НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2024 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»

спеціальності 125 «Кібербезпека»

на тему: Оцінка впливу атаки соціальної інженерії на кібербезпеку підприємства

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-05
(шифр групи)

Ковальов Данііл Костянтинович
(прізвище, ім'я, по батькові) (підпис)

Керівник д.т.н., професор Ланде Дмитро Володимирович
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент к.ф-м.н., доцент Хмельницький Микола Олексійович
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2024 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ
ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

«___»_____2024 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Ковальову Даніілу Костянтиновичу
(прізвище, ім'я, по батькові)

1. Тема роботи: «Оцінка впливу вектору атаки "Соціальна інженерія" на кібербезпеку підприємства.»,
   керівник роботи: Ланде Дмитро Володимирович, доктор технічних наук, професор кафедри інформаційної безпеки

затверджені наказом по університету від « 31 » травня 2024 р. № 2251-с

2. Термін подання здобувачем вищої освіти роботи: 11 червня 2023 р.

3. Вихідні дані до роботи: Попередні дослідження та література на тему оцінки впливу атаки соціальної інженерії на кібербезпеку підприємства

4. Зміст роботи:

Аналіз атак соціальної інженерії на підприємства та вимоги стандартів безпеки, використання симуляції соціальної інженерії для оцінювання ризиків кібербезпеки підприємства. , реалізація симуляції оцінки впливу соціальної інженерії на кібербезпеку

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація

6. Дата видачі завдання: 29 січня 2024 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Формулювання теми дипломної роботи, визначення мети та постановка задач	24.09.2023 – 10.12.2023	Виконано
2	Узгодження теми	12.12.2023 - 15.12.2023	Виконано
3	Визначення структури дипломної роботи	12.01.2024 – 16.01.2024	Виконано
4	Отримання завдання	29.01.2024-30.01.2024	Виконано
5	Ознайомлення з рекомендованою літературою	14.02.2024-19.02.2024	Виконано
6	Робота над першим розділом дипломної роботи	28.02.2024-15.03.2024	Виконано
7	Робота над другим розділом дипломної роботи	20.04.2024-30.04.2024	Виконано
8	Робота над третім розділом дипломної роботи	01.05.2024-18.05.2024	Виконано
9	Аналіз отриманих результатів	19.05.2024-22.05.2024	Виконано
10	Оформлення дипломної роботи	25.05.2024-09.06.2024	Виконано

Здобувач вищої освіти _____ Данііл Ковальов
(підпис) **(Власне ім'я, ПРІЗВИЩЕ)**

Керівник роботи _____ Дмитро Ланде
(підпис) **(Власне ім'я, ПРІЗВИЩЕ)**

РЕФЕРАТ

Дипломна робота має обсяг 58 сторінок, містить 23 рисунка, 12 літературних джерел.

Мета роботи: : проведення оцінки стану кібербезпеки підприємства на атаку соціальної інженерії

Об’єкт дослідження: персонал та системи захисту підприємства від атак соціальної інженерії

Предмет дослідження: метод та техніки оцінки впливу на інфраструктуру атаки соціальної інженерії.

Ключові слова: оцінка , соціальна інженерія, кібербезпека

ABSTRACT

The thesis is 57 pages long, contains 23 figures and 12 references.

Purpose of the work: to assess the state of cybersecurity of the enterprise against social engineering attacks

Object of research: personnel and enterprise protection systems against social engineering attacks

Subject of research: methods and techniques for assessing the impact of social engineering attacks on the infrastructure.

Keywords: assessment, social engineering, cybersecurity

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 8

ВСТУП 9

1 АНАЛІЗ АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ПІДПРИЄМСТВА ТА ВИМОГИ СТАНДАРТІВ БЕЗПЕКИ 11

1.1 Основні поняття про соціальну інженерію, її види та наслідки 11

1.2 Вимоги стандартів безпеки щодо протидії соціальної інженерії 14

Висновки до розділу 1 17

2 ВИКОРИСТАННЯ СИМУЛЯЦІЇ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ДЛЯ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТА. 19

2.1Використання атаки соціальної інженерії, як інструмент для оцінки обізнаності персоналу та стану впровадження безпекових заходів 19

2.2 Методика проведення атаки соціальної інженерії для оцінки впливу на кібербезпеку підприємства 22

2.3 Пропозиція реалізації оцінки впливу соціальної інженерії на кібербезпеку підприємства 30

Висновки до розділу 2 32

3 РЕАЛІЗАЦІЯ СИМУЛЯЦІЇ ОЦІНКИ ВПЛИВУ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА КІБЕРБЕЗПЕКУ ПІДПРИЄМСТВА 34

3.1 Опис загальної структури стеку симульованого підприємства 34

3.2 Кроки підготовки для проведення атаки соціальної інженерії на підприємство 35

3.3 Проведення кампанії з соціальної інженерії 39

3.4 Аналіз результатів проведених кампаній та оформлення звіту з оцінки впливу атаки соціальної інженерії 42

Висновки до розділу 3 44

ВИСНОВКИ 46

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ 47

ДОДАТОК А 49

ДОДАТОК Б 53

ДОДАТОК В 56

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

HTML - HyperText Markup Language

SAAS - Software as a Service

SIEM - Security Information and Event Management

EDR - Endpoint Detection and Response

AICPA SOC - American Institute of Certified Public Accountants System and Organization Controls

YAML - YAML Ain't Markup Language

MITM - Man-In-The-Middle

ВСТУП

Інтернет став невід’ємною частиною нашого життя, він повністю інтегрувався у всі сфери людського існування, технології розвиваються з неперевершеною швидкістю кожного дня. Людство почало використовувати свої навички для спроби атак на різну інформаційну інфраструктуру з метою викрадення конфіденційних даних або інформації. Це найбільша загроза серед кібератак, з якими стикається світ на сьогоднішній день. Вона включає в себе обман людей з метою отримання доступу до даних та інформації , що призводить до небезпечних кібератак.

Актуальність роботи: Атаки, що використовують методи соціальної інженерії, становлять серйозну загрозу для кібербезпеки підприємств. Вони дозволяють зловмисникам отримувати доступ до конфіденційної інформації та критично важливих ресурсів, маніпулюючи людським фактором. Це підсилює вразливість підприємства до інших типів атак і може мати катастрофічні наслідки для його функціонування. Розуміння меж стійкості до впливів соціальної інженерії є ключовим для створення ефективних захисних механізмів та превентивних заходів. Моделювання відповідних атак та аналіз їх наслідків є актуальним завданням для підвищення загального рівня кібербезпеки підприємства.

Мета роботи: Проведення оцінки стану кібербезпеки підприємства на атаку соціальної інженерії

Мета досягається шляхом вирішення наступних задач:

1. Аналіз атак на підприємства , основних векторів та сценаріїв таких виконуваних атак.
2. Аналіз вимог стандартів безпеки, щодо проведення оцінки впливу соціальної інженерії.

3. Створення моделі симуляції оцінки впливу соціальної інженерії за допомогою проведення атаки на умовне підприємство
4. Створення звітності щодо проведених дій та надання рекомендацій

Об’єкт дослідження: персонал та системи захисту підприємства від атак соціальної інженерії

Предмет дослідження: метод оцінки впливу на інфраструктуру атаки соціальної інженерії.

Практичне значення одержаних результатів: полягає у можливості застосування розроблених методів для оцінки впливу реальних атак соціальної інженерії на підприємства. Це сприятиме точнішому визначенню та усуненню вразливостей

Наукова новизна одержаних результатів: Розреблено п’ятиетапний метод до проведення оцінки впливу атак соціальної інженерії на кібербезпеку підприєства.

1.АНАЛІЗ АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ПІДПРИЄМСТВА ТА ВИМОГИ СТАНДАРТІВ БЕЗПЕКИ

1.1 Основні поняття про соціальну інженерію, її види та наслідки

Соціальна інженерія - це дія, спрямована на те, щоб змусити людину виконувати певні дії від несанкціонованих осіб, впливаючи на її емоції та процес прийняття рішень. Це дозволяє, таким чином, передати особу конфіденційні дані або дозволити атакуючому отримати привілеї цілі в певному середовищі. Насамперед, отримання доступу доступе до певної інформації до певних інформаційних середовищ є найактуальнішою проблемою сьогодення.

Розрізняють наступні види соціальної інженерії для використання на підприємствах:

Фішинг - це одна з атак соціальної інженерії, яка передбачає надсилання підроблених електронних листів, текстових повідомлень або повідомлень у соціальних мережах, які виглядають так, ніби вони надійшли з надійного джерела, наприклад банку чи компанії, що видає кредитні картки. Мета полягає в тому, щоб обманом змусити одержувача розкрити конфіденційну інформацію, як-от паролі, PIN-коди або номери кредитних карток.

Спірфішинг - це більш цілеспрямована форма фішингу, спрямована на окремих осіб або організації. Це здійснюється зловмисниками, які збирають інформацію про жертв перед тим, як надсилати електронні листи, розроблені так, щоб вони виглядали дуже персоналізованими з метою збільшення ймовірності того, що одержувачі відкриють їх і діятимуть на них.

Атаки BEC (Business Email Compromise) - тип атаки в якому зловмисник отримує доступ до корпоративної електронної пошти та використовує її для обману співробітників з метою виконання певних дій.

Бейтінг - це тип атаки соціальної інженерії, при якій зловмисники залишають цінні предмети, такі як флеш-накопичувачі або гаманці, у місцях, де їх, ймовірно, знайдуть люди. Коли хтось знаходить предмет, він підключає його до свого комп'ютера або забирає додому, де зловмисне програмне забезпечення може бути встановлено на його комп'ютер або він може бути обкрадений.

Тейлгетінг - тактика, що використовується для отримання несанкціонованого доступу до фізичної локації. У цьому сценарії зловмисник слідує за людиною з авторизованим доступом впритул позаду, коли вона входить на захищену територію.[2]

При побудові IT інфраструктури підприємства можуть використовуватись SAAS подібні рішення. Це можуть бути від повноцінних поштових сервісів до систем SIEM та EDR рішень.

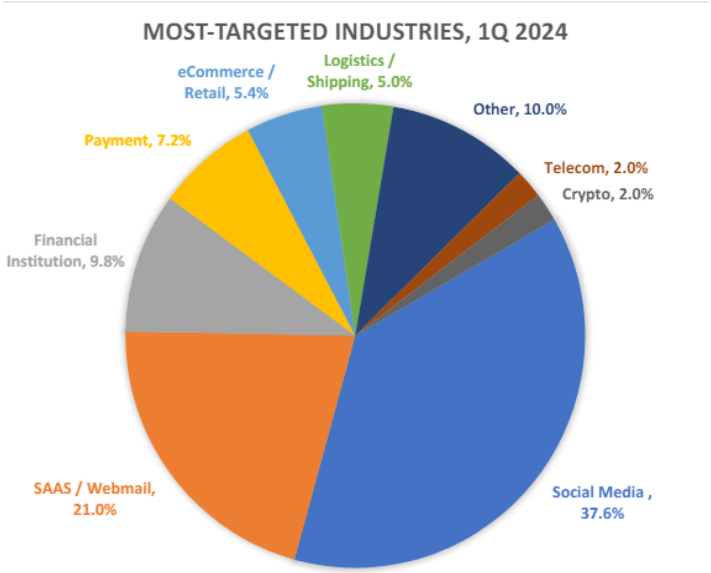


Рисунок 1.1 - Індустрії, на які найбільш націлені атаки за версією APWG в 1 кварталі 2024 року

Згідно з статистичних даних , які надає дослідницький портал APWG в Рисунку 1.1, за перший квартал 2024 року фішингові атаки на підприємства, які використовують SAAS рішення та веб пошту складає рівно 21 відсоток.[1]

Атаки соціальної інженерії можуть мати численні та серйозні наслідки, що впливають як на окремих осіб, так і на організації. До основних наслідків можна віднести до наступних видів:

Фінансові втрати: Одним з найбільш очевидних наслідків є прямі фінансові втрати. Зловмисники можуть викрасти гроші або дані, які мають фінансову цінність. Організації можуть втратити великі суми грошей через шахрайські транзакції, вимоги викупу за відновлення даних або ремонт після атаки.

