Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: *"Дослідження механізмів захисту від соціально-інженерних атак та розробка методів їх виявлення "*

Виконав: студент

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Загорняк В.Ю..
підпис (прізвище та ініціали)

Керівник *Стадник М. А.*
підпис (прізвище та ініціали)

Нормоконтроль
підпис (прізвище та ініціали)

Завідувач кафедри *Загородна Н.В.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2023

АНОТАЦІЯ

Дослідження механізмів захисту від соціально-інженерних атак та розробка методів їх виявлення // Кваліфікаційна робота ОР «Бакалавр» // Загорняк Вадим Юрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-41 // Тернопіль, 2023 // С. – 68, рис. – 24 , табл. – 0, кресл. – 0, додат. – 0.

Ключові слова: СОЦІАЛЬНА ІНЖЕНЕРІЯ, СОЦІАЛЬНО-ІНЖЕНЕРНІ АТАКИ, ФІШІНГ, ВІШІНГ, ЗЛОВМИСНИК, ЗАПОБІГАННЯ, МЕТОДИ ВИЯВЛЕННЯ.

В кваліфікаційній роботі досліджується проблема соціальної інженерії, соціально-інженерних атак, методів їх виявлення та способами боротьби з ними. Метою кваліфікаційної роботи є аналіз існуючих методів захисту від соціальної інженерії а також розробка комплексного методу захисту від соціально-інженерних атак в Х-компанії, і її тестування.

В першому розділі було досліджено типи соціально інженерних атак, та проведено їх історичний огляд. В другому розділі було досліджено методи та засоби виявлення атак. В третьому розділі розроблено комплексну систему захисту від соціально-інженерних атак

ANNOTATION

Study of mechanisms of protection against social engineering attacks and development of methods for their detection // Qualification work of OR "Bachelor" // Zahornyak Vadim Yuriyovych // Ternopil National Technical University named after Ivan Pulyu, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, SBs-41 group // Ternopil, 2023 // P. – 68, fig. – 24, tab. - 0, chair. – 0, add. - 0.

Keywords: SOCIAL ENGINEERING, SOCIAL-ENGINEERING ATTACKS, PHISHING, VISHING, ATTACKER, PREVENTION, DETECTION METHODS.

The Bachelor' work examines the problem of social engineering, social-engineering attacks, methods of their detection and methods of combating them. The purpose of the qualification work was the analysis of insinuating methods of protection against social engineering, as well as the development of a comprehensive method of protection against social engineering attacks in X-company, and its testing.

In the first chapter, the types of socially engineered attacks were investigated, and their historical overview was conducted.

In the second chapter, methods and means of detecting attacks were investigated. In the third section, a complex system of protection against social engineering attacks is developed

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DNC	Democratic National Committee
OAuth	Open Authorization
IVR	Interactive Voice Response
IDS	Intrusion Detection Systems
MFA	Multi-factor authentication
2FA	Двофакторна аутентифікація
SMS	Short Message Service
HTTPS	HyperText Transfer Protocol over Secure
VPN	virtual private network
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
BLADE	Block All Drive-By Exploits
BYOD	Bring Your Own Device
ОС	Операційна Система
ПК	Персональний Комп’ютер

ВСТУП

Сьогодні однією з найбільших загроз кібербезпеці як великих компаній, так і звичайних користувачів, є соціально-інженерні атаки, або ж просто методи соціальної інженерії, що часто застосовують для обходу, або зламу існуючих засобів захисту. Причиною цього є те, що застосування методів соціальної інженерії є доволі дешевим та не потребує глибоко професійних знань інформаційних технологій.

Крістофер Хаднагі привів таку аналогію: що соціальна інженерія це інструменти, наприклад молоток, лопата, ніж або навіть пістолет. Кожен може використовувати ці інструменти для будівництва, приготування їжі, або самозахисту. Проте кожен з цих інструментів можна використати щоб калічити, вбивати та руйнувати. Для того щоб захиститись від соціально-інженерних атак, спочатку необхідно зануритись в темну сторону соціальної інженерії, щоб отримати чітке уявлення про те як все це відбувається.

Питання соціальної інженерії є доволі широким, тому що, перебуваючи за комп'ютером чи іншим пристроєм, який має доступ до Інтернету, люди доволі часто нехтують безпекою в інформаційному просторі.

Вже давно відомо, що людям притаманні різні поведінкові схильності, які зловмисники часто використовують для маніпулювання. Статистика показує, що більшість зламів відбуваються саме через використання соціальної інженерії, а не електронного зламу.

1 СОЦІАЛЬНО ІНЖЕНЕРНІ АТАКИ

1.1 Аналіз історичних даних щодо поширеності соціально інженерних атак

Несанкціонований доступ до інформації або систем зберігання інформації без використання технологічних засобів є соціальною інженерією[1].

Атаки соціальної інженерії – це тип атак на кібербезпеку, які ґрунтуються на маніпулюванні поведінкою людей з метою отримання несанкціонованого доступу до інформації чи систем. Ці атаки використовують різноманітні методи для використання людських слабкостей, таких як довіра, страх і цікавість, щоб оманою змусити людей розкрити конфіденційну інформацію, виконати певну дію або надати доступ до захищених систем [1].

Останніми роками атаки соціальної інженерії стають все більш поширеними, а зловмисники використовують все складніші методи соціально-інженерних атак для заподіяння шкоди проти окремих осіб і організацій. Основні області застосування соціального інжинірингу показано на рис. 1.1.

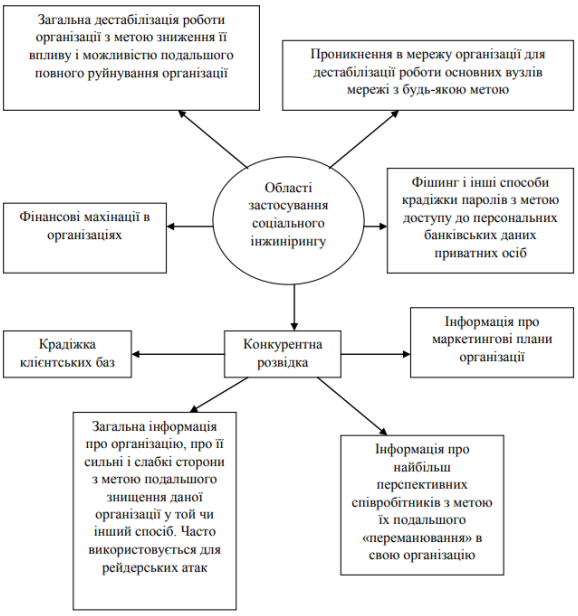


Рисунок 1.1 – Області застосування соціальної інженерії

Згідно зі звітом Verizon [2], атаки соціальної інженерії були найпопулярнішою тактикою, яка використовувалася для витоку даних у 2020 році (рис. 1.2). У звіті також виявлено, що фішинг був найпоширенішою формою атаки соціальної інженерії, на яку припадає 25% усіх зломів. Крім того, опитування Proofpoint показало, що 88% організацій у всьому світі зазнали принаймні одну атаку соціальної інженерії у 2019 році, а 33% зазнали шість або більше атак. Те ж опитування показало, що фішингові атаки були найпоширенішим типом атак соціальної інженерії: 83% респондентів повідомили, що зазнавали фішингових атак протягом останнього року.

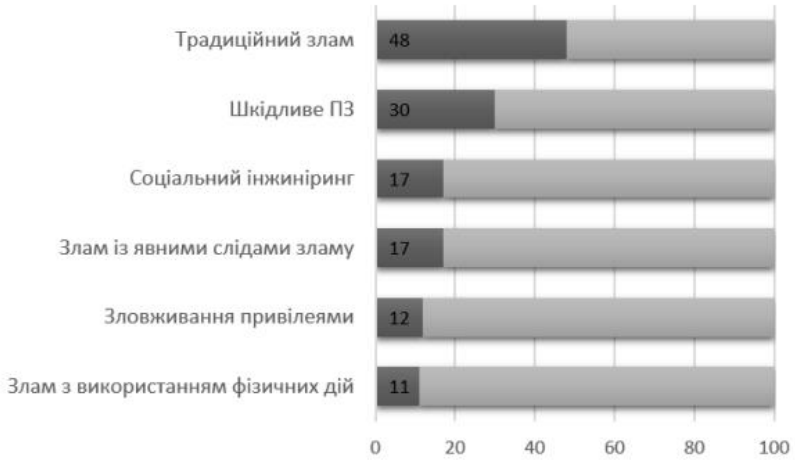


Рисунок 1.2 – Статистика тактик зламу за 2020 рік [2]

Також звіт Verizon про розслідування витоків даних за 2021 рік (Verizon's 2021 Data Breach Investigation Report) [3], соціальна інженерія продовжує набувати тенденції до зростання, яка пов'язана з тим, що, по-перше, все більше кіберзлочинців усвідомлюють ефективність такого виду атак, а по-друге, протягом пандемії з'являється все більше різновидів шахрайства на тему COVID-19: від фішингових листів, в яких зловмисники намагались обманути жертву, видаючи себе за Всесвітню організацію охорони здоров'я, до різних видів шахрайства з вакцинами. Тож вже протягом двох років фішинг – залишається одним із найпоширеніших варіантів злому та став причиною 36% витоку даних у 2020 р. (рис. 1.3), що на 11% більше ніж у 2019 р.

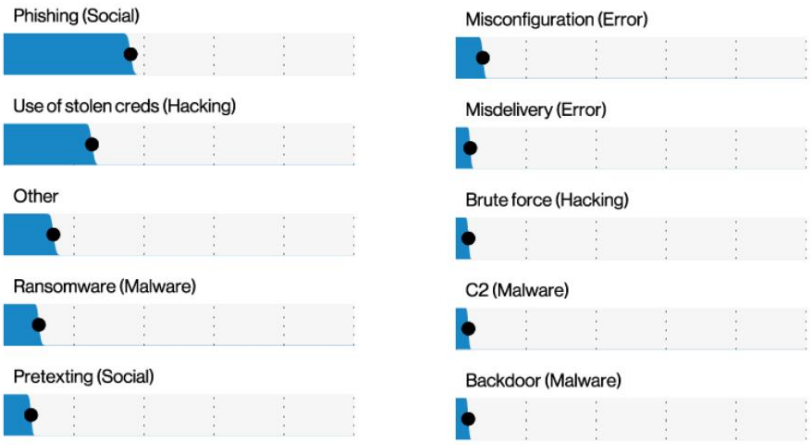


Рисунок 1.3 – Рейтинг атак порушення даних за 2020 рік [3]

Атаки соціальної інженерії не обмежуються великими організаціями. У групі ризику також малі підприємства та окремі особи. Згідно зі звітом Small Business Trends, 43% кібератак спрямовані на малий бізнес, а атаки соціальної інженерії є поширеною тактикою, яка використовується для націлювання на ці організації. Подібним чином люди ризикують стати жертвами атак соціальної інженерії через фішингові електронні листи, шахрайські телефонні дзвінки та інші способи, що використовують зловмисники.

Дані щодо основних трендів кібератак, які були представлені у звіті Check Point Cyber Attack Trends: 2020 Mid-Year Report [4], показують, що більшу частину вкладень, що прикріплюються до фішингових листів, складають файли формату .exe (26%) та .doc (24%) (рис. 1.4).

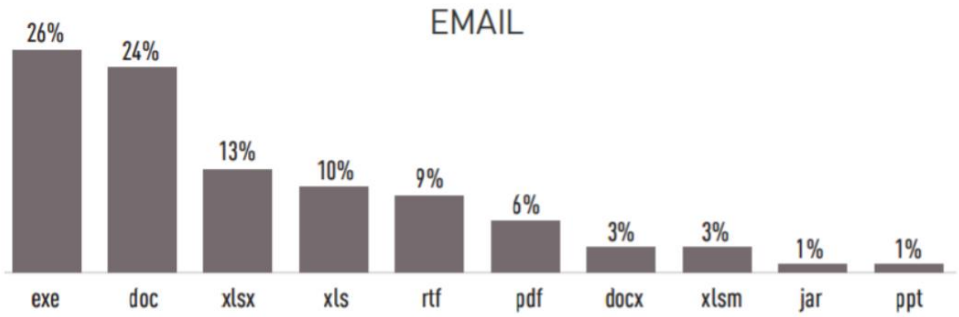


Рис. 1.4 – Розподіл типів шкідливих даних, що передаються електроною поштою [4]

Проаналізувавши тенденції останніх років робимо висновок, що такі атаки будуть здійснюватися дедалі частіше, а разом з тим зловмисники будуть ставати все більш досвідченими, а використання соціальних мереж та інших джерел особистої інформації продовжує зростати, атаки соціальної інженерії, ймовірно, стане ще важче виявити та запобігти.

Розглянемо основну причину популярності таких атак. Основна причина є надзвичайно простою – такі атаки є відносно недорогими (або безкоштовними) та вимагають невеликих технічних знань, що робить їх привабливим варіантом для кіберзлочинців.

Одним із факторів, що спонукають до поширення атак соціальної інженерії, є все більше використання соціальних мереж. Платформи соціальних медіа надають зловмисникам велику кількість інформації про окремих осіб та організації, яку вони можуть використовувати для створення переконливіших фішингових повідомлень або фішингових атак. Наприклад, зловмисник може використати інформацію, зібрану з профілю особи в соціальних мережах, щоб створити фішингове повідомлення, яке нібито надійшло від друга чи колеги.

Іншим фактором, що сприяє поширенню атак соціальної інженерії, є все більше використання мобільних пристроїв. Зараз багато атак соціальної інженерії націлені на мобільні пристрої, використовуючи такі методи, як смішинг і вішинг, щоб обманом змусити людей розкрити конфіденційну інформацію або завантажити зловмисне програмне забезпечення. Мобільні пристрої особливо вразливі до атак соціальної інженерії, оскільки вони часто використовуються для конфіденційних транзакцій і можуть не мати такого рівня безпеки, як настільні комп’ютери.

Атаки соціальної інженерії існують стільки часу, скільки хакери намагаються обійти заходи безпеки. Одним із найперших прикладів соціальної інженерії був телефонний фрікінг, техніка, яка передбачала маніпулювання загальнодоступною телефонною мережею для здійснення безкоштовних міжміських дзвінків. Телефонні фрики використовували свої знання про телефонну систему, щоб переконати операторів надати доступ до обмежених телефонних ліній, обійти системи виставлення рахунків і здійснювати безкоштовні дзвінки.

У 1980-х і 1990-х роках атаки соціальної інженерії стали більш витонченими, оскільки хакери почали використовувати такі методи, як претекстинг, цькування та фішинг, щоб обманом змусити людей розкрити конфіденційну інформацію. У цей час атаки соціальної інженерії часто використовувалися в поєднанні з технічними атаками, такими як шкідливі програми або атаки на відмову в обслуговуванні, щоб отримати доступ до систем

На початку 2000-х років атаки соціальної інженерії продовжували розвиватися, коли зловмисники використовували більш цілеспрямовані методи, такі як фішинг і вішинг, щоб націлитися на конкретних осіб або організації. Ці атаки стали більш витонченими, з використанням особистої інформації, зібраної з соціальних мереж та інших джерел, для створення переконливих повідомлень і отримання доступу до конфіденційної інформації.

Одним із найвідоміших прикладів атаки соціальної інженерії є злам облікового запису електронної пошти Yahoo Сари Пейлін у 2008 році. В атаці був задіяний хакер, який використовував інформацію, зібрану з акаунтів Пейлін у соціальних мережах, щоб скинути її пароль Yahoo та отримати доступ до її електронної пошти. Потім хакер опублікував скріншоти електронних листів в Інтернеті, що викликало великий скандал під час президентської кампанії в США 2008 року.

В останні роки атаки соціальної інженерії стали ще більш поширеними, коли зловмисники використовують все більш витончені методи, щоб обдурити окремих осіб і організації. Яскравим прикладом є злом системи електронної пошти DNC у 2016 році, здійснений російськими хакерами. Атака включала фішингові електронні листи, надіслані співробітникам DNC, що призвело до крадіжки та розголошення конфіденційних електронних листів під час президентської кампанії в Америці 2016 року [5].

Зовсім недавно атаки соціальної інженерії використовувалися в поєднанні з атаками програм-вимагачів, під час яких зловмисники шифрують дані організації та вимагають оплату в обмін на ключ дешифрування. У багатьох випадках атакам програм-вимагачів передують соціально-інженерні атаки, наприклад – фішингові

електронні листи, які обманом змушують людей завантажити зловмисне програмне забезпечення або надати доступ до конфіденційних систем.

Часто шкода від таких атак може бути без перебільшень катастрофічною, для деяких людей чи компаній, тому не лише корпораціям а також звичайним окремим особам варто забезпечити себе від них. Запобігання атакам соціальної інженерії вимагає поєднання технічних і нетехнічних заходів.

До технічних заходів входять такі протоколи автентифікації, як двофакторна автентифікація, і використання програмного забезпечення для захисту від шкідливих програм для виявлення та запобігання фішинговим електронним листам та іншим атакам соціальної інженерії.

Нетехнічні заходи включають навчання співробітників ризикам атак соціальної інженерії та проведення регулярних тренінгів щодо того, як ідентифікувати підозрілі електронні листи, повідомлення, телефонні дзвінки та як відповідати на них. Також важливо встановити чітку політику та процедури обробки конфіденційної інформації та реагування на інциденти безпеки.

Атаки соціальної інженерії стали значною загрозою для організацій будь-якого розміру, і їхня еволюція з часом зробила їх ще небезпечнішими. Ці атаки ґрунтуються на використанні поведінки людей для обходу технічних заходів безпеки, і вони стають дедалі складнішими та їх важко виявити.

Запобігання атакам соціальної інженерії вимагає багатостороннього підходу, який включає технічні та нетехнічні заходи. Запроваджуючи надійні протоколи автентифікації, навчаючи співробітників ризикам атак соціальної інженерії та встановлюючи чіткі політики та процедури обробки конфіденційної інформації, організації можуть зменшити ризик стати жертвою таких типів атак.

Оскільки атаки соціальної інженерії продовжують розвиватися, окремим особам і організаціям важливо залишатися пильними та бути в курсі останніх загроз і тенденцій у кібербезпеці. За допомогою правильних інструментів і стратегій можна захиститися від атак соціальної інженерії та зберегти конфіденційну інформацію в безпеці.

Окрім технічних і нетехнічних заходів, існують також певні «червоні прапорці», на які варто звернути увагу, щоб не стати жертвами атак соціальної інженерії. До них належать:

– Запити конфіденційної інформації – необхідно бути обережним з електронними листами, повідомленнями або телефонними дзвінками, які вимагають конфіденційну інформацію, як-от паролі, або кредитні дані. Законні організації рідко запитуватимуть таку інформацію електронною поштою чи телефоном.

– Термінові або погрозливі повідомлення – необхідно остерігатись електронних листів, повідомлень або телефонних дзвінків, які створюють відчуття терміновості або загрожують негативними наслідками, якщо людина не відповість. Цю тактику часто використовують для тиску на людей, щоб вони надали конфіденційну інформацію або вжили заходів, не обдумуючи це.

– Підозрілі посилання або вкладення – будьте обережні з посиланнями або вкладеннями в електронних листах або повідомленнях, особливо якщо вони надійшли від невідомих відправників або здаються поза контекстом. Вони можуть містити зловмисне програмне забезпечення або вести до фішингових веб-сайтів, призначених для викрадення облікових даних для входу.

– Несподівані повідомлення – будьте обережні з повідомленнями, які здаються неочікуваними або нехарактерними для відправника, особливо якщо вони містять запити грошей або конфіденційну інформацію.

