленням є окремим випадком контрольованого навчання, але вчителем в даному випадку є «середовище». Машина або «агент» не має попередньої інформацією про середовище, але має можливість здійснювати в ній будь-які дії. Середа реагує на ці дії і тим самим

надає агенту дані, які дозволяють йому реагувати на них і вчитися. Фактично агент і середовище утворюють систему зі зворотним зв'язком.

Навчання з підкріпленням використовується для вирішення більш складних завдань, ніж навчання з учителем і без вчителя. Для машинного навчання використовують різні технології та алгоритми. Зокрема, можуть застосовуватися дискримінантний аналіз, байєсовські класифікатори та багато інших математичних методів. [4]

Управління вразливостями інформаційних систем за допомогою методів машинного навчання допоможе не тільки підвищити ефективність виявлення ризиків кібербезпеки, а і допоможе зменшити час на реагування та виправлення потенційних недоліків в архітектурі інформаційних систем.

Література:

1. *Diogenes Y. Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics / Yuri Diogenes., 2018. – 384 с.*
2. *NIST. Creating a Patch and Vulnerability Management Program / NIST., 2013. – 78 с.*
3. *Математические основы теории машинного обучения и прогнозирования [Електронний ресурс] – Режим доступу до ресурсу: http://iitp.ru/upload/publications/6256/vyugin1.pdf*
4. *Великое пробуждение исскуственного интелекта [Електронний ресурс] – Режим доступу до ресурсу: https://vc.ru/21767-the-great-ai-awakening*

ТЕХНОЛОГІЯ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМИ КОРИСТУВАЧАМИ, ЯКІ ВИКОНУЮТЬ ФУНКЦІЇ АДМІНІСТРУВАННЯ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА НА БАЗІ FUDO PAM

Пікулевич В. П.
БСЗМ-71
Державний університет телекомунікацій
м. Київ, Україна

Розглянуто зміст технології управління привілейованими користувачами, які виконують функції адміністрування інфраструктури підприємства на базі Fudo PAM. Визначено мету і основні завдання щодо управління доступами.

Контроль привілейованих користувачів, або Privileged Account Management (PAM) - це група рішень, призначених для здійснення моніторингу і контролю облікових записів співробітників IT-підрозділів,

системних адміністраторів, співробітників аутсорсингових організацій, що займаються адмініструванням інфраструктури компанії, управління аутентифікацією і авторизацією зазначених співробітників, аудиту виконуваних дій, контролю доступу та запису їх сесій. Крім абревіатури PAM для позначення систем контролю привілейованих користувачів, зустрічаються інші найменування даного класу рішень, наприклад, Privileged User Management (PUM), Privileged Identity Management (PIM), Privileged Access Management (PAM), Privileged Password Management (PPM), Privileged Account Security (PAS).

Рішення, що дозволяють контролювати дії облікових записів співробітників, що мають розширені права, відносяться до групи систем управління обліковими даними (IdM / IAM-системи). Вимоги з моніторингу дій, виконуваних від імені облікових записів з підвищеними привілеями, виникли в зв'язку з потребою багатьох організацій передавати деякі завдання адміністрування і обслуговування інфраструктури в руки сторонніх організацій. Передача критичних ресурсів на IT-аутсорсинг має на увазі під собою серйозні ризики.

PAM-системи мають на увазі під собою наявність наступних функцій:

- централізоване управління обліковими записами з розширеними можливостями;
- аудит дій привілейованих співробітників;
- управління настройками пральний захисту;
- контроль доступу співробітників до адміністративних ресурсів;
- управління процесом аутентифікації і авторизації;
- запис сесії, запущеної з-під облікового запису зі списку привілейованих.

Залежно від виконуваних функцій, системи контролю користувачів з розширеними можливостями діляться на чотири категорії:

- рішення, що дозволяють управляти паролями співробітників і здійснювати контроль доступу до загальних облікових записів (SAPM);

- рішення, що дозволяють управляти сесіями привілейованих користувачів до систем організації використовуючи єдину точку входу або Single Sign-On (PSM), а також моніторинг, запис і збереження інформації про дії користувачів в рамках сесії;
- рішення, що дозволяють аналізувати команди, які використовує адміністратор системи, а також виконувати їх фільтрацію (SPM);
- рішення, що дозволяють здійснювати контроль вбудованих або службових облікових записів, які використовуються різними додатками і сервісами для виконання своїх функцій (AAPM).

Зазначені функції дозволяють вирішувати такі бізнес-завдання, як збільшення ефективності роботи співробітників з привілейованими обліковими записами, скорочення витрат на нелояльний персонал, запобігання витокам конфіденційних даних.

За своєю архітектурою PAM-системи можуть бути виконані як у вигляді програмних, так і програмно-апаратних рішень. Більш того, по організації PAM-системи можуть бути:

- локальні, що вимагають високих капітальних витрат і операційних витрат;
- хмарні, які дозволяють скорочувати витрати за рахунок відсутності необхідності організації і підтримки інфраструктури;
- гібридні.

З огляду на сучасні тенденції розвитку технологій і використання мобільних пристроїв для роботи з конфіденційною інформацією або адміністрування систем, рішення по контролю привілейованих користувачів не можуть стояти на місці і їм доводиться вдосконалюватися з кожним днем. При цьому виникають такі складнощі, як:

- охоплення всіх існуючих каналів адміністрування систем;
- оперативне розпізнавання несанкціонованих дій співробітників;
- однозначна ідентифікація користувачів, що здійснюють несанкціоновані дії;

- накопичення доказової бази поведінки привілейованих користувачів.

Тому технології управління привілейованими користувачами, які виконують функції адміністрування інфраструктури підприємства є важливою складовою забезпечення кібербезпеки інформаційних систем підприємства. Централізоване управління доступами, покращує роботу адміністраторів безпеки, підвищує якість процесу адміністрування, що безпосередньо впливає на кількість вразливостей, які мають місце в корпоративній інформаційній системі.

Література:

1. *FUDO PAM – эффективный контроль привилегированных пользователей. Channel for IT Мир корпоративных ИТ [Електронний ресурс] – Режим доступу: https://channel4it.com/publications/FUDO-PAM-prostoy-i-effektivnyy-kontrol-privilegirovannyh-polzovateley-33809.html*
2. *Privileged Access Management как приоритетная задача в ИБ (на примере Fudo PAM). Habr. TS Solution Системный интегратор [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/tssolution/blog/471750/*
3. *FUDO PAM — простой и эффективный контроль привилегированных пользователей. КО IT для бизнеса. [Електронний ресурс] – Режим доступу: https://ko.com.ua/fudo_pam_prostoj_i_jeffektivnyj_kontrol_privilegirovannyh_polzovatelej_128635*

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ВІРТУАЛЬНИХ СЕРВЕРІВ НА ОСНОВІ ВІРТУАЛЬНИХ МАШИН І ВІРТУАЛЬНИХ КОМУТАТОРІВ

Валетка Д. В.
БСЗМ-71
Державний університет телекомунікацій,
м. Київ, Україна

Розглянуто зміст технології віртуальних машин, актульність використання віртуального аппарату. Наведено приклади IT-Загроз. Представлено способи вирішення проблем безпеки на основі Kaspersky Security

Віртуалізація вже стала загальносвітовим трендом. 94% світових компаній з рейтингу Global 500 і 97% найбільших компаній США зі списку Fortune 1000 вже впровадили віртуалізацію серверів. Безумовно, в Україні і в

інших країнах Східної Європи темпи впровадження віртуалізації нижче, але за цією технологією майбутнє. Що ж стосується конкретних компаній, то зазвичай кожна організація проживає певну еволюцію на шляху впровадження технологій віртуалізації. Як правило, все починається з тестового впровадження, коли віртуалізується тестовий сервер, але з часом технологія активно проникає в роботу компанії, і тоді ми вже говоримо про 90%, а часом і 100% віртуалізації серверів.

У міру впровадження віртуалізації в компанії, на віртуальні машини починають переносити значущі для бізнесу дані, такі як пошта, CRM і ERP системи, фінансові програми, втрата яких недопустима для організацій. З огляду на всі ці фактори, можна з упевненістю стверджувати, що потреба в надійній системі захисту, в тому числі і для віртуального середовища, ще ніколи не була настільки актуальною.

Безумовно, віртуалізація серверів і робочих станцій забезпечує підприємствам значні переваги. В першу чергу, це зниження витрат, а також підвищення продуктивності корпоративної мережі, стабільність роботи і централізоване управління. Але не варто недооцінювати загрози для віртуального середовища, адже зараження системи може не тільки звести нанівець всі ті переваги, заради яких впроваджувалися технології віртуалізації, а й завдати істотної шкоди компанії.

Специфічних загроз, актуальних тільки для віртуальних середовищ, насправді мало. Однак все віруси, створені для «фізичних» серверів, представляють таку ж небезпеку і для віртуальних машин. Тому твердження про те, що віртуальні машини менш уразливі в порівнянні з фізичними - всього лише міф. Більш того, зараження однієї віртуальної машини може поставити під загрозу функціонування інших віртуальних машин, що працюють на тому ж хост-сервері. При цьому більшість шкідливих програм здатні зберігатися на віртуальній машині, навіть коли вона неактивна, і відновлювати шкідливі дії при виході її з сплячого режиму.

Існують два основні підходи до захисту віртуального середовища - це використання повноцінного програмного агента або «тонкого клієнта». Не виключено впровадження комбінованого підходу, коли в одній корпоративної мережі застосовуються обидва методи.

Захист з використанням програмних агентів, має на увазі установку антивіруса на кожну віртуальну машину. Така конфігурація повністю справляється із завданням забезпечення антивірусного захисту сервера, але далеко не завжди є найбільш оптимальним рішенням з точки зору продуктивності. Підхід з використанням програмних агентів можна розділити на два підвиди: стандартне рішення, коли на віртуальні машини встановлюється звичайний антивірус, який «не знає» що він використовується в віртуальному середовищі, і так звані «virtualization-aware» рішення.

У першому випадку, як правило, виникає проблема «шквального» сканування, коли антивірусна перевірка запускається одночасно на декількох віртуальних машинах. Обчислювальні ресурси фізичного комп'ютера в цьому випадку можуть бути перевантажені, що призводить до падіння продуктивності і навіть до аварійної зупинки хост-сервера. А також «шквальний» оновлення: ситуація, що викликається одночасним завантаженням оновлень сигнатурних баз антивірусами на декількох віртуальних машинах.

