ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ЕЛЕКТРОННИХ ПОШТ ПРАЦІВНИКІВ ОРГАНІЗАЦІЇ ЗА ДОПОМОГОЮ CYREN INBOX SECURITY»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Кравчук В.В.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

РЕФЕРАТ

Текстова частина магістерської роботи: 58 сторінки, 29 рисунків, 15 джерел.

Об'єкт дослідження – процес захисту корпоративної електронної пошти організації.

Предмет дослідження – технологія захисту корпоративної електронної пошти організації від можливих загроз.

Мета роботи – розробити рекомендації щодо забезпечення захисту електронної пошти на основі обраного продукту.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, розробка рекомендацій щодо захисту корпоративної електронної пошти.

В роботі проведено аналіз проблеми захисту корпоративної електронної пошти співробітників організації, визначені мета та завдання захисту електронної пошти. Проаналізовано можливі загрози для організації та засоби захисту від них.

Досліджені методи та засоби забезпечення захисту на прикладі продукту Cyren Inbox Security. Визначені призначення, основні функції та склад продукту Cyren Inbox Security. Розглянуто процес розслідування інцидентів та роботу у Cyren Inbox Security.

На основі отриманих результатів дослідження, розроблені рекомендації щодо забезпечення захисту корпоративної електронної пошти організації.

Галузь використання – кібербезпека корпоративної інформаційної системи.

КОРПОРАТИВНА ЕЛЕКТРОННА ПОШТА, КІБЕРБЕЗПЕКА, ЗАХИСТ КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ЕЛЕКТРОННОЇ ПОШТИ, CYREN INBOX SECURITY

ABSTRACT

Master’s thesis: 58 pages, 29 figures, 15 sources.

Object of research – the process of protecting the organization's corporate e-mail.

Subject of research – methods and means of protecting the organization's corporate e-mail from possible threats.

The aim of research – to develop recommendations for ensuring the protection of e-mail based on the selected product.

Research methods – study of the literature on this topic, analysis of operating documentation, development of recommendations for corporate e-mail protection.

The paper analyzes the problem of protecting the corporate e-mail of the organization's employees, defines the purpose and tasks of e-mail protection. Possible threats to the organization and means of protection against them are analyzed.

Researched methods and means of protection using the Cyren Inbox Security product as an example. The purposes, main functions and composition of the Cyren Inbox Security product are defined. The incident investigation process and operation at Cyren Inbox Security are reviewed.

Based on the research results, recommendations were developed to ensure the protection of the organization's corporate e-mail.

Field of use – cyber security of the corporate information system.

CORPORATE EMAIL, CYBER SECURITY, PROTECTION OF ORGANIZATION USERS, METHODS, AND MEANS OF EMAIL PROTECTION, CYREN INBOX SECURITY

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – програмне забезпечення

CIS – Cyren Inbox Security

КІС – корпоративна інформаційна система

ОС – операційна система

ПК – персональний комп’ютер

BEC – Business Email Compromise

ВСТУП

Актуальність дослідження. Уявити сучасний світ без електронної пошти вже неможливо. Більшість організацій використовують даний спосіб комунікації як основний. Сам процес спілкування відбувається шляхом пересилання текстових та інших файлів, подібно до того, як при звичайному поштовому листуванні люди обмінюються листами, листівками та іншою кореспонденцією. Через електронну пошту працівники компаній можуть надіслати та отримати потрібну робочу інформацію за лічені секунди. Оскільки часто через кожну поштову скриньку співробітника проходить певний об'єм конфіденційної інформації, яка стосується як компанії, так і, безпосередньо, користувачів, електронна пошта стає однією з цілей атак зловмисників. Атаки на даний спосіб комунікації реалізується з метою отримання даних про компанію, клієнтів, співробітників, а також отримання доступу до облікових записів.

Вищенаведені аргументи актуалізують тему даної магістерської роботи, зміст якої становлять дослідження щодо технології захисту корпоративних електронних пошт на основі продукту Cyren Inbox Security.

Об'єкт дослідження – процес захисту корпоративної електронної пошти організації.

Предмет дослідження – технологія захисту корпоративної електронної пошти організації.

Мета роботи – розробити рекомендації щодо захисту корпоративної електронної пошти на основі використання технологій Cyren Inbox Security.

Наукові завдання:

дослідити сутність проблеми забезпечення захисту корпоративної електронної пошти організації;

встановити сутність завдань захисту корпоративної електронної пошти організації;

визначити засоби та методи захисту корпоративної електронної пошти організації;

проаналізувати основні функції та принципи реалізації захисту корпоративної електронної пошти організації;

розробити рекомендації щодо захисту корпоративної електронної пошти організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, розробка рекомендацій щодо захисту корпоративної електронної пошти організації.

Практичне значення одержаних результатів полягає в розробці рекомендацій, щодо розслідування інцидентів у Cyren Inbox Security, а також у розробці рекомендацій щодо застосування даного продукту в межах організації.

Апробація результатів. Основні наукові результати роботи доповідалися та обговорювалися на Всеукраїнській науково-технічній конференції «Актуальні проблеми кібербезпеки», Навчально-науковий інститут захисту інформації, 27 жовтня 2022 р.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ КОРПОРАТИВНИХ ЕЛЕКТРОННИХ ПОШТ ПРАЦІВНИКІВ ОРГАНІЗАЦІЇ

1.1. Проблема захисту корпоративної електронної пошти працівників

Інтернет - останнє та найважливіше з досягнень XX століття, яке змінило світ і відбилося життя кожної людини. Він увібрав у себе всі досягнення людства як в інформаційній сфері, так і в комунікаційній галузі. Серед базових користувачів особливе місце займає електронна пошта, завдяки якій будь-хто за лічені хвилини може переслати повідомлення, що містить як текстові, так і звукові, графічні, програмні файли. Електронною поштою можна отримувати найсвіжіші світові новини, читати повідомлення в телеконференціях, здійснювати бізнес-угоди, обмін даними.[1]

Електронна пошта багато в чому схожа на звичайну пошту, коли лист - текст, з стандартним заголовком (конвертом) доставляється за вказаною адресою, яка визначає місцезнаходження машини та ім'я адресата, і поміщається у файл, званий поштовою скринькою, для того, щоб адресат міг його дістати і прочитати у зручний час .

Для кожного користувача виділяється область пам'яті - електронна поштова скринька, доступ до якої здійснюється за адресою, що повідомляється, та паролем, який користувач створює сам, даний пароль буде відомий тільки йому. Ставши абонентом комп'ютерної мережі та отримавши свою електронну адресу, користувач може використовувати для комунікації як в житті, так і в робочих цілях.

