ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ФІШИНГОВІ АТАКИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Виконав студент 5 курсу, групи БСЗ-51
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Манилюк М. О.
(прізвище та ініціали)
Керівник Чумак Н.С.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“24” березня 2023 року

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

Манилюку Миколаю Олександровичу
(прізвище, ім’я, по батькові)

1. Тема бакалаврської роботи:
«Дослідження шляхів та розробка рекомендацій щодо виявлення та реагування на фішингові атаки в корпоративній інформаційній системі».
керівник бакалаврської роботи Чумак Н.С.
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «24 » 02. 2023 року № 26 .

2. Строк подання студентом бакалаврської роботи 29.05.2023 р.

3. Вихідні дані до бакалаврської роботи
Інформаційна система організації;
Фішінгові атаки;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз проблеми виявлення фішингових атак в корпоративній інформаційній системі
Методи та засоби протидії фішинговим атакам в корпоративній інформаційній системі.

Розробка рекомендацій щодо виявленнтая а реагування на фішингові атаки в корпоративній інформаційній системі.

5. Перелік графічного матеріалу

Тема бакалаврської роботи.

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

Аналіз впливу фішингових атак на корпоративну інформаційну систему

Підходи проведення фішингових атак

Багаторівневий підхід до захисту від фішингу

Рішення Cyren Inbox Security

Рекомендації щодо виявлення та реагування на фішингові атаки в корпоративній інформаційній системі.

Висновки.

6. Дата видачі завдання 24.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Аналіз наукової та технічної літератури з питань теми бакалаврської роботи.	23.02.2023 р.	
2.	Аналіз проблеми виявлення фішингових атак в корпоративній інформаційній системі	06.03.2023 р.	
3.	Методи та засоби протидії фішинговим атакам в корпоративній інформаційній системі.	20.04.2023 р.	
4.	Розробка рекомендацій щодо протидії та реагуванню на фішингові атаки в корпоративній інформаційній системі.	30.04.2023 р.	
5.	Висновки.	02.05.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	07.05.2023 р.	
7.	Підготовка доповіді до захисту.	15.05.2023 р.	

Студент Манилюк М. О.

(підпис) прізвище та ніціали

Керівник бакалаврської роботи Чумак Н.С.

(підпис) прізвище та ніціали

ВІДГУК РЕЦЕНЗЕНТА
на бакалаврську роботу

студенту Манилюку Миколаю Олександровичу

на тему: «Дослідження шляхів та розробка рекомендацій щодо виявлення та реагування на фішингові атаки в корпоративній інформаційній системі».

Актуальність: Фішингові атаки дуже актуальні та залишаються серйозною проблемою в сучасну цифрову епоху. Ці атаки зазвичай здійснюються через електронну пошту, соціальні мережі або платформи обміну миттєвими повідомленнями. Організації вживають заходів для боротьби з фішинговими атаками, наприклад, запроваджують протоколи безпеки, проводять регулярні тренінги для співробітників і проводять інформаційні кампанії, а також використовують передові рішення безпеки, такі як фільтри електронної пошти, багатофакторна автентифікація та технології шифрування. Тому тема бакалаврської роботи є актуальною і своєчасною.

Позитивні сторони:

1. Зміст роботи відповідає завданню. Студент показав високий рівень знань і ступінь підготовленості її до майбутньої роботи за фахом.
2. Обґрунтовано необхідність захисту корпоративної інформаційної системи від фішингових атак. Достатньо успішно викладено матеріали застосування рішення щодо протидії фішинговим атакам.
3. Текст викладено грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою бакалаврської роботи.

Недоліки:

1. В роботі доцільно було б провести порівняльний аналіз рішень протидії фішинговим атакам.

Вищезгадані зауваження не впливають на загальну позитивну оцінку бакалаврської роботи.

Висновок: робота заслуговує оцінку "добре", а студент – Манилюк Миколай Олександрович гідний присвоєння кваліфікації: бакалавр за спеціальністю кібербезпека спеціалізації Інформаційна та кібернетична безпека.

Якість бакалаврської роботи	
Виконано на замовлення підприємст	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	*
Має практичну цінність	*
Проект-частина комплексної теми	

Підпис рецензента

_____ _____
(П.І.Б.)

_____
(посада, науковий ступінь, вчене звання)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студентка Манилюк М. О. до захисту бакалаврської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розробка рекомендацій щодо виявлення та реагування на фішингові атаки в корпоративній інформаційній системі».
Бакалаврська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Манилюк М. О. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2018 року по 2023 рік повністю виконала навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Берестяна Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студент ***Манилюк М. О.*** обрав тему роботи, метою якої було розробити рекомендації щодо щодо протидії та реагуванню на фішингові атаки в корпоративній інформаційній системі.. Перелік використаних джерел свідчить про вміння розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Манилюк М. О. показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити бакалаврську роботу студента Манилюк М. О. на оцінку **«добре»** та присвоїти йому кваліфікацію бакалавр за спеціальністю кібербезпека спеціалізації Інформаційна та кібернетична безпека.

Керівник бакалаврської роботи _____ Чумак Н.С.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студент Скрицький М. Є.
(прізвище та ініціали)
допускається до захисту даної бакалаврської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

“____” _____ 2023 року

РЕФЕРАТ

Текстова частина бакалаврської роботи: 53 сторінки, 14 рисунків, 1 таблиця, 9 джерел.

Об'єкт дослідження – процес виявлення фішингових атак в корпоративній інформаційній системі.

Предмет дослідження – методи та засоби протидії фішинговим атакам в корпоративній інформаційній системі.

Мета роботи – розробити рекомендації щодо виявлення та протидії фішингових атака в корпоративній інформаційній системі.

Методи дослідження – опрацювання літератури за даною темою, теоретичне дослідження, порівняльний аналіз.

В роботі проведено аналіз впливу фішингових атак на корпоративну інформаційну систему організацій. Розглянуто багаторівневий підхід до захисту від фішингу. В роботі досліджено архітектуру та функції рішення Cyren Inbox Security та розроблено рекомендації користувачам та фахівцям з кібербезпеки щодо виявлення та протидії фішинговим атакам.

Галузь використання – матеріали роботи можуть бути використані фахівцями з кібербезпеки для виявлення та протидії фішинговим атакам.

КІБЕРБЕЗПЕКА, ФІШИНГ, ІНФОРМАЦІЙНА СИСТЕМА, , ІНФОРМАЦІЯ, КОРИСТУВАЧІ, ОРГАНІЗАЦІЯ, ТЕХНОЛОГІЇ, АТАКА, ПРОТИДІЯ, ВИЯВЛЕННЯ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КІС – Корпоративна Інформаційна Система

ПЗ – Програмне Забезпечення

API – Application Programming Interface

ATP – Advanced Threat Protection

BEC – Business Email Compromised

CIRS – Cyren Incident Response Service

GUI – Graphical User Interface

HTML – HyperText Markup Language

IP – Internet Protocol

IM – Instant Messaging

PDF – Portable Document Format

PHP – Hypertext Preprocessor

URL – Uniform Resource Locator

VoIP – Voice over IP

ВСТУП

Актуальність роботи.

Проблема виявлення фішингових атак в інформаційній системі організації сьогодні є дуже актуальною, оскільки фішингові атаки стають все більш витонченими та поширеними.

Фішингові атаки можуть мати серйозні наслідки для організацій, зокрема фінансові втрати, репутаційну шкоду та юридичну відповідальність. Крім того, фішингові атаки також можуть поставити під загрозу конфіденційність, цілісність і доступність конфіденційної інформації та систем, піддаючи ризику операції та активи організації.

Тому виявлення фішингових атак в інформаційній системі організації має вирішальне значення для запобігання або пом'якшення збитків, завданих такими атаками. Цього можна досягти шляхом впровадження заходів безпеки, таких як фільтри спаму, автентифікація електронної пошти, навчання та підвищення обізнаності користувачів, а також плани реагування на інциденти. Крім того, організації можуть використовувати такі передові технології, як штучний інтелект і машинне навчання, щоб виявляти фішингові атаки та реагувати на них у реальному часі.

Тому тема бакалаврської роботи, щодо управління мобільними пристроями в організації є актуальною.

Об'єкт дослідження – процес виявлення фішингових атак в корпоративній інформаційній системі.

Об'єкт дослідження – методи та засоби протидії фішинговим атакам в корпоративній інформаційній системі.

Предмет дослідження – методи та засоби протидії фішинговим атакам в корпоративній інформаційній системі.

Мета роботи – розробити рекомендації щодо виявлення та протидії фішингових атака в корпоративній інформаційній системі.

Наукові завдання:

дослідити вплив фішингових атак на корпоративну інформаційну систему організацій;

- провести аналіз підходів до проведення фішингових атак;

- дослідити підходи виявлення та реагування на фішингові атаки;

- розробити рекомендації користувачам та фахівцям з кібербезпеки щодо виявлення та реагування на фішингові атаки.

Методи дослідження - опрацювання літератури за даною темою, теоретичне дослідження, порівняльний аналіз.

Практичне значення одержаних результатів полягає у розробці рекомендацій щодо виявлення та реагування фішинговим атакам.

1 АНАЛІЗ НЕОБХІДНОСТІ ВПРОВАДЖЕННЯ РІШЕНЬ ПРОТИДІЇ ФІШИНГОВИМ АТАКАМ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

1.1. Аналіз впливу фішингових атак на корпоративну інформаційну систему

Фішинг — це тип кібератаки, коли зловмисник видає себе за надійну організацію чи особу, щоб обманом змусити жертву розкрити конфіденційну інформацію, таку як облікові дані для входу, дані кредитної картки або особисті дані. Ці атаки можуть здійснюватися через різні канали, такі як електронна пошта, миттєві повідомлення, соціальні мережі або навіть телефонні дзвінки.

Завдяки дистанційній роботі фішингові електронні листи стають все більш поширеними. Відповідно до щорічного звіту Trend Micro про кібербезпеку за 2020 рік, більшість співробітників вважали, що IT-відділи або використання VPN допоможуть зменшити кількість фішингових атак. Але правда в тому, що працівники все ще отримують фішинг.

У першому кварталі 2022 року обсяг фішингу зріс на 4,4% порівняно з першим кварталом 2021 року. Загальна кількість фішингових сайтів, спостережуваних у першому кварталі 2022 року, стабільно зростала з січня по березень, показуючи значно меншу волатильність, ніж у 2021 році. Однак загалом обсяг фішингу в першому кварталі 2022 року був таким же, як і в першому кварталі 2021 року. щомісячний обсяг був передбачуваним і не мав непостійної активності, свідками якої ми були минулого року. Забігаючи наперед, ми очікуємо, що масштабні атаки спричинять сплески активності протягом 2022 року, оскільки опортуністичні актори будуть націлені на вразливі бренди та компанії [1].