У другому випадку, при використанні Virtualization-aware рішення, антивірус розподіляє завдання по скануванню віртуальних машин таким чином, щоб не перевантажувати цим хост-сервер і не створювати пікових навантажень на систему.

Втім, в будь-якому випадку установка антивіруса на кожну віртуальну машину неминуче призводить до багаторазового дублювання антивірусного движка і сигнатурних баз, що може негативно позначатися на продуктивності системи в цілому.

Спеціалізовані рішення використовують принципово інший підхід: для антивірусного сканування виділяється одна віртуальна машина, на яку встановлюється спеціалізоване антивірусне рішення - Kaspersky Security for Virtualization. Завдяки цьому досягається оптимальний баланс захисту і продуктивності: виходить, що за захист всіх віртуальних машин на цьому хост-сервері відповідає один антивірус - з одним антивірусним движком і одним екземпляром антивірусних баз.

Є й інші переваги: все нові віртуальні машини, а так само ті віртуальні машини, які з якихось причин тривалий час були вимкнені, при включенні відразу ж автоматично потрапляють під захист Kaspersky Security for Virtualization, у якого завжди найсвіжіша база сигнатур.

Ще однією важливою перевагою Kaspersky Security for Virtualization, що виділяють це рішення на тлі інших, є єдина консоль адміністрування Kaspersky Security Center, з якою тепер можна управляти захистом всієї корпоративної інфраструктури - починаючи від смартфонів, ноутбуків і робочих станцій, і закінчуючи серверами, і в тому числі віртуальними.

Kaspersky Security для віртуальних середовищ є зручним у використанні рішенням, що забезпечує належний рівень захисту і підтримку максимальної щільності віртуальних машин на хост-сервері. Kaspersky Security для віртуальних середовищ забезпечує антивірусний захист без установки антивірусного агента для віртуальних серверів і віртуальних робочих станцій, надає єдину консоль адміністрування як для фізичних пристроїв і віртуальних машин, так і для мобільних пристроїв. Нове рішення виключає можливість виникнення «шквального» сканування, проломів в системі захисту, що з'являються при запуску віртуальних машин після періоду неактивності (Instant-On Gap), а також попереджає дублювання антивірусних сигнатурних баз.

Централізоване антивірусне ядро виключає необхідність встановити антивірусну програму рішення і сигнатурні бази на кожну гостьову машину. На віртуальних машинах функціонує тільки тонкий клієнт (драйвер, що

забезпечує взаємодію віртуальної машини і віртуального пристрою безпеки). Завдяки новітньому антивірусного ядра, в ході перевірки використовуються найсучасніші методи виявлення загроз, а також інтелектуальні технології для мінімізації кількості помилкових спрацьовувань.

Основні відмінності і одночасно конкурентні переваги рішення «Лабораторії Касперського» - це можливість централізованого управління і новітнє антивірусне ядро. Kaspersky Security для віртуальних середовищ надає адміністраторам можливість управляти безпекою фізичних і віртуальних машин, а також мобільних пристроїв з єдиної консолі адміністрування Kaspersky Security Center. Фахівці «Лабораторії Касперського» розуміють, що в корпоративній мережі компанії, яка впровадила віртуалізацію, поєднуються фізичні та віртуальні машини, однаково потребують захисту. На відміну від рішень інших розробників, які змушують своїх клієнтів використовувати для фізичної і віртуальної середовищ різні консолі адміністрування, Kaspersky Security Center забезпечує централізоване управління всіма завданнями щодо захисту від шкідливого ПО з єдиної консолі. Крім того, Kaspersky Security для віртуальних середовищ працює на базі новітнього антивірусного ядра «Лабораторії Касперського», яке, поряд з частими оновленнями, забезпечує високий рівень виявлення загроз.

Література:

1. *Безопасность в виртуальной среде* https://hi-tech.ua/article/bezopasnost-v-virtualnoy-srede/
2. *Безопасность Виртуализации* https://habr.com/ru/post/243895/

АКТУАЛІЗАЦІЯ ІСНУЮЧИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПЕРІОД ПАНДЕМІЇ

Гахов С.О., Гаркавенко Д.М.
аспірант АКБ-125
Державний університет телекомунікацій
м. Київ, Україна

2020 рік продемонстрував вагомість впливу пандемії COVID-19 на розвиток кібератак, спрямованих на корпоративні мережі. У зв'язку з оперативним впровадженням засобів дистанційної роботи корпорації були змушені нехтувати власними політиками і стандартами безпеки. Уразливість систем віддаленого доступу, низький рівень підготовки співробітників і конфігурація користувацького обладнання, що не відповідає мінімальним внутрішнім вимогам корпорації, призвели до різкого зниження рівня захищеності мережевої безпеки корпорацій, незважаючи на те, що дане рішення дозволило зберегти бізнес в цілому.

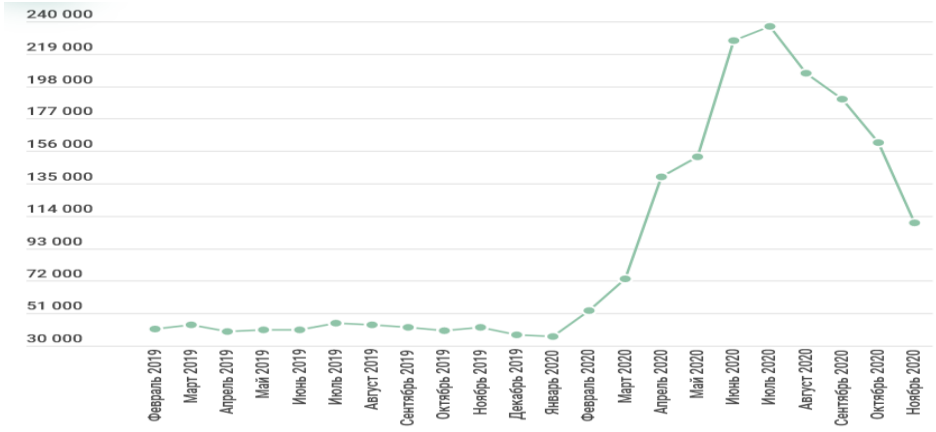


Figure 1: Кількість кіберінцидентів всередині фінансових організацій за період 2019-2020 рік, статистичні дані надані Global Research & Analysis Team 2 грудня 2020 [5]

Аналіз даних про діяльність APT угруповань за 2-3 квартал 2020 року показав, що зловмисники акцентують свою увагу на експлуатації вразливостей мережевих пристроїв. Яскравим прикладом є тенденція атак на мережеві шлюзи, розглянуті в статтях [2][3][4].

Окрім цього, зріс рівень складності проведення атак [5], наприклад, використання легітимних служб популярних сервісів або компрометація

прошивки завантажувача UEFI, що значно ускладнює детекцію інцидентів системами виявлення вторгнень, заснованих на правилах.

Одночасно з цим спостерігається зростання активності зловмисників, які використовують уразливості протоколів, що надають віддалений доступ до комп'ютера в силу того, що якість конфігурації RDP-серверів значно знизилась в силу збільшення їх кількості.

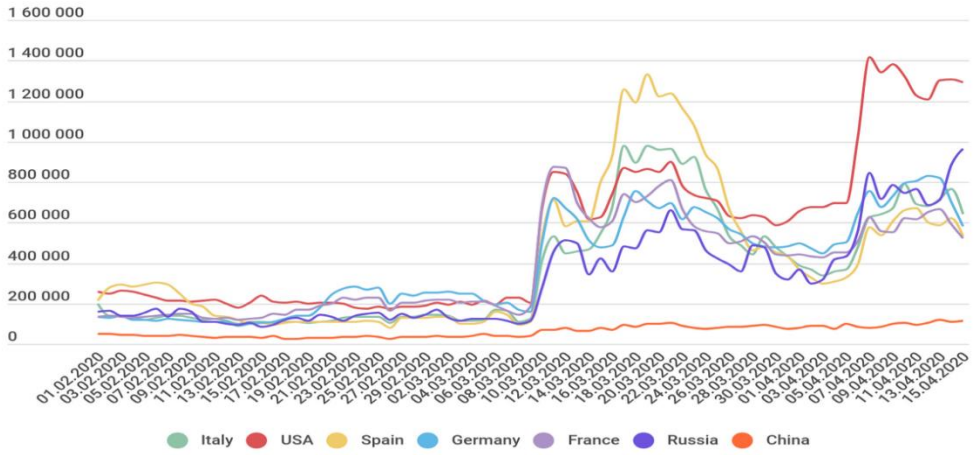


Figure 3: Розподіл атак на RDP-сервера по країнам в 2020 році. Статистичні дані надані securelist 29 квітня 2020 [5].

Даний тренд вказує на необхідність актуалізації існуючих методів забезпечення інформаційної безпеки. Згідно з даними, наданими SANS Institute, детектори аномалій і BREACH атак, в сукупності з дотриманням класичних заходів, значно підвищують захищеність системи щодо мережевої безпеки підприємства.

Звісно, впровадження системи аналізу мережевого трафіку неможливий на ранніх етапах зрілості оскільки у корпорації, як мінімум, повинні бути впроваджені відповідні інструменти управління, але аналіз трафіку надає значні переваги на превентивному етапі, де виявлення аномалій і порушень заплановано. Послідовність застосування тих чи інших заходів безпеки не повинно порушуватися на догоду впровадження нових.

Завдання пошуку аномалій можливо ефективно вирішити за допомогою кластеризації даних мережевої активності. Як правило, завдання кластеризації даних вирішуються алгоритмами, похідними від карт Кохонена.

Враховуючи специфіку сфери застосування, доцільним є використання інкрементно зростаючого нейронного газу – IGNG, що є похідним від GNG.

GNG або нейронний газ – це адаптивний алгоритм нейронної мережі, натхненний самоорганізаційною картою Кохонена, що направлений на оцінку щільності розподілення даних. В простір даних впроваджують нейрони, котрі при роботі алгоритму підлаштовують розташування.

Нейронний газ не використовує гіпотезу про стаціонарність даних, що дозволяє приймати не фіксований масив даних, а функцію, залежну від часу.

Основною перевагою IGNG над GNG є висока швидкість навчання та обробки даних.

Основні принципи алгоритму IGNG полягає у використанні мережі адаптивного резонансу з подальшим пошуком найближчого нейрону на первинному етапі. Якщо різниця не перевищує деякий поріг – корегується вага, інакше проводиться зміна координати нейрона у просторі даних. Якщо поріг не був подоланий, то створюються нові нейрони, що краще наближають значення ідентифікованих даних.