Електронна пошта (E-mail) – одна з перших служб Інтернету. За минулі роки вона не втратила популярності і залишається потрібною для великого відсотку користувачів мережі. Адреса електронної пошти стала для сучасного суспільства настільки ж обов'язковою, як домашня адреса та номер телефону, яка

використовується і для комунікації між як працівниками більшості компаній, так і в звичайному повсякденному житті. Основне призначення електронної пошти – дати користувачам можливість обміну даними та інформацією, а важливою перевагою є те, що віддаленість адресата практично не відіграє жодної ролі з точки зору не тільки швидкості доставки. Процес відбувається шляхом пересилання текстових та інших файлів, подібно до того, як при звичайному поштовому листуванні люди обмінюються листами, листівками та іншою кореспонденцією. Даний засіб зв'язку закрепився на робочих місцях багатьох організацій для обміну інформацією, що стосується тих чи інших процесів роботи. Вражаюча швидкість такого обміну з іншими країнами електронною поштою відсунули на другий план переговори по телефону та поштові послуги для надсилання документації. Через кожну поштову скриньку працівників організацій проходить немала кількість персональної та конфіденційної інформації, яка стосується не тільки самих людей, а й безпосередньо підприємств. Витік або втрата такої інформації може призвести до неприємних наслідків, як втрата клієнтів, проектів, програш тендерів, втрата репутації на ринку, тощо. Тому захист електронної пошти працівників є одним з важливих моментів з забезпечення безпеки інформації на підприємстві. [2]

Щодня пересилається понад 333 мільярди електронних листів по всьому світу, а працівники в середньому отримують 120 електронних листів на день. Цим користуються кіберзлочинці, які за допомогою атак на корпоративну електронну пошту, використовуючи шкідливе програмне забезпечення, фішингові кампанії, рекламні розсилки та багато інших методів, викрадають цінну конфіденційну інформацію. Більшість кібератак починаються з попередньо створеного зловмисного електронного листа. Згідно з даними, що надає Центр розгляду скарг на шахрайство в Інтернеті ФБР (IC3), у 2020 році збитки від кіберзлочинності через електронні пошти становили понад 4,1 млрд доларів США, а найбільшої шкоди завдали порушення безпеки корпоративних електронних скриньок.[3]

Електронна пошта була розроблена, щоб бути максимально відкритою та доступною. Але саме через свою доступність, безпека електронної пошти сама по собі не є надійною. Це дозволяє зловмисникам використовувати електронну пошту як спосіб створення проблем у спробі отримати прибуток. За допомогою, наприклад, спам-кампаній або ж компрометації бізнес-електронної пошти (BEC) зловмисники намагаються скористатися відсутністю безпеки електронної пошти для виконання своїх дій. Оскільки більшість організацій покладаються на електронну пошту для ведення бізнесу, зловмисники використовують саме її, намагаючись викрасти потрібну інформацію. Оскільки електронна пошта є відкритим форматом, її може переглядати кожен, хто може її перехопити, що викликає занепокоєння щодо безпеки. Це стало проблемою, оскільки організації почали надсилати конфіденційну інформацію саме через даний формат комунікації. Зловмисник може легко прочитати вміст електронного листа, перехопивши його. Більшість організацій встановили політику щодо того, як керувати цим потоком інформації. Одна з перших політик, яку встановлює більшість організацій, стосується перегляду вмісту електронних листів, що проходять через їхні сервери електронної пошти. Важливо розуміти, що міститься в електронному листі, щоб діяти належним чином. Після того, як базові політики набудуть чинності, організація може запровадити різні політики безпеки для цих електронних листів. Такі політики можуть бути простими, як видалення всього виконуваного вмісту з електронних листів до більш глибоких дій, як, наприклад, надсилання підозрілого вмісту в інструмент ізольованого програмного середовища для детального аналізу. Якщо ці політики виявляють інциденти безпеки електронної пошти, організація повинна мати дієву інформацію про масштаб атаки. Це допоможе визначити, яку шкоду могла б завдати атака. Щойно організація має доступ до всіх електронних листів, які надсилаються, вона може застосувати політику шифрування електронної пошти, щоб запобігти потраплянню конфіденційної інформації електронної пошти в чужі руки. Зазвичай підприємства обирають послуги безпеки

споживчого рівня, які не пропонують необхідного захисту. Статистика кібербезпеки показує, що бізнес є прибутковою мішенню для кіберзлочинців.[4]

Рис.1.1. Статистика за жовтень 2022 року від Esimplicity Technologies

Навіть на невеликі підприємства та бізнеси припадає 13 відсотків ринку кібербезпеки, і це число швидко зростає. Все через те, що кіберзлочинці знають, що на крадіжках у менших компаній можна заробити більше грошей, ніж у великих, які мають більше ресурсів і персоналу, присвяченого кібербезпеці.

Кіберзлочинність – це величезний бізнес. Згідно з даними ФБР, майже половина всіх кіберзлочинів відбувається не тільки на великі корпорації. Причина цього проста: малі фірми надто обережні щодо безпеки електронної пошти. Зазвичай вони обирають послуги безпеки споживчого рівня. Це означає, що захист електронної пошти недостатньо надійний, щоб захистити їх від хакерів і атак з використання шкідливого програмного забезпечення. Загрози для організацій і окремих осіб, які надсилаються електронною поштою, продовжують ставати все більш витонченими, оскільки спамери впроваджують нові тактики для уникнення систем фільтрації спаму та вірусів. [5]

Безпеку електронної пошти можна визначити як використання різних методів для захисту конфіденційної інформації в електронному листуванні та облікових записах

від несанкціонованого доступу, втрати або компрометації. Простіше кажучи, безпека електронної пошти дозволяє організації захистити загальний доступ до однієї чи кількох адрес електронної пошти чи облікових записів. Забезпечення безпеки комунікації через електронну пошту може здійснюватися з використання різних методів захисту конфіденційної інформації в електронному листуванні та облікових записах.

Такі запобіжні заходи вживаються головним чином проти несанкціонованого доступу, втрати або ж компрометації. Це дозволяє окремій особі чи організації захистити загальний доступ до однієї чи кількох адрес електронної пошти. Безпека електронної пошти захищає вміст облікового запису, який зазвичай служить популярним засобом розповсюдження зловмисного програмного забезпечення, спаму та фішингових атак. Зазвичай це робиться за допомогою оманливих повідомлень, щоб спонукати одержувачів оприлюднити конфіденційну інформацію, відкрити вкладені файли або натиснути гіперпосилання, які встановлюють шкідливе програмне забезпечення на пристрої жертви. Зупинка атак у точці входу. Електронна пошта також є загальною точкою входу для зловмисників, які прагнуть закріпитися в корпоративній мережі та зламати цінні бізнес-дані. Отже, безпека електронної пошти необхідна як для індивідуальних, так і для корпоративних облікових записів електронної пошти, і існує кілька заходів, які організації повинні вжити для посилення безпеки електронної пошти. Постачальник послуг забезпечує безпеку електронної пошти, використовуючи надійні паролі та механізми контролю доступу на сервері електронної пошти. Тут повідомлення електронної пошти шифруються та підписуються цифровим підписом, коли вони розміщуються у папці «Вхідні» або передаються на/або з електронної адреси абонента. Також використовує брандмауер і програми фільтрації спаму на основі програмного забезпечення, щоб обмежити доставку небажаних, ненадійних і шкідливих повідомлень електронної пошти до папки "Вхідні" користувача.