– Пропозиції надто гарні, щоб бути правдою – будьте обережні з пропозиціями, які здаються занадто гарними, щоб бути правдою, наприклад пропозиціями безкоштовних продуктів чи послуг або обіцянками великих сум грошей. Вони часто використовуються, щоб спонукати людей надати конфіденційну інформацію або завантажити зловмисне програмне забезпечення.

Соціальна інженерія, є набагато складнішою ніж може здатись спочатку, хоч ми вже маємо визначення для неї, проте її продовжують вивчати, адже соціально-інженерні атаки розвиваються на сам перед за допомогою людей які мають навички

заставити іншу людину зробити щось, що їй потрібно, вчинити дії які не відповідають вашим інтересам, та навіть відчувати коли жертва попала в пастку.

Атаки соціальної інженерії були значною загрозою для організацій та окремих осіб протягом десятиліть, і вони продовжують розвиватися та ставати все більш витонченими з часом. Ці атаки ґрунтуються на використанні людської поведінки та обході технічних заходів безпеки, що ускладнює їх виявлення та запобігання.

Однак, запровадивши багатосторонній підхід, який включає технічні та нетехнічні заходи, окремі особи та організації можуть зменшити ризик стати жертвами атак соціальної інженерії. Крім того, уважність до несподіваних або підозрілих повідомлень може допомогти людям не стати жертвами таких атак.

Оскільки кібербезпека продовжує розвиватися, людям і організаціям важливо залишатися пильними та бути в курсі останніх загроз і тенденцій у кібербезпеці. Вживаючи профілактичних заходів для запобігання атакам соціальної інженерії та залишаючись в курсі нових загроз, ми можемо допомогти захиститися від значних ризиків, які створюють такі типи атак.

1.2 Типи соціально інженерних атак

Як ми вже зрозуміли атаки соціальної інженерії передбачають маніпуляцію та обман людей з використанням їх довіри, з метою отримання несанкціонованого доступу до важливої інформації. Ці атаки зазвичай використовують вразливі місця людини, а не якісь технічні недоліки, Для того що б запобігти соціально-інженерним аткам, необхідно спершу дізнатись які бувають типи цих атак розглянемо деякі з них: phishing (фішінг), pretechting (претекстинг), baiting (цькування), Quid Pro Quo (щось на щось), tailgating (теілгатінг), vishing (вішинг) та інші: [1] див. (рис. 1.5).

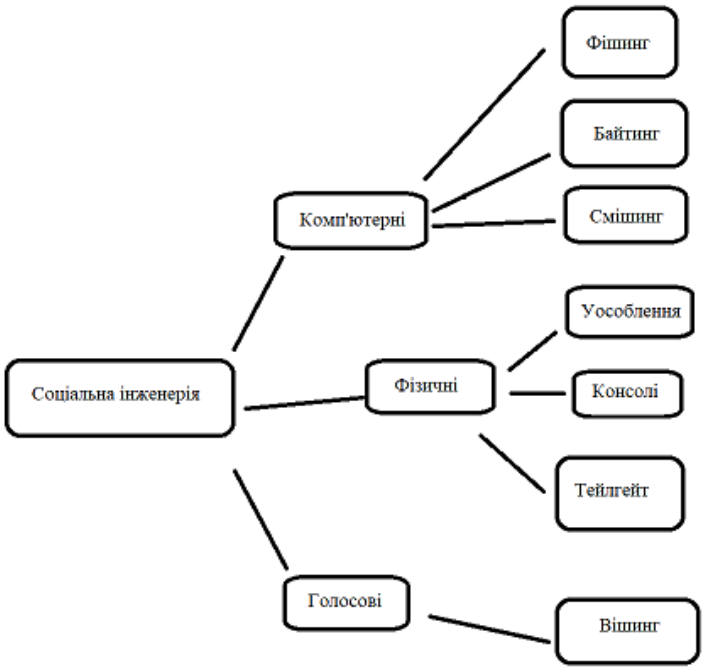


Рисунок 1.5 – Види атак соціальної інженерії [1]

– Фішинг: Мабуть іноді ви отримували електронні повідомлення наприклад з банку чи іншого онлайн-сервісу, які вимагали “підтвердити” дані вашого облікового запису, номер кредитки або ж іншу конфіденційну інформацію [6]. Якщо це так, то скоріш за все ви вже знаєте як виглядає фішинг-атака. Мета фішингу – здобуття цінних даних, які наприклад можуть бути продані, або використані для зловмисних цілей, наприклад вимагання, викрадення грошей або особистих даних. Взагалі вперше концепція фішингу була описана ще в 1987 році в документах з конференції «Безпека системи: перспективи хакера». В тому документі описувалася техніка зловмисників, яка полягає в імітації авторитетних організацій або сервісів. А назву таку дали через те що техніка використовує логіку “вилову” як рибалка.

Раніше для виманювання користувацьких даних кіберзлочинці часто використовували оманливі доменні імена. Проте сьогодні зловмисники роблять більш складні методи, тому фальшиві сторінки вкрай схожі на свої легітимні аналоги. Кіберзлочинці, які використовують цей метод, зазвичай ретельно досліджують свою жертву, що в свою чергу значно ускладнює ідентифікацію

вмісту як шкідливого. Фішинг спрямований на такі галузі як виробництво, інформаційний сектор, рітейл, охорона здоров'я, житловий сектор, держсектор, фінанси, освіта та інші, див. (рис. 1.6) [7].

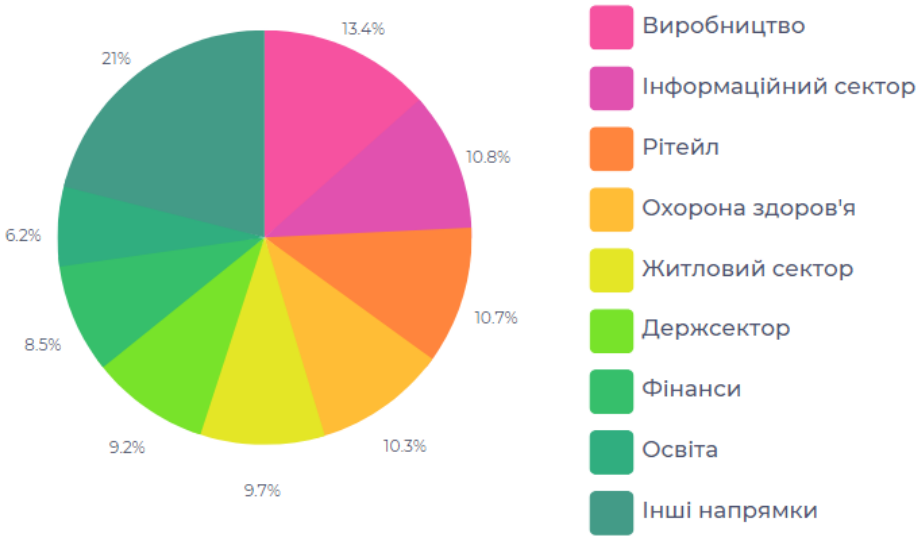


Рисунок 1.6 – На які напрямки спрямований фішинг [7]

У 2001 році було скоєно одну з перших велих спроб, хоча й не вдало. Кіберзлочинці скористалися хаосом терористичних атак 11 вересня 2001 року, надсилаючи електронного листа жертвам із заявою про підтвердження їх особи. Згодом отримані дані були використані для викрадення банківських даних.

У 2005 році кіберзлочинці за допомогою фішингу викрали понад 900 мільйонів доларів у користувачів у Сполучених Штатах [1].

У минулому зловмисники використовували функції Microsoft OAuth API для здійснення фішингових атак. Протокол OAuth дозволяє програмам сторонніх розробників видавати маркери доступу, не знаючи облікових даних. Суть атаки полягає в наступному. Фішингові електронні листи містять посилання на файли, які нібито знаходяться в OneDrive або SharePoint. Однак після натискання посилання та введення облікових даних користувачам відкривається форма із запитом на доступ до їхнього облікового запису Office 365. Якщо жертва необережна, вона може надати потрібні дозволи одним клацанням миші. У

результаті зловмисники отримали список контактів, файлів та особистих повідомлень див. (рис. 1.7).

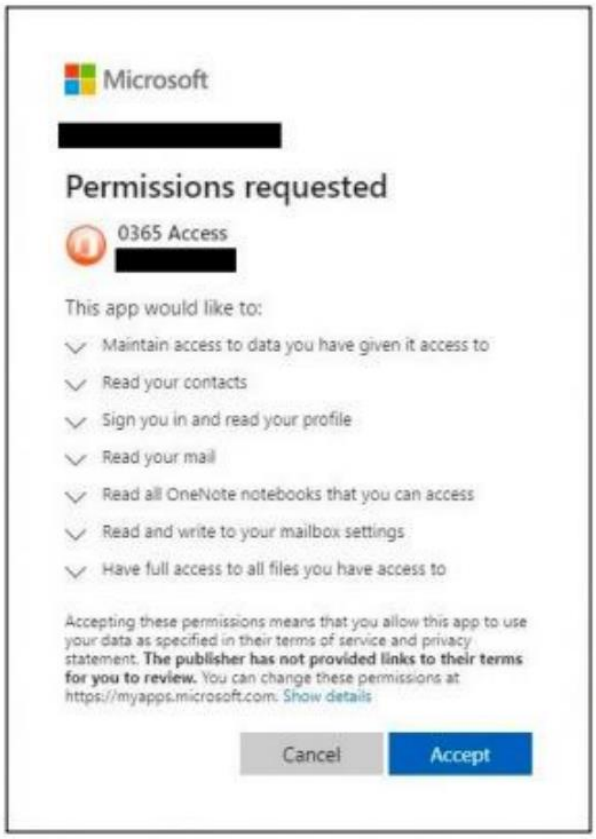


Рисунок 1.7 – Запит від фішингового додатку O365 Access [1]

– Pretexting: це ще одна форма соціальної інженерії, яка передбачає створення вигаданого сценарію або приводу, щоб обманом змусити людей розкрити конфіденційну інформацію [8]. Зловмисники можуть видаватися за довірених осіб, як-от персоналу технічної підтримки або представників банку, щоб маніпулювати жертвами, щоб вони надали конфіденційні дані. Ця атака не обмежується взаємодією між зловмисником та жертвою в онлайн форматі – вона може відбуватися через інші форми спілкування, зокрема особисто. Складні атаки можуть намагатися змусити жертву виконати дію, яка використовує фізичні та, або цифрові недоліки організації. Наприклад, суб’єкт загрози може видати себе за зовнішнього аудитора IT-послуг і використовувати цей псевдонім, щоб переконати групу фізичної безпеки організації дозволити суб’єкту загрози увійти в будівлю. Багато суб’єктів загрози, які використовують цей тип атаки, маскуються

під співробітників або відділу кадрів у фінансовому відділі. Такі маніпуляції дозволяють їм націлюватися на керівників високого рівня, або інших співробітників із великими привілеями, які є більш цінними для зловмисників. У той час як фішингові атаки, як правило, використовують терміновість і страх, щоб використовувати жертви, атаки з використанням претекстів створюють помилкове відчуття довіри у цільової жертви. Це вимагає від суб'єктів загрози створити достовірну історію, яка не викликає у жертв підозри щодо нечесної гри. Pretexting використовує такі методи: Phishing, vishing/smishing, baiting, piggybacking, scareware та tailgating. Ось деякі поширені види шахрайства з його використанням: шахрайство з криптовалютою – це шахрайство часто можна побачити на професійних мережевих платформах. Зловмисник може надіслати жертві повідомлення під виглядом досвідченого інвестора з можливістю «швидко збагатитися». Зловмисник може навіть створити веб-сайт, який виглядає легітимним і може містити підроблені відгуки, щоб завоювати довіру жертви. Якщо жертва надсилає гроші, а потім намагається їх зняти, зловмисник скаже, що це не можливо зробити через податки, додаткові комісії або мінімальний баланс рахунку, якого не було досягнуто, шахрайство з видаванням себе за іншу особу – щоб завоювати довіру жертви, зловмисник може спробувати видати себе за когось, кого жертва знає. Це може бути хтось із тієї ж організації або друг у соціальних мережах. Приклад повідомлення, яке може отримати жертва: «Привіт, це служба технічної підтримки вашої організації, нам потрібно підтвердити інформацію вашого облікового запису». Жертва більш довірлива, особливо якщо зловмисник представляється легітимною особою в організації, наприклад, генеральним директором із «терміновим запитом», романтичні шахрайства – подібно до шахрайства з криптовалютою, романтичні шахраї намагатимуться переконати жертву інвестувати у щось за допомогою криптовалюти. Замість приводу залучення досвідченого інвестора, шахрай завоює довіру жертви, вдаючи, що виявляє романтичний інтерес до жертви. Тоді зловмисник може згадати про можливість інвестування та

спонукати жертву надсилати великі суми, але, звичайно, вони ніколи не отримають прибутку.

– Quid Pro Quo: атака quid pro quo характеризується обміном «віддай бери». Це буквально означає, обмін тобто щось за щось [9]. Це поняття обміну є вирішальним, оскільки як люди ми підкоряємося закону психологіної взаємності. Це означає, що кожного разу, коли хтось дає нам щось або робить нам послугу, ми відчуваємо обов'язок повернути цю послугу.

У випадку quid pro quo обіцяна вигода в обмін на інформацію зазвичай набуває форми послуги.

Припустімо, до вас звернувся IT-працівник і запропонував провести аудит вашого комп'ютера, щоб видалити потенційні віруси, які можуть знизити продуктивність комп'ютера. Але для цього йому потрібен ваш логін і пароль. Ви надаєте йому цю інформацію без будь яких обговорень, адже ви місяцями скаржились на уповільнення роботи комп'ютера. За винятком того, що цей обмін доброї волі може бути невдалим, і що ви, можливо, щойно потрапили в пастку атаки quid pro quo.

Атаки Quid pro quo базуються на маніпуляції та зловживанню довірою. Як і baiting, атаки quid pro quo є методами соціальної інженерії. Таким чином, обидві ці кіберзагрози покладаються на психологічні маніпуляіції та зміцнення довіри, щоб отримати конфіденційні дані від надто довірливої жертви. Однак під час атак quid pro quo хакер пропонує жертві послугу в обмін на конфіденційну інформацію.

Крім того, атаки quid pro quo часто простіші, ніж атаки з цькуванням. І вони не вимагають ні великої підготовки, ні складних інструментів.

Один із найпоширеніших сценаріїв атак quid pro quo включає самозванів, які видають себе за IT працівника. Хакер зв'язується з якомога більшою кількістю співробітників компанії на їхній прямій лінії, щоб запропонувати ймовірну IT-підтримку.

Хакер обіцяє швидко вирішити проблему в обмін на відключення антивірусної програми. Після вимкнення фальшивий технік може встановлювати

зловмисне програмне забезпечення на комп'ютери жертв, видаючи себе за оновлення програмного забезпечення.

В іншому поширеному сценарії хакер прагне викрасти облікові дані співробітника. І тут шахрай зв'яжеться зі співробітником, представившись технічним фахівцем з ІТ-компанії, що спеціалізується на усуненні помилок і проблем із програмним забезпеченням. Задавши потерпілому кілька запитань, щоб визначити, які у нього проблеми з ПК, він запропонує поглянути на нього:

"Не біда, я негайно вирішу ваші проблеми! Все, що мені потрібно, це ваш логін і пароль!" Це червоний прапорець, про який слід знати!

– Baiting: Вітаємо, ви виграли приз! Якщо ви коли небудь бачили таке повідомлення, то мабуть можна дати 110% що це обіцянка, одна з форм соціальної інженерії [10]. Воно схоже на «троянського коня » в реальному світі, оскільки покладається на цікавість або жадібність жертви. Це відрізняється від, скажімо, нападу quid pro quo, де жертва може відчувати себе зобов'язаною «повернути послугу». Це багато в чому схоже на фішінгові атаки. Однак те, що відрізняє їх від інших типів соціальної інженерії - це обіцянка предмета або товару, який хакери використовують, щоб заманити жертв. Наприклад, зловмисник може пропонувати користувачам безкоштовне завантаження музики чи фільмів, якщо вони нададуть свої облікові дані для входу на певний сайт. Приманка може приймати різні форми: Онлайн-завантаження – посилання на шкідливі файли, які можна надсилати електронною поштою, соціальними мережами чи програмами обміну миттєвими повідомленнями. Програми обміну миттєвими повідомленнями, такі як Facebook та месенджери Instagrame, надсилатимуть посилання підписникам, які натискатимуть ці типи посилань. Пристрої, заражені шкідливим програмним забезпеченням – зловмисник може заразити комп'ютер шкідливим програмним забезпеченням і продати його в темній мережі. Потенційні покупці можуть протестувати пристрій, підключивши його до своєї мережі та подивившись, чи не заразяться вони. Спокусливі пропозиції – ці електронні листи запрошують людей купити щось за зниженою ціною, або навіть безкоштовно. Посилання веде до зловмисного програмного забезпечення замість товару.

Візьмемо приклад з кінцевою метою проникнути в мережу компанії. Соціальні інженери хочуть запровадити зловмисне програмне забезпечення на підключені до мережі комп’ютери та поширити шкідливий код. Один із способів зробити це — пообіцяти винагороду («приманку»). Наприклад, співробітники можуть отримати заражені флешки як винагороду за участь в опитуванні. Або зловмисники можуть залишити заражені USB-накопичувачі в кошику з подарунками, розміщеному у фойє компанії, щоб працівники просто забрали їх, повертаючись на роботу див. (рис. 1.8).

Рисунок 1.8 – Логер замаскований під накопичувач [10]

Іншою можливістю є стратегічне розміщення зіпсованих пристроїв для цільових співробітників. Якщо пристрої позначені інтригуючими ярликами, як-от «Конфіденційно» або «Інформація про зарплату», пристрої можуть бути надто спокусливими для деяких працівників. Ці співробітники можуть просто схопити наживку та вставити заражений пристрій у комп’ютери своєї компанії і таким чином потрапити у пастку.

Специфіка цькування полягає в тому, щоб спокусити жертву взяти наживку, звідки і назва. Спокусливим змістом може бути обіцянка подарунка або можливість отримати винагороду. Тому завдання хакера – створити пастку для своєї жертви.

– tailgating: це фізична атака соціальної інженерії, коли особа намагається потрапити в зону обмеженого доступу, де їй заборонено перебувати. По суті, визначення tailgating – це коли хтось пробирається в заборонену зону за допомогою когось іншого [11]. Це може бути, якщо слідкувати за кимось дуже близьким, хто несе щось, і просити його: «Притримайте двері, будь ласка!». Або зловмисник може ввести людей в оману, видаючи себе за когось іншого. Проте кінець атаки відрізняється від інших атак соціальної інженерії. Тому що, це фізичне вторгнення з метою отримання доступу до конфіденційних даних, грошей. Ось кілька прикладів таких атак: Людина видає себе за водія доставки та чекає біля будівлі. Коли працівник отримує дозвіл служби безпеки та відкриває двері, зловмисник просить працівника «притримати двері». Таким чином отримує доступ до компанії через уповноважену особу.

Самозванці можуть грати багато ролей, наприклад, праівники з ремонту, особи, які вдають, що тримають важкі коробки. Будь-хто, кому ви не подумаєте, “він виглядає підозріло”, щоб притримати двері. Опинившись усередині, вони можуть використовувати інші атаки соціальної інженерії, щоб викрасти інформацію від нічого не підозрюючих співробітників.