Нейрони також мають параметр віку, на відмінність від GNG, де цей параметр притаманний лише дугам.

Новий нейрон не є активним деякий час. Якщо етап навчання мережі закінчився, то нові неактивні нейрони не приймають участі у кластерізації.

Цикл роботи алгоритму починається з пустого графу. Параметр σ ідентифікується як середньоквадратичне відхилення по навчальній вибірці (1):

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(i - \acute{x})^2} \quad (1)$$

Параметр $\bar{x}$ – середнє між координатами по вибірці.

Основний цикл зменшує значення σ, що є порогом близькості, та розраховує різницю між попереднім рівнем якості кластерізації та рівнем, який отримали у результаті кластерізації процедурою IGNG. Якість кластерізації знаходять за індексом CHI – чим більшим є це значення, тим

краще. Якщо різниця між індексами після кластерізації та до неї буде негативною – кластерізація виконана успішно.

Алгоритм має три взаємовиключних етапи:

– Не знайдено жодного нейрону.

– Знайдено один нейрон, що задовольняє умовам.

– Знайдено два нейрона, що задовольняють умовам.

Після виконання одного з цих етапів інші не виконуються.

На першому кроці виконується пошук нейрона, що найкраще наближує семпл даних (2):

$$c_1 = \underset{dist(\xi, w_c)}{min} \quad (2)$$

Якщо не було знайдено жодного задовольняючого умові $dist(\xi, w_c) \leq \sigma$ нейрона – створюють новий неактивний нейрон з координатами семплу у просторі даних. Якщо такий нейрон було знайдено, то проводиться пошук другого нейрону аналогічним чином. Якщо його немає – він створюється.

Якщо знайдено два нейрона, що задовольняють умовам, їх координати корегуються наступним чином(3):

$$\epsilon(t)h_{c,c_i} = \begin{cases} \epsilon_b, \text{якщо} c = c_i \\ \epsilon_n, \text{якщоєзв'язокс} c_i \\ 0, \text{уіншихвипадках} \end{cases} \quad (3)$$

Де:

$\epsilon(t)$ – шаг адаптації.

c_i – номер нейрона.

h_{c,c_i} – функція сусідства нейрона c з переможцем.

Вона вертає 1 для прямих сусідів, або 0 у інших випадках. Це означає, що шаг адаптації w не є нульовим лише для прямих сусідів.

$$\Delta w_c = \epsilon(t)h_{c,c_i}\|\xi - w_c\| \quad (4)$$

$$w_c = w_c + \Delta w_c \quad (5)$$

На наступному кроці (4, 5) створюється чи оновлюється дуга між нейронами-переможцями, а вік усіх інших дуг зростає. Слід за цим видаляють усі дуги, якщо їх вік перевищує α_{max}. На наступному етапі

видалюються усі активні нейрони, з котрих не виходять ніякі дуги, а вік усіх нейронів-сусідів нейрона-переможця зростає. Якщо вік неактивного нейрона перевищує age_{mature}, він становиться активним.

Остаточний граф включає лише активні нейрони.

Growing Neural Gas не є алгоритмом кластерізації сам по собі; він зменшує розмір вхідний вибірки до деякого набору типових представників, що значно спрощує подальший пошук аномалій.

Література:

1. *Киберугрозы для финансовых организаций в 2021 году [Електронний ресурс] // Securelist. – Режим доступу: https://securelist.ru/cyberthreats-to-financial-organizations-in-2021/99420/.*
2. *Forget Your Perimeter: RCE in Pulse Connect Secure [Електронний ресурс] //gosecure. – Режим доступу: https://www.gosecure.net/blog/2020/08/26/forget-your-perimeter-rce-in-pulse-connect-secure/*
3. *Hacker groups chain VPN and Windows bugs to attack US government networks [Електронний ресурс] // zdnet. – Режим доступу: https://www.zdnet.com/article/hacker-groups-chain-vpn-and-windows-bugs-to-attack-us-government-networks/*
4. *SonicWall VPN Portal Critical Flaw (CVE-2020-5135) [Електронний ресурс] // tripwire. – Режим доступу: https://www.tripwire.com/state-of-security/vert/sonicwall-vpn-portal-critical-flaw-cve-2020-5135/*
5. *Прогнозы по продвинутым угрозам на 2021 год [Електронний ресурс] // securelist – Режим доступу: https://securelist.ru/apt-predictions-for-2021/99366/*

ЗАХИСТ ТРАФІКУ В МЕРЕЖАХ ДЛЯ IOT НА ОСНОВІ КЛІЄНТ-СЕРВЕРНОЇ АРХІТЕКТУРИ

Кіктєв В. В.
студент 4 курсу, групи БСД-44
Державного університету телекомунікацій
(066) 022 96 99, flamgail@gmail.com
м. Київ, Україна

У наші часи все більш популярнішим стає термін IoT. Інтернет речей (IoT) – концепція мережі передачі даних між фізичними об'єктами, оснащеними вбудованими засобами і технологіями для взаємодії один з одним або з зовнішнім середовищем [1, с. 4]. Ми можемо віддалено або локально управляти нашим житлом за допомогою розумних пристроїв. У той же час постає питання захисту персональних даних від зловмисників, які можуть їх використовувати проти вас у своїх незаконних цілях, що може піддати вас небезпеці або фінансових втрат. Тому в першу чергу варто задуматися про захист нашої мережі IoT.

Головна мета в захисті мереж IoT – це не допустити потрапляння трафіку в неналежні руки. Навіть, якщо трафік можна буде перехопити, то наша мета – зробити його зашифрованим і не дозволити зловмиснику розшифрувати його. Ми досліджували мережу IoT на основі клієнт-серверної архітектури, так як це одна з найпоширеніших варіацій реалізації даних мереж.

Найбільш поширеним є клієнт-серверна архітектура. «Клієнт-сервер» – обчислювальна або мережева архітектура, в якій завдання або мережева навантаження розподілені між постачальниками послуг, званими серверами, і замовниками послуг, званими клієнтами [2, с. 2]. Фактично клієнт і сервер – це програмне забезпечення. У мережі інтернету речей сервер спілкується з пристроями і датчиками, обробляє інформацію, посилає потрібні команди, і зберігає в собі всі дані. Самі пристрої виконують свою певну функцію, тобто є джерелом даних про навколишнє оточення і посилають всі дані для обробки на сервер. І саме цей процес передачі є найбільш вразливим місцем у всій системі. Найбільш ефективним способом захисту є використання MQTT (Message Queue Telemetry Transport) – це легкий, компактний і відкритий протокол обміну даними створений для передачі даних на віддалених локаціях, де потрібно невеликий розмір коду і є обмеження по пропускній здатності каналу. Перераховані вище напрями дозволяють застосовувати його в системах M2M (Machine-to-machine) і IoT (Internet of Things) [3, с. 5].

Основні особливості протоколу MQTT:

– Асинхроний протокол;
– Компактні повідомлення;
– Робота в умовах нестабільного зв’язку на лінії передачі даних;
– Підтримка декількох рівнів якості обслуговування (QoS);
– Легка інтеграція нових пристроїв.

Для забезпечення безпеки в MQTT протоколі реалізовані наступні методи захисту:

– Автентифікація клієнтів. Пакет CONNECT може містити в собі поля USERNAME і PASSWORD. При реалізації брокера можна використовувати ці поля для автентифікації клієнта;

– Контроль доступу клієнтів через Client ID;

– Підключення до брокера через TLS/SSL.

Досліджуючи проблемні аспекти систем на базі клієнт-серверної архітектури на прикладі IoT і хмар актуальними є проблеми стійкості до помилок та захищеності, самоадаптації, управління якістю сервісів, масштабованості.

Розглядаючи в роботі наше завдання задаємся наступним формальним кортежем:

$$(S, A, P, R, C, f) \quad (1)$$

де: S – *система IoT зі всіма вбудованими пристроями;* A – *модель можливих атак на систему S;* P – *показники захищеності та показник складності атаки;* R – *вимоги до захисту системи на основі показників P;* C – *безліч компонентів клієнт-серверного захисту з використанням показників P*.

Будування відображення *f*, на основі значень *S, A і P* дозволяє отримати набір складників клієнт-серверного захисту *C* щоб задовольнити вимоги *R*. Вимоги захищеності обумовлюється набором специфічних атак з *A*. Здійсненність вимог обґрунтованості визначають коректність спрацьовування компонентів захисту з мінімізацією помилок першого і другого роду в процесі виявлення атак.

Таким чином ми захищаємо наш трафік від зловмисників, шляхом додавання методу шифрування і додаткових заходів безпеки. Якщо використовувати програму моніторингу трафіку можна переконатися, що всі передані дані є зашифрованими і не піддаються розшифруванню. Таким чином ми можемо не хвилюватися, що наші дані будуть використані проти нас.

Література:

1. *Internet Of Things. Gartner IT glossary. Gartner (5 May 2012). – «The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment».*
2. *Валерий Коржов. Многоуровневые системы клиент-сервер. Издательство Открытые системы (17 июня 1997).*
3. *Bryan Boyd et al. Building Real-time Mobile Solutions with MQTT and IBM MessageSight. IBM Redbooks, 2014.*

ЗАХИСТ ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА

Хорольський К. А.
студент 4 курсу, групи БСД-44
+380 96 840 80 45, horolskiy00@gmail.com
Гахов С. О.
доцент кафедр ІКБ
Державнйи університет телекомунікацій
м. Київ, Україна

Сьогодні ми використовуємо підключення до інтернету пристрою у всіх аспектах нашого життя. Ми виходимо в інтернет для пошуку інформації, покупок, банківських операцій, виконання домашніх завдань, ігор і підтримки зв'язку з сім'єю і друзями через соціальні мережі. В результаті наші пристрої містять величезну кількість особистої інформації про нас. Це можуть бути банківські та інші фінансові документи, а також медична інформація-інформація, яку ми хочемо захистити. Якщо ваші пристрої не захищені, викрадачі особистих даних та інші шахраї можуть отримати доступ і вкрасти вашу особисту інформацію. Спамери можуть використовувати ваш комп'ютер в якості "зомбі-дрона" для розсилки спаму, який виглядає так, як ніби він виходить від вас. Шкідливі віруси або шпигунські програми можуть потрапити на ваш комп'ютер, сповільнюючи його роботу або знищуючи файли.

- Тримати свій пристрій в безпеці.

