

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПISKA

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології протидії людино-
орієнтованим кібератакам на інформаційні системи»

Виконав студент 2-го курсу групи КБм-22-1
спеціальності 125 «Кібербезпека»

 Словінський В.В.

Керівник, професор кафедри комп'ютерної інженерії та
кібербезпеки, доктор технічних наук, доцент

 Воротніков В.В.

Рецензент, доцент комп'ютерної інженерії та кібербезпеки,
кандидат технічних наук, доцент

 Россінський Ю.М.

Житомир – 2023

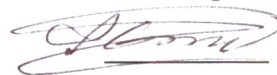
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

13 жовтня 2023 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу магістра

Студент: Словінський Вадим Валерійович

Тема роботи: **«Методи та технології протидії людино-орієнтованим кібератакам на інформаційні системи»**

затверджена Наказом університету від 13 жовтня 2023 р. № 572/с

Термін здачі студентом закінченої роботи 11 грудня 2023 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Об'єктом дослідження є процес захисту інформаційних системи, зокрема їх вразливість до людино-орієнтованих кібератак.
2. Предметом дослідження є методи та технології протидії людино-орієнтованим кібератакам.

Обладнання та програмне забезпечення:

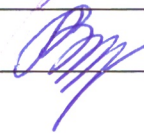
1. ZAP
2. WPSCAN

3. BlankGrabber
4. Zphisher
5. Metasploit

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	А.А. Єфіменко	 2.11.23	2.11.23
2	А.А. Єфіменко	 6.11.23	6.11.23
3	А.А. Єфіменко	 10.11.23	10.11.23

Студент  В.В. Словінський

Керівник  В.В. Воротніков

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка задачі	2 листопада 2023	
2	Формування технічного завдання	4 листопада 2023	
3	Проектування структури роботи	7 листопада 2023	
4	Написання 1 розділу	7 листопада 2023 – 15 листопада 2023	
5	Написання 2 розділу	16 листопада 2023 – 24 листопада 2023	
6	Написання 3 розділу	25 листопада 2023 – 7 грудня 2023	
7	Перевірка	11 грудня 2023	
8	Захист	26 грудня 2023	

Студент _____ Словінський В.В.

Керівник _____ Воротніков В.В.

РЕФЕРАТ

Метою випускної кваліфікаційної роботи є дослідження різних методів та технологій, спрямованих на протидію людино-орієнтованим кібератакам, таким як фішинг, вішинг та інші форми соціальної інженерії, що впливають на інформаційні системи підприємств. Пояснювальна записка до дипломної роботи містить 34 сторінок та 2 додатки. У роботі буде розглянуто такі аспекти, як ідентифікація людино-орієнтованих загроз, аналіз вразливостей інформаційних систем, а також застосування сучасних технологій захисту, включаючи штучний інтелект, машинне навчання та інтегровані системи безпеки.

Для досягнення цієї мети використовуватимуться різні джерела, включаючи наукові статті, спеціалізовані веб-ресурси, актуальні книги та практичні досвіди у галузі кібербезпеки. У дипломній роботі будуть розглянуті різні підходи та методики протидії людино-орієнтованим кібератакам, їхні переваги та недоліки. Окрім того, будуть надані рекомендації щодо розробки ефективної стратегії протидії таким атакам на інформаційні системи підприємств.

Ключові слова: ЗАХИСТ, МЕТОДИ ТА ТЕХНОЛОГІЇ, ЗАГРОЗИ, ЛЮДИНО-ОРІЄНТОВАНІ КІБЕРАТАКИ, ФІШИНГ, ВІШИНГ, СОЦІАЛЬНА ІНЖЕНЕРІЯ.

ABSTRACT

The objective of this thesis is to explore various methods and technologies aimed at countering human-oriented cyber attacks, such as phishing, vishing, and other forms of social engineering, that impact enterprise information systems. The explanatory note to the thesis includes 34 pages and 2 APPENDICES. The study will examine aspects such as identification of human-oriented threats, analysis of vulnerabilities in information systems, and the application of modern protection technologies, including artificial intelligence, machine learning, and integrated security systems.

To achieve this goal, various sources will be utilized, including scientific articles, specialized web resources, relevant books, and practical experience in the field of cybersecurity. The thesis will consider different approaches and methodologies for countering human-oriented cyber attacks, their advantages and disadvantages. Additionally, recommendations will be provided for developing an effective strategy to counter such attacks on enterprise information systems.

Keywords: PROTECTION, METHODS AND TECHNOLOGIES, THREATS, HUMAN-ORIENTED CYBER ATTACKS, PHISHING, VISHING, SOCIAL ENGINEERING.

ЗМІСТ

ВСТУП.....	9
РОЗДІЛ 1: АНАЛІЗ СУЧАСНИХ ЛЮДИНО-ОРІЄНТОВАНИХ КІБЕРАТАК.....	11
1.1. Поняття та характеристики людино-орієнтованих кібератак.....	11
1.2. Методи та стратегії, які використовують кіберзлочинці.....	16
1.3. Аналіз вразливостей інформаційних систем.....	22
1.4. Вплив людино-орієнтованих кібератак на різні сфери.....	24
РОЗДІЛ 2: ПРОЕКТУВАННЯ МЕТОДІВ ТА ТЕХНОЛОГІЙ ПРОТИДІЇ...	29
2.1. Перегляд сучасних підходів до кібербезпеки.....	29
2.2. Розробка комплексних стратегій протидії.....	31
2.3. Інноваційні технологічні рішення в кібербезпеці.....	34
2.4. Організаційні та нормативно-правові аспекти захисту.....	38
2.5. Психологічні аспекти протидії людино-орієнтованим атакам.....	42
РОЗДІЛ 3: ТЕСТУВАННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНИХ МЕТОДІВ.....	47
3.1. Методологія тестування розроблених рішень.....	47
3.2. Проведення пілотних тестів на модельних системах.....	51
3.3. Аналіз результатів тестування.....	57

3.4 розробка комплексних рекомендацій з кібербезпеки: стратегії попередження та забезпечення ефективного захисту від людино- орієнтованих кіберзагроз.....	61
ВИСНОВКИ.....	65
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	67

ВСТУП

Актуальність теми. В епоху, коли інформаційні технології невинно прогресують і глибоко інтегруються в усі аспекти нашого життя, важливість кібербезпеки набуває нових масштабів. Значну увагу заслуговують людино-орієнтовані кібератаки, які застосовують методи соціальної інженерії та психологічного впливу для досягнення своїх мет. Ці атаки особливо небезпечні через свою складність та важкість у виявленні, створюючи реальні загрози для безпеки даних і систем. Відповідно, визнання цієї загрози та розробка ефективних методів її протидії є важливими кроками у захисті інформаційних систем та даних.

У світлі цих викликів, людино-орієнтовані кібератаки, такі як фішинг, соціальна інженерія та інші форми обману, стають дедалі більш поширеними і витонченими. Ці атаки націлені на маніпуляцію людьми, щоб отримати несанкціонований доступ до конфіденційної інформації або інфраструктури, що може призвести до значних фінансових втрат, витоку конфіденційних даних та критичних порушень в роботі систем.

Мета дослідження: Головна мета цієї роботи полягає у розробці та аналізі ефективних методів і технологій протидії людино-орієнтованим кібератакам, з акцентом на інформаційні системи. Це передбачає всебічний аналіз різних аспектів кіберзагроз, детальну оцінку існуючих підходів до кібербезпеки та розробку комплексних стратегій захисту. Для досягнення цієї мети необхідно провести глибоке дослідження існуючих загроз, виявити ключові вразливості сучасних систем та розробити інноваційні рішення, здатні ефективно протистояти цим викликам.

Об'єкт дослідження: Об'єктом дослідження є процес аналізу вразливостей інформаційних систем до людино-орієнтованих кібератак. Розглядаються різні типи систем, від корпоративних мереж до державних інформаційних ресурсів, особливо з огляду на їх важливість та вразливість до таких видів атак.

Предмет дослідження: Предметом дослідження є методи та технології протидії людино-орієнтованим кібератакам. Це включає в себе аналіз існуючих підходів до захисту інформаційних систем, розробку нових стратегій та технічних рішень, а також оцінку їхньої ефективності. Особлива увага приділяється виявленню вразливостей, які можуть бути використані зловмисниками, та розробці комплексних заходів для усунення або мінімізації ризиків, пов'язаних з цими атаками.

1. АНАЛІЗ СУЧАСНИХ ЛЮДИНО-ОРІЄНТОВАНИХ КІБЕРАТАК

1.1. Поняття та характеристики людино-орієнтованих кібератак

З наростанням залежності від цифрових систем і мереж, людино-орієнтовані кібератаки виокремлюються як одна з найбільш хитромудрих та небезпечних загроз у сфері кібербезпеки. Цей пункт присвячений детальному розгляду поняття "людино-орієнтована кібератака", яке охоплює широкий спектр методів і стратегій, націлених на маніпулювання людьми для отримання несанкціонованого доступу до інформації або систем. Ми розглянемо історичний контекст та еволюцію таких атак, зосередимось на основних методах та стратегіях, що використовуються зловмисниками, а також проаналізуємо психологічні аспекти, які лежать в основі цих атак. Окрім цього, буде проведено класифікацію та детальний аналіз різних типів людино-орієнтованих кібератак та визначено потенційні вразливості в інформаційних системах, які можуть сприяти успіху таких атак.

Людино-орієнтовані кібератаки представляють собою вид кіберзлочинності, який включає в себе маніпулювання людьми з метою отримання доступу до конфіденційної інформації або компрометації систем безпеки. Ці атаки, як правило, базуються на використанні соціальної інженерії, замість прямого технічного втручання, та мають на меті використовувати людські емоції, довіру та інші психологічні фактори для досягнення своїх цілей.

Основна характеристика таких атак полягає у маніпуляції та обмані. Зловмисники ретельно планують свої дії, вибираючи жертв на основі їх соціального статусу, професійних обов'язків або навіть особистих інтересів. Вони створюють переконливі сценарії, які можуть включати підроблені електронні листи, повідомлення в соціальних мережах або навіть телефонні дзвінки, щоб ввести жертву в оману та змусити її виконати певні дії, такі як розкриття паролів, конфіденційної інформації або навіть здійснення фінансових операцій.

З історичної точки зору, людино-орієнтовані кібератаки еволюціонували з простих форм шахрайства до високорозвинених стратегій, які використовують складні техніки соціальної інженерії. У минулому, такі атаки часто полягали у прямому обмані або введенні в оману через телефонні дзвінки або листування. З розвитком цифрових технологій та Інтернету, атаки стали більш витонченими, використовуючи електронну пошту, соціальні мережі та інші онлайн-платформи для розсилання фішингових повідомлень або створення підроблених веб-сайтів.

Сучасні методи людино-орієнтованих кібератак можуть включати складні схеми, такі як використання психологічних тригерів для викликання співчуття, страху або інших емоцій, щоб переконати жертву виконати дії, які її власні інстинкти могли б заборонити. Наприклад, кіберзлочинці можуть використовувати техніку "спуфінгу" — створення електронних листів або веб-сайтів, які виглядають як легітимні, але насправді є шахрайськими. Інший поширений метод — "бейтінг", коли жертві пропонуються привабливі умови або нагороди в обмін на виконання певних дій, які ведуть до компрометації її безпеки. [1]

Освіта та обізнаність користувачів є ключовими факторами у протидії таким атакам. Розуміння того, як і чому людино-орієнтовані атаки виявляються ефективними, дозволяє краще підготуватися та розвинути стратегії для їх попередження та мінімізації потенційних шкідливих наслідків. Вивчення цієї теми відкриває широкі можливості для подальших досліджень та розробки ефективних методів захисту від цих складних та витончених кіберзагроз.

Людино-орієнтовані кібератаки використовують різноманітні методи та стратегії, які спрямовані на експлуатацію людських слабкостей та психологічних вразливостей. Основна мета таких атак – обдурити користувачів або спонукати їх до дій, які можуть призвести до витоку конфіденційної інформації або навіть до компрометації цілих систем. Серед типових методів, які використовують зловмисники, можна виділити фішинг, соціальну інженерію, вішинг, спуфінг та бейтінг.

Фішинг – це один з найпоширеніших методів, який включає надсилання електронних листів або повідомлень, які мімікують під легітимні запити від відомих організацій або осіб. Такі листи часто містять посилання, які ведуть на підроблені веб-сайти, де жертвам пропонується ввести свої персональні дані, такі як логіни, паролі або банківські реквізити.

Соціальна інженерія використовує психологічні маніпуляції для залучення жертв до виконання необдуманих дій. Це може включати створення сценаріїв, які викликають у жертви відчуття терміновості, страху або жалю, спонукаючи їх виконати певні дії, які можуть призвести до компрометації.

Вішинг – це форма фішингу, яка використовує телефонні дзвінки замість електронних листів. Зловмисники можуть представлятися співробітниками банків, технічної підтримки або інших організацій, щоб обдурити жертву та отримати конфіденційну інформацію.

Спуфінг включає використання підроблених електронних листів, веб-сайтів або навіть номерів телефонів, щоб ввести в оману жертву та переконати її у легітимності контакту. Це може призвести до витоку конфіденційної інформації або навіть до установки шкідливого програмного забезпечення.

Бейтінг використовує привабливі пропозиції або нагороди як приманку для залучення жертви до виконання певних дій, які можуть призвести до компрометації.

Прикладами відомих сценаріїв таких атак можуть бути масові кампанії з фішингу, які використовували електронну пошту для поширення шкідливих вірусів, чи випадки, коли зловмисники використовували соціальні мережі для здобуття довіри жертви та подальшого отримання конфіденційної інформації. Ці методи демонструють, як зловмисники використовують людську наївність, довіру та інші психологічні фактори, щоб досягти своїх цілей. Вивчення цих методів дозволяє краще зрозуміти механізми кібератак та розробити стратегії для їх протидії.

Для розуміння масштабів проблеми, варто розглянути графік фішингових атак за останні роки, який показує як розвивається дане напрямлення людино-орієнтовної атаки.