Втрата конфіденційної інформації: Атаки соціальної інженерії часто спрямовані на викрадення конфіденційної інформації, такої як паролі, номери кредитних карток, персональні дані тощо. Це може призвести до серйозних

проблем для жертв, включаючи крадіжку особистих даних і подальше фінансове шахрайство.

Репутаційні наслідки: Організації, які стають жертвами таких атак, можуть зазнати великих репутаційних втрат. Довіра клієнтів, партнерів та інвесторів може бути підірвана, що вплине на довгостроковий успіх бізнесу.

Юридичні наслідки: Компанії можуть зіткнутися з юридичними проблемами, якщо вони не зможуть належним чином захистити дані своїх клієнтів. Це можуть бути штрафи, судові позови та вимоги про відшкодування збитків.

Втрата продуктивності: Після атак соціальної інженерії організації часто змушені витрачати значні ресурси на розслідування інцидентів, відновлення систем та впровадження додаткових заходів безпеки.

Емоційний стрес: Жертви атак соціальної інженерії, особливо якщо вони призводять до втрати важливих персональних або фінансових даних, можуть відчувати значний емоційний стрес, тривогу і недовіру до систем безпеки.

Компрометація систем безпеки: Якщо зловмисники отримують доступ до внутрішніх систем організації, це може призвести до масштабних компрометації інших систем та інфраструктури. Відновлення після таких інцидентів може вимагати значних зусиль і витрат.[8]

1.2 Вимоги стандартів безпеки щодо протидії соціальної інженерії

Стандарти безпеки становлять все більшу цінність в використанні їх на підприємствах. Більшість підприємств встановлюють вимоги партнерства,

щоб інші мали за собою аудити безпеки або ж впроваджені стандарти кібербезпеки. В них включають технічні заходи, навчання персоналу, створення політик безпеки та впровадження кращих практик для мінімізації ризиків. Вони розроблені для забезпечення комплексного підходу до захисту від соціальної інженерії, що включає як технічні аспекти, так і підвищення обізнаності та компетенції співробітників. Впровадження та дотримання цих вимог є важливим для забезпечення стійкості інформаційних систем і збереження конфіденційності даних. І кожен з стандартів відрізняється в вимогах протидії соціальній інженерії.

1.2.1 ISO 27001:2022

В додатку А пункту 6.3 включають вимоги щодо організації проведення до обізнаності, освіти та навчання в сфері інформаційної безпеки, що є важливим аспектом захисту організації від загроз соціальної інженерії.

Це передбачає регулярне проведення тренінгів та навчальних програм, що мають на меті підвищення рівня знань працівників щодо сучасних методів соціальної інженерії та способів захисту від них. Це включає ознайомлення з типовими сценаріями атак, методами фішингу, вішингу та інших форм соціальної інженерії, а також практичні рекомендації щодо реагування на такі загрози. Навчальні програми повинні бути адаптовані під різні рівні співробітників, забезпечуючи, щоб кожен з них розумів свою роль у захисті інформаційних активів компанії. [7]

1.2.2 CIS Critical Security Controls

На відмінну від інших стандартів, цей передбачує не тільки організаційі, а й технічних заходи в контексті протидії соціальній інженерії.

CIS CSC Control 9 (Email and Web Browser Protections) передбачає впровадження захисту електронної пошти та веб-браузерів, які є основними каналами для атак соціальної інженерії, таких як фішинг. Впровадження фільтрів електронної пошти, антивірусного програмного забезпечення та блокування шкідливих веб-сайтів знижує ризик успішного проведення таких атак.

CIS CSC Control 14 (Implement a Security Awareness and Training Program) є ключовим заходом проти соціальної інженерії, оскільки він фокусується на навчанні працівників розпізнаванню та протидії атакам соціальної інженерії. Програми підвищення обізнаності з безпеки та регулярні тренінги допомагають створити культуру безпеки в організації, де кожен працівник знає, як захистити себе та компанію від соціальних атак.[6]

1.2.3 AICPA SOC 2 (System and Organization Controls)

SOC 2, на відміну від CIS Critical Security Controls, не включає специфічних контролів, які б прямо вказували на протидію соціальній інженерії. Втім, деякі аспекти стандарту можна застосувати для захисту від таких атак.

SOC 2 Принцип: Контроль доступу - передбачає реалізацію політик і процедур, що гарантують, що доступ до систем і даних надається лише авторизованим особам. Захист від соціальної інженерії тут полягає в тому, що організація має навчити своїх працівників ідентифікувати спроби несанкціонованого доступу через соціальну інженерію, такі як фішинг або виманювання паролів.

SOC 2 Принцип: Захист інформації - включає в себе впровадження політик і технологій для захисту інформації від несанкціонованого доступу або розкриття. Заходи можуть включати використання шифрування, двофакторної автентифікації та захист електронної пошти. Це також допомагає зменшити ризик використання соціальної інженерії для доступу до конфіденційної інформації.

SOC 2 Принцип: Освітня програма з безпеки - включає в себе створення і регулярне оновлення програм навчання співробітників для підвищення їхньої обізнаності про методи соціальної інженерії, такі як фішинг, шахрайські дзвінки та інші тактики маніпуляції.[5]

Висновки до розділу 1

У цьому розділі було розглянуто аналіз загроз соціальної інженерії, з якими можуть зіткнутися підприємства, а також демонструє, які відповідні стандарти безпеки вимагають зміцнити захист проти цих загроз. Розглядаючи різноманітні види атак, такі як фішинг, спірфішинг, BEC, бейтінг та тейлгетінг, текст вказує на їх потенційні фінансові, інформаційні, репутаційні, юридичні та емоційні наслідки для підприємств і їх співробітників. За допомогою стандартів як ISO 27001:2022, CIS Critical Security Controls та AICPA SOC 2, розділ обґрунтовує необхідність комплексного підходу до захисту, що включає як технічні заходи, так і навчання персоналу.

Цей аналіз підкреслює критичну роль освітніх програм та регулярних тренінгів у підвищенні рівня обізнаності співробітників, щоб мінімізувати ризики і забезпечити відповідність сучасним вимогам кібербезпеки. Враховуючи постійно зростаючі загрози в цифровому світі, стандарти

безпеки відіграють ключову роль у захисті організацій та їх стейкхолдерів від соціальної інженерії.

2. ВИКОРИСТАННЯ СИМУЛЯЦІЇ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ДЛЯ ОЦІНЮВАННЯ ВПЛИВУ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТА

Симуляція атаки соціальної інженерії в контексті оцінки впливу стану кібербезпеки є інструментом , щоб виконувати оцінювання співробітників в розпізнаванні та протидії спробам. Також дозволить перевірити впровадження систем захисту від наступних атак з використанням шкідливого програмного забезпечення.

2.1 Використання атаки соціальної інженерії, як інструмент для оцінки обізнаності персоналу та стану впровадження безпекових заходів

Підхід проведення атаки соціальної інженерії може дозволити організаціям аналізувати і вдосконалювати свої стратегії захисту від кіберзагроз на основі реальних сценаріїв. Основні процеси, які можна вивчати за допомогою таких симуляцій, включають:

Аналіз реакції персоналу на фішингові атаки: в рамках симуляції можна відправляти персоналу фішингові електронні листи, що імітують реальні атаки. Такі листи можуть містити запрошення клікнути по посиланню або ввести конфіденційні дані. Моніторинг реакцій працівників на такі листи допомагає виявити, наскільки добре вони підготовлені розпізнавати потенційні загрози.

Використання технік інженерії суспільної думки: Можна також провести інтерв'ю чи опитування, імітуючи дзвінки від імені технічної підтримки або керівництва компанії. Це дозволяє оцінити, наскільки працівники готові довіряти інформації, яка надходить від осіб, що видають себе за колег або керівництво, і чи готові вони виконувати їхні запити без додаткової перевірки.

Тестування фізичної безпеки: симуляції можуть також включати спроби несанкціонованого доступу до офісних приміщень. Наприклад, особа, яка вдає з себе нового співробітника або кур'єра, може спробувати отримати доступ до захищених ареалів. Такі симуляції допомагають оцінити ефективність систем контролю доступу та обізнаність персоналу щодо необхідності здійснення перевірок.

Розробка та оцінка процедур реагування на інциденти: після проведення симуляцій важливо аналізувати і відпрацьовувати процедури реагування на інциденти. Оцінка того, як швидко і ефективно команда з реагування змогла впоратися з виявленою загрозою, дозволяє виявити слабкі місця в планах кіберзахисту та відповідним чином їх коригувати.

Навчання та звітність: результати симуляцій слід використовувати для розробки або вдосконалення навчальних програм для співробітників. Поширення інформації про зустрічені помилки і найбільш ефективні методи їх усунення може значно знизити ймовірність успіху реальних атак.[3]

На відміну від традиційних методів оцінки безпеки, таких як тест на проникнення з використанням вразливостей або аудит безпеки, симуляції соціальної інженерії дозволяють оцінити людський фактор, який є одним з найслабкіших ланок в ланцюзі кібербезпеки. Використання симуляцій дозволяє отримати більш реалістичну картину готовності організації до реальних атак, що допомагає краще розуміти і мінімізувати ризики.

Крім того, регулярна оцінка таких загроз дозволяє підприємству залишатися в курсі новітніх методів та технік, які використовують зловмисники.

Специфічність проведення оцінки впливу атаки соціальної інженерії на кібербезпеку підприємства залежить від ряду факторів, які можуть значно відрізнятися в залежності від типу, розміру та галузі діяльності компанії.

Для великих корпорацій, які мають численний штат співробітників та складну інфраструктуру, оцінка зазвичай охоплює широке коло аспектів. Вона може включати аналіз комунікаційних каналів, взаємодію між різними відділами, а також індивідуальні ризики для ключових співробітників, які мають доступ до критично важливої інформації. Особлива увага приділяється вразливостям, пов'язаним з підрядниками та партнерами, оскільки ланцюжок поставок часто є мішенню для зловмисників.

Для середніх компаній, де ресурси можуть бути обмеженішими, оцінка впливу може зосереджуватися на конкретних бізнес-процесах та ключових функціях. Тут важливо знайти баланс між детальністю аналізу та економічною доцільністю. Часто це включає аналіз потенційних векторів атаки через електронну пошту, соціальні мережі та інші комунікаційні канали, які найчастіше використовуються співробітниками.

Малі підприємства, з обмеженим бюджетом на кібербезпеку, можуть зосереджуватися на основних ризиках та використовувати більш спрощені методи оцінки. Вони можуть орієнтуватися на навчання співробітників щодо основних методів соціальної інженерії та створення простих, але ефективних політик безпеки. Для таких підприємств важливо, щоб оцінка була максимально практичною і спрямованою на швидке впровадження заходів захисту.

