ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЇ ПРОТИДІЇ СОЦІАЛЬНОМУ ІНЖИНІРИНГУ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В УМОВАХ ДИСТАНЦІЙНОЇ РОБОТИ СПІВРОБІТНИКІВ»

Виконав студент 6 курсу, групи БСЗМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Гуляєва О.І.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2021 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Гуляєвій Оксані Ігорівні
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технології протидії соціальному інжинірингу на об'єктах інформаційної діяльності в умовах дистанційної роботи співробітників»

керівник магістерської роботи Гайдур Галина Іванівна, д.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «11» жовтня 2021 року № 170.

2. Строк подання студентом магістерської роботи 15.12.2021 р.

3. Вихідні дані до магістерської роботи
об'єкти інформаційної діяльності;
програмні комплекси для протидії атакам соціальної інженерії;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Огляд сутності соціоінженерного підходу.
2. Аналіз методів та засобів протидії соціальному інжинірингу на об'єктах інформаційної діяльності в умовах дистанційної роботи співробітників.
3. Розроблення варіанта технології протидії соціальному інжинірингу на об'єктах інформаційної діяльності на базі Sophos Phish Threat.

5. Перелік графічного матеріалу
1. Тема магістерської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу сутності соціоінженерного підходу.

4. Результати аналізу методів та засобів протидії соціальному інжинірингу.

5. Призначення та можливості рішення Sophos Phish Threat.

6. Симуляція фішингової атаки на об’єкті інформаційної діяльності в умовах дистанційної роботи співробітників на базі Sophos Phish Threat

7. Аналіз результатів атаки

8. Рекомендації щодо застосування технології протидії соціальному інжинірингу на об’єктах інформаційної діяльності на базі Sophos Phish Threat

9. Висновки за результатами роботи.

6. Дата видачі завдання 27.09.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми протидії соціальному інжинірингу на об’єктах інформаційної діяльності в умовах дистанційної роботи співробітників.	27.09.2021 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	11.10.2021 р.	
3.	Аналіз методів та засобів протидії соціальному інжинірингу.	25.10.2021 р.	
4.	Проведення симуляції фішингової атаки на об’єкті інформаційної діяльності в умовах дистанційної роботи співробітників на базі Sophos Phish Threat	08.11.2021 р.	
5.	Розроблення рекомендацій щодо застосування технології протидії соціальному інжинірингу на об’єктах інформаційної діяльності	01.12.2021 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	10.12.2021 р.	
7.	Підготовка доповіді до захисту.	15.12.2021 р.	

Студент _____ Гуляєва О.І.
(підпис) прізвище та ініціали

Керівник магістерської роботи _____ Гайдур Г.І.
(підпис) прізвище та ініціали

РЕФЕРАТ

Текстова частина магістерської роботи: 60 сторінок, 16 рисунків, 16 джерел.

Об'єкт дослідження – процес забезпечення протидії атакам соціальної інженерії на об'єктах інформаційної діяльності в умовах дистанційної роботи співробітників.

Предмет дослідження – технологія протидії атакам соціальної інженерії на об'єктах інформаційної діяльності.

Мета роботи – розробити рекомендації щодо застосування технології протидії соціальному інжинірингу на об'єктах інформаційної діяльності в умовах дистанційної роботи співробітників.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, симуляція фішингової атаки на об'єкті інформаційної діяльності та аналіз її результатів.

В роботі проведено аналіз проблеми протидії соціальному інжинірингу на об'єктах інформаційної діяльності в умовах дистанційної роботи співробітників. Проаналізована сутність соціоінженерного підходу, існуючі форми та методи соціальної інженерії на об'єктах інформаційної діяльності.

Досліджено методи та засоби протидії соціальному інжинірингу на об'єктах інформаційної діяльності в умовах дистанційної роботи співробітників. Визначено призначення, основні функції та склад програмного комплексу Sophos Phish Threat.

На основі досліджень проведених в роботі, розроблено рекомендації щодо застосування технології протидії соціальному інжинірингу на об'єктах інформаційної діяльності в умовах дистанційної роботи співробітників.

Галузь використання – кібербезпека на об'єктах інформаційної діяльності.

СОЦІАЛЬНА ІНЖЕНЕРІЯ, ЛЮДСЬКИЙ ЧИННИК, АТАКА, МЕТОДИ, ЗАХИСТУ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ, ТИПИ АТАК, ФІШИНГ, КОРИСТУВАЧІ, ВПЛИВ, ПОЛІТИКИ БЕЗПЕКИ, ЗАХИСТ ВІД ЗАГРОЗ.

ABSTRACT

Master's thesis: 60 pages, 16 figures, 16 sources.

Object of research – the process of counteracting attacks of social engineering on the objects of information activities in the conditions of remote work of employees.

Subject of research – technology of counteraction to attacks of social engineering on objects of information activity

The aim of research – develop recommendations for the application of technology of counteracting social engineering at the objects of information activities in the conditions of remote work of employees.

Research methods – elaboration of literature on this topic, analysis of operational documentation, international standards and their comparison, simulation of phishing attacks on the object of information activities and analysis of its results.

The analysis of the problem of counteraction to social engineering at the objects of information activity in the conditions of remote work of employees is carried out in the work. The essence of the socio-engineering approach, the existing forms and methods of social engineering at the objects of information activity are analyzed.
Methods and means of counteracting social engineering at the objects of information activity in the conditions of remote work of employees are investigated. The purpose, main functions and composition of the Sophos Phish Threat software package have been determined.

Based on the research conducted in the work, recommendations for the use of technology to combat social engineering at the objects of information activities in the conditions of remote work of employees.

Field of use – cybersecurity on the object of information activities.

SOCIAL ENGINEERING, HUMAN FACTOR, ATTACK, METHODS OF PROTECTION AGAINST ATTACKS OF SOCIAL ENGINEERING, TYPES OF ATTACKS, FISHING, USERS, INFLUENCE, SECURITY POLICIES, THREAT PROTECTION.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …….. 10

ВСТУП ……..……. 11

1 ОГЛЯД СУТНОСТІ СОЦІОІНЖЕНЕРНОГО ПІДХОДУ ……... 13

1.1. Поняття соціального інжинірингу …… 13
1.2. Форми та методи соціальної інженерії на об’єктах інформаційної діяльності …… 17
1.3. Аналіз статистичних даних щодо кіберінцидентів методом соціальної інженерії …….. 32
1.4. Вимоги нормативних документів з протидії методам соціальної інженерії ……. 35

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ПРОТИДІЇ СОЦІАЛЬНОМУ ІНЖИНІРИНГУ НА ОБ’ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В УМОВАХ ДИСТАНЦІЙНОЇ РОБОТИ СПІВРОБІТНИКІВ …… 40

2.1. Метод протидії соціальному інжинірингу шляхом профілактики та зменшення негативного впливу атак …… 40
2.2. Тестування на проникнення за соціоінженерним підходом з використанням утиліти Social-Engineer Toolkit …….. 47
2.3. Метод моделювання дій об’єкта та суб’єкта соціоінженерного впливу ……. 52
2.4. Метод виявлення і повідомлення про атаки соціальної інженерії людиною за допомогою інструментального засобу Cogni-Sense ... 54

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ПРОТИДІЇ СОЦІАЛЬНОМУ ІНЖИНИРІНГУ НА ОБ’ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ НА БАЗІ SOPHOS PHISH THREAT …….. 56

3.1. Технологія управління утилітою Sophos Phish Threat та проведення на її базі симуляції фішингової атаки на об’єкті інформаційної діяльності в умовах дистанційної роботи співробітників …… 56
3.2. Аналіз результатів атаки …… 63

3.3. Розроблення рекомендацій щодо застосування технології протидії соціальному інжинірингу на об’єктах інформаційної діяльності використовуючи інструменти утиліти Sophos Phish Threat ……...…… 64

ВИСНОВКИ …… 70

ПЕРЕЛІК ПОСИЛАНЬ ……. 71

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) ……. 73

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ДСТУ	Державний стандарт України
ВООЗ	Всесвітня організація охорони здоров'я
ПЗ	Програмне забезпечення
ПК	Персональний комп'ютер
СІ	Соціальна інженерія; Соціальний інженер
APWG	Anti-Phishing Working Group
IEC	International Electrotechnical Commission;
ISO	International Organization for Standardization
IT	Information Technologies
SaaS	Software as a Service
SSL	Secure Sockets Layer
PwC	PricewaterhouseCoopers
KPMG	Klynveld Peat Marwick Goerdeler
URL	Uniform Resource Locator
НТК	Науково-технічна конференція
КСЗІ	Комплексна система захисту інформації
SMS	Short Message Service
RFID	Radio Frequency IDentification
BDO	Binder Dijker Otte
USAID	United States Agency for International Development

ВСТУП

Актуальність дослідження. Локдауни, заборони та обмеження, встановлені урядами у зв'язку з пандемією COVID-19, змусили багато компаній перевести робітників на дистанційну роботу, що спровокувало миттєве зростання ризиків для бізнесу. Із пандемією коронавірусу у 2,5 рази збільшилась кількість атак на робітників, які працюють дистанційно.

У PwC зазначають, що карантинні обмеження призвели до того, що навіть деякі спеціалізовані команди із захисту даних не були готові до нових умов. Процеси та процедури, що ефективно працювали раніше, стали недоступними або неефективними.

Загроза такого потужного вірусу сама по собі стала хорошою приманкою для фішингу, повідомляє KPMG: у листах, де нібито надавали інформацію про пандемію, насправді виманювали дані та паролі користувачів. Кіберзлодії використовували заражені документи Microsoft, надсилаючи їх під виглядом листів від міністерства охорони здоров'я чи ВООЗ.

Вищезгадані факти вкотре переконують, що однією з найслабших ланок у системах кіберзахисту є люди. Підвищена обізнаність може бути потужною протидією. Щоб захиститися від атак соціальної інженерії, варто навчати працівників вживати заходів безпеки, особливо якщо в компанії дозволена робота з власних девайсів.

Об'єкт дослідження – процес забезпечення протидії атакам соціальної інженерії на об'єктах інформаційної діяльності в умовах дистанційної роботи співробітників.

Предмет дослідження – технологія протидії атакам соціальної інженерії на об'єктах інформаційної діяльності.

Мета роботи – розробити рекомендації щодо застосування технології протидії соціальному інжинірингу на об'єктах інформаційної діяльності в умовах дистанційної роботи співробітників.

Наукові завдання:

теоретично дослідити способи та методи захисту від атак соціальної інженерії на об’єктах інформаційної діяльності;

провести симуляцію фішингової атаки на об’єкті інформаційної діяльності;

проаналізувати основні уразливості підприємства до атак соціальної інженерії;

розробити рекомендації щодо застосування технології протидії соціальному інжинірингу на об’єктах інформаційної діяльності в умовах дистанційної роботи співробітників.

Галузь застосування – кібербезпека на об’єктах інформаційної діяльності.

Практичне значення одержаних результатів полягає у розробці рекомендацій щодо впровадження технологій протидії соціальному інжинірингу на об’єктах інформаційної діяльності в умовах дистанційної роботи співробітників.

Апробація результатів дипломної роботи. Основні наукові результати були представлені на:

IX Всеукраїнській студентській науковій Інтернет-конференції «Сучасні інформаційні технології в освіті і науці» (м. Умань, 2018, Уманський державний педагогічний університет ім. Павла Тичини);

Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки» (м. Київ, 2020, Державний університет телекомунікацій)

Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки» (м. Київ, 2021, Державний університет телекомунікацій)

Публікації. Основні наукові результати відображені у тезах доповіді на НТК.

1 ОГЛЯД СУТНОСТІ СОЦІОІНЖЕНЕРНОГО ПІДХОДУ

1.1. Поняття соціального інжинірингу

Соціальна інженерія – це низка не технічних прийомів маніпулювання користувачами, які використовуються кіберзлочинцями під час атак [1].

Соціальний інжиніринг заснований на початковому прагненні людей надати допомогу іншим. Це найменш технічний, але й найбільш ефективний засіб в арсеналі зловмисників.

Вперше, поняття «хакер» і «соціальна інженерія» ввів Кевін Митник. Він вважав, що в той час, поки розробники безперервно винаходять все досконаліші технології захисту, унеможливлюючи використання технічних вразливостей, кіберзлочинці все частіше використовують людський чинник[2].

За останні 2 роки у світі відбулося багато подій (чого вартує Covid-19 і практика дистанційної роботи), які відкрили неабиякі можливості для соціальних інженерів. Будь-яка гучна новина чи подія у світі генерує у соціальних інженерів масу ідей. Якщо тема «у тренді», то тим простіше буде отримати інформацію від жертви шляхом фішингу та подальшого злому.

Інформаційні ресурси окремих організацій і фізичних осіб являють собою певну цінність, мають матеріальне вираження і вимагають захисту від різноманітних загроз. Тому захист інформації в корпоративних інформаційних системах полягає в створенні та підтриманні в дієздатному стані комплексної системи захисту інформації (КСЗІ), а також зменшення потенційних збитків. Оскільки КСЗІ включає обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію, то на оцінювання технічної захищеності інформації суттєво впливає врахування нетехнічного аспекту, зокрема, персоналу (рис. 1.1).

Комплексною, система забезпечення інформаційної безпеки, буде тільки тоді, коли крім технічних методів захисту інформації буде проведене серйозне навчання співробітників, застосовані політики безпеки і технології протидії соціальним інженерам.

Тому, так важливо для підприємства вкладати час і гроші у підготовку, навчання і тестування цього життєво важливого компонента безпеки.

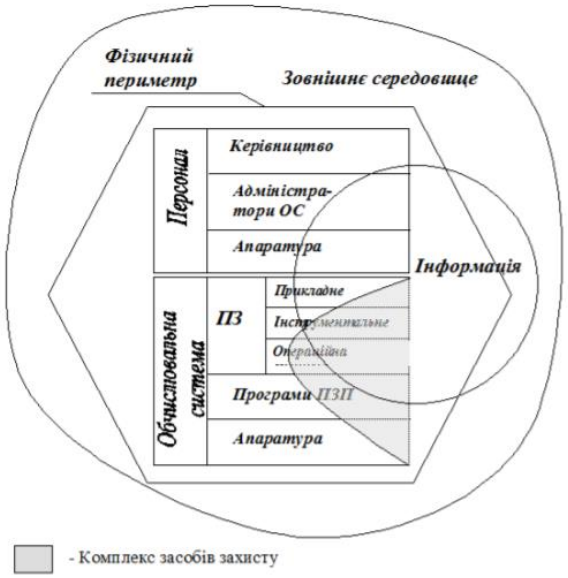


Рис. 1.1. Елементи комп’ютерної системи

Багато співробітників організацій не знають про загрози, пов'язані з соціальним інжинірингом. Вони отримали доступ до інформації, не розбираючись в деталях роботи, і не усвідомлюючи важливості оброблюваної інформації. Соціальний інженер, часто, вибирає собі жертву з числа співробітників з низьким рівнем володіння комп'ютером [3, с. 13].

Основні сфери застосування соціального інжинірингу [4]:

підрив репутації підприємства з подальшим його руйнуванням;

фінансові махінації на підприємстві;

доступ до персональних банківських даних приватних осіб з метою крадіжки коштів;

розкрадання клієнтських баз даних;

розвідка сильних і слабких сторін організації з метою подальшого її знищення;

розвідка інформації про маркетингові плани організації

розвідка інформації про найбільш перспективних співробітників з метою їх подальшого «переманювання» в свою організацію.

Використання соціоінженерного підходу передбачає цілеспрямований вплив на свідомість (підсвідомість) персоналу проти волі, але за його згодою (рис 1.2.). Такий вплив дозволяє управляти поведінкою керівництва, адміністратора, користувачів через слабкості, інтереси, потреби, схильності, переконання, звички, психічний та емоційний стан. Маніпулювання цими вразливостями і виражається в таких формах як шахрайство, обман, афера, інтрига, містифікація, провокація. Разом з тим, використанню кожної з означених форм маніпулювання передує визначення їх сутності шляхом ретельних планування, організації та контролювання.

Рис. 1.2. Використання соціоінженерного підходу

У рамках соціоінженерного підходу використання атак соціальної інженерії орієнтоване на отримання “несанкціонового” доступу до інформації при оцінюванні її захищеності шляхом “негативного” інформаційно-психологічного впливу на свідомість або підсвідомість персоналу (рис 1.3.).

Соціальні інженери використовують багато тонкощів при атаці. Серед них:

людські почуття – виклик співчуття у співрозмовника;

професійний жаргон - співробітники довіряють тим, хто знає професійний жаргон, внутрішню форму спілкування їх організації, яка прихована від сторонніх очей;

знання термінології - соціальний хакер повинен орієнтуватися в термінології;

знання посад і повноважень співробітників - хто з працівників компанії має доступ до інформації, яка його цікавить, хто в якому підрозділі працює, де

розташовані підрозділи, яке програмне забезпечення встановлено на корпоративних комп`ютерах.