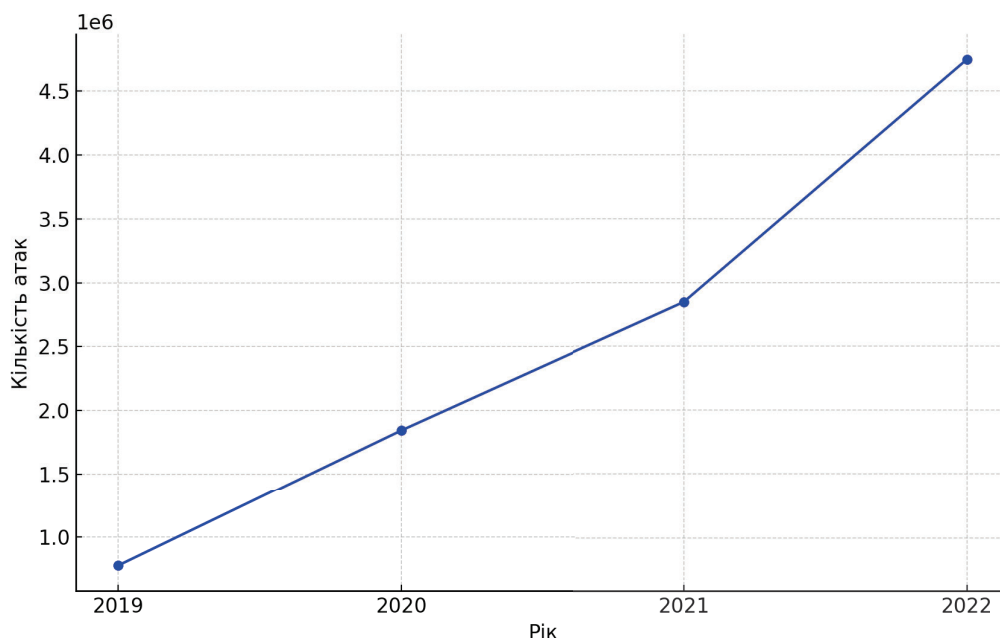


Рисунок 1 – Кількість фішингових листів за 2019-2022 роки (кількість атак вимірюється в трильйонах)

Психологічний аспект людино-орієнтованих кібератак відіграє вирішальну роль у успіху цих атак, оскільки кіберзлочинці активно використовують психологічні маніпуляції для досягнення своїх цілей. Майстерність кіберзлочинців у психологічних маніпуляціях дозволяє їм ефективно впливати на своїх жертв, використовуючи різноманітні тактики, щоб спонукати їх до виконання певних дій або розголошення конфіденційної інформації. априклад, кіберзлочинці можуть надсилати електронні листи, які виглядають як офіційні повідомлення від банку або іншої установи, попереджаючи про нібито проблеми з обліковим записом жертви та вимагаючи негайних дій. Інші методи включають створення ситуацій, коли жертва відчуває соціальний тиск або потребу виконати певні дії, щоб відповідати очікуванням інших. [4]

Вивчення способів, якими атакуються індивіди та організації, показує, що кіберзлочинці часто вибирають своїх жертв на основі конкретних характеристик,

таких як недостатнє розуміння технологій, високий рівень довіри або недостатня обізнаність щодо питань кібербезпеки. У корпоративному середовищі такі атаки можуть бути спрямовані на працівників з доступом до цінної інформації або критичних систем, де вони використовують соціальну інженерію, щоб обійти традиційні системи безпеки.

Розуміння цих психологічних аспектів є ключовим для розробки ефективних стратегій протидії людино-орієнтованим кібератакам. Це включає не лише технічні заходи безпеки, але й освітні програми, які зосереджуються на підвищенні обізнаності працівників та користувачів щодо потенційних кіберзагроз та методів їх виявлення. Ключ до успішної протидії полягає у розумінні того, що людський фактор часто є найслабшою ланкою в системі кібербезпеки, та у розробці комплексного підходу до захисту, який включає як технічні, так і організаційні аспекти.

Аналіз вразливостей цільових об'єктів в контексті людино-орієнтованих кібератак виявляє ключові аспекти інформаційних систем та людської поведінки, які роблять їх вразливими до таких загроз. Ці вразливості можуть бути як технічними, так і пов'язаними з людським фактором, і їх розуміння є критично важливим для розробки ефективних стратегій захисту.

У сфері інформаційних технологій, вразливості часто пов'язані з недостатньою сек'юритизацією систем, такою як слабкі паролі, відсутність двофакторної аутентифікації, неправильне налаштування мережевих протоколів або застаріле програмне забезпечення. Ці технічні вразливості можуть стати точками входу для кіберзлочинців.

Пропозиції щодо зменшення цих вразливостей включають комплексний підхід до кібербезпеки. Серед основних заходів – регулярне оновлення та патчування програмного забезпечення, використання сильних паролів і двофакторної аутентифікації, а також регулярні аудити безпеки інформаційних систем. Що стосується людського фактору, важливо проводити регулярні навчальні сесії та тренінги для працівників, щоб підвищити їх обізнаність про потенційні кіберзагрози та правильні способи дії у випадку виявлення підозрілої

діяльності. Важливо також створити культуру безпеки в організації, де кожен працівник відчуває відповідальність за загальну кібербезпеку.

В цілому, зменшення вразливостей до людино-орієнтованих кібератак вимагає поєднання технічних заходів безпеки, освітніх ініціатив та зміцнення корпоративної культури безпеки. Тільки комплексний підхід може забезпечити ефективний захист від таких складних і витончених загроз.

У цьому підрозділі було розглянуто різноманітні аспекти людино-орієнтованих кібератак, включаючи їхнє визначення, основні методи та стратегії, психологічний аспект, різновиди атак та аналіз вразливостей цільових об'єктів. Встановлено, що центральним елементом таких атак є маніпулювання людською психологією, використання соціальної інженерії та психологічних маніпуляцій. Фішинг, соціальна інженерія, вішинг, спуфінг та бейтінг були ідентифіковані як основні методи, що використовуються в таких атаках.

Аналіз показав, що індивіди та організації часто стають уразливими через недостатню обізнаність про ризики, технічні слабкості систем та людські фактори, такі як відсутність критичного мислення щодо кібербезпеки. Виходячи з цього, для зменшення вразливостей важливо використовувати комплексний підхід, який включає як технічні заходи безпеки, так і навчання та підвищення обізнаності співробітників.

Заключно, ефективна протидія людино-орієнтованим кібератакам вимагає не тільки технічного забезпечення та оновлення систем, але й постійного освітнього процесу, спрямованого на збільшення обізнаності усіх учасників інформаційного процесу, що дозволить створити ефективний бар'єр проти цих складних та різноманітних загроз.

1.2. Методи та стратегії, які використовують кіберзлочинці

У цьому підрозділі ми зосередимося на детальному аналізі різноманітних методів та стратегій, які застосовують кіберзлочинці. Особлива увага буде приділена розумінню того, як зловмисники адаптують та удосконалюють свої методики для проникнення в інформаційні системи та здійснення шкідливої діяльності. Метою цього аналізу є ідентифікація ключових підходів, які використовують кіберзлочинці, та вивчення ефективних методів їх протидії.

Фішингові атаки представляють собою складну стратегію обману, яка використовується кіберзлочинцями для введення в оману користувачів і змушування їх розкривати конфіденційну інформацію. Зазвичай цей процес включає створення підроблених електронних листів або веб-сайтів, що імітують легітимні ресурси. Ключовим елементом таких атак є їхня здатність переконати жертву, що дія необхідна або невідкладна, наприклад, шляхом попередження про нібито проблеми з безпекою облікового запису або пропозиції про виграш у лотереї.

Важливим аспектом фішингу є використання психологічних прийомів для маніпуляції жертвою. Зловмисники часто вдаються до тактик, які викликають відчуття терміновості або страху, спонукаючи людей діяти імпульсивно, без належного розмірковування. Це може включати погрози блокування облікового запису, фінансові збитки або інші негативні наслідки в разі невиконання вимог.

Виявлення та протидія фішинговим атакам вимагає обізнаності та вдумливості з боку користувачів. Ефективні заходи включають ретельну перевірку походження електронних листів, недовіру до листів з невідомих джерел або з незвичайними проханнями, а також використання двофакторної аутентифікації та інших технологічних рішень для захисту облікових записів. Важливо також постійно підвищувати рівень обізнаності про кіберзагрози, особливо у корпоративному середовищі, де наслідки успішної фішингової атаки можуть бути особливо руйнівними.[7]

Використання шкідливого програмного забезпечення (ПЗ) є ще одним з основних методів, які використовують кіберзлочинці для компрометації систем. Цей процес включає розробку та розповсюдження вірусів, троянських коней, шпигунських програм та інших видів шкідливих програм. Основна мета таких дій – непомітно проникнути в інформаційні системи та виконувати шкідливі дії, такі як крадіжка даних, знищення файлів або навіть взяття контролю над цілими системами.

Шкідливе ПЗ може бути розповсюджене різними способами. Одним з найпоширеніших є використання фішингових атак, де користувачів спонукають завантажити шкідливі файли через електронні листи або шахрайські веб-сайти. Інший метод – експлуатація вразливостей у програмному забезпеченні, де зловмисники використовують неправильно налаштоване або застаріле ПЗ для впровадження своїх шкідливих програм.

Троянські коні, які маскуються під легітимні програми, але містять шкідливі компоненти, є одним з найбільш підступних засобів кібератак. Вони можуть надати зловмисникам віддалений доступ до системи жертви, дозволяючи виконувати різноманітні шкідливі дії. Шпигунське ПЗ, в свою чергу, зосереджене на стеженні за діяльністю користувачів, записуючи натискання клавіш, веб-перегляд та іншу інформацію.[16]

Для протидії шкідливому ПЗ важливо використовувати надійні антивірусні програми, регулярно оновлювати всі компоненти системи та здійснювати постійний моніторинг мережевої активності. Крім того, освітні програми для користувачів та співробітників, які зосереджені на виявленні шкідливих програм та підозрілих повідомлень, також відіграють важливу роль у захисті від таких загроз. Належне управління цифровою безпекою та обізнаність про поточні кіберзагрози є ключовими елементами ефективної стратегії захисту від шкідливого програмного забезпечення.

Атаки з використанням експлойтів становлять собою ще одну серйозну загрозу в сфері кібербезпеки, де зловмисники використовують вразливості в програмному та апаратному забезпеченні для проникнення в системи. Експлойти

– це коди або техніки, які використовують слабкі місця в системах, дозволяючи кіберзлочинцям отримати несанкціонований доступ, виконати шкідливі команди або навіть повністю контролювати систему.

Одним із засобів проведення таких атак є використання вразливостей у програмному забезпеченні, таких як операційні системи, веб-браузери або додатки. Ці вразливості можуть виникати через помилки в кодуванні або неналежне налаштування систем. Кіберзлочинці шукають такі слабкі місця, часто використовуючи відомі бази даних вразливостей, а потім розробляють експлойти для їх експлуатації.

Атаки, що використовують експлойти на апаратному рівні, включають вразливості в компонентах комп'ютерного обладнання, наприклад, у процесорах або мережевих картках. Ці атаки можуть бути більш складними для виявлення та усунення, оскільки вони вимагають фізичного оновлення або заміни обладнання.

Для протидії таким атакам важливо регулярно оновлювати та патчувати всі компоненти системи, включаючи програмне та апаратне забезпечення. Також ефективним є використання спеціалізованого програмного забезпечення для виявлення та блокування експлойтів. Аудити безпеки та використання інструментів для виявлення вразливостей можуть виявити потенційні слабкі місця, перш ніж вони будуть експлуатуватися зловмисниками.

Ефективна стратегія захисту від атак з використанням експлойтів вимагає комплексного підходу, що включає технічні, організаційні та освітні заходи для забезпечення всебічного захисту інформаційних систем від цього типу кіберзагроз.

Соціальна інженерія та маніпуляції представляють собою один з найбільш підступних методів кіберзлочинності, який використовується для обману людей. На відміну від традиційних кібератак, які спираються на технічні засоби, соціальна інженерія використовує людські емоції та психологічні слабкості для досягнення своїх цілей.

Основні прийоми соціальної інженерії включають створення довіри, викликання співчуття або страху, використання тиску або авторитету та обіцянку вигоди. Наприклад, зловмисники можуть прикидатися співробітниками служби підтримки або представниками відомих компаній, щоб переконати жертву надати особисту інформацію або виконати дії, які можуть призвести до витоку даних чи фінансових втрат.

Також використовуються схеми, які створюють ілюзію терміновості чи необхідності негайної дії, спонукаючи людину діяти без достатнього аналізу ситуації. Це може бути, наприклад, шахрайське повідомлення про необхідність негайної зміни паролю або про сплату неіснуючого боргу.

Для протидії таким атакам важливо розвивати критичне мислення та обізнаність серед співробітників та користувачів. Це включає регулярні тренінги та інформування про поширені схеми соціальної інженерії, а також навчання, як правильно реагувати на підозрілі запити або повідомлення. Також корисним є впровадження корпоративних політик та процедур, які допомагають ідентифікувати та управляти ризиками, пов'язаними з людським фактором.

Розширені тривалі атаки (APT) становлять собою особливо складну форму кіберзагроз, спрямовану на конкретні організації або інфраструктури. Відрізняючись від традиційних кібератак своєю тривалістю та витонченістю, APT спрямовані на довготривале проникнення в системи з метою крадіжки конфіденційної інформації або підризу інфраструктур.

Основною характеристикою APT є їхній цілеспрямований характер. Зловмисники, які проводять APT, ретельно планують свої дії, використовуючи різноманітні методи для проникнення в системи. Це може включати в себе соціальну інженерію, експлойти, шкідливе програмне забезпечення та різноманітні тактики маскуванню.

Після проникнення в систему, APT зазвичай залишаються невиявленими протягом тривалого часу, що дозволяє зловмисникам збирати цінну інформацію або готувати інші дії. Вони можуть використовувати спеціальні інструменти для

збору даних, моніторингу мережевого трафіку та управління зараженими системами.