Рис. 1.1. Обсяг фішингових атак [1]

У першому кварталі фінансові компанії були найбільше об’єктами фішинг-атаки щодо крадіжки облікових даних, що становить 53,8% усіх атак. Протягом чотирьох кварталів поспіль фінансові показники зазнавали жорстких цілей і вони продовжують представляти більшість атак у 1 кварталі, незважаючи на падіння на 7,4% порівняно з 4 кварталом.У першому кварталі технологічний сектор загалом був більш націленим. Соціальні мережі очолювали групу, на яку припало 21,5% фішингових даних щодо крадіжки облікових даних і відчуває найбільше збільшення обсягу атак (+9,6%). Веб-пошта/онлайн-сервіси (5,5%), електронна комерція (1,9%) і хмарне сховище/хостинг (1,7%) також зазнали збільшення кількості атак.

Телекомунікаційна галузь була єдиною галуззю, яка зазнала падіння в першому кварталі, зменшившись на 10,3% у порівнянні з четвертим кварталом і склавши 14,3% зафіксованих фішингових атак.

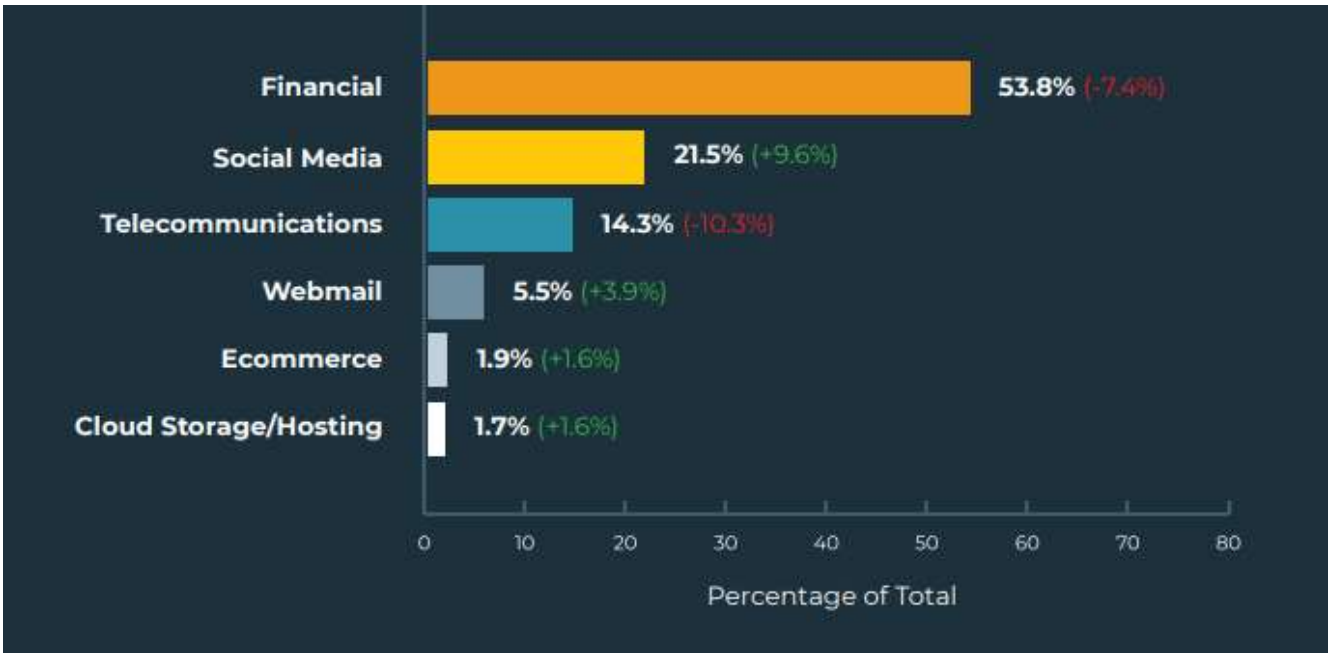

Рис 1.2. Статистика фішингу по сфері діяльності [1]

Методи проведення. Перший квартал 2022 року став першим за п’ять кварталів поспіль, коли більшість фішингових сайтів було створено за допомогою платної реєстрації доменів або зламаних сайтів. Майже 52% фішингових сайтів зловживали платними послугами. Ця віха частково сприяла постійному зростанню зловживань щоквартально протягом 2021 року та, нарешті, збільшенню кількості платних реєстрацій доменів на 3,2% з четвертого кварталу. Злом існуючих веб-сайтів залишався найпоширенішим методом інсценування в першому кварталі, що становить 35,1% усіх інцидентів. Компрометація існуючих веб-сайтів залишалася найпоширенішим методом інсценування в першому кварталі, що становить 35,1% усіх інцидентів.

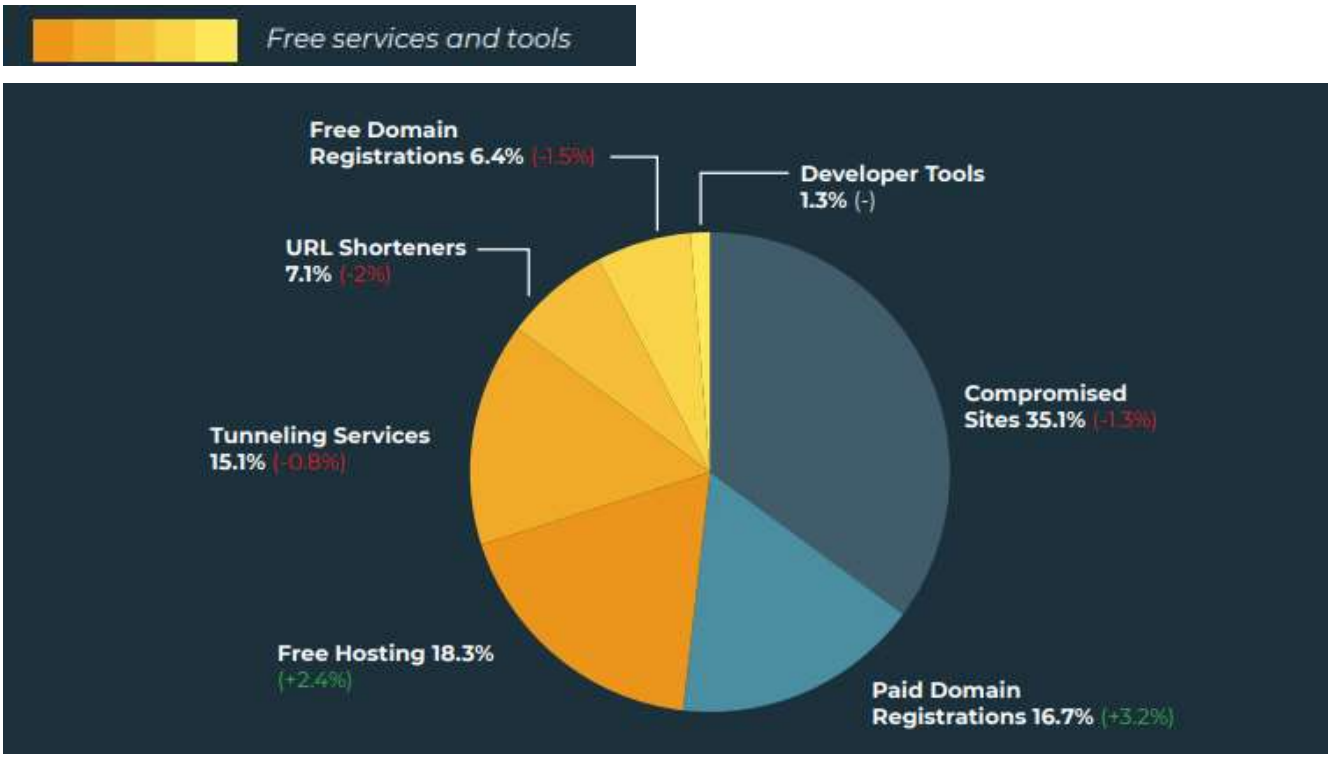

Рис.1.3. Статистика щодо методів проведення

Проведемо аналіз фішингових атак на корпоративних користувачів.

У першому кварталі зросла кількість зловмисних електронних листів, націлених на скриньки вхідних повідомлень користувачів, після незначного падіння звітів у четвертому кварталі. Починаючи з першого кварталу 2021 року кількість електронних листів, про які співробітники повідомляють як зловмисні, невпинно зростає та становить значну загрозу для організацій. Хоча більшість електронних листів, про які повідомляють співробітники, не класифікуються як зловмисні, для запобігання атакам, які все частіше проникають через фільтри електронної пошти, потрібна ідентифікація та повідомлення про підозрілу діяльність навченим персоналом.

Хоча майже 82% повідомлених електронних листів було класифіковано як загрозу не виявлено, частка повідомлень, які були визнані настільки зловмисними або підозрілими, що взаємодію можна було вважати небезпечною, зросла до 18,3% повідомлень.

Рис 1.4. Кількість фішингових листів [1]

Загрози, які знайдено в корпоративних вхідних ящках.

Інциденти крадіжки облікових даних і атаки соціальної інженерії на основі реагування становлять 96,2% від усіх загроз електронної пошти, виявлених у корпоративних скриньках у першому кварталі. Крадіжка облікових даних була найбільш домінуючим типом загрози, що спричинило майже 60% атак. Це означає збільшення частки на 6,9% порівняно з четвертим кварталом і збільшує розрив між крадіжкою облікових даних та іншими загрозами електронної пошти.

Хоча кількість успішних атак програм-вимагачів, націлених на бізнес, продовжує зростати, частка Malware Delivery знизилася на 5,9%, що становить трохи менше 4% загроз, виявлених у корпоративних папках вхідних повідомлень. Загрози на основі реагування залишалися дещо стабільними, становлячи 37,5% усіх загроз електронною поштою.