Особливості атак з використанням людського фактору:

не вимагають значних витрат;

не вимагають спеціальних знань;

можуть тривати протягом тривалого терміну;

важко відслідковуються.

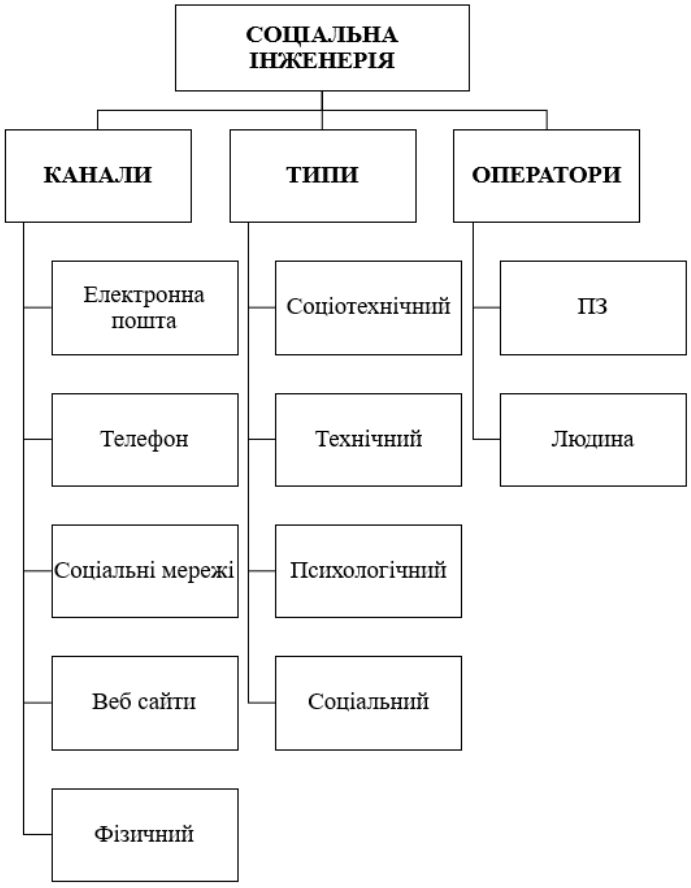


Рис. 1.3. Класифікація ознак реалізації атак соціальної інженерії

Реалізація атаки соціальної інженерії:

визначення мети впливу на об`єкт;

збір інформації про об`єкт;

виявлення найбільш зручної мішені впливу;

створення необхідних умов для впливу;

примус до виконання потрібної дії;

досягнення потрібного результату.

1.2. Форми та методи соціальної інженерії на об’єктах інформаційної діяльності

В умовах пандемії Covid-19, коли користувачі підключаються до корпоративних мереж вдома (в дорозі або громадських місцях), атаки соціальної інженерії є серйозною загрозою для компаній. Організація безпеки систем співробітників, які працюють вдома, у більшості випадків, обмежується технічними засобами. Політика безпеки повинна вимагати, щоб домашні системи даних працівників були захищені брандмауерами (міжмережевими екранами), які блокуватимуть спроби зловмисників отримати доступ по мережі ззовні.

Важливо відзначити, що в умовах дистанційної роботи всі комунікації між співробітниками відбуваються шляхом телефонних розмов, використання різноманітних месенджерів (Telegram, Viber, What’s App, Skype) та програм для організації відеоконференцій (Zoom, Google Meet), що збільшує шанси соціального інженера здійснити вдалу атаку.

Методи соціальної інженерії можна поділити на дві групи[5]:

1. *Віддалена соціальна інженерія* реалізується шляхом використання:

«Телефону». Завдяки телефонії, соціальний інженер може залишатися анонімним і в той же час мати прямий зв’язок з об’єктом впливу. Останнє важливо тому, що безпосередній контакт не дає співрозмовнику часу обміркувати поведінку у вірогідних ситуаціях, зважати на всі за та проти. Вирішувати необхідно швидко, до того ж під тиском соціального інженера. Оскільки під час телефонної розмови відбувається обмін тільки звуковою інформацією, то велику роль у прийнятті рішень відіграє інтонація і голос співрозмовника. Дані характеристики підбираються у відповідності з моделлю поведінки соціального інженера для отримання інформації про об’єкт впливу, наприклад:

а) керівник – людина, яка звикла віддавати команди, цінує свій час, досягає поставленої мети. Манера розмови жорстка, нетерпляча. Повна впевненість у собі і легка (або повна) зверхність до персоналу. Своїм тоном показує, що проблема, з якою звернувся – дрібниця, яку необхідно вирішити якомога швидше. Ніяких

прохань – тільки вимоги і вказівки. У відповідь на недовірливі або перевіряючі репліки – допустиме незадоволення і залякування співрозмовника;

б) адміністратор офісу або помічник керівника – дівчина (здебільшого) з приємним голосом. Завдання – виконати конкретне доручення керівника, не відволікаючись на умовності. Вона володіє інформацією про керівника, його справи, у своїй мові користується достовірними або недостовірними фактами, які складно перевірити. Характер розмови – м'який, з легким фліртуванням (якщо співрозмовник – чоловік). Реакція на небажання співпрацювати – бурхливе розчарування, скарга, що скаже керівнику;

в) технічний співробітник – працівник підприємства, який характеризується дружелюбним відношенням до співробітників. Його намір – усунути несправність. Супроводжується використанням технічної термінології для відображення своєї компетентності. На відмову співпрацювати – реакція здивування, оскільки співпраця у першу чергу вигідна для співробітника. Не використовується жодних вмовлять тому, що йому дається зрозуміти, що без його участі проблема тільки ускладнюється. Допустиме залякування тяжкими наслідками.

г) звичайний співробітник компанії – працівник, що виконує свої обов'язки і наляканий виникненням неочікуваної проблеми. Чітко виражений мотив швидкого вирішення усіх проблем і повернення до своєї рутинної роботи. Відсутність уявлення про характер проблеми, зацікавленість тільки в її вирішенні. Характер спілкування – показати безнадійність свого положення і готовність віддатися у руки спеціалісту.

«Глобальної мережі Інтернет». Найбільш розповсюдженими способами реалізації методів соціальної інженерії з її допомогою є:

а) листування електронною поштою;

б) листування через месенджери (Skype, Viber, Telegram, What's App);

Станом на сьогодні у месенджерах таке явище, як атаки соціальної інженерії на власників каналів, стало набагато частішим. Атакуючі намагаються заволодіти обліковими записами адміністраторів, розсилаючи їм заражені файли під виглядом рекламної презентації. Шкідливий файл найчастіше має таке розширення: «.scr»,

«.com», рідше – «.doc». І має назву на зразок «умови_співпраці» або «проморолик»[6].

в) обмін повідомленнями на форумах, чатах та блогах. У даних випадках вдала реалізація соціальної інженерії обумовлена правильністю розроблення сценарію спілкування;

г) спілкування через програми для організації відеоконференцій (Zoom, Google Meet). Дуже популярний метод спілкування між співробітниками в умовах дистанційної роботи.

2. *Особистий контакт.* Найбільш складний і небезпечний метод соціальної інженерії. Крім перерахованих вимог до сценарію спілкування і моделі поведінки, соціальний інженер повинен приділяти увагу своїй зовнішності і манерам «живого» спілкування. Для правильного візуального сприйняття, необхідно правильно підібрати:

колір одягу та взуття;

манери та жести при спілкуванні;

положення в просторі відносно співрозмовника.

Сьогодні цей метод полегшується для хакерів через сприятливі умови, які створила пандемія, а саме це носіння захисної медичної маски та дотримання дистанції між людьми.

Проаналізувавши різні існуючі класифікації атак соціальної інженерії, ми також можемо класифікувати ці атаки на дві основні категорії: прямі та непрямі.

Атаки, віднесені до першої категорії, використовують прямі контакти між зловмисником і жертвою, щоб здійснити напад. Вони стосуються нападів, що здійснюються через фізичний контакт, зоровий контакт або голосову взаємодію. Вони також можуть вимагати присутності нападника біля жертви для виконання нападу. Прикладами таких атак є: physical access (фізичний доступ), shoulder surfing (серфінг через плече), dumpster diving (аналіз смітників), phone social engineering (телефонна соціальна інженерія), pretexting (попередньо підготовлені атаки), impersonation on help desk calls (видавання себе за працівника

служби підтримки), and stealing important documents (крадіжка важливих документів).

Атаки, віднесені до категорії непрямих, не вимагають присутності зловмисника для запуску нападу. Атаку можна запустити дистанційно через шкідливе програмне забезпечення, яке передається у вкладеннях електронної пошти або SMS повідомленнях. Прикладами таких атак є: phishing (фішинг), fake software (підроблене ПЗ), Pop-Up windows (спливаючі вікна), ransomware (програми вимагачі), SMSishing (фішинг через СМС повідомлення), online social engineering (онлайн соціальна інженерія), and reverse social engineering (зворотна соціальна інженерія).

Форми атак соціального інжинірингу (Рис 1.4.):

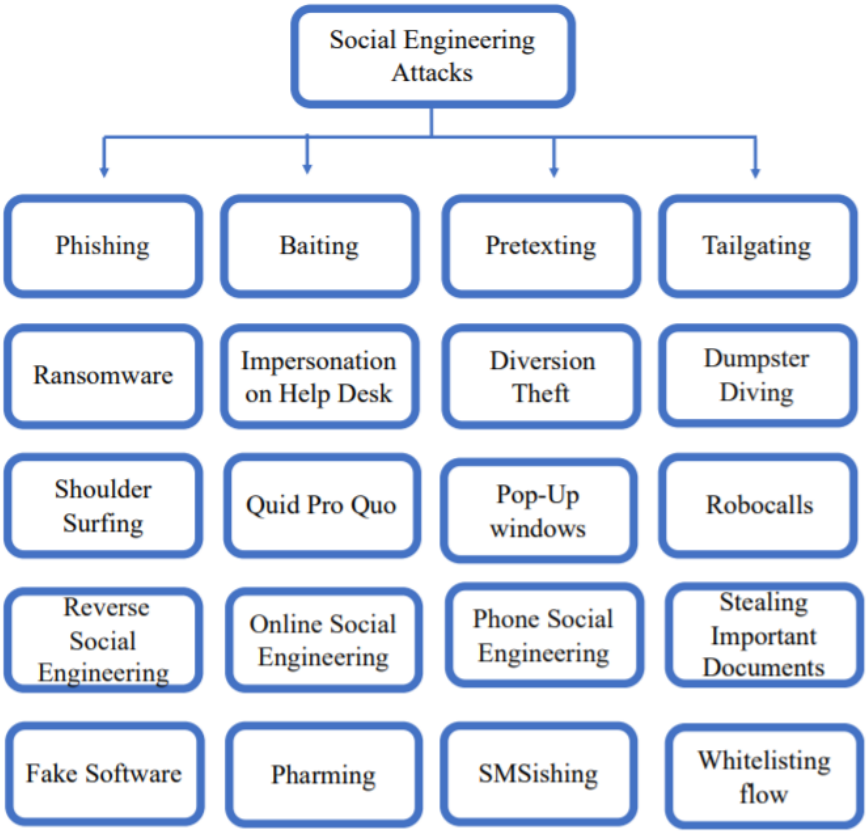


Рис. 1.4. Форми атак соціального інжинірингу

1. Phishing – найпопулярніша атака соціальної інженерії. Це масове розсилання електронних листів від нібито офіційних адресантів великій групі адресатів. Листи спонукають користувачів до відкриття вкладення листа, переходу за гіперпосиланням на веб-сторінку сайту з формою, де необхідно ввести свій логін,

пароль і іншу особисту інформацію. Його метою є виманювання у довірливого або неуважного персоналу комп'ютерної системи персональних даних. Часто фішингові листи містять граматичні та лексичні помилки.

Фішингові атаки можна розділити на п'ять категорій:

1) Spear phishing – це форма фішингу, під час якої зловмисник надсилає повідомлення, спрямовані на конкретну групу людей, або навіть просто окрему особу в якому спонукає його до обов'язкового перегляду та відповіді на отриманий лист з метою викрадення даних або маніпулювання ними в зловмисних цілях.

2) Whaling phishing - це тип атаки, спрямованої на керівників організацій, коли зловмисники маскуються під законних, відомих і надійних осіб і заохочують жертву поділитися дуже конфіденційною інформацією або надіслати банківський переказ на шахрайський рахунок. Під час такої атаки зловмисники надсилають електронний лист, який виглядає як достовірний електронний лист із надійного джерела, часто лист надходить з контакту всередині компанії або облікового запису партнера, постачальника чи клієнта. Електронний лист буде містити достатню кількість особистих даних або посилань, щоб переконати одержувача в його достовірності. Whaling атаки також можуть спонукати користувача натиснути на посилання, яке веде на підроблений веб-сайт, який виглядає ідентично з «офіційним» сайтом, де можна збирати інформацію або завантажувати шкідливе програмне забезпечення. Під час whaling атаки жертв можуть заохочувати поділитися конфіденційними даними, такими як відомості про заробітну плату, податкові декларації або номери банківських рахунків, або їх можуть попросити авторизувати банківський переказ на шахрайський банківський рахунок. Для зловмисників мета whaling атаки зазвичай полягає в крадіжці грошей або даних. Whaling атаку набагато важче розпізнати, ніж стандартну фішингову атаку, оскільки зловмисники зазвичай витрачають набагато більше часу на те, щоб повідомлення електронної пошти та веб-сайти виглядали достовірними. Деякі поширені ознаки того, що електронний лист може бути частиною whaling атаки:

а) адреса електронної пошти відправника не відповідає точному домену компанії, від якої вказано електронну пошту.

б) запит на надання конфіденційної інформації або перерахування грошей на рахунок.

в) почуття терміновості, яке спонукає одержувача діяти швидко, з натяком або загрозою несприятливих наслідків, якщо запитувану дію не буде виконано негайно.

3) Vishing phishing – отримання інформації шляхом входження в довіру під час телефонних дзвінків. Мета соціальних інженерів відтворити «офіційні дзвінки» від імені банків та інших IVR (Interactive Voice Response) систем. Основні сценарії телефонного шахрайства:

а) дзвінки соціально ізольованим (в'язням) або одиноким людям (схеми, що реалізуються шляхом встановлення романтичних стосунків);

б) дзвінки особам, що мають фінансові труднощі (схеми, коли зловмисник пропонує жертві беззаставний кредит (за умови, що остання сплатить авансом комісію, або ж зловмисник представляється жертві колектором, вимагаючи сплатити неіснуючий борг), а також інвестиційні програми під небувало високі проценти);

в) термінова допомога члену сім'ї/ другу – шахрай, який зазвичай орієнтується на людей похилого віку і користується тим, що вони недочувають, видає себе за їхнього онука чи онуку. «Онук» говорить, що він потрапив у біду і потребує грошей. Таких випадків досі дуже багато. Зловмисники використовують дані з соціальних мереж, щоб історії звучали правдоподібно, і говорять приглушеними голосами, вдаючи, що вони плачуть;

г) лотереї – зловмисники повідомляють людині, що вона виграла у розіграші призу, в якому вона насправді ніколи не брала участь. Жертву просять сплатити комісійні за видачу або доставку подарунку чи грошей. Їй також можуть запропонувати зателефонувати за номером з високим тарифом оплати, щоб отримати приз. Часто шахраї використовують назви реальних розіграшів з тим, щоб жертва могла переконатися в їхній законності;

д) шахраї телефонують жертвам, видаючи себе за представників судових чи податкових органів. У деяких випадках шахрай вимагає негайно здійснити

погашення заборгованості, наприклад, простроченого штрафу за порушення правил паркування або прострочених податків. Шахрай може погрожувати тим, що несплата призведе до збільшення суми заборгованості чи навіть терміну ув'язнення.

4) Interactive voice response phishing (інтерактивний фішинг голосової відповіді) - атака виконується за допомогою інтерактивної системи голосової відповіді, щоб змусити ціль ввести приватну інформацію так, ніби запит надходить від законного бізнесу або банку.

5) Business email compromise phishing (фішинг з метою компрометації ділової електронної пошти) – подібно до whaling phishing, націлений на великих «риб» у корпоративних підприємствах, щоб отримати доступ до їхньої ділової електронної пошти, календаря, платежів, бухгалтерської чи іншої приватної інформації. Соціальний інженер використовує ці дані для надсилання електронних листів, змінюючи попередні листи, змінюючи розклад зустрічей, читаючи професійну інформацію про підприємство та зв'язуючись з клієнтами або постачальниками послуг. Зловмисник починає з дослідження високопоставлених співробітників через соціальні мережі, щоб знати та розуміти їх професійну інформацію, як-от дозволений діапазон грошей, які ціль може отримати від банку. Отримавши потрібну інформацію, зловмисник надсилає дуже переконливий діловий лист, щоб змусити звичайного співробітника натиснути посилання або завантажити вкладення електронної пошти, щоб скомпрометувати мережу компанії. Зловмисник вибирає певний час відповідно до календаря цілі та вставляє в електронний лист повідомлення про надзвичайну ситуацію, щоб співробітник швидко діяв.