Аналіз АРТ вимагає розуміння витончених методів, які використовуються для проникнення та збереження доступу до цільових систем. Це включає вивчення того, як зловмисники обходять заходи безпеки, маскують свою присутність та здійснюють збір інформації. [2]

Для протидії АРТ важливо мати комплексний підхід до кібербезпеки, який включає передові технології моніторингу та виявлення, регулярні аудити безпеки, а також розвиток культури обізнаності та готовності до кіберзагроз серед співробітників. Ключ до ефективного захисту від АРТ полягає не тільки у застосуванні технологій, але й у забезпеченні постійного навчання та адаптації до змінюваного ландшафту кіберзагроз.

Кібершпигунство та кібервійна являють собою дві важливі аспекти сучасного ландшафту кіберзагроз, де як державні, так і приватні актори здійснюють шпіонаж та проводять операції, що можуть мати глобальні наслідки. Ці діяльності часто здійснюються з метою збору конфіденційної інформації, політичного впливу, або навіть для дестабілізації цілих держав.

Кібершпигунство зазвичай включає використання складних методів і технологій для нелегального збору конфіденційної інформації з комп'ютерних систем. Це може включати проникнення в мережі урядових установ, корпорацій, науково-дослідних центрів або навіть окремих осіб. Методи кібершпіонажу часто включають в себе фішинг, використання шкідливого ПЗ, а також експлойти, які використовують вразливості в програмному забезпеченні.

Кібервійна, з іншого боку, є більш агресивною формою кібердіяльності, яка може включати атаки на критичну інфраструктуру, таку як енергетичні мережі, системи водопостачання або фінансові установи. Ці атаки можуть мати серйозні наслідки, включаючи економічні збитки, соціальний хаос або навіть загрозу життю людей. Кібервійськові операції часто здійснюються у відповідь на політичні конфлікти або як частина стратегії національної безпеки.

Для протидії кібершпіонажу та кібервійськовим операціям важливо використовувати комплексні системи безпеки, включаючи постійний моніторинг мережі, застосування передових технологій виявлення та запобігання вторгнень, а також проведення регулярних аудитів та тренінгів для підвищення обізнаності та готовності до потенційних загроз. Розуміння цих аспектів кіберзагроз є ключовим для розробки ефективних стратегій захисту на національному та міжнародному рівнях, забезпечуючи таким чином захист критично важливих ресурсів та збереження національної безпеки. [9]

1.3 Аналіз вразливостей інформаційних систем

Аналіз технічних вразливостей систем є ключовим елементом у забезпеченні кібербезпеки. Цей процес включає ретельне вивчення слабких місць в програмному забезпеченні, а також аналіз застарілого обладнання або неправильного налаштування системи. Недоліки в програмному забезпеченні можуть бути пов'язані з помилками в коді, недостатнім тестуванням або відсутністю регулярних оновлень безпеки. Ці проблеми можуть стати відкритими дверима для кіберзлочинців, які шукають шляхи для проникнення в системи.

Застаріле обладнання та застарілі технології також створюють значні ризики, оскільки вони часто не підтримують сучасні стандарти безпеки або не сумісні з новітніми оновленнями безпеки. Це може залишити системи вразливими до атак, які використовують відомі вразливості.

Неправильне налаштування системи також є важливим фактором, що сприяє вразливості. Це може включати в себе слабкі налаштування безпеки, неправильне управління доступом або відсутність належного моніторингу мережевої активності. Такі недоліки можуть забезпечити зловмисникам легкий доступ до системи, уможливіючи крадіжку даних, розповсюдження шкідливого програмного забезпечення або навіть повне взяття контролю над системою.

Вивчення та розуміння цих технічних вразливостей є фундаментальним для розробки ефективних стратегій захисту. Це включає в себе регулярні аудити безпеки, оновлення програмного забезпечення та обладнання, а також впровадження ретельних процедур налаштування та моніторингу систем. Тільки через такий всебічний підхід можна мінімізувати ризики, пов'язані з технічними вразливостями, і забезпечити надійний захист інформаційних систем.

Організаційні та управлінські вразливості в інформаційних системах часто виникають через недоліки в управлінських процесах та політиках, що може призводити до суттєвих ризиків безпеки. На відміну від чисто технічних вразливостей, ці проблеми залежать від способу, яким організації управляють та контролюють свої інформаційні ресурси.

Однією з ключових проблем у цьому контексті є недостатня або застаріла політика безпеки. Це може включати відсутність чітких правил щодо обробки та зберігання конфіденційної інформації, неналежне управління доступом до критичних систем, або відсутність належних процедур реагування на інциденти безпеки. Такі недоліки створюють можливості для ненавмисних помилок співробітників або умисних атак ззовні.

Процедури аудиту та моніторингу безпеки також відіграють критичну роль. Неадекватні аудити або відсутність систематичного моніторингу можуть залишити вразливості непоміченими, що створює сприятливі умови для кібератак. Це особливо важливо в контексті швидкого розвитку технологій, де нові загрози можуть з'являтися дуже швидко.

Крім того, людський фактор часто є найбільш вразливою частиною будь-якої системи безпеки. Недостатнє навчання співробітників, низька обізнаність щодо кіберзагроз або відсутність відповідальності та взаєморозуміння внутрішніх процедур можуть призвести до серйозних проблем безпеки.

Враховуючи ці фактори, важливо для організацій розробляти всебічну та адаптовану до сучасних реалій політику безпеки, забезпечувати регулярні аудити та оцінки ризиків, а також впроваджувати культуру безпеки, де кожен

співробітник розуміє свою роль та відповідальність у забезпеченні захисту інформаційних ресурсів.

Вразливості, пов'язані з людським фактором, є одними з найбільш значних і часто недооцінених елементів у загальній структурі кібербезпеки. Помилки або необережні дії співробітників можуть легко стати причиною серйозних порушень безпеки, навіть у системах із сильними технічними захистами.

Недостатня обізнаність співробітників про кібербезпеку часто призводить до помилкових дій, таких як відкриття шкідливих вкладень у фішингових електронних листах, використання слабких або легкодоступних паролів, неналежне управління доступом до конфіденційної інформації або неправильне використання корпоративних мереж. Це може призвести до витоку даних, встановлення шкідливого програмного забезпечення або навіть повного компрометування систем. [5]

Відсутність відповідного навчання також є критичною проблемою. Без регулярного та ефективного навчання, співробітники можуть не бути обізнані щодо поточних кіберзагроз або не вміти правильно реагувати на інциденти безпеки. Це особливо важливо в контексті постійно змінюваного ландшафту кіберзагроз, де нові методи атак швидко з'являються і еволюціонують.

Враховуючи це, критично важливим є впровадження комплексних програм навчання та постійне інформування співробітників про ризики та кращі практики у сфері кібербезпеки. Це включає роз'яснення про наслідки необачних дій в інтернеті, навчання розпізнаванню фішингових атак, а також створення культури безпеки, де кожен працівник розуміє свою роль у захисті інформаційних активів організації. Такий підхід не тільки зменшує ризик виникнення інцидентів, але й забезпечує більш стійкий захист від потенційних кібератак.

1.4 Вплив людино-орієнтованих кібератак на різні сфери

Вплив людино-орієнтованих кібератак на корпоративний сектор охоплює широкий спектр наслідків, починаючи від фінансових збитків до втрати довіри клієнтів і репутаційних ризиків. Підприємства, які стають жертвами таких атак, можуть зіткнутися з величезними витратами на відновлення систем, виплати компенсацій клієнтам та правові витрати. Окрім безпосередніх фінансових втрат, існує також ризик тривалої шкоди для бренду та довіри клієнтів, що може мати далекосяжні наслідки для ділової репутації компанії.

Значний вплив мають також порушення роботи систем, втрата даних або їх крадіжка, що може призвести до зупинки виробничих процесів та інших критичних операцій. Це, у свою чергу, може призвести до втрати конкурентоспроможності та ринкових позицій.

У контексті України за останні кілька років були зафіксовані численні випадки людино-орієнтованих кібератак, які мали значні наслідки для національної безпеки та економіки. Відомі інциденти включають масштабні фішингові атаки та розповсюдження шкідливого програмного забезпечення, що призвело до компрометації важливих державних та приватних систем. Ці події підкреслили необхідність посилення заходів кібербезпеки на національному рівні та збільшення обізнаності серед корпоративного сектору щодо потенційних ризиків та методів протидії таким загрозам.

Державні установи

Вплив людино-орієнтованих кібератак на державні установи має далекосяжні наслідки, які стосуються не лише безпосередньо вразливості інформаційних систем, але й загальної національної безпеки, державного управління та критичної інформаційної інфраструктури. Такі атаки можуть включати спроби здобуття доступу до конфіденційних державних даних, зламу комунікаційних систем, а також намагання дестабілізувати урядові операції.

Національна безпека є особливо вразливою, оскільки кібератаки можуть призвести до витоку секретної інформації, порушення військових комунікацій

або навіть маніпулювання важливими даними. Це створює потенційні загрози не тільки для внутрішньої стабільності країни, але й для її міжнародних відносин.

У контексті державного управління, людино-орієнтовані кібератаки можуть порушити нормальну роботу урядових служб, включаючи соціальні, фінансові та логістичні системи. Це може призвести до затримок у наданні важливих державних послуг, що, в свою чергу, може вплинути на довіру громадян до уряду.

Що стосується України, за останні роки країна зазнала значних кібератак, спрямованих на державні установи та критичну інфраструктуру. Ці атаки включали, серед іншого, впровадження шкідливого ПЗ, що призвело до порушення роботи урядових систем, втрати даних та збоїв у роботі критичних послуг. Наприклад, відомі кібератаки, такі як NotPetya, завдали серйозної шкоди українській інфраструктурі, викликаючи значні фінансові втрати та дестабілізацію державних служб. Ці інциденти підкреслюють необхідність посилення кібербезпеки на державному рівні та важливість розвитку відповідних стратегій для захисту від подібних загроз у майбутньому. [8]

Людино-орієнтовані кібератаки мають значний вплив на індивідуальних користувачів, оскільки вони часто стають цілями для крадіжки особистої інформації, фінансових втрат та зазнають емоційного стресу внаслідок таких інцидентів. Ці атаки можуть включати фішинг, шахрайство з кредитними картками, крадіжку ідентичності та інші види махінацій.

Одним з найпоширеніших наслідків для індивідуальних користувачів є крадіжка особистої інформації. Це може стосуватися банківських даних, паролів, особистої ідентифікаційної інформації, які зловмисники можуть використовувати для незаконних фінансових операцій або для додаткових шахрайських дій.

Фінансові втрати можуть бути безпосередньо пов'язані з крадіжкою грошей з банківських рахунків або кредитних карток, а також з втратами, спричиненими необхідністю відновлення компрометованих систем або зміни особистої ідентифікаційної інформації.

Емоційний вплив таких атак також не слід недооцінювати. Відчуття порушення приватності, стрес та тривога через втрату контролю над особистою інформацією можуть мати довготривалі психологічні наслідки для жертв. Це особливо важливо в контексті зростаючої залежності від цифрових технологій та інтернет-послуг у повсякденному житті.

У випадку України, з огляду на збільшення кіберзлочинності, індивідуальні користувачі також стикаються з ризиками, пов'язаними з цифровими шахрайствами та іншими видами атак. Це підкреслює важливість обізнаності про кіберзагрози та необхідність вжиття заходів щодо особистої кібербезпеки, включаючи обережність при обробці особистої інформації в інтернеті та використанні надійних методів захисту.

Глобальні наслідки людино-орієнтованих кібератак охоплюють широкий спектр важливих аспектів, від міжнародної торгівлі до політичних відносин та загальної економічної стабільності. Такі атаки можуть мати величезний вплив на глобальну економіку, порушуючи нормальне функціонування бізнесу, створюючи політичну напруженість між країнами та підриваючи довіру до міжнародних інституцій.

Вплив на міжнародну торгівлю включає збої в ланцюгах поставок, втрати виробничих потужностей, а також ризики для фінансових транзакцій. Це не лише створює безпосередні фінансові втрати для компаній, але й може призвести до тривалих затримок і збитків у глобальних поставках товарів та послуг.

Політичні відносини також потерпають від кібератак, оскільки вони часто використовуються як інструмент геополітичного протистояння. Кібератаки можуть бути спрямовані на урядові структури, політичні партії або навіть виборчі процеси, що викликає напруженість і підриває довіру між державами.

Що стосується України, країна зіткнулася з кількома значними кібератаками, які мали міжнародні наслідки. Наприклад, у червні 2017 року вірус NotPetya, спочатку спрямований на Україну, швидко поширився по всьому світу, порушивши роботу численних міжнародних компаній, включаючи Maersk, Merck, Saint-Gobain та інші. Ця атака не лише завдала серйозних збитків

українській інфраструктурі, але й вплинула на глобальні економічні процеси, демонструючи, наскільки швидко кіберзагрози можуть перетворитися на глобальні кризи.

Ці приклади підкреслюють необхідність глобальної співпраці та координації у сфері кібербезпеки, а також важливість розробки комплексних стратегій для захисту від таких загроз на національному та міжнародному рівнях.

[3]

2.ПРОЕКТУВАННЯ МЕТОДІВ ТА ТЕХНОЛОГІЙ ПРОТИДІЇ

2.1. Перегляд сучасних підходів до кібербезпеки

Оцінка сучасних технологій кібербезпеки включає в себе аналіз широкого спектру інноваційних інструментів та методів, які використовуються для захисту інформаційних систем. Штучний інтелект (ШІ) та машинне навчання є одними з передових технологій в цій галузі. Вони здатні аналізувати великі обсяги даних, виявляючи незвичайну поведінку або патерни, які можуть вказувати на потенційні безпекові загрози. Це особливо корисно для виявлення складних атак, які можуть залишитися непоміченими традиційними системами безпеки.

Крім цього, криптографія грає ключову роль у захисті даних та комунікацій. Застосування сучасних криптографічних методів, таких як шифрування з відкритим ключем, забезпечує безпечне зберігання та передачу конфіденційної інформації. Це знижує ризики пов'язані з несанкціонованим доступом або витоком даних.