Компанії, що працюють в специфічних галузях, таких як фінансові установи, медичні заклади або державні органи, можуть мати свої особливі вимоги до оцінки впливу соціальної інженерії. В цих випадках необхідно

враховувати специфічні регуляторні вимоги, що стосуються конфіденційності даних, захисту персональних даних та інших аспектів, характерних для даної галузі.

Важливо розуміти, що ефективність оцінки впливу залежить від її адаптації до конкретних умов підприємства. Кожна організація має свої унікальні характеристики, які визначають найбільш вразливі місця та потенційні загрози. Тому підхід до проведення оцінки повинен бути гнучким та враховувати всі ці нюанси.

2.2 Методика проведення атаки соціальної інженерії для оцінки впливу на кібербезпеку підприємства

Оцінка впливу на кібербезпеку підприємства з використанням соціальної інженерії може бути дуже ефективною, але вимагає ретельного планування та узгодження всіх деталей, а саме:

Законність дій: Необхідно впевнитися, що всі заходи соціальної інженерії проводяться у відповідності до законодавства та етичних норм. Порушення можуть призвести до юридичних наслідків та шкоди репутації компанії.

Дозволи та згода стейкхолдерів: Важливо отримати офіційний дозвіл від керівництва підприємства на проведення тестування. Це включає визначення рівня доступу, який може бути отриманий, і до яких систем або даних можна буде доторкнутися.

Планування та координація: Детальний план проведення тестування повинен бути розроблений і затверджений. Він має включати конкретні методи соціальної інженерії, такі як фішинг, телефонні дзвінки.

Безпека та мінімізація ризиків: Необхідно забезпечити, що методи, які використовуються, не призведуть до реального компрометування систем або втрати даних.

Також важливими вимогами є визначення область проведення дій на підприємстві:

Цілі тестування: Чітке визначення цілей, які повинні бути досягнуті. Це може включати перевірку ефективності існуючих заходів безпеки або оцінку рівня обізнаності співробітників про кіберзагрози.

Об'єкти тестування: Визначення конкретних систем, мереж або груп співробітників, які будуть піддаватися тестуванню. Це допоможе уникнути непорозумінь та забезпечити фокусування на найбільш критичних аспектах.

Методи соціальної інженерії: Перелік методів, які будуть використовуватися під час тестування. Це може включати фішинг, вішинг (голосовий фішинг), передзвони, фізичний доступ тощо.

Часові рамки: Визначення тривалості тестування, включаючи початок і закінчення кожного етапу. Це допоможе координувати дії та уникнути випадкових порушень у роботі підприємства.

Критерії успіху: Визначення показників, які будуть використовуватися для оцінки успішності тестування. Це може бути кількість успішних спроб проникнення, рівень обізнаності співробітників або час, необхідний для виявлення і реагування на атаку.

Після визначення початкових дій в яких буде проводитись оцінка, необхідним є визначитись, за якою методологією проводити оцінку впливу атаки соціальної інженерії на кібербезпеку підприємства. Методика провення , яка складається з 5 кроків.

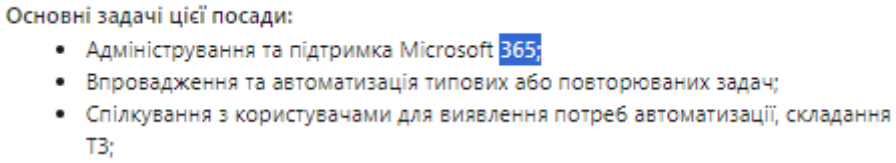
Рисунок 2.1 – Методика проведення тестування атаки соціальної інженерії на підприємство

2.2.1 Збір інформації

Етап збору інформації в тесті соціальної інженерії полягає у збиранні якомога більшої кількості даних про цільову організацію та її працівників. Це включає аналіз офіційного вебсайту організації, її профілів у соціальних мережах, а також прес-релізів і новинних статей, щоб зрозуміти структуру, ключовий персонал, культуру та останні новини.

Досліджуються також публічні записи, такі як реєстрація бізнесу та інші документи. Ідентифікація ключового персоналу відбувається через пошук профілів працівників у професійних мережах, таких як LinkedIn, а також через вебсайт компанії. Особисті акаунти працівників у соціальних мережах можуть розкрити їхні інтереси та звички.

Збирається технічна інформація за допомогою сторонніх сервісів для отримання деталей про домени організації, а також інструментів для ідентифікації IP-адрес та мережевої інфраструктури.


Основні задачі цієї посади:

- Адміністрування та підтримка Microsoft 365;
- Впровадження та автоматизація типових або повторюваних задач;
- Спілкування з користувачами для виявлення потреб автоматизації, складання ТЗ;

Рисунок 2.2 –Фрагмент вакансії, де згадується використання сервісів

Розуміння культури та робочих процесів організації досягається через пошук злитих внутрішніх документів або комунікацій в інтернеті та аналіз вакансій. Виявляються можливі слабкі місця, такі як поведінкові патерни працівників та існуючі заходи безпеки. Інформація, зібрана на цьому етапі, використовується для створення переконливих атак соціальної інженерії на наступних етапах.

2.2.2 Підготовка контенту та створення фішингового веб-сайту

На цьому етапі зібрана раніше інформація використовується для створення фішингового контенту, який виглядає правдоподібно та привабливо для цільової аудиторії.

Спочатку розробляються електронні листи, повідомлення або інші методи комунікації, які будуть використовуватися для взаємодії з цільовими особами. Важливо, щоб контент був максимально персоналізованим та відповідав стилю та тону комунікації організації, щоб зменшити підозри у потенційних жертв.

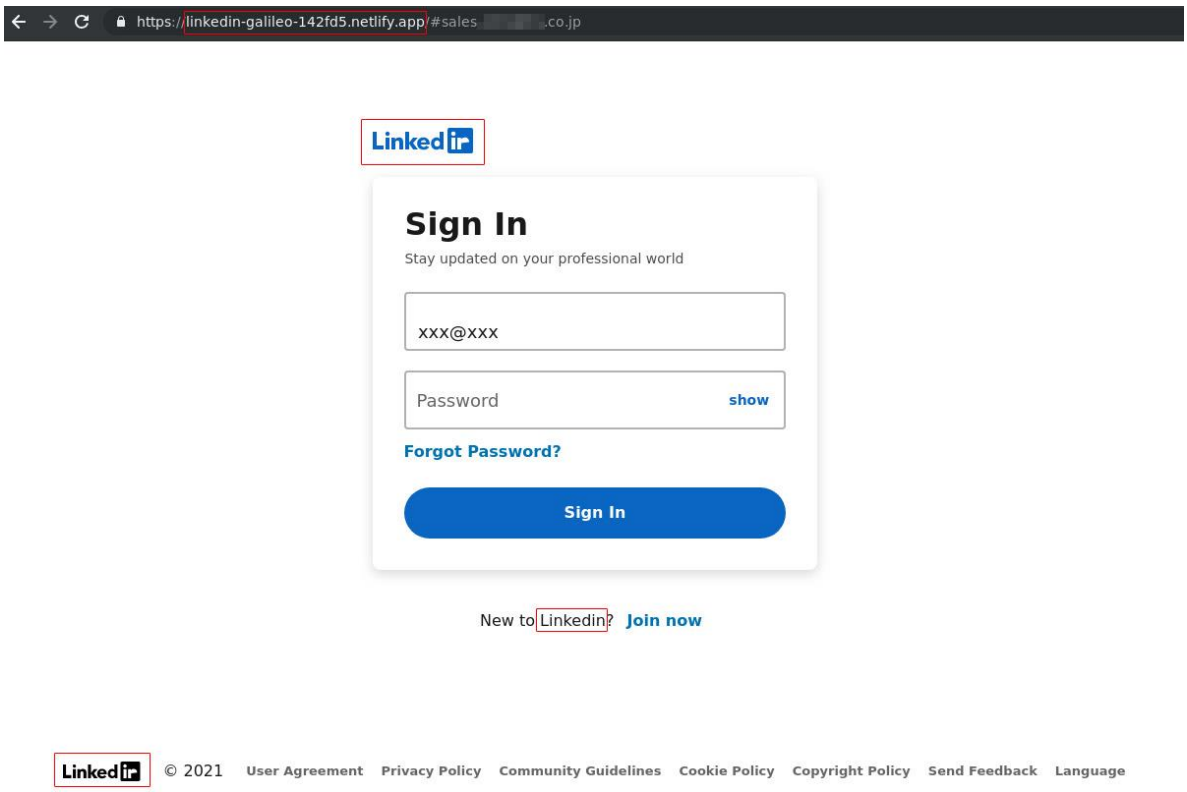


Рисунок 2.3 – Приклад фішингової сторінки

Паралельно створюється фішинговий вебсайт, який має виглядати ідентично до справжнього вебсайту організації або іншого авторитетного ресурсу. Для цього використовуються спеціальні інструменти та технології, що дозволяють копіювати дизайн, логотипи та інший візуальний контент. Важливо забезпечити, щоб фішинговий вебсайт мав правдоподібний URL, який схожий на справжній, але має незначні відмінності, які важко помітити.

Тестується функціональність вебсайту, зокрема форми для введення даних, щоб переконатися, що вони правильно зберігають введену інформацію. Всі ці підготовчі дії спрямовані на те, щоб зробити фішингову атаку максимально ефективною та непомітною для цільових осіб, збільшуючи шанси на успішний збір конфіденційної інформації.

2.2.3 Взаємодія з цільовими особами

Метою цього етапу є залучення цільових осіб до фішингової пастки. На цьому етапі відправляються підготовлені на попередньому етапі фішингові повідомлення, які спонукають цільових осіб взаємодіяти з фішинговим вебсайтом або надати конфіденційну інформацію іншим шляхом.

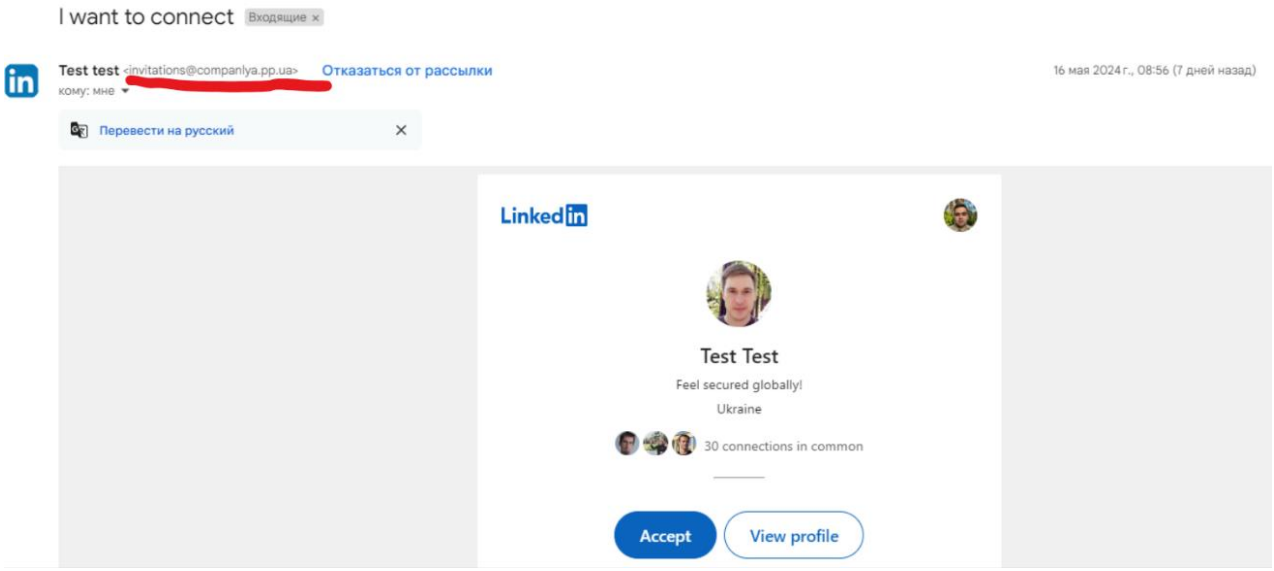


Рисунок 2.4 – Приклад спірфішингової поштової розсилки

Фішингові електронні листи, які можуть містити посилання на фішинговий веб-сайт або вкладення з шкідливим програмним забезпеченням, розсилаються цільовим особам. Важливо, щоб ці листи були максимально персоналізованими та правдоподібними, виглядали як офіційна комунікація від організації або авторитетного джерела. Крім того, використовуються платформи соціальних мереж для надсилання повідомлень або створення публікацій, що містять фішингові посилання. Це може бути особливо ефективно, якщо цільові особи активно користуються соціальними мережами.