2. Pretexting — атака, проведена за заздалегідь підготовленим сценарієм. Такі атаки спрямовані на розвиток почуття довіри жертви до зловмисника. Атаки зазвичай здійснюються по телефону. Цей метод часто вимагає попередньої підготовки і пошуку даних про жертву у відкритих джерелах (в основному через соціальні мережі). Претекстинг полягає у видачі себе за іншу людину перед жертвою атаки для отримання бажаних даних.

3. Baiting (атаки приманки, які також називають «дорожнє яблуко») - це атака, коли користувачів просять натиснути посилання, щоб отримати безкоштовні речі. Атака здійснюється шляхом використання незахищених комп'ютерних матеріалів, таких як носії даних або USB-накопичувачі, «ненароком» загублених у кав'ярні, що містять шкідливе програмне забезпечення. Коли жертви підключають USB-накопичувач до своїх комп'ютерів, він діє як троянський кінь у реальному світі та атакує комп'ютер. Ця атака виконує зловмисні дії у фоновому режимі, не помічаючись жертвами.

4. Tailgating – атаки які полягають у фізичному доступі до зони або будівлі, переслідуючи когось, хто має допуск до цього місця. Вони дозволяють зловмисникам несанкціоновано проникати в будівлі. Наприклад, зловмисники просять відкрити двері в будівлю, оскільки вони забули ідентифікаційну картку своєї компанії або картку RFID (радіочастотної ідентифікації). Наприклад, атаки на RFID-картки є однією з найпоширеніших атак для доступу до заборонених будівель у зловмисних цілях. Завдяки їх широкому застосуванню та низькій вартості, системи RFID вважаються технологією, що використовується компаніями для контролю доступу до своїх об'єктів. Незважаючи на свої переваги, вони мають уразливості, які можна використати, щоб викликати серйозні проблеми з безпекою компаній. Атаки RFID можуть здійснюватися на кількох рівнях моделі системи взаємозв'язку (ISO). Наприклад, на фізичному рівні пристрої RFID та фізичний інтерфейс призначені для маніпулювання зв'язком RFID. Ці атаки можуть призвести до тимчасового або постійного пошкодження RFID-карт. На рівні мережевого рівня зловмисник маніпулює мережею RFID, наприклад, спілкування між об'єктами RFID та обмін даними між цими об'єктами.

5. Ransomware attack (атака програми-вимагача) – це ще одна загроза, яка спрямована на окремих осіб і компанії. Наслідки атаки програм-вимагачів можуть бути дорожчими, ніж сам викуп. Постраждалі компанії можуть роками страждати від атаки програми-вимагача через втрату бізнесу, клієнтів, даних та продуктивності. Атаки програм-вимагачів обмежують та блокують доступ до даних і файлів жертви, шифруючи їх. Щоб відновити ці файли, жертві погрожують

опублікувати їх, якщо не заплатить викуп. Цей платіж необхідно здійснити за допомогою криптовалюти, яка є нерегульованою цифровою валютою, яку важко відстежити. Існує два способи аналізу атаки програм-вимагачів: статичний і динамічний. Статичний аналіз виконується висококваліфікованими інженерами та спеціалістами з мов програмування, розробляючи програми для аналізу та розуміння атаки, щоб зупинити її або повернути зашифровані файли. Динамічний аналіз передбачає дистанційне спостереження за функціями шкідливого програмного забезпечення. Він вимагає, щоб надійні системи запускали недовірені програми без пошкодження систем.

Атака програм-вимагачів включає шість етапів: (1) створення шкідливого програмного забезпечення; (2) розгортання; (3) встановлення; (4) командування та управління; (5) руйнування; та (6) вимагання. Створення зловмисного програмного забезпечення полягає в розробці програмного забезпечення-вимагача або використанні існуючого для виявлення будь-якої вразливості в системі жертви, щоб створити метод обходу систем автентифікації. Розгортання полягає в доставці програмного забезпечення-вимагача шляхом обходу цих засобів захисту через створений метод обходу систем автентифікації. Інсталяція складається із запуску програм-вимагачів і зараження системи. На етапі командування та контролю програма-вимагач активна, коли жертва має інтернет-з’єднання для зв’язку з командним центром, або пасивна, коли вона знаходиться в автономному режимі. На стадії знищення програма-вимагач починає блокувати або шифрувати дані та блокує екрани. Вимагання полягає в комунікації з жертвою з вимогою викупу в обмін на звільнення заблокованих файлів із попередженням про обмеження часу. Повернення файлів після оплати жертвою не гарантується. Після запуску атаки програмного забезпечення-вимагача на комп’ютері у жертв є лише три варіанти: (1) сплатити викуп, щоб повернути зашифровані файли; (2) спроба відновити файли з резервних копій, якщо такі є; або (3) втрата даних після відмови сплатити викуп.

6. Tabnabbing (використання вкладок) або fake software attacks - це ще одна форма фішингової атаки. Людина переходить по посиланню на сайт, який довго завантажується, і тоді коли людині набридає чекати, вона переходить на іншу

вкладку займатись далі своїми справами. Цей тип атаки перезаписує наявну вкладку з веб-сайтом зловмисника. Щоразу, коли жертва повертається на цю вкладку, вона думає, що вийшла з певного веб-сайту, і спробує увійти знову, і як тільки жертва увійде в свій обліковий запис, зловмисник захопить облікові дані. Для запуску цієї атаки можна використовувати програму Social-Engineer Toolkit.

7. Pharming – це ще одна атака соціальної інженерії, яка за своєю природою схожа на фішинг, за винятком того, що вона спрямована на отримання приватних фінансових даних за допомогою підробки домену (рис. 1.5.). На відміну від фішингу, фармінг використовує підробку домену, а не електронного листа, щоб обманом змусити жертв відвідати шкідливі веб-сайти, які виглядають як «офіційні» сайти. Pharming використовує недоліки дизайну сайтів та непомітні виправлення в доменних ім'ях (DNS). Він просто маніпулює компонентами системи імен домену та хосту, перенаправляючи користувача з одного веб-сайту на інший. Коли жертва вводить назву сайту в пошуковій системі, через неуважність, вона просто переходить на веб-сайт зловмисника, який є «абсолютною» копією офіційного сайту. Оскільки жертва бачить правильну веб-адресу в адресному рядку, це ускладнює виявлення фармінгу. Користувач може отримати вірус через лист на електронній пошті, скачаний файл або при відвідуванні якогось сайту. Користувач переходить за посиланням і потрапляє на підроблений сайт. Таким чином соціальні інженери перехоплюють особисту інформацію — номер картки/рахунку, пароль або ПІН-код.

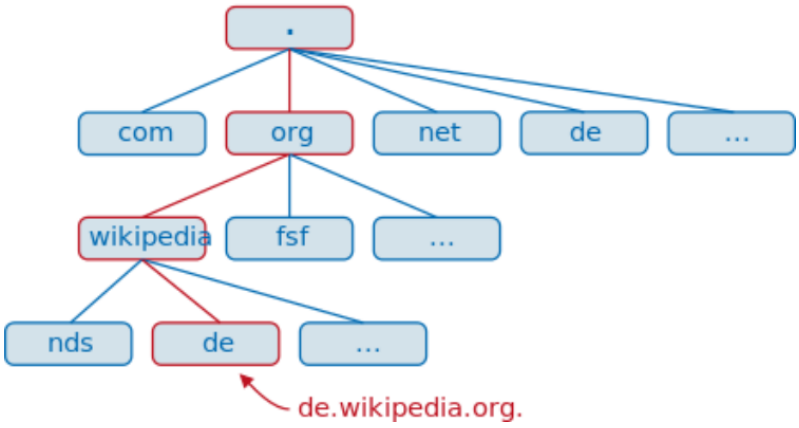


Рис. 1.5. Підробка домену під час фармінгу

8. Reverse Social Engineering Attacks – це атака, коли зловмисники стверджують, що тільки вони можуть вирішили проблему мережі або якусь іншу технічну проблему. Атака відбувається за три основні кроки: (1) спричинення такої проблеми, як збій мережі; (2) реклама того, що зловмисник є єдиною особою, яка може вирішити цю проблему; (3) вирішення проблеми з отриманням потрібної інформації та виходом без виявлення.

9. Pop-Up Windows (атаки спливаючих вікон) – це вікна, які з'являються на екрані жертви і повідомляють про втрату з'єднання. Користувач реагує повторним введенням інформації для входу, яка запускає шкідливу програму, яка вже встановлена у вікні. Ця програма віддалено пересилає назад інформацію для входу зловмиснику. Наприклад, спливаючі вікна можуть бути сповіщеннями, які з'являються випадковим чином для онлайн-реклами, щоб заманити жертву натиснути на це вікно. Спливаючі вікна також можуть бути фальшивими повідомленнями про виявлення вірусу на комп'ютері жертви. Спливаюче вікно запропонує жертві завантажити та встановити рекомендоване антивірусне програмне забезпечення для захисту комп'ютера. Вони також можуть бути фальшивими попередженнями про те, що сховище комп'ютера заповнене і що його потрібно відсканувати та очистити, щоб заощадити більше місця. Жертва панікує і швидко реагує, щоб усунути проблему, що активує шкідливе програмне забезпечення, яке міститься у спливаючому вікні.

10. Smishing – різновид фішингу, де отримання конфіденційних даних здійснюється шляхом масового розсилання повідомлень в месенджерах від нібито офіційних адресантів великій групі адресатів, які містять шкідливі посилання або вміст.

Найпопулярніший варіант smishing атаки в нашій країні – це повідомлення про несподівані виграші. Наприклад, вам повідомляють, що ви виграли автомобіль, велику суму коштів чи сучасну техніку, хоча не брали участі в різних конкурсах, а просто стали щасливчиком. В SMS-повідомленні може бути посилання на підроблений сайт, на якому необхідно ввести свої конфіденційні дані нібито для отримання виграшу. Але навіть якщо такого посилання немає, а користувач повірив

у виграш, з нього спробують будь-яким чином отримати гроші: наприклад, під приводом того, що згідно із законодавством виграш оподатковується, і суму податку необхідно перерахувати на вказаний рахунок, щоб його отримати.

Також, зовсім недавно з’явилась схема smishing атаки проти продавців на онлайн платформі купівлі та продажів OLX:

псевдопокупець знаходив продавця на онлайн-майданчику;

одразу писав у сторонній месенджер, намагався увійти в довіру;

надсилав сторонні посилання та переконував перейти по них (які вели на фішинговий сайт)

ділився фейковими правилами роботи сервісу, квапив і навіть тиснув, щоб жертва самостійно заповнила на сайті поля зі своїми платіжними даними;

отримував від жертви-продавця на фішинговому сайті CVV-код, баланс та термін дії картки, щоб у результаті вивести вкрадені гроші на віртуальний рахунок.

11. Shoulder surfing – метод застосовується в транспорті, в кафе та інших громадських місцях, що дозволяють через плече жертви спостерігати за комп’ютерними пристроями і телефонами. Він використовується для отримання інформації, такої як PIN-коди, паролі та інші конфіденційні дані.

12. Quid pro quo - при використанні цього виду атаки зловмисники обіцяють жертві вигоду в обмін на факти. Наприклад, зловмисник дзвонить в компанію, представляється співробітником технічної підтримки і пропонує встановити «необхідне» програмне забезпечення. Після того, як отримано згоду на установку програм, порушник отримує доступ до системи і до всіх даних, що зберігаються в ній.

13. Dumpster Diving – атаки полягають у зборі конфіденційних документів зі сміття компанії або викинутого обладнання, наприклад старих комп’ютерних матеріалів, дисків, компакт-дисків і DVD, USB-накопичувачів.

14. Diversion Theft - атаки полягають у неправильному спрямуванні транспортної компанії для доставки кур'єром посилки або листа в потрібне місце.

15. Stealing important documents - атаки полягають у крадіжці документів із чийогось столу для користування в особистих інтересах.

Також існує необхідність проаналізувати, як з плином часу змінюються фішингові сценарії, зокрема під впливом COVID-19; які сценарії залишаються незмінні і, як і раніше, б'ють у ціль, а які зжили себе і нагадують про себе хіба що поодинокими випадками поразки.

Всі фішингові сценарії можна розділити на три великі умовні групи:

Макрос сценарії – сценарії, де користувач повинен дозволити виконання макросів. Як приклад недавньої атаки можна навести запуск шифрувальника через макроси.

Парольні сценарії - сценарії, де користувач повинен ввести в систему свої логін та пароль. Тут можна згадати незвичайну атаку з використанням абетки Морзе.

Сценарії з виконуваними файлами – сценарії, де користувач повинен завантажити та встановити файл, що виконується. Телефонний скам нібито від компанії Microsoft, а також атаки на користувачів LinkedIn з використанням безфайлового бекдору more_eggs.

Тепер розглянемо кілька реалізацій цих сценаріїв, які застосовуються на практиці.

Макросні сценарії:

1. Розпродаж офісного майна. Вам на пошту приходить лист із привабливою пропозицією: "У нас залишилося кілька списаних ноутбуків, майже нових, не битих, не фарбованих і всього за третину від закупівельної ціни." Або ж: "Плануємо нові закупівлі, старі меблі віддамо за безцінь, тільки заберіть." І до листа прикріплено таблицю Excel з макросами.

2. Інвентаризація обладнання. Теж часта ситуація і, що найгірше, дуже правдоподібна: "Погляньте, чи є в даному документі ваше обладнання?"

3. Оновлення бонусної програми. Розсилка, яка розповідає про можливі бонуси за залучення до компанії нових співробітників чи партнерів.

4. Перерахунок заробітної плати, премія. Зазвичай файл із макросами розсилається від імені головного бухгалтера. Зміна умов нарахування премії,

перерахунок заробітної плати та загалом будь-які зміни у графіку виплат стабільно викликають інтерес. У випадку пандемії виглядає цілком правдоподібно.

5. Банківські документи. Ще одна варіація фінансового сценарію. Підозрілі рухи тризначних сум. Операції з вашого рахунку. Нові умови зарплатної програми. Люди емоційно сприймають новини, пов'язані з їхніми фінансами, та зловмисник може зіграти на цьому.

6. Графік вихідних та святкових днів. Як показує практика, цей сценарій добре спрацьовує перед святами, коли потрібно багато встигнути, і рівень уважності до побутових дрібниць різко знижується. Перенесення свят, скорочені або несподівано збільшені вихідні дні – чудові інфоприводи для зловмисника.

7. Акт звіряння рахунків та інша документація. Досить рідкісний сценарій, але від цього не менш дієвий. Він може спрацювати, якщо зловмисник провів попередню розвідку та з'ясував, з якими клієнтами/партнерами компанія-жертва зараз співпрацює.

Парольні сценарії:

1. Новий офіс. Пандемія багатьох змусила переїхати в більш бюджетні або оптимальні планування приміщення (наприклад, коворкінги замість багатоповерхових кабінетних офісів). Зловмисник може запросити жертву на вебінар для обговорення переїзду або на корпоративний мітинг на тему “Ідеальний офіс: ваші пропозиції”. Якщо він буде досить переконливим, такий сценарій може увінчатися успіхом.

2. Запрошення на внутрішню зустріч або вебінар.. Все залежить від специфіки роботи компанії та фантазії зловмисника. Внутрішній мітап, запрошення на безкоштовний вебінар з технічної англійської, участь в обговоренні майбутнього корпоративу. Вибір безмежний, а в умовах віддаленої роботи мало кого можна здивувати пропозицією зателефонувати.

3. Внутрішньокорпоративні подарунки. Старий сценарій, який не втрачає своєї актуальності. Відмінно показує себе у періоди свят, особливо якщо у компанії є корпоративний магазин із мерчем. Тому новина про знижку на будь-що або

компенсацію корпоративного харчування з великою ймовірністю буде зустрінута тепло.

4. Інтеграція з популярними сервісами та банками. Розвиток попередньої теми. Промокоди – дуже спокуслива річ, адже люди люлять знижки. Хто не захоче отримати доступ до навчальних курсів чи безкоштовну підписку на кіносервіс напередодні гучної прем'єри? Щодо банків, тут завжди можна розіграти карту “зміни зарплатного проекту з більш вигідними умовами”.

5. Хтось входить до вашого облікового запису! Це також старий-добрий ефективний сценарій. Тут потрібно зіграти на пильності співробітника та зробити так, щоб ініціатива виходила від нього. Не зрозумівши, що відбувається насправді, користувач може перейти по помилковому засланні для скидання пароля або вийти на зв'язок зі зловмисником, відповівши на лист.

6. Автоматичне сповіщення із Jira/Wiki/Confluence/чата. Розрахунок на те, що співробітники користуються цими програмами щодня, через що вже не звертають уваги на супроводжуючий текст сповіщень. Жертва потрапляє на фішингову копію сторінки трекера, де вводить облікові дані. У цьому сценарії на руку зловмисників грає і те, що не всі встигли добре познайомитися з новими колегами, які приєдналися до компанії під час пандемії/на віддаленні, особливо якщо компанія велика.