Також важливою є роль систем виявлення вторгнень та запобігання вторгненням, які використовуються для моніторингу мережевої активності та блокування підозрілого трафіку. Ці системи постійно оновлюються для виявлення нових видів атак, забезпечуючи таким чином більш ефективний захист проти найсучасніших загроз.

У сфері кібербезпеки також набуває поширення використання технологій блокчейну, які можуть забезпечити додатковий рівень безпеки за рахунок децентралізованого зберігання даних та прозорості транзакцій. Це допомагає зменшити ризики зламу або маніпуляції інформацією.

Підходи до захисту від кібератак постійно еволюціонують, оскільки кіберзлочинці постійно розвивають нові методики та стратегії. В цьому контексті важливо розробляти та застосовувати різні стратегії захисту, щоб ефективно протистояти потенційним загрозам. Ці стратегії включають як проактивні, так і реактивні підходи до управління кіберризиками.

Проактивні стратегії спрямовані на запобігання кібератакам ще до того, як вони відбудуться. Вони включають регулярні аудити та оцінки вразливостей, навчання співробітників, розробку та впровадження сильних політик безпеки, та використання передових технологій для захисту систем. Наприклад, використання штучного інтелекту та машинного навчання для виявлення підозрілих патернів поведінки може допомогти ідентифікувати потенційні загрози до того, як вони стануть проблемою. [13]

З іншого боку, реактивні стратегії фокусуються на мінімізації шкоди після відбуття атаки. Це включає розробку планів реагування на інциденти, які дозволяють швидко і ефективно реагувати на кібератаки, зменшуючи їх вплив та відновлюючи нормальну роботу систем. Реактивні заходи також включають постійне моніторинг мережевої активності та аналіз безпекових інцидентів для постійного вдосконалення захисних стратегій.

Роль освіти та навчання у сфері кібербезпеки не може бути переоцінена, оскільки вони є критичними компонентами в загальній стратегії захисту інформаційних систем. Підвищення рівня обізнаності та навичок співробітників щодо кіберзагроз та методів їхньої протидії є ключовим для запобігання безпековим інцидентам.

Освітні програми та тренінги дозволяють співробітникам краще розуміти, як вони можуть стати цілями кібератак, і навчають їх виявляти підозрілі дії, такі як фішингові електронні листи чи шкідливі вкладення. Навчання також зосереджується на навчанні безпечних практик, таких як використання сильних паролів, застосування двофакторної аутентифікації та уникнення підозрілих веб-сайтів.

Крім того, регулярні симуляції кібератак можуть допомогти співробітникам краще зрозуміти реальні загрози та навчити їх ефективно реагувати в кризових ситуаціях. Це особливо важливо для підготовки до потенційних інцидентів, оскільки забезпечує розуміння процедур реагування на інциденти та дозволяє швидко відновлювати нормальну роботу після атак.

Також хорошою практикою є впровадження політик безпеки на практиці. Цей процес включає розробку та виконання стандартів, процедур та рекомендацій, які мають на меті мінімізувати ризики та захистити інформаційні активи. [10]

Розробка політик безпеки починається з визначення ключових активів та потенційних загроз. На цій основі розробляються специфічні стандарти та процедури, які враховують особливості діяльності та структуру організації. Це може включати правила щодо користування мережевими ресурсами, управління доступом до даних, процедури резервного копіювання та відновлення даних, а також дії у випадку безпекових інцидентів.

Дотримання політик безпеки забезпечується через регулярні перевірки та аудити. Це включає моніторинг виконання встановлених правил та процедур, аналіз ефективності заходів безпеки та впровадження необхідних корективних дій у разі виявлення проблем.

Врешті-решт, успішне впровадження політик безпеки залежить від постійного оцінювання та адаптації до змінюваних умов та загроз. Це вимагає гнучкості та відкритості до інновацій, що дозволяє організації ефективно реагувати на нові виклики у сфері кібербезпеки.

2.2. Розробка комплексних стратегій протидії

Інтеграція технологій та процедур безпеки є ключовою для створення ефективної та комплексної системи кібербезпеки. Цей процес включає поєднання різноманітних інструментів, технологій та методик, щоб забезпечити всебічний захист від широкого спектру кіберзагроз.

Основною метою інтеграції є створення цілісної системи, яка може ефективно виявляти, протистояти та відновлюватися після кібератак. Для досягнення цього, важливо інтегрувати технології виявлення та запобігання вторгнень, шифрування даних, системи управління ідентифікацією та доступом, а також інструменти моніторингу та аналізу.

Одним з кроків є інтеграція штучного інтелекту та машинного навчання для більш точного виявлення та аналізу потенційних загроз. Це дозволяє системам безпеки швидко адаптуватися до нових видів кібератак, навіть якщо вони раніше не були відомі.

Ще одним аспектом інтеграції є поєднання фізичних та цифрових заходів безпеки. Це включає в себе захист фізичних серверів та мережевих пристроїв, а також використання різноманітних програмних інструментів для захисту даних та систем.

Крім технічних рішень, важливим є врахування організаційних аспектів, таких як розробка та впровадження ефективних політик безпеки, процедур відповіді на інциденти та навчання співробітників. Це допомагає створити обізнану та підготовлену до ризиків культуру в організації.

Інтеграція різних елементів безпеки у єдину систему дозволяє не тільки захистити організацію від існуючих загроз, але й гнучко адаптуватися до нових викликів у майбутньому, забезпечуючи стабільний та ефективний захист від кібератак.

Аналіз та управління ризиками у сфері кібербезпеки є важливими компонентами стратегії протидії кібератакам. Це процес, який включає ідентифікацію потенційних загроз, оцінку вразливостей, які можуть бути використані зловмисниками, та розробку ефективних стратегій для мінімізації цих ризиків.

На першому етапі, ідентифікація ризиків, проводиться аналіз потенційних загроз, що можуть вплинути на інформаційні системи. Це можуть бути зовнішні загрози, такі як хакерські атаки, фішинг, шпигунське програмне забезпечення, а також внутрішні загрози, такі як помилки співробітників або неналежне управління даними.

Після ідентифікації загроз проводиться оцінка ризиків, яка включає аналіз потенційного впливу та ймовірності виникнення кожної із загроз. Це допомагає визначити, які ризики є найбільш критичними та потребують негайної уваги.

На основі цього аналізу розробляються стратегії управління ризиками, які включають різні заходи для їх зменшення або усунення. Це може включати технічні рішення, такі як впровадження сучасних технологій захисту, а також організаційні заходи, такі як розробка політик безпеки, навчання персоналу та розробка планів реагування на інциденти. [14]

Ефективне управління ризиками вимагає постійного моніторингу та адаптації до змінюваних умов. Це забезпечує, що стратегії захисту залишаються актуальними та ефективними у відповідь на нові види загроз та викликів у сфері кібербезпеки.

Планування реагування на інциденти кібербезпеки є важливою частиною комплексної стратегії протидії кібератакам. Цей процес включає розробку детальних планів, які визначають, як організація повинна реагувати на різні види безпекових порушень. Ефективне реагування на інциденти може значно зменшити збитки від атак та прискорити процес відновлення.



Рисунок 2 – План реагування на інциденти кібербезпеки

План реагування на інциденти зазвичай включає наступні ключові елементи:

1. Процедури виявлення: Це включає в себе механізми для швидкого і точного виявлення кібератак або безпекових порушень. Використання сучасних систем виявлення та моніторингу дозволяє оперативно ідентифікувати підозрілі дії або аномалії в системі.

2. Процедури ізоляції: У випадку виявлення атаки важливо швидко ізолювати уражені системи або мережі, щоб запобігти поширенню загрози. Це може включати відключення від мережі, блокування підозрілого трафіку або відокремлення уражених ділянок системи.

3. Процедури відновлення: Відновлення після атаки включає в себе відновлення зіпсованих або втрачених даних з резервних копій, відновлення функціональності систем та впровадження необхідних змін для запобігання майбутнім атакам.

4. Аналіз після атаки: Після реагування на інцидент важливо провести детальний аналіз, щоб зрозуміти, як атака була здійснена, які вразливості були використані, та як можна покращити стратегії безпеки для запобігання подібним інцидентам у майбутньому.

Розробка ефективних планів реагування на інциденти є важливою частиною стратегії протидії кібератакам, оскільки вона забезпечує, що організація підготовлена відповідати на інциденти швидко та ефективно, мінімізуючи потенційні збитки та прискорюючи процес відновлення. [21]

2.3. Інноваційні технологічні рішення в кібербезпеці

Інноваційні технологічні рішення в кібербезпеці відіграють вирішальну роль у боротьбі з людино-орієнтованими кібератаками. Оскільки ці атаки часто базуються на використанні соціальної інженерії та психологічних маніпуляцій для введення в оману співробітників і отримання доступу до конфіденційної інформації, традиційні методи захисту можуть бути недостатніми. Саме тому

розвиток та впровадження передових технологій та методик є ключовими для ефективного захисту організацій від таких специфічних загроз.

Застосування штучного інтелекту, машинного навчання, розширених аналітичних інструментів та інтерактивних методів навчання відкриває нові можливості для ідентифікації та протидії цим складним атакам. Ці технології можуть допомогти виявляти аномалії у поведінці користувачів, відслідковувати сигнали фішингу та навчати співробітників визначати та уникати потенційних загроз. Такий інтегрований підхід є необхідністю в сучасному світі, де кіберзагрози стають все більш витонченими та важко виявними.

Поведінковий аналіз та алгоритми штучного інтелекту (ШІ) відіграють ключову роль у виявленні та протидії людино-орієнтованим кібератакам. Штучний інтелект може аналізувати великі обсяги даних значно швидше та ефективніше, ніж це здатна зробити людина. Використання алгоритмів ШІ для моніторингу поведінки користувачів включає в себе спостереження за їх звичайними діями та визначення відхилень від цієї поведінки. Наприклад, несподівані спроби доступу до конфіденційних даних, незвичайні часи входу в систему або нехарактерні мережеві запити можуть бути індикаторами фішингу чи інших видів соціальної інженерії.

Крім того, алгоритми машинного навчання можуть "навчатися" з історичних даних про безпекові інциденти, постійно покращуючи свою здатність виявляти нові та складні кібератаки. Це включає адаптацію до нових методів, які використовують зловмисники, та розробку більш точних моделей для прогнозування потенційних атак.

Використання ШІ для поведінкового аналізу також сприяє більш швидкому реагуванню на інциденти. У випадку виявлення підозрілої активності системи можуть автоматично вживати заходів, таких як блокування доступу до підозрілих користувачів або сповіщення адміністраторів безпеки.

Таким чином, інтеграція алгоритмів ШІ у системи кібербезпеки відкриває нові можливості для захисту від людино-орієнтованих атак, забезпечуючи більш глибокий та комплексний аналіз поведінки користувачів та мережевих операцій.

Розвиток систем фішинг-розвідки є критично важливим у контексті боротьби з людино-орієнтованими кібератаками, особливо коли йдеться про спроби фішингу та соціальної інженерії. Ці технології фокусуються на виявленні та блокуванні спроб обману, заснованого на використанні підроблених електронних листів, веб-сайтів або інших комунікаційних каналів.

Однією з ключових функцій таких систем є аналіз контенту електронних листів. Це включає в себе сканування тексту на предмет підозрілих фраз, перевірку вкладень на наявність шкідливого програмного забезпечення та оцінку загалом надійності відправника. За допомогою алгоритмів машинного навчання та штучного інтелекту, ці системи можуть виявляти навіть дуже витончені спроби фішингу, які традиційні фільтри безпеки можуть пропустити.

Крім аналізу електронних листів, розвідка фішингу також включає моніторинг веб-сторінок. Це може бути аналіз веб-сайтів на предмет підозрілого або шкідливого контенту, перевірка автентичності доменних імен та оцінка загальної безпеки сайтів. Такий підхід дозволяє ідентифікувати та блокувати фішингові сайти, які імітують законні ресурси для крадіжки конфіденційної інформації.

Системи фішинг-розвідки також часто включають інструменти для освіти та навчання користувачів, допомагаючи їм виявляти та уникати потенційних фішингових атак. Це може включати регулярні тренінги, симуляції фішингових атак та інформаційні кампанії.

У цілому, розвиток та впровадження систем фішинг-розвідки є ключовим елементом у стратегії кібербезпеки будь-якої організації, забезпечуючи важливий рівень захисту від людино-орієнтованих атак.

Інтерактивне навчання та симуляції атак є важливими інструментами у боротьбі з людино-орієнтованими кібератаками, зокрема з тими, що базуються на соціальній інженерії. Ці методи навчання залучають співробітників у реалістичні сценарії, допомагаючи їм розвивати необхідні навички та рефлексії для виявлення та протидії атакам.

Інтерактивне навчання може включати в себе онлайн-курси, ігрові симуляції та віртуальні тренінги, які імітують різні види соціальної інженерії, включаючи фішинг, спуфінг або шкідливі атаки. Через практичний досвід у таких симуляціях співробітники навчаються розпізнавати сигнали загрози та відповідно реагувати на них.

Симуляції атак можуть бути особливо ефективними, оскільки вони дозволяють співробітникам пережити віртуальні кібератаки в контрольованому середовищі. Це не тільки допомагає їм краще зрозуміти, як діють зловмисники, але й вчить ефективним стратегіям протидії. Наприклад, симуляції можуть включати імітацію фішингових електронних листів або повідомлень, що дозволяє співробітникам практикувати ідентифікацію та відповідне реагування на такі загрози. [11]

Розширені аналітичні інструменти відіграють вирішальну роль у виявленні та протидії людино-орієнтованим кібератакам. Ці інструменти забезпечують глибокий аналіз даних, що дозволяє виявляти складні та часто приховані загрози, які можуть бути пропущені стандартними безпековими рішеннями.

Одним з ключових елементів таких інструментів є їхня здатність аналізувати великі обсяги даних для виявлення аномальної поведінки користувачів або нестандартних мережевих запитів. Це може включати незвичайні моделі доступу до даних, непередбачувані зміни в поведінці користувачів або незвичні комунікації між системами. Наприклад, спроби доступу до чутливих даних з неавторизованих або незвичайних місць можуть вказувати на потенційні спроби фішингу або інші атаки соціальної інженерії.