Однак tailgating не працює в усіх корпоративних установах. Наприклад, у великих компаніях кожен, хто заходить у будівлю, повинен провести картку. Однак на підприємствах середнього розміру зловмисники можуть зав’язати розмову з працівниками та використовувати цю демонстрацію фамільярності, щоб пройти.

Основною метою зловмисника в цьому типі соціальної інженерії є отримання фізичного доступу до сайту. Вхід до зони обмеженого доступу, електронний контроль доступу, наприклад, за допомогою картки RFID, просто заходить позаду людини, яка має законний доступ. Дотримуючись загальної ввічливості – законна особа зазвичай притримує двері для нападника.

Найвідомішим прикладом такої атаки є, ймовірно, добре відома історія Френка Абаньєйле, історію якого ви, ймовірно, дізналися у фільмі «Спіймай мене, якщо зможеш». Абаньяле обманював багатьох людей і входив у багато заборонених зон, куди його не пускали. Упевненість змусила його відвідати багато місць і обдурити багатьох людей.

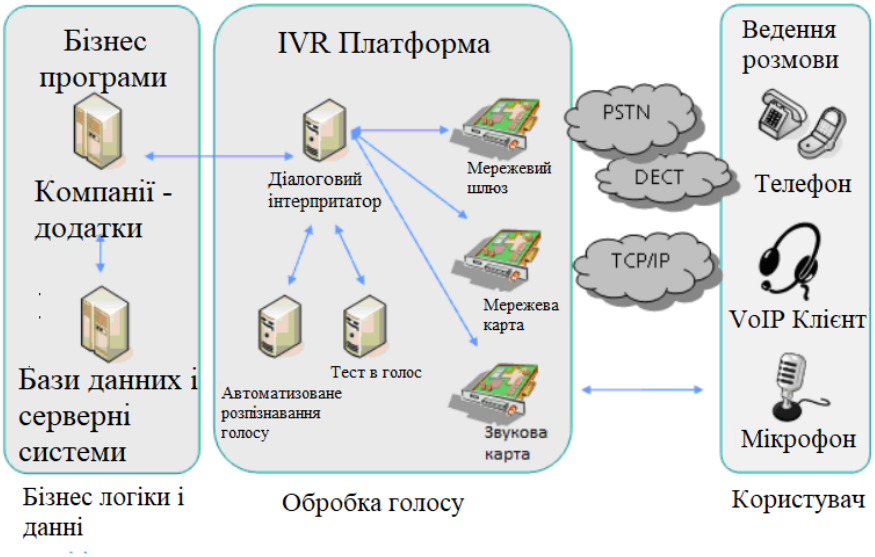
– Vishing: Ця технологія базується на використанні попередньо записаних систем обміну голосовими повідомленнями з метою відтворення «офіційних дзвінків» від банків та інших систем IVR [12]. Як правило, жертви отримують запит (часто через фішинговий електронний лист) зв'язатися зі своїм банком, щоб підтвердити або оновити будь-яку інформацію. Система вимагає аутентифікації користувача шляхом введення PIN-коду або пароля. Головна відмінність вішингу полягає в тому, що в будь-якому випадку задіяний телефон. Принцип роботи системи IVR показано на рисунку 1.9.

Голосові фішингові атаки можуть бути одноразовими атаками з метою отримання доступу до облікових записів, даних кредитної картки чи особистої інформації, або вони можуть використовуватися як частина багатоетапної атаки, отримання інформації та встановлення стосунків із жертвами для використання на наступних етапах.

Щомісяця Європейці отримують 2,4 мільярда робо-дзвінків. Статистика, пов'язана з нападами на організації, є малодоступною, оскільки багато компаній не бажають ділитися випадками недоліків у своїх внутрішніх системах, якщо вони не призводять до порушення, про яке слід повідомити. Однак, враховуючи його успіх у споживачів і зростаючу обізнаність про вішинг та інші форми соціальної інженерії, ми спостерігаємо все більше повідомлень про напади. Вішинг працює, видаючи себе за законну особу по телефону, а потім використовуючи психологічні тактики, щоб переконати жертву надати інформацію або отримати доступ до зловмисника. Атака спрацьовує, тому що жертви часто не знають цінності інформації, яку вони надають, і вважають, що вони допомагають.

Голосовий фішинг – це швидка взаємодія в режимі реального часу, яка дозволяє зловмиснику здійснити цілеспрямовану та персоналізовану атаку, яка

може адаптуватися та змінюватися у відповідь на реакцію жертви. Досвідчений зловмисник може думати на ходу і адаптувати свій підхід до того, що найбільше підходить для жертви.



Риунок. 1.9 – Принцип дії IVR систем [13]

Відомо, що деякі зловмисники використовують програмне забезпечення для зміни голосу, щоб створити більш правдоподібну атаку. Цей тип атаки соціальної інженерії ідеально підходить для використання принципу терміновості, щоб залякати та змусити швидко вжити заходів, не даючи жертві часу на роздуми чи підтвердження дійсності запиту. Зловмисник наголошує на важливості виконання дій зараз, коли зловмисник перебуває в Інтернеті, таким чином вони можуть обговорювати весь процес і переконатися, що він виконаний правильно [13].

1.3 Загальні статистичні дані

За даними Verizon Communications Inc. Нижче наведено статистику злому глобальних інформаційних систем станом на 2021 рік.

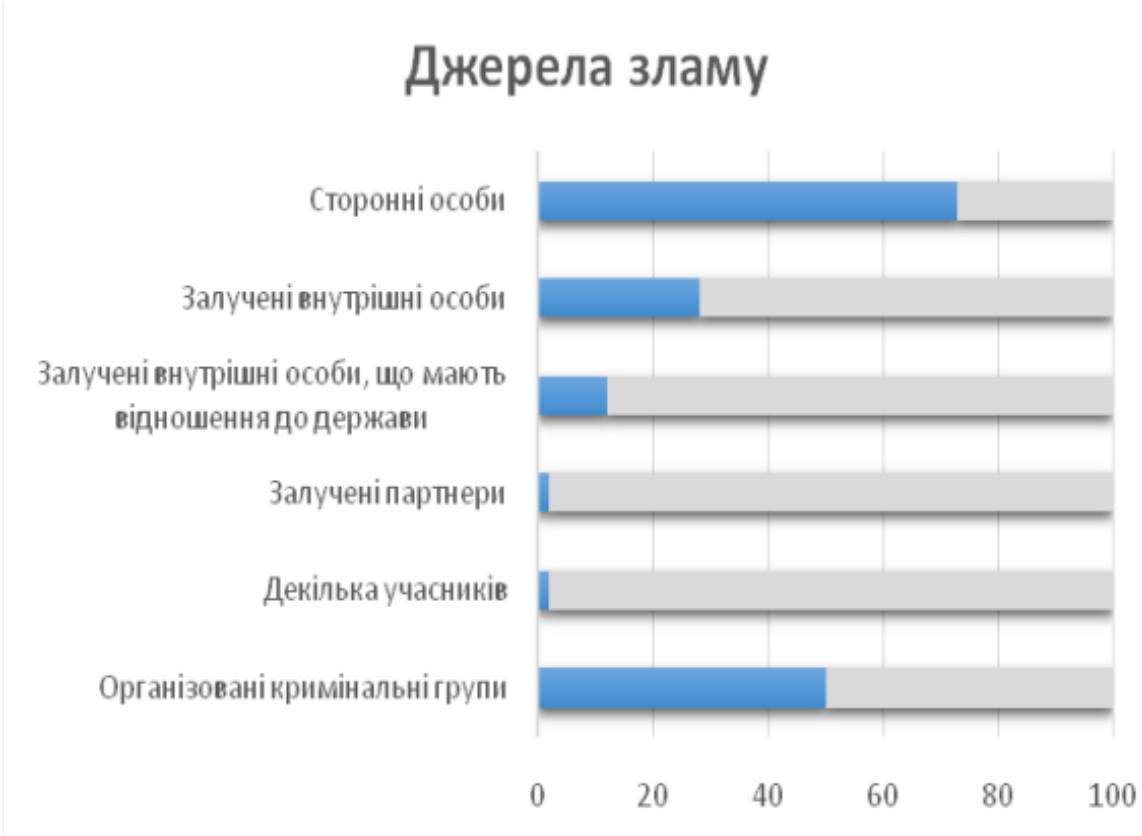


Рисунок 1.10 – Різновиди джерел зламу [13]

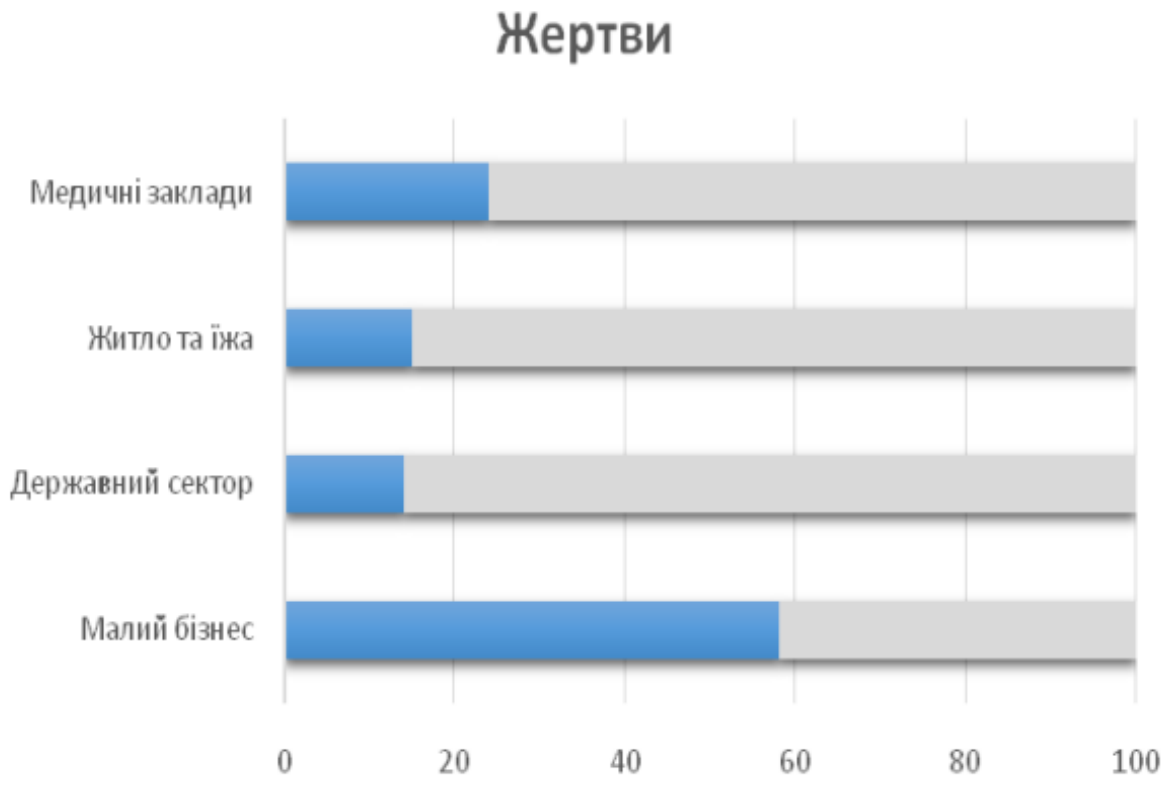


Рисунок 1.11 – Основні цілі зламу [13]

Рисунок 1.12 – Основні застосовані техніки зламу [13]

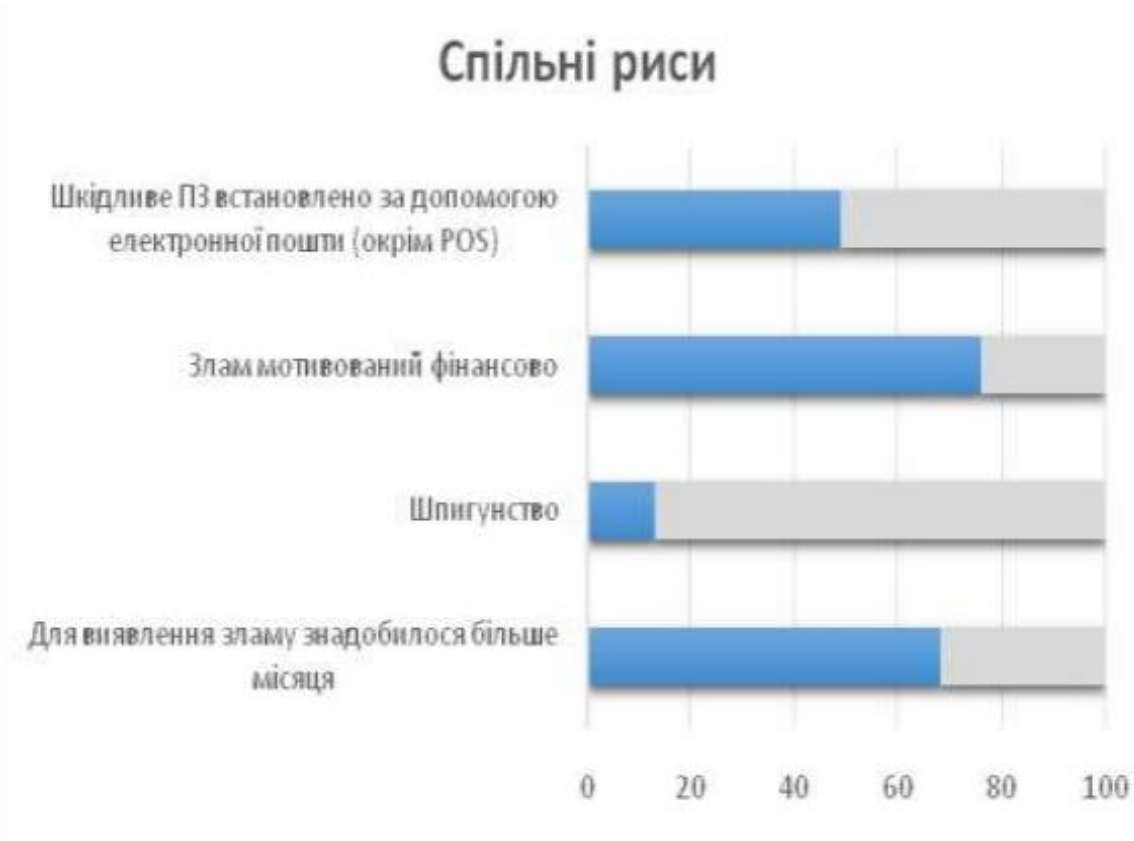


Рисунок 1.13 – Загальні риси зламу [13]

Соціальні інженерні атаки є серйозною загрозою для індивідів, підприємств та організацій. Вони використовують вразливості людей замість технічних слабкостей для отримання неправомірного доступу до систем, збору конфіденційної інформації або маніпулювання ними. Знання різних типів соціальних інженерних атак дозволяє розуміти методи та тактики, якими користуються зловмисники, та забезпечувати ефективні заходи захисту.

У першому розділі були розглянуті такі типи соціальних інженерних атак, як фішинг, претекстування, приманювання, послуга "чому не сказати", підман, спірфішинг та вішинг. Кожен з цих типів атак має свої особливості і мету, проти яких необхідно застосовувати відповідні контрзаходи.

Розуміння типів соціальних інженерних атак є ключовим для розроблення ефективних заходів захисту та проведення навчання співробітників щодо тактик, які використовують зловмисники. Важливо підтримувати пильність, надавати пріоритет особистій безпеці та впроваджувати кращі практики кібербезпеки.

2 МЕТОДИ ВИЯВЛЕННЯ АТАК

2.1 Існуючі методи виявлення кібератак

Як уже відомо зростаюча залежність від технологій та інтернету робить наш світ більш вразливим перед кібератаками. Кіберзлочинці стають все більш винахідливими і використовують різноманітні методи для здійснення своїх нападів. Щоб захистити комп'ютерні системи та мережі від таких загроз, необхідно виявляти кібератаки якомога раніше за допомогою таких систем як системи виявлення вторгнень (Intrusion Detection Systems, IDS) див. (рис. 2.1), системи виявлення вторгнень на основі аналізу поведінки (Behavior-based Intrusion Detection Systems), системи виявлення вторгнень на основі машинного навчання (Machine Learning-based Intrusion Detection Systems) та системи виявлення інтелектуальних загроз (Advanced Threat Detection Systems).

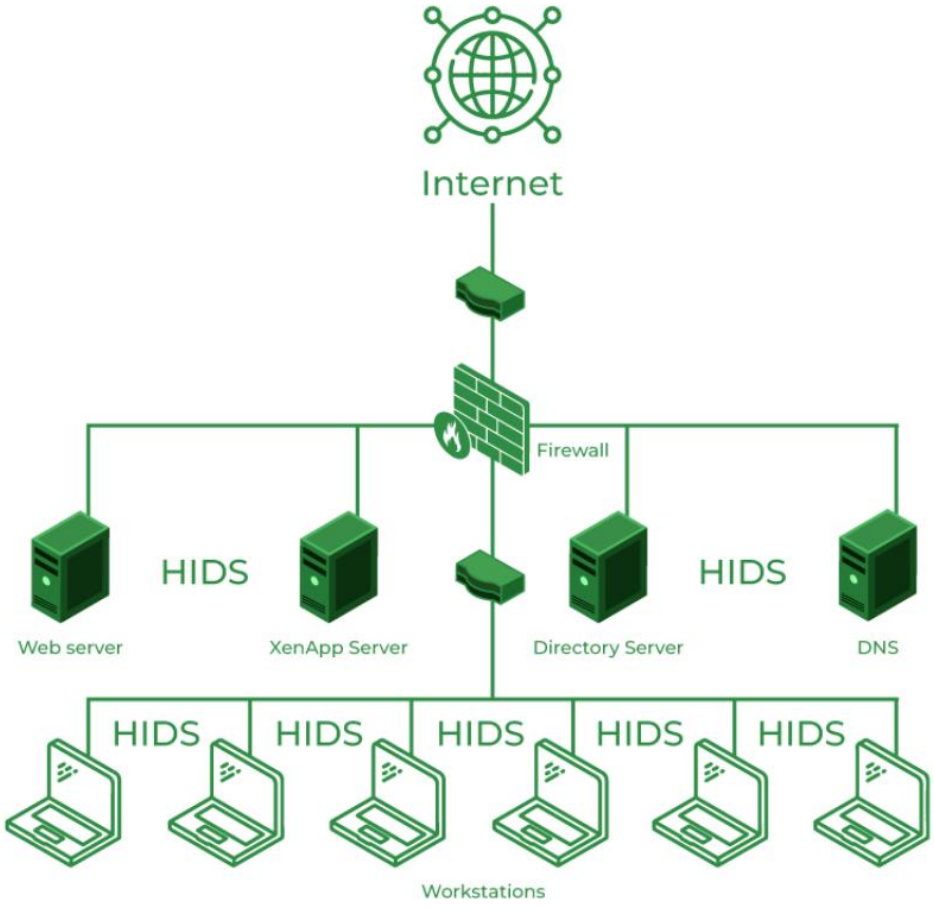


Рисунок 2.1 – Intrusion Detection Systems [33]

Системи виявлення вторгнень (Intrusion Detection Systems, IDS) – є одним з найпоширеніших методів виявлення кібератак. Вони моніторять мережевий трафік та аналізують його на предмет підозрілих активностей. IDS можуть бути розташовані на різних рівнях мережі, включаючи хост-рівень, сегмент мережі та периметр мережі. Вони можуть виявляти широкий спектр атак, таких як вторгнення на основі підписів, аномальна поведінка, атаки на вразливості та багато інших. Системи виявлення вторгнень є програмними або апаратними рішеннями, призначеними для моніторингу та аналізу мережевого трафіку з метою виявлення незвичайної або підозрілої активності. Основний принцип роботи IDS полягає у порівнянні активності мережі з певними зразками відомих атак або аномалій. Існує декілька видів систем виявлення вторгнень, кожен з яких має свої особливості та переваги. Найбільш поширеними є:

системи виявлення вторгнень на основі підписів (Signature-based IDS) - ці системи використовують базу даних з відомими підписами відомих атак. Вони аналізують мережевий трафік та порівнюють його з цими підписами. Якщо виявляється збіг, система сповіщає про можливу кібератаку [14];

– системи виявлення вторгнень на основі аналізу поведінки (Behavior-based IDS) – вивчають нормальну поведінку системи та користувачів. Вони будують профіль звичайної активності і виявляють будь-які зміни або незвичайну поведінку, яка може вказувати на кібератаку [15];

– системи виявлення вторгнень на основі аналізу аномалій (Anomaly-based IDS) – аналізують мережевий трафік та порівнюють його зі зразком нормальної активності. Якщо виявляються аномалії або незвичайні зміни, система сповіщає про можливу кібератаку [16].