7. Тестування нового сервісу %service_name%. Зловмисник пропонує жертві перевірити, чи зможе вона увійти до “тестованого” сервісу, який нібито перебуває на стадії впровадження. Якщо сторінка входу виглядатиме досить правдоподібно і підтримуватиме корпоративний стиль, жертва може потрапити на цей прийом і ввести свої облікові дані.

8. Запис на вакцинацію. Цей сценарій стає все більш ймовірним. Люди, яким не терпиться повернутися до нормального життя, поставляться до такого листа з великою довірою.

Сценарії з виконуваними файлами:

Проаналізувавши статистику успішних атак соціальної інженерії, можна зробити висновок, що переважна більшість користувачів ставляться із підозрою до

заклику завантажити та встановити якесь ПЗ на свою робочу станцію. Тим не менш, поки зловмисники не відмовилися від подібних сценаріїв:

1. Запрошення на співбесіду або онлайн-зустріч. Це може бути привабливий лист від "рекрутера" реальної компанії. Для проведення співбесіди пропонується встановити нову програму або внутрішній месенджер.

2. Встановлення нового сервісу/"пропатченої" версії старого сервісу. Вдаючись представником IT-відділу, зловмисник може попросити користувача встановити нову версію ПЗ, в якій, наприклад, виправлені серйозні вразливості. Підійде і варіант з новим, більш гнучким та безпечним VPN, який запускається у “тестовому” режимі.

Це далеко не всі можливі сценарії — фантазія шахраїв безмежна.

1.3. Аналіз статистичних даних щодо кіберінцидентів методом соціальної інженерії

Сьогодні, соціальні інженери по всьому світу вигідно використовують панічні настрої, пов'язані з побоюваннями за здоров'я в період пандемії, збільшення кількості працівників на дистанційній роботі, та той факт, що більшість людей почали користуватися новими технологіями для спілкування з близькими. Справедливо відмітити, що атаки СІ щодня видозмінюються і актуалізувати необхідну інформацію щодо протидії їм практично нереально.

У січні-квітні 2020-го Інтерпол зафіксував близько 907 тисяч спам-листів, 48 тисяч шкідливих URL та 737 інцидентів зі шкідливим ПЗ, пов’язаних із коронавірусом. Наприклад, Trickbot використовує тематику фінансової допомоги, а AZORult розповсюджується завдяки шкідливим сайтам, що видають себе за інформативні сайти по COVID-19.

Згідно досліджень компанії Positive Technology кількість атак з використанням методів соціальної інженерії помітно збільшилася: якщо у III кварталі 2020 року частка таких атак становила 67%, то у поточному кварталі (III

квартал 2021 року) вона зросла до 83%. Зловмисники не стоять на місці та постійно вдосконалюють методи обману жертв (рис. 1.6.) [7].

Під час пандемії, працюючи з дому, 47% людей ставали жертвами фішингових афер. Про це йдеться у дослідженні Deloitte щодо впливу COVID-19 на кібербезпеку.

Аналізуючи звіти компаній ESET та Check Point можна стверджувати, що найчастіше шкідливі вкладення надсилаються користувачам у вигляді виконуваних файлів Windows (у 74% випадків). Багато компаній по всьому світу використовують продукти Microsoft. Це може бути електронна пошта, онлайн обмін файлами або віртуальне спілкування. Якщо вірити аналітиці компанії Terranova Security 20% усіх співробітників, швидше за все, перейдуть за фішинговим посиланням у електронному листі, а 67,5% співробітників вводитимуть свої облікові дані на фішинговому веб-сайті.

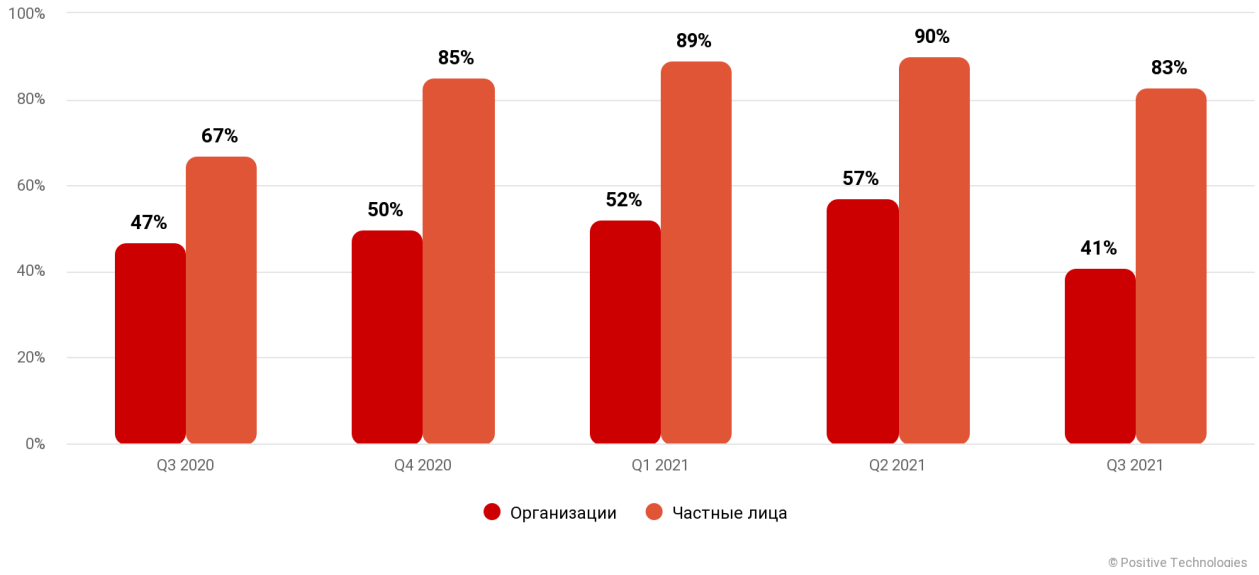


Рис. 1.6. Статистика компанії Positive Technology щодо атак з використанням методів соціальної інженерії

Крім того, 80% фахівців з безпеки зіткнулися зі зростанням загроз з моменту переходу на віддалену роботу. З цих 80% респондентів 62% вважають, що з переходом на віддалену роботу, кількість загроз, так званих, фішингових кампаній, побільшало, ніж будь-яких інших.

Тренди фішингу змінилися на тлі пандемії COVID-19. Ми можемо спостерігати значні зміни у способах та формах трудової діяльності, включаючи тенденції до переходу на віддалену роботу та прискорену цифрову трансформацію.

Використання технологій штучного інтелекту та дистанційних технологій кардинально змінило те, як ми взаємодіємо з онлайн-середовищами. 76% власників бізнесу визнали збільшення випадків можливого шахрайства з початком пандемії, стверджує компанія BDO.

І з огляду на те, що понад чверть власників бізнесу постраждали від злому системи безпеки під час локдауну, їх твердження небезпідставні!

Мало того, що підприємствам потрібно більше точок підключень до інтернету, але для роботи також використовуються і персональні пристрої, що призводить до зростання вразливостей. Цю тіньову IT-мережу неможливо проконтролювати, що ставить власників бізнесу в більш вразливе становище, ніж вони могли очікувати.

У найближчі чотири роки партнери-імплементатори USAID «Кібербезпека критично важливої інфраструктури України» працюватимуть над покращенням кіберстійкості України, а для цього зокрема і надаватимуть підтримку приватному бізнесу. Український ринок кібербезпеки тим часом оцінюють у $ 100 млн, з яких близько половини складає держзамовлення.

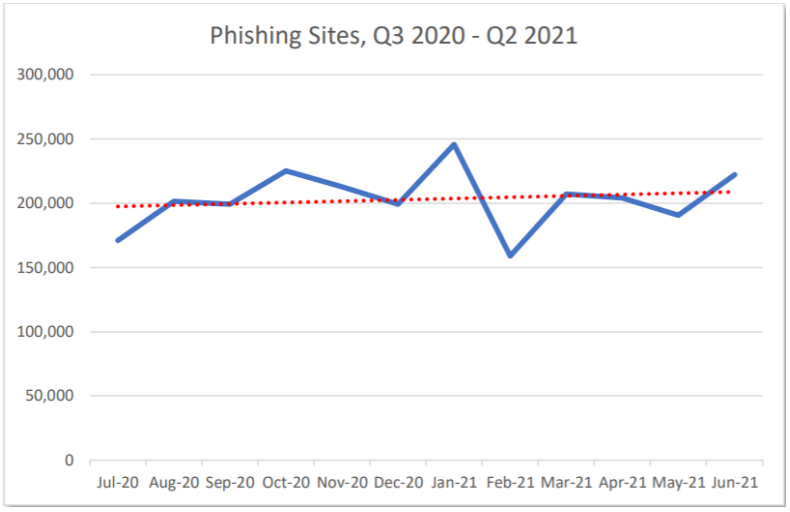


Рис. 1.7. Кількість фішингових атак з серпня 2020 року по червень 2021 року (за даними APWG)

За даними звіту «Phishing Activity Trends Report 2 nd Quarter 2021» опублікованого 22 вересня 2021 року компанією APWG (Anti-Phishing Work Group) кількість фішингових атак за останній рік залишалася стабільною, але приблизно вдвічі більше, ніж з середини 2019 року до середини 2020 року.

Червень 2021 став третім найгіршим місяцем в історії звітності APWG тому, що зафіксував 222 127 атак (рис. 1.7.)[8].

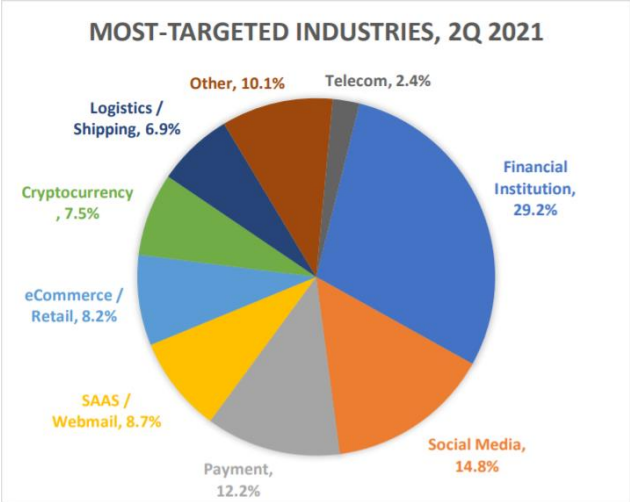


Рис. 1.8. Цільові галузі для фішингових атак II квартал 2021 року (за даними APWG)

Фішинг націлений на криптовалюту — зріс з 2% усіх атак у першому кварталі до 7,5% у другому (рис.1.8) [8].

1.4. Вимоги нормативних документів з протидії методам соціальної інженерії

Національний стандарт України ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.» (ISO/IEC 27001:2013; Cor 1:2014, IDT), прийнятий наказом ДП «УкрНДНЦ» від 18.12.2015 №193[9].

В стандарті об’єктом нашої уваги слугують пункти:

про ролі та обов’язки щодо ІБ, а саме про те, що їх треба чітко визначати та розподілити.

про те, що в місцях віддаленої роботи для захисту інформації, яка доступна, обробляється чи зберігається повинні бути запроваджені політики безпеки та заходи підтримання безпеки.

про те, що усі співробітники організації (за необхідністю і підрядники) мають проходити належне навчання й тренінги для поінформованості та регулярно отримувати оновлені дані щодо політик безпеки і процедур безпеки організації, суттєвих для їх посадових функцій.

ДСТУ ISO/IEC 27032:2016. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки [10].

Найбільш актуальним розділом стандарту в рамках нашої теми є розділ *12.5 «Засоби управління захистом від атак соціальної інженерії»*. В ньому говориться про архітектуру засобів управління які застосовуються для управління та мінімізації ризиків кібербезпеки стосовно атак соціальної інженерії. Серед таких засобів:

політики безпеки (мають бути визначені та задокументовані). Вони регулюють створення, збирання, зберігання, передачу, обмін, обробку та загальне використання корпоративної, персональної інформації та інтелектуальної власності в Інтернеті та в кіберпросторі.

процеси категоризації та класифікації інформації мають бути реалізовані для підтримки політик, що підвищують обізнаність та захист корпоративної класифікованої та персональної конфіденційної інформації, охоплюючи інтелектуальну власність.

обізнаність та навчання в галузі безпеки, охоплюючи регулярне оновлення відповідних знань, є важливим елементом протидії атакам соціальної інженерії.

тестування. Організація повинна розглянути проведення періодичних тестів для визначення рівня обізнаності та дотримання відповідних політик і практик.

технічні засоби. Додатково до встановлення політик та практик протидії атакам соціальної інженерії повинні бути розглянуті та, де можливо, застосовані технічні засоби управління для мінімізації незахищеності й потенційної експлуатації зловмисниками.

Також йдеться про те, що єдиним ефективним способом зменшення загроз соціальної інженерії є поєднання:

технологій захисту;

політик безпеки, що встановлюють основоположні правила для особистої поведінки як приватної особи, так і працівника;

відповідної просвіти й тренування.

Указ Президента України від 26 серпня 2021 року №447 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"»[11].

В стратегії говориться про те, що пандемія COVID-19 матиме довготривалий вплив на світовий порядок, посилюючи роль електронних комунікацій у повсякденному спілкуванні та роботі, що підвищує ступінь вразливості процесів обробки інформації, зокрема персональних даних. Це вимагає забезпечення належного рівня їх захищеності та змушує державу і бізнес впроваджувати додаткові механізми і заходи щодо належного функціонування і захисту всіх необхідних для життєдіяльності інформаційних ресурсів і систем.

Однією із цілей стратегії є професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки – Україна проведе докорінну реформу системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки, а також здійснить заходи щодо збереження наявного кваліфікованого кадрового потенціалу суб'єктів кібербезпеки, стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням появи нових кіберзагроз і викликів, створення національних інформаційних систем, платформ і продуктів. Вітчизняний науково-технічний потенціал першочергово залучатиметься до вирішення завдань забезпечення кібербезпеки держави. Цифрові навички, кіберобізнаність щодо сучасних кіберзагроз та протидії ним стануть невід'ємними елементами освіти кожного громадянина України.

Для досягнення цієї цілі в Україні буде проведено наукові дослідження у сфері кібербезпеки, реформовано систему підготовки та підвищення кваліфікації

кадрів, а також розгорнуто навчальні програми, курси, тренінги з кібернавчання для всіх верств населення шляхом:

забезпечення координації наукового співтовариства під час проведення наукових досліджень і розробок у сфері кібербезпеки та залучення його до заходів з реалізації державної політики у сфері кібербезпеки;

визначення довгострокових напрямів проведення досліджень і розробок у сфері кібербезпеки, а також розроблення дієвої програми державної підтримки (на основі проектного підходу) стратегічно важливих для кібербезпеки держави наукових установ і організацій, проведення наукових досліджень у цій сфері для потреб національної безпеки і оборони;

забезпечення стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням розвитку новітніх інформаційно-комунікаційних технологій, зокрема, технологій хмарних та квантових обчислень, 5G-мереж, Інтернету речей, штучного інтелекту, а також появи нових засобів реалізації кіберзагроз з метою створення вітчизняних систем, платформ і продуктів у сфері кібербезпеки;

удосконалення системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки;

розроблення Загальнонаціональної програми кіберграмотності, спрямованої на підвищення рівня цифрової грамотності населення України, зокрема, шляхом включення питань стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії ним до навчальних програм загальної середньої, професійної (професійно-технічної), фахової передвищої та вищої освіти;

утворення центрів, що будуть здійснювати узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій та вітчизняних розробок у цій сфері;

забезпечення матеріального стимулювання фахівців у сфері кібербезпеки, які перебувають на військовій, державній службі, у тому числі на державній службі особливого характеру, службі в правоохоронних органах або працюють за трудовим договором у державному секторі і безпосередньо виконують функції із забезпечення кібербезпеки та кіберзахисту, з урахуванням рівнів оплати праці таких фахівців у приватному секторі;

залучення суб'єктів національної системи кібербезпеки до міжнародних програм навчання і підвищення кваліфікації персоналу.

Висновки з розділу 1

Визначено поняття соціального інжинірингу, розглянуто найпоширеніші форми та методи соціальної інженерії на об’єктах інформаційної діяльності, проаналізовано статистичні дані щодо кіберінцидентів методом соціальної інженерії та досліджено вимоги нормативних документів з протидії методам соціальної інженерії. Особливу увагу приділено сценаріям фішингових атак і досліджено як з плином часу вони змінюються, зокрема, під впливом COVID-19.