Розширені аналітичні інструменти часто використовують складні алгоритми та методи машинного навчання для пошуку кореляцій та закономірностей, які можуть бути неочевидні для людини. Це дозволяє їм виявляти складні атаки, які використовують витончені методи для уникнення виявлення стандартними засобами безпеки.

Крім виявлення загроз, ці інструменти також можуть використовуватися для проведення постінцидентного аналізу. Це включає в себе вивчення даних про

інциденти для виявлення слабких місць системи та розробки рекомендацій щодо посилення заходів безпеки.

Використання розширених аналітичних інструментів дозволяє організаціям не тільки виявляти та реагувати на поточні загрози, але й прогнозувати майбутні виклики, підвищуючи загальний рівень кібербезпеки та підготовленість до людино-орієнтованих кібератак.

2.4. Організаційні та нормативно-правові аспекти захисту

У цьому розділі ми зосередимося на критично важливих елементах, які визначають, як організації можуть структурувати та управляти своїми процесами кібербезпеки відповідно до внутрішніх та зовнішніх вимог. У цьому контексті важливо розглянути не лише технічні аспекти захисту, але й організаційні структури, політики та процедури, які підтримують цілісну та ефективну стратегію кібербезпеки.

Особливу увагу буде приділено розробці внутрішніх політик безпеки, які відповідають як організаційним цілям, так і зовнішнім нормативно-правовим вимогам. Це включає аналіз регуляторного середовища, у якому діє організація, та визначення кращих практик для забезпечення відповідності цим вимогам.

Додатково буде розглянуто, як оцінка ризиків і управління вразливостями на організаційному рівні може допомогти у прогнозуванні та запобіганні потенційним загрозам. Також важливою є роль навчання персоналу та розвитку компетенцій у сфері кібербезпеки, а також залучення зовнішніх експертів для надання спеціалізованої допомоги та порад.

Розробка та впровадження внутрішніх політик безпеки є фундаментальним елементом у забезпеченні ефективного захисту організації від кіберзагроз. Цей процес вимагає ретельного аналізу організаційних потреб, цілей та специфіки діяльності для розробки політик, які будуть не тільки відповідати цим вимогам, але й забезпечувати комплексний захист.

На першому етапі розробки політик важливо визначити ключові активи організації, які потребують захисту, та потенційні ризики для цих активів. Це

може включати конфіденційні дані, інтелектуальну власність, інфраструктурні компоненти та інші критичні ресурси. Під час цього аналізу також важливо враховувати поточне регуляторне середовище та законодавчі вимоги, щоб забезпечити, що політики будуть відповідати всім нормативним стандартам.

Наступним кроком є розробка конкретних стандартів та процедур, які будуть впроваджені в організації. Це може включати політики доступу до даних, процедури криптографічного захисту, регламенти щодо фізичної безпеки обладнання та інші важливі аспекти. Важливим є забезпечення, що ці політики є зрозумілими для всіх співробітників та легко впроваджуваними в повсякденній роботі.

Після розробки політик наступним етапом є їх впровадження та моніторинг дотримання. Це може включати організацію навчальних сесій для співробітників, встановлення процесів перевірки та аудиту, а також регулярне оновлення політик у відповідності до змін в технологічному середовищі та зовнішньому регуляторному ландшафті.

У цілому, розробка та впровадження внутрішніх політик безпеки є необхідністю для створення стабільного та безпечного робочого середовища. Це не тільки забезпечує захист від зовнішніх та внутрішніх загроз, але й допомагає підвищити загальну обізнаність та відповідальність усіх співробітників щодо кібербезпеки.

Дотримання законодавчих та регуляторних вимог є фундаментальним аспектом кібербезпеки, особливо у контексті швидкого розвитку цифрових технологій та зростаючої кількості кіберзагроз. В Україні, де сектор кібербезпеки постійно розвивається та адаптується до нових викликів, важливо забезпечити відповідність законодавству, а також міжнародним стандартам.

Одним з ключових моментів є розуміння та впровадження законодавчих вимог, що стосуються кібербезпеки. Це може включати закони про захист даних, правила щодо зберігання та передачі конфіденційної інформації, а також вимоги до рівня безпеки інформаційних систем. Україна, зі своїм активним цифровим сектором, постійно працює над удосконаленням свого законодавства у сфері кібербезпеки, щоб відповідати як національним, так і глобальним стандартам.

Крім законодавчого регулювання, організаціям в Україні важливо звертати увагу на міжнародні стандарти, такі як ISO/IEC 27001, що встановлюють вимоги до систем управління інформаційною безпекою. Дотримання цих стандартів не лише забезпечує високий рівень захисту, але й сприяє підвищенню довіри клієнтів та партнерів. [18]

Також важливим є розуміння специфіки нормативно-правового регулювання в контексті ведення міжнародної діяльності. Це вимагає від українських організацій бути в курсі регуляторних змін не тільки в Україні, але й у країнах, де вони ведуть бізнес або мають партнерів.

Оцінка ризиків та управління вразливостями є важливими процесами в рамках кібербезпеки організації, особливо в контексті забезпечення захисту від людино-орієнтованих кібератак. Ці процеси включають в себе кілька ключових етапів, кожен з яких спрямований на зниження ризику та підвищення загального рівня безпеки.

Першим кроком є ідентифікація потенційних ризиків та вразливостей. Це означає проведення всебічного аналізу існуючих систем, процесів та практик з метою виявлення слабких місць, які можуть бути використані для кібератак. В Україні, з огляду на зростаючі кіберзагрози, такий аналіз стає ще більш актуальним, особливо в секторах, що мають критичне значення для національної безпеки та економіки.

Другий етап полягає в оцінці ризиків, що включає визначення ймовірності виникнення кібератак та потенційного впливу, який вони можуть мати на організацію. Це допомагає встановити пріоритети у вжитті заходів безпеки, забезпечуючи, що ресурси сконцентровані на найбільш критичних аспектах.

Третім важливим аспектом є управління вразливостями. Після ідентифікації та оцінки ризиків, необхідно розробити та впровадити стратегії, які допоможуть зменшити або усунути виявлені вразливості. Це може включати технічні рішення, такі як оновлення систем та застосування патчів, а також організаційні заходи, такі як зміна процесів та поліпшення навчання персоналу.

Врешті-решт, процес оцінки ризиків та управління вразливостями має бути безперервним, оскільки кіберзагрози постійно еволюціонують. Регулярний перегляд та оновлення політик безпеки, процедур та технічних заходів є ключовими для забезпечення тривалого захисту від потенційних кібератак.

Залучення зовнішніх експертів та консультантів відіграє важливу роль у розробці та вдосконаленні стратегій кібербезпеки організацій. Це стає особливо актуальним у сучасному світі, де кіберзагрози постійно еволюціонують та стають більш складними.

Зовнішні експерти можуть надати цінні знання та досвід, які можуть бути важко доступні всередині організації. Вони можуть допомогти ідентифікувати слабкі місця в існуючих системах безпеки, запропонувати передові рішення та технології для їх зміцнення, а також допомогти в розробці більш ефективних стратегій протидії кібератакам.

Консультативні агентства та незалежні консультанти можуть також надати допомогу у розумінні нормативно-правового середовища, що є критично важливим для забезпечення відповідності діяльності організації законодавчим та регуляторним вимогам.

Включення зовнішніх фахівців у процес розробки стратегій кібербезпеки також дозволяє організаціям зберігати гнучкість та адаптивність, що є ключовими в умовах швидкозмінного кіберпростору. Вони можуть надати свіже бачення, допомогти виявити нові можливості та підходи, а також допомогти у впровадженні передових глобальних практик.

У цілому, організаційні та нормативно-правові аспекти захисту є критично важливими для забезпечення ефективної кібербезпеки. Розробка внутрішніх політик безпеки, дотримання законодавчих вимог, оцінка ризиків, навчання персоналу, а також залучення зовнішніх експертів допомагають створити комплексний та багаторівневий підхід до захисту від кіберзагроз. Важливо, що ці процеси повинні бути постійними та адаптованими до змін у технологіях, загрозах та законодавчому середовищі, особливо в контексті динамічного цифрового простору України. [12]

2.5. Психологічні аспекти протидії людино-орієнтованим атакам

У цьому розділі ми зосередимось на розумінні та протидії психологічним аспектам кібератак. Оскільки багато людино-орієнтованих кібератак базуються на маніпуляції та обмані, важливо розглянути, як можна застосувати психологічні знання для підвищення рівня кібербезпеки. Це включає аналіз того, як зловмисники використовують соціальні та психологічні впливи, а також розробку ефективних стратегій для підготовки та захисту співробітників від таких атак.

Розуміння психології соціальної інженерії є ключовим для протидії людино-орієнтованим кібератакам. Зловмисники часто використовують психологічні прийоми для маніпуляцій та обману, ефективно впливаючи на поведінку жертви для отримання доступу до конфіденційної інформації або систем. Основні з цих психологічних прийомів включають в себе використання довіри, авторитету та впливу.

1. Використання довіри: Одним з найпоширеніших прийомів соціальної інженерії є використання довіри. Зловмисники створюють образ надійності або знайомства, щоб знизити пильність жертви. Наприклад, вони можуть імітувати повідомлення від відомих компаній або колег, використовуючи знайомі логотипи та форматування.

2. Експлуатація авторитету: Часто зловмисники вдаються до використання авторитету, наприклад, прикидаючись керівниками або представниками влади. Це може спонукати жертву виконувати певні дії або надавати інформацію, якої в інших умовах вона б не розкрила.

3. Соціальний вплив та психологічний тиск: Зловмисники можуть також використовувати тактики соціального впливу, включаючи створення терміновості або використання страху. Наприклад, вони можуть стверджувати, що якщо жертва не виконає певні дії негайно, це матиме негативні наслідки.

Розуміння цих психологічних прийомів та механізмів соціальної інженерії є критично важливим для розробки ефективних стратегій протидії цим видам

атак. Це включає в себе не тільки технічні заходи безпеки, але й розробку відповідних програм навчання та підготовки для співробітників, аби вони могли відповідно реагувати на потенційні спроби маніпуляцій.

Розробка стратегій протидії психологічним маніпуляціям є ключовим елементом в боротьбі проти людино-орієнтованих кібератак. Оскільки зловмисники використовують психологічні прийоми для маніпулювання жертвами, важливо навчити співробітників розпізнавати та ефективно протистояти таким спробам. Ось декілька ключових методів та підходів, які можуть бути використані:

1. Підвищення обізнаності про тактики соціальної інженерії: Проведення тренінгів та семінарів, спрямованих на освіту співробітників про різноманітні методи соціальної інженерії, що використовують зловмисники. Це допомагає співробітникам краще розуміти ризики та бути підготовленими до виявлення підозрілої поведінки або запитів.

2. Розвиток критичного мислення: Навчання співробітників не приймати інформацію на віру, а використовувати критичне мислення для оцінки ситуації. Це означає перевірку джерел інформації, встановлення чи існують реальні підстави для запитів, та відмову від негайного реагування на термінові вимоги, які можуть бути маніпулятивними.

3. Створення чітких процедур реагування**: Розробка та впровадження чітких інструкцій для співробітників щодо дій у випадку підозрілих запитів або повідомлень. Це може включати кроки для перевірки та звітування таких інцидентів до відповідних відділів безпеки.

4. Використання симуляцій та тренінгів: Проведення практичних тренінгів та симуляцій, які імітують різні сценарії соціальної інженерії, допомагаючи співробітникам розвинути практичні навички ідентифікації та протидії таким атакам.

5. Створення культури безпеки: Підтримка культури безпеки у всій організації, де кожен співробітник відчуває відповідальність за захист

інформаційних активів. Це включає постійне нагадування про важливість безпеки та заохочення до відкритого спілкування про можливі загрози.

Реалізація цих стратегій сприяє створенню обізнаного та підготовленого колективу, який може ефективно протистояти психологічним маніпуляціям, що є невід'ємною частиною людино-орієнтованих кібератак. [15]

Розробка сценаріїв симуляції атак є важливим інструментом для практичного навчання співробітників, забезпечуючи їм можливість здобути реальний досвід у виявленні та реагуванні на психологічні маніпуляції, які часто використовуються у людино-орієнтованих кібератаках. Ці сценарії дозволяють співробітникам "прожити" різні типи атак у безпечному та контрольованому середовищі, що допомагає їм краще розуміти, як діяти в реальних ситуаціях.

Сценарії симуляцій можуть охоплювати різноманітні види атак, включаючи фішинг, використання шкідливого програмного забезпечення, атаки на основі соціальної інженерії та інші. Через реалістичне моделювання таких атак, співробітники навчаються виявляти підозрілі сигнали та реагувати на них адекватно, наприклад, не відкриваючи підозрілі вкладення або не вводячи конфіденційні дані на підозрілих веб-сайтах.

Одним із ключових аспектів розробки ефективних сценаріїв симуляції є їх адаптація до специфіки організації та актуальних загроз. Це означає, що сценарії повинні бути оновлені з урахуванням найновіших тенденцій у сфері кібербезпеки та включати ситуації, які могли б статися в реальному робочому середовищі співробітників.

Крім того, важливо забезпечити зворотний зв'язок після кожної симуляції, щоб співробітники могли зрозуміти, що було зроблено правильно, а що потребує покращення. Такий підхід сприяє не лише розвитку навичок, але й підвищує загальну обізнаність персоналу щодо потенційних кіберзагроз.

У підсумку, розробка та використання сценаріїв симуляції атак є ефективним способом підготовки співробітників до виявлення та протидії психологічним маніпуляціям, що є ключовим аспектом захисту від людино-орієнтованих кібератак.

Психологічна підтримка та консультування для співробітників, які можуть зіткнутися зі стресом або травмою в результаті кібератак, є важливою частиною комплексної стратегії кібербезпеки. Кібератаки можуть викликати значний психологічний тиск, особливо якщо вони ведуть до втрати конфіденційної інформації або порушення нормальної діяльності.