Системи виявлення вторгнень виконують кілька важливих функцій для запобіганю несанкіцонованому доступу , наприклад:

– виявлення кібератак – IDS виявляють незвичайну або підозрілу активність, що може свідчити про кібератаку;

– сигналізація та сповіщення – IDS сповіщають про виявлення підозрілої активності, надсилаючи алерти адміністратору системи або безпековій команді;

– запобігання атакам – IDS можуть приймати заходи для заборони або обмеження доступу до системи або мережі, щоб запобігти атакам;

– аналіз інцидентів – IDS збирають дані про виявлені інциденти та забезпечують можливість аналізувати їх з метою вдосконалення системи безпеки.

Незважаючи на ефективність IDS, вони також стикаються з деякими викликами. Деякі атаки можуть бути важко виявити, особливо нові або непідписані атаки.

Одним з майбутніх напрямків розвитку IDS є поєднання їх з іншими методами виявлення, такими як системи машинного навчання та штучного інтелекту. Це дозволить покращити точність виявлення та знизити кількість ложних спрацьовувань.

Системи виявлення вторгнень на основі аналізу поведінки (Behavior-based Intrusion Detection Systems) є одним з видів систем виявлення вторгнень, які використовуються для моніторингу та виявлення незвичайної або підозрілої активності в комп'ютерних системах та мережах. Замість використання підписів атак, ці системи аналізують нормальну поведінку системи та користувачів і виявляють будь-які зміни або відхилення від цієї норми, що може свідчити про кібератаку. Основний принцип роботи систем виявлення вторгнень на основі аналізу поведінки полягає у створенні профілю звичайної активності системи та користувачів. Цей профіль розробляється шляхом аналізу даних про активність, таких як мережевий трафік, журнали подій, виконані операції і т.д. Система виявлення вторгнень навчається розрізняти нормальну активність від незвичайної або підозрілої.

Важливим елементом систем на основі аналізу поведінки є алгоритми машинного навчання та аналізу даних. Вони використовуються для створення моделей, які можуть виявляти аномалії та незвичайну активність, що не відповідає звичайному профілю поведінки. Ці моделі навчаються на основі історичних даних, які включають нормальну активність та відомі випадки кібератак.

Один з підходів, використованих у системах на основі аналізу поведінки, - це статистичний аналіз. Він використовує статистичні методи для виявлення аномалій

в активності. Наприклад, можуть бути використані методи кластеризації для виявлення груп аномальної активності або методи виявлення відхилень для виявлення значних змін у поведінці системи.

Інший підхід полягає в застосуванні нейронні мережі для машиного навчання, для виявлення патернів або правил, що характеризують кібератаки або незвичайну активність. Ці моделі навчаються на основі набору тренувальних даних, що містить як нормальну, так і аномальну активність, і використовуються для класифікації нових даних як нормальних або підозрілих.

Одним з переваг систем на основі аналізу поведінки є їх здатність виявляти нові атаки або зміну поведінки, яку не було зафіксовано раніше. Оскільки ці системи засновані на аналізі змін, вони можуть виявити ранні етапи нової атаки, навіть якщо немає підписів або відомих моделей цих атак.

Проте, системи на основі аналізу поведінки також мають свої обмеження. Вони можуть виявляти підозрілу активність, але не завжди можуть точно визначити, чи ця активність є кібератакою. Велика кількість ложних спрацьовувань може виникати, коли система помилково класифікує нормальну активність як підозрілу. Тому важливо ретельно налаштовувати систему та проводити постійне навчання моделей для покращення їх точності.

У майбутньому розвиток систем виявлення вторгнень на основі аналізу поведінки буде спрямований на використання більш складних методів машинного навчання, розширення набору аналізованих даних та забезпечення їх інтеграції з іншими системами безпеки, що дозволить отримати більш комплексний підхід до виявлення кібератак і забезпечення безпеки комп'ютерних систем і мереж.

Системи виявлення вторгнень на основі машинного навчання (Machine Learning-based Intrusion Detection Systems) є потужним інструментом для виявлення кібератак та підозрілої активності в комп'ютерних системах і мережах. Вони використовують методи машинного навчання для автоматичного виявлення аномалій та патернів, що свідчать про кібератаку, на основі аналізу великих обсягів даних.

Одним із ключових елементів систем виявлення вторгнень на основі машинного навчання є побудова моделей, які можуть відрізняти нормальну активність від аномальної. Ці моделі навчаються на тренувальних даних, які містять інформацію про різні типи активності, включаючи нормальну активність та відомі типи кібератак. Алгоритми машинного навчання використовують ці дані для виявлення закономірностей та патернів, що характеризують атаки.

Існують різні підходи до використання машинного навчання у системах виявлення вторгнень. Один з них - навчання з вчителем (supervised learning). При цьому модель навчається на основі розмічених даних, де для кожного прикладу вказується його клас (нормальний або атака). Модель будується таким чином, щоб відрізняти характеристики нормальної активності від характеристик атак. Інший підхід - навчання без вчителя (unsupervised learning). При цьому модель навчається на нерозмічених даних, і вона сама виявляє закономірності та аномалії. Вона шукає відхилення від нормальної активності та групує подібні зразки разом. Також використовуються підходи напівнаглядного навчання (semi-supervised learning), коли модель навчається на розміченому невеликому підмножині даних і на нерозміченому більшому підмножині. Це дозволяє використовувати великий обсяг нерозмічених даних для покращення ефективності моделі.

Перевагою систем виявлення вторгнень на основі машинного навчання є їх здатність виявляти нові атаки та підозрілу активність, які не були включені у відомі підписи атак. Це дозволяє реагувати на постійно змінюючийся ландшафт кіберзагроз і бути більш адаптованими до нових видів атак.

Однак, системи виявлення вторгнень на основі машинного навчання також мають свої обмеження. Вони можуть страждати від ложних спрацьовувань, коли нормальна активність помилково класифікується як аномальна. Це може виникати через недостатню репрезентативність тренувальних даних або недостатню увагу до особливостей конкретного середовища. У майбутньому розвиток систем виявлення вторгнень на основі машинного навчання буде спрямований на використання більш складних алгоритмів машинного навчання, включаючи глибоке навчання (deep learning), а також на покращення якості тренувальних даних та розробку нових

методів оцінки ефективності систем. Також важливим напрямком є інтеграція систем виявлення вторгнень на основі машинного навчання з іншими методами виявлення та захисту, щоб створити комплексні та ефективні системи забезпечення безпеки комп'ютерних систем і мереж.

Системи виявлення інтелектуальних загроз (Advanced Threat Detection Systems) є важливим компонентом сучасних кібербезпекових стратегій. Ці системи розроблені для виявлення складних та високоризикових кібератак, які використовують розумні та хитрі методи, щоб уникнути традиційних заходів захисту. Основна мета систем виявлення інтелектуальних загроз полягає в ідентифікації атак, які можуть пройти незамітно через традиційні системи виявлення вторгнень. Ці системи використовують різноманітні методи, включаючи аналіз поведінки, машинне навчання та аналітику великих даних, щоб виявити складні патерни, які можуть вказувати на наявність інтелектуальної загрози.

Одним з ключових елементів систем виявлення інтелектуальних загроз є аналіз поведінки. Вони збирають та аналізують великий обсяг даних, що стосуються активності користувачів, мережевого трафіку та системних параметрів. За допомогою алгоритмів машинного навчання та штучного інтелекту, системи можуть виявити відхилення від норми та незвичайну активність, що може свідчити про наявність складної атаки. Іншим важливим аспектом є використання аналітики великих даних. Системи виявлення інтелектуальних загроз збирають та обробляють великі обсяги структурованих і неструктурованих даних з різних джерел, таких як журнали подій, логи мережі, дані з сенсорів та зовнішніх джерел. За допомогою аналітики великих даних, системи можуть виявляти складні взаємозв'язки та патерни, які можуть свідчити про наявність складних загроз.Окрім цього, системи виявлення інтелектуальних загроз використовують інтелектуальні алгоритми, які здатні виявляти нові та невідомі загрози на основі аналізу поведінки та характеристик атак. Вони використовують навчання з підсиленням (reinforcement learning), глибоке навчання (deep learning), нейронні мережі та інші методи штучного інтелекту, щоб виявляти складні та еволюційні загрози.

Перевагою систем виявлення інтелектуальних загроз є їх здатність виявляти атаки, які можуть уникнути традиційним системам виявлення вторгнень. Вони спроможні виявляти складні патерни та аномальну активність, яка може вказувати на використання розумних та хитрих методів атаки. Однак, системи виявлення інтелектуальних загроз також мають свої обмеження. Вони можуть вимагати значних обчислювальних ресурсів та інфраструктури для аналізу великих обсягів даних. Крім того, вони можуть страждати від хибних спрацьовувань, особливо при роботі з незвичайними або недостатньо представленими данними.

Існують різноманітні методи, від систем виявлення вторгнень до систем виявлення інтелектуальних загроз, які допомагають виявляти кібератаки та реагувати на них. Кожен метод має свої переваги та обмеження і повинен використовуватися в комплексі з іншими заходами безпеки. Швидке виявлення кібератак дозволяє реагувати на них на ранніх етапах та зменшує наслідки таких атак для організацій та користувачів.

2.2 Методи виявлення соціально-інженерних атак

Захиститись від атак соціальної інженерії буває складно через людський актор – соціально-інженерні атаки спрямовані на маніпулювання людьми і використовують психологічні методи для отримання довіри та доступу до конфіденційної інформації. Люди можуть бути схильними до помилок, довірливими або піддаються соціальному впливу, що робить їх вразливими перед такими атаками. Софістикованість атак - зловмисники, що здійснюють соціально-інженерні атаки, можуть бути досить витонченими і майстерними в своїй роботі. Вони використовують різноманітні методи та стратегії, включаючи піддаванняся дослідженню цільової особи, використання прихованих технік маніпуляції, вигадування вигаданих історій та використання даних з відкритих джерел для здійснення атак. Технологічні вразливості - деякі соціально-інженерні атаки можуть використовувати вразливості в системах, таких як слабкі місця в програмному забезпеченні, піддавання атакам через веб-сайти або недостатньо

захищені мережі. Це робить можливим успішне зламання системи, навіть якщо користувачі є обережними. Швидкість та неочікуваність - Соціально-інженерні атаки можуть бути швидкими та неочікуваними. Зловмисники можуть використовувати ситуації, коли люди знаходяться в стресових або невпевнених умовах, що зменшує їхню бджілість та зроблює їх більш схильними до помилок. Соціальна інформація - зловмисники можуть здобувати соціальну інформацію про своїх цілей через різні джерела, такі як соціальні мережі, пошукові системи або публічні бази даних. Це дозволяє їм підготуватись до атаки та використовувати персоналізовані методи для залучення жертви [17].

Проте щоб захиститись від таких атак спочатку їх необхідно виявити і це також буває нелегко через суб'єктивність - соціально-інженерні атаки базуються на маніпуляції психологічними факторами та використанні людських слабкостей. Це може робити атаки складними для виявлення, оскільки кожна особа має власний спосіб реагування на маніпуляцію і може бути схильною до психологічного впливу. Підступність - зловмисники, які здійснюють соціально-інженерні атаки, можуть бути витонченими і досвідченими. Вони можуть використовувати різні техніки, щоб замаскувати свої наміри та виглядати вірогідними. Наприклад, вони можуть використовувати фальшиві ідентифікаційні дані, вигадувати переконливі історії або використовувати ім'я відомих організацій або осіб. Використання технологій - деякі соціально-інженерні атаки можуть використовувати технічні засоби, такі як фішингові електронні листи, підроблені веб-сайти або шкідливе програмне забезпечення. Ці атаки можуть бути складними для виявлення, оскільки зловмисники можуть використовувати техніки, що приховують їх сліди або піддаватися недостатньому виявленню антивірусними програмами. недостатня освіта та усвідомленість - багато людей не мають достатньої освіти щодо соціально-інженерних атак і не завжди розпізнають ознаки підозрілої поведінки або запитів. Недостатня усвідомленість про ці загрози може робити важким виявлення атак та може призвести до успіху зловмисників. Застосування різноманітних методів - соціально-інженерні атаки можуть використовувати різні методи та стратегії. Вони можуть бути специфічно налаштованими під конкретну

жертву або контекст і можуть використовувати поєднання технічних та психологічних методів.

Оскільки соціально-інженерні атаки включають в себе маніпуляцію людьми з метою отримання неправомірного доступу до конфіденційної інформації або зловживання довірою. Ці атаки можуть відбуватися у реальному житті або через канали зв'язку, наприклад електронна пошта, соціальні мережі, телефонні дзвінки тощо. Існує кілька методів виявлення соціально-інженерних атак:

– Навчання персоналу: Найефективніший спосіб запобігання соціально-інженерним атакам - це навчання персоналу. Регулярні навчальні програми, які надають співробітникам інформацію про типові схеми атак та методи їх виявлення, можуть значно знизити ризик успішного проведення атак.

Персонал повинен мати базове розуміння про те, що таке соціальна інженерія, які є типи атак і як вони можуть впливати на організацію. Це включає ознайомлення з основними методами маніпуляції, такими як фішинг, фізичний доступ та використання соціальних мереж, Персонал повинен бути здатним розпізнавати ознаки можливих соціально-інженерних атак. Це можуть бути незвичайні запити на інформацію, підозрілі електронні повідомлення, незнайомці, що намагаються отримати доступ до облікових записів або фізичний доступ до приміщень і т.д. Також персонал повинен бути ознайомлений з політиками безпеки організації та дотримуватись їх. Це можуть бути правила щодо обмеження доступу до конфіденційної інформації, використання паролів, двофакторної аутентифікації, обмеження доступу до фізичних приміщень і т.д. Персонал повинен бути навчений основам соціальної інженерії, щоб бути здатним розпізнати спроби маніпуляції з їх боку. Це включає розуміння тактик маніпуляції, шляхи виявлення фішингових повідомлень та посилань, аналіз підозрілих ситуацій. Соціальні інженери постійно вдосконалюють свої методи, тому важливо, щоб персонал організації мав постійну підвищену свідомість та оновлював свої знання щодо нових трендів і методів атак.

– Фільтрація спаму та фішингових повідомлень: Використання програмного забезпечення для фільтрації спаму та фішингових повідомлень може допомогти виявити підозрілі листи або посилання, які намагаються зловживати

вашою довірою. Наприклад антиспам-фільтри - використання антиспам-фільтрів допомагає виявляти та блокувати спамові повідомлення. Ці фільтри аналізують заголовки, вміст повідомлення, адреси відправників та інші параметри для виявлення підозрілих або небажаних повідомлень. Вони можуть використовувати різні методи, такі як евристичний аналіз, списки заблокованих адрес і ключових слів, для ідентифікації спаму. Аналіз вмісту - фільтри можуть проводити аналіз вмісту повідомлення для виявлення фішингових атак. Вони шукають підозрілі фрази, посилання на підроблені веб-сайти, примусові запити на конфіденційну інформацію та інші ознаки, що вказують на фішинговий зміст. Якщо повідомлення вважається підозрілим, його можна перемістити в спеціальний спам-фільтр або помітити як потенційно шкідливе. Перевірка адреси відправника - фільтри можуть перевіряти адресу відправника повідомлення, щоб виявити підроблені або підозрілі адреси. Наприклад, вони можуть порівнювати адресу відправника з базою відомих шахрайських адрес або перевіряти, чи відповідає вона стандартам форматування адреси електронної пошти. Чорні списки та блокування доменів - фільтри можуть використовувати чорні списки або блокувати певні домени, від яких відправляються спамові або фішингові повідомлення. Це може бути основано на історичних даних про зловживання або на основі репутації домену. Навчання з використанням машинного навчання - деякі системи фільтрації використовують технології машинного навчання для виявлення нових типів спаму та фішингу. Вони навчаються розпізнавати патерни та ознаки шкідливого вмісту, що допомагає виявляти його навіть у випадках, коли він раніше не був відомий.

– Двофакторна автентифікація: Використання двофакторної автентифікації додає додатковий шар безпеки до процесу входу в систему. Крім звичайного пароля, вимагається додатковий елемент, такий як одноразовий код, відбиток пальця або sms-повідомлення з підтвердженням. Це допомагає уникнути несанкціонованого доступу, навіть якщо хтось володіє основними автентифікаційними даними. Двофакторна автентифікація є потужним інструментом для підвищення безпеки та захисту від соціально-інженерних атак. Вона вимагає від користувача надання двох незалежних способів підтвердження

своєї ідентичності для отримання доступу до облікового запису або системи. Ось ключові аспекти такі як другий фактор - крім стандартного пароля, 2FA вимагає від користувача надання ще одного фактора підтвердження, який є незалежним від пароля. Це може бути як фізичний об'єкт - наприклад, спеціальний апаратний пристрій, такий як аутентифікатор або USB-ключ, який містить унікальний код або генерує одноразові паролі, отримання повідомлення - наприклад, одноразовий код, який надсилається на мобільний телефон користувача через SMS або мобільний додаток, біометричні дані - наприклад, відбиток пальця, розпізнавання обличчя або сканування сітківки ока. 2FA надає додатковий рівень захисту, оскільки навіть якщо зловмисник зламає або дізнається пароль користувача, він все ще не зможе отримати доступ без додаткового фактора підтвердження. Це значно ускладнює заволодіння обліковим записом навіть у разі компрометації пароля. Широке застосування - 2FA використовується в багатьох різних сферах, включаючи онлайн-платформи, соціальні мережі, банківські системи, електронну пошту, хмарні сервіси та багато іншого. Багато провайдерів послуг активно рекомендують або вимагають використання 2FA для підвищення безпеки своїх користувачів, а також ефективним підходом є поєднання різних типів факторів, таких як щось, що ви знаєте (пароль), щось, що ви маєте (фізичний пристрій), і щось, що ви є (біометричні дані). Це називається мультифакторною автентифікацією (MFA) і забезпечує ще більший рівень безпеки.