Виходячи з результатів аналізу першого розділу постає необхідність проаналізувати основні методи та засоби протидії соціальному інжинірингу на об’єктах інформаційної діяльності в умовах дистанційної роботи співробітників, оцінити їх недоліки та переваги в тих чи інших випадках.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ПРОТИДІЇ СОЦІАЛЬНОМУ ІНЖИНІРИНГУ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В УМОВАХ ДИСТАНЦІЙНОЇ РОБОТИ СПІВРОБІТНИКІВ

2.1. Метод протидії соціальному інжинірингу шляхом профілактики та зменшення негативного впливу атак

Пандемія уже змінила світ докорінно. Навіть в країнах, де темпи вакцинації достатньо високі, багато робітників стверджують, що не готові повертатись в офіси, вимагають продовження дистанційної роботи. Тож нові продукти та послуги, які допоможуть забезпечити кіберзахист в таких умовах, точно будуть мати попит.

Атаки соціальної інженерії представляють значні ризики безпеки, і усунення цих атак має бути частиною стратегії управління ризиками компаній та організацій. Як відомо, найкращий метод захисту - це профілактика. Це твердження стосується усіх сфер нашого життя і атаки соціальної інженерії не є виключенням. Компанії повинні взяти на себе зобов'язання щодо заохочення співробітників навчатися основам кібербезпеки, кібергігієни та правил поводження з різними видами інформації. Нижче наведені основні методи профілактики відносно різних форм атак соціального інжинірингу.

Щоб виявити *атаки через телефонні дзвінки*, необхідно перевірити джерело дзвінків за допомогою контактів, попросити передзвонити співрозмовника в якому ви не впевнені або почати задавати запитання особистого змісту, щоб перевірити особу абонента. Найефективніший спосіб зупинити ці атаки – не відповідати на підозрілі дзвінки або дзвінки з невідомого номеру.

Щоб запобігти *атакам «служби підтримки»*, можна запровадити в компанії кодове слово або PIN-код, яке працівник служби підтримки повинен сказати на початку розмови.

Для *атак на основі електронної пошти* деякі компанії використовують електронні адреси honeypot, які також називають спам-пастками, щоб збирати та публікувати спам для співробітників. Коли лист надсилається з одного зі списку

honeypot, сервер розглядає його як шкідливий і тимчасово блокує. Інші процедури, які можна виконати, включають: перевірку джерел електронної пошти перед тим, як натиснути посилання або відкрити вкладення, перевірка заголовку електронного листа, дзвінок відправнику (колезі, клієнту або іншій відомій вам людині), якщо є підозра, і відправляти в спам або блокувати електронні листи з виграшами або знижками. Для фішингових атак можна використовувати інструменти для внесення в чорний список і блокування фішингових веб-сайтів. Прикладами цих інструментів є антифішинговий фільтр McAfee, фільтр фішингу Microsoft і Web sense.

Під час *атак «серфінг через плече»* особи повинні бути більш обізнаними про те, що їх оточує, включаючи людей або камери, коли вони вводять конфіденційну інформацію.

Під час *атак «занурення у смітник»* конфіденційні викинуті документи та матеріали мають бути повністю знищені за допомогою шредерів, пристрої пам’яті мають бути захищені або стерті, а важливі файли мають бути заблоковані.

Атакам на основі троянів можна запобігти, не дозволяючи використовувати свій персональний або робочий комп’ютер іншим людей, використовувати антивірус для сканування USB перед його відкриттям і виконувати антивірусні інструкції та попередження, перевіряти будь-які несподівані листи на електронній пошті, а також не підбирати, та не використовувати знайдені цифрові носії.

Щоб запобігти *атакам підробленого програмного забезпечення*, люди повинні уважно перевіряти веб-адресу та веб-сторінки сайту, на якому вони мають вводити свої автентифікаційні дані, оскільки справжні веб-сайти завжди мають щось особливе, на відміну від підроблених. Антивірус в цій ситуації може бути обмежений через неуважність та поспіх людини, він може ловити ці атаки та надсилати попередження, які більшість користувачів ігнорує, закриваючи вікно й рухаючись далі.

Також потрібно звернути увагу на *методи зменшення негативного впливу атак соціальної інженерії.* Вони спрямовані на те, щоб врятувати те що ще можна, після того, як людину вже атакували або систему компанії вже зламали. Атаки на

основі людини є складними і їх важко виявити, що робить їх пом’якшення необхідним. Серед них:

формування культури корпоративної безпеки серед співробітників компанії є методом пом’якшення наслідків атак, спрямованих на організації чи групи осіб. Вона допомагає жертві атаки не соромитися маніпуляції, оскільки соціальний інженер використовує довірливість людини, а не те, що жертва має низький інтелект. Знання цієї культури підвищує відповідальність за безпеку, повідомляючи про всі атаки фахівцю з кібербезпеки якнайшвидше, працівник запобігає більшій шкоді. Цей метод пом’якшення заощаджує дорогоцінний час для реагування на атаку та зупинення поширення атаки на мережу компанії.

поширення обізнаності про психологічні тригери атак соціальної інженерії це метод пом’якшення атак, пов’язаних із дзвінками чи електронними листами, де говориться про виграш у лотерею, в якій вони не приймали участь. Якщо люди отримують таку інформацію, вони повинні скептично сприймати таку інформацію, і знати що ніхто не віддасть їм статки електронною поштою або як пожертвування. Така обізнаність співробітників може перешкодити відповісти на запит зловмисника.

Методи зменшення негативного впливу атак соціальної інженерії на людину засновані на людських судженнях про те, чи є активність законною або шкідливою. *Вони передбачають два підходи: (1) аудит і політика; (2) освіта, навчання та поінформованість.*

Аудит та політика відноситься до правил і процедур безпеки, запроваджених у компаніях, щоб допомогти співробітникам виявити атаки соціальної інженерії. Політичний підхід можна розглядати як стратегію захисту, щоб контролювати реакцію співробітника під час атаки соціальної інженерії.

Освіта, навчання та підвищення обізнаності використовуються для ефективного застосування аудиту та політичного підходу. Вони спрямовані на забезпечення розгортання в організації визначених політик і процедур безпеки.

Людські методи зменшення негативного впливу атак соціальної інженерії є обов’язковими для компаній, щоб пом’якшити атаки соціальної інженерії та

мінімізувати їх вплив на використання слабких і вразливих місць співробітників. Вони в основному пов’язані з ефективністю прийняття рішень і виконання дій, щоб класифікувати діяльність як зловмисну.

Однак людські рішення є відносними і, таким чином, неефективними, оскільки людське судження є суб’єктивним навіть при гарній обізнаності щодо атак соціальної інженерії.

Для підвищення точності людських методів пом'якшення необхідні методи пом'якшення на основі технологій. *Існує три технологічні методи пом’якшення наслідків:*

біометричні дані - методи, засновані на біометричних даних, спрямовані на протидію атакам фізичного видавання себе за іншу особу (за співробітника компанії) шляхом створення підробленого профілю з його/її особистими даними. Біометрія відрізняє справжніх співробітників від підроблених профілів за їхніми біологічними ознаками. Цими унікальними рисами можуть бути відбитки пальців, розпізнавання обличчя, аналіз сітківки ока і голос. Методи на основі біометричних даних можуть бути ефективними, лише якщо зловмисник піддається біометричним тестам.

датчики - техніка на основі сенсорів передбачає використання датчиків для ідентифікації людей. Наприклад, перевірка співробітників за допомогою пропусків.

штучний інтелект - системи штучного інтелекту здатні навчатися, адаптуватися та змінювати свої параметри відповідно до ситуації.

Штучний інтелект стрімко розвивається та стає потужним інструментом вирішення проблем усіх сфер життя суспільства. Проте варто відзначити, що сучасні вчені досі не визначилися чи можна створити «мислячий» штучний інтелект, деякі вважають, що це можливо при великій обчислювальній потужності комп'ютера і достатньої складності алгоритмів, інші вважають, що комп'ютер ніколи не зможе мислити, відчувати емоцій та наслідків свого рішення, так як це робить людина.

Тому, будемо дотримуватися ідеї, що штучний інтелект, насамперед, це набір алгоритмів із заданими шаблонами, який також може змінювати деякі алгоритми

та доповнювати шаблони в процесі навчання, ґрунтуючись на математичних обчисленнях та теорії ймовірності.

При правильному створенні алгоритмів і достатньому налаштуванні математичних обчислень, штучний інтелект прийматиме найбільш вірні з погляду можливостей рішення.

Також штучний інтелект не може приймати рішення, які суперечать логікі його шаблонів. Саме тому впровадження правильно налаштованої інформаційної системи може захистити компанію від більшості атак методами соціальної інженерії

Найбільш вигідний варіант впровадження - це створення інформаційної системи, яка зможе аналізувати вміст листів електронної пошти перед відкриттям їх працівником, а також контролювати дзвінки, що надходять. Дана система після перегляду великої кількості листів зможе виробити шаблони, які будуть визначати адресата повідомлень (діловий партнер або потенційний зловмисник), також така система зможе аналізувати посилання, додані до листа. Фішингові посилання зазвичай структурно виділяються, а отже їх не важко виявити, проте працівник може, не вдумуючись натиснути на нього, а впроваджена система цього не допустить. Також розроблений штучний інтелект повинен містити шаблони номерів та електронних адрес компаній-партнерів та перевіряти їх менш ретельно, що, безсумнівно, прискорить його роботу.

Кардинальною особливістю застосування саме штучного інтелекту є навчання системи, шляхом переналаштування шаблонів, а також можливість не автономної роботи, а в парі з людиною. Таким чином, рішення має зменшити ймовірність успішної атаки на користувачів, причому найбільш помітним буде ефект у великих компаній, в яких з одного боку є велика вибірка для навчання експертної системи та, з іншого боку – проблеми з кваліфікацією численного персоналу (користувачів інформаційної системи).

Дуже мала кількість компаній в даний час мають достатньо ресурсів, щоб проводити розробки штучного інтелекту. Однак багато компаній побоюються, що впроваджені системи для співробітників можуть на першому етапі призвести до

збоїв у роботі та втрати виручки, а надалі уповільнити робочий процес на всіх рівнях.

Окремо варто уточнити що ефективність системи захисту оцінюється за двома критеріями:

Відношенням витрат на захист до вартості об'єкта, що захищається (потенційного збитку);

Відношенням прибутку до витрат зловмисника на злом системи.

Якщо зловмисник витрачає на злом більше, ніж отримує, систему захисту можна вважати успішною, однак у міру поширення типових засобів захисту, неефективний злом однієї компанії може стати ефективним при перекладі методу в «масове» виробництво. Що вимагає удосконалити систему захисту. Хороша експертна система здатна в цьому випадку самонавчатись, зменшуючи ефективність атаки зловмисника.

Резюмуючи все сказане вище, перерахуємо *недоліки рішення:*

проблема проектування;

великі терміни впровадження, пов'язані з необхідністю навчання системи та операторів;

великі фінансові витрати;

зменшення продуктивності;

ризик злому чи обходу експертної системи.

Варто зазначити, що обране рішення з урахуванням розібраних недоліків є об'єктивним і може використовуватися як експертна система для роботи разом із користувачем.

Як можливі реалізації задуманого рішення розглянемо 3 приклади існуючих інформаційних систем і проведемо їх аналіз, оцінку переваг та недоліків.

1. Штучний інтелект компанії Avast званий ними MDE (in-memory database) використовує методи машинного навчання та успішно упізнає шкідливі посилання та шкідливе програмне забезпечення.

Перевагою цього рішення є багатофакторна оцінка отриманих даних, за рахунок чого система може дати точний результат перевірки та виключити такі

методи як «фішинг», «троянський кінь», «дорожнє яблуко» та випадки, коли у методі «шантаж» використовується шкідливе програмне забезпечення.

Дана система не може відслідковувати в отриманих повідомленнях і дзвінках можливі повідомлення зловмисників, не має бази даних «довірених» джерел, що є вагомим недоліком при виборі його як готового рішення захисту від атак методами соціальної інженерії [14].

2. Інженери з Массачусетського технічного університету створили *штучний інтелект здатний визначати приховані соціальні зв'язки*. Даний алгоритм також успішно зможе розпізнавати потенційних соціальних інженерів з листів.

Дана система дозволяє аналізувати великі обсяги тексту, за рахунок чого може бути ефективна проти методів «претекстинг», «кві про кво», «зворотна соціальна інженерія» та випадків, коли для методу "шантаж" використовуються засоби зв'язку.

Проте цей штучний інтелект ще знаходиться на стадії розробки і може бути доопрацьований ще не скоро. Також варто зазначити, що дане рішення ніяк не може відстежити шкідливе програмне забезпечення і не може оцінювати текст швидко. Відсутність можливості швидкого отримання експертної оцінки вмісту листа може суттєво позначитися на роботи компанії та призвести до збитків [15].

3. Третьою є система виявлення та запобігання атак, заснована на аналізі аномалій. IPS/IDS системи - це пристрої, які призначені для виявлення атак на корпоративну мережу. Підпис у рамках поняття IPS/IDS систем — це набір правил, який зіставляє заздалегідь налаштовані шаблони до пакетів, що проходять через пристрій. Системи виявлення та запобігання вторгненням мають тисячі налаштованих за замовчуванням шаблонів, які потребують лише активації.

З появою все більш витончених атак компанія Cisco Systems постійно створює додаткові шаблони. Ці системи дозволяють проводити перевірку на основі репутації відправника. Даний механізм будується з урахуванням вже скоєних кібер-атак. Пристрій IPS, що функціонує на підставі даного алгоритму, збирає дані з інших систем запобігання вторгненням, які знаходяться в глобальній мережі.

Як правило, блокування здійснюється на підставі IP-адрес, універсальних локаторів ресурсу, або Uniform Resource Locator (URL), доменних систем тощо.

У цьому рішенні важливо відзначити відсутність можливості відстеження вхідних телефонних дзвінків, що робить користувача інформаційної системи вразливим до методів, що ґрунтуються на прямому контакті працівника компанії та зловмисника [16].

Всі вищезгадані реалізації задуманого рішення ігнорують один або кілька типів атак методами соціальної інженерії, що робить компанію вразливою до різних типів атак, тому необхідні додаткові розробки в даній галузі та створення спеціалізованого штучного інтелекту.

2.2. Тестування на проникнення за соціоінженерним підходом з використанням утиліти Social-Engineer Toolkit

Тестування на проникнення за соціоінженерним підходом орієнтоване на автоматизуванні створення і реалізування векторів атак. Для цього використовується інструментальний засіб соціального інженера (Social-Engineer Toolkit, SET).

Social-Engineer Toolkit – це компонент Kali Linux, фреймворк з відкритим вихідним кодом для тестування на проникнення, призначений для соціальної інженерії. SET має ряд векторів атак на запит, які дозволяють вам швидко зробити правдоподібну атаку.

Основні вектори атаки SET:

1) E-mail attack vector

Для використання цієї атаки в головному меню потрібно обрати пункт "Spear-Phishing Attack Vectors".

Для початку потрібно визначитися з кількістю цілей, адже SET надає два режими розсилки:

індивідуальне розсилання;

масове розсилання.

Для *масового розсилання* необхідний заздалегідь сформований файл зі списком цільових адрес. Формат даного файлу дуже простий - одна адреса на рядок, і він знаходиться в /pentest/exploits/SET/config/mailing_list.txt. Процедура схожа на написання звичайного листа — необхідно заповнити тему листа та його зміст. Є можливість створити шаблон і надалі використовувати його при необхідності, щоб кожного разу не повторювати те саме введення.

Що стосується надсилання листа, то тут є три варіанти:

Gmail-аккаунт;

свій Sendmail open-relay;

open-relay сервер – його можна знайти в мережі Інтернет

Завдяки open-relay можна відсилати листи з чужих адрес, але не варто забувати, що жертва може використовувати механізм "reverse lookups", який здатний визначити відповідність доменного імені відправника листа.

Бойове навантаження (Meterpreter Reverse_TCP, Reverse VNC, Reverse TCP Shell) разом з експлойтом прозоро вибираються з metasploit та йдуть усередині приєднаного до листа PDF-файлу, який може бути як заготовкою SET, так і будь-яким твоїм PDF-вкладенням. Залишається підняти listener і чекати, поки людський фактор зіграє злий жарт.

2) Web attack vector

Даний вектор атаки надає більш цікаві, витончені та різнопланові способи атаки на користувачів, ніж перший. Тут можна використовувати загальну межу - підроблену веб-сторінку на веб-сервері, що автоматично піднімається. Хоча сучасні браузери і намагаються боротися проти підроблених сайтів, остаточне рішення про те, чи довіряти чи не довіряти сайту, приймає людина, де зазвичай людей підводить звичайна «неуважність».

Для того, щоб користувач не помітив помилки в адресному рядку, можна застосувати ARP-spoofing.

У такому разі жертва замість оригінального сайту потрапляє на фальшивий сайт.