1. Значення психологічної підтримки**: У випадку успішної кібератаки співробітники можуть відчувати провину, стрес або навіть травму. Психологічна підтримка допомагає їм впоратися з цими емоціями та зменшує довгострокові негативні наслідки для їхнього психічного здоров'я.

2. Проведення консультувань та сесій зі стрес-менеджменту: Забезпечення доступу до професійних психологів або терапевтів, які можуть надати індивідуальні або групові консультації. Такі сесії допоможуть співробітникам розробити стратегії впорядкування стресу та подолання труднощів, пов'язаних з кібератаками.

3. Створення безпечного середовища для обговорення проблем: Важливо створити атмосферу відкритості, де співробітники можуть вільно висловлювати свої переживання та обговорювати вплив кібератак на їхнє професійне та особисте життя.

4. Розвиток програм допомоги персоналу (EAP): Реалізація програм допомоги персоналу, які включають психологічну підтримку, може бути важливим кроком у забезпеченні всебічної підтримки співробітників.

У цьому розділі ми розглянули різноманітні психологічні аспекти протидії людино-орієнтованим кібератакам. Від розуміння психології соціальної інженерії до розробки стратегій протидії психологічним маніпуляціям, важливість навчання та підвищення обізнаності співробітників, а також значення психологічної підтримки, ми підкреслили необхідність комплексного підходу. Це включає як технічні, так і психологічні аспекти, забезпечуючи, що організація може ефективно протистояти не тільки технологічним викликам кіберзагроз, але й психологічним аспектам, що супроводжують ці атаки. [17]

3. ТЕСТУВАННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНИХ МЕТОДІВ

3.1. Методологія тестування розроблених рішень

Тестування не лише забезпечує виявлення помилок та недоліків у розроблених методах, але й служить як ключовий інструмент для оцінки їх ефективності та практичності. В цьому контексті, важливо розуміти, що методологія тестування повинна бути гнучкою та адаптивною, щоб вона могла ефективно працювати з різними типами розроблених рішень.

Ми розглянемо ключові аспекти, які необхідно враховувати при виборі та реалізації методології тестування. Це включає в себе визначення цілей тестування, вибір відповідних тестових сценаріїв, а також встановлення критеріїв оцінки результатів тестування. Ефективна методологія повинна бути здатною адекватно оцінювати не тільки функціональність, але й ефективність розробленого рішення у різних умовах його застосування. [20]

Людино-орієнтовані атаки (social engineering attacks) це тип кібератак, які замість використання технічних недоліків системи, спираються на маніпуляцію людською психологією для отримання доступу до конфіденційної інформації або систем. Ось основні типи таких атак:

Кожен вид людино-орієнтованої атаки має свої унікальні цілі та способи реалізації. Ось цілі основних типів таких атак:

1. Фішинг (Phishing): Це вид шахрайства, при якому зловмисники намагаються обманом отримати конфіденційну інформацію, таку як логіни, паролі, номери кредитних карт, інформацію про банківські рахунки тощо. Це зазвичай робиться шляхом відправлення електронних листів, які виглядають так, ніби вони від законної організації (наприклад, банку), але насправді ведуть до фальшивих веб-сайтів.⁵ Цільовий фішинг (Spear Phishing): Варіант фішингу, який зосереджений на конкретних особах або організаціях. Зловмисники проводять підготовчу роботу, збираючи інформацію про своїх цілей, щоб створити дуже переконливі та персоналізовані повідомлення.

2. Вейлінг (Whaling): Це форма цільового фішингу, яка спрямована на "великих риб" – вищих керівників компаній або інших значущих осіб. Ці атаки часто мають за мету отримання конфіденційної інформації компанії або великих фінансових вигод.

3. Вішинг (Vishing): Це атаки, що виконуються через голосові засоби зв'язку, такі як телефонні дзвінки. Під час вішингової атаки, шахраї можуть використовувати переконливі сценарії, щоб змусити жертву надати особисту або фінансову інформацію.

4. Приманка (Baiting): Цей тип атаки використовує фізичні або цифрові "приманки", щоб залучити жертву. Наприклад, зловмисники можуть залишити заражені USB-накопичувачі в місцях, де їх можуть знайти потенційні жертви, сподіваючись, що ці жертви підключать їх до своїх комп'ютерів.

5. Квітінг (Quid Pro Quo): Це тип атаки, де шахраї обіцяють користувачам якусь вигоду в обмін на певну інформацію або доступ. Наприклад, шахрай може зателефонувати до кількох людей у великій компанії з "пропозицією допомоги" у вирішенні комп'ютерної проблеми. Як тільки хтось погоджується, шахрай просить надати логін і пароль для виправлення помилки, чим фактично отримує несанкціонований доступ.

6. Бейтінг (Baiting): Як уже було зазначено раніше, це метод, коли зловмисники використовують привабливі пропозиції для залучення жертви. Це можуть бути безкоштовні цифрові завантаження або фізичні об'єкти, такі як USB-накопичувачі, які містять шкідливе програмне забезпечення. Жертва, спокушена "приманкою", виконує дію, яка призводить до компрометації її безпеки.

7. Спірфінг (Spoofing): Це метод, при якому зловмисники прикидаються іншою особою, компанією або пристроєм, щоб обдурити жертву та отримати конфіденційну інформацію або спровокувати виконання певних дій. Спірфінг може включати електронну пошту (email spoofing), де зловмисник надсилає листи, які здаються від легітимної джерела, або IP-спірфінг, де атакуючий маскує свою IP-адресу під іншу.

Це найпоширеніші види лідиноорієнтовних кібератак. Будь яку з цих видів атак щоб успішно реалізувати потрібно правильно підготувати. Маючи загальну інформацію як реалізуються ці види атак, можна розбити реалізацію на 5 пунктів, так звану піраміду, в якій буде показано як проходить весь процес



Рисунок 3 – Піраміда процесу людино орієнтованої кібератаки

Збір даних з відкритих джерел — фундамент діяльності соціального інженера. На цей етап варто вкладати найбільше часу при плануванні атаки, тому він займає першу та найважливішу сходинку піраміди. Однак одній з важливих складових цього етапу рідко надається належна увага. Збір даних це по суті розвідка з відкритих джерел. Маючи вхідну інформацію про людину/організацію, починається збір інформації за допомогою машинного (додаткових програм, інформації в мережі інтернет, соціальні мережі ітд), та фізичного (огляд місцевості/людини/огранізації, ітд). Простими словами використовується OSINT отримання даних про ціль. [19]

Опираючись на дані, зібрані з відкритих джерел, логічно зробити наступний крок: почати розробку приводу для атаки. Ця частина роботи соціального інженера повинна базуватися на раніше зібраній інформації. На цьому етапі підготовки стає зрозуміло, які зміни та доповнення необхідно внести у вихідний план атаки, а також якими додатковими інструментами та реквізитом доведеться обзавестися.

Розробка легенди, звісно, не обмежується підготовкою. Наступний етап — планування за моделлю трьох «К»:

- Який ваш план? Яка ваша мета? Яка мета клієнта?

Визначившись з цілями, ви легко відповісте на наступні запитання;

- коли краще провести атаку;

- хто повинен бути поруч на випадок, якщо знадобиться допомога?

Проведення атаки

Ось де починається справжнє веселощі. Завершивши всі етапи підготовки, ви зможете ринутися у бій. Вам потрібно бути готовими до всього, але при цьому не варто обмежувати свої дії надто детальним сценарієм. Я завжди рекомендую складати план, тому що зазвичай це допомагає заощадити чимало часу та сил. Однак у плані не варто описувати кожен рух — це тільки заважатиме вам, якщо станеться якась несподіванка. Коли ваш мозок зрозуміє, що сценарій вам більше не помічник, ви почнете запинатися і нервувати. Ви покажете свій страх, а це може завадити вам досягти мети операції. Тому я пропоную писати не детальний сценарій дій, а скоріше план, якому можна буде слідувати, зберігаючи творчу свободу.

По суті, звіт це кульмінація, заради якої потрібні всі попередні етапи. Якщо послідовно виконати кожен з описаних кроків, вас чекає успіх не тільки як соціального інженера, але й як спеціаліста з систем безпеки, який взяв на себе зобов'язання перед клієнтом. Тому що зловмисники з усього світу, які займаються соціальною інженерією, готують атаки за цією самою схемою. Тільки ось звітів не складають, звичайно ж.

Враховуючи наведені вище етапи, можна зробити висновок, що ефективне проведення людино-орієнтованих кібератак вимагає не тільки глибокого розуміння психології та поведінки людини, але й вміння гнучко адаптувати план атаки залежно від розвитку ситуації. Складність та непередбачуваність людського фактору робить кожен напад унікальною, вимагаючи від соціального інженера не тільки технічних знань, але й креативності та психологічної гнучкості. Таким чином, успіх в області соціальної інженерії залежить не лише від ретельної підготовки та стратегічного планування, але й від здатності швидко адаптуватися до нових викликів та змінних обставин, що виникають під час проведення атаки.

3.2. Проведення пілотних тестів на модельних системах

У рамках нашої практичної частини, ми зосередимося на детальному розгляді та виконанні людино-орієнтованої кібератаки. Для прикладу тести будуть проходити в компанії “Horisons” яка знаходиться в Берліні. Ми будемо використовувати різні методи й атаки в залежності і цілі яка поставлена. Наприклад, ми розглянемо, як вішинг (атаки через голосовий зв'язок) та спуфінг (підробка ідентифікаційних даних) можуть бути ефективно інтегровані в цей сценарій.

В рамках цих сценаріїв ми також аналізуємо, як різні етапи людино-орієнтованої кібератаки взаємодіють між собою, формуючи більш складну та багатовимірну стратегію. На кожному етапі ми розглянемо потенційні ризики, можливості та методи, які зловмисник може застосувати для досягнення своєї цілі. Зокрема, ми зосередимо увагу на таких аспектах, як вибір цілі, розробка легенди, підготовка та виконання атаки, а також на можливих способах виявлення та запобігання таким атакам.

Цей підхід не лише дозволяє нам детально зрозуміти механізми та тактики, які використовуються в рамках кібератак, але й дає можливість глибше проаналізувати психологічні аспекти, які впливають на успіх атаки. Він також відкриває шлях до обговорення етичних та правових аспектів таких дій,

розкриваючи важливість розуміння соціальної інженерії не лише як засобу атаки, але й як важливого елементу в стратегіях кібербезпеки.

Тест №1 Отримати віддалений доступ до комп'ютера компанії.

Отримати віддалений доступ до комп'ютера компанії, це задача яка має багато варіантів вирішення завдання. Тут потрібно розуміти конкретику задачі, чи доступ до будь якого комп'ютера офісу чи саме до якого відділу.

Найпростіший варіант, це Приманка (Baiting). Головною задачею цього способу є підключення флеш до комп'ютера. Підготовка займає усього 2 етапи, а саме розвідка місцевості де потенційні робітники можуть взяти флеш, а другий це встановлення вірусного ПО, яке буде автоматично запускатись при підключенні флеш до комп'ютера.

Підготовка флеш до роботи складається також з двох частин , створення .exe файлу який буде слугувати бекдором до комп'ютера, та написання VBS скрипту який буде автоматично запускати .exe. Також Варто придумати наповнення флешки “живими” документами, фотографіями, ітд. Тобто підробити флеш під звичайну втрачені особисту річ.

Що до ознайомлення з місцем де буде “загублена” флешка, то він відбувається фізичним шляхом, тобто, вивчаючи місця де співробітники компанії можуть взяти флешку (місця для паління персоналу, стоянки, кафе/їдальня в офісі, тощо).

Реалізація цього способу досить проста, і не ефективна на 100%.

Інший варіант це дізнатись більше про компанію яка буде ціллю, наприклад у нас це компанія Horisons. Ми розіб'ємо цю задачу на під задачі, а саме почнемо пошук в Google, і далі по мірі отримання інформації будемо звертатись до різних інших інструментів, які допоможуть нам отримати більше інформації про компанію.

Почнемо з того що просто введемо назву компанії і її розташування. Маємо перші відомості про компанію

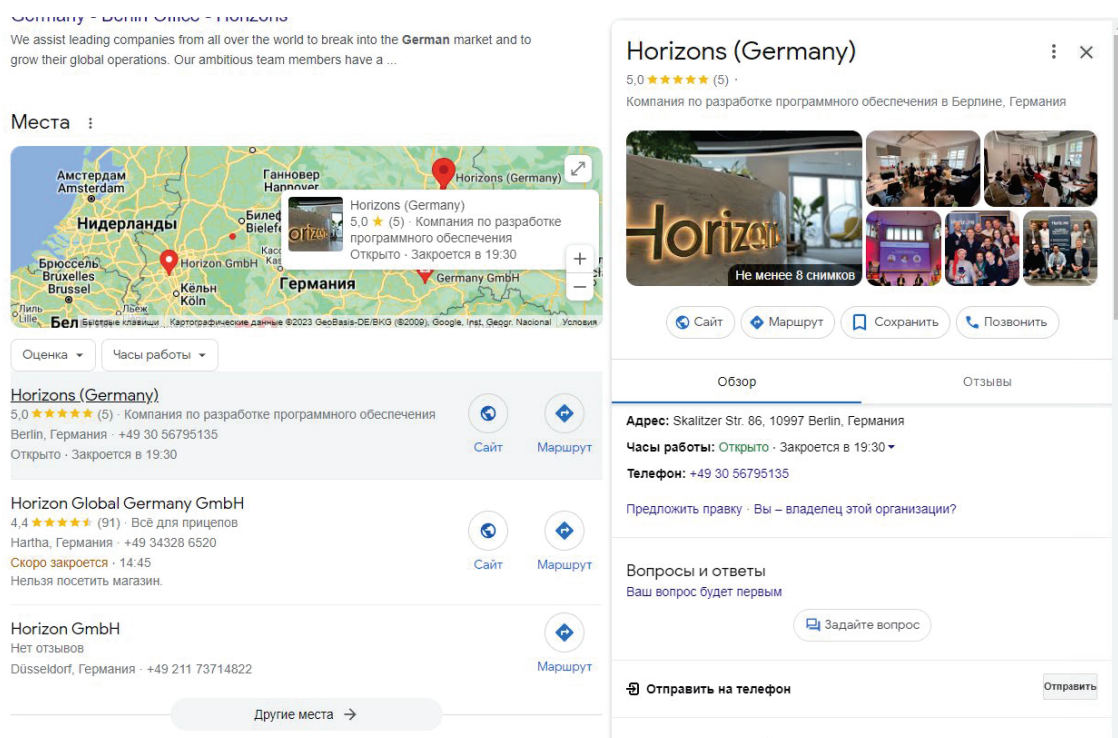


Рисунок 4 – Результати пошуку компанії в google

Маємо перші результати, а саме робочий номер телефону, сайт, адресу та графік роботи. Ця вхідна інформація надає більше місця для пошуку інформації. Далі пошуком на сайті компанії можемо знайти пошту компанії, телефон, соціальні мережі, блог компанії. Маючи доступ до соціальних мереж можемо побачити де, коли і як останні рази компанія проводила час, відпочивала, чи мала якісь заходи. В нашому випадку компанія орендувала зал для проведення корпоративу в честь дня народження компанії. Можемо використати цю інформацію для проведення атаки. А саме спочатку знайдемо пошту отелю таким же методом як ми знайшли пошту компанії, о спробуємо написати з історією замовлення залу також, це потрібно щоб зрозуміти чи є в готеля фірмовий стиль листів які вони відкривають. В нашому випадку він є, тому ми копіюємо його, і вставляємо свій завчасно придуманий текст, який буде містити текст про додаткову оплату святкування та пдф файл під назвою (Invoice). Сам же пдф файл ми зробимо як Invoice, + паралельно вшиємо бекдодр за допомогою утиліти Metasploit. Вшивання шкідливого ПО в пдф файл має багато різних варіантів, від готових рішень до самостійного змінювання файлу, та використання

вразливостей програм які відкривають ПДФ файли. Цього буде більш ніж достатньо щоб зацікавити людину відкрити заражений пдф файл, який буде надавати віддалений доступ до комп'ютера жертви.