– Захист від перехоплення даних: Важливо використовувати захищені канали зв'язку для передачі конфіденційної інформації. Використання шифрування є ефективним способом захисту від перехоплення даних під час їх передачі. Шифрування даних забезпечує їх конфіденційність шляхом перетворення звичайного тексту в зашифрований формат, який може бути розшифрований тільки з використанням правильного ключа. Це робить дані незрозумілими та некорисними для неправомірних осіб, які можуть перехопити їх під час передачі через мережу. Використання безпечного протоколу передачі - при передачі даних по мережі важливо використовувати безпечні протоколи, такі як HTTPS для веб-сайтів або VPN (віртуальна приватна мережа) для забезпечення шифрування

трафіку. Ці протоколи забезпечують захищену трансляцію даних між клієнтом і сервером, що ускладнює можливість перехоплення та зламування інформації. Захист бездротових мереж - якщо ви використовуєте бездротову мережу, важливо захистити її від несанкціонованого доступу. Використовуйте безпечний протокол шифрування, такий як WPA2 або WPA3, для захисту мережі паролем. Також важливо уникати відкритих та ненадійних мереж, особливо при обробці чутливих даних. Оновлення програмного забезпечення - регулярне оновлення програмного забезпечення на комп'ютерах, мобільних пристроях та інших пристроях є важливим кроком для запобігання перехоплення даних. Оновлення включають виправлення вразливостей, які можуть бути використані зловмисниками для отримання доступу до системи та перехоплення даних. Використання мережевих брандмауерів та антивірусного програмного забезпечення - мережеві брандмауери та антивірусне програмне забезпечення можуть допомогти виявляти та блокувати шкідливий трафік, що може спрямовуватись на перехоплення даних. Ці захисні заходи допомагають уникнути вторгнень та забезпечити безпеку вашої мережі та пристроїв.

– Моніторинг активності: Системи моніторингу можуть допомогти виявити незвичайну або підозрілу активність в системі, наприклад логування подій - важливо мати налагоджену систему логування, яка реєструє події та дії, що відбуваються в системі. Це включає входи в систему, зміни привілеїв, відправку або отримання конфіденційних даних тощо. Логи дозволяють виявити незвичайну або підозрілу активність, а також сприяють у розслідуванні подій у разі інциденту, аналіз поведінки користувачів - використання аналітичних інструментів для моніторингу та аналізу поведінки користувачів може допомогти виявити аномалії. Наприклад, системи машинного навчання можуть навчитися розпізнавати типові маліціозні патерни або виявляти зміни в звичайному поведінці користувачів, що може свідчити про соціально-інженерну атаку, моніторинг мережевої активності - слід ретельно спостерігати за мережевою активністю, щоб виявити незвичайний трафік або намагання несанкціонованого доступу. Моніторинг мережі може включати в себе виявлення підозрілих IP-адрес, спроб перехоплення

аутентифікаційних даних або виявлення аномально великого обсягу передачі даних, автоматизовані сповіщення та тривоги - розробка систем, які автоматично сповіщають про підозрілі активності або аномалії, може бути дуже корисною. Це може включати відправку сповіщень адміністраторам системи або активування тривог для швидкого реагування на потенційні загрози [1].

Використання сильних паролів: Важливо використовувати складні, унікальні паролі для кожного облікового запису. Це ускладнює завдання зловмисникам, які намагаються отримати доступ до вашої інформації, є деякі рекомендації щодо створення надійних паролів, наприклад довжина – довжина пароля повинна містити щонайменше 8-12 символів, чим довший пароль тим важче його зламати методом перебору. Складність - Використовуйте поєднання різних типів символів, таких як великі та малі літери, цифри та спеціальні символи. Це підвищує складність паролю та ускладнює його відтворення або злам. Використання випадкових символів - не варто використовувати очевидні або легко вгадувані паролі, такі як дати народження, імена членів сім'ї або послідовність символів. Замість цього краще використовувати генератори випадкових паролів або комбінації, які неможливо вгадати. Унікальність - кожен обліковий запис повинен мати унікальний пароль. Не варто використовувати один і той же пароль для кількох різних сервісів або сайтів. Якщо один пароль стає відомим зловмисникам, це не дозволить їм отримати доступ до всіх облікових записів. Регулярна зміна паролів - рекомендується періодично змінювати паролі для забезпечення додаткового рівня безпеки. Використання парольних менеджерів - для зручності та безпеки можна використовувати парольні менеджери. Вони допомагають генерувати, зберігати та автоматично заповнювати складні паролі для облікових записів. На рисунку 2.2 зображені деякі рекомендації щодо розкриття атаки, спрямованої на отримання інформації.

Рисунок 2.2 – Рекомендація щодо розкриття атаки, спрямованої на отримання інформації [33]

Соціально інженерні атаки часто маскуються під довірені комунікації та використовують соціальні інженерні методи для отримання довіри. Однак, існують різні методи та практики, які можна застосовувати для захисту від соціально-інженерних атак. Навчання персоналу щодо виявлення та усвідомлення підступів, фільтрація спаму та фішингових повідомлень, використання двофакторної автентифікації, захист від перехоплення даних, моніторинг активності та використання сильних паролів є ефективними способами зменшення ризиків. Крім того, важливо проводити попередні дослідження в галузі захисту від соціально-інженерних атак і використовувати нові технології та методи, щоб залишатись крок попереду зловмисників. Захист від соціально-інженерних атак є неперервним процесом, оскільки атаки постійно еволюціонують, тому важливо підтримувати свої системи та методи захисту оновленими та реагувати на нові загрози швидко і ефективно. Загальна свідомість та освіта про соціально-інженерні атаки також відіграють важливу роль у захисті. Користувачі повинні бути освіченими щодо типів атак, їхніх наслідків та методів захисту, щоб бути більш пильними та усвідомленими під час взаємодії зі сторонніми джерелами.

Захист від соціально-інженерних атак вимагає комплексного підходу, який поєднує технічні рішення, навчання персоналу та свідоме використання кінцевими користувачами. Тільки шляхом поєднання цих факторів можна створити надійну систему захисту, яка мінімізує ризики соціально-інженерних атак і забезпечує безпеку в цифровому середовищі.

3 РОЗРОБКА КОМПЛЕКСНОГО МЕТОДУ ЗАХИСТУ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

3.1 Захист від атак соціальної інженерії

Соціальні інженери можуть завдати серйозної шкоди своїм жертвам. Ця шкода може бути соціальною, економічною чи репутаційною. Зараз, як ніколи, важливо зрозуміти, яких запобіжних заходів можна вжити, щоб запобігти, пом’якшити та стримати руйнування, яке потенційно може бути спричинене в результаті атаки соціальної інженерії. Таким чином, у цьому розділі описано загальні стратегії пом’якшення соціальної інженерії, які компанії та окремі особи можуть застосувати, щоб захистити себе від потенційних атак соціальної інженерії.

3.1.1 Фізична безпека

Для будь-якого бізнесу, який дбає про безпеку, у всій організації без винятку має бути забезпечена надійна фізична безпека. Якщо безпека слабка, зловмисники не матимуть проблем з доступом до станцій, які їм потрібні для здійснення цифрової атаки. Крім того, після встановлення та впровадження чітких і лаконічних політик безпеки їх слід періодично перевіряти, щоб визначити рівень обізнаності персоналу щодо безпеки. Це вкрай необхідно для виявлення та усунення будь-яких потенційних прогалин. Постійно нагадувати, що можливість нападу дійсно реальна; це може статися будь-коли, без попередження, див. (рис. 3.1) [20].

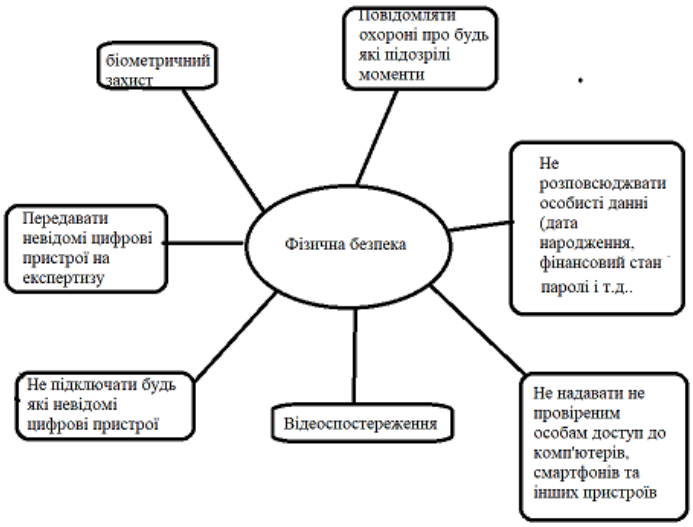


Рисунок 3.1 – Методи захисту від фізичних атак соціальної інженерії

Хорошою практикою є розміщення табличок у всіх приміщеннях, які нагадують працівникам не підключати USB-накопичувачі чи будь-які інші цифрові пристрої, які вони знайдуть поблизу приміщення. Натомість вони мають передати їх до відповідного відомства на експертизу. Крім того, вони повинні бути пильними та повідомляти охороні про будь-яку підозрілу поведінку, незалежно від того, наскільки незначною вони її вважають.

Фізичну безпеку можна підсилити за допомогою комплексного покриття систем відеоспостереження, систем зв’язку, а використання біометричних даних для ідентифікації співробітників може значно допомогти захистити бізнес від потенційної атаки. Майкл Ербшоле стверджує наступне щодо фізичної безпеки: «Суть тут полягає в тому, що незалежно від того, наскільки якісною є кібербезпека, якщо особа може увійти на об’єкт і отримати доступ до систем, ця особа фактично обійшла захист кібербезпеки.» За наявності достатнього фізичного контролю компанія може відбити істотну атаку соціальної інженерії. Однак без впровадження суворих протоколів фізичної безпеки компанія фактично тримає свої двері відкритими для неавторизованих відвідувачів зі злими намірами. Вони мають право відвідувати та проникати в приміщення, розвантажувати шкідливі програми, трояни, шпигунські програми та обходити елементи керування для доступу до

потрібних даних. Загалом, усвідомлення ризиків та обережність є ключовими аспектами фізичного захисту від соціальної інженерії.

3.1.2 Внутрішня (цифрова) безпека

Ще одним логічним кроком, який слід зробити в боротьбі з соціальною інженерією, є розгортання серії цифрових захисних сервісів і програмних засобів. Це має бути реалізовано, щоб звести нанівець ризик атак. Варто також зазначити, що хоча використання цифрових служб безпеки може бути ефективним у боротьбі з певними типами атак соціальної інженерії, вони можуть виявитися абсолютно марними в інших типах атак. Наприклад, надійний захист від спаму з оновленим чорним списком у поєднанні з захистом від вірусів/шкідливих програм і хорошим брандмауером може значно захистити вас та компанії від фішингових атак.

Враховуючи вищесказане, ці заходи виявляться абсолютно недостатніми проти фізичного цькування чи переслідування. Це не обов'язково означає, що підприємствам не слід інвестувати в механізми захисту програмного забезпечення, оскільки вони все одно забезпечують частковий захист. Що стосується захисту цифрових даних і активів, то більше того якщо вживаються заходи безпеки, тим краще. Пояснюючи серйозність ускладнень, які можуть виникнути, якщо підприємства не використовують механізми цифрового захисту, деякі TEISME (інформаційні малі середні підприємства за допомогою технологій) дозволяють зловмисникам отримати «статус системного адміністратора», конфіденційні завантаження такі файли, як паролі, імплантувати «снайпери» (те, що називають інтернет-псами або шпигунськими програмами), копіювати транзакції, вставляти «люки», щоб дозволити легке повернення, або імплантувати програми, які можна активувати пізніше для різноманітних цілей. [21]

Щоб усунути деякі з перерахованих вище ризиків, можна скористатися механізмами ізольованого програмного середовища бути дуже продуктивним. Пісочниця — це створення ізольованої віртуальної машини, використання якої захистить мережу від розповсюджувальних шкідливих програм. Використання

пісочниці проти деяких атак візуального обману настільки ефективне, що деякі популярні браузери (Chromium [22], Firefox [23]) мають вбудовані технології ізольованого програмного середовища, щоб запобігти використанню через інтернет-браузери.

У 2010 році Лонг Лу і його колеги розробили і випробували цікаву незалежну від браузера концепцію ОС. Система під назвою BLADE [24], що означає «Block All Drive-By Exploits», спрямована на запобігання автоматичному неавторизованому виконанню бінарних файлів у системі. Мимовільні завантаження відбуваються, коли відбувається пряме підключення до скомпрометованого веб-сайту, що призводить до встановлення зловмисного програмного забезпечення без авторизації веб-користувача. Використовуючи підхід запобігання виконанню без згоди, автор ОС розробив BLADE як драйвер ядра. Це розширення ядра дозволяло системі застосовувати правило, яке забороняло будь-які виконувані файли в системі, які не мали явної згоди користувача. Будь-які завантаження, які відбуваються, спрямовуються в пісочницю, де вони зберігаються та очікують подальших інструкцій від авторизованого користувача. Під час початкової стадії оцінювання система працювала на 100% ефективності, забороняючи всі 18 896 спроб завантажень із зламаних веб-сайтів. Немає жодних оновлень щодо проекту після останньої попередньої оцінки. Це свідчить про те, що проект не був реалізований, можливо, через брак коштів або ресурсів. Тим не менш, це залишається чудовою концепцією; Якщо його зробити з відкритим вихідним кодом і розробити далі, щоб охопити всі виконувані файли, а не лише ті, що завантажуються з браузерів, це могло б стати чудовим інструментом для захисту системи від технічних маніпуляційних інструментів, які використовують соціальні інженери.

Інші спеціальні заходи можуть виявитися дуже ефективною стратегією пом’якшення атак соціальної інженерії. Такі заходи включають проактивний моніторинг, агресивну автентифікацію/облік користувачів і використання цільових алгоритмів машинного навчання та аналізу. Можна спостерігати за нормальною поведінкою системи, і вона може самонавчати розрізняти законні та незаконні дії

користувача та невідповідності даних/пакетів. Зокрема, системи машинного та поведінкового навчання стали настільки ефективними, що вони здатні виявляти та зупиняти складні атаки соціальної інженерії, такі як фішинг. Група технічних ентузіастів під керівництвом Джанлуки та Олів'є [25] розробила векторну машинну систему навчання, яка має здатність ідентифікувати та блокувати фішингову електронну пошту.

Автори описують систему як систему, що працює на основі моніторингу звичок користувачів і розробки профілів користувачів. Профіль базується на стилі письма користувача, використанні розділових знаків, розпізнаванні символів, частоті слів, вмісті електронної пошти вхідних повідомлень, звичайному часі отримання та доставки електронної пошти та інших параметрах. Після розробки профілю він оновлюється щоразу, коли надсилається або отримується електронний лист. Коли алгоритм досягає основного стану, він блокує всі електронні листи, які він вважає фішинговою атакою. Автори стверджували, що досягли рівня хибнопозитивного виявлення нижче 0,05% на етапі фінального оцінювання, що є чудовим досягненням, враховуючи різноманітність вмісту, який може з'явитися в електронному листі з фішинговою атакою aspear. Механізми внутрішньої безпеки, описані вище, а також багато інших рішень безпеки, доступних через спеціалізованих онлайн-постачальників, можуть служити потужним щитом, який можна використовувати для захисту компаній від атак соціальної інженерії. Після впровадження ці рішення можуть потребувати постійного ручного моніторингу. Прикладом цього може бути щоденний, щотижневий або щомісячний аналіз виявлених і заблоковані атаки. Такі процедури необхідні, щоб гарантувати, що законні з'єднання не припиняються без потреби.

Ці цифрові захисні заходи можуть блокувати перші кілька спроб соціальних інженерів. Однак компанії повинні розуміти, що соціальні інженери та хакери присвятили себе пошуку експлойтів, часто присвячуючи цьому свій повний робочий день. Це особливо стосується випадків, коли вони визначили хорошу мотивацію для злому певної компанії. Система може заблокувати певну кількість спроб, але тоді зловмисник може взяти верх і знайти технічну експлойт, що надасть

йому потрібний доступ. Постійно аналізуючи спроби атак і відповідно оновлюючи інфраструктуру, підприємства можуть краще захистити себе від цих атак.

3.1.3 Впровадження ефективної політики та процедур безпеки

Через динаміку сучасного IT-світу, яка постійно змінюється, вкрай важливо, щоб керівники та співробітники були обізнані про поточну політику та процедури безпеки своєї компанії. Політика безпеки містить процедури та вказівки, які визначають методи захисту даних і активів організації. Необхідно мати стислий і чітко визначений набір правил для максимальної ефективності, і ці правила повинні бути доступні всім працівникам, незалежно від рангу. З огляду на це, політики також мають бути захищені від несанкціонованого доступу, який може допомогти зловмисникам отримати уявлення про внутрішню роботу компанії. Відсутність чіткої політики безпеки може, по суті, стати причиною переважної невідповідності серед працівників, що призводить до успішних атак і штрафів з боку влади. Мітнік вичерпно написав про корисність добре вивченої політики безпеки. У його книзі є обширний і присвячений розділ «Мистецтво обману», призначений для авторів політики та дослідників. Про важливість організованої та узгодженої політики безпеки Мітнік зазначає: «Розроблені на зниження ризику семантичних атак, добре підтримувані політики та організаційні процедури допомагають пом’якшити та значно знизити ризик виникнення потенційного експлойту, не покладаючись на технічні можливості користувачів».

Наведене вище твердження чітко пояснює, що політика безпеки не лише важлива для виживання компанії, вона є невід’ємним інструментом захисту працівників від будь-якої потенційної шкоди. Тому вкрай важливо, щоб менеджери були в курсі будь-яких змін у політиці безпеки компанії. Це також вони несуть відповідальність за те, щоб зміни були доведені до відома їхніх співробітників, і щоб вони впроваджувалися послідовно в усьому світі. В дослідженні, опублікованому в грудні 2015 року, Райан і Джордж пишуть: «Політика та процедури мають бути гнучкими до невідомих і непередбачених атак і, отже,

відповідати мінливому ландшафту загроз. Фіксовані рекомендації можуть швидко застаріти, оскільки постійно розробляються нові методи атаки». [26]

Таким чином, ми зрозуміли, що одна з найбільших переваг застосування політик і процедур безпеки полягає в тому, що вони не тільки захищають компанію від атак зловмисників, але й від потенційних судових позовів. Прикладами цього є політика щодо захист даних, заборона інформації, пов'язаної з бізнесом, у соціальних мережах, а також політики щодо використання BYOD (Bring Your Own Device). Такі процедури можуть запобігти судовим позовам, які можуть виникнути в разі успішної атаки та репресій з боку місцевої влади через невідповідність бізнесу. Добре підтримувана та регулярно оновлювана політика є кінцевим результатом комплексного дослідження, оновлених законів та уроки, отримані з попередніх атак. Це походить від політики інших успішних компаній у тій самій галузі та може призвести до значного зниження ризиків безпеки. Впровадження політики безпеки безпосередньо пов'язане з використанням комп'ютера на роботі. Працівник самовільно доступ до скомпрометованого веб-сайту або жертва фішингової атаки поставить підприємство під загрозу через те, що їхня робоча станція підключена до мережі. Потужні та ефективні політики доступу до комп'ютера та авторизації разом із кваліфікованим брандмауером і надійним корпоративним антивірусом мають бути достатніми, щоб зупинити будь-яке ненавмисне нанесення потенційної шкоди IT-інфраструктурі компанії.