Також заманити користувача на підроблений сайт можна за допомогою XSS, email-розсилки, дзвінка з техпідтримки провайдера. В принципі тут справа обмежується фантазією пентестера або зловмисника. Говорячи про пошту, варто згадати про перший вектор атаки, який може чудово працювати і через Інтернет. Для цього при розсилці в текст листа додаємо URL, попередньо стислий за допомогою сервісу www.bit.ly (або подібним до нього). Природно, вектор атаки через пошту не надає можливості надсилання нормального файлу, але ніхто не заважає після створення файлу підмінити його на нормальний /pentest/exploits/SET/src/program_junk/<name_file>.pdf.

Так як цей вектор зводиться до створення підробленого сайту та заманювання на нього жертви, то SET бере на себе першу частину плану і справляється з нею на "відмінно", надаючи нам три варіанти створення такого типу сайтів:

Заготовані сайти Gmail, Google, Facebook, Twitter та Java Required

Клонування сайту

Власний сайт

Серед заготованих сайтів, напевно, варто зупинитися тільки на "Java Required", при попаданні на який з'являється сторінка з повідомленням, що для її перегляду необхідна Java, і докладна інструкція про те, як її встановити. Найкраще цей шаблон вибирати при проведенні атаки Java Applet.

Другий режим найлегший - це повне клонування веб-сторінки будь-якого сайту. Для цього достатньо лише повідомити toolkit'у необхідну URL-адресу, а далі — справа техніки. За кілька секунд ми вже маємо копію будь-якої веб-сторінки.

Останній режим дозволяє підняти свій власний сайт, вказавши лише директорію на диску, де він розташований. Тут можна розгорнути як якийсь великий сайт, так і просто сторінку з помилками "404", "Ідуть профілактичні роботи", "Йде завантаження...", "Зміст даного сайту несумісний з вашим браузером, спробуйте відкрити посилання за допомогою IE" . Головне, щоб жертва нічого не запідозрила і якнайдовше пробула на сайті.

Перше, що ми бачимо, зайшовши до пункту web-attack – це *The Java Applet атака*. Java Applet спуфіт підроблений Java Certificate, і, якщо ціль приймає його,

на ній запускається metasploit payload. Найголовнішою перевагою даного методу є те, що нас не цікавить, якою ОС та яким браузером користується користувач, головне, щоб у нього на машині стояла Java.

Ну і, звичайно, експлуатацію вразливостей браузерів ніхто не скасовував, і для цього є пункт *The Metasploit Browser Exploit Method*. Тут SET на створену нами сторінку поміщає експлойт, який чекатиме свого часу. Оскільки більшість нових експлойтів пробивають до IE (не факт, що жертва ним користується), то можна, застосувавши соціальну інженерію, змусити користувача зайти за посиланням саме за допомогою IE - як показує практика, це цілком можливо.

Метод "Credential Harvester" дуже простий як у реалізації, так і в застосуванні, адже його завдання полягає в зборі всієї інформації, яку користувач ввів на сторінці підготовленого нами сайту. Так що за його допомогою дуже просто дізнатись автентифікаційні дані нічого не підозрюваного користувача.

У багатьох людей при серфінгу інтернету відкрито багато вкладок: для відвідуваних сайтів, щоб щось переглянути в майбутньому і т.д. З великою кількістю відкритих вкладок і з часом досить важко згадати, що відкрив сам, а що скинули подивитися по месенджеру. Саме на це і розрахована *Tabnabbing-атака*. Дана атака формує спеціальну сторінку, на якій спочатку написано "Please wait while the site loads...", а потім, коли користувачеві набридає чекати завантаження сторінки, і він перемикається на іншу вкладку в браузері, наша підготовлена сторінка змінить свій вигляд на вигляд сторінки від популярного поштового сервісу, куди потрібно ввести автентифікаційні дані. Вже наступного разу, коли жертва переглядатиме свої вкладки, вона натрапить на знайомий йому інтерфейс і, можливо, захоче перевірити свою пошту в даному вікні. А далі ця сторінка працює аналогічно методу Credential Harvester.

Метод *"Man Left in the Middle Attack*" використовує HTTP REFERER для збору даних із полів, які користувач заповнив на сайті. Цей метод є єдиним, для якого можна не створювати підроблений сайт, але необхідно наявність уразливості типу XSS на реальному сайті, дані з якого нас цікавлять, для її

проведення. Виходить, ми просто використовуємо XSS на реальному сайті в режимі Credential Harvester і отримуємо потрібний нам результат.

3) CD/DVD/USB attack vector

Далеко не у всіх в налаштуваннях відключено автозавантаження, та й LNK-експлойт розповсюджений, тому цей напрямок проникнення в систему досі представляє певний інтерес. SET дозволяє створити потрібний матеріал для такої атаки. Для цього необхідно скористатися пунктом меню Infectious Media Generator, який люб'язно поцікавиться про твої переваги в payload, Encoder, кількості ітерацій кодування навантаження (для AV bypass) і порту для reverse-connect. В результаті в кореневій папці SET з'явиться папка autorun з двома файлами: program.exe (наш payload) і autorun.inf, що запускає program.exe. Записуємо отриманий матеріал на CD/DVD/USB та підсовуємо жертві.

4) Teensy USB hid attack vector

Teensy USB HID (human interface device) – це затратний і витончений вектор атаки. Teensy - це дуже маленький програмований пристрій з mini-USB інтерфейсом. Teensy USB має AVR-процесор з частотою 16 МГц, флеш-пам'ять 32-128 Кб, RAM-пам'ять 2,5-8 Кб і коштує приблизно 400-600 грн, залежно від моделі.

Він запрограмований і визначається в системі як USB-клавіатура, в результаті цього, він може обійти будь-яку заборону автозавантаження і т.д. Також він не потребує спеціальних драйверів і, маючи дуже маленький розмір, може бути непомітно встановлений на комп'ютер, поки власник ПК відволікся. Пристрій має таймер і датчик, що дає можливість запуску через деякий час після встановлення. Єдиним недоліком є те, що він визначається у системі трохи довше, ніж звичайний USB пристрій. SET генерує навантаження в teensy.pde, який потім за допомогою Arduino IDE та Teensy Loader USB заливається на пристрій. Варто відзначити, що як навантаження можна використовувати Powershell HTTP GET MSF, WSCRIPT HTTP GET MSF та Powershell based Reverse Shell.

Перевагами методу з використанням утиліти Social-Engineer Toolkit є: автоматизованість процесу протидії використанню соціальної інженерії та правдоподібність векторів атак.

Недоліком є кваліфікованість і обізнаність користувача (жертви).

2.3. Метод моделювання дій об’єкта та суб’єкта соціоінженерного впливу

Метод моделювання дій об’єкта та суб’єкта соціоінженерного впливу (оптимізація соціальної інженерії(SEO)) орієнтується на виокремлення двох ключових ролей – нападника та захисника. Один з них (нападник) прагне перемогти, а інший (захисник) – протидіяти соціоінженерному впливові. Якщо здатність до протистояння захисника краща, ніж нападника, то їх міняють місцями за результатами порівняння між собою.

Рис. 2.9. Схема використання оптимізатора соціальної інженерії

На рис. 2.9. показана блок-схема запропонованого методу. У цьому алгоритмі кожне рішення є аналогом людини, а риси і навички кожної людини є аналогом усіх змінних кожного рішення в пошуковому просторі. Щоб запустити алгоритм,

два випадкових рішення ініціалізуються, і краще рішення вибирається як атакуючий, а інше називається захисником.

Для імітації навчання та перенавчання захисника в нападника розроблено кілька випадкових експериментів для кожної риси захисника. Нападник намагається перевірити кожну рису захисника, щоб розпізнати найбільш ефективну рису. Аналогом навчання та перенавчання в пошуковому просторі є копіювання ознаки від нападника до тієї ж риси у захисника та обчислення швидкості перенавчання нападника від захисника, одночасно.

Наступний крок - це визначення атаки від нападника до захисника є аналогом зміни позиції захисника розумним способом у можливому просторі. Щоб виявити атаку, розглядаються чотири різні методи, такі як:

отримання - у цій техніці нападник зловживає захисником безпосередньо як керівництво для досягнення бажаних цілей.

фішинг- щоб здійснити цю техніку, зловмисник удає, що наближається до захисника, а потім захисник переміщається до місця, де він хоче бути.

диверсійна крадіжка - у цій техніці зловмисник спочатку наводить захисника на позицію, яка насправді є обманом для захисника.

претекстинг - під час цієї техніки нападник зображає деякі риси, яким довіряє захисник і таким чином керує захисником.

Ці згадані методи використовуються випадковим чином для пошуку можливого простору. Алгоритм розроблений таким чином, що користувач може використовувати одного оператора з чотирьох.

Наступний етап - відповідь на атаку. Нова позиція захисника оцінюється та порівнюється зі старою позицією. Потім вибирається найкраща позиція для захисника, і якщо нова позиція захисника краща за нападника, захисник і нападник обмінюються.

В кінці, щоб завдати удару захиснику, зловмисник знищує захисника і випадковим чином вибирає нову людину для виконання правил SE, він знищується і генерується новим випадковим рішенням у просторі пошуку. У запропонованому SEO етап локального пошуку або експлуатації здійснюється шляхом навчання та

перенавчання між нападником і захисником. Крім того, помічаючи атаку SE та реагуючи на неї, робить дію посилення.

Умовою зупинки може бути максимальний час моделювання або якість найкращого коли-небудь знайденого рішення або інша умова, обрана користувачем [12].

Перевагою використання даного методу є можливість виокремлення ролей як нападника, так і захисника. Проте його результативність залежить від наявних шаблонів атак соціальної інженерії. Як наслідок, можливості запобіганню їх реалізації.

2.4 Метод виявлення і повідомлення про атаки соціальної інженерії людиною за допомогою інструментального засобу Cogni-Sense

Протягом останніх кількох років концепція людського сенсора як датчика знайшла все більше застосування для виявлення загроз та несприятливих умов у фізичному просторі. Ці успіхи у фізичному просторі послужили мотивацією для застосування та оцінки концепції виявлення загроз і в кіберпросторі, особливо для атак семантичної соціальної інженерії, де технічні механізми безпеки традиційно були обмежені за обсягом або точністю.

Фреймворк «людина-як-сенсор-безпеки» (human-as-a-sensor-security(HaaSS)) і практична реалізація у вигляді Cogni-Sense (прототипу програми Microsoft Windows) це експериментальна програма, розроблена для того, щоб дозволити та заохочувати користувачів активно виявляти та повідомляти про атаки семантичної соціальної інженерії проти них.

Для виявлення атак семантичної соціальної інженерії користувачам потрібен інтерфейс, який надає їм функціональні можливості для повторного повідомлення про підозрілу або аномальну активність, яка використовує оманливі вектори атак, а не технічну експлуатацію; для яких людина-користувач часто є більш точним датчиком, ніж технічні системи безпеки організації.

Архітектура Cogni-Sense складається з чотирьох ключових компонентів високого рівня: (1) HaaSS платформа датчиків виявлення (тобто додаток Cogni-Sense), (2) централізованої хмарної платформи для класифікації та реагування на безпеку, (3) інтерфейс центру операцій безпеки (наприклад, веб-браузер), який використовується для доступу до хмарної платформи, та (4) модуль забезпечення безпеки для процесу відповіді на виконання правил, який забезпечує інтеграцію між хмарною платформою та зовнішніми платформами безпеки [13].

Перевагою даного методу є залученість користувачів до активного забезпечення кібербезпеки. Водночас можливе приховування інформації про реалізування атаки соціальної інженерії окремим користувачем. Допоки об’єктом атаки не стане інший користувач.

Висновок з розділу 2

Здійснено аналіз різних методів та технологій протидії соціальному інжинірингу, в тому числі експериментальних, розглянуті їх основні переваги та недоліки.

Встановлено, що методи протидії атакам соціального інжинірингу з використанням людських ресурсів є обов’язковими для компаній, однак людські рішення є відносними і не дуже ефективними, тому для підвищення точності людських методів необхідні методи протидії атакам соціальної інженерії на основі технологій.

Аналізуючи другий розділ, постає необхідним розробити варіант технології протидії соціальному інжинірингу на об’єктах інформаційної діяльності. Для цього необхідно провести симуляцію фішингової атаки на базі утиліти Sophos Phish Threat та розробити рекомендації щодо ефективного використання даної технології.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ПРОТИДІЇ СОЦІАЛЬНОМУ ІНЖИНИРІНГУ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ НА БАЗІ SOPHOS PHISH THREAT

3.1. Технологія управління утилітою Sophos Phish Threat та проведення на її базі симуляції фішингової атаки на об'єкті інформаційної діяльності в умовах дистанційної роботи співробітників

3.1.1. Опис технології Sophos Phish Threat

Phish Threat є частиною Sophos Central, хмарної уніфікованої консолі безпеки. Рішення Sophos Central реалізовано за принципом Synchronized Security (SynSec) або Security Heartbeat, в якому процес забезпечення інформаційної безпеки це єдина система, де кожен компонент забезпечення інформаційної безпеки з'єднаний один з одним в реальному часі.

Технологія Security Heartbeat (Рис. 3.10.) забезпечує зв'язок між компонентами безпеки, забезпечуючи спільне функціонування системи та її моніторинг.

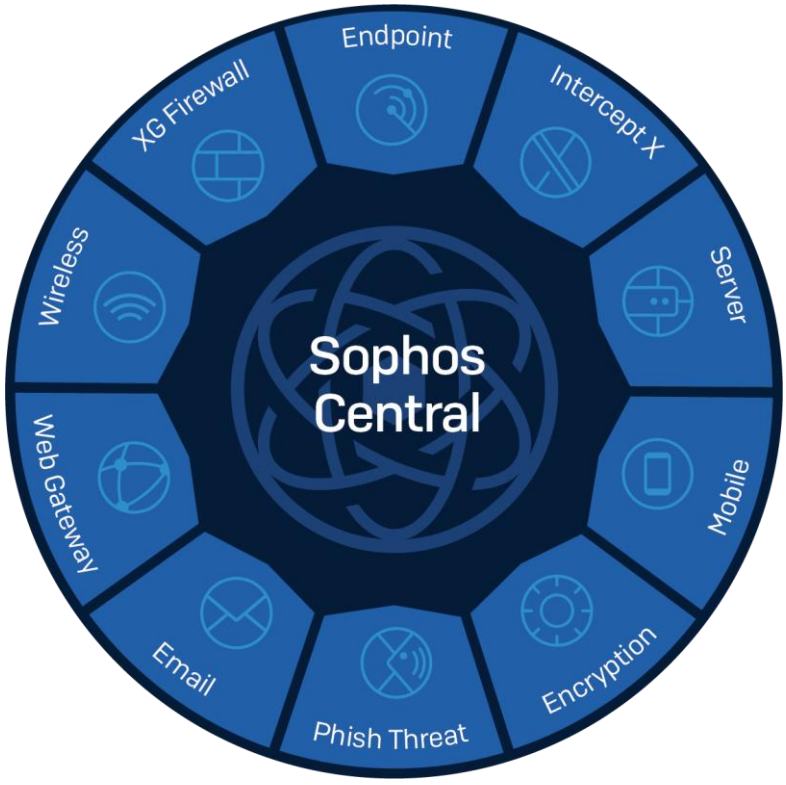


Рис.3.10. Рішення інтегровані у Sophos Central

У Sophos Central інтегровані рішення наступних класів:

Endpoint Protection – класичний сигнатурний антивірус;

Server Protection – спеціалізований антивірус для серверів;

Intercept-X – антивірус нового покоління (без сигнатур та з технологіями штучного інтелекту);

Sophos XG Firewall – фаєрвол нового покоління;

Mobility Management (EMM) — управління мобільними пристроями та контроль доступу до корпоративної пошти та файлів;

Data Protection (Encryption);

Secure Wi-Fi - точки доступу, що керуються як з хмари, так і локально через Sophos UTM / Sophos XG;

Web Security – класичне рішення для фільтрації веб-трафіку;

E-mail Security - хмарне/локальне анти-спам/антивірус рішення;

Phish Threat – підвищення обізнаності співробітників, проведення тестових фішингових розсилок;

Cloud Optix – аудит хмарних інфраструктур.

У Sophos Central концепція SynSec базується на трьох важливих принципах:

1) Виявлення (виявлення невідомих загроз) - продукти Sophos під керуванням Sophos Central в автоматичному режимі діляться інформацією між собою для виявлення ризиків і невідомих погроз, що включає в себе: (1) аналіз мережевого трафіку з можливістю ідентифікувати додатки з високим ризиком та шкідливий трафік; (2) виявлення користувачів із високою групою ризику шляхом кореляційного аналізу їхніх дій у мережі.

2) Аналіз (миттєвий та інтуїтивний) - аналіз інцидентів у режимі реального часу забезпечує миттєве розуміння поточної ситуації в системі. Відображення повного ланцюжка подій, які призвели до інциденту, включаючи всі файли, ключі реєстру, URL-адреси і т.д.