Фішингові повідомлення часто включають елементи терміновості або страху, щоб змусити цільові особи діяти негайно, не замислюючись. Наприклад, повідомлення про заблокований акаунт або невідкладну необхідність оновити особисту інформацію. Використовуються також

обіцянки виграшів, знижок або інших привабливих пропозицій для заохочення цільових осіб до взаємодії з фішинговим веб-сайтом.

Після відправки фішингових повідомлень проводиться відстеження взаємодії з ними за допомогою аналітичних інструментів. Відстежується кількість кліків на посилання, заповнення форм та інших дій. Зібрані дані аналізуються для виявлення реакції цільових осіб на фішингові повідомлення, факторів, що впливають на їх рішення взаємодіяти або ігнорувати повідомлення, та загальних патернів поведінки. За умови , взаємодії з фішинговими повідомленнями, можуть бути надіслані подальші інструкції або запити для збору додаткової інформації або подальшого затягування цільової особи у пастку.

2.2.4 Аналіз результатів

Четвертий етап тесту соціальної інженерії - це аналіз результатів. На цьому етапі зібрані дані та взаємодії з цільовими особами ретельно аналізуються для оцінки ефективності фішингової кампанії. Основна мета цього етапу полягає в тому, щоб зрозуміти, наскільки успішно вдалося обманути цільових осіб та отримати від них конфіденційну інформацію.

Перш за все, проводиться збір і перевірка всіх даних, отриманих під час фішингової кампанії. Це включає облікові дані, паролі, особисту інформацію та інші конфіденційні дані, які цільові особи могли надати. Всі ці дані систематизуються та аналізуються, щоб визначити, які саме техніки та підходи були найбільш ефективними.

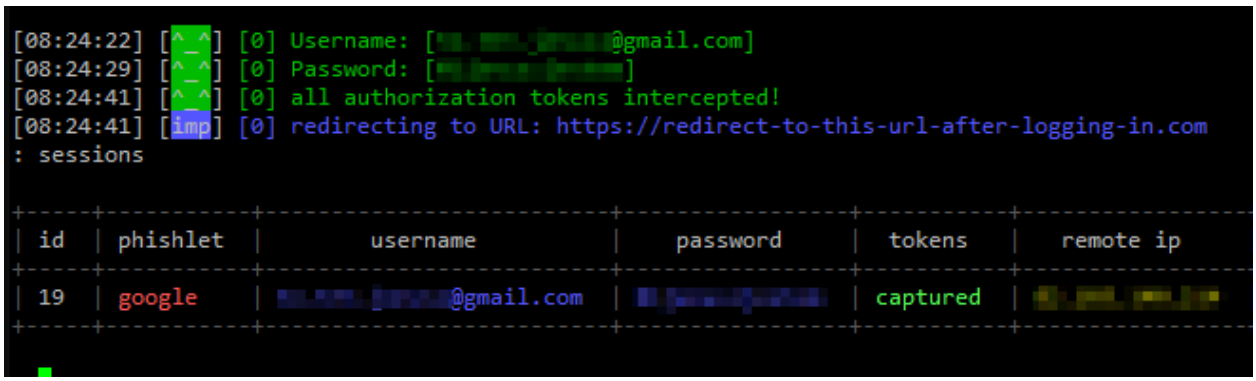


Рисунок 2.5 – Приклад перехоплених даних через фішингове посилання

Далі аналізується кількість цільових осіб, які взаємодіяли з фішинговими повідомленнями, зокрема, хто відкрив листи, перейшов за посиланнями та надав свої дані. Це дозволяє оцінити відсоток успішних атак та зрозуміти, які методи впливу були найбільш переконливими. Також аналізуються часові рамки, протягом яких цільові особи реагували на фішингові повідомлення, що допомагає визначити оптимальний час для проведення таких кампаній у майбутньому.

Крім того, вивчаються патерни поведінки цільових осіб. Це включає аналіз того, як різні групи людей реагували на фішингові атаки, які фактори впливали на їх рішення взаємодіяти або ігнорувати повідомлення. Ці дані допомагають виявити слабкі місця в організації, які можна використовувати для підвищення ефективності майбутніх атак.

2.2.5 Звітність

На цьому етапі створюється звіт, який включає кілька основних компонентів. По-перше, складається виконавче резюме, де надається загальний огляд тесту, включаючи його цілі, обсяг та основні результати. У цьому розділі також висвітлюються найбільш важливі результати, такі як

кількість успішних і невдалих атак, типи використаних атак та їх загальний вплив.

Детальні результати містять опис зібраної під час розвідки інформації, аналіз фішингового веб-сайту, включаючи його дизайн та функціональність, а також статистику взаємодії з цільовими користувачами. Оцінка ефективності існуючих заходів безпеки також входить до цього розділу.

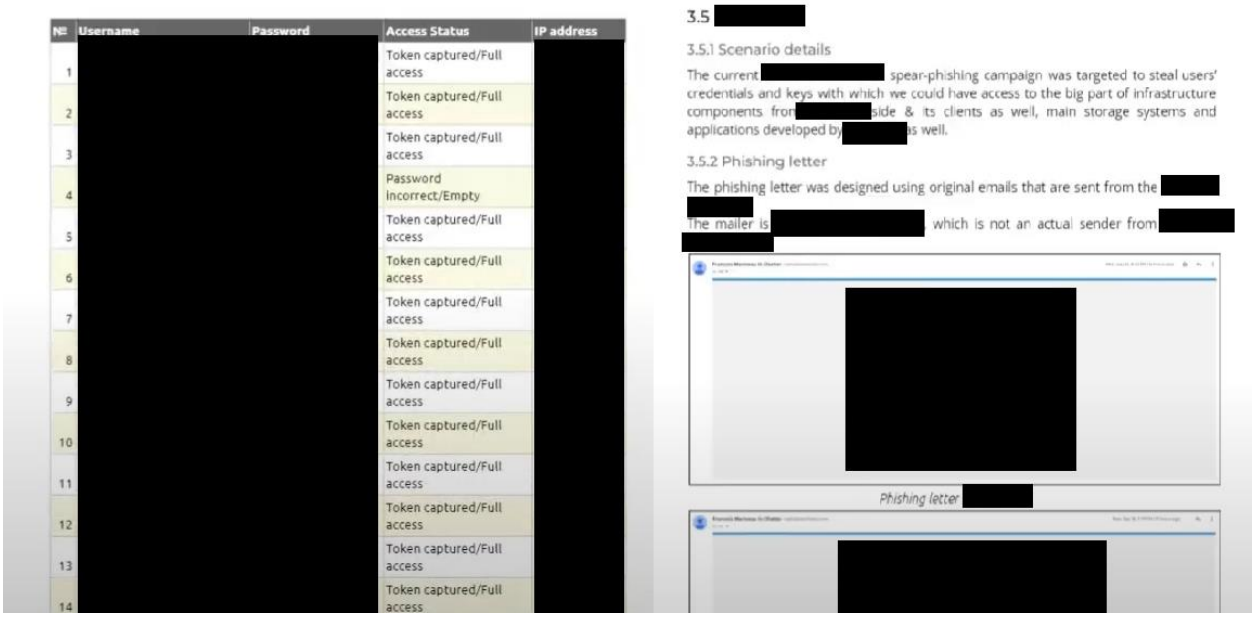


Рисунок 2.6 Приклад звіту з тестування соціальної інженерії

Наприкінці звіту додаються додатки, які можуть містити сирові дані або журнали, зібрані під час тесту, та детальний опис методологій, що використовувалися під час тестування. Це забезпечує прозорість і можливість відтворення результатів.

2.3 Пропозиція реалізації оцінки впливу соціальної інженерії на кібербезпеку підприємства

Для оцінки впливу соціальної інженерії на кібербезпеку підприємства пропонується проведення симуляції інфраструктури підприємства і здійсннення атаки соціальної інженерії на цю інфраструктуру. Процес починається зі створення віртуальної моделі інфраструктури підприємства, яка включає всі основні компоненти, такі як сервери, робочі станції та інші елементи IT-інфраструктури.

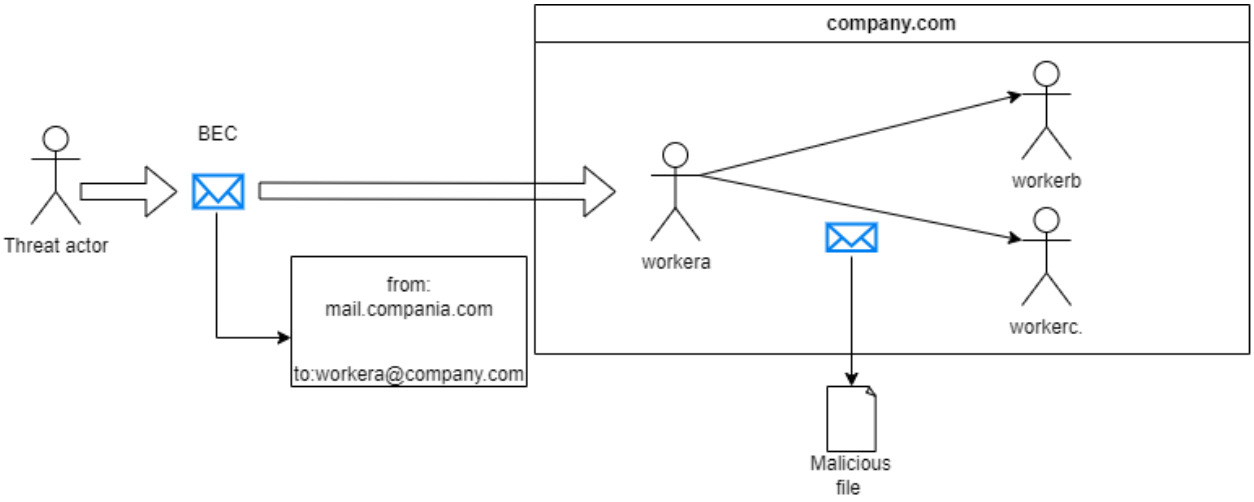


Рисунок 2.7 – Схема прикладу атаки соціальної інженерії

Наступним етапом є розгортування інфраструктирури атакуючого, яка має за собою представляти:

1.Привласнення домену який бути діяти в рамках соціальної інженерії

2. Розгортання системи поштового серверу для використання атаки на підприємство

3. Підроготовка робочої станції атакуючого , а саме встановлення необхідних ПЗ для проведення атаки.

Наступним етапом є розробка сценаріїв соціальної інженерії, що можуть включати фішинг атаки, атаки з використанням шкідливого програмного забезпечення, методи впливу на співробітників для отримання конфіденційної інформації тощо.