Проблема забезпечення безпеки електронної пошти є важливою через такі вірогідні причини:

- Електронна пошта є звичайною мішенню для кіберзлочинців. Перше, що отримують співробітники, як тільки вони приєднуються до будь-якої фірми, це офіційний обліковий запис електронної пошти. Співробітники використовують свої відповідні ідентифікатори для доступу до інформації компанії та щоденного спілкування з колегами. Кожен офіційний зв'язок з компанією використовує електронну пошту як засіб передачі даних. Тому, коли співробітники працюють віддалено, як це спостерігається в ситуації з пандемією COVID-19, вони, як правило, використовують свою офіційну електронну пошту майже для всього спілкування. Такі комунікації є вразливими, і співробітники ризикують піддатися атакам з боку кіберзлочинців. Кіберзлочинці часто використовують фішинг, приманки, соціальну інженерію та багато інших типів атак, щоб використовувати тріщини в системі безпеки.

- Невеликий пробіл може вплинути на всю організацію. Діра в безпеці електронної пошти може дозволити зловмисному або шпигунському програмному забезпеченню проникнути в усю комунікаційну мережу, сіючи хаос у всій організації. Ситуація погіршується, коли мережу організації вражає смертельне програмне забезпечення-вимагач. Навіть досвідчені професіонали та досвідчені співробітники стають жертвами такої тактики. Ці кіберзлодії також можуть викристати отриману конфіденційну інформацію, виносячи її у відкритий доступ або продаючи учасникам торгів у разі особистої помсти.

- Вирішальне значення для організацій для захисту конфіденційної інформації. Більшість інформації компанії може включати дуже конфіденційну інформацію, яка може бути використана проти організації або в злочинних цілях. Кіберзлочинці також можуть націлюватися на повсякденне спілкування та змінювати повідомлення, що може призвести до неправильного розуміння та змусити спілкуватися.[6]

-

1.2. Аналіз загроз та атак, які реалізуються через електронну пошту

Електронна пошта залишається інструментом номер один для ділового спілкування. Мережа електронної пошти відкрита практично для будь-кого, а її гнучкість, надійність і зручність означають, що вона не скоро зникне. Але попри всі свої переваги, електронна пошта також може стати джерелом серйозних кібератак. Атаки соціальної інженерії, такі як фішинг, можуть призвести до витоку даних, атак зловмисного програмного забезпечення та мільярдних збитків для компаній у всьому світі. Далі проаналізуємо найпоширеніші атаки, які здійснюються злочинцями для отримання певної інформації підприємств.

– *Фішинг*

Це різновид кіберзлочинності, за якої кіберзлочинці надсилають спам-повідомлення зі зловмисними посиланнями, призначені для того, щоб цільовий користувач завантажив зловмисне програмне забезпечення або перейшов за посиланнями на підроблені веб-сайти. Фішинг залишається найпоширенішою формою кіберзлочинності. З британських компаній, які зазнали кібератак у 2022 році, 83% вважають, що атака була фішинговою. Згідно зі статистикою від AAG IT, у 2021 році 323 972 інтернет-користувачі в усьому світі стали жертвами саме фішингових атак. Це означає, що половина користувачів, які стали жертвами кіберзлочинності, стали жертвами фішингових атак. Це незважаючи на те, що заходи кібербезпеки Google блокують 99,9% спроб фішингу від користувачів. Із середньою втратою 136 доларів США за фішингову атаку це становить 44,2 мільйона доларів, викрадених кіберзлочинцями через фішингові атаки у 2021 році.[6]

Фішингові атаки здебільшого націлені на жертви через електронні листи. У 2021 році в середньому на 100 користувачів Інтернету припадало 16,5 витоку електронних листів. Ці зламані бази даних продаються на чорних ринках темної мережі, тобто кіберзлочинці можуть придбати їх і використовувати адреси для фішингових атак.

У 2021 році було виявлено майже 1 мільярд електронних листів, що вплинуло на 1 з 5 користувачів Інтернету. Це може частково пояснити постійну поширеність фішингових атак. Для компаній як ніколи важливо серйозно ставитися до кібербезпеки. Особливо в жорстко регульованих галузях, таких як юридичний сектор.

Дослідження 2019 року підкреслило, що фішинг був найпопулярнішим способом атаки для кіберзлочинців. Ці фішингові кампанії використовували 65% усіх відомих груп. Основним мотивом цих атак був переважно збір розвідданих, 96% груп використовували цілеспрямовані атаки з цієї причини.

У 2022 році найпоширеніша URL-адреса, включена у фішингові листи, посилається на веб-сайти з доменом «.com» — 54%. Наступним за поширеністю доменом є «.net» з менш ніж 8,9%. Найпоширеніші доменні імена з «.com» у другому кварталі 2022 року: Adobe, Google, Myportfolio, Backblazeb2, Weebly.[7]

Фішинговий електронний лист спрямований для використання соціальної інженерії для використання співробітників вашої організації. Якщо зловмисник може змусити користувача натиснути на шкідливе посилання або відкрити заражене вкладення, він може викрасти облікові дані та інші особисті дані або встановити зловмисне програмне забезпечення на комп’ютері співробітника. Звідти кіберзлочинець може розширити свій доступ до корпоративної мережі, щоб викрасти конфіденційні дані або здійснити інші атаки. Понад 90% кібератак починаються з фішингового електронного листа, адже це найлегший спосіб доставити потрібне посилання до жертви. Часто набагато легше переконати співробітника, що йому потрібно вжити заходів щодо свого облікового запису Netflix або надіслати платіж постачальнику, ніж виявити та використати вразливість у системах компанії.

Щодня Google блокує близько 100 мільйонів фішингових листів. Наведена нижче статистика, доказує, що при організації даного вище атак, злочинці маскують створені фішингові сайти під офіційні та найпопулярніші.

У першому кварталі 2022 року LinkedIn був найбільш імітованим брендом у спробах фішингу в усьому світі. У першому кварталі 2022 року топ-5 найбільш

імітованих брендів: LinkedIn (52%), DHL (14%), Google (7%), Microsoft (6%), FedEx (6%). [7]

Найпоширенішими посиланнями на зловмисне програмне забезпечення, знайденими у фішингових електронних листах у 2021 році, були трояни із сімейства «Agensla». Вони викрадають облікові дані для входу, що зберігаються в браузерах, і облікові дані з електронних листів.

Фішинг вважається найбільш руйнівною формою кіберзлочинності для британського бізнесу в 2022 році, пов'язаної з загрозливими суб'єктами, які видають себе за цю організацію в Інтернеті. Користувачі Інтернету покоління Z (18-40 років) найчастіше стають жертвами фішингових атак – 23% порівняно з 19% користувачів Інтернету покоління X (41-55 років).