3) Реагування (автоматичне реагування на інциденти) - налаштування політик безпеки дозволяє в автоматичному режимі за лічені секунди реагувати на зараження та інциденти. Це забезпечується: (1) миттєвою ізоляцією заражених

пристроїв та зупинкою атаки в режимі реального часу (навіть у межах однієї мережі/широкомовного домену); (2) обмеження доступу до мережевих ресурсів компанії для пристроїв, які не відповідають політикам; (3) віддалений запуск сканування пристрою при виявленні вихідного спаму.

Ми розглянули основні принципи захисту, на яких ґрунтується робота Sophos Central. Тепер перейдемо до опису технологія Sophos Phish Threat, яка цікавить нас в рамках кваліфікаційної роботи.

Sophos Phish Threat навчає та перевіряє кінцевих користувачів за допомогою:

1) автоматизованих симуляцій атак - імітує низку типів фішингових атак, щоб допомогти виявити слабкі місця в системі безпеки організації. Є можливість змоделювати понад 500 реалістичних і складних фішингових атак всього за кілька кліків.

Аналітики Sophos Labs щодня відстежують мільйони електронних листів, URL-адрес, файлів та інших точок даних на предмет останніх загроз. Цей постійний потік інформації гарантує, що навчання користувачів охоплює поточну тактику фішингу з соціально релевантними шаблонами моделювання атак, які охоплюють кілька сценаріїв.

2) якісного навчання щодо безпеки - посилення безпеки організації та можливості користувачів розширюються шляхом демонстрації понад 60 інтерактивних навчальних модулів, які навчать співробітників як діяти при конкретних загрозах, таких як підозрілі електронні листи, збір облікових даних, надійність пароля та відповідність нормативним вимогам.

3) ефективних показників звітності - інформаційна панель Phish Threat надає миттєві результати кампанії щодо вразливості користувачів і дозволяє вимірювати загальні рівні ризику для всієї групи користувачів за допомогою реальних даних про фактор поінформованості, зокрема, результати проведених кампаній, покриття тестування, кількість днів з останньої кампанії. Детальні звіти надають глибше уявлення про ефективність на рівні організації або окремого користувача.

Надбудова Outlook, що входить до комплекту, надає користувачам можливість повідомляти про імітовані атаки прямо з папки "Вхідні", що дозволяє відстежувати справжню обізнаність у папці "Вхідні", надаючи нове уявлення про систему безпеки організації.

Утиліта Sophos Phish Threat на своїй панелі управління має 3 розділи:

1) Розділ «Аналіз» складається з двох вкладок:

Dashboard (Інформаційна панель) – тут міститься інформація про активні кампанії, показники поінформованості користувачів та відповідність навчанню.

Reports (Звіти) – тут показується статистика про користувачів, які: зареєстровані у імітованій кампанії атаки; піддались атаці; кілька разів піддались атаці; повідомили про загрози під час імітованих атак; відкрили електронний лист із моделюванням атаки і не повідомили про це; ввели облікові дані під час імітованої атаки; відкривали вкладення під час імітованої атаки; пройшли навчання; не пройшли один або кілька тренінгів.

2) Розділ «Управління» складається з двох вкладок:

People (Люди) – тут відображається інформація про доданих користувачів та групи користувачів, а саме: їх ім’я, поштова адреса, логін обміну, остання активність, приналежність до групи, роль в програмі. В цій вкладці можна додавати нових користувачів різними способами: вручну, імпортувати їх з CSV файлу, синхронізувати з Active Directory, або Azure AD. Також в цьому розділі можна надсилати персональний лист користувачу, з інструкцією для розгортання цієї програми в себе на комп’ютері і надавати користувачам різні ролі (Super Admin матиме повний доступ до всього; An Admin, Read-only Admin, і Custom Admin матимуть повний та відповідно обмежений доступ лише для читання до певних наборів функцій. User матиме доступ лише до порталу самообслуговування)

Campaigns (Кампанії) – тут можна створити нову кампанію атаки або серію атаки. Також на вкладці відображається інформація про: активні, заплановані, попередні та чернетки кампаній.

3) Розділ «Конфігурація» - в цьому розділі єдина вкладка:

Settings (Налаштування) – тут можна; керувати налаштуваннями служби каталогів; керувати конфігурацією надбудови Outlook, щоб кінцеві користувачі повідомляли про підозрілі електронні листи; переглядати домени та IP-адреси для внесення в білий список; надсилати нагадування електронною поштою вибраним адміністраторам перед запуском кампанії; налаштовувати домен надсилання для автоматичної реєстрації на навчання та електронних листів з нагадуванням.

3.1.2 Симуляція фішингової атаки на базі Sophos Phish Threat

За допомогою Sophos Phish Threat можна провести аудит - симулювати фішингову атаку і перевірити, наскільки співробітники компанії схильні до цього типу загроз.

Аудит проводився з дозволу керівника компанії, на базі якої я проходила переддипломну практику. Про його хід було проінформовано тільки керівництво вищого рівня.

Для тестування були відібрані співробітники з відділу кадрового та адміністративного забезпечення (4 людини) і відділу бухгалтерії (3 людини), які працюють з фінансами компанії та фінансово-обліковою інформацією, нараховують співробітникам зарплати, мають доступ до персональних даних. Вони не мають технічної освіти і обізнаності в кібербезпеці та кібергігієні.

Перш ніж створювати першу кампанію, потрібно переконатися, що IP-адреси та домени Sophos Phish Threat для надсилання додані в білий список на шлюзі електронної пошти, пристрої брандмауера чи будь-якому іншому місці, де фільтрується вхідна електронна пошта та веб-трафік.

Тепер перейдемо до створення фішинг розсилки — на вкладці Campaigns натискаємо кнопку «New Campaign». Процес поділений на етапи, зверху можна побачити їхнє проходження.

На першому етапі (Рис. 3.11.) необхідно вказати назву кампанії (в нашому випадку це «Співробітники кадрів та бухгалтерії»), потім вибрати тип розсилки. Це може бути:

Phishing - заманювання цільового користувача натиснути посилання в електронному листі.

Credential Harvesting – заманювання цільового користувача ввести облікові дані на підробленому веб-сайті. Зверніть увагу, що паролі не збираються.

Attachment - заманювання цільового користувача відкрити вкладений файл в електронному листі.

Training - зареєструвати цільового користувача для обов'язкового навчання на основі обраних навчальних модулів.

В рамках кваліфікаційної роботи вибрано тип розсилки «Phishing». Також на цьому етапі можна вибрати мову розсилки.

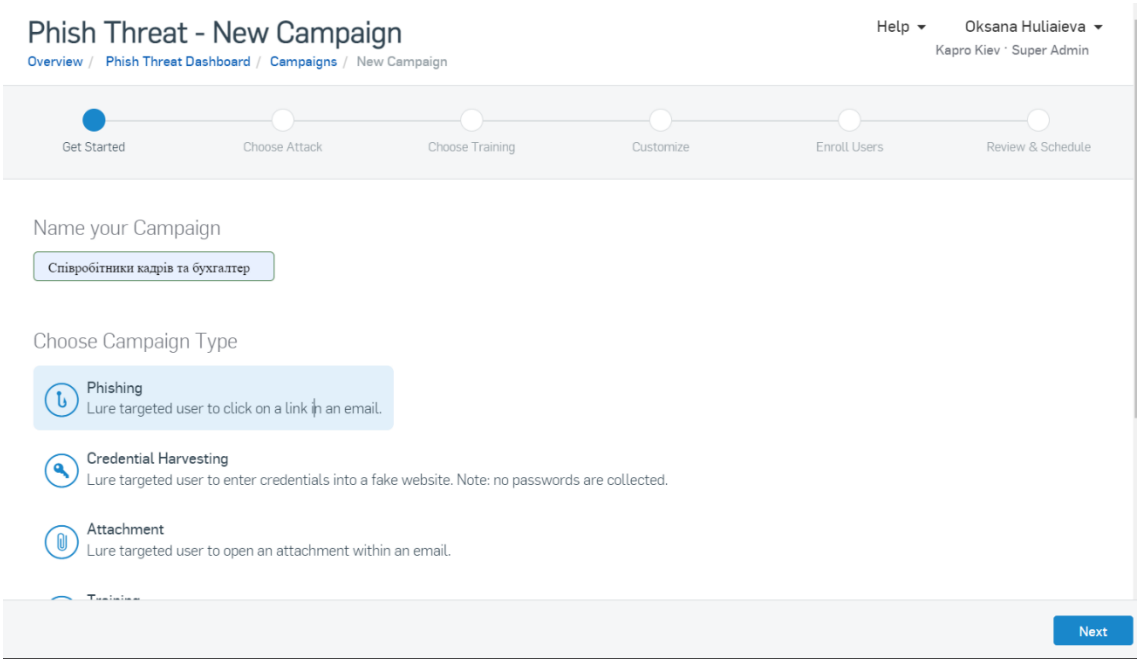
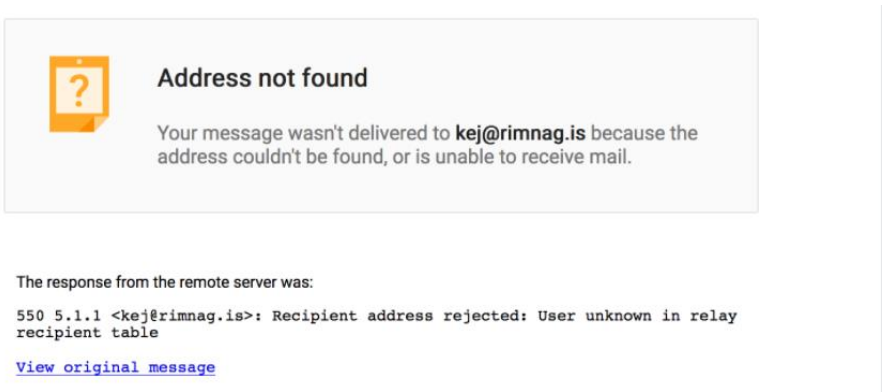


Рис. 3.11. Перший етап створення кампанії фішингової атаки

На другому етапі вибираємо шаблон фішингового листа. У цьому відношенні Sophos має велику різноманітність для вибору. Аналітики SophosLabs відстежують останні тенденції реальних атак та регулярно оновлюють шаблони. Тут є можливість замаскувати свою кампанію. Можна вибрати до 5 атак, і кожен зареєстрований користувач отримає один випадково вибраний електронний лист.

В нашому випадку вибрано атаку «Address Not Found» - вона означає що, користувач отримає лист з наступним змістом (Рис. 3.12). В листі підставимо адресу, на яку користувач потенційно міг відправляти електронний лист (керівнику, колезі).



Рим 3.12. Зміст листа для атаки «Address Not Found»

На третьому етапі необхідно вибрати тренінг для користувача, який буде продемонстрований йому як навчальний матеріал. На даний момент тренінги не доступні українською або російською, тому можна використовувати їх як базу для створення власних семінарів усередині компанії. Можна також задати URL на власний внутрішній тренінг, наприклад, у внутрішній базі знань.

На цьому етапі вибрано відео-тренінг під назвою «Intro To Phishing».

На четвертому етапі кастомізуємо нашу розсилку. Прописуємо ім'я та адресу електронної пошти, які будуть вказані як відправник, редагуємо шаблон листа – можемо вставити потрібні картинки та написати текст будь-якою мовою.

На цьому етапі адресу відправника вказуємо no-reply@gmailmsg.com, а в тілі листа (Рис. 3.12) змінюємо електронну адресу на ksuhabadrak@gmail.com

На п'ятому етапі вибираємо користувачів/групи - тут ми можемо вибрати релевантний відділ, для якого готували шаблон листа. Зверніть увагу, що користувач повинен мати адресу електронної пошти з доменним ім’ям компанії. Адреса електронної пошти з загальнодоступним доменним ім’ям (gmail.com, yahoo.com) не допускаються до використання.

На шостому етапі вказуємо часовий інтервал, в який буде проводитися розсилка фішингу. Можна розіслати листи всім користувачам одночасно, а можна зробити більш хитро - відправляти поступово, наприклад по 20% кожні 2 години (всього - 5 годин на всю розсилку). Це корисно при великій кількості користувачів і щоб не всі користувачі одночасно отримали один і той же лист.

Ще раз перевіряємо правильність вказаних даних і натискаємо заповітну кнопку Done. Ось такий вигляд має фішинговий лист, який надійшов колегам (Рис.

3.13.). При переході за посиланням відкривається сторінка з написом «This wasn’t a real attack, but it could have been» і кнопка, для переходу на сторінку тренінгу.

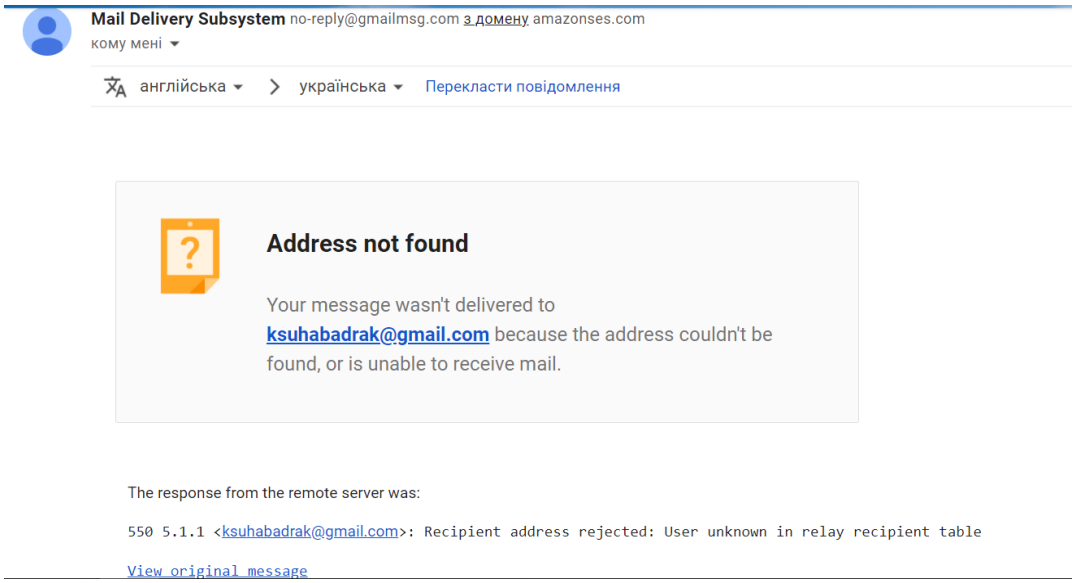


Рис. 3.13. Вигляд фішинг листа, який надійшов колегам

3.2. Аналіз результатів атаки

У звіті про розсилку фішингових листів відображаються типи пристроїв, що зазнали атаки, кількість розісланих повідомлень, відкритих повідомлень, відсоток користувачів, які перейшли за посиланням і відсоток користувачів які пройшли навчання. Також можна побачити, хто з користувачів найшвидше відкрив фішинговий лист.

Кінцевий користувач приймає рішення про те, чи відкривати вкладення, чи проходити за посиланням.

Аналізуючи звіт про атаку проведену нами (Рис. 3.14) можна побачити, що всі 7 листів було доставлено, 7 співробітників відкрили лист, 5 людей перейшло за посиланням і тільки 1 людина повністю пройшла навчання.

Критичний показник переходу за посиланням у 71% показує, що більша половина співробітників відділу погано обізнана в питаннях соціальної інженерії, і як наслідок, персональні дані співробітників, фінансово-облікова інформація та фінанси компанії знаходяться під загрозою.

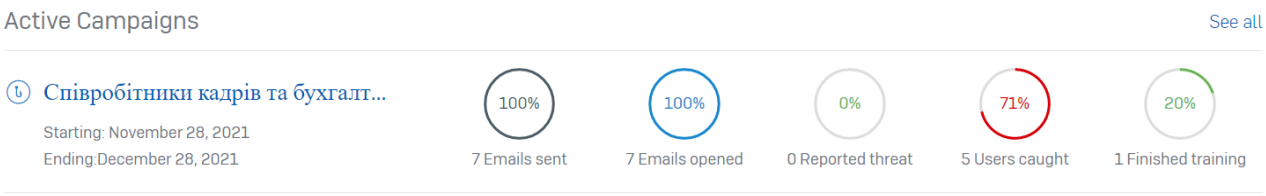


Рис. 3.14. Звіт про розсилку фішингових листів

Також на дашборді видно що 43% людей відкрило лист через ПК і 57% через мобільний пристрій. Також видно, що 80% співробітників перейшло за посиланням через мобільний пристрій.