Після цього необхідно провести тестування, де співробітники підприємства будуть піддані цим сценаріям соціальної інженерії. Важливо, щоб співробітники не знали про проведення тесту заздалегідь, щоб отримати реалістичні результати. Під час тестування фіксуються всі дії співробітників.

На основі зібраних даних проводиться аналіз результатів тестування. Це включає оцінку вразливостей, які були виявлені, аналіз слабких місць у процедурах безпеки та рівні обізнаності співробітників щодо кіберзагроз. [4] На основі цього аналізу розробляються рекомендації щодо покращення системи безпеки підприємства, що можуть включати додаткові тренінги для співробітників, зміни в політиках безпеки, впровадження нових технологічних рішень для захисту від соціальної інженерії тощо.

Висновки до розділу 2

Симуляція атаки соціальної інженерії – це потужний інструмент, що допомагає підприємствам оцінити рівень кібербезпеки, а також підготовленість співробітників до протидії загрозам. Застосовуючи реалістичні сценарії атак, організації можуть виявити слабкі місця у своїх системах безпеки та навичках персоналу.

Такі симуляції дозволяють аналізувати кілька ключових процесів. Один з них – це реакція персоналу на фішингові атаки. Тут можна надсилати підроблені електронні листи, які виглядають як справжні, та спостерігати, як співробітники реагують: чи переходять за посиланнями, чи вводять конфіденційні дані. Інший важливий процес – це використання технік інженерії суспільної думки, де можна проводити інтерв'ю або телефонні дзвінки, видаючи себе за співробітників технічної підтримки або керівництва.

Важливим є також розробка та оцінка процедур реагування на інциденти, коли після симуляцій аналізується, наскільки швидко та ефективно команда змогла впоратися з загрозою.

Процес оцінки впливу соціальної інженерії включає кілька етапів. Спочатку проводиться збір інформації про організацію та її співробітників, використовуючи відкриті джерела та технічні інструменти. Далі розробляється фішинговий контент, створюється підроблений веб-сайт, що виглядає як справжній, та розсилаються фішингові повідомлення. Важливо, щоб ці повідомлення були максимально правдоподібними та персоналізованими.

Після цього настає етап взаємодії з цільовими особами, коли відстежується їхня реакція на фішингові повідомлення та збираються дані про їхню поведінку. Зібрана інформація аналізується для оцінки успішності атаки та виявлення слабких місць у безпеці. На основі цього аналізу готується детальний звіт з рекомендаціями щодо покращення системи безпеки та проведення додаткових тренінгів для співробітників.

Головним моментом в симуляціях соціальної інженерії є етичність та законність проведення таких тестувань, а також узгодження з керівництвом підприємства. Це допомагає уникнути юридичних наслідків та зберегти репутацію компанії.

3. РЕАЛІЗАЦІЯ СИМУЛЯЦІЇ ОЦІНКИ ВПЛИВУ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА КІБЕРБЕЗПЕКУ ПІДПРИЄМСТВА

На основі наведеної вище інформації про метод реалізації оцінки впливу соціальної інженерії на кібербезпеку підприємства, було прийнято за рішенням реалізації симуляції підприємства, які використовують публічні сервіси та проведення атаки соціальної інженерії на це підприємство для встановлення оцінки впливу на проникнення систем. Дана симуляція буде проведена з

3.1 Опис загальної структури стеку симульованого підприємства

Підприємство передбачає за собою робочі поштові акаунти які використовуються кількома працівниками підприємства. В підприємстві визначено домен як **kompaniya.xyz** та використання таких сервісів:

1. LinkedIn – соціальна мережа для пошуку потенційних нових співробітників компанії.

2. GitHub – платформа, яка використовується для контролю версій та спільної розробки програмного забезпечення.

3. Microsoft 365 – пакет хмарних сервісів та додатків від компанії Microsoft. Підприємство використовує різні інструменти та сервіси, такі як:

3.1 Office додатки: Word, Excel, PowerPoint

3.2 OneDrive - Хмарне сховище, яке дозволяє зберігати, синхронізувати та ділитися файлами з будь-якого пристрою.

3.3 Microsoft Teams - платформа для співпраці, яка включає в себе чат, відеоконференції.

Така симуляція підприємства дозволить максимально визначити вплив атаки соціальної інженерії на кібербезпеку підприємства. Вона охоплює різні аспекти роботи підприємства та ключові сервіси, що дозволяє виявити слабкі місця та покращити заходи безпеки.

3.2 Кроки підготовки для проведення атаки соціальної інженерії на підприємство

Для розгортання системи було обрано хмарне рішення від DigitalOcean , яка буде використовуватись для атаки на симульоване підприємство.

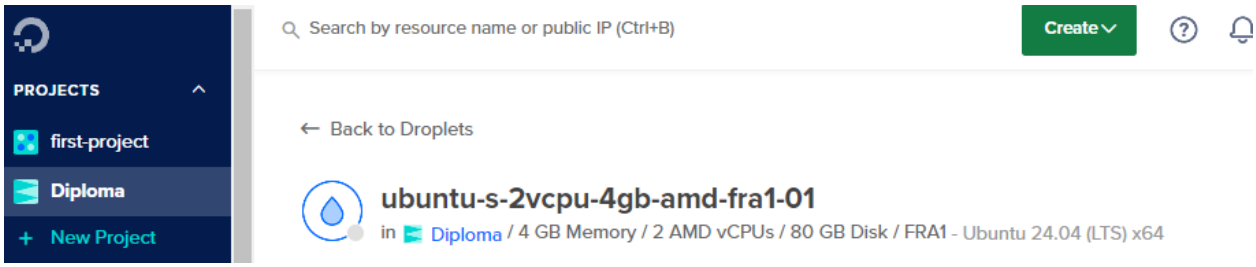


Рисунок 3.1 – Сторення віртуальної машини в DigitalOcean

Було створено віртуальну машину з розташуванням ОС Ubuntu. Такий варіант дозволяє мати можливість розміщувати фішингові кампанії[9] та збирати дані користувачів на постійній цілодобовій основі.

Для того щоб атакуючий міг відправляти поштові фішингові посилання було обрано сервіс Namecheap, який дозволяє реєстрацію доменних імен, mail-хостинг, SSL-сертифікати.

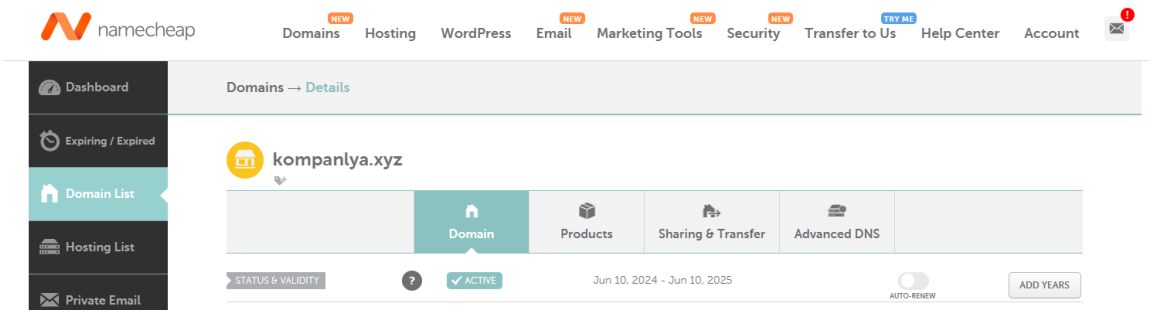


Рисунок 3.2 – Було привласнено домен kompanlya.xyz

У рамках реалізації розміщення симуляції було обрано використання схожого домену для фішингу під назвою “**kompanlya.xyz**”. Мета привласнення такого домену - зловити користувачів, які випадково вводять неправильну адресу або не помічають незначних відмінностей.

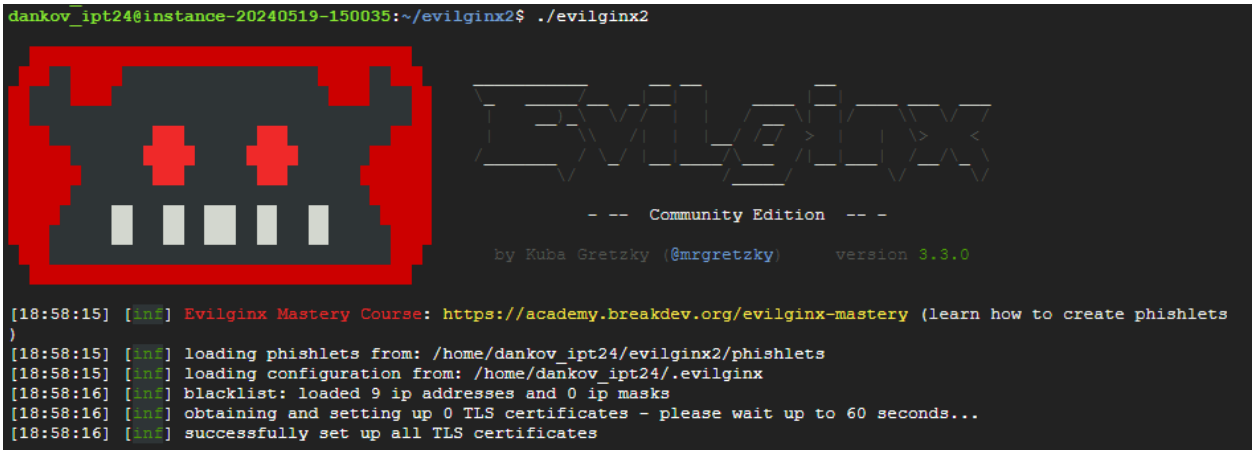


Рисунок 3.3 – Початкова сторінка Evilginx

Для реалізації розміщення фішингових сайтів та збирання даних компаній було обрано програмне забезпечення Evilginx[10]. Це є інструментом для проведення фішингових атак з використанням техніки, відомої як man-in-the-middle (MITM) proxy. Для створення конкретних фішингових сторінок використовуються phislets. Це текстові файли з розширенням YAML, що дозволяє атакуючому перехоплювати та зберігати дані для аутентифікації, такі як паролі та перехоплювати сесії.

В останню чергу, для того щоб підготувати розсилки, було створено HTML-додатки до поштових відправлень, з метою забезпечення можливості створення розсилок з додаванням інтерактивних та візуально привабливих елементів, що покращують сприйняття інформації та залучають більше уваги одержувачів.

3.3 Проведення кампанії з оцінки атаки соціальної інженерії на підприємство

LinkedIn:

Під час проведення кампанії з соціальної інженерії з поштової скриньки “workerb@kompanlya.xyz” будуть відправлені HTML-додаток на пошту користувача “workera@kompaniya.xyz”, що містять інтерактивні та візуально привабливі елементи, спрямовані на привернення уваги одержувачів.