90% фішингових атак, які надсилаються через програми обміну повідомленнями, надсилаються через WhatsApp. Наступним найвищим відсотком є Telegram з 5,04%.

У 2021 році середній показник кліків для фішингової кампанії становив 17,8%. Фішингові кампанії, які були більш цілеспрямованими та додавали телефонні дзвінки, мали середній коефіцієнт кліків 53.2% – в 3 рази ефективніше.

Під час сканування безпеки мільйонів електронних листів було виявлено, що ті, які містили загрози безпеці: 12% доставляли шкідливі програми, 6% були зламаними діловими електронними листами або шахрайством з генеральним директором.

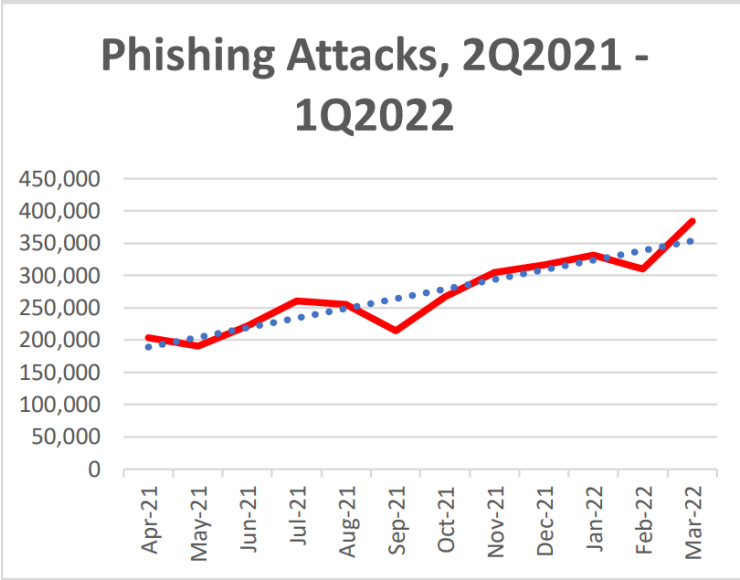


Рис.1.2. Статистика росту кількості фішингових атак 2021-2022 років

З облікових даних фішингових електронних листів 45% нібито надійшли від Microsoft, ще 17% були присвячені фінансам, 9,3% повідомлень були шкідливими. З цих 9,3%, 38% мали лише URL-адресу, а 36% мали додаток.[8]

Фішинг був найпопулярнішим видом зараження в азіатських організаціях у 2021 році, з 43% атак на континенті. Це пов'язано з використанням вразливості та випереджає атаки грубою силою (7%) і використання вкрадених облікових даних (7%).

Фішинг також був поширеним у європейських організаціях до 2021 року з 42% атак. Це трохи менше, ніж використання вразливості (46%) і випереджає атаки грубою силою (12%). У Північній Америці фішинг використовувався в 47% атак на організації в 2021 році, більше, ніж використання вразливостей (29%) і груба сила (9%).

У першому кварталі 2022 року член-засновник APWG OpSecSecurity виявив, що фішингові атаки на фінансовий сектор, до якого входять банки, залишаються найбільшим набором атак, на які припадає 23,6 відсотка всіх фішингових атак(Рис.1.3.).

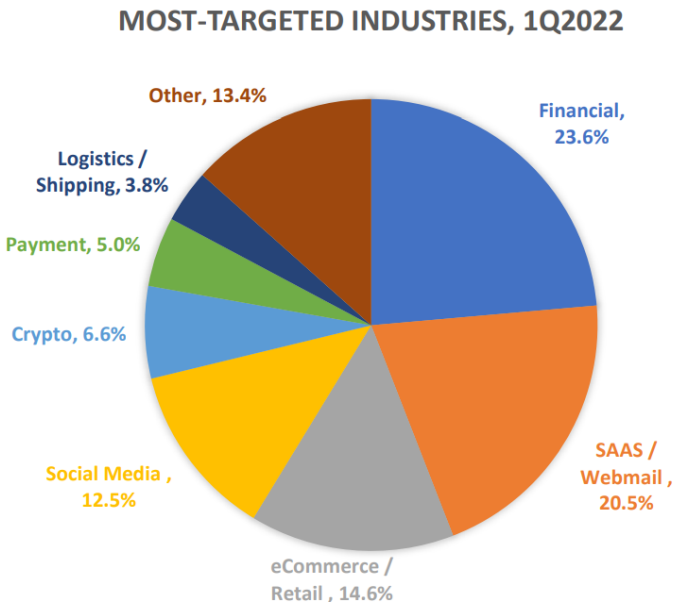


Рис.1.3. Найбільш постраждалі індустрії

Атаки на веб-пошту та постачальників програмного забезпечення як послуги (SAAS) залишаються поширеними, а атаки на сайти роздрібної торгівлі/електронної комерції впали з 17,3 до 14,6 відсотка після сезону святкових покупок. Фішинг проти наборів соціальних мереж зріс з 8,5 відсотка всіх атак у 4 кварталі 2021 року до 12,5 відсотка в 1 кварталі 2022 року. Фішинг проти об'єктів криптовалюти, таких як криптовалютні біржі та постачальники гаманців, залишався стабільним з кінця 2021 року, підвищившись з 6,5 до 6,6 відсотка в останньому кварталі.

– *Spear phishing(цільовий фішинг)*

Це атака електронною поштою, націлена на конкретну особу. Отже, у той час як для масового фішингу використовується мережа — надсилання електронних листів якомога більшій кількості потенційних жертв — прямий фішинг, щоб націлитися на одну конкретну жертву. Злочинці вже зібрали деякі особисті дані особи, такі як її ім'я, назва компанії, посада, адреса електронної пошти тощо. Вони націлені на жертв, які розміщують особисту інформацію в Інтернеті. Вони можуть переглядати окремі профілі під час сканування платформи соціальних мереж. У профілі вони зможуть

знайти місцезнаходження людини, оточення в околицях, список друзів, адресу електронної пошти та будь-які публікації про нещодавно придбані продукти.[10]

Маючи особисті дані під рукою, кіберзлочинець може звернутися до людини на ім'я та попросити її відкрити додаток, у листі, де може бути фішингове посилання, шкідливе програмне забезпечення, або натиснути посилання, яке переведе на підроблений веб-сайт, де його просять надати імена користувачів, паролі, номери банківських рахунків, коди сортування, PIN-коди тощо.

– *Business Email Compromise (BEC) та CEO fraud.*

Знову ж таки, фішинг також може бути загальним терміном, оскільки існує багато різних типів фішингових атак. Деякі з наведених нижче прикладів, зокрема компрометація бізнес-електронної пошти (BEC) і шахрайство з генеральним директором, майже завжди є фішинговими атаками. В даному випадку злочинець видає себе за людину, що займає керівничу посаду у компанії жертви або ж просто рядового співробітника. Через такі листи, злочинець може отримати будь-яку конфіденційну інформацію як про компанію так і про співробітників, це можуть бути банківські дані, дані про процес роботи, про нові проекти, тощо. Нижче приведено декілька прикладів листів, з типом атаки BEC та CEO fraud (рис.1.4., рис.1.5).