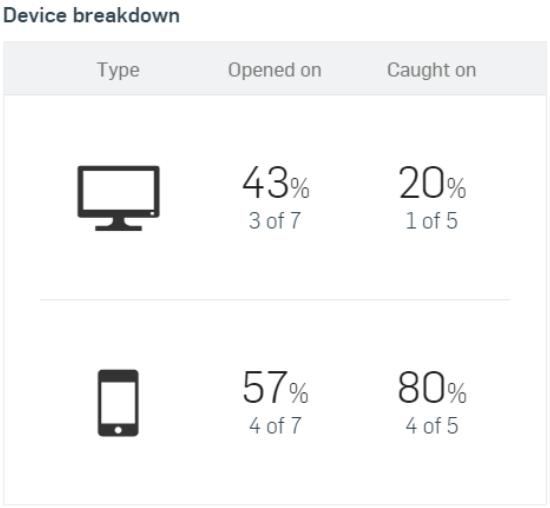


Рис. 3.15. Дашборд розподілу пристроїв

Багато людей думають, що їх смартфони більш безпечні, ніж комп'ютери. Як зазначає WillisWire кіберзлочинність, спрямована на мобільні пристрої, стрімко розвивається, як і використання мобільних пристроїв.

Одним із факторів ризику є те, що ви використовуєте свій смартфон на ходу, часто, коли відволікаєтеся або поспішайте.

3.3. Розроблення рекомендацій щодо застосування технології протидії соціальному інжинірингу на об’єктах інформаційної діяльності використовуючи інструменти утиліти Sophos Phish Threat

В роботі розглянули інструмент Sophos Phish Threat для проведення фішингової розсилки в компанії, який є досить гнучким в налаштуваннях, і, крім іншого, містить тренінги для профілактики реальних фішингових атак у майбутньому.

Проаналізувавши реальні відгуки користувачів утиліти, виділила основні її переваги та недоліки:

Переваги:

1) Простота інтеграції за допомогою стандартних API та інструментів;
2) Простота розгортання та використання;
3) Низька вартість в порівнянні з конкурентами;
4) Наявність готових шаблонів, які неймовірно корисні для команд SOC з нестачею ресурсів, а також для управлінських команд, які вимагають швидкого результату;
5) Можливість адаптувати шаблони або створювати суто користувацькі шаблони, що дає змогу націлюватися на певні відділи або на певних співробітників в організації;
6) Можливість імітації внутрішньої пошти компанії, щоб визначити сфери необхідного навчання;
7) Звіти з кампаній, які дозволяють визначати часові рамки та тенденції показників, оцінювати ризики, завдяки яким можна легко побачити рентабельність інвестицій з часом;
8) Використовуючи програму, немає необхідності звертатись до сторонніх компаній для проведення пентесту, які тягнуть за собою додаткові витрати;

Недоліки:

1) Деякі з готових навчальних матеріалів занадто короткі, мають дилетантський вигляд та не глибокий сенс;
2) Служба підтримки Sophos не прислухається до скарг користувачів, не вирішує і не визнає проблеми, не надає зворотного зв’язку;
3) Невеликий вибір тестових сценаріїв, відсутність деяких важливих шаблонів тестування, мало готових інтерактивних навчальних модулів, але багато пасивного відеонавчання;
4) Не має готових начальних модулів та відео російською чи українською мовою;

5) Навчання триває лише до тих пір, поки кампанія розсилає електронні листи;

6) Погано працює у великих організаціях, чудово підходить для невеликих компаній;

7) Не інтегрується з власним інструментом корпоративного навчання;

Рекомендації щодо застосування технології Sophos Phish Threat

1) Потрібно якісно спланувати стратегію протидії атакам CI, щоб використовувати інструмент більш ефективно. Більшість організацій використовують утиліту без стратегії;

2) Використовуйте кілька шаблонів для фішингу в одній кампанії, щоб ваші користувачі не могли попередити один одного про тест;

3) Атаки проводьте згідно чіткого плану, поступово та в різних відділах.

4) Зробіть технологію *Sophos Phish Threat* частиною ваших поточних операцій безпеки та стратегій навчання. Її потрібно використовувати регулярно, а не раз на рік, щоб справити враження на керівників.

5) Подбайте про те, щоб шлюз електронної пошти, пристрої брандмауера чи будь-яке інше місце, де фільтрується вхідна електронна пошта та веб-трафік не блокувала жодні посилання чи повідомлення від Sophos.

6) Встановіть спочатку пробну версію продукту (на 1 місяць), щоб впевнитись що інфраструктура Sophos підходить для ваших потреб.

7) Створюйте власні навчальні модулі для користувачів, які не пройшли тест на фішинг українською чи російською мовою.

Підчас вибору технології Sophos Phish Threat, користувачі порівнювали її з іншими, серед яких: технології безпеки Wombat, Mimecast, KnowBe4 (MediaPRO), F-Secure, Trustwave, CyberVista, PhishLabs, Proofpoint, PhishingBox, Barracuda, Kaspersky, Rapid7, Global Learning Systems, SecurityAdvisor, Cofense.

Необхідно пам'ятати, що фішинг насамперед спрямований на персонал із низьким рівнем грамотності у сфері інформаційної безпеки. Але це не означає, що на прийоми хакерів не ведуться співробітники ІБ- та ІТ-компаній. Від атаки не застраховано ніхто. Чим вища і важливіша посада, тим більший інтерес жертва

становить. Потрібно тримати співробітників у тонусі, перевіряючи їх обізнаність, регулярно нагадувати про можливі ризики та проводити навчання. Для тренінгів можна використовувати блок схему виявлення фішингу (Рис. 3.16.), щоб користувачі могли вміти розпізнати фішингові листи і бути впевнені в тому, що не стануть жертвою фішингу.

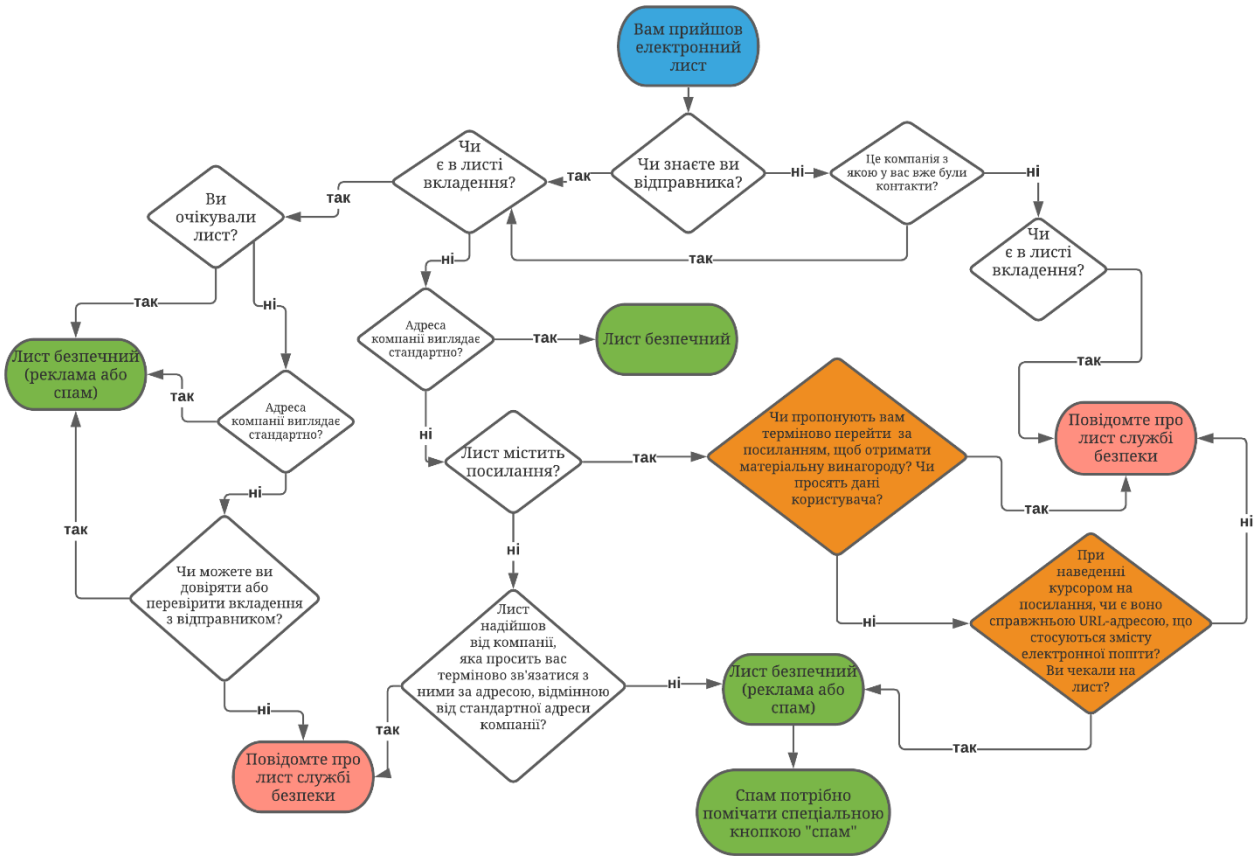


Рис. 3.16. Блок схема виявлення фішингу

Нижче наведені рекомендації для виявлення фішинг-листів.

1. *Зверніть увагу на відправника*. Рішення для захисту електронної пошти зазвичай довіряють нещодавно створеним доменам електронної пошти, які ще не були помічені як небезпечні, тому краще сподіватися на себе та перевіряти легітимність домену. Зловмисник може зареєструвати домен, схожий на домен вашої компанії. Крім того, подивіться – чи справді такий відправник існує? Бухгалтерія, ІТ-відділ, відділ маркетингу – чи з цієї адреси від них зазвичай надходять листи? І, нарешті, якщо в полі “Відправник” стоїть незнайома адреса, не зайвим буде уточнити у більш обізнаних осіб: чи справді такий працівник існує?

2. *Зверніть увагу на тон і стиль листа.* Зазвичай зловмисники намагаються зробити свої листи гранично нейтральними, щоб мінімізувати кількість ознак, за якими можна відрізнити фальшиве повідомлення від сьогодення. Згадайте, в якому стилі зазвичай витримано листи від умовного відділу технічної підтримки? Чи схожий на них лист, який ви отримали? Можливо, тон занадто офіційний чи, навпаки, неформальний?

3. *Не переходьте за сумнівними посиланнями.* Припустимо, вам надійшов лист із повідомленням про поставлене в Jira завдання від незнайомого колеги або про те, що хтось поділився з вами файлом у корпоративній системі. Не переходьте безпосередньо за посиланнями, якщо не впевнені у справжності такого листа. Ви завжди можете увійти в потрібну корпоративну систему звичним способом і виявити оновлення та сповіщення там.

4. *Уточніть у колег.* Якщо лист виглядає правдоподібним, але ви все одно сумніваєтеся, не соромтеся звернутися за допомогою до колег. Запитайте у сісадміну, чи вони тестують оновлення? Напишіть головному бухгалтеру і поцікавтеся, чи змінилися правила нарахування премії? Не треба боятися зайвий раз виявити пильність, адже це мале зусилля з вашого боку може запобігти величезним збиткам для компанії.

5. *Попередьте службу безпеки.* Якнайшвидше попередьте службу безпеки вашої компанії, особливо якщо ви потрапили на прийом і ввели свої справжні логін і пароль або запустили макроси. Можливо, це помилкова тривога або навіть навчання, які проводяться вашою компанією, а можливо реальна атака. У такому разі, чим раніше вжито заходів, тим краще. Були випадки, коли подальше проведення атаки ставало неможливим саме через своєчасне звернення співробітників до служби безпеки.

6. *Пройдіть навчання з протидії соціальній інженерії.* Беріть активну участь у навчальних програмах вашої компанії та підвищуйте рівень обізнаності. Фантазія зловмисників безмежна, а отже, і заходи захисту мають розвиватися та своєчасно впроваджуватися у виробничий процес. Навчання та пильність – ключ до успіху.

7. *Удосконаліть технічні заходи*. Це можна зробити в рамках своїх можливостей та обов'язків, а також звернувшись за допомогою до відділу технічного забезпечення та підтримки вашої компанії. Не лінуйтеся змінювати паролі, у яких минув термін давності, не ігноруйте положення політики ІБ. Не розповсюджуйте в соціальних мережах інформацію, яка може допомогти зловмисникам провести атаку на вас як на співробітника компанії (старі-добрі фотографії перепусток та бейджів).

8. *Вчасно оновлюйте ПЗ та ОС на вашій робочій станції.* Не соромтеся уточнити, якщо не особисто, то через відділ, що забезпечує безпеку. Не треба боятися здатися смішним, оскільки зловмисники часто використовують образ людей, наділених великими повноваженнями, а отже, у певний момент саме ваша пильність може врятувати ситуацію.

Висновки з розділу 3:

Здійснено аналіз технології управління утилітою Sophos Phish Threat та проведено на її базі симуляцію фішингової атаки на об’єкті інформаційної діяльності в умовах дистанційної роботи співробітників. Виходячи з результатів атаки розроблено рекомендації щодо застосування технології протидії соціальному інжинірингу на об’єктах інформаційної діяльності та блок-схему виявлення фішингових листів.

Для розробки рекомендацій розглянуто основні переваги та недоліки технології протидії соціальному інжинірингу, проаналізовано всі можливі подібні технології захисту від атак соціальної інженерії.

ВИСНОВКИ

Розроблено варіант технології протидії соціальному інжинірінгу на об’єктах інформаційної діяльності на базі Sophos Phish Threat.

В ході виконання поставлених задач отримано наступні наукові та практичні результати:

– шляхом аналізу вимог нормативних документів у сфері соціальної інженерії та дослідження існуючих методів та засобів захисту протидії соціальному інжинірингу на об’єктах інформаційної діяльності в умовах дистанційної роботи співробітників було виявлено необхідність в розробці рекомендації щодо застосування простої та ефективної технології протидії методам соціальної інженерії;

– розглянуто теоретичні аспекти створення різноманітних технологій протидії методам соціального інжинірингу, проаналізовано технічні засоби захисту від соціального інжинірингу;

– здійснено аналіз технології управління утилітою Sophos Phish Threat та проведено на її базі симуляцію фішингової атаки на об’єкті інформаційної діяльності в умовах дистанційної роботи співробітників;

– виходячи з результатів атаки розроблено рекомендації щодо застосування технології протидії соціальному інжинірингу на об’єктах інформаційної діяльності;

– розроблено блок-схему виявлення фішингових листів для використання її у процесі навчання співробітників.

ПЕРЕЛІК ПОСИЛАНЬ

1. Phishing [Електронний ресурс]: Types of Cyber Threat / ESET, spol.s r.o - Режим доступу: World Wide Web. – URL: https://www.eset.com/uk/types-of-cyber-threats/phishing/

2. Мітнік Кевін Д. Мистецтво обману / Кевін Д. Мітнік, Вільям Л. Саймон. – М.: Компанія АйТі, 2004. – 360 с

3. Ездаков А. Як захистити інформацію / А. Ездаков // Мережі. - 2010. № 8. - с. 11-19.

4. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. — К.: ДУТ, 2015.— 288 с.

5. Кузнецов М. В. Социальная инженерия и социальные хакеры: учебник / М. В. Кузнецов, И. В. Симдянов. - СПб.: БХВ-Петербург, 2007. – 10 с.

6. Skileo. Про фішинг… [Електронний ресурс] - Режим доступу: World Wide Web. – URL: https://www.skileo.com.ua/pro-fishynh/

7. Актуальные киберугрозы: III квартал 2021 года [Электронный ресурс]: Аналитические статьи / Positive Technologies - Режим доступу: World Wide Web. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q3/

8. Phishing Activity Trends Report 2th Quarter 2021 [Електронний ресурс] / APWG - Unifying the Global Response To Cybercrime - Режим доступу: World Wide Web. – URL: https://docs.apwg.org/reports/apwg_trends_report_q2_2021.pdf

9. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою: ДСТУ ISO/IEC 27001:2015 Введ. 2015.12.18. – К.: ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості», 2015. – 22 с.

10. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки: ДСТУ ISO/IEC 27032 - 2016. Введ. 2018.01.01. – К.: ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості», 2018. – 44 с.

11. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" [текст]: Указ Президента України №447 від 26 серпня 2021 року [Електронний ресурс] / Верховна Рада України – Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text

12. Fathollahi-Fard M. A., Hajiaghaei-Keshteli M., Tavakkoli-Moghaddam R., ”The Social Engineering Optimizer (SEO)”, Engineering Applications of Artificial Intelligence. 2018. Vol. 72, P. 267-293.

13. Heartfield R., Loukas G., “Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework”. Computers & Security. 2018. Vol. 76, P. 101–127.

14. AVAST. A New Toy in the Avast Research Lab [Електронний ресурс] - Режим доступу: World Wide Web. – URL: https://blog.avast.com/2012/12/03/new-toy-research-lab/

15. An algorithm that mimics our tribal instincts could help AI learn to socialize [Електронний ресурс]: MIT Technology Reviev - Режим доступу: World Wide Web. – URL: https://www.technologyreview.com/2019/01/22/103542/an-algorithm-that-mimics-our-tribal-instincts-could-help-ai-learn-to-socialize/

16. Системы обнаружения и предотвращения вторжений [Электронный ресурс]: ИТ БАЗА ЗНАНИЙ / Мерион Нетворкс - Режим доступу: World Wide Web. – URL: https://wiki.merionet.ru/seti/2/ids-ips/