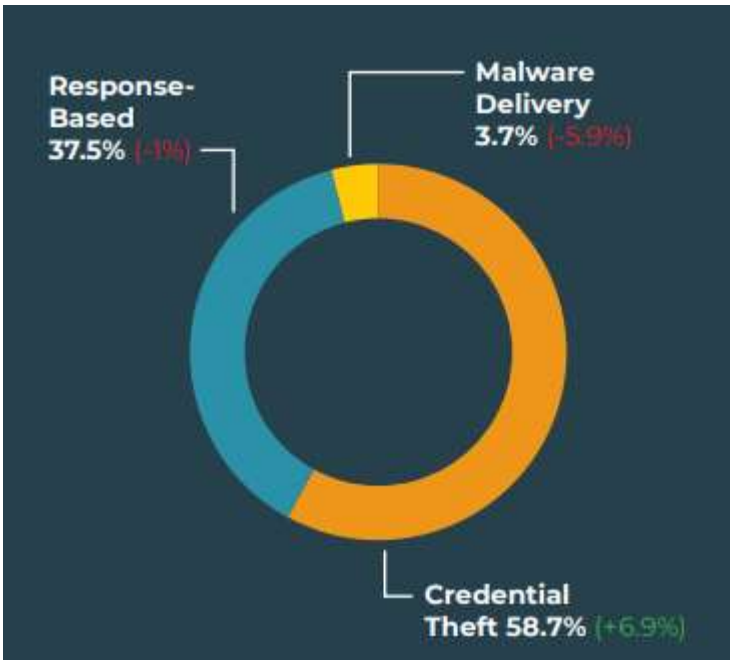

Рис. 1.5. Статистика загроз, які знайдено в корпоративних вхідних ящках.

Як видно з показаної статистики, необхідно значну увагу звертати на захист користувачів від фішингових атак.

1.2. Аналіз підходів до проведення фішингових атак

Фішинг – це коли зловмисники намагаються обманом змусити користувачів зробити «неправильну річ», наприклад натиснути погане посилання, яке завантажить зловмисне програмне забезпечення або спрямує їх на хитрий веб-сайт [2].

Фішинг може здійснюватися за допомогою текстового повідомлення, соціальних мереж або по телефону, але термін «фішинг» в основному використовується для опису атак, які надходять електронною поштою. Фішингові електронні листи можуть потрапляти безпосередньо до мільйонів користувачів і ховатися серед величезної кількості доброякісних електронних листів, які отримують зайняті користувачі. Атаки можуть встановлювати зловмисне програмне забезпечення (наприклад, програми-вимагачі), саботувати системи або викрадати інтелектуальну власність і гроші.

Фішингові електронні листи можуть вразити організацію будь-якого розміру та типу. Ви можете потрапити в масову кампанію (де зловмисник просто хоче зібрати нові паролі чи заробити легкі гроші) або це може бути першим кроком у цілеспрямованій атаці на вашу компанію, метою якої може бути щось важливе. більш конкретно, як-от крадіжка конфіденційних даних. У цілеспрямованій кампанії зловмисник може використовувати інформацію про ваших співробітників або компанію, щоб зробити свої повідомлення ще більш переконливими та реалістичними. Це зазвичай називають фішингом .

Кількість фішингових підходів, що застосовуються для крадіжок особистих даних постійно зростає, випробовуються нові варіанти. Виходячи з того, як працює фішинг, їх жертви та ціль, на яку націлюються нападники, можна класифікувати фішинг на типи.

А) Deceptive Phishing (Оманливий Фішинг) - найпоширеніший метод атаки на сьогоднішній день і включає надсилання повідомлень про необхідність перевірки інформації про акаунт, збій системи, що вимагає від користувачів повторного введення своєї інформації, фіктивні платежі за рахунок, нові безкоштовні послуги, що вимагають швидких дій, та багато інших шахрайств транслюються широкій групі одержувачів з надією, що необачний відповість натиснувши посилання, або підписавшись на фіктивний сайт, де може бути зібрана конфіденційна інформація.

Б) Spear Phishing (Ціленаправлений фішинг) - цільові фішингові атаки схожі на Deceptive Phishing (оманливий фішинг), за винятком того, що вони націлені на окрему людину, відділ або організацію. При цій формі фішингу фішингових електронного листа відправляється законним особою, часто з тієї ж компанії, яка займає довірчу позицію. Цей фішинг може надсилатись з зовні надійного зовнішнього джерела, який виглядає законним і спеціально націлений на окрему особу або підрозділ в організації.

В) Content-Injection Phishing (Фішинг з впровадженням контенту) - це форма фішингу, при якій фішер вставляє шкідливий контент на законний веб-сайт. Цей контент може перенаправляти користувачів на інший веб-сайт за вибором фішера,

встановити шкідливе ПЗ на комп'ютер користувача або вставити фрейм на законний веб-сайт, який буде перенаправляти дані, введені користувачем назад фішеру.

1.3. Багаторівневий підхід до захисту від фішингу

Типовий захист від фішингу часто покладається виключно на те, що користувачі можуть помітити фішингові електронні листи. Цей підхід матиме лише обмежений успіх. Натомість необхідно розширити захист, включивши більше технічних заходів. Це покращить стійкість проти фішингових атак, не порушуючи продуктивність ваших користувачів. Тоді з’являється кілька можливостей виявити фішингову атаку, а потім зупинити її, перш ніж вона завдасть шкоди. Ви також визнаєте, що деякі атаки будуть проходити, оскільки це допоможе вам спланувати інциденти та мінімізувати завдану шкоду.

Пом’якшення, щодо захисту від поділяються на чотири рівні, на яких ви можете будувати свій захист:

Ускладніть зловмисникам доступ до ваших користувачів.

Допоможіть користувачам ідентифікувати й повідомляти про ймовірні фішингові листи.

Захистіть свою організацію від впливу непомічених фішингових листів.

Швидко реагуйте на інциденти.

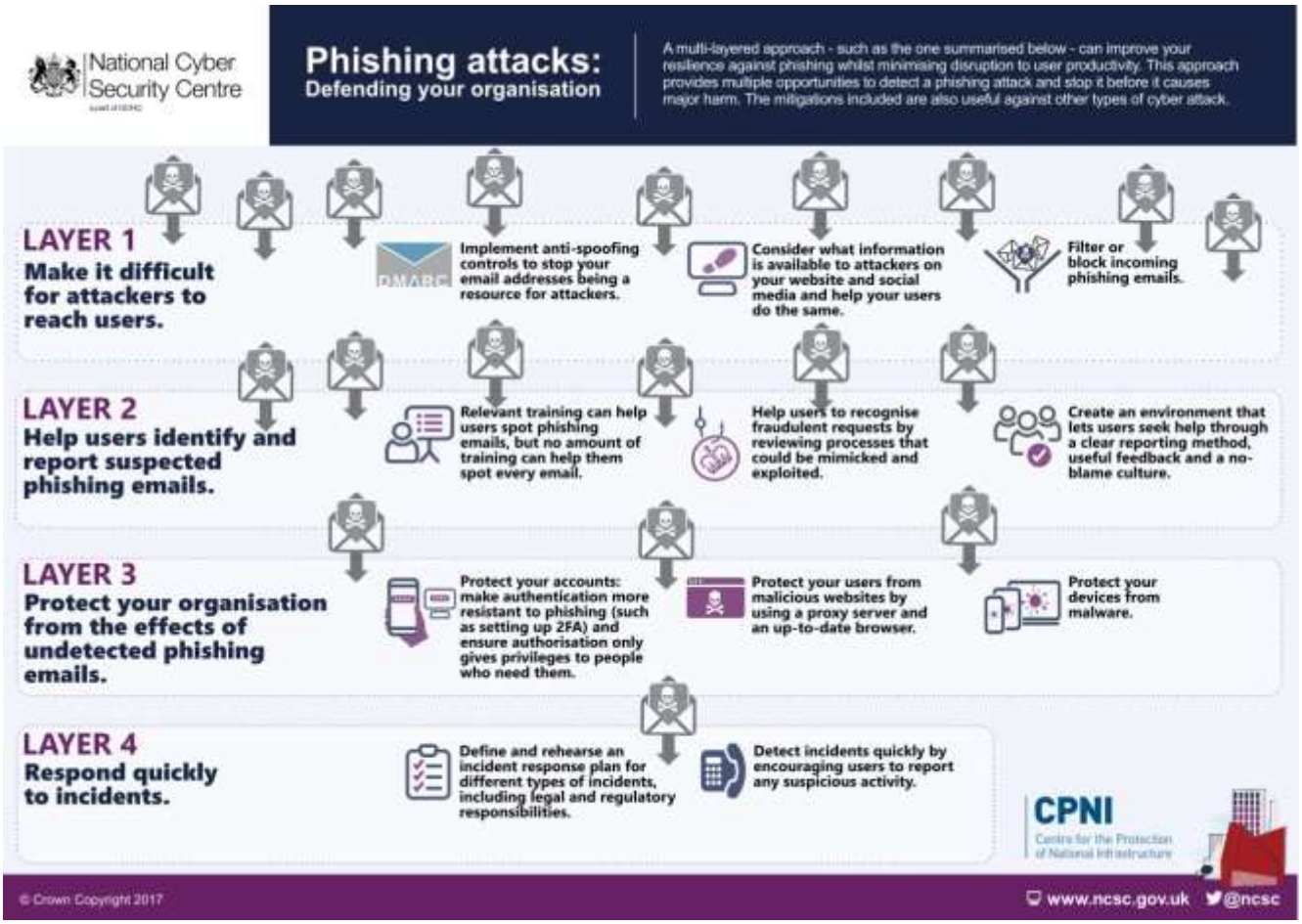

Рис. 1.6. Багаторівневий підхід до захисту від фішингу [2]

Деякі із запропонованих засобів пом’якшення можуть бути неможливими в контексті вашої організації. Якщо ви не можете впровадити їх усі, спробуйте вирішити принаймні деякі пом’якшення на кожному з рівнів . Пом’якшення в межах кожного рівня підсумовано в наступній інфографіці.

Розглянемо кожний рівень.

Ускладніть зловмисникам доступ до ваших користувачів.

1. Не дозволяйте вашим адресам електронної пошти бути ресурсом для зловмисників.

Зловмисники «підробляють» надійні електронні листи, створюючи вигляд, що їхні електронні листи надіслані авторитетними організаціями (наприклад, вашою). Ці підроблені електронні листи можна використовувати для нападу на ваших клієнтів або людей у вашій організації.

Ускладніть підробку електронної пошти з ваших доменів, використовуючи засоби захисту від спуфінгу: DMARC, SPF і DKIM , і заохочуйте своїх контактів робити те саме.

2. Зменшіть інформацію, доступну для зловмисників

Зловмисники використовують загальнодоступну інформацію про вашу організацію та користувачів, щоб зробити свої фішингові (і особливо фішингові) повідомлення більш переконливими. Це часто збирають із веб-сайту та облікових записів у соціальних мережах (інформація, відома як «цифровий слід»).

Це можна зробити наступним шляхом.

Подумайте, що повинні знати відвідувачі вашого веб-сайту, а які деталі непотрібні (але можуть бути корисними для зловмисників)? Це особливо важливо для високопоставлених членів вашої організації, оскільки ця інформація може бути використана для створення персоналізованих атак (тип стрімкого фішингу, спрямованого на великого фішинга, наприклад, на члена правління, який має доступ до цінних активів).