3.1.4 Тестування на проникнення

Якщо компанія вжила достатньо заходів безпеки та відчуває впевненість, що вона захистила себе від атаки, доцільно пошукати повторну думку досвідченого та професійного тестера на проникнення. Основна мета тесту на проникнення – визначити технічні вразливості та слабкі місця в мережі, системах і програмах, що використовуються бізнесом. Крім перевірки стійкості цифрових активів компанії, багато фірм, які перевіряють проникнення, також пропонують свої послуги для визначення перспектив безпеки співробітників бізнесу. Застосовуючи ту саму

тактику, що й зловмисний соціальний інженер, але за згодою компанії, офіційний тестувальник проникнення намагатиметься отримати доступ до системи за допомогою людських маніпуляцій, прямого злому чи використання інших прийомів. Такі трюки варіюються від телефонних текстів і фішингу, до бейтингу, tailgating та інших атак використання браузера. Після завершення симуляції атаки фірма, яка керує атакою, надає роботодавцю звіт із детальним описом виявлених уразливостей, ймовірних причин слабких місць і стратегій усунення. Підприємство може слідкувати за відгуками, щоб усунути виявлену вразливість. Якщо центром імітованої атаки були внутрішні співробітники, а також інфраструктура, тоді компанія також може виявити, яка техніка маніпулювання людьми була використана для отримання доступу до потрібної інформації. Отримана інформація може бути дуже корисною для захисту мережі та співробітників у підготовці до атаки в реальному житті. Коментуючи важливість тестування на проникнення, Стів зазначає: недостатньо часто захищати та оновлювати, хоча ці два елементи, безумовно, мають велике значення для забезпечення безпечного середовища. Ще один основний пункт глибокої безпеки – це часте тестування. Тестування гарантує, що політики безпеки дотримуються, і впровадження цих політик безпеки є успішним».

У сучасну епоху існує безпрецедентна складність і частота атак, націлених на бізнес, і з експоненційним зростанням кібер-злочинної діяльності для компаній стає все більш важливим вживати всіх доступних їм заходів безпеки . Вищезгадана заява Стіва чітко підкреслює корисність оновленої та безпечної системи. Із зауваження також зрозуміло, що тестування на проникнення дозволяє компаніям виявляти слабкі місця в повсякденному впровадженні політики безпеки. Navigant також повідомляє, що тестування Cenzic Security, проведене того ж року, призвело до виявлення технічних недоліків у 96% випадків. Середня втрата в 6 200 200 доларів США є значною сумою, тоді як тестування безпеки коштувало б лише незначну частину цієї суми. Ця неймовірна статистика дає всі підстави для компаній, які піклуються про безпеку, виробити звичку проходити регулярні тести на проникнення. Подальші дослідження показують, що в 2015 році більше

половини всіх підприємств Великобританії постраждали від атаки програм-вимагачів [27], шкідливої програми, яка зазвичай передається через фішингові атаки.

Окреме дослідження показує, що кожен п’ятий бізнес у Великобританії, який постраждав від атак програм-вимагачів, змушений закритися. Це викликано різними причинами, починаючи від високих вимог викупу до втрати даних, негативного розголосу та судових позовів. Щоб перемогти ракову хворобу кіберзлочинності, компанії повинні вийти за межі звичайної ділової практики, щоб залишатися на вершині гри. Проблеми безпеки в сучасному цифровому світі, м’яко кажучи, динамічні, складні та заплутані. Тому надійна кібербезпека та постійне тестування інфраструктури та співробітників мають бути головним пріоритетом компанії. Цілісна та всеосяжна стратегія управління ризиками, кібербезпека допоможе підприємствам значно захистити себе від небезпек кіберзлочинності та атак соціальної інженерії. За допомогою автоматизованих технологій можна виявити життєво важливі прогалини в безпеці та відповідним чином усунути їх.

3.1.5 Навчання користувачів і обізнаність про безпеку

Люди легше доступні та зручніші для експлуатації, ніж машини, і тому людський елемент у бізнесі залишається найбільш вразливим для соціальних інженерів. Політики, які забезпечують надійні паролі, двофакторну автентифікацію для входу в робочий кабінет, брандмауери найвищого класу та IDS, стають зайвими, якщо співробітники не розуміють важливості підтримки безпеки своїх PIN-кодів, паролів і доступу картки. З моменту появи сучасних технологій соціальні інженери та хакери зрозуміли, що людська ланка в будь-якому технологічному рівнянні завжди є найбільш корисним елементом. Люди – це формований ключ, яким можна легко маніпулювати, щоб отримати доступ до будь-якої мережі, системи чи даних. Таким чином, тенденція доступу до цілей за допомогою «тільки технологій» змінюється. Отримання інформації від когось під

фальшивими приводами, маніпуляціями, обманом і примусом тепер є загальноприйнятим.

Наступна цитата влучно підсумовує причину збільшення кількості атак на співробітників, а не на інфраструктуру: «Навіщо витрачати зусилля на злам паролів, коли ви можете запитати про це» – невідомо. По суті, найефективніший засіб пом'якшення стратегією соціальної інженерії є освіта. Завдяки періодичному та систематичному навчанню з питань безпеки та частим нагадуванням про необхідність бути насторожі та бути пильним щодо підозрілої поведінки, підприємства можуть ефективно перетворити свою найслабшу ланку на найсильнішу. Співробітникам життєво важливо розуміти важливість захисту конфіденційної інформації, а також важливість знання того, як соціальний інженер може завдати удару. З більшою обізнаністю вони можуть розвинути знання про різні вектори атаки та створити здатність розрізняти розсіяну та пряму атаку. Співробітники можуть дізнатися, що соціальний інженер не запитуватиме код безпосередньо; вони не ляпнуть: «Дайте, будь ласка, код доступу до серверної кімнати?»

Натомість вони пов'язуватимуть невеликі фрагменти інформації, які вони отримали з часом, розшифровуватимуть підказки та сигнали, надані їм кількома співробітниками, а потім з'єднуватимуть шматочки головоломки, щоб розкопати інформацію, яку вони шукали. Найважливішим заходом, який може захистити компанію від атаки соціальної інженерії, є постійна програма інформування про інформаційну безпеку. Слово «продовження» наголошено навмисно; нещодавнє дослідження [27] показало, що після відвідування сесії бізнес-тренінгу працівники зазвичай забувають 50% інформації за годину, 70% за 24 години та 90% за тиждень. Таким чином, хоча підготовча робота до навчання, а також сама доставка можуть бути інтенсивними та дорогими вручну, це все ж необхідний крок, який компанії повинні зробити, якщо вони хочуть захистити себе від атак соціальної інженерії.

Гвідо Роблінг, поважне ім'я в галузі академічних кіл, який на сьогоднішній день має понад сотню публікацій і має численні академічні нагороди, дає такий коментар щодо важливості обізнаності про безпеку: «Лише дві речі справді

допомагають проти соціальної інженерії: обізнаність і контроль -спис. Користувачі повинні знати про соціальну інженерію, як вона працює, і бути напоготові, коли виникають «дивні» телефонні дзвінки чи електронні листи». Повідомлення, яке Гвідо намагається донести, не може бути більш зрозумілим; Абсолютна безпека ніколи не може бути гарантована, але, граючи розумно та навчаючи співробітників обізнаності з безпекою, компанії можуть перетворити своїх неосвічених працівників на освічених та винахідливих сторожів. По суті, працівники перетворюються із пасивів на активи.

3.2 Аналіз стратегій пом'якшення

У наведеному підпункті розділу було представлено та обговорено п'ять різних стратегій, які фірми можуть застосувати для захисту від атак соціальної інженерії. У цьому розділі метою є, розробити найефективніший і корисний підхід, який справді може переломити плани зловмисників.

3.2.1 Проінформованість про безпеку

Раніше людям доводилося докладати зусиль, щоб навчитися хакерству та соціальній інженерії. Тепер, коли Інтернет доступний (і переповнений інформацією), вивчення методів експлуатації стало набагато простішим. Доступні навчальні посібники та наявність спеціалізованих веб-сайтів для навчання соціальної інженерії означає, що «вільний час і відданість» – це все, що потрібно, щоб оволодіти мистецтвом соціальної інженерії. Потреба для підприємств бути обережними щодо цієї постійно зростаючої загрози зараз є фундаментальною.

Відсутність обережності зрештою призведе до катастрофи. Тому з багатьох дій, які може вжити компанія, поінформованість про безпеку є, мабуть, найефективнішою проти атак соціальної інженерії. Як неодноразово згадувалося раніше, компанії можуть вживати всіх доступних їм заходів безпеки, але якщо їхні співробітники не поінформовані про ризики розголошення внутрішньої

конфіденційної інформації незнайомцям, усі існуючі заходи безпеки втрачають сенс. Також важливо розуміти, що обізнаність у сфері безпеки стосується не лише працівників, які користуються телефонами та комп'ютерами. Від високопоставлених менеджерів до охоронців, прибиральників і персоналу громадського харчування, кожен в організації повинен мати 10 чітке уявлення про ризики, пов'язані з атаками соціальної інженерії. Залучення всіх співробітників до навчання з питань безпеки (включно з персоналом, не пов'язаним з IT) не тільки допомагає їм зрозуміти необхідність залишатися пильними, але й гарантує, що вони сприймають програму безпеки в цілому; що, як наслідок, покращить перспективи безпеки всієї організації. Грагг [28] у своєму дослідженні багато говорить про необхідність мати добре сформовану обізнаність щодо безпеки серед усіх працівників. Він припускає, що кожна організація повинна мати конкретну політику безпеки, спрямовану на соціальну інженерію. Далі він припускає, що кожен працівник повинен пройти навчання з питань безпеки, тоді як ті, ким легко маніпулювати, також повинні пройти навчання опору. Сара Грейнджер, медіа-новатор і автор, стверджує, що: «Бойові стратегії... вимагають дій як на фізичному, так і на психологічному рівнях. Необхідно навчати працівників. Помилка багатьох корпорацій полягає в тому, що планують атаку лише з фізичного боку. Це залишає їх широко відкритими з соціально-психологічної точки зору». Це влучне спостереження. Доповнюючи це твердження, Мартін стверджує, що аргументи на користь інформаційної безпеки в бізнесі є дуже сильними. Він стверджує, що якщо фізична безпека є двигуном, то обізнаність персоналу є маслом, яке рухає цю систему вперед . Висловлюючи свої думки,

Шухайлі стверджує, що з огляду на постійну зміну ландшафту безпеки та все більшого впровадження технологій людьми, необхідність підтримувати сучасний рівень обізнаності є обов'язковою . Подібним чином Агентство Європейського Союзу з мережевої та інформаційної безпеки (ENISA) стверджує, що освічені працівники допоможуть підвищити узгодженість та ефективність існуючих засобів контролю інформаційної безпеки та потенційно стимулюватимуть впровадження економічно ефективних засобів контролю. По суті, комплексна програма навчання

поступово зменшить витрати на ІТ-безпеку. Реальні переваги навчання співробітників правилам безпеки в Інтернеті нескінченні. Компанії не тільки заощадять гроші завдяки зменшенню кількості порушень безпеки (та відповідних штрафів), вони також захистять себе від необхідності реагувати на будь-яку негативну пресу та нав'язливий контроль з боку влади, що часто відбувається після порушення.

Крім того, відмінна репутація серед клієнтів компанії як компетентної та суворої щодо безпеки, підтверджена результатами періодичних тестів на проникнення, означає, що перспективи зростання клієнтури можуть бути нескінченними. Для порівняння візьмемо, наприклад, випадок Talk Talk. Ця організація за відносно короткий проміжок часу міцно зарекомендувала себе як бюджетний широкосмуговий провайдер і лідер у сфері волоконної оптики. Тим не менш, вони почали привертати негативну увагу ЗМІ та громадськості після трьох послідовних гучних порушень безпеки протягом одного року. Ці порушення призвели до втрати 101 000 клієнтів і фінансових втрат у розмірі приблизно 60 мільйонів фунтів стерлінгів. [29] Щоб ще більше підтвердити нашу думку про те, що обізнаність співробітників про безпеку є ефективною стратегією боротьби з атаками соціальної інженерії, ми присвятимо наступний розділ цього розділу практичним прикладам. Ми будемо оцінювати покращення безпеки до та після того, як працівники відвідали курс з безпеки. Аналіз цих випадків продемонструє, що обізнаність у сфері безпеки є вирішальною.

Приклади: Компанія А – невелика фінансова установа . Компанії А було відомо про цілеспрямовані спроби фішингу, спрямовані на МСП. Однак вони не змогли навчити своїх співробітників знанням безпеки, за винятком деяких ключових співробітників у своєму ІТ-відділі. У рамках нової ініціативи деякі з нещодавно прийнятих на роботу співробітників отримали дуже обмежений і базовий доступ до ІТ-безпеки. Після цього компанія вирішила зробити навчання з питань безпеки обов'язковим для всього персоналу, уклавши контракт із постачальником навчання з безпеки ІТ. У рамках навчального процесу були проведені тести на фішинг до та після проведення тренінгу. Згідно зі звітом,

початкові тести показали, що 39% співробітників компанії з високою ймовірністю клацнуть фішинговий електронний лист, що може призвести до серйозного порушення безпеки.

У відповідь на рекомендації компанія запровадила обов'язковий тренінг для менеджерів тривалістю 40 хвилин із скороченою 15-хвилинною версією для інших співробітників. Після того, як усі співробітники пройшли навчання з питань безпеки, було проведено ще один тест, щоб визначити, як працівники реагуватимуть на фішингові електронні листи. Звіт показав, що жоден із співробітників не перейшов за фішинговим посиланням. Імовірність того, що співробітники стануть жертвою фішингової атаки, впала з 39% до 0%. Компанія Б - Транспортно-логістичний бізнес. У компанії В працювало понад 3000 співробітників, більшість із яких отримували надані компанією КПК і ноутбуки. Після того, як новий менеджер із безпеки взяв на себе керівництво його офісом, він зауважив, що серед співробітників поширені погані IT-практики. Наприклад: зловживання правами доступу користувача; відкритий обмін паролями між співробітниками; обмін обліковими даними доступу; використання простих паролів (наприклад, 123456); співробітники залишають комп'ютери розблокованими, коли вони знаходяться поза робочим столом, і несанкціоноване розкриття інформації третім особам. Аудит також виявив, що в більшості випадків до інциденту призвело незнання або ненавмисна помилка співробітника. Це було стандартом IT-безпеки протягом багатьох років, тому компанія вирішила діяти та розпочала роботу над широкомасштабною інформаційною кампанією з IT-безпеки.

Після консультацій компанія запровадила стандарт PDCA (Plan, Do, Check, Act) для управління інформаційною безпекою, прописаний у ISO 27110:2005. Після запровадження обов'язкових тренінгів із безпеки (тривалістю 120 хвилин на модуль) у компанії помітно покращилося ставлення співробітників до інформаційної безпеки. На заняттях тренери активно заохочували співробітників використовувати більш розумні та надійні паролі. Дані оцінки перед навчанням показують, що 57,9% співробітників використовували прості паролі, які були зламані тестувальниками проникнення приблизно за дві години. Аудит,

проведений незабаром після тренінгу, показує, що використання простих паролів скоротилося відразу до 20%. Загалом після тренінгу з безпеки компанія помітила значне покращення серед персоналу щодо дотримання політики безпеки. Після того, як компанія запровадила постійну програму підвищення обізнаності щодо безпеки для всього персоналу, показники ненавмисних порушень безпеки, несанкціонованого розголошення та неправильних IT-практик значно впали. Компанія С - Велика глобальна виробнича компанія. У компанії С працює понад 5000 співробітників по всьому світу, і вона десятиліттями займається виробництвом.

Незважаючи на надійні системи автентифікації та фільтрації, компанія почала помічати атаки зловмисного програмного забезпечення на свою інфраструктуру – переважно через фішингові атаки та зараження браузера. Співробітники взагалі не були обізнані про IT-безпеку, і в компанії не було ні політики, ні плану, щоб розповісти користувачам про шкідливі наслідки бездумного натискання URL-адреси. Було підраховано, що ці інфекції обходяться фірмі в понад 700 000 доларів США щорічно лише у вигляді витрат на ремонт. Побоюючись гіршого, компанія вирішила придушити зростаючу кількість заражень шкідливим програмним забезпеченням. Вони уклали контракт з провайдером тренінгів з безпеки в Інтернеті, який пропонував курс кількома мовами. Оскільки більшість співробітників використовували комп’ютери компанії для електронної пошти та перегляду Інтернету, компанія зосередила свої зусилля на підвищенні рівня безпеки в трьох ключових сферах: безпека електронної пошти, безпечніший веб-перегляд і навчання URL-адресам. Завдяки тісній співпраці з постачальником курсів безпеки компанії вдалося навчити 95% своїх співробітників за дванадцять місяців.

Повідомляється, що до програми навчання компанія мала справу з 72 зараженнями шкідливим програмним забезпеченням на день. У огляді, проведеному через чотири місяці після початку програми.Усі перелічені вище приклади мають одну спільну рису: компанії не мали ефективного плану підвищення обізнаності щодо безпеки. Це призвело до зловживань IT, заражень і

атак на їх інфраструктуру. Потім ми помічаємо, що спостерігалося значне зменшення проблем, пов'язаних з IT, після того, як заклади запровадили ефективну програму навчання з питань безпеки. Також очевидно, що всі три компанії отримали швидку віддачу від інвестицій, які вони зробили в проведенні курсів обізнаності. Це було правдою з точки зору загальної економії вартості заходів з виправлення ситуації.

Зрештою, їхні співробітники також розвинули здорове почуття підозри щодо кібератак, що саме по собі є тим, що розумний і розумний роботодавець повинен заохочувати та очікувати від своїх працівників. Тут також слід розуміти, що огляд цих тематичних досліджень мав лише одну головну увагу, а саме загальний вплив після проведення курсів підвищення обізнаності. Якщо роботодавці також почнуть інтегрувати інші методи захисту, описані в цьому розділі, вигоди від такого рішення будуть позитивно далекосяжними, а його наслідки будуть довгостроковими. Захист, досягнутий завдяки комплексній багаторівневій і довготривалій стратегії захисту, потенційно може забезпечити майже імунітет компаній від кібератак і атак соціальної інженерії.

Соціальні інженери знаходяться в постійному пошуку нових технічних і психологічних вразливостей, щоб вони могли продовжувати експлуатувати свої цілі. На жаль, неосвічені та наївні працівники полегшують соціальним інженерам завдання маніпуляції. Мимоволі необізнані працівники простягають руку допомоги зловмисним соціальним інженерам і в кінцевому підсумку стають частиною сутички, яка приносить довгострокові труднощі компанії, яка їм довірилася. Однак, як детально сказано в цьому розділі, існують численні заходи, які підприємства можуть вжити, щоб запобігти тому, щоб стати жертвою атак соціальної інженерії. Одним із них є знання безпеки, яке можна досягти кількома способами:

– Навчання на місці - можна домовитися про підготовку внутрішнього співробітника, який може проводити регулярні внутрішні тренінги, щоб, у свою чергу, навчати інших співробітників обізнаності з безпекою. Крім того, для цієї мети можна найняти зовнішніх тренерів. Головне, щоб ці сесії не були тривалими; їх слід проводити невеликими порціями з регулярними перервами. Таким чином,

аудиторія легко засвоїть повідомлення, і вона не страждатиме від втоми на тренуваннях. Іншим важливим фактором, який слід враховувати, є те, що сесії не повинні містити технічного жаргону. Співробітники, які не виконують технічних обов'язків, не зобов'язані розуміти, як працювати з брандмауером або як працюють програми захисту від шкідливих програм. Навчання має проводитися простою, легкою для розуміння мовою з чіткими цілями та зосереджено на виявленні та запобіганні виникненню соціальної інженерії.

– Внутрішня мережа – внутрішня мережа компанії може бути дуже винахідливою для сприяння програмам підвищення рівня безпеки. Наприклад, компанія може інтегрувати курс безпеки, підготовлений уповноваженим персоналом на місці або зовні, і вказати програму як навчальний посібник у помітному розділі внутрішньої мережі. Менеджери повинні заохочувати працівників регулярно переглядати вміст, щоб інформація закарбувалася у свідомості працівників. Інтранет також є хорошим засобом для розповсюдження сповіщень про безпеку серед працівників щодо недавніх ризиків безпеці з інструкціями щодо того, як боротися із загрозою та кому повідомляти про інцидент.