Тест №2 Отримати логін і пароль до сайту компанії

Отримавши інформацію з минулого тесту, ми маємо сайт компанії. І тепер ціль це провести сканування сайту щоб знати всі вразливості і місця для потінційного входу до сайту, також хто адмініструє сайт, чи є на ньому зареєстрований.

Для цього можемо почати з сканування доменного імені сайту через такі інструменти як Shimon, Whois, Ctnsys, Hunted Search та іншими популярними сканерами, можемо дізнатись базову інформацію про сайт а саме його ip, cms, провайдера, і так далі.

В нашому випадку сайт на популярній cms Вордпрес. Тому можемо пропустити сайт через утиліту WPScan, щоб дізнатись більше саме про cms, її плагіни та оновлення, а також вразливості які є на цьому сайті. WPScan вказав на те що сайт тривалий час не оновляв версію Вордпрес .а також плагіни до нього, і вказав на те що сайт не приховує файли і каталоги сайту. Ввівши Також хорошою практикою є використання утиліти OWASP ZAP, яка також покаже нам вразливості сайту.

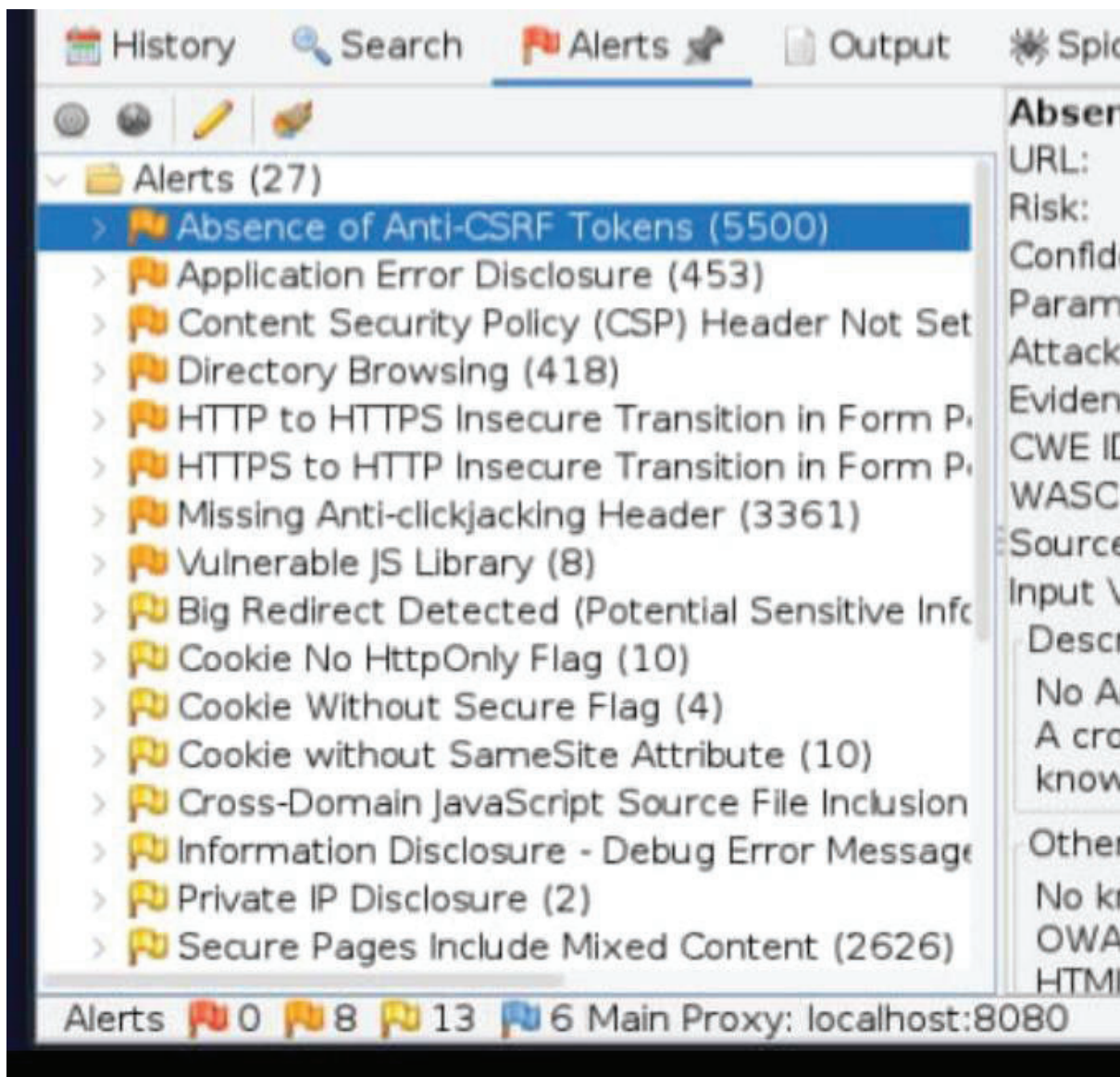


Рисунок 5 – результати тестування інструментом OWASP ZAP

Однією з головних вразливостей є те що немає токєну проти CSRF атак, це можна використати для отримання доступу до сайту.

Наступним кроком буде отримати логіни юзерія і зареєстровані на сайті. першим і головним це буде admin, nfrj; можуть бути і інші юзери, тому потрібно до адреси сайту вставити /wp-json/wp/v2/users , це виведе нам json файл з усіма юзерами, де ми можемо вибрати нашу ціль (зазвичай до юзерів пишуть опис що є цим юзером (редактор контенту Катерина Лозова)). Маючи вразливість на сайті, і знаючи людину яка веде контент на сайті, можемо знайти дані про цю людину на самому сайті в розділі про нас /команда, і дізнатись пошту цілі. Далі залишається вигадкування легенди і створення фішингового листа з лінком на

який перейде жертва. Для цього вивчаємо усі обов'язки цілі в компанії, і створюємо історію в якій ми цікавимось діяльністю людини, наприклад хочемо запропонувати роботу в іншій компанії або додатковий дохід, паралельно в текст вставляючи лінк який маємо маскою на “надійний” сайт чи джерело, щоб людина не мала сумніву при переході. Іншим етапом буде створення Сторінки з шкідливим кодом та фейковою формою, яка саме і буде При відвідуванні шкідливого сайту, автоматично генерувати запит на сайт WordPress, намагаючись або увійти в систему під раніше відомими обліковими даними, або створити новий обліковий запис.

В реалізації цієї атаки ми отримали доступ до адмін панелі Вордпрес з правами редактора контенту, при цьому жертва навіть не зрозуміла як це відбулось.

Тест №3 Масове зараження компанії фішинговим листом

Проста в реалізації і досить небезпечна тактика масової розсилки листів всім співробітникам компанії може понести за собою погані наслідки для компанії як в фінансовому так і в репутаційному характері.

Підготовка до такої кампанії складається з 3 частин: 1) отримання емейлів співробітників 2) створення вразливої програми, яка після встановлення на комп'ютер жертви блокує його дані і вимагає за це фінансову нагороду 3) створення листа з вразливими посиланнями на програму вимагача.

Перша частина. Отримання пошт користувачів має багато варіантів вирішення питання, починаючи від пошуку злитих даних про компанію і її працівників, закінчуючи перебором логіну пошти. В нашому випадку ми знайшли базу мейлів компанії, яка нас цікавить (вони закінчуються на @horisons.in.com).

Другою частиною буде створення сховища з .exe файлом для того щоб людина могла перейти і скачати його собі на комп'ютер. для цього можемо використовувати готові сервіси типу Drive, Mega (залежить від місця розташування компанії) і так далі. Та сам софт який і буде програмою вимагачем.

Остання частина це ознайомлення з діяльністю компанії, її останніми заходами та корпоративною культурою. В нашому випадку компанія мала вебінар з програмою редагування та доповнення тексту за допомогою ШІ, це можемо використати як основу нашого листа і нашої легенди.

Далі створюємо від імені компанії яка проводила вебінар лист з текстом про захід який був і наданням на 7 днів безкоштовної пробної версії програми, з посиланням на сховище з шкідливим файлом і розсилаємо його усім співробітникам компанії. Хорошим результатом було б встановлення “Пікселю” в лист для відслідковування взаємодії листа, посилання та співробітників компанії, тобто скільки людей відкрили лист, скільки людей перейшли по посиланню ітд.

3.3. Аналіз результатів тестування

Вступ до аналізу результатів тестування пілотних випробувань людино-орієнтованих кібератак у компанії "Horisons" розкриває ключові аспекти застосування різних стратегій та методик в сфері соціальної інженерії. Зосередженість на детальному вивченні вразливостей цільової компанії, використання методів, таких як вішинг, спуфінг та інших способів маніпуляції, дозволила нам зробити висновки щодо ефективності та потенційних ризиків кожного застосованого підходу.

Проведені тести включали отримання віддаленого доступу до комп'ютерів компанії, виявлення логіну та пароля до сайту "Horisons", а також масове зараження компанії через фішингові листи. Кожен з цих тестів демонструє важливість знання й розуміння цільової системи, вміння аналізувати потенційні слабкості та вибирати оптимальні тактики для досягнення поставлених цілей. Аналіз результатів дає змогу не лише оцінити рівень вразливості системи, але й надає інсайти для розробки ефективних стратегій кібербезпеки.

У першому тесті з метою отримання віддаленого доступу до комп'ютера компанії "Horisons" було використано метод "Приманка (Baiting)". Суть методу полягала у використанні фізичної "приманки" — флеш-накопичувача,

обладнаного шкідливим програмним забезпеченням. Підготовка включала два ключові етапи: по-перше, розвідку місцевості, де потенційно могли перебувати співробітники компанії і могли б взяти флешку, і по-друге, підготовку самої флешки, що включала встановлення .exe файлу, який служив бекдором, і VBS скрипту для автоматичного запуску цього файлу. Для збільшення вірогідності використання флешки співробітниками, на неї також були завантажені звичайні документи та фотографії, щоб вона виглядала як персональний носій даних.⁷

Результати: Використання методу "Приманка" дозволило отримати віддалений доступ до одного з комп'ютерів компанії. Однак, успіх цієї атаки суттєво залежав від людського фактору — чи знайде хтось і використає флеш-накопичувач.

Роль Людського Фактору: Людино-орієнтований аспект цього тесту полягає у сподіванні на цікавість або недбалість співробітників. Весь успіх атаки базувався на тому, що співробітник знайде флешку та вирішить підключити її до свого робочого комп'ютера, що демонструє важливість людської складової в рамках соціальної інженерії.

Висновок: Цей тест підкреслює, як важливим елементом у людино-орієнтованих атаках є людська поведінка та реакції. Основна вразливість у цьому випадку — це не технічні недоліки системи, а людська схильність до помилок або цікавості. Такий підхід демонструє, що розуміння психології та поведінки людей є ключовим у плануванні та виконанні ефективних атак соціальної інженерії.

Розбір Другого Тесту: Отримання Логіну та Пароля до Сайту Компанії

1. Вивчення та Аналіз Сайту: У цьому тесті основна увага була сконцентрована на аналізі веб-сайту компанії "Horisons". Використовуючи інструменти такі як Shodan, Whois, Censys, Hunter Search, а також WPScan для виявлення вразливостей специфічних для WordPress, команда здійснила ретельне сканування сайту. Це дозволило виявити ключові інформаційні відомості про сайт, включаючи його IP-адресу, версію CMS, провайдера хостингу та потенційні вразливості.

2. Використання Вразливостей: Знайдені вразливості, зокрема, відсутність захисту від CSRF атак, були використані для планування подальшого втручання. Виявлено, що сайт мав застарілі версії WordPress і плагінів, що створювало додаткові ризики.

3. Отримання Інформації про Користувачів: За допомогою спеціального запиту (`/wp-json/wp/v2/users`) команда змогла отримати інформацію про користувачів сайту, включаючи імена, ролі та інші дані, що могли бути використані для подальших атак.

4. Планування Фішингової Атаки: На основі зібраної інформації була спланована фішингова атака. Це включало створення переконливого фішингового листа, який мімікрував під офіційне повідомлення від компанії, та вміщує посилання, яке переправовувало до фейкової сторінки з шкідливим кодом.