Допоможіть своїм співробітникам зрозуміти, як обмін їх особистою інформацією може вплинути на них і вашу організацію, і розробіть це в чітку політику цифрового сліду для всіх користувачів.

Будьте в курсі того, що ваші партнери, підрядники та постачальники роздають про вашу організацію в Інтернеті.

3. Фільтруйте або блокуйте вхідні фішингові листи

Фільтрування або блокування фішингового електронного листа до того, як воно досягне ваших користувачів, не тільки зменшує ймовірність фішингового інциденту; це також зменшує час, який користувачі повинні витрачати на перевірку електронних листів і звітування про них. Ваша служба фільтрації/блокування може бути вбудованою службою постачальника електронної пошти на базі хмари або спеціальною службою для вашого власного сервера електронної пошти.

Це робиться наступним чином. Перевіряйте всю вхідну електронну пошту на наявність спаму, фішингу та зловмисного програмного забезпечення.

Передбачувані фішингові електронні листи слід відфільтрувати або заблокувати, перш ніж вони дійдуть до вашого користувача. В ідеалі це має бути зроблено на сервері, але це також можна зробити на пристроях кінцевих користувачів (тобто в поштовому клієнті).

Для вхідної електронної пошти слід дотримуватися політики захисту від спуфінгу домену відправника. Якщо відправник має політику DMARC із політикою карантину або відхилення, тоді вам слід виконати прохання, якщо перевірки не вдасться.

Якщо ви користуєтеся хмарним постачальником електронної пошти, переконайтеся, що його служба фільтрації/блокування відповідає вашим потребам і що вона ввімкнена за умовчанням для всіх ваших користувачів. Якщо ви розміщуєте власний сервер електронної пошти, переконайтеся, що перевірена служба фільтрації/блокування на місці. Це можна реалізувати локально та/або придбати як хмарну службу. Знову переконайтеся, що він увімкнено за замовчуванням для всіх ваших користувачів.

Служби фільтрації зазвичай надсилають електронну пошту до папок спаму/сміття, тоді як служби блокування гарантують, що вони ніколи не досягнуть вашого користувача. Правила, що визначають блокування або фільтрацію, необхідно налаштувати відповідно до потреб вашої організації. Якщо відфільтрувати всі підозрілі електронні листи до папок спаму/сміття, користувачам доведеться керувати великою кількістю електронних листів, що збільшить їх робоче навантаження та залишить відкритою можливість клацання. Однак якщо ви заблокуєте всі підозрілі електронні листи, деякі законні електронні листи можуть бути втрачені. Можливо, вам доведеться з часом змінити правила, щоб забезпечити найкращий компроміс і відповідати мінливим потребам і способам роботи вашого бізнесу.

Фільтрування електронної пошти на пристроях кінцевих користувачів може запропонувати додатковий рівень захисту від шкідливих електронних листів. Однак це не повинно компенсувати неефективні заходи на основі сервера, які можуть повністю блокувати велику кількість вхідних фішингових листів.

Електронну пошту можна фільтрувати або блокувати за допомогою різноманітних методів, зокрема: IP-адрес, доменних імен, списку дозволених/заборонених адрес електронної пошти, загальнодоступного спаму та списків заборонених відкритих ретрансляцій, типів вкладень і виявлення шкідливих програм [2].

Допомога користувачам ідентифікувати й повідомляти про ймовірні фішингові листи.

1. Уважно продумайте свій підхід до навчання фішингу.

Навчання ваших користувачів, зокрема у формі симуляції фішингу, є тим рівнем, якому часто приділяється надмірна увага під час захисту від фішингу. Ваші користувачі не можуть компенсувати недоліки кібербезпеки деінде. Відповіді на електронні листи та натискання посилань є важливою частиною сучасного робочого середовища, тому нереалістично очікувати, що користувачі будуть постійно бути пильними.

Помітити фішингові електронні листи важко, а фішинг ще важче виявити. Поради, надані в багатьох навчальних пакетах, засновані на стандартних попередженнях і знаках, допоможуть вашим користувачам помітити деякі фішингові листи, але вони не можуть навчити кожного виявляти всі фішингові електронні листи.

Це робиться наступним чином. Поясніть, що фішингові повідомлення важко помітити, і ви не очікуєте, що люди зможуть ідентифікувати їх у 100% випадків. Ніколи не карайте користувачів, які насилу розпізнають фішингові листи; це погана ідея з багатьох причин . Користувачі, які бояться репресій, не повідомлятимуть про помилки негайно, якщо взагалі повідомлять.

Навчання має сприяти готовності ваших користувачів повідомляти про майбутні інциденти та запевнити їх у тому, що можна звертатися за подальшою підтримкою, коли щось виглядає підозрілим. Це повідомлення потребує підтримки всіх відділів, включаючи відділ кадрів, підтримку та вище керівництво.

Переконайтеся, що ваші користувачі розуміють природу загрози, яку створює фішинг, особливо ті відділи, які можуть бути більш уразливими до нього.

Відділи, які працюють із клієнтами, можуть отримувати велику кількість небажаних електронних листів, тоді як персонал, уповноважений на доступ до конфіденційної інформації, управління фінансовими активами або адміністрування IT-систем, представлятиме більший інтерес для зловмисника (і може стати об’єктом складної фішингової кампанії). Переконайтесь, що ці більш вразливі верстви персоналу усвідомлюють ризики та запропонуйте їм додаткову підтримку.

Допоможіть своїм користувачам помітити типові ознаки фішингових повідомлень, як-от терміновість або повноваження, які змушують користувача діяти.

Використання симуляції фішингу не зробить вашу організацію більш безпечною . Деякі компанії проводять тренінги для користувачів, які змушують учасників створити власну фішингову електронну пошту, що дає їм набагато більше уявлення про використовувані методи.

2. Спростіть своїм користувачам розпізнавання шахрайських запитів

Зловмисники можуть використовувати процеси, щоб обманом змусити користувачів надати інформацію (зокрема паролі) або здійснити неавторизовані платежі. Подумайте, які процеси можуть імітувати зловмисники, і як їх переглянути та вдосконалити, щоб фішингові атаки було легше виявити.

Крім того, подумайте про те, як будуть сприйняті електронні листи, які ви надсилаєте постачальникам і клієнтам. Чи можуть ваші одержувачі легко відрізнити вашу справжню електронну пошту від фішингової атаки? Зрештою, не можна очікувати, що їхні користувачі (як ваші) будуть шукати та розпізнавати всі ознаки фішингу. Не думайте, що надання особистої інформації підтвердить вашу особу; викрадена або досліджена інформація використовується фішерами, щоб зробити свої електронні листи більш переконливими.

Для цього необхідно переконайтеся, що співробітники знайомі зі звичайними методами роботи для ключових завдань (наприклад, як здійснюються платежі), щоб вони були краще підготовлені для розпізнавання незвичайних запитів.

Зробіть процеси більш стійкими до фішингу, забезпечивши перевірку всіх важливих запитів електронною поштою за допомогою другого типу зв’язку

(наприклад, SMS-повідомлення, телефонний дзвінок, вхід в обліковий запис або підтвердження поштою чи особисто). Інші приклади зміни процесів включати використання іншого методу входу або обмін файлами через хмарний обліковий запис із контрольованим доступом замість надсилання файлів у вигляді вкладень.

Подумайте про те, як ваші вихідні повідомлення виглядають для постачальників і клієнтів. Чи очікує одержувач електронного листа та чи впізнає він вашу електронну адресу? Чи є у них спосіб дізнатися, чи справжні посилання?

Розкажіть своїм постачальникам або клієнтам, на що слід звернути увагу (наприклад, «ми ніколи не запитуватимемо ваш пароль» або «наші банківські реквізити ніколи не зміняться»). Це дає одержувачу ще один шанс виявити фіш.

3. Створіть середовище, яке спонукатиме користувачів повідомляти про спроби фішингу

Створення культури, у якій користувачі можуть повідомляти про спроби фішингу (включно з тими, на які натискають), дає вам важливу інформацію про типи фішингових атак, які використовуються. Ви також можете дізнатися, які типи електронних листів приймають за фішинг, і як це може вплинути на вашу організацію.

Тому, необхідно становити ефективний процес, за допомогою якого користувачі повідомлятимуть, що вони вважають, що спроба фішингу могла пройти повз технічний захист вашої організації. Чи процес зрозумілий, простий і зручний у використанні? Чи впевнені користувачі в тому, що звіти будуть розглянуті?

Швидко надсилайте відгуки про вжиті дії та пояснюйте, що їхні внески мають значення.

Подумайте про те, як ви можете використовувати неформальні канали зв’язку (через колег, команди або внутрішні дошки оголошень), щоб створити середовище, у якому користувачам буде легко «вголос попросити» підтримки та вказівок, коли вони можуть зіткнутися зі спробою фішингу.

Уникайте створення культури покарання або звинувачення навколо фішингу. Важливо, щоб користувачі відчували підтримку, щоб висловитися, навіть якщо вони «клацнули» і пізніше подумали, що щось може бути підозрілим.

Захистіть свою організацію від впливу непомічених фішингових листів.

1. Зловмисне програмне забезпечення часто приховано у фішингових електронних листах або на веб-сайтах, на які вони посилаються. Добре налаштовані пристрої та ефективний захист кінцевої точки можуть зупинити встановлення зловмисного програмного забезпечення, навіть якщо клацнути електронний лист. Існує багато інших засобів захисту від зловмисного програмного забезпечення, і вам потрібно враховувати свої потреби в безпеці та способи роботи, щоб забезпечити правильний підхід. Деякі засоби захисту є специфічними для певних загроз (наприклад, вимкнення макросів), а деякі можуть не підходити для всіх пристроїв (програмне забезпечення для захисту від шкідливих програм може бути попередньо встановлено на деяких пристроях і не потрібне на інших). Нарешті, вплив зловмисного програмного забезпечення на вашу ширшу систему залежатиме від того, як її налаштовано.

Для цього необхідно запобігти зловмисникам використовувати відомі вразливості, використовуючи лише підтримуване програмне забезпечення та пристрої. Переконайтеся, що програмне забезпечення та пристрої завжди оновлюються з останніми виправленнями.

Запобігайте випадковому встановленню користувачами зловмисного програмного забезпечення з фішингового електронного листа, обмеживши облікові записи адміністратора лише тими, кому потрібні ці права. Люди з обліковими записами адміністратора не повинні використовувати ці облікові записи для перевірки електронної пошти чи перегляду веб-сторінок.

2. Захистіть своїх користувачів від шкідливих веб-сайтів

Посилання на шкідливі веб-сайти часто є ключовою частиною фішингового електронного листа. Однак, якщо посилання не може відкрити веб-сайт, атака не може продовжуватися.