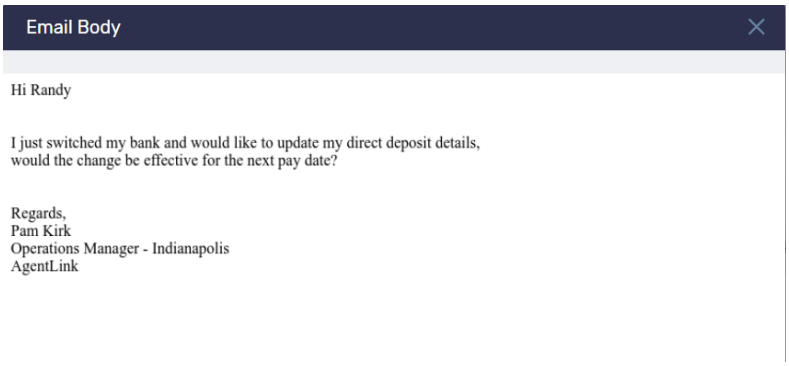


Рис.1.4. Приклад BEC, запрос на зміну банківських даних

В першому випадку(рис.1.4) зловмисник просить змінити банківські дані, щоб отримати виплату. Якщо ортимувач відповідає на даний лист, відправник надсилає

потрібні дані і таким чином отримує виплату вже на свій рахунок, видаючи себе за співробітника компанії.

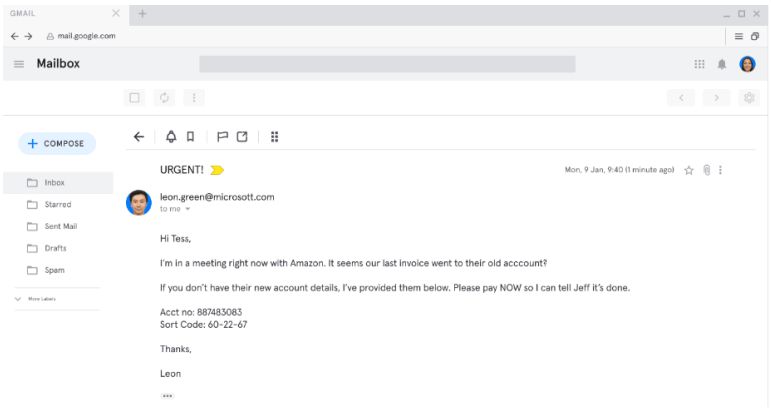


Рис.1.5. Приклад CEO fraud

На другому варіанті(рис.1.5), зловмисник просить провести оплату вже від лиця керівника та просить зробити це як можна швидше. Найчастіше при атаці BEC, зловмисник просить зробити ті ці інші дії, наголошуючи, що виконати все потрібно у найближчий час. Таким чином, шахраї сподіваються на людський фактор, коли працівник бачить наказ від керівника з умовою швидкої реакції, він може не встигнути зрозуміти через яку саме пошту був надісланий лист і просто виконати всі вказані завдання.

– *Спам/Скам.*

Даний тип атаки розуміється, як організоване та несанкціоноване використання програми для надсилання тисяч повідомлень її користувачам. Ці повідомлення надсилаються фальшивими або зламаними профілями та часто містять нереальну рекламу та посилання, на які справжні користувачі просять натиснути. Спамери використовують багато форм зв’язку для масової розсилки своїх небажаних повідомлень. Деякі з них є маркетинговими повідомленнями про продаж небажаних товарів. Інші типи спаму можуть поширювати зловмисне програмне забезпечення, обманом змусити вас розкрити особисту інформацію або налякати, щоб ви подумали, що вам потрібно заплатити, щоб уникнути проблем.[9]

Спам-фільтри електронної пошти вловлюють багато таких типів повідомлень, а оператори телефонного зв’язку часто попереджають вас про «ризик спаму» від невідомих абонентів. Нижче наведено кілька типів спаму, на які варто звернути увагу.

Фішингові електронні листи. Через спам злочинці також можуть надсилати фішингові посилання, з ціллю отрмання, наприклад, даних від обікового запису.

Адам Куджава, директор Malwarebytes Labs, каже про фішингові електронні листи: «Фішинг — це найпростіший вид кібератаки, який водночас є найнебезпечнішим і найефективнішим. Це тому, що він атакує найбільш вразливий і потужний комп’ютер на планеті: людський розум».[10]

Підробка електронної пошти. В даному випадку злочинець підроблює справжню адресу, тобто лист буде виглядати як від законного відправника, де користувача будуть просити вжити певних дій. Добре виконані підробки містять знайомий бренд і вміст, часто від великої відомої компанії, такої як PayPal або Apple. Поширені спам-повідомлення електронної пошти:

- Вимога про оплату неоплаченого рахунку.
- Запит на скидання пароля або підтвердження облікового запису.
- Перевірка покупок, які ви не робили.
- Запит на оновлену платіжну інформацію.
- Шахрайство служби технічної підтримки.

У шахрайстві технічної підтримки спам-повідомлення вказує на те, що у вас є технічна проблема, і вам слід зв’язатися зі службою технічної підтримки, зателефонувавши за номером телефону або натиснувши посилання в повідомленні. Подібно до спуфінгу електронної пошти, ці типи спаму часто повідомляють, що вони надходять від великої технологічної компанії, такої як Microsoft.

Гарячі теми в новинах можна використовувати в спам-повідомленнях, щоб привернути увагу. У 2020 році, коли світ зіткнувся з пандемією Covid-19 і спостерігалося збільшення кількості робочих місць з дому, деякі шахраї розсилали

спам-повідомлення, обіцяючи віддалену роботу з оплатою в біткойнах. У тому ж році ще одна популярна тема спаму була пов’язана з пропозицією фінансової допомоги малому бізнесу, але шахраї зрештою попросили надати реквізити банківського рахунку.

Шахрайство з попередньою оплатою, які іноді називають електронними листами «нігерійського принца», оскільки він був передбачуваним відправником повідомлень протягом багатьох років, обіцяє фінансову винагороду, якщо ви спочатку наддасте грошовий аванс. Відправник зазвичай вказує, що цей готівковий аванс є певною комісією за обробку або заставою для розблокування більшої суми, але після оплати вони зникають. Щоб зробити це більш особистим, подібний тип шахрайства полягає в тому, що відправник видає себе за члена сім’ї, який потрапив у біду та потребує грошей.