– Скрінсейвери – скрінсейвери можуть відігравати важливу роль у підвищенні обізнаності про безпеку серед працівників. Їх можна використовувати для відображення коротких нагадувань на такі теми, як безпека пароля, заборона відходу, виклик будь-кому без бейджа/перепустки компанії, повідомлення про будь-яку підозрілу поведінку відповідним відділам тощо. Необхідно докласти зусиль, щоб забезпечити використання більших, більш жирних шрифтів і відповідних і релевантних зображень, щоб контент можна було переглядати та розуміти з розумної відстані.

– Плакати – показ яскравих та яскравих плакатів із великими шрифтами може ефективно привернути увагу. Розміщення коротких і цілеспрямованих повідомлень про проблеми безпеки, що стосуються бізнесу, може стати ефективною стратегією підвищення обізнаності серед працівників. Загальні нагадування про безпеку на плакатах слід регулярно чергувати, що надасть

працівникам можливість. Плакати з більш важливими та конкретними нагадуваннями можна розміщувати на видній частині робочого місця.

– Нагадування вручну – короткі та прямі нагадування також можна доставляти працівникам за допомогою друкованих аркушів. У випадках, коли інтранет або інші ресурси персоналу недоступні, це може бути доступною моделлю для інформування працівників про ризики, пов'язані з соціальною інженерією. Менеджери також можуть запровадити систему, у якій ці ручні/фізичні нагадування розповсюджуються на робочому місці зі списком імен співробітників і датою. Таким чином, кожен, хто прочитав і зрозумів вміст, може підписати форму, підтверджуючи, що він переглянув нагадування про безпеку, а до тих, хто цього не зробив, можна буде повторно звернутися з нагадуваннями.

– Онлайн-курси – роботодавці також мають можливість вибрати одного з багатьох постачальників онлайн-тренінгів з безпеки. Онлайн-курси не лише забезпечують самостійне навчання та гнучкість, але деякі провайдери також пропонують інтеграцію з внутрішньою мережею та спеціалізоване програмне забезпечення в пакеті. Таким чином, менеджери можуть відстежувати прогрес своїх співробітників зі своїх комп'ютерів. Незважаючи на те, що багато веб-сайтів онлайн-навчання стягують плату за надання курсів, у мережі також є чудові та безкоштовні ресурси, наприклад www.cybrary.it. Ці веб-сайти можуть бути дуже ефективними в розширенні знань працівників про ризики, пов'язані з соціальною інженерією, і мають додаткову перевагу у вигляді нульових витрат для роботодавців, що виявляється дуже корисним для підприємств, які відчувають нестачу в готівці.

Безсумнівно, багаторівнева програма захисту буде більш ефективною проти атак соціальної інженерії, ніж один метод захисту. Щоб стати компетентними в питаннях захисту, співробітники повинні розуміти методи експлуатації, які використовують соціальні інженери. Часто буває так, що єдиною причиною, по якій зловмисникам вдається отримати доступ до цілі, є те, що вони успішно використовують слабкі сторони співробітників. Тому компанії повинні витрачати свій час і зусилля на те, щоб переконатися, що їхня робоча сила справді розуміє та

оцінює загрозу соціальної інженерії. Визнаючи загальні методи експлуатації, які соціальні інженери використовують для здійснення атак, працівники можуть відігравати величезну роль у захисті, а саме вживаючи превентивних заходів. Використовуючи креативність у своїх власних витончених методах, підприємства також можуть викликати у своїх працівників різноманітні поведінкові захисні інстинкти. Чудовим способом досягти цього є проведення регулярних сеансів мозкового штурму, щоб співробітники могли заздалегідь надсилати нові ідеї щодо захисту та вчитися на досвіді один одного.

3.3 Розробка комплексного методу захисту від соціально-інженерних атак в Х-компанії

Соціально-інженерні атаки, такі як фішинг, вимагання викупу (ransomware) або витоки даних, можуть призвести до незаконного доступу до конфіденційної інформації компанії. Такі атаки можуть призвести до фінансових втрат через шахрайство, крадіжку фінансових реквізитів або шахрайські перекази.

Усі ці аспекти підкреслюють важливість розробки комплексного методу захисту від соціально-інженерних атак для компаній. Це дозволяє забезпечити безпеку даних, уникнути фінансових втрат, зберегти репутацію та підвищити безпеку персоналу.

Ознайомившись та проаналізувавши різні методи захисту від соціально-інженерних атак, а також з їхнми плюсами та недолками, мною було розроблено та поетапно впроваджено комплесний метод захисту від атак соціальної інженерії для Х-компанії.

3.3.1 Інформування працівників

На сам перед в компанії було створено список дозволених встановлених програм для всіх працівників, згідно з яким працівники не можуть (не повинні) встановлювати, або використовувати програми, що не передбачені у списку. Якщо працівник для комфортної роботи хоче використовувати програму, яка не

зазначена у списку, він повинен звернутись із цим питанням до свого керівника див. (рис. 3.2).

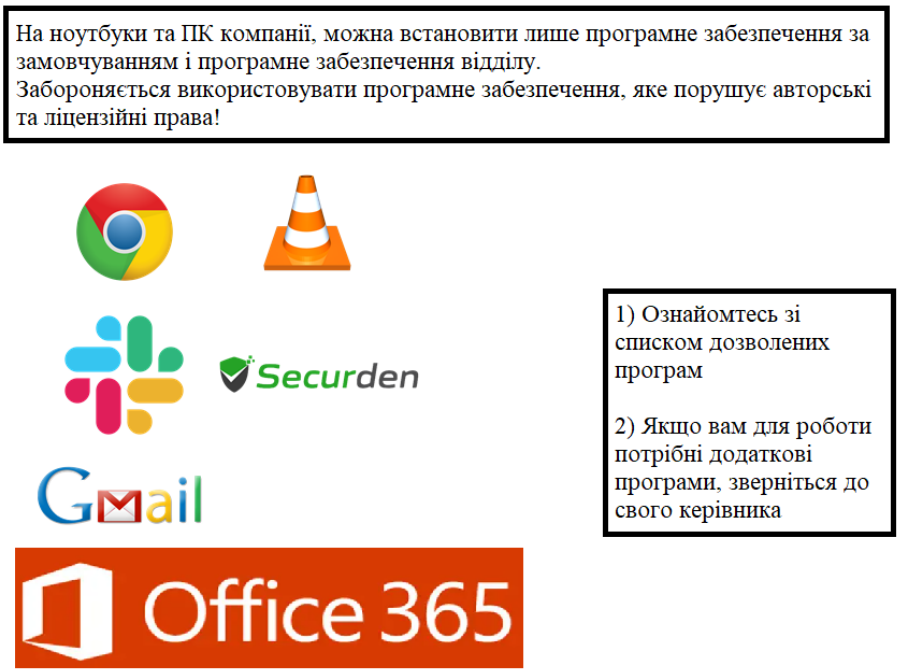


Рисунок 3.2 – Список дозволених програм

Також були розроблені правила створення паролів див. (рис. 3.3).

Правила створення паролів	Додаткові вказівки
1) Пароль повинен містити в собі мінімум 8 символів. 2) Пароль повинен містити в собі один з особливих символів (-, +, /, \, @, #, $, &). 3) Пароль повинен складатись з різним регістром символів (A - a, B - b).	1) Не використовувати один пароль для всіх програм. 2) Пароль не повинен складатись з важливих для вас дат, таких як дні народження. 3) Не повідомляйте свої паролі нікому окрім керівника.

Рис. 3.3 – Правила при створенні паролів

Надійний пароль дуже важливий, адже чим він більший та складніший, тим складніше соціальному інженеру на базі ваших данних підібрати пароль методом підбору.

3.3.2 Двофакторна автентифікація

Навіть якщо працівники дотримуються всіх правил при створені паролів, зловмисник може різними методами дізнатись його, тож для більшої безпеки всі працівники повинні використовувати двофакторну автентифікацію пов’язаною із номером працівника див. (рис. 3.4).

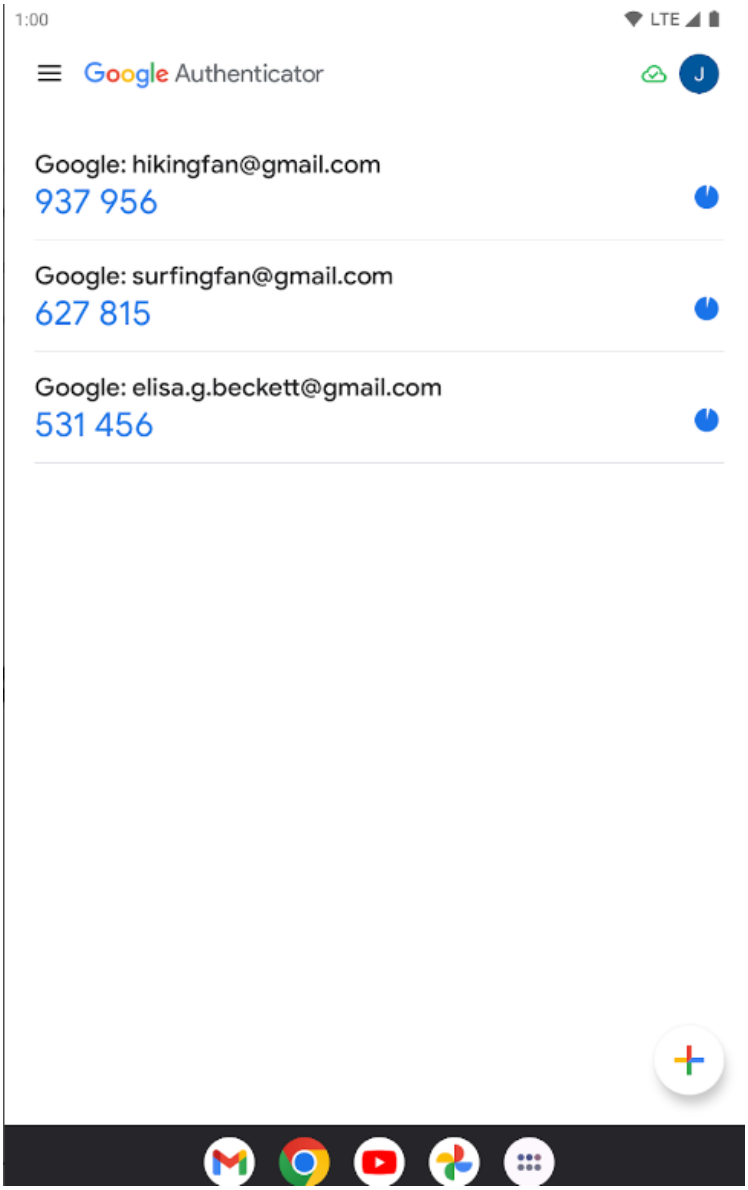


Рисунок 3.4 – Двофакторна автентифікація

Двофакторна автентифікація значно підвищить рівень безпеки в компанії, адже малоймовірно, що зловмисник буде мати доступ до телефона співробітника.

3.3.3 Відстеження локації

В ноутбуки та ПК компанії було впроваджено систему відстеження локації за допомогою Windows 10 див. (рис. 3.5).

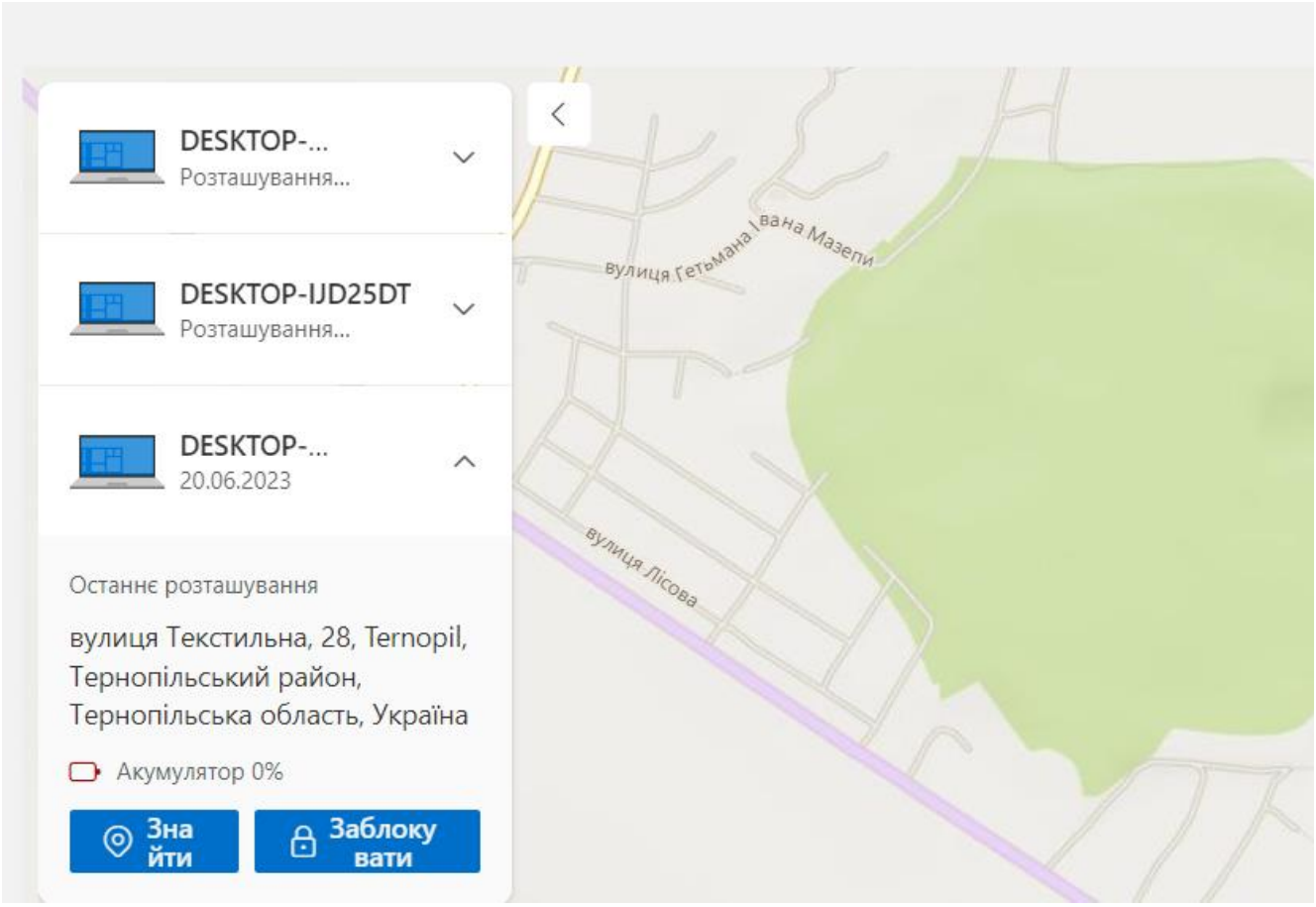


Рисунок 3.5 – Відстежування пристроїв компанії за допомогою служби розташування Windows

На всіх пристроях компанії встановлений Windoss 10. У випадку, якщо хтось викраде ноутбук, або ПК, то компанія може злегкістю відстежити його, та в разі необхідності віддалено заблокувати.

3.3.4 Блокування екрану

Блокування екрана на робочому місці, коли працівник відходить від ПК, є важливим заходом з точки зору безпеки та конфіденційності інформації див. (рис. 1.6).

Якщо працівник залишає ПК без блокування екрана, інші люди можуть отримати доступ до його робочої станції. Це може призвести до несанкціонованого використання його облікового запису, крадіжки конфіденційної інформації або пошкодження даних.Робоча станція може містити конфіденційну інформацію працвника, або інші важливі данні компанії, Блокування екрана допомагає захистити цю інформацію від небажаних поглядів.

Якщо працівник не блокує екран, інші люди можуть зловживати його обліковим записом або вносити не бажані зміни, що може призвести до проблем та помилок.

Рисунок 3.6 – Блокування екрану на Windows

Блокування екрана легке і швидке діло, але може мати значний вплив на безпеку робочого місця працівника та безпеку даних його компанії. Тому рекомендується завжди блокувати екран, коли працівник відходить від свого робочго місця, навіть якщо відсутність буде тривати лише на декілька хвилин.

3.3.5 Тренінги

Проведення тренінгів безпеки в інтернеті для працівників має декілька важливих причин:

– Свідомість про загрози: Тренінги безпеки в інтернеті допомагають працівникам усвідомити різноманітні загрози, з якими вони можуть стикатися в онлайн-середовищі. Це включає фішинг, шкідливі програми, соціальний інжиніринг та інші види кібератак. Знання про такі загрози допомагають працівникам розпізнавати підозрілі ситуації та уникати потенційно небезпечних дій.

– Захист від витоку даних: Тренінги безпеки наголошують на важливості захисту конфіденційної інформації та основних принципах керування даними. Вони надають працівникам настанови щодо використання сильних паролів, захисту віддаленого доступу, шифрування даних тощо. Це допомагає запобігти витоку важливих даних компанії і зберегти конфіденційність інформації.

– Безпека електронної пошти та соціальних мереж: Тренінги безпеки в інтернеті також охоплюють аспекти безпеки електронної пошти та соціальних мереж. Вони навчають працівників розпізнавати спам, фішингові повідомлення, шкідливі посилання та інші підступи, які можуть стати джерелом кібератак або порушити безпеку інформації.

– Захист компанії: Недбалість або необережність працівників можуть стати причиною кіберінцидентів, що мають серйозні наслідки для компанії. Проведення тренінгів безпеки допомагає зміцнити культуру безпеки в організації та зменшити ризик виникнення інцидентів, пов'язаних з кібербезпекою.

Див. (рис. 3.7)

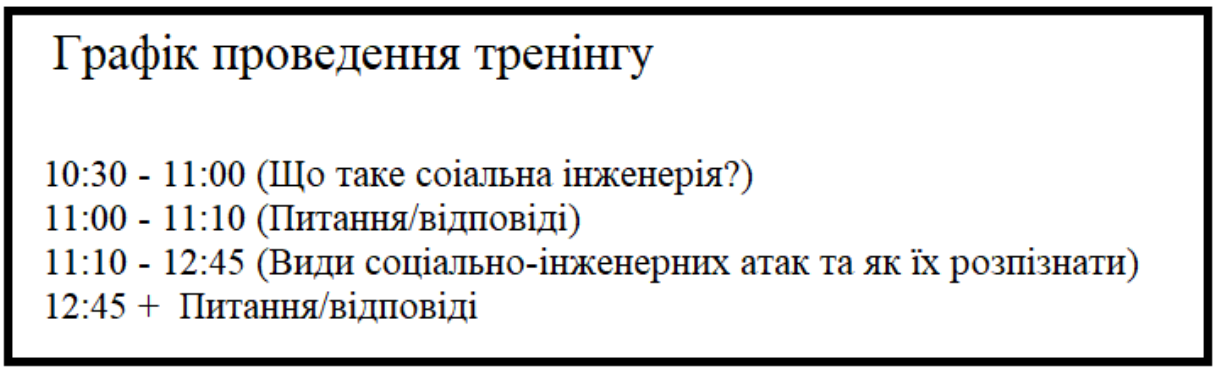


Рисунок 3.7 – Графік тренінгу “Соціальна інженерія, або як не стати жертвою шахраїв в інтернеті”

Завершальним етапом програми слід проводити отримання підписів співробітників про угоду слідування встановлених політик безпеки і принципів поведінки. Відповідальність, яку повинні будуть брати на себе співробітники, підписавши угоду, допоможе уникати сумнівів (тобто надходити як хто-небудь просить, або надходити як того вимагає політики безпеки).