Завантажити рекомендовані оновлення від виробника вашого пристрою або постачальника операційної системи, особливо для такого важливого програмного забезпечення, як ваш інтернет-браузер.

Ці оновлення можуть усунути недоліки програмного забезпечення, які дозволяють хакерам переглядати вашу діяльність або красти інформацію.

- Антивірусне програмне забезпечення

Антивірусне програмне забезпечення захищає пристрій від вірусів, які можуть знищити ваші дані, уповільнити або привести до збою вашого пристрою або дозволити спамерам відправляти електронну пошту через ваш профіль. Антивірусний захист сканує файли на наявність вірусів, а потім видаляє все шкідливе.

Анти-шпигунське програмне забезпечення та брандмауери також є важливими інструментами для запобігання атак на ваш пристрій.

- Надійні паролі

Захист своїх пристроїв і облікових записів від зловмисників, вибравши паролі, які важко вгадати.Треба використовувати надійні паролі, які містять не менше восьми символів, комбінацію букв, цифр і спеціальних символів. Не треба використовувати слово, яке легко можна знайти в словнику, або будь-яке посилання на особисту інформацію, наприклад День народження.

- Резервне копіювання комп'ютера.
- Захист мережі Wi-Fi

Також домашню мережу Wi-Fi потрібно обов'язково тримати закритою. Для цього використовується пароль. В іншому випадку сторонні можуть легко проникнути в ПК і скористатися будь-якою інформацією, включаючи і конфіденційну[1].

- Відмова від використання громадських ПК і бездротових мереж

Використання громадських ПК несе в собі величезні ризики витоку персональної інформації, зараження шкідливим ПЗ, контролю переміщення мережі, збору паролів, поширення вірусів.

- Використання піратського програмного забезпечення.

Завжди будьте обережні з програмами, які ви завантажуєте і запускаєте. Завантажуйте і запускайте тільки те програмне забезпечення, яке широко відомо і заслуговує довіри або рекомендовано надійними сайтами[2].

- Віруси на USB носіях.

Література:

1. *https://uk.wikipedia.org/wiki/Захист_у_мережах_Wi-Fi*
2. *https://support.microsoft.com/uk-ua/windows/захист-комп-ютера-вдома-c348f24f-a4f0-de5d-9e4a-e0fc156ab221*

БІЗНЕС МОДЕЛЬ ІОТ ПРИСТРОЇВ ЗА ДОПОМОГОЮ BITCOIN NETWORK

Гай Д.О
Державнйи університет телекомунікацій
м. Київ, Україна

Анотація. Розглянуто та запропоновано бізнес модель з використанням Lightning Network. Змодельована принципова схема цього методу в логістичному напрямку.

Lightning Network (LN) - платіжний протокол якій виконує операції над блокчейном, що дозволяє проводити миттєві транзакції між вузлами. LN - надає нову бізнес модель в системі Інтернет речей. Завдяки такій технології можливо збільшити потенціал до закупівлі IoT. Перевагою такої системи є можливість використовувати IoT у мережевих транзакцій. Тим не менше, неможливо запустити LN на обмеженому ресурсами IoT пристроїв через вимоги до зберігання, пам'яті та обробки. Тому в цій роботі ми пропонуємо ефективну та безпечний протокол, який дозволяє пристрою IoT використовувати функції LN через вузол LN шлюзу. Ідея полягає у залученні IoT пристрій у операціях LN із цифровим підписом шляхом заміни оригінальні канали з двома підписами 2 з 2 на мультипідписи 3 із 3 каналів[1]. Наш протокол примушує шлюз LN запитувати криптографічний підпис пристрою IoT для всіх операцій на каналі. У нашій системі є п’ять об’єктів, які є пристроєм IoT, шлюз IoT, шлюз LN, вузол LN та місту між пунктами призначення вузлів LN, як показано на рис. 1.

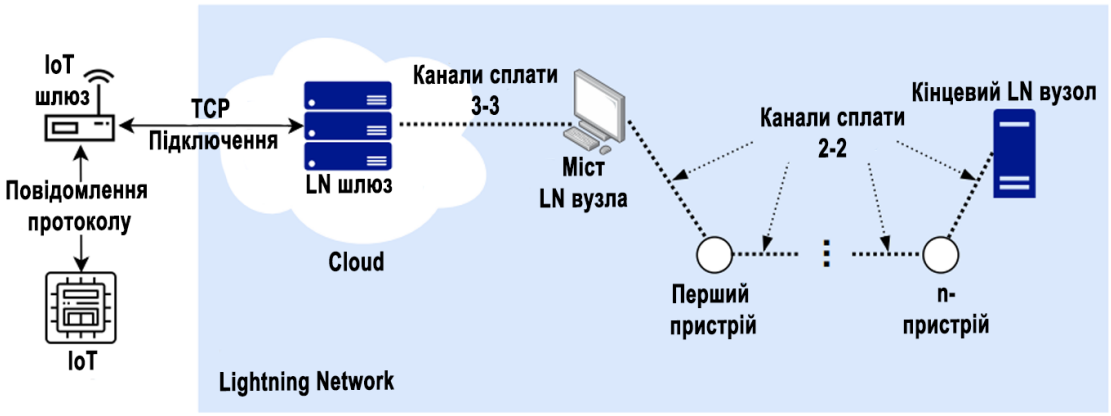


Рис. 1 — Модель використання LN з IoT

Пристрій IoT хоче сплатити цільовому вузлі LN за товари чи послуги. Шлюз IoT є відповідальний за підключення з пристроєм IoT до Інтернету. За допомогою цього Інтернет-з'єднання, пристрій IoT може досягти шлюзу LN, який управляє вузлами Bitcoin та LN і можуть розміщуватися в будь-якому місці. Вузл мосту LN - це вузол, до якого здійснюється шлюз LN відкриває канал на запит пристрою IoT. Цей вузол може бути будь-яким вузлом LN в Інтернеті і визначається шлюзом LN. Через вузол мосту LN, пристрій IoT платежі перенаправляються на кінцевий вузол LN на вказаний IoT-пристрій.

Щоб оцінити запропонований метод, потрібно створили установку де пристрій IoT підключається до шлюзу LN для надсилання платежів на LN. Щоб імітувати пристрій IoT можливо використовувати Raspberry Pi і шлюз LN якій може бути налаштований на настільному комп'ютері. Настільний комп'ютер повинен розташовуватися на віддаленому місці, а Raspberry P поряд. В цій установці використовується програмне забезпечення bitcoind [2], для вузла LN – можливо використовували lnd від Lightning Labs [3] в якому є повна реалізація протоколу LN. Цю систему дуже зручно використовувати під час логістичних перевезень. Коли автомобіль потрапляє в діапазон зв'язку платного збору бездротової системи вона надсилає запит шлюзу IoT та виконує ініціювання платежу. IoT шлюз передає цей запит шлюз LN, який негайно створює платіж LN і відправляє його на вузол LN платного центру. Після завершенні транзакції машину повідомлено про успішну оплату. Щоб

це працювало швидко і коректо процес відправлення платежу повинен бути завершений перед автомобілем і не виходити із діапазону зв'язку бездротової системи платного зв'язку.

Висновок. У цій роботі запропонували безпечний та ефективний протокол надання можливості пристроям IoT використовувати LN біткойна для надсилання платежів.

Література:

2. *Bitcoin.org, "Running a full node," accessed 2021-03. [Online]. Available:*
3. *L.Labs,"Lightning network daemon," accessed 2021-03. [Online]. Available: https://github.com/lightningnetwork/lnd*

МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ДОСТУПУ КОРИСТУВАЧІВ ДО ІНТЕРНЕТ

Деркач В. М.
БСД-45
Державний університет телекомунікацій
м. Київ, Україна

Визначено мету і основні завдання щодо забезпечення безпечного доступу користувачів до Інтернет. Розглянуто методи та засоби забезпечення безпечного доступу користувачів до Інтернет на базі DNS-платформи Quad9. Розроблено рекомендації щодо застосування методів та засобів забезпечення безпечного доступу користувачів до Інтернет.

Сучасні людина та бізнес не уявляються без застосування глобальної мережі Інтернет. У той же час Інтернет несе загрозу злочинних дій по відношенню до них. Тому постає гостра проблема забезпечення безпечного доступу користувачів до Інтернету.

Для того, щоб Інтернет став ефективним інструментом, користувачі повинні довіряти своїй здатності користуватися онлайн-послугами та не боятися крадіжок, шахрайства або зловживання їх пристроями зловмисниками. Державні та приватні оператори мереж потребують захисту від зловмисного використання ресурсів інфраструктури та атак на своїх

користувачів або клієнтів. Тому постає проблема створення та використання відповідних методів та засобів забезпечення безпечного доступу користувачів до Інтернет.

Необхідно зазначити, що кіберзлочинці продовжують атакувати державні та приватні організації із загрозливою швидкістю. Зловмисники часто націлені на державні та приватні організації, тому що знають, що їх командам безпеки необхідно запускати складні системи, а також мати справу з численними сторонніми системами і службами. Багато команд з кібербезпеки також борються зі скороченням бюджетів на безпеку і нестачею кваліфікованих фахівців з кібербезпеки і мережевих технологій для заповнення відкритих вакансій. Пандемія COVID-19 і подальше зростання віддаленої роботи державних службовців і запитів громадян на доступність державних ресурсів в Інтернеті тільки погіршили їх проблеми з безпекою [1].

За даними McAfee кіберзлочинці зосередили свою увагу на домашній поверхні атаки, збільшивши кількість різних схем фішингових повідомлень по каналах зв'язку. Кількість шкідливих фішингових посилань, заблокованих McAfee, зросла з березня по листопад 2020 року більше ніж на 21%, в середньому понад 400 посилань на будинок. Це збільшення є значним і передбачає потік фішингових повідомлень з шкідливими посиланнями, що потрапляють в домашні мережі через пристрої з більш слабкими заходами безпеки [2].

Пересічні та бізнес-користувачі можуть додатково вибирати брандмауери DNS. Серед добре відомих загальнодоступних брандмауерів DNS є:

Cloudflare (1.1.1.1 та 1.0.0.1);

Cisco (208.67.222.222 та 208.67.220.220);

Google (8.8.8.8 та 8.8.4.4);

Quad9 (9.9.9.9 та 149.112.112.112).