Результати та Людино-орієнтований Аспект: Успішно проведена фішингова атака призвела до отримання доступу до адміністративної панелі WordPress з правами редактора контенту. Цей успіх вказує на важливість людського фактору у безпеці інформаційних систем. Незважаючи на технічні вразливості, ключовим елементом успіху стала здатність атакувати через соціальну інженерію, використовуючи вразливості у поведінці та звичках користувачів.

Висновок: Другий тест підкреслює, що крім технічних аспектів кібербезпеки, велике значення мають людські фактори, такі як освіта, обізнаність та критичне мислення користувачів. Навіть найбільш захищені системи можуть бути вразливими, якщо люди, які ними користуються, не знають про ризики або не дотримуються правил безпеки.

Розбір Третього Тесту: Масове Зараження Компанії Фішинговим Листом

Підготовка до Розсилки: Основна мета полягала у масовій розсилці фішингових листів співробітникам компанії "Horisons". Спершу було здійснено збір електронних адрес співробітників. Для цього використовувалися різні

методи, включаючи пошук витоків даних про компанію та використання спеціалізованих інструментів для визначення електронних адрес.

Розробка Шкідливого Програмного Забезпечення: Другим кроком було створення шкідливого програмного забезпечення (зазвичай використовуються програми-вимагачі), яке містилося на зовнішніх ресурсах і до якого вели посилання у фішингових листах.

Створення Фішингових Листів: Листи були розроблені таким чином, щоб виглядати переконливо та офіційно, імітуючи реальні корпоративні повідомлення. У листах містилося посилання, яке вело до шкідливого програмного забезпечення, а також використовувалися інструменти для відслідковування взаємодії з листом (наприклад, пікселі для відстеження відкриття листа).

Результати та Людино-орієнтований Аспект: Цей тест продемонстрував високу ефективність фішингових атак при масовому розповсюдженні. Навіть при наявності технічних захистів, людський фактор залишається ключовою ланкою у ланцюжку кібербезпеки. Реакція співробітників на переконливі фішингові листи, ігнорування базових правил кібербезпеки (не відкривати підозрілі листи та не переходити за невідомими посиланнями) дозволила зловмисникам досягти своїх цілей.

Висновок: Третій тест відзначається своєю ефективністю у демонстрації значення освіти та обізнаності в області кібербезпеки серед співробітників. Він наголошує на тому, що технічні засоби захисту, хоч і є важливими, не можуть повністю запобігти кібератакам, якщо не поєднуються з правильною поведінкою та обізнаністю користувачів. Таким чином, підвищення рівня обізнаності співробітників про ризики та методи кібератак є критично важливим для забезпечення всебічного захисту компанії від кіберзагроз.

Проаналізувавши результати трьох тестів, які були проведені в компанії "Horisons", можна зробити декілька ключових висновків. По-перше, ефективність людино-орієнтованих кібератак значною мірою залежить від психологічних та поведінкових факторів цільових користувачів. Людська

цікавість, недбалість, або недостатня обізнаність у сфері кібербезпеки часто стають ключовими чинниками, які зловмисники використовують для успішної реалізації своїх замірів.

По-друге, хоча технічні засоби захисту є важливими, вони не можуть повністю запобігти кібератакам без належної поведінки та обізнаності користувачів. Це демонструє важливість включення елементів психологічної підготовки та навчання з кібербезпеки у загальну стратегію захисту компанії.

Інші Методи Людино-орієнтованих Атак та Роль Людського Фактору

Окрім описаних вище методів, існують інші стратегії соціальної інженерії, які включають, але не обмежуються:

Квітінг (Quid Pro Quo): Обіцянка винагороди в обмін на певну інформацію або доступ.

Спірфінг (Spoofing): Підробка електронної пошти або інших комунікаційних каналів для введення в оману.

Соціальні мережі: Використання інформації з соціальних мереж для розробки цільових атак.

Людина часто є головною вразливістю в системах безпеки будь-якої компанії. Відсутність обізнаності, помилкові дії або недостатньо суворе дотримання протоколів безпеки можуть стати причиною серйозних проблем. Тому навчання персоналу основам кібербезпеки та регулярне оновлення знань у цій галузі є необхідністю для забезпечення комплексного захисту від кіберзагроз.

3.4 Розробка комплексних рекомендацій з кібербезпеки: стратегії попередження та забезпечення ефективного захисту від людино-орієнтованих кіберзагроз

Цей розділ має на меті розробити всеосяжні рекомендації та стратегії для захисту від людино-орієнтованих кіберзагроз, засновані на аналізі результатів тестів, проведених в компанії "Horizons". Ці тести демонстрували, як через вразливості, пов'язані з людським фактором, можуть бути реалізовані різні форми кібератак. Розробка ефективних стратегій захисту вимагає глибокого

розуміння як технічних аспектів, так і психологічних механізмів, що використовуються в соціальній інженерії.

Аналіз Тестів та Результатів

Тест "Приманка" та Важливість Обізнаності: Тест з використанням методу "Приманка" показав, що навіть прості фізичні пристрої можуть стати інструментами для віддаленого доступу до корпоративних систем. Це підкреслює необхідність проведення регулярного навчання співробітників з питань кібербезпеки, зокрема щодо ризиків використання невідомих пристроїв.

Фішингова Атака та Захист Ідентифікаційних Даних: Успішна фішингова атака на логіни та паролі до сайту компанії демонструє, як можна маніпулювати співробітниками для отримання конфіденційної інформації. Рекомендується впровадити двофакторну аутентифікацію та постійно оновлювати співробітників щодо методів фішингу та способів їх виявлення.

Масова Фішингова Розсилка та Значення Комплексного Підходу: Масова фішингова розсилка, яка призвела до зараження систем компанії, вказує на необхідність комплексного підходу до кібербезпеки. Крім технічних рішень, важливим є розвиток культури кібербезпеки в компанії, що включає регулярне навчання співробітників, розробку чітких процедур і політик безпеки.

Розгорнуті Рекомендації та Стратегії для Забезпечення Ефективного Захисту від Людино-орієнтованих Кіберзагроз

Розвиток Культури Кібербезпеки в Компанії

Регулярні Тренінги та Освітні Програми: Важливо систематично проводити навчальні заходи для співробітників, які охоплюють основні принципи кібербезпеки, розпізнавання фішингових атак, безпечне використання електронної пошти та інтернету. Такі тренінги повинні включати практичні вправи та симуляції атак, щоб співробітники могли краще зрозуміти ризики та навчитися ефективно реагувати на потенційні загрози.

Внутрішня Комунікація та Підвищення Обізнаності: Регулярне інформування персоналу про актуальні кіберзагрози, нові методи шахраїв та

зміни в політиці безпеки компанії. Можуть використовуватися електронні бюлетені, вебінари, інформаційні зустрічі.

Впровадження Технічних Заходів Безпеки

Двофакторна Аутентифікація (2FA): Увімкнення 2FA для всіх корпоративних систем і сервісів, щоб додатково захистити облікові записи від несанкціонованого доступу.

Регулярне Оновлення ПЗ та Застосування Патчів Безпеки: Необхідно вчасно оновлювати всі програми і операційні системи до останніх версій, щоб усунути відомі вразливості.

Застосування Програмного Забезпечення для Захисту від Фішингу та Малвару: Встановлення та налагодження надійного антивірусного та антиспамного програмного забезпечення на всіх пристроях.

Розробка і Впровадження Комплексної Політики Безпеки

Чіткі Процедури та Політики Безпеки: Розробка детальних інструкцій та правил для співробітників щодо використання корпоративних ресурсів, обігу інформації та реагування на інциденти безпеки.

Політика Мінімальних Привілеїв: Обмеження доступу до систем та даних відповідно до ролі та обов'язків співробітника, щоб звести до мінімуму можливість зловмисного або помилкового використання інформації.

Регулярний Аудит та Тестування Системи Безпеки

Проведення Регулярних Пентестів: Залучення зовнішніх фахівців для тестування системи на вразливості та розробка планів щодо усунення виявлених проблем.

Симуляція Кібератак: Регулярне проведення тренувальних кібератак для перевірки реакції персоналу та ефективності технічних засобів захисту.

Розробка Плану Реагування на Інциденти

Чіткий План Реагування на Інциденти Безпеки: Розробка детального плану дій на випадок різних кіберінцидентів, включаючи фішинг, витоки даних, вірусні атаки. План повинен включати кроки щодо ізоляції інциденту, мінімізації шкоди та відновлення роботи.

Загалом, ефективність захисту від людино-орієнтованих кіберзагроз лежить у комплексному підході, що об'єднує освіту та обізнаність співробітників, регулярне оновлення та підтримання технічних засобів безпеки, та розробку чітких процедур і політик. Тільки такий всеосяжний підхід може гарантувати реальний захист від широкого спектру кіберзагроз.

ВИСНОВКИ

У цій випускній кваліфікаційній роботі було проведено глибоке дослідження людино-орієнтованих кібератак, що виявилось актуальним та важливим у контексті зростаючої залежності від цифрових технологій. Поняття та характеристики людино-орієнтованих кібератак були ретельно проаналізовані, підкреслюючи їхню специфіку та відмінності від інших видів кіберзагроз. В роботі було визначено, що головною характеристикою таких атак є використання соціальної інженерії та психологічних маніпуляцій для обману жертв та отримання несанкціонованого доступу до систем або інформації.

Дослідження охоплює широкий спектр методів та стратегій, які використовують кіберзлочинці, включаючи фішинг, вішинг, спуфінг, бейтінг та інші тактики. Аналіз показав, що ці методи неперервно еволюціонують, стаючи все більш витонченими та складними, що вимагає постійної уваги та адаптації з боку інформаційних систем.

У роботі було здійснено детальний аналіз вразливостей інформаційних систем, виявляючи ключові технічні та організаційні проблеми, які можуть сприяти успіху кібератак. Розглянуто було важливість регулярних оновлень програмного забезпечення, правильного налаштування систем та розвитку комплексної стратегії кібербезпеки, заснованої на ретельному аудиті та моніторингу.

Особливу увагу в роботі приділено аналізу впливу людино-орієнтованих кібератак на різні сфери: корпоративний сектор, державні установи, індивідуальних користувачів та на глобальний рівень. Виявлено, що наслідки таких атак можуть бути різноманітними та мають значний вплив на фінансову стабільність, довіру клієнтів, національну безпеку та міжнародні відносини.

Теоретична частина роботи ґрунтується на глибокому вивченні літератури та аналізі існуючих досліджень у галузі кібербезпеки. Це дозволило зрозуміти фундаментальні аспекти людино-орієнтованих кібератак та розробити теоретичну базу для практичної частини дослідження.

Практична частина диплому включала аналіз реальних випадків кібератак, а також розробку рекомендацій та стратегій для покращення кібербезпеки на корпоративному та національному рівнях. Використання практичних прикладів допомогло ілюструвати реальні ризики та важливість ефективних заходів безпеки.

Робота також звертає увагу на важливість освіти та обізнаності в сфері кібербезпеки, підкреслюючи, що навчання та розвиток культури безпеки серед співробітників є ключовими для попередження успішних кібератак.

У заключній частині роботи робляться висновки про необхідність комплексного підходу до кібербезпеки, який включає як технічні, так і організаційні аспекти, а також необхідність адаптації до постійно змінюваного цифрового ландшафту.

У підсумку, ця дипломна робота є важливим внеском у розуміння загроз, пов'язаних з людино-орієнтованими кібератаками, та розробку ефективних стратегій захисту від них. Робота підкреслює важливість інтегрованого підходу до кібербезпеки, що включає обізнаність, освіту та технічні рішення, щоб захистити суспільство від цих складних та постійно еволюціонуючих загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Johnson, Thomas A. "Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare" – CRC Press, 2020.
2. "Cybersecurity: The Insights You Need from Harvard Business Review" – Harvard Business Review Press, 2020.
3. Erickson, Jon. "Hacking: The Art of Exploitation, 2nd Edition" – No Starch Press, 2020.
4. Hadnagy, Christopher. "Social Engineering: The Science of Human Hacking, 2nd Edition" – Wiley, 2019.
5. Carey, Marcus J.; Jin, Jennifer. "Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World" – Wiley, 2019.
6. Weidman, Georgia. "Penetration Testing: A Hands-On Introduction to Hacking" – No Starch Press, 2nd Edition, 2018.
7. Yaworski, Peter. "Real-World Bug Hunting: A Field Guide to Web Hacking" – No Starch Press, 2019.
8. McDonald, Malcolm. "Web Security for Developers: Real Threats, Practical Defense" – No Starch Press, 2020.
9. Diogenes, Yuri; Ozkaya, Erdal. "Cybersecurity – Attack and Defense Strategies" – Packt Publishing, 2018.
10. Prasad, Prakhar. "Mastering Modern Web Penetration Testing" – Packt Publishing, 2016.
11. Gilbert, Karl; Caudill, Benjamin. "Hands-On AWS Penetration Testing with Kali Linux" – Packt Publishing, 2019.
12. McNab, Chris. "Network Security Assessment: Know Your Network" – O'Reilly Media, 3rd Edition, 2017.
13. Kim, Peter. "The Hacker Playbook 3: Practical Guide To Penetration Testing" – Secure Planet, 2018.
14. McClure, Stuart; Scambray, Joel; Kurtz, George. "Hacking Exposed 7: Network Security Secrets and Solutions" – McGraw-Hill Education, 2019.

15. Bazzell, Michael. "Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information" – CreateSpace Independent Publishing Platform, 2018.
16. Hassan, Nihad A.; Hijazi, Rami. "Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence" – Apress, 2018.
17. Summers, Grady. "Cyber Kill Chain: Understanding Advanced Persistent Threats" – Wiley, 2019.
18. Holland, Rick. "The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence" – O'Reilly Media, 2019.
19. Hadnagy, Christopher. "The Art of Deception. Social Engineering in Fraudulent Schemes" – Wiley, 2020.
20. Grey, Joe. "Practical Social Engineering: A Primer for the Ethical Hacker" – 2022.
21. Hadnagy, Christopher; Fincher, Michele. "Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails" – John Wiley & Sons, Inc., 2015.