Такі тренінги необхідно проводити як мінімум один раз на на рік для повторення всіх цих правил та навчанню нових співробітників.

3.3.6 Робота з електроною поштою

Було інтегровано програму PAB в електронну пошту співробітників. Коли співробітник отримує електронне повідомлення, він може використовувати Phish Alert Button, щоб позначити його як підозріле або потенційний фішинг. Зазвичай це здійснюється шляхом натискання на кнопку Phish Alert або аналогічного функціоналу див. (рис. 3.8).

Після натискання на Phish Alert Button, сповіщення про підозріле повідомлення надсилається адміністраторам або безпековій команді організації. Вони отримують повідомлення про підозрілу електронну пошту, яке було позначено співробітником.

Аналіз і реагування: Адміністратори або безпекова команда перевіряють позначене повідомлення та аналізують його, щоб визначити, чи насправді воно є фішинговим атакою чи іншим видом кіберзагрози. Якщо підтверджується фішинговий характер повідомлення, вживаються відповідні заходи безпеки, такі як блокування або сповіщення користувачів, і проводяться подальші розслідування.

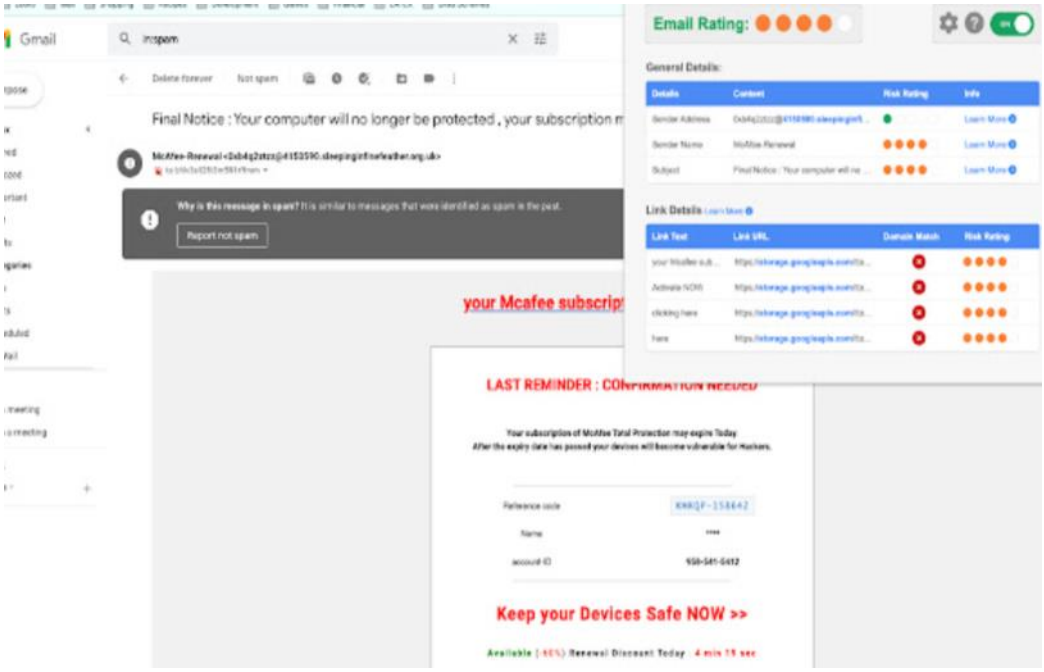


Рисунок 3.8 – Phish Alert Button

Phish Alert Button допомагає створити механізм швидкого виявлення та реагування на фішингові атаки. Це розширює безпеку організації та допомагає уникнути потенційних кіберзагроз.

3.3.7 Тетсування впровадженого комплексного методу

Після впровадження розробленого комплексного методу останнім кроком було визначення його ефективності. Протягом місяця 50-тьом співробітникам було надіслано фішингові атаки, Резльтати:0 співробітників повідомили про фішинг за допомогою Phish Alert Button, 2 клікнули на посилання і 38 проігнорували, або не відкрили лист, з чого було зроблено висновки в ефетивності розробленого комплексного методу захисту від соціально-інженерних атак

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при переломах

При дослідженні механізмів захисту від соціально-інженерних атак роботодавці та працівники зобов’язані не нехтувати основами охорони праці і технікою безпеки, та бути уважними, адже навіть працюючи за ПК є ризик через свою власну, або чужу неуважність отримати значну шкоду – переломи, порізи та інші травми.

Перелом – це ушкодження кістки з порушенням її цілісності. Травматичні переломи розділяють на відкриті (є ушкодження шкіри в зоні перелому) і закриті (шкірний покрив не порушений). При відкритому переломі травма не викликає сумнівів. Закритий перелом не такий очевидний, особливо, якщо він неповний, коли порушується частина поперечника кістки, частіше у вигляді тріщини [30].

Для усіх переломів характерні:

– різкий біль при будь-яких рухах і навантаженнях;

– зміні положення і форми кінцівки, її укорочення;

– порушення функцій кінцівки (неможливість звичних дій або ненормальна рухливість);

– набряклість і синець в зоні перелому.

Надання першої допомоги при переломах кінцівок багато в чому визначає результат травми: швидкість загоєння, попередження ряду ускладнень (кровотеча, зміщення відламків, шок) і переслідує три мети:

– створення нерухомості кісток в області перелому (що попереджає зміщення відламків і ушкодження їх краями посудин, нервів і м'язів);

– профілактику шоку;

– швидку доставку потерпілого до медичної установи.

Перша допомога при закритому переломі: насамперед якщо є можливість викликати швидку, то варто зробити це. Після чого необхідно забезпечити нерухомість пошкодженої кінцівки, поклавши її на щось м’яке і забезпечити

спокій. На передбачувану зону перелому покласти що-небудь холодне. Самому постраждалому можна дати випити гарячий чай або знеболювальний засіб.

Якщо немає можливості викликати швидку допомогу, а транспортувати потерпілого доведеться власноруч, то заздалегідь необхідно накласти шину з будь-яких підручних матеріалів (дошки, лижі, палиці, лозини, парасольки). Будь-які два тверді предмети прикладають до кінцівки з протилежних сторін поверх одягу і надійно, але не туго (щоб не порушувати кровообіг) фіксуються бинтом або іншими відповідними підручними матеріалами (пояс, ремінь, стрічка, мотузок). Фіксувати потрібно два суглоби - вище і нижче місця перелому. При переломі гомілки фіксуються гомілковостопний і колінний суглоби, а при переломі стегна - усі суглоби ноги. Якщо під рукою зовсім нічого не виявилось, пошкоджену кінцівку слід прибинтовувати до здорової (руку - до тулуба, ногу - до другої ноги). Транспортування потерпілого з переломом ноги здійснюється в положенні лежачи.

Перша допомога при відкритому переломі: Відкритий перелом небезпечніший за закритий, оскільки є можливість інфікування. Якщо є кровотеча, її потрібно зупинити. Якщо кровотеча незначна, то досить накласти пов'язку, що давить. При сильній кровотечі накладаємо джгут, не забуваючи відмітити час його накладення. Якщо час транспортування займає більше 1,5-2 годин, то кожні 30 хвилин джгут необхідно послабляти на 3-5 хвилин. Шкіру навколо рани необхідно обробити антисептичним засобом. У разі його відсутності рану потрібно закрити бавовняною тканиною. Після чого слід накласти шину, так само як і у разі закритого перелому, але уникаючи місця, де виступають назовні кісткові уламки і доставити потерпілого до медичної установи [30].

4.2 Правила запобігання та безпеки при короткому замиканні

Сьогодні майже неможливо уявити повсякденне життя без електричної енергії. Електрика стала настільки звичною, що іноді ми забуваємо, що користуватися нею потрібно вкрай обережно, щоб уникнути небезпеки ураження електричним струмом та виникнення пожежі.

Однією з основних причин виникнення пожеж є порушення правил пожежної безпеки при влаштуванні та експлуатації електроустановок. Джерелом запалювання при порушенні правил пожежної безпеки при влаштуванні та експлуатації електроустановок є коротке замикання, перевантаження та великі перехідні опори. Серед причин виникнення пожеж, які пов'язані з електромережами, найбільш розповсюдженими є [31]:

– коротке замикання. Воно виникає при надмірних чи тривалих перевантаженнях або через механічне пошкодження ізоляції між дротами. При цьому різко збільшується сила струму і кількість теплоти, що призводить до загоряння ізоляції і горючих предметів, що знаходяться поруч від розплавлених частинок металу дроту, які розлітаються довкола;

– поганий контакт, який виникає через послаблення або окиснення контакту і призводить до ослаблення сили струму. Запобіжники в такому випадку не спрацьовують. Через це виникає місцевий перегрів, який може призвести до пожежі;

– перевантаження мережі, коли в неї підключають електроприлади з більшою загальною потужністю, ніж та, на яку розраховано мережу. Тривалі перевантаження призводять до руйнування ізоляції.

У більшості випадків пожежам можна й необхідно запобігти. Тому під час користування електроенергією в побуті, або в офісах потрібно дотримуватися наступних правил [31]:

– захист від коротких замикань. Для цього автомати та пробкові запобіжники повинні бути справними і заводського виготовлення;

– необхідно слідкувати за станом ізоляції електропроводів електроприладів, забезпечуючи їхній своєчасний ремонт;

– не використовувати в побуті саморобні електроприлади;

– виключити можливість доступу дітей до електроприладів та відкритих розеток;

– бути обережним при користуванні електроенергією у вологих приміщеннях та у приміщеннях із земляною, цегляною і бетонною підлогою;

– електронагрівальні прилади, телевізори, побутові електроприлади та апаратура повинні вмикатися в електромережу тільки за допомогою справних штепсельних з'єднань та електророзеток заводського виготовлення;

– відстань від приладів електроопалення до горючих матеріалів та будівельних конструкцій має становити не менше 0,25 м.

Під час користування електрикою забороняється[32]:

– прокладати електричні проводи і кабелі транзитом через пожежовибухонебезпечні зони;

– експлуатувати кабелі і проводи з ізоляцією, що пошкоджена або втратила в процесі експлуатації захисні властивості;

– залишати без нагляду кабелі та проводи з неізольованими струмопровідними частинами;

– застосовувати саморобні подовжувачі;

– застосовувати для опалення приміщення нестандартне (саморобне) електронагрівальне обладнання або лампи розжарювання;

– користуватися пошкодженими розетками, вимикачами та іншими електровиробами;

– залишати без догляду увімкнені в електромережу нагрівальні прилади, телевізори тощо;

– використовувати вимикачі, штепсельні розетки для підвішування одягу та інших предметів, заклеювати ділянки електропроводки папером чи тканиною;

– застосовувати для електромереж радіо- та телефонні проводи.

– використовувати побутові електронагрівальні прилади (праски, чайники) без негорючих підставок.

Для гасіння електроприладів, які перебувають під напругою, можна використовувати тільки пісок, вуглекислотні та порошкові вогнегасники. Ці вогнегасники застосовують для гасіння електроустановок та електрообладнання, що перебуває під напругою до 1000 В, з відстані не менше 1 м. Непридатними для гасіння електрообладнання під напругою є водяні та водопінні вогнегасники.

Компанії обов’язково мусять потурбуватись про облаштування аварійних виходів. Кількість та вимоги стосовно облаштування аварійних виходів з будівель на вулицю зобов’язані відповідати вимогам ДБН В.1.1-7-2002 «Пожежна безпека об’єктів будівництва», ДБН В.2.2-9-2009 «Громадські будинки та споруди», ДБН В.2.2-28:2010 «Будинки адміністративного та побутового призначення», ДБН В.2.2-16-2005 «Культурно-видовищні та дозвіллєві заклади» та іншим будівельним стандартам залежно від виду приміщення [32]:

– у приміщенні, яке обладнано одним аварійним виходом, дозволяється одночасно розміщувати не більше 50 людей;

– двері на маршруті евакуації повинні відчинятися в напрямку виходу з будівлі. За наявності людей у приміщенні двері аварійних виходів можуть замикатися лише на внутрішні замки, які відкриваються без ключа;

– килими й інше подібне покриття підлоги у приміщеннях з одночасним перебуванням понад 50 осіб повинні міцно кріпитися до підлоги, щоб запобігти їх скручуванню;

– сходові марші і площадки повинні мати справні огорожі із поручнями, котрі не повинні зменшувати ширину сходових маршів і площадок;

– маршрут до аварійного виходу має бути забезпечений евакуаційним освітленням. Світлові покажчики «Вихід» необхідно постійно утримувати справними. У залах для глядачів, виставкових, актових залах та інших подібних приміщеннях вони мають бути увімкнуті на весь час перебування людей (проведення заходу).

При дослідженні методів захисту від соціальної інженерії працівники зобов’язані ознайомитись з правилами техніки безпеки та неухильно дотримуватись їх.

ВИСНОВКИ

У ході дослідження було проведено огляд літератури з питань соціально-інженерних атак та існуючих методів їх виявлення.

Були визначені основні типи соціально-інженерних атак та їх характеристики, а також виявлено поточні методи та механізми захисту.

Було проведено аналіз існуючих методів виявлення соціально-інженерних атак. Вимоги до алгоритмів виявлення були визначені, такі як оптимальність, ефективність, здатність до виявлення нових атак та мінімізація помилкових спрацювань. Було запропоновано алгоритм дій для боротьби з соціальною інженерією.

Було розроблено, впроваджено та протестовано коплексний метод захисту від соціально-інженерних атак в Х-компанії

Дослідження механізмів захисту від соціально-інженерних атак та розробка алгоритмів їх виявлення є актуальними і важливими завданнями у сфері кібербезпеки. Для подальшого розвитку даної теми рекомендується дослідження нових методів та алгоритмів, а також використання більш розширених наборів даних, для алгоритмів машинного навчання.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Епізод 44 подкасту Social-Engineer. Розмова з доктором Заком за посиланням: www.social-engineer.org/podcast/ep-044-do-you-trust-me/

2. Стаття Social Engineering Attacks Prevention: A Systematic Literature Review. Veni Syafitri & Zarina Shukur & Umi Astma Mokhtar & Rossilaviti Suleiman & Muhammed Azwan Ibrahim.

3. Verizon's 2021 Data Breach Investigation Report. За посиланням: https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

4. Check Point Cyber Attack Trends: (2020). Mid-Year Report. За посиланням: https://www.antivirus.cz/Blog/Documents/Check-Point-Cyber-Attack-Trends-2020-Mid-Year-Report.pdf

5. Стаття OnlineUA: Кібератака на DNC 2016. За посиланням: https://novyny.online.ua/u-rosiyskiy-kiberatatsi-na-partiyu-obami-pobachili-zagrozliviy-signal_n744871/

6. Стаття ESET: Фішинг. За посиланням: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/

7. Стаття NV Бізнес: Фішинг і соціальна інженерія: пастки для бізнесу і як їх обійти. За посиланням: https://biz.nv.ua/ukr/kibervoiny_i_biznes/fishing-i-sotsialna-inzhenerija-pastki-dlja-biznesu-i-jak-jih-obijti-1930358.html

8. Стаття Crowdstrike: Що таке претестинг? За посиланням: https://www.crowdstrike.com/cybersecurity-101/pretexting/

9. Стаття Meilfence: Соціальна інженерія: атаки Quid Pro Quo. За посиланням: https://blog.mailfence.com/quid-pro-quo-attacks/

10. Стаття Powerdmark: What is a Baiting Attack, and How to Prevent it? За посиланням: https://powerdmarc.com/what-is-a-baiting-attack/?nonitro=1

11. Стаття Meilfence: Social Engineering: What is Tailgating? За посиланням: https://blog.mailfence.com/what-is-tailgating/

12. Стаття Red GOAD: What is Vishing? За посиланням: https://red-goat.com/what-is-vishing/

13. Стаття Wikipedia: IVR-Architecture. За посиланням: https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:IVR-Architecture_ru.png

14. Стаття Wikipedia: Intrusion detection system. За посиланням: https://en.wikipedia.org/wiki/Intrusion_detection_system

15. Стаття OmniSecu.com: Types of Intrusion Detection Systems (IDS). За посиланням: https://www.omnisecu.com/security/infrastructure-and-email-security/types-of-intrusion-detection-systems.php

16. Стаття Wikipedia: Anomaly-based intrusion detection system. За посиланням: https://en.wikipedia.org/wiki/Anomaly-based_intrusion_detection_system

17. Стаття SANS: Cyber Security Training, Certifications, Degrees and Resources.За посиланням: https://www.sans.org/emea/

18. Збірник тез доповідей ІІІ Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів Ст. 50-52.

19. Метод захисту даних наукових дослідженьвід атак за допомогою алгоритмів соціальноїінженерії. За посиланням: https://doi.org/10.36059/978-966-397-267-1/30

20. Kevin Mitnick (2005) Art of Intrusion C: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers, 1st edn., New Jersey, US: John Wiley & Sons.

21. Charles A. Shoniregun (2014) Impacts and Risk Assessment of Technology for Internet Security (Advances in Information Security), 1st edn., New York, US: Springer

22. The Chromium Projects (Unknown) Sandbox FAQ (Accessed: 11th July 2016)

23. Mozilla Wiki (Unknown) Security/Sandbox (Accessed: 11th July 2016).

24. Long Lu, Vinod Yegneswaran, Phillip Porras, Wenke Lee (2019) BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections

25. Gianluca Stringhini, Olivier Thonnard (2020) That Ain’t You: Blocking Spearphishing Through Behavioral Modelling, Available

at:http://www0.cs.ucl.ac.uk/staff/G.Stringhini/papers/spearphishing-dimva2021.pdf(Accessed: 11th July 2021).

26. Ryan Heartfield, George Loukas (2015) 'A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks', ACM Computing Surveys, 48(3), Article 37.

27. Navigant (2019) Cyber Security Trends for 2019 – Part 1, Available at:http://www.navigant.com/insights/hot-topics/technology-solutions-experts-corner/cyber-security-trends-2019-part-1/ (Accessed: 12th August 2020).

28. TOM MENDELSOHN (2020) More than half of UK firms have been hit by ransomware—report, Available at: http://arstechnica.co.uk/security/2016/08/more-than-half-of-uk-firms-have- been-hit-by-ransomware-report/ (Accessed: 12th August 2020).

29. Art Kohn (2020) Brain Science: The Forgetting Curve–the Dirty Secret of Corporate Training, Available at: http://www.learningsolutionsmag.com/articles/1379/brain-science-theforgetting curvethe-dirty-secret-of-corporate-training (Accessed: 13th August 2020).

30. David Gragg (2002) A Multi-Level Defense Against Social Engineering, Available at:https://www.sans.org/readingroom/whitepapers/engineering/multi-level-defense-social-engineering- 920 (Accessed: 15th August 2016

31. Kate Palmer, Cara McGoogan (2016) TalkTalk loses 101,000 customers after hack, Available at: http://www.telegraph.co.uk/technology/2016/02/02/talktalkloses-101000-customers-after-hack/ (Accessed: 17th August 2016)

32. Стаття СОП: Вимоги пожежної безпеки для приміщень різного призначення. За посиланням: https://pro-op.com.ua/article/391-vimogi-pozhezhnoi-bezpeki-dlya-primishchen-riznogo-priznachennya

33. Стаття geeksforgeeks: Intrusion Detection System (IDS). За посиланням: https://www.geeksforgeeks.org/intrusion-detection-system-ids/