Quad9 – це безкоштовна рекурсивна платформа DNS з довільним доступом, яка забезпечує кінцевим користувачам надійний захист, високу

продуктивність і конфіденційність. Quad9 був розроблений Global Cyber Alliance (GCA), міжнародною некомерційною організацією, заснованою партнерством правоохоронних і дослідницьких організацій, орієнтованих на боротьбу з системними кіберризиками реальними, вимірними способами.

Quad9 блокує відомі шкідливі домени, запобігаючи підключення комп'ютерів і пристроїв Інтернету речей організації та користувачів до шкідливих або фішингових сайтів. Кожен раз, коли користувач Quad9 натискає на посилання веб-сайту або вводить адресу в свій веб-браузер, Quad9 перевіряє сайт за списком доменів, складеним більш ніж з 18 різних партнерів з аналізу загроз. Кожен партнер по аналізу загроз надає список шкідливих доменів, заснований на евристичному аналізі чинників, таких як виявлення відсканованих шкідливих програм, поведінку мережевих IDS в минулому, розпізнавання візуальних об'єктів, оптичне розпізнавання символів (OCR), структура і зв'язок з іншими сайтами, а також з окремими повідомленнями про підозрілу або зловмисну поведінку.

На основі результатів Quad9 дозволяє або відхиляє спробу пошуку, запобігаючи підключення до шкідливим сайтам при збігу. Quad9 направляє запити DNS вашої організації через захищену мережу серверів по всьому світу. Його настройка дуже проста, так як не потрібно ніякої реєстрації, і, що найбільш важливо, вона служить дуже винахідливою безкоштовної службою блокування, доступною для будь-якої організації або окремої особи.

Брандмауери DNS працюють так само, як і інші брандмауери, перериваючи потік інформації до шкідливим мережевим місцезнаходженням. На рівні DNS можна заблокувати шкідливі домени, запобігаючи потенційно шкідливій комунікації [3].

Крок 1 (рисунок 1) починається з необхідності перетворити доменне ім'я в маршрутизацію Інтернет-адреса. Це може бути ініційовано користувачем, який переглядає Інтернет, або додатком, який намагається отримати доступ до мережного ресурсу, шкідливим програмним забезпеченням або відповідними командами. Незалежно від джерела всі

запити відправляються на брандмауер DNS.

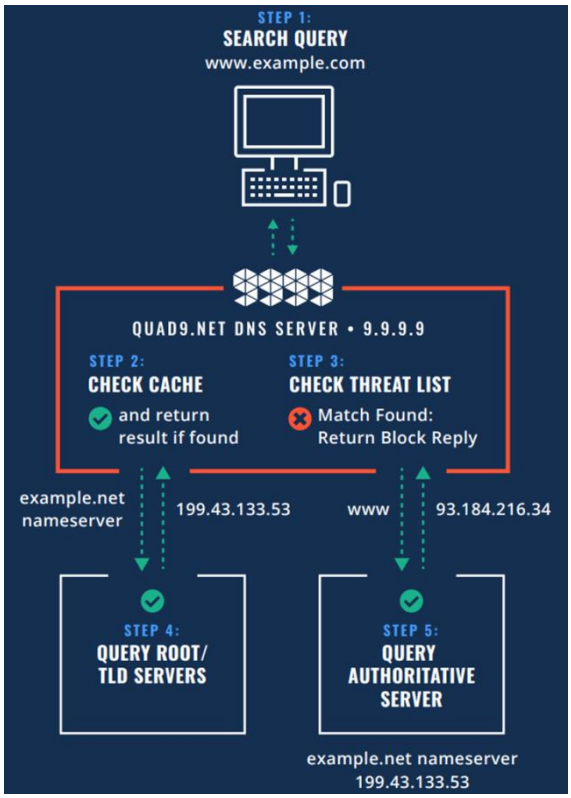


Рис. 1. Принцип роботи DNS-платформи Quad9 [3]

На кроці 2 брандмауер DNS перевіряє свій локальний кеш, щоб визначити, кешований чи ні дозвіл. Якщо він знайдений, він поверне маршрутизацію адреса; якщо він не знайдений, брандмауер DNS перевірить запитане доменне ім'я за списком відомих шкідливих адресатів. Якщо запит відповідає зловмисному місцю призначення, брандмауер DNS поверне блокуючу відповідь, яка ефективно запобігає доступу джерела до зловмисного місця призначення.

Однак, якщо доменне ім'я не кешовано і не виявлено в списку зловмисних адресатів, воно буде брати участь в процесі DNS як зазвичай, запитуючи адреси у серверів кореневого домену або домену верхнього рівня (TLD) і, в кінцевому підсумку, у DNS-сервера, який знає маршрутизацію адреса запитаного доменного імені.

За оцінками [3] зроблено висновок, що брандмауер DNS є важливим засобом контролю проти однієї третини порушень в наборі даних Data Breach Investigations Report за останні п'ять років.

Дуже багато організацій та підприємств ще не використовують брандмауер DNS. Наприклад, Cisco Umbrella стверджує, що 68% організацій цього не роблять.

Основними рекомендаціями щодо забезпечення безпечного доступу користувачів до Інтернет є:

для організацій та підприємств: найближчим часом варто дослідити можливості брандмауерів DNS як додаткового рівня забезпечення безпеки та впровадити у себе;

фізичним особам: варто використовувати брандмауер DNS, наприклад Quad9;

виробникам систем: вважаємо, що виробники систем повинні серйозно подумати про те, щоб використовувати в своїх системах за замовчуванням сервіс брандмауера DNS або зробити інші кроки, щоб спростити його включення;

виробникам маршрутизаторів: необхідно втілити механізм застосування брандмауера DNS та зміни його провайдерів;

органам стандартизації та регуляторам: необхідно враховувати застосування брандмауерів DNS та розглядати в багатьох стандартах безпеки.

Таким чином, запропоновані в роботі рекомендації мають сприяти забезпеченню підвищеної безпеки приватних осіб, бізнес-користувачів і їх клієнтів в мережах, пристроях, цифрових активах і продуктах IoT.

Застосування рішення Quad9 на базі DNS-платформи забезпечує ефективний додатковий рівень захисту. Це досягається шляхом маршрутизації DNS-запитів через мережу серверів безпеки по всьому світу. Рішення Quad9 базується на даних про загрози, які зібрані від ряду авторитетних компаній, що займаються кібербезпекою, для оцінки ризиків кожного веб-сайту, що відвідує користувач в режимі реального часу і блокує доступ до них.

Література:

1. *Michael Aliperti. Malware, Malicious Domains, and More: How Cybercriminals Attack SLTT Organizations [Електронний ресурс] – Режим доступу: https://www.standingstonebank.com/wp-content/uploads/sites/174/September-Cyber-Tip-Newsletter.pdf.*
2. *McAfee Labs Threats Report. November 2020 [Електронний ресурс] – Режим доступу: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf.*
3. *THE ECONOMIC VALUE OF DNS SECURITY. Adam Shostack, Jay Jacobs and Wade [Електронний ресурс] – Режим доступу: Baker https://www.globalcyberalliance.org/wp-content/uploads/GCA-DNS-Security-Report.pdf.*

МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНУ СИСТЕМУ ПІДПРИЄМСТВА

Панченко В. Ю.
БСД-45
Державний університет телекомунікацій
м. Київ, Україна

Визначено мету і основні завдання щодо виявлення та попередження вторгнень в інформаційну систему підприємства. Розглянуто методи та засоби виявлення та попередження вторгнень в інформаційну систему підприємства. Розроблено рекомендації щодо застосування методів та засобів виявлення та попередження вторгнень в інформаційну систему підприємства.

Сьогодні підприємства широко застосовують інформаційні технології для підвищення ефективності свого бізнесу. Треба передбачати можливий вплив зловмисників та вживати заходів підвищення безпеки інформаційних систем підприємств та організацій.

Дана проблема ще більш загострюється у сьогоднішніх умовах пандемії COVID-19, коли значна частина підприємств перейшла на відділену роботу працівників-користувачів їх інформаційних систем.

Для виявлення несанкціонованого доступу до інформаційної системи підприємства та протидії йому використовують систему виявлення та запобігання вторгненням (Intrusion Prevention System, IPS). Вважається, що система IPS має бути обов'язковою для сучасних компаній, що працюють з цифровими даними і піклуються про безпеку інформації. Вона відстежує

активність в мережі в реальному часі і швидко вчиняє дії по запобіганню атак ззовні.

Системи IPS доповнюють міжмережеві екрани, захист інформації в яких відбувається шляхом обмеження трафіку з певними властивостями для запобігання зовнішніх вторгнень. IPS аналізує трафік та реагує при виявленні підозрілої активності. Ці технології доповнюють один одного, створюючи потужний бар'єр на шляху зловмисників.

Від правильного визначення умов функціонування інформаційної системи підприємства, вибору та обґрунтування складу методів та засобів виявлення та попередження вторгнень та ефективного їх застосування залежить ефективність забезпечення кібербезпеки інформаційних систем підприємства.

Як зазначається в [1] захист периметра не може зупинити зловмисника від бічного переміщення всередині корпоративної мережі для доступу до записів і їх ексфільтрації. У той же час на атаки за участю інсайдерів, які вже знаходяться в периметрі, доводиться все більший відсоток зломів. Замість того, щоб покладатися на безпеку на основі периметра, підприємства повинні зосередитися на моніторингу, виявленні та блокування шкідливого внутрішнього трафіку в якості основного компонента своєї стратегії безпеки.

Для належного захисту від кіберзагроз, що проникають через периметр, а також від зловмисників зсередини, підприємствам слід реалізувати стратегію розподіленого внутрішнього брандмауера. Внутрішні брандмауери проактивно забезпечують видимість і захист від внутрішніх загроз, а також мінімізують збиток від кібератак, що виходять за межі традиційного периметра мережі [1].

VMware NSX Distributed IDS/IPS – це програма для управління трафіком, призначена для аналізу внутрішнього горизонтального трафіку та виявлення загроз бічного переміщення. Механізм працює в межах гіпервізора для оптимізації перевірки пакетів. VMware NSX Distributed IDS/IPS поєднує провідні в галузі набори сигнатур, декодери протоколів та механізми, що

базуються на виявленні аномалій, для пошуку відомих та невідомих атак у потоці трафіку [2]. Архітектура рішення показана на рисунку 1.