Скорочення від «спам зловмисного програмного забезпечення» або «зловмисний спам», malspam – це спам-повідомлення, яке доставляє зловмисне програмне забезпечення на пристрій. Нічого не підозрюючи читачі, які натискають посилання або відкривають вкладення електронної пошти, отримують певний тип такого ПЗ, включаючи програми-вимагачі, трояни, боти, криптомайнери, шпигунські програми та кейлоггери. Звичайним способом доставки є включення шкідливих сценаріїв у вкладення знайомого типу, таких як документ Word, PDF-файл або презентація PowerPoint. Після відкриття додатку, на машині запускаються сценарії та отримують завантаження зловмисного ПЗ. [9]

На рисунку нижче(рис.1.6), наведений приклад сторінки з фішингом, коли зловмисник надсилає посилання на PDF-файл, який знаходиться на тому чи іншому ресурсі. Отримувач переходить по посиланню на файл, після натискає «відкрити» чи «передивитись», і після автоматично переходить на сторінку, де для отримання доступу до інформації потрібно ввести свої дані облікового запису у Microsoft.

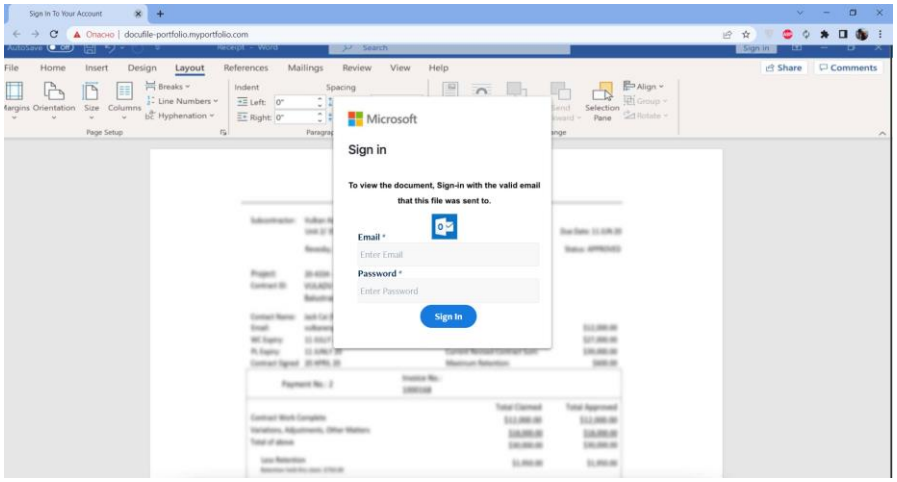


Рис.1.6. Приклад сторінки з фішингом

В даному випадку, користувач вводить свої дані, але доступ до файлу не отримає, а буде автоматично переведений або ж на свою поштову скриньку, або ж на сайт Microsoft, також можливо при введені буде повідомлення про не вірність даних, а після декількох спроб, користувач все одно не отримає доступ, але тим часом пароль від облікового запису вже буде у зловмисника.

За статистикою наведеною нижче(рис.1.7), за останній рік найбільше спам листів було надіслано з типом реклами та пропонуванням послуг, а також дорослого контенту. На другому місці йдуть листи з фінансовими шахрайствами, а найменше було надіслано скаму.

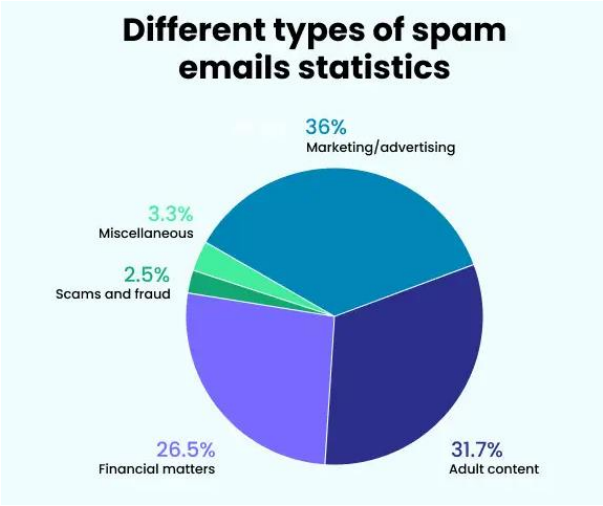


Рис.1.7. Типи спаму, які були надіслані за останній рік, у %

1.3. Аналіз можливих способів захисту електронної пошти

На даний час проблема захисту електронної корпоративної пошти працівника компанії, є дуже важливою, адже перераховані вище загрози, можуть вплинути на репутацію та роботу цілою компанії загалом. Тому для того, щоб попередити витік інформації та забезпечити захист користувачів від фішингу, зловмисного ПЗ чи ВЕС, керівники підприємств мають забезпечити використання того чи іншого програмного забезпечення або ж звернутись до компаній які надають послуги з захисту електронної пошти користувачів. В другому випадку, компанії з захисту мають доступ до поштової скриньки, сканують та перевіряють листи, що надходять, на наявність однієї з розглянутих загроз.

Безпека електронних листів залежить не тільки від складності та унікальності пароля до облікового запису. Треба також не забувати про забезпечення захисту вмісту повідомлення під час передачі. Листи можуть легко опинитися під контролем зловмисників, тому існують додаткові рівні захисту вмісту та процесу відправки повідомлень. Одним з найпопулярніших способів є шифрування листів на транспортному рівні, що забезпечує безпеку повідомлення при передачі. Такий метод дуже схожий на просте вкладення листа в конверт, в даному випадку є можливість побачити звідки та куди направляється повідомлення, проте його зміст буде доступний тільки після відкриття так званого «конверта», тобто отриманого листа. Ще один варіант захисту, це повне шифрування. Тут відправник шифрує інформацію та відправляє її отримувачу, який після розшифровує його, та отримує доступ до інформації, в результаті всі надіслані дані при передачі мають зашифрований вигляд. [11]

Для забезпечення захисту, також слід проводити перевірку вмісту листів на наявність посилань на шкідливі сайти та спам. В даному випадку можна використовувати допоміжні утиліти для сканування поштової скриньки і завдяки цьому одразу знаходити листи з фішинговими посиланнями, спам, який має скрите шкідливе програмне забезпечення. Тому, щоб захистити пошту від великої кількості

небажаних та шкідливих листів, зазвичай деякі поштові сервери мають, так званий, «чорний» список відомих відправників спаму та фішингу, які були визначені. Також можна фільтрувати повідомлення за типом додатку, яке присилають разом з листом або ж дозволяти відправку тільки від перевірених та надійних джерел.

Зловмисники нерідко використовують найпростіший метод для поширення загроз через електронну пошту — маскування шкідливих листів під легітимні. Але існують такі варіанти, як обмежити такого роду діяльність, хоча на даний момент вони не дуже поширені. Такі методи можуть допомогти перевіряти справжність вмісту листа та контролювати користувачів, а також і облікові записи, яким дозволено надсилати інформацію з домену підприємства.

Процес використання аутентифікації та авторизації користувачів є важливою частиною управління поштовим сервером, так само як і швидке видалення облікових записів або зміна паролів акаунтів, які більше не активні та не використовуються. Як приклад, це стосується акаунтів, які належали співробітникам, які більше не працюють в даній компанії

Ще один метод захисту – це багатофакторна аутентифікація. Один з найефективніших рівнів захисту пошти та доступу до облікових записів. В даному випадку, ідентифікація особистості здійснюється через використання одноразового ключа, що відправляється в SMS-повідомленні. [11]

Також для посилення захисту електронної пошти важливо регулярно оновлювати ПЗ, як операційну систему, так і додаток або браузер, які використовуються для доступу до пошти. Даний метод допоможе усунути уразливості, які дають змогу зловмисникам отримати доступ до електронних листів.