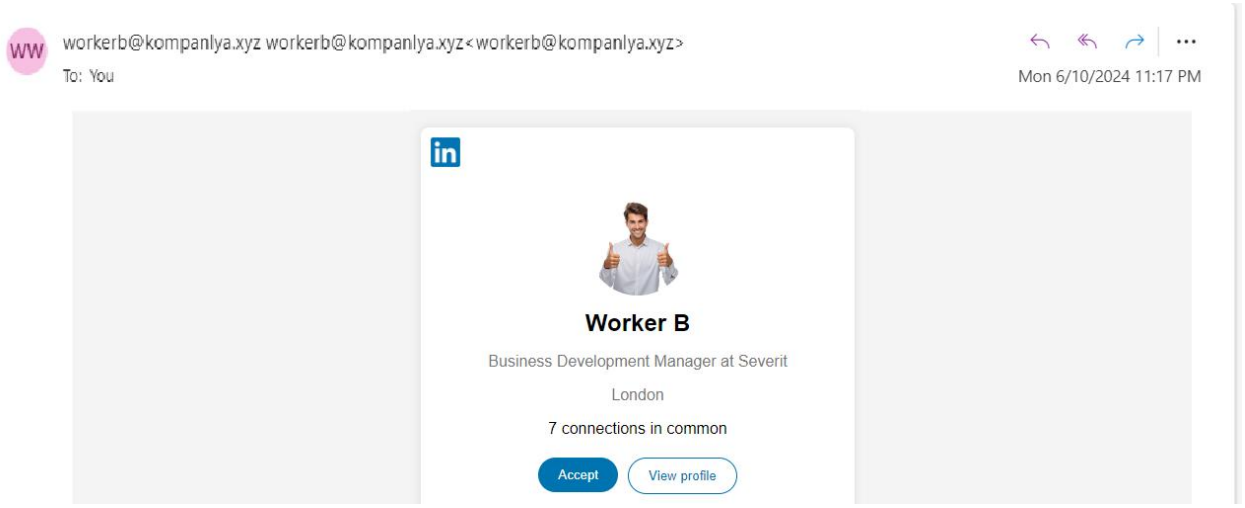


Рисунок 3.4 – Поштова розсилка з HTML додатком кампанії LinkedIn

Цей додаток міститить посилання на фішинговий сайт LinkedIn, розміщеного на інстансі. І для цього буде активований відповідний phishlet, який імітує справжній вебсайт для входу.

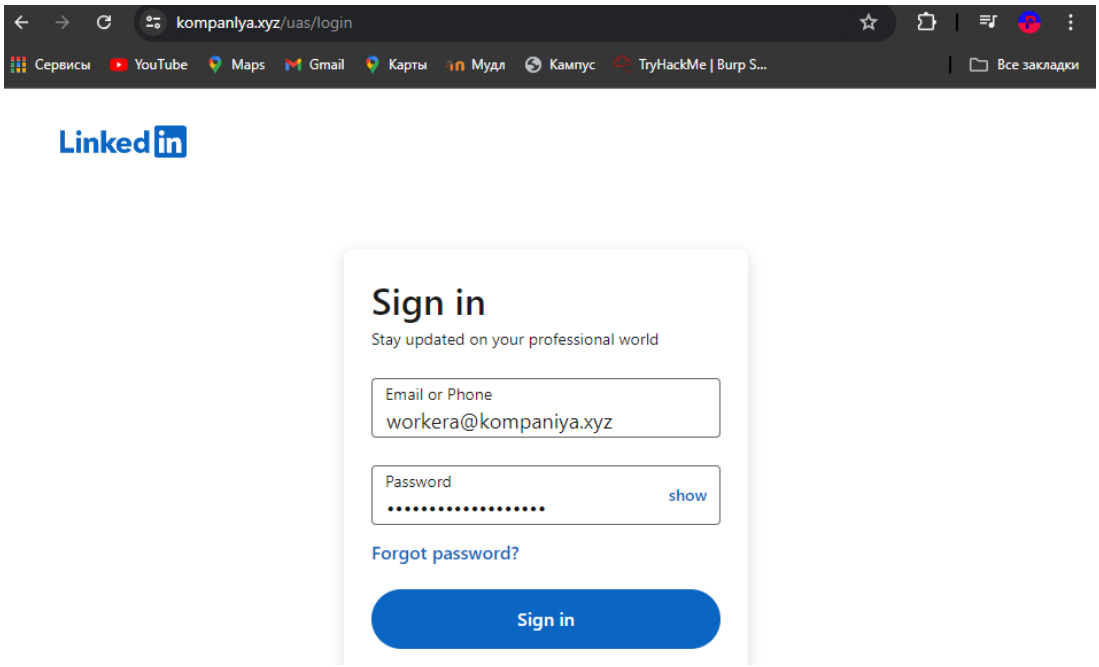


Рисунок 3.5 – Фішингова сторінка Linkedin

Після переходу на kompanlya.xyz/uas/login і введення облікових даних користувачами, інформація буде перехоплена та відображена в інтерфейсі Evilginx.

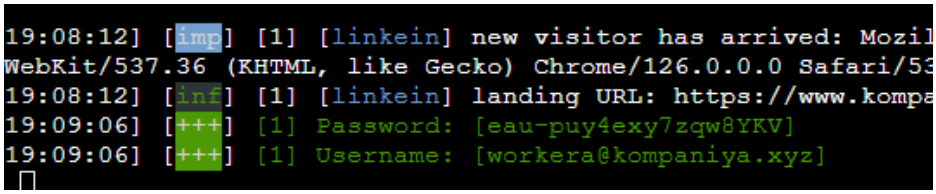


Рисунок 3.6 – Перехоплені дані з кампанії LinkedIn в Evilgnix

В результаті кампанії було отримано дані з логіном та паролем до сервісу Linkedin.

Microsoft 365:

Під час проведення кампанії з соціальної інженерії з поштової скриньки “workerb@kompanlya.xyz” будуть відправлені HTML-додаток на пошту користувача “workera@kompaniya.xyz”, що містять інтерактивні та

візуально привабливі елементи, спрямовані на привернення уваги одержувачів.

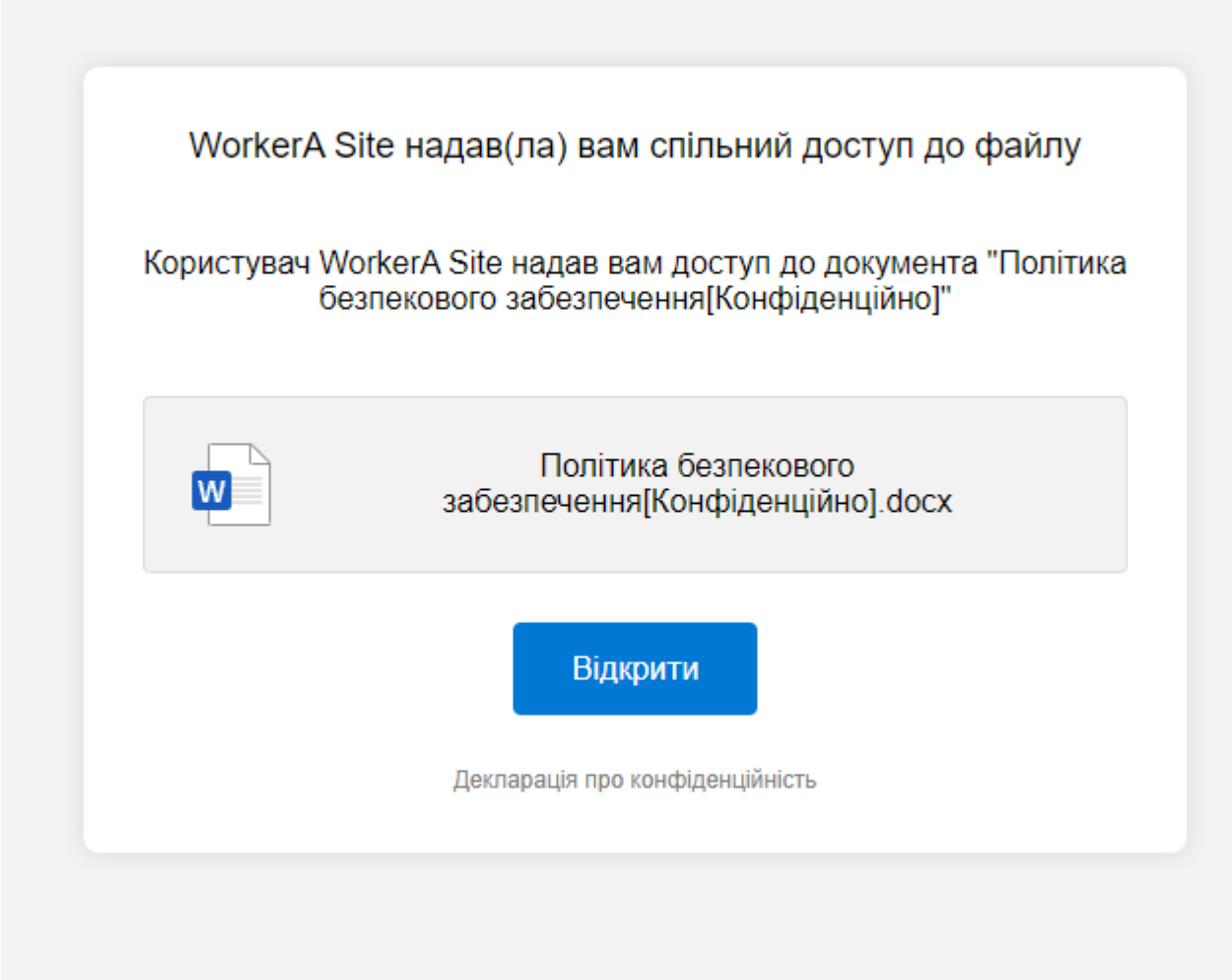


Рисунок 3.7 - Поштова розсилка з HTML додатком Microsoft 365

Цей додаток міститить посилання на фішинговий сайт login.companlya.xyz , розміщеного на інстансі. І для цього буде активований відповідний phishlet який імітує справжній вебсайт для входу.

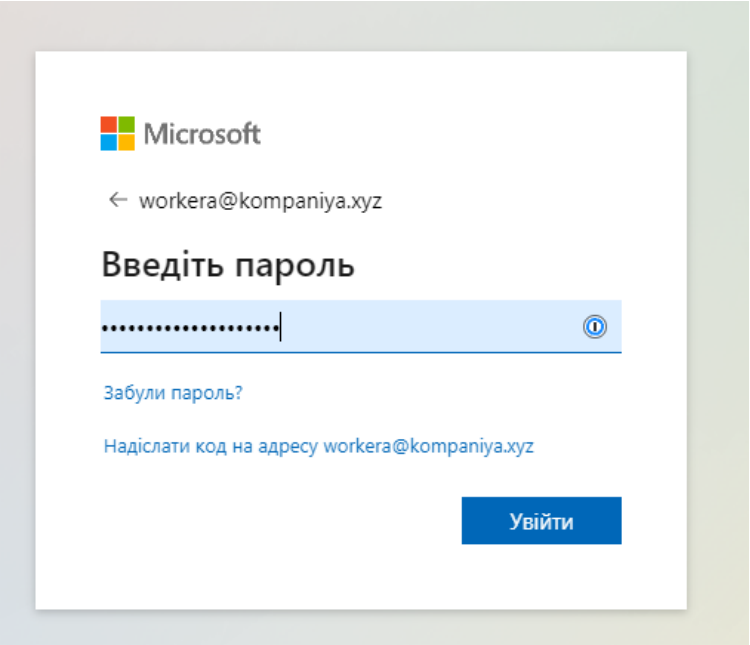


Рисунок 3.8 - Фішингова сторінка Microsoft 365

Після переходу за цим посиланням і введення облікових даних користувачами, інформація буде перехоплена та відображена в інтерфейсі Evilginx.

```
new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Appl
cko) Chrome/126.0.0.0 Safari/537.36 (188.163.114.148)
landing URL: https://www.kompanlya.xyz/yiSIMgBe
[eau-puy4exy7zqw8YKV]
[workera@kompaniya.xyz]
```

Рисунок 3.9 - Перехоплені дані з кампанії Microsoft 365 в Evilgnix

В результаті кампанії було отримано дані з логіном та паролем до сервісу Microsoft 365.