Тому, більшість сучасних веб-переглядачів блокуватимуть відомі фішингові та шкідливі сайти. Зауважте, що на мобільних пристроях це не завжди так.

Організації повинні запустити проксі-сервіс, власний або хмарний, щоб блокувати будь-які спроби отримати доступ до веб-сайтів, на яких було виявлено розміщення зловмисного програмного забезпечення або фішингових кампаній.

Організації державного сектору повинні використовувати службу DNS державного сектору , яка не дозволить користувачам розпізнавати домени, відомі як шкідливі.

3. Захистіть свої облікові записи за допомогою ефективної автентифікації та авторизації.

Паролі є основною мішенню для зловмисників, особливо якщо вони призначені для облікових записів із такими привілеями, як доступ до конфіденційної інформації, обробка фінансових активів або адміністрування IT-систем. Вам слід зробити процес входу в усі облікові записи більш стійким до фішингу та обмежити кількість облікових записів із привілейованим доступом до абсолютного мінімуму.

Тому, додайте додатковий захист процесу входу, налаштувавши багатофакторну автентифікацію (MFA) , яка також називається «двоетапною перевіркою» в деяких веб-службах. Наявність другого фактора означає, що зловмисник не може отримати доступ до облікового запису, використовуючи лише вкрадений пароль.

Розгляньте можливість використання менеджерів паролів , деякі з яких можуть розпізнавати справжні веб-сайти та не виконуватимуть автозаповнення на підроблених веб-сайтах. Подібним чином ви можете використовувати метод єдиного входу (де пристрій автоматично розпізнає справжній веб-сайт і входить на нього). Застосування цих методів означає, що введення паролів вручну стає незвичайним, і користувачеві легше розпізнати підозрілий запит.

Розгляньте можливість використання альтернативних механізмів входу (наприклад, біометричних даних або смарт-карт), які вимагають більше зусиль для викрадення, ніж паролі.

Шкода, яку може завдати зловмисник, пропорційна привілеям, призначеним обліковим даним, які він вкрав. Надайте привілейований доступ лише тим людям, яким це потрібно для виконання своїх ролей. Регулярно переглядайте їх і скасовуйте привілеї, якщо вони більше не потрібні.

Видаліть або призупиніть облікові записи, які більше не використовуються, наприклад, коли член вашої організації залишає або переходить на нову роль.

Перегляньте свою політику щодо паролів . Це може (наприклад) зменшити ймовірність повторного використання пароля персоналом для домашніх і робочих облікових записів.

Швидко реагуйте на інциденти.

Дізнавшись про інцидент раніше, ніж пізно, можна обмежити шкоду, яку він може завдати.

Тому, переконайтеся, що користувачі заздалегідь знають, як вони можуть повідомляти про інциденти. Майте на увазі, що вони можуть не мати доступу до звичайних засобів зв'язку, якщо їхній пристрій зламано.

Використовуйте систему реєстрації безпеки , щоб виявити інциденти, про які ваші користувачі не знають. Щоб зібрати цю інформацію, ви можете використовувати інструменти моніторингу, вбудовані у ваші стандартні служби (наприклад, хмарні панелі безпеки електронної пошти), створити внутрішню команду або передати керовану службу моніторингу безпеки.

Майте план реагування на інцидент

Після виявлення інциденту вам потрібно знати, що робити, щоб якомога швидше запобігти подальшій шкоді.

Для цього необхідно переконатися, що ваша організація знає, що робити у випадку різних типів інцидентів. Наприклад, як примусово скинути пароль, якщо пароль зламано?

Плани реагування на інциденти слід відпрацьовувати до того, як станеться інцидент.

2. МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ ФІШИНГОВИХ АТАК НА БАЗІ CYREN INBOX SECURITY

2.1. Призначення та основні можливості Cyren Inbox Security

Cyren Inbox Security - це додаткове рішення для захисту електронної пошти, яке повністю інтегрується з Microsoft 365 (раніше Office 365), і є першою службою, яка поєднувала безперервний моніторинг електронної пошти і виявлення загроз з автоматичним відповіддю і виправленням для кожної поштової скриньки в організації. Cyren Inbox Security також є першою пропозицією, що забезпечує автоматизовану структуру для краудсорсінгового виявлення загроз і збору інформації безпосередньо від користувачів (рис.2.1) [3].

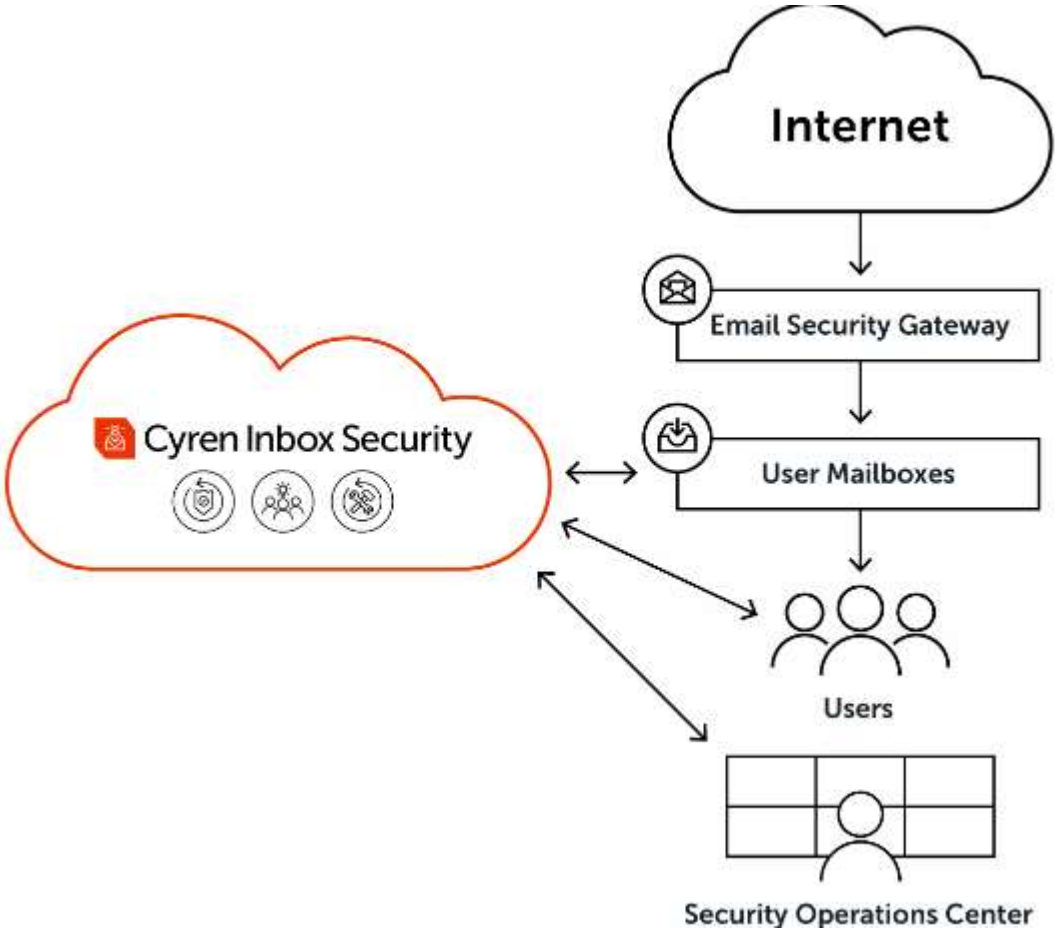

Рис. 2.1. Архітектура Cyren Inbox Security [3]

Cyren Inbox Security - це служба, повністю заснована на API, яка забезпечує безпроблемну адаптацію і природну роботу з Microsoft 365, а розгортання займає всього кілька хвилин. Cyren Inbox Security встановлює безперервний, адаптивний і автоматизований рівень захисту прав в поштовій скриньці користувача, де це найбільше необхідно [3].

Cyren Inbox Security, представлений у вигляді власної хмарної служби, забезпечує:

- Постійний моніторинг та виявлення антифішингу

Постійне повторне сканування вхідних, вихідних та доставлених електронних листів у всіх папках забезпечує швидке виявлення показників ухиляючихся атак, тоді як аналіз у режимі реального часу поведінки користувачів та поштової скриньки виявляє аномалії, що вказують на можливу загрозу.

- Автоматична відповідь на фішинг і виправлення

Платформа реагування на основі політик автоматизує дії щодо виправлення становища в окремих поштових скриньках і у всіх поштових скриньках в організації, а автоматизовані робочі процеси управління інцидентами додатково скорочують накладні витрати на розслідування і прискорюють усунення загроз.

- Виявлення користувачів з краудсорсингу

Плагін поштової скриньки дозволяє користувачам сканувати і повідомляти про підозрілі електронні листи на свій розсуд, а також автоматично закривати цикл зворотного зв'язку при попередженнях, що підсилює навчання безпеки і забезпечує цінний краудсорсінговий аналіз загроз, який повертається в систему для поліпшення виявлення загроз.

Cyren Inbox Security використовує широкий набір хмарних обчислень і технології безпеки для виявлення ухильних фішингових атак і надає найбільш передові можливості виявлення загроз, в тому числі перевірку заголовків електронної пошти, корисного навантаження, URL-адреси і вкладення в реальному часі (рис.2.2) [4].