Окрім описаних вище методів захисту, також можна використовувати додаткові утиліти, ПЗ, які допоможуть слідкувати за вмістом листів, що надходить на пошту, блокуючи фішингові сайти або ж шкідливе програмне забезпечення, яке при отриманні користувач спробує відкрити на своєму робочому місці.

Такий вид програмного забезпечення забезпечує фундаментальні можливості безпеки шлюзів електронної пошти, зокрема захист від загроз, таких як зловмисне програмне забезпечення, фішинг, спам і віруси. Вони відстежують величезну кількість електронних листів і блокують ті, що містять такі загрози.

Для забезпечення захисту поштових скриньок також важливо використовувати надійну службу електронної пошти. Більшість підприємств уже використовують такі служби електронної пошти, як Gmail або Outlook.

Багато популярних постачальників послуг електронної пошти, такі як Gmail і Microsoft, надають усі інструменти, необхідні компанії для розміщення корпоративної електронної пошти. Подібним чином сучасні хост-обміни представляють інший шлях, яким компанії можуть скористатися для створення електронної пошти організації. Сучасні служби електронної пошти необхідні для підтримки безпечного середовища електронної пошти. Вони включають такі речі, як: регулярні оновлення, завдяки тому, що розробники постійно аналізують загрози та виправляють потенційні записи, електронна пошта залишається безпечнішою. Удосконалені фішингові фільтри, коли постачальники послуг електронної пошти мають надійне сховище механізмів ідентифікації фішингу та спаму, що допомагає обом не потрапляти у папку "Вхідні". Багатофакторна автентифікація, як було зазначено раніше, це найкраща практика безпеки. [11]

Одним з методів захисту також можуть бути ефективні спам-фільтри. Постачальники послуг електронної пошти вже відфільтровують певну кількість електронних листів, щоб вони взагалі не потрапляли до папки "Вхідні" (або папки спаму). Однак це не завадить компанії самостійно розробити ефективний набір спам-фільтрів. Більшість постачальників дозволяють налаштувати фільтри спаму в обліковому записі, щоб ще більше обмежити доступ до співробітників. Як варіант це може бути використання тактики білого списку для облікових записів, які мають отримувати лише внутрішні повідомлення: будь-який контакт, який не входить до схваленого списку, буде заблоковано, встановлення антивіруса електронної пошти на

корпоративних комп’ютерах, якими користуються працівники, які надсилають або отримують зовнішні електронні листи: багато антивірусних програм тепер інтегруються з електронною поштою, щоб забезпечити додатковий рівень фільтрації.

Дуже важливо навчати співробітників виявляти фішингові листи. Фішинг стає все важче виявити. Хоча багато людей впевнено розпізнають фішингові електронні листи, за останній час спостерігалося зростання кількості персоналізованих і цілеспрямованих фішингових атак. Деякі з них вводили в оману навіть найпроникливіших одержувачів, оскільки вони дуже добре зібрані та підібрані під певного користувача. Для цього можна розробити програму навчання та регулярних тренінгів, коли користувачі можуть вивчити як саме виглядає небезпечний лист і чим він може нашкодити як компанії так і самому отримувачу.

Навчальна програма з питань безпеки, спрямована на виявлення фішингових електронних листів, може зменшити ймовірність того, що спроба буде успішною. Обов’язково потрібно повідомляти про деякі з останніх інновацій у фішингу, наприклад про компрометацію корпоративної електронної пошти, тому декілька тренінгів у рік, допоможуть попередити всі можливі проблеми, адже вони неефективні, якщо відбуваються лише раз. [3]

Також можна допомогти користувачам уникнути фішингових електронних листів, встановивши чітку політику спілкування електронною поштою. Коли, чому та від кого керівники чи співробітники можуть очікувати отримання електронних листів: треба повідомити, що випадкові електронні листи з проханням виконати завдання не є нормою. Електронна пошта, яка раптом надіслала вказівку «встановити це нове антивірусне програмне забезпечення», має негайно викликати тривогу. Якщо користувач підозрює шахрайський електронний лист, потрібно, щоб була можливість зв’язуватися з колегами, іншими способами та пересилати електронний лист до IT-спеціалістів. Для цього потрібні або спеціальні люди, які будуть перевіряти вміст листа, або ж можна звернутись у компанії які надають такі послуги.

Обов’язково потрібно, щоб кожен співробітник був обережним з вкладеннями та посиланнями, адже вони є найбільшими способами зараження системи зловмисним програмним забезпеченням.

Додатки легко не помітити. У 2019 році компанія Trend Micro виявила, що найпоширеніші типи файлів, що містять зловмисне програмне забезпечення, — це ті, які офісний працівник може очікувати отримати. До них належали PDF-файли, електронні таблиці Excel, документи Word і архівні папки. Крім того, багато з них надходять замаскованими під рахунки-фактури, експорт бази даних або інший, здавалося б, законний діловий документ. Хакери можуть легко вставити код у вкладення, яке активується після завантаження файлу. Тому дуже важливо приділити увагу та навчити співробітників не завантажувати та не відкривати файли від неперевірених відправників.[3]

Для облікових записів електронної пошти, які отримують лише внутрішні повідомлення, корисно прийняти стратегію білого списку, де лише схвалені контакти потрапляють до папки "Вхідні". Для облікових записів, які отримують електронні листи із зовнішніх джерел, це непрактично. Тому потрібно навчити користувачів обережно ставитися до небажаної кореспонденції, особливо якщо вона нібито щось пропонує. Деякі політики, які слід прийняти, можуть бути такими: не відповідати на небажані електронні листи з пропозиціями або вимогами, перевірка особу відправника, перехресно посилаючись на нього в LinkedIn або перевіривши компанію, яку він нібито представляє.

Щоб отримати доступ до папки "Вхідні", хакеру спочатку потрібна адреса електронної пошти. Тому також треба приділити увагу навчанню користувачів розглядати адреси електронної пошти як інформацію, яку необхідно знати. Тобто заборонити публікувати робочі адреси електронної пошти на сторінках веб-сайтів, у соціальних мережах чи інших публічних форумах, використовувати електронну пошту для підтримки, обслуговування клієнтів або інших публічних запитів,

розсилати електронні листи лише кваліфікованим потенційним клієнтам, постачальникам і діловим партнерам, яким це потрібно.[3]

2 АНАЛІЗ МЕТОДУ ТА ЗАСОБУ ЗАХИСТУ КОРПОРАТИВНИХ ЕЛЕКТРОНИХ ПОШТ ПРАЦІВНИКІВ ОРГАНІЗАЦІЇ НА БАЗІ CYREN INBOX SECURITY

2.1. Призначення, можливості та функції продукту Cyren Inbox Security

Cyren Inc. – це хмарна компанія, що займається технологіями Інтернет-безпеки, що надає підприємствам послуги безпеки як послуги (SECaaS) і аналізу загроз.