GitHub:

Під час проведення кампанії з соціальної інженерії з поштової скриньки “workerb@kompanlya.xyz” будуть відправлені HTML-додаток на пошту користувача “workera@kompaniya.xyz”, що містять інтерактивні та візуально привабливі елементи, спрямовані на привернення уваги одержувачів.

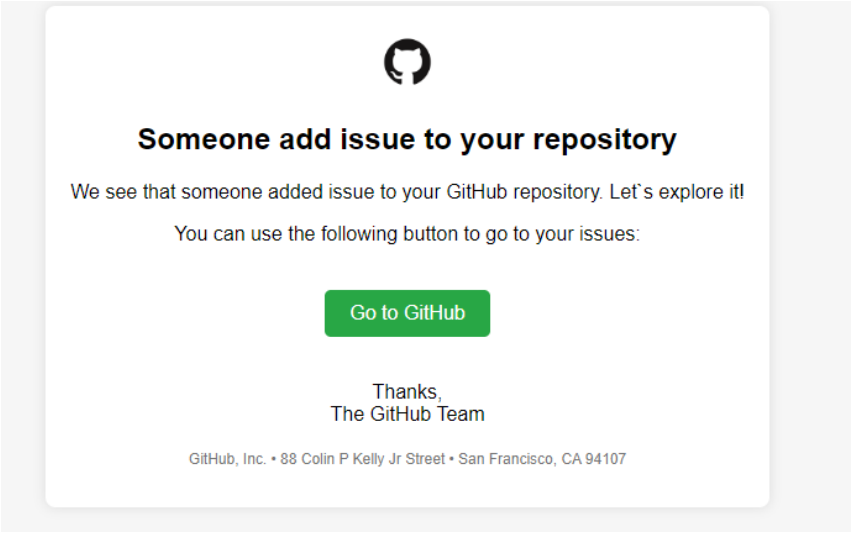


Рисунок 3.10 - Поштова розсилка з HTML додатком Github

Після переходу на посилання kompanlya.xyz/login і введення облікових даних користувачами, інформація з даними буде перехоплена та відображена в інтерфейсі Evilginx.

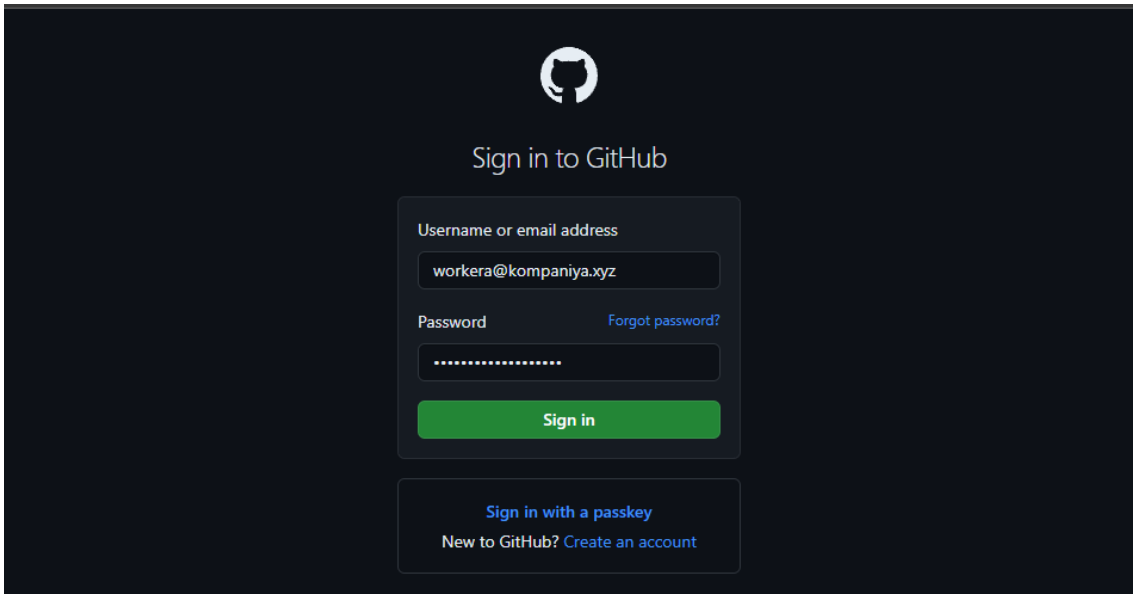


Рисунок 3.11 - Фішингова сторінка Github

На відміну від інших кампанії ,в результаті було отримано дані з логіном та паролем та було перехоплено веб-сесію до сервісу GitHub.

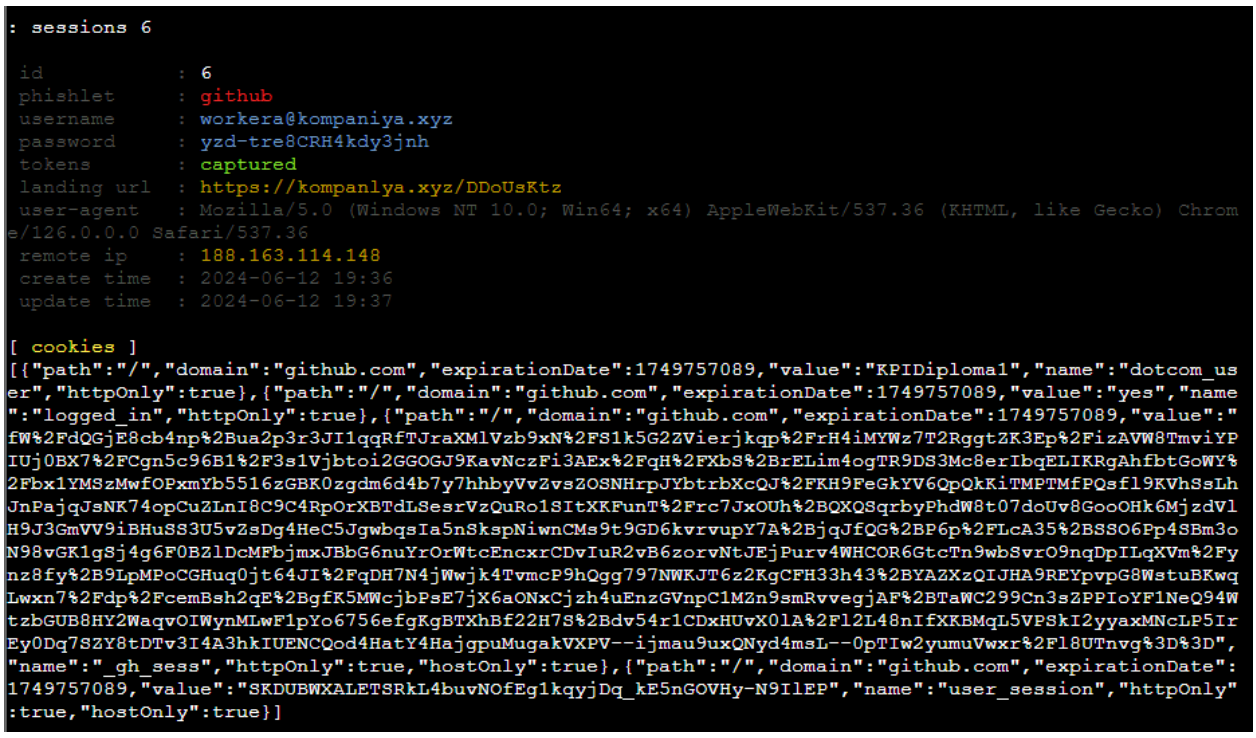


Рисунок 3.12 - - Перехоплені дані з кампанії Github в Evilgnix

3.4 Аналіз результатів проведених кампаній та оформлення звіту з оцінки впливу атаки соціальної інженерії

Аналіз результатів проведених кампаній з соціальної інженерії передбачає в собі можливості перевірки доступу до ресурсів, вивчення ресурсів даних та висновків щодо ефективності захисних заходів підприємства. Для того, спочатку необхідно зібрати всю інформацію, що стосується проведених кампаній, включаючи кількість успішних та невдалих спроб атак.[11]

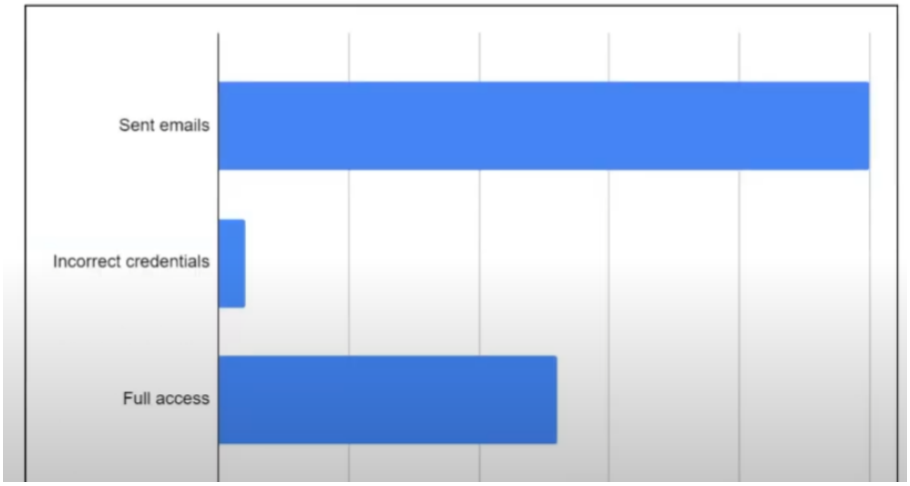


Рисунок 3.13 – Статистика по усім кампаніям з розсилки

Оцінка впливу таких кампаній включає аналіз, як працівники реагували на фішингові листи, а саме, скільки з них відкривали підозрілі повідомлення та скільки працівників надали конфіденційну інформацію.

Phishing Campin	№	Username	Password	Access Status
Linkedin	1	workera@kompaniya.xyz	_stc_T..3tJBfPX****	Granted/Access is present
	2	workerb@kompaniya.xyz	Nicetry123:)	Not actual credentials
Github	1	workera@kompaniya.xyz	yzd-tre8CRH4kdy3****	Granted/Access is present
Microsoft 365	1	workera@kompaniya.xyz	02012001wor***	Granted/Access is present

Рисунок 3.14 – Таблиця з прикладного звіту де вказуються зібрані логіни/паролі

Під час аналізу потрібно звернути увагу на виявлені слабкі місця в системі кібербезпеки. Це можуть бути технічні недоліки, недостатня обізнаність працівників або недотримання політик безпеки. Важливо визначити, які саме аспекти дозволили зловмисникам успішно здійснити атаки, та які наслідки це мало для підприємства.

Звіт для kompaniya.xyz

Рекомендація щодо протидії соціальній Інженерії

Підвищення обізнаності працівників

- **Регулярні тренінги та навчання:** Організовувати регулярні навчальні заходи, тренінги та семінари для працівників щодо виявлення та реагування на атаки соціальної інженерії.
- **Симуляційні вправи:** Проводити фішингові тестування та інші симуляційні вправи для перевірки готовності працівників та підвищення їх обізнаності.

Розробка та впровадження політик безпеки

- **Чіткі інструкції:** Розробити та впровадити чіткі політики та процедури щодо обробки конфіденційної інформації, а також дій у випадку підозри на соціальну атаку.
- **Регулярний моніторинг:** Встановити системи моніторингу та аудиту для забезпечення виконання політик безпеки.