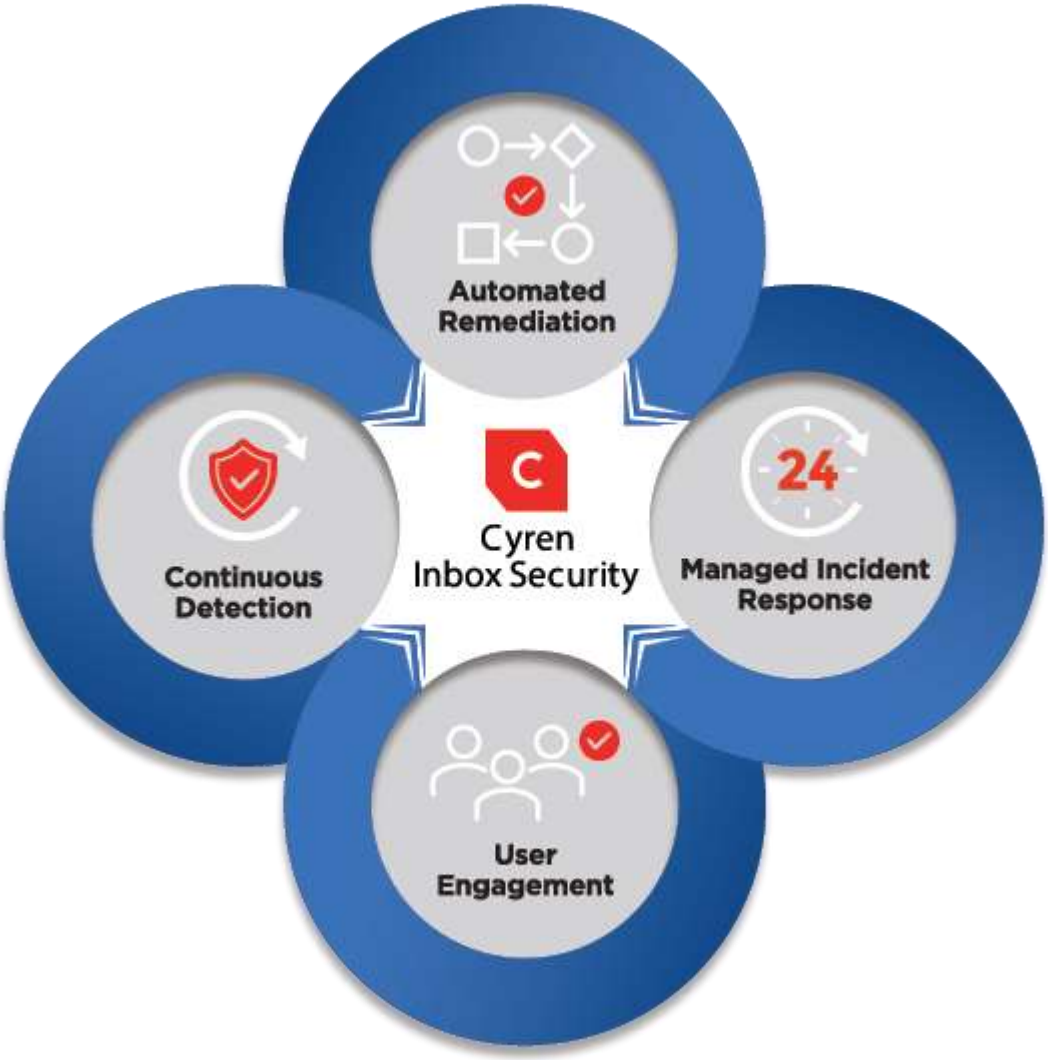

Рис.2.2. Функції Cyren Inbox Security [4]

Глобальна хмара безпеки обробляє 25 мільярдів транзакцій електронної пошти та веб-безпеки щодня; визначає 9 нових загроз і блокує більше 3000 відомих загроз щосекунди.

2.2. Функції сервісу Cyren Inbox Security

Сервіс Cyren включає простий в установці і використанні плагін Outlook, що знижує навантаження на підтримку користувачів з боку служби підтримки IT і включає аналітику загроз, зібрану з краудсорсингу, щоб допомогти ідентифікувати і захистити від фішингових атак. Кнопка в електронному листі дозволяє

користувачеві клацнути по ньому, щоб сканувати будь-який підозрілий електронний лист, і отримати негайні результати. Якщо відповідь негативна і користувач не згоден, користувач може клацнути, щоб відправити електронний лист в Security Lab для експертного аналізу безпеки.

Можливості автоматичного виправлення та управління інцидентами забезпечує швидке видалення загроз з організацій.

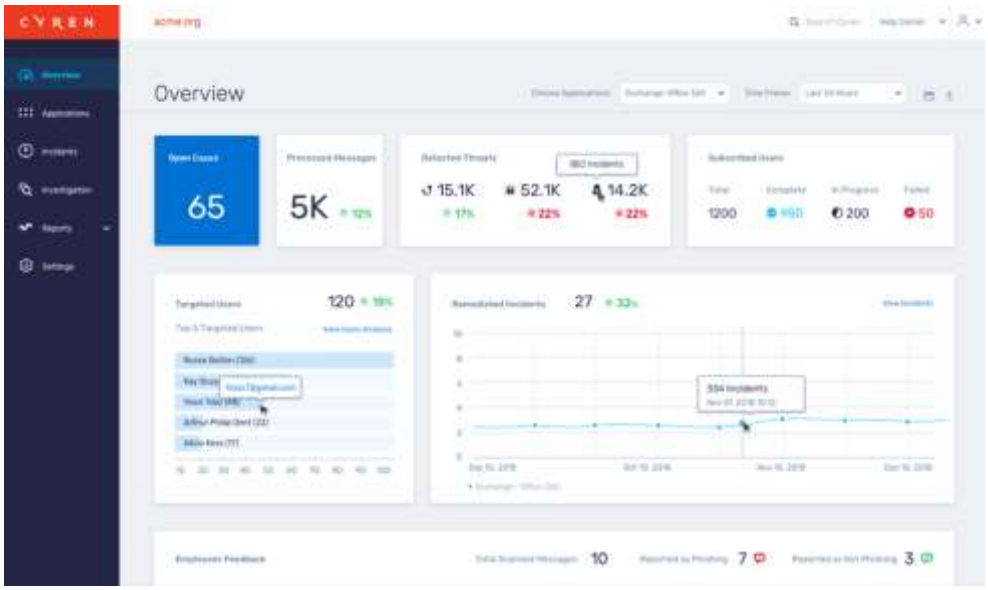

Рис 2.3. Інтерфейс Cyren Inbox Security [16]

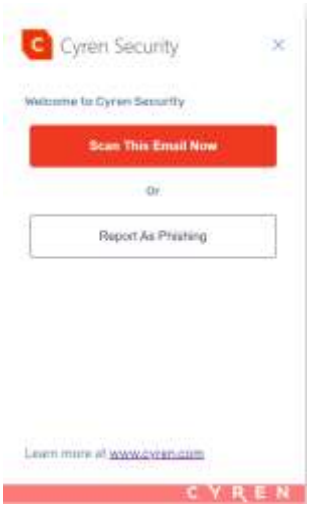

Рис.2.4. Влаштований плагін Cyren Security в Outlook

Коли користувач Cyren Inbox Security натискає червону кнопку PhishScan, щоб повідомити про підозру на електронну пошту, інциденти можна віднести до однієї з трьох категорій:

• Фішингова загроза виявлена CIS, але не повинна бути;

• Фішингова загроза не виявлена CIS, але повинна бути;

• Неприємні електронні листи (не загроза безпеці, але небажані електронні листи).

Кожне повідомлення про загрозу досліджується та перевіряється експертами CIR, щоб визначити, чи загроза є реальною чи ні. Перевірені загрози можуть спричинити автоматичне повторне сканування та виправлення, наприклад, для знищення фішингової атаки. Коли повідомлена користувачем загроза недійсна, інцидент вирішується та закривається аналітиками CIS.

Щодня аналітики Cyren Incident Response Service (CIRS) розслідують і усувають безліч інцидентів, таких як:

А) Атака Business Email Compromised

Один із найпоширеніших типів атак BEC, який спостерігається у системі безпеки Cyren Inbox.

Найбільш часто використовувані моделі атаки підробки електронної пошти включають:

- Ім'я відправника та поштова адреса не співпадають (підроблені заголовки - це показник №1 підробленого електронного листа)
- Тема електронного листа (як правило, коротка і проста: "Привіт", "Завдання" тощо)
- Короткий і вимогливий вміст електронного листа (переконання потенційної жертви діяти швидко)
- Масштаб атаки (орієнтований спеціально на кількох співробітників, які мають доступ до корпоративної конфіденційної інформації та / або коштів)

Незважаючи на те, що невеликі атаки BEC трапляються частіше, Cyren Inbox Security спостерігали масову атаку підробки електронної пошти, націлену на численних співробітників однієї компанії одночасно рис 2.5. та 2.6.

Рис. 2.5. BEC, спрямована на працівників організації

Рис. 2.6. Результати автентифікації для підробленої електронної пошти

Зловмисник використав ряд методів, які зробили повідомлення візуально більш справжнім та допомогли обійти існуючі методи фільтрації електронної пошти:

- електронна пошта, надіслана із домену законного відправника, який належить надійному постачальнику веб-пошти
- відображене ім'я виглядає так, як ніби воно надійшло від справжньої особи, а електронна пошта не містить ніяких підозрілих даних.
- адреса відправника не відображається для одержувача, якщо вона відкрита в мобільному додатку. Мобільний телефон залишається лідером у середовищі читання електронних листів, оскільки 42% усіх електронних листів відкривається на смартфонах або планшетах.

Надсилаючи підроблений електронний лист такій кількості співробітників, ця атака видається дуже незвичною з точки зору масштабу для типів атак BEC.

Зазвичай обмеження кількості потенційних жертв підробки електронної пошти BEC становить до 10, а в середньому - близько чотирьох.

Незважаючи на те, що ця атака була невидима для традиційного Secure Email Gateway і досягла поштових скриньок співробітників, цільова компанія використовує CIS, і в результаті атака була зупинена. Кожен електронний лист було автоматично сканувати і позначено як підозріле Cyren Inbox Security, інформуючи одержувачів про те, що електронний лист може бути нелегальним. Крім того, в результаті служби реагування на інциденти Cyren з її цілодобовою підтримкою для розслідування фішингу, використовуваної цільової організацією, кожна копія електронного листа була додатково досліджена, позначена як фішингова і видалена з поштової скриньки всього через кілька хвилин після того, як електронні листи спочатку були доставлені.

Б) Фішинг атака з використанням вкладенням

Одна з останніх фішингових атак, виявлених Cyren Inbox Security, полягала в спробі отримати особисті паролі одержувачів електронних листів через прикріплену html-сторінку, яка представляла собою файл Excel під назвою «Microsoft Office Center».

Співробітники декількох організацій, що використовують рішення Cyren Inbox Security, почали отримувати електронні листи, відправлені з автоматично згенерованих адрес електронної пошти, розміщених на зламаному домені відправника <server5.fngnetde-dns.com>.

Псевдонім відправника відображало цільову організацію <[Company] Invoicé Repot>, а тема пропонувала «Invoiće ID: XXXXXX is ready for paymeńt» рис 2.7. та 2.8. Фішери вміло використовували спеціальні символи в темі і видимій частині імені (é, ń), щоб звести до мінімуму ймовірність автоматичної фільтрації спаму в електронній пошті за ключовими словами «Рахунок-фактура» і «Платіж».