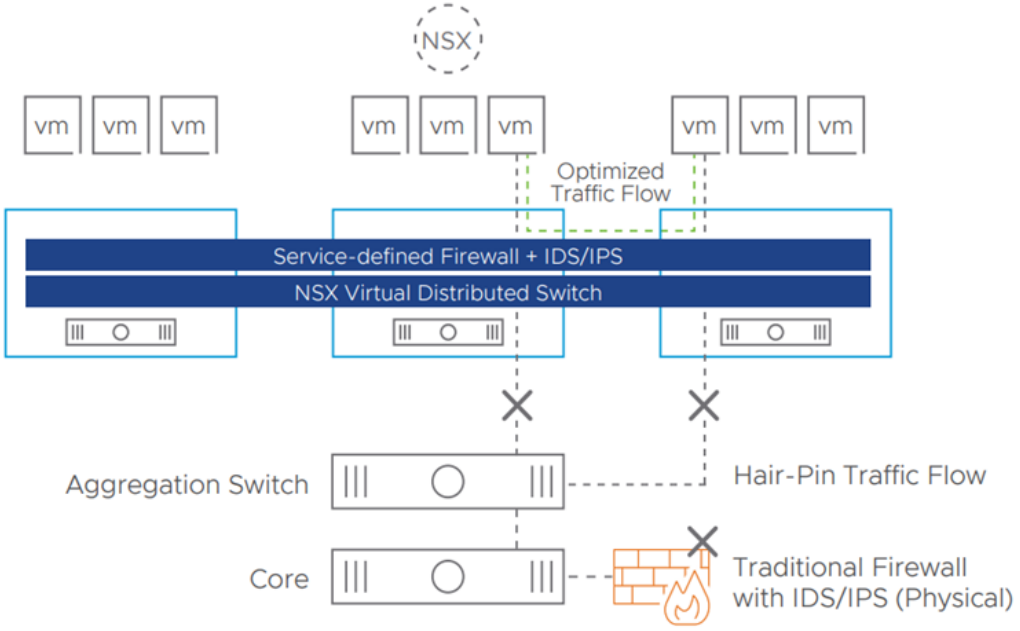


Рис. 1. Архітектура VMware NSX Distributed IDS/IPS [2]

Основними перевагами рішення VMware NSX є [2]:

гнучка пропускна здатність, яка полягає в усуненні вузьких місць в обладнанні за рахунок можливості перевірки, що автоматично масштабується з кожним робочим навантаженням;

спрощена мережева архітектура, яка сприяє уникненню необхідності направляти трафік на централізовані пристрої і зменшенню перевантаження мережі за допомогою повністю розподіленої архітектури;

зменшення кількості помилкових спрацьовувань – більше робочих навантажень з нульовим кількістю помилкових спрацьовувань з ретельно підібраними наборами правил і більш точною відповідністю сигнатур на основі точного контексту програми;

підвищення ефективності використання ємності, сутність якого полягає у повторному використанні існуючих невикористаних обчислювальних ресурсів, усуваючи необхідність в додатково виділених пристроях.

Роботу VMware NSX Distributed IDS/IPS забезпечують модулі регулярних виразів, що визначають схеми потоків трафіку. Ці модулі

запрограмовані на пошук відомих загроз на основі схем потоків трафіку за допомогою мови конфігурації. Оператори мережі і систем безпеки використовують схеми, виражені за допомогою мови конфігурації IDS/IPS. В даний час в більшості систем IDS/IPS крім виявлення загроз на основі сигнатур використовуються такі методи забезпечення безпеки, як перевірки відповідності протоколів і портів, а також виявлення аномального трафіку [2].

Як висновок, від правильного визначення умов функціонування інформаційної системи підприємства, вибору та обґрунтування складу методів та засобів виявлення та попередження вторгнень та ефективного їх застосування залежить ефективність забезпечення кібербезпеки інформаційних систем підприємства.

Література:

1. *Five Critical Requirements for Internal Firewalling in the Data Center. White Paper – March 2020. VMware [Електронний ресурс] – Режим доступу: https://www.vmware.com/content/dam/learn/en/amer/fy21/pdf/492966_Five_Critical_Requirements_for_Internal_Firewalling_in_the_Data_Center.pdf.*
2. *VMware NSX Distributed IDS/IPS. A new paradigm for east-west security. White Paper – December 2019 [Електронний ресурс] – Режим доступу: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmw-nsx-distributed-ids-ips-tech-white-paper-dec.pdf.*

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ДОСТУПУ ВІДДАЛЕНИХ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВА

Ткаченко О. В.
БСД-45
Державний університет телекомунікацій
м. Київ, Україна

Визначено мету і основні завдання щодо захисту доступу віддалених користувачів до інформаційних систем підприємства. Розглянуто методи та засоби захисту доступу віддалених користувачів до інформаційних систем підприємства. Розроблено рекомендації щодо застосування методів та засобів захисту доступу віддалених користувачів до інформаційних систем підприємства.

Організація правильної та безпечної віддаленої роботи користувачів інформаційних систем підприємства є необхідною умовою забезпечення

виживання бізнесу в умовах пандемії COVID-19 та постійних кібернетичних впливів. Від правильного визначення умов функціонування інформаційної системи підприємства, вибору та обґрунтування складу методів та засобів захисту доступу віддалених користувачів до інформаційних систем підприємства та ефективного їх застосування залежить ефективність забезпечення кібербезпеки інформаційних систем підприємства.

Сучасним підходом до забезпечення захисту віддаленої роботи користувачів інформаційних систем підприємства при широкому застосуванні хмарних сервісів є застосування технології SASE (Secure Access Service Edge), яка об'єднує функції мережевої безпеки, такі як Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS) і Zero Trust Network Access (ZTNA), з можливостями Software-defined Wide Area Network (SD-WAN) для забезпечення потреби підприємств в динамічному безпечному доступі до IT-ресурсів (рис.1).

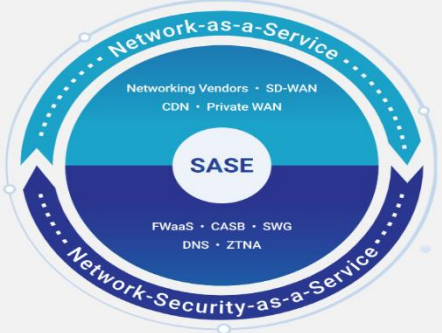


Рис. 1. Зміст технології SASE [1]

Ці можливості надаються в основному у вигляді відповідних засобів «як сервіс» і засновані на визначенні та керуванні обліковими записами, керуванні доступом до актуальних даних, визначенні та застосуванні політик безпеки, а також на дотриманні відповідності вимогам регуляторів.

Програмно визначена розподілена корпоративна мережа (SD-WAN) дозволяє підприємству сегментувати WAN-трафік на основі його походження або призначення. Як правило, усі корпоративні програми сегментовані у віртуальні приватні хмари (VPC) та трафік у віртуальні мережі (VNET) для досягнення необхідної ізоляції, яку вимагають бізнес-

підрозділи, що володіють програмами. SD-WAN дозволяє досягти всеохоплюючої сегментації на WAN, виділяючи трафік на конкретні сегменти WAN і відображаючи ці сегменти WAN на конкретні VPC та VNET. Політика додатків тепер може застосовуватися до кожного сегменту WAN, таким чином забезпечуючи безперебійне наскрізне безпечне хмарне підключення для всіх програм [2].

Технологія SASE поєднує можливості SD-WAN з функціоналом сервісів мережевої безпеки, які в повному обсязі доставляються і управляються з єдиної хмарної платформи та включає в себе такі базові компоненти забезпечення безпеки [2]:

шлюз веб-безпеки (SWG), який дозволяє запобігти кібератакам і витоку даних шляхом фільтрації небажаного контенту, що міститься в веб-трафіку, блокує дії неавторизованих користувачів і сприяє реалізації корпоративної політики безпеки. Шлюзи безпеки можуть бути впроваджені в будь-якому місці, що робить їх ідеальним варіантів для організації віддаленої роботи співробітників;

агент з управління безпечним доступом в хмару (CASB) виконує кілька функцій забезпечення безпеки для хмарних сервісів: виявляє тіньову активність (неавторизовані корпоративні IT-системи), захищає конфіденційні дані за допомогою систем DLP і систем контролю доступу, забезпечує відповідність вимогам регламентів щодо захисту даних тощо;

платформа контролю доступу до мережі з нульовою довірою (ZTNA) блокує внутрішні ресурси, захищаючи їх від можливості публічного доступу та допомагає убезпечити систему від потенційних витоків даних. Це досягається шляхом запиту автентифікації в режимі реального часу для дозволу доступу кожному окремо взятому користувачеві до будь-якого захищеного додатку;

рішення на базі мережевих екранів Firewall-as-a-Service (FWaaS) захищають хмарні платформи, інфраструктуру і додатки від кібератак. На відміну від традиційних мережевих екранів, FWaaS не є фізичним пристроєм,

а являє собою набір сервісів безпеки, в числі яких фільтрація URL-адрес, функція запобігання вторгнень і єдине управління політиками безпеки в рамках усього мережевого трафіку.

Найбільш повно даним вимогам відповідають рішення Fortinet, які реалізують технологію SASE. На рис. 2 наведено схема типової ідентифікації користувача Fortinet ZTA та управління доступом.

Рис. 2. Типова ідентифікація користувача Fortinet ZTA та управління доступом

Таким чином, при правильному впровадженні методів та засобів SASE дозволяє підприємствам використовувати безпечний доступ незалежно від того, де знаходяться користувачі, робочі навантаження, пристрої або програми. Це стає критично важливою перевагою, оскільки все більше користувачів переходять на віддалену роботу, SaaS-додатки швидко впроваджуються, а дані швидко переміщаються між центрами обробки даних, філіями і гібридними і багатохмарними середовищами.

Література:

1. *Что такое SASE? | Технология безопасного пограничного доступа [Електронний ресурс] – Режим доступу:* https://www.cloudflare.com/ru-ru/learning/access-management/what-is-sase/.
2. *IDC TECHNOLOGY SPOTLIGHT. SD-WAN: Security, Application Experience and Operational Simplicity Drive Market Growth. April 2019 [Електронний ресурс] – Режим доступу:* https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/intelligent-wan/idc-tangible-benefits.pdf.

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ МЕРЕЖІ SD-WAN ФІЛІЇ ПІДПРИЄМСТВА

Фічоряк В. Я.
БСД-45
Державний університет телекомунікацій,
м. Київ, Україна

Визначено мету і основні завдання щодо захисту мережі SD-WAN філії підприємства. Розглянуто методи та засоби захисту мережі SD-WAN філії підприємства. Розроблено рекомендації щодо застосування методів та засобів захисту мережі SD-WAN філії підприємства.