Технічні заходи захисту

- **Багаторівнева аутентифікація:** Впровадити багаторівневі системи аутентифікації для захисту доступу до критичних систем та даних.
- **Фільтри електронної пошти:** Використовувати сучасні антивірусні програми та фільтри для виявлення та блокування фішингових та шкідливих листів.

Рисунок 3.15 – Рекоменданції з прикладного звіту де вказуються рекомендації до протидії атакам соціальної інженерії

Оформлення звіту повинно включати докладний опис проведених кампаній, отримані результати та висновки.[12] У звіті необхідно відобразити всі зібрані дані, включаючи статистику інцидентів, економічні, репутаційні та правові наслідки успішних атак. На основі цього аналізу розробляються рекомендації для покращення кібербезпеки, які допоможуть підприємству запобігти майбутнім атакам соціальної інженерії.

Висновки до розділу 3

Проведена симуляція атаки соціальної інженерії на підприємство показала значний вплив таких атак на кібербезпеку. Аналіз показав, що використання фішингових технік дозволяє успішно отримувати конфіденційну інформацію користувачів через помилки в доменних іменах і інтерактивні HTML-додатки в листах. Основні вразливості виявлені у працівників, які недостатньо обізнані про фішингові загрози, а також у технічних аспектах захисту інформації. Отримані результати дозволяють розробити конкретні рекомендації для покращення безпеки, включаючи

підвищення обізнаності працівників, впровадження більш надійних технічних засобів захисту та вдосконалення політик безпеки підприємства.

ВИСНОВКИ

У результаті виконання даної роботи були вирішені наступні завдання:

1. Розглянуто базові принципи та методи аналізу атак на підприємства. Сформовано основні етапи аналізу атак, розуміння сценаріїв атак. Окремо розглянуті особливості процесу аналізу для різних типів атак, включаючи фішинг, атаки на ланцюги постачання. Визначено важливість підвищення обізнаності персоналу щодо можливих загроз і методів захисту.

2. Проаналізовано вимоги міжнародних і національних стандартів безпеки щодо оцінки впливу соціальної інженерії. Було підкреслено значущість дотримання стандартів, таких як ISO 27001,CIS CSC та AICPA SOC 2 для забезпечення відповідності безпеки. Розроблено структуровані підходи до проведення оцінки впливу соціальної інженерії, що дозволяє систематизувати процеси захисту.

3. Створено модель симуляції оцінки впливу соціальної інженерії шляхом проведення атаки на умовне підприємство. Практичне тестування дозволило ідентифікувати слабкі місця в захисних системах підприємства. Оцінка реального рівня загроз допомогла підприємству підготуватись до можливих атак.

4. Розроблено детальну звітність щодо проведених дій, включаючи аналіз атак, оцінку впливу соціальної інженерії та результати симуляцій. Звітність містить конкретні рекомендації щодо покращення безпеки, які базуються на виявлених слабких місцях та прогнозованих наслідках атак. Надано практичні поради для підвищення рівня готовності підприємства до кібератак, що включають впровадження нових політик безпеки, навчання персоналу та покращення технічних заходів захисту.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

[1] Phishing Activity Trends Report [Електронний ресурс] – Режим доступу до ресурсу: https://docs.apwg.org/reports/apwg_trends_report_q1_2024.pdf.

[2] Cristopher Hadnagy, Social Engineering: The Science of Human Hacking[Електронний ресурс] – Режим доступу до ресурсу: https://duikt.edu.ua/uploads/l_2112_74001205.pdf

[3] Social EngineeringJan-Willem Bullée and Marianne Junger[Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/355168646_Social_Engineering

[4] Social Engineering: Hacking the Human Report [Електронний ресурс] – Режим доступу до ресурсу: https://www.lancaster.ac.uk/media/lancaster-university/content-assets/documents/cyber-foundry/SocialEngineering.pdf

[5] AICPA SOC2 [Електронний ресурс] – Режим доступу до ресурсу: https://www.scribd.com/document/407628788/SOC2-pdf

[6] CIS Critical Security Controls [Електронний ресурс] – Режим доступу до ресурсу: https://paper.bobylive.com/Security/CIS/CIS_Controls_v8_Guide.pdf

[7] ISO 27001:2022 [Електронний ресурс] – Режим доступу до ресурсу: https://www.scribd.com/document/635648085/pdf-iso-iec-27001-2022

[8] Social Engineering Attacks Impact on Businesses[Електронний ресурс] – Режим доступу до ресурсу: https://blog.uniqkey.eu/impact-of-social-engineering-attacks/

[9] Simulate A Phishing Attack On Twitter Using Evilginx[Електронний ресурс] – Режим доступу до ресурсу: https://hamzamhirsi.medium.com/simulate-a-phishing-attack-on-twitter-using-evilginx-fd0d72a934c2

[10] Evilginx [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/kgretzky/evilginx2

[11] Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools and Solutions[Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/340238493_Analysis_and_Findings_of_Social_Engineering_Industry_Experts_Explorative_Interviews_Perspectives_on_Measures_Tools_and_Solutions

[12] Social engineering and cyber security[Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/315351300_SOCIAL_ENGINEERING_AND_CYBER_SECURITY

ДОДАТОК А

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>LinkedIn Profile</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            background-color: #f4f4f4;
            margin: 0;
            padding: 0;
            display: flex;
            justify-content: center;
            align-items: center;
            height: 100vh;
        }
        .container {
            background-color: #fff;
            width: 400px;
            border-radius: 8px;
            box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
            padding: 20px;
            position: relative;
        }
        .linkedin-logo {
            position: absolute;
            top: 10px;
            left: 10px;
```

```
}
.linkedin-logo img {
    width: 30px;
    height: 30px;
}
.profile-header {
    text-align: center;
    margin-top: 50px;
}
.profile-header img {
    border-radius: 50%;
    width: 100px;
    height: 100px;
}
.profile-header h2 {
    margin: 10px 0;
}
.profile-header p {
    color: #777;
}
.connections {
    text-align: center;
    margin-bottom: 20px;
}
.buttons {
    display: flex;
    justify-content: center;
    gap: 10px;
    margin-bottom: 20px;
}
```

```
        .buttons a {
            text-decoration: none;
        }
        .buttons button {
            padding: 10px 20px;
            border: none;
            border-radius: 20px;
            cursor: pointer;
        }
        .buttons .accept {
            background-color: #0073b1;
            color: #fff;
        }
        .buttons .view {
            background-color: #fff;
            color: #0073b1;
            border: 1px solid #0073b1;
        }
    </style>
</head>
<body>
    <div class="container">
        <div class="linkedin-logo">
            <img
src="https://upload.wikimedia.org/wikipedia/commons/c/ca/LinkedIn_logo_initials.png" alt="LinkedIn">
        </div>
        <div class="profile-header">
            <img   src="https://png.pngtree.com/png-vector/20230918/ourmid/pngtree-man-in-shirt-smiles-and-gives-thumbs-up-to-show-approval-png-image_10094381.png" alt="Jake Mitchell">
```

```
            <h2>Worker B</h2>
            <p>Business Development Manager at Severit</p>
            <p>London</p>
        </div>
        <div class="connections">
            <p>7 connections in common</p>
        </div>
        <div class="buttons">
            <a href="https://www.komanlya.xyz/saq/login " target="_blank"><button class="accept">Accept</button></a>
            <a href=" https://www.komanlya.xyz/saq/login " target="_blank"><button class="view">View profile</button></a>
        </div>
    </div>
</body>
</html>
```

ДОДАТОК Б

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>GitHub Password Reset</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            background-color: #f6f6f6;
            margin: 0;
            padding: 20px;
            display: flex;
            justify-content: center;
        }
        .email-container {
            background-color: #fff;
            max-width: 600px;
            border-radius: 8px;
            box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
            padding: 20px;
        }
        .email-header {
            text-align: center;
            margin-bottom: 20px;
        }
        .email-header img {
            width: 50px;
            height: 50px;
```

```
        }
        .email-body {
            text-align: center;
            margin-bottom: 20px;
        }
        .email-body h2 {
            margin-top: 0;
        }
        .reset-button {
            display: inline-block;
            padding: 10px 20px;
            background-color: #28a745;
            color: #fff;
            text-decoration: none;
            border-radius: 5px;
            margin: 20px 0;
        }
        .footer {
            text-align: center;
            color: #777;
            font-size: 12px;
            margin-top: 20px;
        }
    </style>
</head>
<body>
    <div class="email-container">
        <div class="email-header">
            <img
src="https://github.githubassets.com/images/modules/logos_page/GitHub-
Mark.png" alt="GitHub Logo">
```

```
        </div>
        <div class="email-body">
            <h2>Someone add issue to your repository</h2>
            <p>We see that someone added issue to your GitHub repository. Let`s explore it!</p>
            <p> You can use the following button to go to your issues:</p>
            <a href="https://kompanlta.xyz/login" class="reset-button">Go to GitHub</a>
            <p> <a href=""></a></p>
            <p>Thanks,<br>The GitHub Team</p>
        </div>
        <div class="footer">
            <p></p>
            <p>GitHub, Inc. • 88 Colin P Kelly Jr Street • San Francisco, CA 94107</p>
        </div>
    </div>
</body>
</html>
```

ДОДАТОК В

```
<!DOCTYPE html>
<html lang="uk">
<head>
    <meta charset="UTF-8">
    <title>Document Access Notification</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            background-color: #f2f2f2;
            display: flex;
            justify-content: center;
            align-items: center;
            height: 100vh;
            margin: 0;
        }
        .container {
            background-color: white;
            border-radius: 8px;
            box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
            width: 500px; /* Increased width */
            padding: 30px; /* Increased padding */
            text-align: center;
        }
        .header {
            font-size: 18px; /* Reduced font size */
            margin-bottom: 40px; /* Increased margin */
        }
        .content {
```

```
    font-size: 16px; /* Reduced font size */
    margin-bottom: 40px; /* Increased margin */
}
.file {
    display: flex;
    align-items: center;
    justify-content: center;
    background-color: #f2f2f2;
    border: 1px solid #ddd;
    border-radius: 4px;
    padding: 20px; /* Increased padding */
    margin-bottom: 40px; /* Increased margin */
}
.file img {
    width: 48px; /* Increased size */
    height: 48px; /* Increased size */
    margin-right: 15px; /* Increased margin */
}
.file span {
    font-size: 16px; /* Reduced font size */
}
.button {
    background-color: #0078d4;
    color: white;
    padding: 15px 30px; /* Increased padding */
    border: none;
    border-radius: 4px;
    text-decoration: none;
    font-size: 16px; /* Reduced font size */
}
```

```
        .footer {
            font-size: 12px; /* Reduced font size */
            color: gray;
            margin-top: 40px; /* Increased margin */
        }
    </style>
</head>
<body>
    <div class="container">
        <div class="header">
            WorkerA Site надав(ла) вам спільний доступ до файлу
        </div>
        <div class="content">
            Користувач WorkerA Site надав вам доступ до документа "Політика безпекового забезпечення[Конфіденційно]"
        </div>
        <div class="file">
            <img src="https://upload.wikimedia.org/wikipedia/commons/f/fb/.docx_icon.svg" alt="Word Icon">
            <span>Політика безпекового забезпечення[Конфіденційно].docx</span>
        </div>
        <a href="login.kompanlya.xyz" class="button">Відкрити</a>
        <div class="footer">
            Декларація про конфіденційність
        </div>
    </div>
</body>
</html>
```