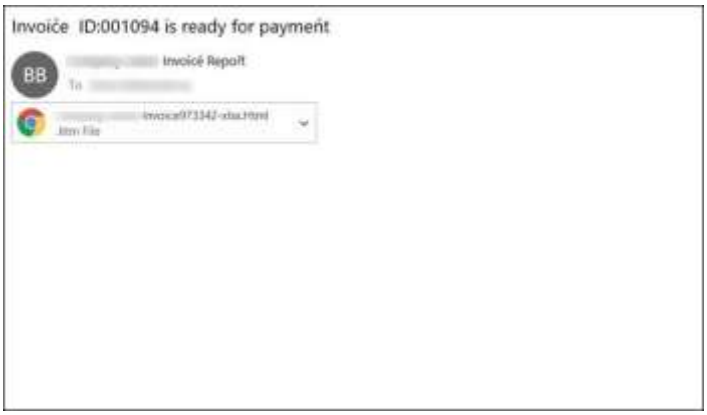

Рис. 2.7. Фішинговий лист з html файлом

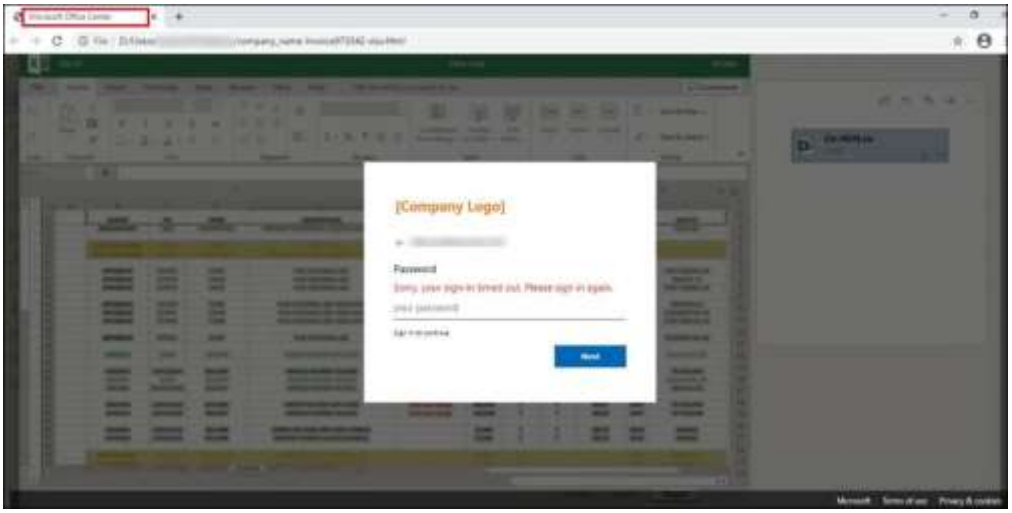

Рис. 2.8. Фішинговий html файл

Тіло листа було порожнім, але лист містив вкладення html, передає xlsx-файл рахунку-фактури, в якому згадувалася конкретна цільова компанія в його назві, що збільшувало шанси одержувача відкрити файл. Після відкриття на тлі Excel з'явилася підроблена сторінка входу під назвою «Microsoft Office Center» з метою вкрасти пароль користувача.

Скрипт містив окрему функцію, надайте телефону візуалізацію фішинговою кампанії (рис2.9):

```
<script>
function myFunction() {
var ml = " [base64 encoded recipient's email address]";
var logi = "[base64 encoded https://logo.clearbit.co/targeted_brand_logo]";
var ulb= atob(logi);
var go = atob(ml);
document.getElementById('mypic').setAttribute('src',ulb)
document.getElementById("myText").innerHTML = go;
document.getElementById('myvalue').value = go;
 }
  </script>
```

Рис. 2.9. Скрипт фішинг вкладення

Мінлива ml відповідає за адреса електронної пошти одержувача, а var logi додає зображення цільового логотипу бренду на фішингову сторінку. Зображення були взяті з logo.clearbit.com - законного інструменту Logo API від Clearbit, в якому безкоштовно доступні сотні логотипів компаній. Цей скрипт не тільки персоналізує атаку, але і значно збільшує потенційну кількість компаній, які можуть бути атаковані зловмисником, змінюючи тільки змінну логотипу.

Поле пароля у вкладенні HTML відповідає за крадіжку особистої інформації. Це виконується в формі PHP з публікацією методу і URL-адресою, яка відправить всі вставлені облікові дані і інформацію про пароль зловмиснику (Рис2.10).

Рис. 2.10. URL-адреса, куди надходить вся інформація

Діюча URL-адреса використовує законний японський сайт у ворожих цілях: enctype = ”multipart / form-data”, що вказує на те, що вся надіслана інформація про логін та пароль була б розділена на кілька частин та відправлена на фішинг-сервер.

В) Атака із шкідливим програмним забезбеченням

Співробітник отримує електронний лист від надійного і добре відомого відправника або від відомого бренду з запам'ятовується темою (наприклад, «Рахунок-фактура», «Підтвердження оплати» і т. Д). Лист містить прикріплений

файл, який зловмисник заархівувати і захищений паролем. Пароль створює ілюзію, що вкладення має містити конфіденційну особисту інформацію, яку необхідно захистити.

Пароль для відкриття файлу з zip-архіву включений в електронного листа:

Рис.2.11. Приклад шкідливої електронної пошти

Після введення пароля та відкриття файлу користувач заражається шкідливим програмним забезпеченням. Зазвичай це троян атака.

Троянська програма Emotet - найпоширеніша з усіх, з якими стикається Cyren Inbox Security. Зазвичай він розсилається через шкідливий спам і фішингові електронні листи, що містять заражені файли Microsoft Word або PDF. При відкритті файлу жертву обманом змушують включити макроси і запустити логіку шкідливого ПЗ.

Як видно з наведеного нижче прикладу, жертва відкрила зашифроване, заархівоване вкладення - файл Microsoft Word. Цей файл підробляє майстер активації Microsoft Office, який спонукає одержувача «Дозволити редагування» і «Дозволити вміст» для перегляду і редагування файлу.

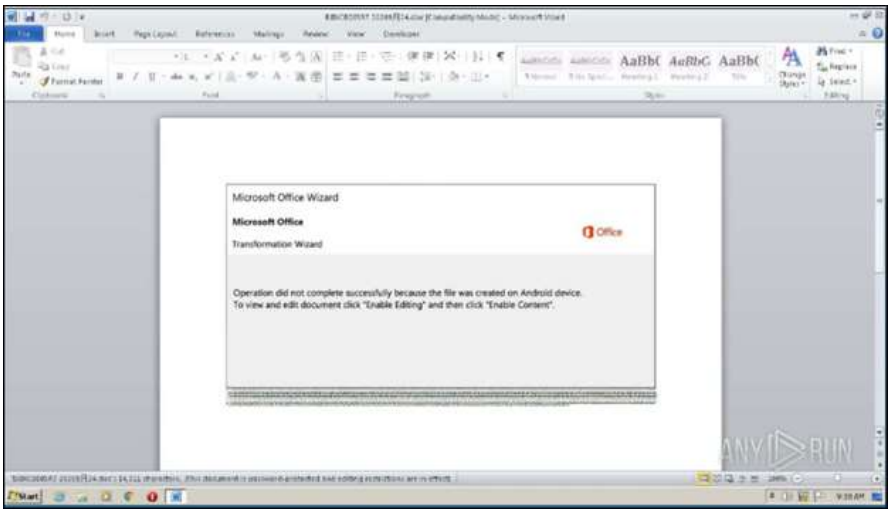

Рис. 2.13. Приклад вмісту зараженого Emotet документа Microsoft Word

Якщо користувач буде слідувати процесам «Дозволити редагування» і «Дозволити контент», він включить шкідливі макроси, вкорінені в ньому. А жертва цього навіть не помітить. Файл починає непомітно запускати сценарій PowerShell. Як результат, Emotet завантажить та виконає додаткове шкідливе програмне забезпечення, яке буде встановлено безпосередньо на ПК жертви та обійде всі можливі виявлення.

Атаки із використанням захищених паролем файлів zip (і користуючись перевагами нашої соціальної інженерії) практично невидимі для більшості методів фільтрації електронної пошти.

Для того, щоб заблокувати подібні атаки в Cyren Inbox Security використовується блокування електронних листів з яких надходять такого роду атаки. Крім того, для того, щоб швидко зупинити атаку, CIS надає можливість знайти всі електронні листи за темою та заблокувати, як «Malware», див рис. 2.10. Це зручно в тому випадку, коли листи зі шкідливим програмним забезпеченням надсилаються з різних електронних адресів, та вкладення мають різний хеш.

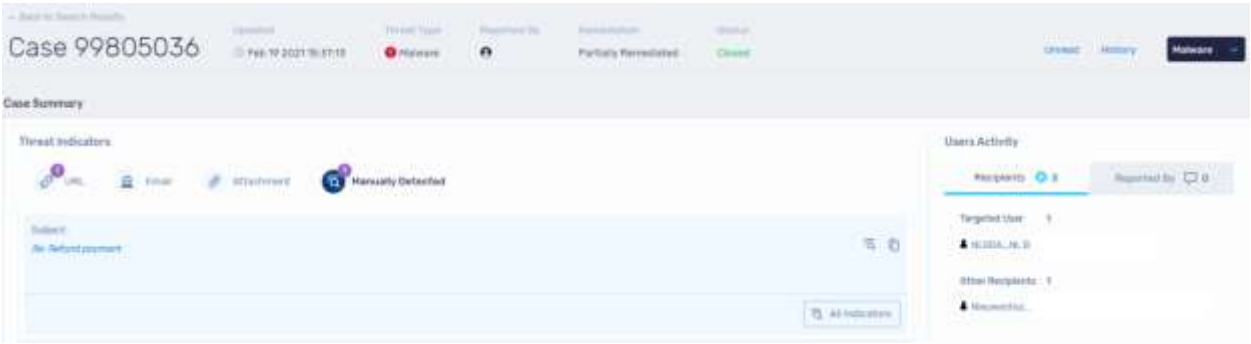

Рис. 2.14 Пошук фішингових електронних листів через тему

Завдяки CIS всі електронні листи, що були знайдені вручну, можуть бути негайно вирішені, через кнопку “Resolve as”, як шкідливі, також адміністратори, можуть вибрати, яку саме політику застосувати для цього інцидента. Електронні листи можуть бути відправлені в “Junk email”, або в “Deleted items”, окремо може бути вибрана функція додавання банеру, який повідомляє про те, що лист є фішинговим.