Сьогодні підприємства все частіше впроваджують хмарні сервіси з можливістю швидкого розгортання нових сервісів і впровадження новітніх функцій з мінімальними зусиллями щодо розгортання. Це зумовило впровадження програмно-визначених технологій, що забезпечують більш високу продуктивність і гнучкість при одночасному зниженні витрат.

В умовах стрімкого зростання кількості підключених пристроїв і майже щоденних звітів про експлойти інтеграція безпеки на межі мережі підприємства стає критично важливою. Рішення SD-WAN (Software-defined Wide Area Network) має об'єднувати безпеку і запобігати витоку даних, захищати підключені пристрої і забезпечувати конфіденційність інформації між сайтами і аж до хмари. Інструменти централізованого адміністрування безпеки мають забезпечувати однакове розгортання політик у всій корпоративній мережі, зменшуючи одну з найбільш поширених сьогодні вразливостей в організаціях – людську помилку.

Від правильного визначення умов функціонування інформаційної системи підприємства, вибору та обґрунтування складу методів та засобів захисту мережі SD-WAN філії підприємства та ефективного їх застосування залежить ефективність забезпечення кібербезпеки інформаційних систем підприємства.

SD-WAN – це технологія для налаштування і реалізації корпоративної глобальної мережі, заснованої на програмно-визначеній мережі (SDN), для

ефективної маршрутизації трафіку в віддалені точки, такі як філії. Технологія SD-WAN забезпечує значні переваги в гнучкості і маневреності за рахунок зняття тягаря управління трафіком з фізичних пристроїв і передачі його програмному забезпеченню, що є суттю SDN [1].

SD-WAN працює, відокремлюючи додатки від базових мережевих служб за допомогою віртуального накладення на основі політик. Це накладення відстежує наведені цифри щодо базових мереж в реальному часі і вибирає оптимальну мережу для кожної програми на основі політик конфігурації [1]. Там, де SDN розгорнута в мережі постачальника послуг, забезпечується гнучке розгортання і рішення на основі використання між сайтами з високою пропускною здатністю (наприклад, штаб-квартирою і центрами обробки даних), послуги SD-WAN допомагають оптимізувати потоки трафіку для підвищення продуктивності і запобігання витратам на сайтах філій.

Заміна традиційних маршрутизаторів філій на пристрої, які оцінюють і використовують різні транспортні технології в залежності від їх продуктивності, дозволяє підприємствам направляти великі частини свого трафіку через економні послуги, такі як широкосмуговий доступ. Основна мета технології SD-WAN – надати безпечне і просте WAN-з'єднання бізнес-класу з підтримкою хмарних обчислень з використанням якомога більшої кількості відкритих і програмних технологій [1].

В корпоративних системах розгортають різні типи архітектур SD-WAN (рис. 1) [1]:

локальна SD-WAN – розгорнута виключно локально, дешевше, ніж інші архітектури, оскільки вона може встановлювати з'єднання лише між віддаленими сайтами, а не хмарними службами. Приклад використання цієї архітектури SD-WAN – це компанії, які розміщують більшу частину своїх бізнес-додатків локально;

SD-WAN з підтримкою хмари – хмарне рішення SD-WAN може використовувати хмарні шлюзи для зв'язку з корпоративними хмарними

додатками. Це може бути що завгодно: від хмарного програмного забезпечення CRM до офісних додатків;

SD-WAN з підтримкою хмари і магістраль – рішення дозволяє використовувати найближчу точку присутності або POP постачальника послуг. Це може бути високошвидкісна волоконно-оптична лінія SD-WAN компанії, яка може значно підвищити продуктивність корпоративної мережі.

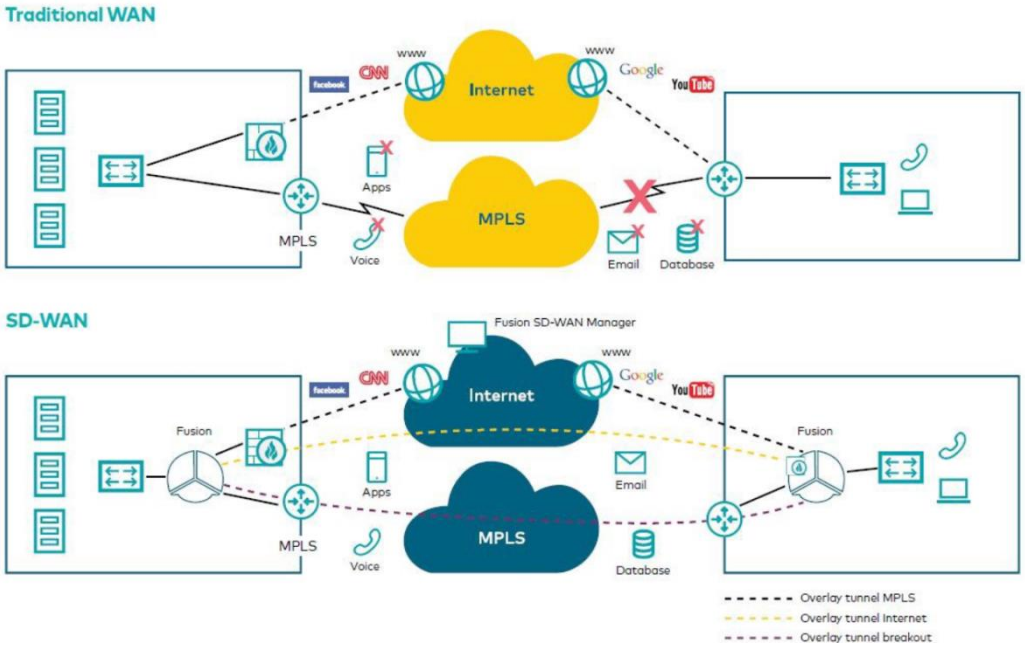


Рис. 1. Архітектури побудови корпоративних мереж [1]

Fortinet пропонує рішення SD-WAN з апаратно прискореною функціональністю SD-WAN та NGFW, інтегрованим як єдиний пристрій. Це дозволяє запропонувати перевірку безпеки рівнів 4-7, включаючи перевірку зашифрованого трафіку (SSL/TLS), з мінімальним впливом на продуктивність та пропускну здатність мережі. Без спеціального обладнання, такого як специфічна схема додатків SD-WAN (ASIC), перевірка трафіку SSL/TLS різко зменшує пропускну здатність мережі [2].

Рішення Fortinet Secure SD-WAN може ідентифікувати понад 5000 унікальних програм на основі класифікації перших пакетів. Це дозволяє Secure SD-WAN застосовувати пріоритет для конкретних додатків та направляти його на оптимальний вибір транспортного носія, щоб максимізувати продуктивність програми та надійність [2].

Рис. 2. Компоненти архітектури Secure SD-WAN [3]

Рішення Fortinet Secure SD-WAN складається з декількох компонентів (рис. 2). Компоненти, які складають рішення Fortinet Secure SD-WAN, включають: FortiGate, FortiManager, FortiAnalyzer та FortiDeploy [3].

FortiGate працює під управлінням FortiOS – ядра рішення Secure SD-WAN. FortiManager забезпечує оркестровку і управління. FortiAnalyzer і FortiDeploy допомагають об'єднати всі рішення, надаючи рішення, яке не має аналогів у інших постачальників [3].

В основі побудови Fortinet Secure SD-WAN застосовується міжмережевий екран наступного покоління (NGFW). Варіант розгортання пристрою FortiGate 80F в філії підприємства показано на рис. 3.

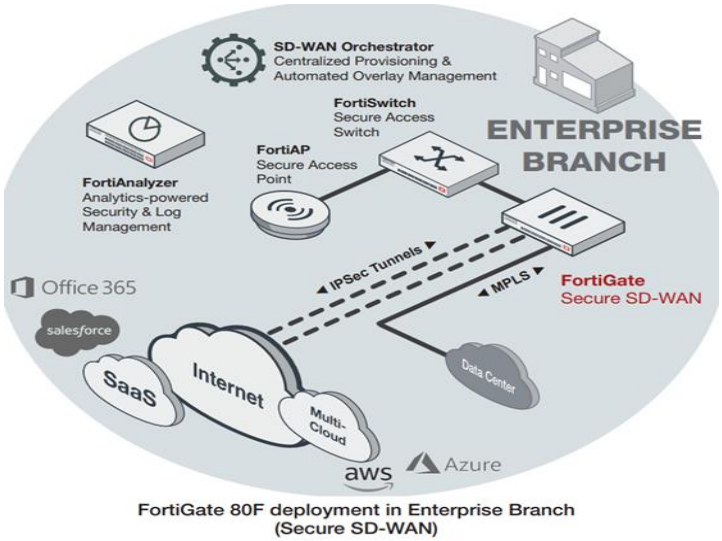


Рис. 3. Варіант розгортання пристрою FortiGate 80F в філії підприємства [4]

Як висновок, впровадження у мережі філії підприємства прямого доступу в Інтернет також забезпечує «пряме підключення» до мінливого ландшафту загроз. Філії з SD-WAN тепер вимагають розширених можливостей безпеки на межі мережі. Недостатньо просто надати прямий доступ в Інтернет за допомогою SD-WAN – організаціям потрібна безпечна SD-WAN з вбудованим захистом від загроз. Fortinet Secure SD-WAN надає стек безпеки на межі філії, де він буде надавати прямі послуги, не перетинаючи корпоративну WAN.

Література:

1. *Top Business Benefits of SD-WAN. Posted on November 8, 2019, by Vedran Bozicevic [Електронний ресурс] – Режим доступу: https://www.globaldots.com/blog/top-business-benefits-of-sd-wan.*
2. *SD-WAN Vendors List: Comparison of Top Providers [Електронний ресурс] – Режим доступу: https://www.fortinet.com/ru/products/sd-wan-providers.*
3. *Fortinet Secure SD-WAN Reference Architecture. White Paper [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/document-library/ra-sd-wan-reference-architecture.pdf.*
4. *FortiGate 80F Series. FortiGate 80F, 80F-Bypass, and 81F [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf.*

МІНІМІЗАЦІЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Матвієнко В.В
студент БСЗМ-61
Державний університет телекомунікацій,
м.Київ, Україна

Мінімізація ризиків інформаційної безпеки підприємства є нагальною потребою будь-якої сучасної організації. Актуальність теми обумовлена тим, що протягом останніх років інформація стала відігравати важливу роль в усіх сферах людського життя, що пов’язано з поступовим становленням інформаційного суспільства. Зі збільшенням складності і надійності методів захисту інформації, удосконалюються також методи несанкціонованого доступу до конфіденційної інформації. У результаті наноситься певний

економічний збиток підприємству, який у ряді випадків може призвести до нездоланних наслідків.