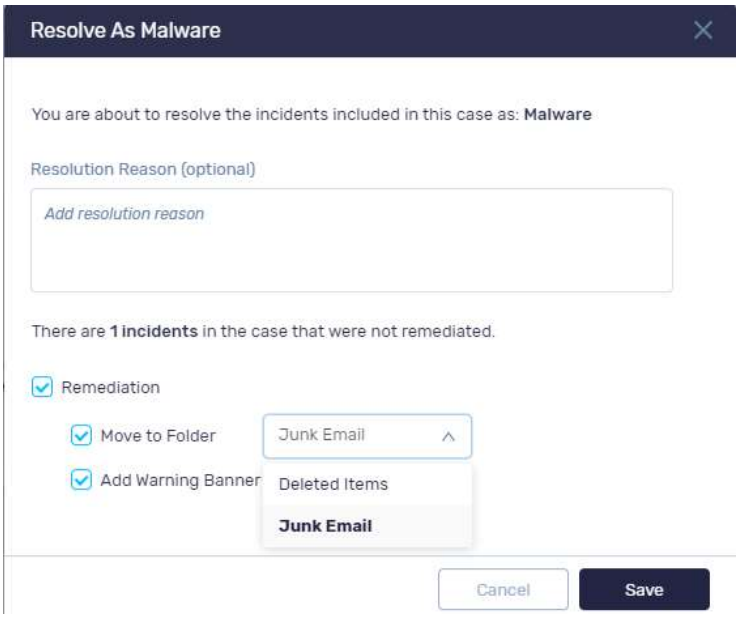

Рис. 2.15. Вирішення інцидентів, через кнопку “Resolve as” в CIS

Адміністратор чи аналітик має можливість обрати, як саме закрити інциденти, а саме вирішити їх як, “Phishing”, “Malware”, “Clean” або “Other”.

Рис. 2.16. Варіанти закриття інцидентів в CIS

Для кожного клієнта CIS надає можливість створити конектори, завдяки яким користувачі можуть бути поділені на групи та для кожного конектора застосовується різна політика, яка застосовується при виявленні фішингових атак. Політика полягає в тому, які дії мають бути виконані при виявленні шкідливих електронних листів системою. Всього існує чотири варіанта:

- Створення інцидента (від цього буде залежати ці з`явиться інцидент в CIS)
- Переміщення електронних листів в конкретну папку (Спам, видаленні листи, інше)
- Додавання червоного банера (Повідомляє, що лист небезпечний, та був
- Додавання інформативного банера (Рекомендовано бути обережнем при відкритті)

Рис. 2.17. Список дій для створення політики в CIS

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ФІШИНГОВІ АТАКИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

3.1 Рекомендації для фахівців кібербезпеки

Загальними рекомендаціями фахівцям з кібербезпеки щодо виявлення фішингових атак в організації будуть наступні.

Застосуйте фільтри електронної пошти. Застосування фільтрів електронної пошти може допомогти виявити фішингові електронні листи та запобігти їх потраплянню в папку "Вхідні" співробітників. Фільтри електронної пошти можна налаштувати для блокування електронних листів із відомих джерел фішингу, підозрілих IP-адрес, а також для позначення електронних листів, які містять підозрілі посилання чи вкладення.

Проводьте регулярне моделювання фішингу. Проведення регулярних симуляцій фішингу може допомогти перевірити обізнаність співробітників і готовність виявляти фішингові атаки та реагувати на них. Ці симуляції можна використовувати для виявлення областей, де працівники потребують додаткового навчання, і для посилення найкращих практик виявлення фішингових атак і звітування про них.

Проводьте аналіз трафіку електронної пошти. Аналіз трафіку електронної пошти може допомогти виявити закономірності та аномалії, які можуть свідчити про фішингову атаку. Це може включати аналіз джерела, призначення та вмісту електронних листів для виявлення підозрілої активності.

Використовуйте аналіз загроз: використання аналізу загроз може допомогти виявити нові загрози фішингу. Це може включати моніторинг галузевих каналів розвідки про загрози, аналіз соціальних мереж на наявність фішингових кампаній і використання інструментів розвідки з відкритим кодом (OSINT) для виявлення фішингових доменів і IP-адрес.

Запроваджувати багатофакторну автентифікації (MFA): впровадження багатофакторної автентифікації може допомогти запобігти фішинговим атакам, які

намагаються викрасти облікові дані для входу. МЗС вимагає від співробітників надавати додаткові фактори автентифікації, такі як код або біометрична автентифікація, на додаток до пароля.

Проводьте регулярні тренінги з питань безпеки. Проведення регулярних тренінгів з питань безпеки може допомогти навчити співробітників найновішим тактикам фішингу та найкращим практикам виявлення фішингових атак і повідомлення про них. Це може включати навчання тому, як ідентифікувати фішингові електронні листи, як повідомляти про підозрілу активність і як ефективно використовувати інструменти безпеки.

Впроваджуючи ці рекомендації, фахівці з кібербезпеки можуть підвищити готовність своєї організації виявляти фішингові атаки та реагувати на них.

3.2Рекомендації для кінцевих користувачів

Для користувачів інформаційної системи основними рекомендаціями щодо протидії фішингових атак можна виділити наступне:

1. Перевірте адресу електронної пошти відправника. Один із найпростіших способів виявити фішинг — це перевірити адресу електронної пошти відправника. У фішингових електронних листах часто використовуються підроблені адреси електронної пошти або дещо інша версія легітимної електронної адреси. Завжди ретельно перевіряйте адресу електронної пошти, перш ніж натискати будь-які посилання чи відкривати вкладення.

2. Шукайте орфографічні та граматичні помилки: фішингові листи часто містять орфографічні та граматичні помилки. Законні організації зазвичай мають команду професіоналів, які перевіряють їхні електронні листи перед їх розсиланням.

3. Не натискайте на посилання: уникайте натискань на посилання в електронних листах, особливо якщо електронний лист надійшов з невідомого або підозрілого джерела. Натомість наведіть вказівник миші на посилання, щоб

перевірити, чи URL-адреса відповідає законному веб-сайту організації. Якщо він не збігається або виглядає підозріло, не натискайте його.

4. Перевірте запит: якщо в електронному листі запитується особиста інформація, облікові дані для входу або будь-яка інша конфіденційна інформація, завжди перевіряйте запит, зв’язавшись безпосередньо з організацією за допомогою відомого та надійного методу.

5. Використовуйте засоби захисту від фішингу: багато служб електронної пошти та веб-браузерів мають засоби захисту від фішингу, які можуть допомогти виявити та запобігти фішинговим атакам. Завжди вмикайте ці інструменти та оновлюйте їх.

6. Будьте в курсі: будьте в курсі останніх фішингових шахрайств і тактик, які використовують зловмисники. Регулярно читайте блоги з питань безпеки та новинні статті, щоб бути в курсі останніх загроз і способів захисту.

Головне, що повинні пам’ятати користувачі корпоративної інформаційної системи це те, що фішингові атаки можуть бути дуже переконливими, тому важливо бути обережним і пильним, отримуючи електронні листи, особливо ті, які просять надати особисту інформацію або містять підозрілі посилання чи вкладення.

ВИСНОВКИ

Дана бакалаврська робота присвячена дослідженню вирішення завдання щодо виявлення та протидії фішинговим атакам в корпоративній інформаційній системі організації.

Основні результати роботи полягають у наступному:

В результаті аналізу виявлено проблему щодо фішингових атак що може призвести до витоку конфіденційної інормації. Найбільш розповсюдженою фішинговою атакою є атака через електронну пошту.

В роботі розглянуто багаторівневий підхід для захисту від фішингу. Такий підхід дозволяє впровадити заходи щодо виявлення та реагування на фішингові атаки. Реалізація такого підходу дозволить пом’якшити рівень впливу на корпоративну інформаційну систему організації за рахунок ускладнення доступу до користувачів, допоможе повідомляти користувачам про ймовірну атаку фахівців, швидко реагувати на атаку.

Досліджено архітектуру та функціональні можливості рішення Cyren Inbox Security, яке встановлює безперервний, адаптивний і автоматизований рівень захисту прав в поштовій скриньці користувача, де це найбільше необхідно.

В результаті роботи сформульовано рекомендації користувачам та фахівціям з кібербезпеки щодо виявлення та реагування фішинговим атакам.

ПЕРЕЛІК ПОСИЛАНЬ

1. Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions. [Електронний ресурс] – Режим доступу: https://arxiv.org/ftp/arxiv/papers/1705/1705.09819.pdf

2. Phishing – A Growing Threat to E-Commerce. [Електронний ресурс] – Режим доступу: https://arxiv.org/ftp/arxiv/papers/1112/1112.5732.pdf

3. Phishing Activity Trends Report, 4th Quarter 2020. [Електронний ресурс] – Режим доступу: https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf

4. Email: Click with Caution How to protect against phishing, fraud, and other scams. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

5. State of the Phish: At a Glance. [Електронний ресурс] – Режим доступу: https://www.proofpoint.com/sites/default/files/infographics/pfpt-us-sotp-infographic.pdf

6. Best Practices for Protecting Against Phishing, Ransomware and Email Fraud. [Електронний ресурс] – Режим доступу: https://assets.barracuda.com/assets/docs/dms/Osterman_Research_Best_Practices_for_Protecting_Against_Phishing,_Ransomware_and_Email_Fraud_(American_English).pdf

7. Analysis of Phishing Attacks and Countermeasures. [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/235947501_Analysis_of_Phishing_Attacks_and_Countermeasures

8. 2020 PHISHING AND FRAUD REPORT Phishing During A Pandemic. [Електронний ресурс] – Режим доступу: https://www.f5.com/content/dam/f5-labs-v2/article/articles/threats/22--2020-oct-dec/20201110_2020_phishing_report/F5Labs-2020-Phishing-and-Fraud-Report.pdf

9. Tutorial and Critical Analysis of Phishing Websites Methods. [Електронний ресурс] – Режим доступу: https://core.ac.uk/download/pdf/206070797.pdf

10. Phishing: An Analysis of a Growing Problem. [Електронний ресурс] – Режим доступу: https://www.sans.org/reading-room/whitepapers/threats/phishing-analysis-growing-problem-1417

11. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. [Електронний ресурс] – Режим доступу: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

12. Phishing Landscape 2020 A Study of the Scope and Distribution of Phishing. [Електронний ресурс] – Режим доступу: http://www.interisle.net/PhishingLandscape2020.pdf

13. Exploiting common URL redirection methods to create effective phishing attacks. [Електронний ресурс] – Режим доступу: https://www.helpnetsecurity.com/2021/05/10/exploiting-url-redirection-methods/

14. Phishing through the prism of graphic design. [Електронний ресурс] – Режим доступу: https://www.cyren.com/blog/articles/phishing-through-the-prism-of-graphic-design

15. Cyren Inbox Security. [Електронний ресурс] – Режим доступу: https://www.cyren.com/tl_files/downloads/Cyren_Datasheet_InboxSecurity_200421_v1.4.1.pdf

16. An Essential Phishing Protection Solution For Every Office 365 Mailbox. [Електронний ресурс] – Режим доступу: https://www.cyren.com/products/cyren-inbox-security

17. Cyren Incident Response Service (CIRS). [Електронний ресурс] – Режим доступу: https://www.cyren.com/files/downloads/Cyren_Datasheet_CIRS_200805_v6.1.pdf

18. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. [Електронний ресурс] – Режим доступу: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)