Покращення обізнаності персоналу. Як правило, кіберзлочинці намагаються отримати доступ до корпоративних даних через “найслабше місце” компанії - недосвідчений персонал. Спочатку зловмисники надсилають фішингове повідомлення, яке майже ідентичне з реальним, і співробітник відкриває його. Після цього, сценарії бувають різними - на пристрій завантажується програма-вимагач, троян, шпигунська програма або інше шкідливе ПЗ. Тому першим кроком у справі посилення інформаційної безпеки компанії має бути інформування співробітників щодо актуальних загроз та способів захисту від них. Кожен співробітник повинен усвідомити необхідність захисту даних компанії та клієнтів. Тому керівництво має проводити навчання усіх відділів, які працюють з даними, щодо принципів інформаційної безпеки та захисту даних, можливих способів атак зловмисників, а також методів їх уникнення.

Захист фізичних носіїв даних та робочих пристроїв. Незахищені дані роблять підприємства вразливими до кібератак та інфікування шкідливим ПЗ. Оскільки у разі втрати чи викрадення USB-накопичувачів, ноутбуків чи смартфонів компанії співробітник ставить під загрозу всі корпоративні дані. У гіршому випадку потрапляння пристрою в чужі руки може призвести до шантажу. Щоб уникнути подібних ситуацій рекомендується:

- завжди виходити з систем та ресурсів, які містять конфіденційні дані;
- шифрувати всі корпоративні дані за допомогою спеціалізованих рішень, які надають можливість керувати ключами шифрування віддалено, а також дозволяють встановлювати політики щодо файлів, жорстких дисків, портативних дисків, карт пам’яті та електронних листів. Таким чином у разі втрати робочого пристрою зловмисники не зможуть прочитати корпоративні дані;

- здійснювати регулярне резервне копіювання файлів. Таким чином можна відновити дані у будь-який час.

Сегментування мережі та контроль користувачів, які намагаються увійти. У цілях інформаційної безпеки конфіденційні дані потрібно розміщувати на окремих серверах, забезпечуючи при цьому додатковий захист за допомогою брандмауерів або інших служб безпеки. Таким чином встановлюється безліч бар'єрів, які знижують ризик викрадення даних. Крім цього, необхідно здійснювати моніторинг користувачів, які отримують або намагаються отримати доступ до мережі. Це дозволить адміністраторам оперативно виявляти та зреагувати на будь-яку підозрілу поведінку.

Співпраця з перевіреними постачальниками послуг. Будь-який договір про обслуговування, постачання чи інший вид співпраці повинен включати детальні вимоги щодо безпеки. Багато постачальників хмарних послуг регулярно проходять тестування на проникнення різних загроз, щоб відповідати стандартам інформаційної безпеки в певній галузі діяльності.

Найважливіше те, що постачальник послуг повинен мати рівень безпеки, який відповідає вашому. У разі відсутності відповідного захисту корпоративних систем та партнерських сервісів ви можете висунути необхідні вимоги.

Захист віддаленого доступу до мережі підприємства. Будь-який пристрій співробітника чи клієнта для віддаленого доступу до робочої мережі повинен відповідати нормам інформаційної безпеки, які вимагають наступного:

- підключення через віртуальну приватну мережу (VPN);
- використання двохфакторної автентифікації під час входу в систему або підключення до VPN;
- отримання доступу за допомогою віртуальної машини як опції підключення за замовчуванням, якщо це можливо.

• використання комплексного рішення з безпеки для захисту від проникнення програм-вимагачів, шпигунських програм та інших видів загроз, а також запобігання фішинг-атакам.

Наведені рекомендації щодо мінімізації ризиків разом дозволяють вивести інформаційну безпеку підприємств на абсолютно новий рівень. Будь-яка компанія, яка зберігає та опрацьовує особисті дані користувачів, може стати жертвою хакерської атаки. Однак у випадку дотримання усіх правил інформаційної безпеки, компанії буде завдано набагато менших збитків та мінімальних збоїв бізнес-процесів.

Література:

1. *Нові виклики для інформаційної безпеки підприємства: як мінімізувати потенційні ризики - URL: https://eset.ua/ua/blog/view/67/novyye-vyzovy-dlya-informatsionnoy-bezopasnosti-predpriyatiya-kak-minimizirovat-potentsialnyye-riski;*
2. *Пригодюк О. М. Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства. URL: http://vtn.chdtu.edu.ua/article/view/153279/152656;*
3. *Южаков М. А. Ідентифікація збитків підприємства від втрати інформації. URL: https://ela.kpi.ua/bitstream/123456789/18428/1/69Ivanytska.pdf.*

БАНКІВСЬКІ ТРОЯНИ

Порохницький О.А.
студент УБД-31
Державний університет телекомунікацій
м. Київ, Україна

Перші повноцінні банківські трояни почали з’являтися на мобільні платформи ще в 2011 році. Вони мали певний функціонал такий як копіювання SMS-повідомлень та mTAN- кодів, але до повноцінних троянів не дотягували.

На сьогодні більшість троянських програм на Android маскуються під універсальні програми такі як відеокодеки в тому числі маскуються в каталозі Google play. Були випадки коли трояни вбудовувалися в справжні банківські програми і їх розповсюджували с підробленого сайту банку.

Ще до одного з векторів можна додати фішингові SMS- повідомлення. Користувачу приходить лист в якому є якась певна пропозиція та звертаються до нього за ім’ям яке завчасно роспарсили за допомогою бази даних зловмисники. При переході потенційну жертву відправляють на проміжний сайт на якому підтверджується інформація що користувач зайшов з мобільного пристрою.

Також як окремий вид Банківських троянів можна зазначити Банкботи, ці трояни на відміну від звичайних можуть отримувати команди і виконувати їх на зараженому пристрої.

Як же ш ці банківські трояни поширюються ? Через велике розповсюдження Андроїд пристроїв створення троянів стало цілою індрустрією тож в даркнеті з’явилися оголошення про надання в оренду троянів пізніше були надані білди за допомогою яких кожен міг зібрати під свої потреби.

Тож як захиститися? Не бути уважним при встановленні програм з сторонніх джерел, перевіряти що які права запитує програма, а також по можливості користуватися антивірусами для Android.

Література:

1. *URL: https://spy-soft.net/banking-trojans/*

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Яценко І.Л.
БСЗМ -61
Державний університет телекомунікацій
м. Київ, Україна

Інформація є одним із головних ділових ресурсів, який забезпечує організації додану вартість, і внаслідок цього потребує захисту, а слабкі місця в захисті інформації можуть призвести до фінансових втрат, і нанести збиток комерційним операціям. Тому в наш час питання розробки системи

управління інформаційною безпекою та її впровадження в організації є концептуальними. Захист бізнесу та знань компанії від знищення або витоку є найбільш значущою метою більшості систем інформаційної безпеки. У той же час заходи з інформаційної безпеки не повинні обмежувати або ускладнювати процеси обміну інформацією в компанії, оскільки це може поставити під загрозу розвиток організації.

Побудова системи управління інформаційною безпекою дозволяє чітко визначити, як взаємопов'язані процеси та підсистеми інформаційної безпеки, хто за них відповідає, які фінансові та трудові ресурси необхідні для їх ефективного функціонування.

Одним з ключових чинників успішності системи управління інформаційною безпекою підприємства – це побудова її на базі міжнародних стандартів ISO/IEC 27001. Міжнародний стандарт ISO 27001 надає інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої системи управління інформаційною безпекою в контексті розгляду бізнес ризиків.

Система управління інформаційною безпекою на основі стандарту ISO 27001 дозволяє:

- зробити більшість інформаційних активів найбільш зрозумілими для менеджменту компанії;
- виявляти основні загрози безпеки для існуючих бізнес-процесів;
- розраховувати ризики і приймати рішення на основі бізнес цілей компанії;
- забезпечити ефективне управління системою в критичних ситуаціях;
- проводити процес виконання політики безпеки (знаходити і виправляти слабкі місця в системі інформаційної безпеки);
- чітко визначити особисту відповідальність;
- досягти зниження і оптимізації вартості підтримки системи безпеки;
- полегшити інтеграцію підсистеми безпеки в бізнес-процеси;

- продемонструвати клієнтам, партнерам, власникам бізнесу свою прихильність до інформаційної безпеки;

- отримати міжнародне визнання і підвищення авторитету компанії, як на внутрішньому ринку, так і на зовнішніх ринках;

- підкреслити прозорість і чистоту бізнесу перед законом завдяки відповідності стандарту.

При цьому для ефективного впровадження системи управління інформаційної безпеки на підприємстві, необхідно не тільки виконати всі розробки і впровадження (інвентаризація активів; оцінка захищеності інформаційної системи; оцінка інформаційних ризиків; обробка інформаційних ризиків; впровадження вибраних заходів обробки ризиків; контроль виконання та ефективність вибраних заходів; роль керівництва компанії в системі управління інформаційною безпекою), а також провести навчання співробітників.

Навчання співробітників можна виконувати у формі очних та заочних курсів з подальшим тестуванням. Доцільно організувати навчанням співробітників за допомогою системи дистанційного навчання, в рамках якого можуть бути представлені різні курси та ігрові методики навчання.

Крім того, для досягнення заданих цілей необхідне визначення відповідальних за інформаційну безпеку, розробка політик і правил доступу до інформаційних ресурсів, методів контролю інформаційної безпеки на підприємстві.

Система управління інформаційною безпекою забезпечує вибір адекватних і пропорційних методів і засобів контролю та захисту інформації та дає компанії такі переваги, як управління інформаційною безпекою компанії в рамках єдиної корпоративної політики, управління ризиками та їх своєчасне виявлення, зниження ризиків від зовнішніх і внутрішніх загроз, систематизація процесів забезпечення інформаційної безпеки. У свою чергу це забезпечує компанії конкурентну перевагу, демонструючи здатність

керувати інформаційними ризиками, і, тим самим, забезпечує довіру зацікавлених сторін, при цьому також збільшується капіталізація компанії.

Література:

1. *Система управління інформаційною безпекою. URL: https://core.ac.uk/download/pdf/48401951.pdf*
2. *Система управління інформаційною безпекою, як ключовий чинник успішності організації. URL: https://ua.ikmj.com/isms/*