Веб-безпека, безпека DNS, хмарне ізольоване програмне середовище, служби захисту від вхідного/вихідного спаму, виявлення та блокування фішингу в реальному часі, захист від програм-вимагачів, фільтрація URL-адрес, репутація IP для електронної пошти, виявлення атак зловмисного програмного забезпечення, запобігання атакам ботнетів і пошук загроз у хмарі. Cyren також забезпечує захист кінцевих точок, включаючи захист від зловмисного програмного забезпечення для мобільних пристроїв, фільтрацію URL-адрес для мобільних пристроїв і захист вхідного/вихідного шлюзу Інтернету речей (IoT). Основними корпоративними клієнтами, які користуються послугами Cyren, є Microsoft, Google, Check Point, Dell, T-Mobile і Intel.[12]

За оцінками компанії, її хмара безпеки наразі обробляє понад 25 мільярдів транзакцій безпеки, згенерованих понад 1,3 мільярдами користувачів у 180 країнах, щоб виявляти кіберзагрози в міру їх появи.

Cyren проводить революцію в безпеці в Інтернеті, використовуючи розширений хмарний інтелект для забезпечення найшвидшого захисту.

CyrenInbox Security (CIS) допомагає організаціям, які використовують Office 365, виявляти та автоматично виправляти розширений фішинг, компрометацію бізнес-електронної пошти та зловмисне програмне забезпечення, які пройшли крізь їхні існуючі засоби захисту, покращуючи стан безпеки електронної пошти та зменшуючи витрати на ручний пошук та усунення загроз.

Cyren Inbox Security використовує власну інтеграцію API Office 365 для постійного виявлення загрози електронною поштою, які надходять на поштові скриньки користувачів. Набір автоматизованих засобів усунення несправностей визначає та пом'якшує широкий спектр зловмисних атак, які не виявляються засобами захисту периметра, наприклад: уникнення фішингових атак із використанням таких методів, як відкладена активація URL-адрес, приховані URL-адреси з вкладенням, складне шифрування, справжні та дійсні сертифікати SSL тощо, шахрайство BEC, CEO та інші цілеспрямовані атаки соціальної інженерії, нові фішингові кампанії нульового дня, захоплення облікових записів (викрадення облікових даних) і моніторинг внутрішньої електронної пошти.[13]

Хмарне рішення CyrenInbox Security (CIS) дозволяє організаціям установити додатковий критичний рівень безпеки електронної пошти на рівні вхідних повідомлень. У випадку надходження листа з невідомим фішингом або ж з іншими загорозами, які зазвичай долають традиційні бар'єри безпеки, CIS виявляє їх і виправляє автоматично. Завдяки своїм превагам CyrenInbox Security надає гарантію постійного моніторингу пошти та швидкого реагування на ту чи іншу загрозу:

– Захист від фішингу

Cyren Inbox Security використовує широкий набір хмарних обчислень і технологій безпеки Cyren для виявлення уникливих фішингових атак і надання найдосконаліших можливостей виявлення загроз, включаючи перевірку в реальному часі заголовків електронних листів(Email Headers), корисного навантаження, URL-адрес і вкладень, а також машинне навчання, повторюваний шаблон виявлення, репутація IP, евристична кластеризація, обробка природної мови та захист від самозванців(атаки типу BEC/CEO).

– Безперервне виявлення

Даний продукт захищає від нових, раніше невідомих загроз, постійно скануючи кожен електронний лист у кожній папці поштової скриньки кожного користувача.

Компанія відстежує поведінку поштової скриньки та взаємодію користувачів у ній та виявляє аномалії. Потім усі ці дані порівнюються в режимі реального часу, щоб визначити, чи є електронний лист зловмисним, і чи потрібно вжити заходів.

– Автоматизоване відновлення

Можливості автоматизованого виправлення та керування інцидентами забезпечити швидке видалення загроз із організації комплексно. Автоматизоване між корпоративне усунення фішингу видаляє підозрілі повідомлення з усіх заражених поштових скриньок по всій організації. Основа виправлення на основі політики підтримує широкий набір дій, включаючи теги та доставки, переміщення до папку, видалити та надіслати сповіщення. Надійні робочі процеси керування інцидентами та справами, а також обширні криміналістичні дисплеї знімають велику частину слідчих витрат з команди безпеки та забезпечують швидке реагування та виправлення.

– Краудсорсингове виявлення користувачів.

Одна з послуг, що надає Cyren, це простий в установці та використанні плагін Outlook, який забезпечує краудсорсингову аналітику загроз, яка допомагає ідентифікувати та захиститись від фішингових атак. При використанні продукту, у користувача є можливість просканувати нове повідомлення, натиснувши помітну кнопку. Якщо ж користувач не згоден з результатом сканування, він може надіслати відгук, де буде обраний лист та відмічено, що саме у листі піддалось сумнівам(посилання, вкладення або ж сам відправник). Після цього аналітики додатково перевіряють лист і все, що в ньому міститься. Результати дослідження надсилаються автоматично до користувача, після того як аналітик зробив свій висновок та закрив даний випадок, як легітимний лист або ж як, наприклад, фішинг чи BEC.

– Цілодобова служба реагування на загрози

Cyren надає цілодобову керовану службу реагування на загрози (TRS) для користувачів Cyren Inbox Security. Cyren TRS зосереджено на розслідуванні, аналізі та вирішенні інцидентів відкритої загрози, про які повідомляють користувачі поштової

скриньки, а також на розслідуванні підозрілих інцидентів із низьким рівнем достовірності. Якщо аналіз Cyren повторно класифікує електронний лист як підозрілий, його буде автоматично видалено з поштової скриньки звітів і всіх поштових скриньок користувачів у організації. [13]

2.2. Принцип роботи Cyren Inbox Security.

CIRS — це цілодобова керована служба для користувачів Cyren Inbox Security. Експерти з реагування на загрози зосереджені на розслідуванні, аналізі та вирішенні інцидентів із загрозами, про які повідомляють користувачі поштової скриньки Office 365, а також на розслідуванні підозрілих інцидентів із низьким рівнем довіри, виявлених системою CIS. Вся робота аналітиків відбувається через Cyren Inbox Security UI(рис.2.1). Після того, як експерт отримує доступ до головного екрану, одразу відображається інформація щодо інцидентів за останній час, який можна обрати, вказавши за останні декілька днів або ж за останню добу(рис.2.2). Також надається одразу інформація про те, яка кількість інцидентів була виявлена за вказаний час та яка загальна кількість листів була надіслана. Також надається інформація про виявлені загрози такі, як фішинг, шкідливе ПЗ, атаки типу BEC, а також спам/скам(рис.2.3).[14]

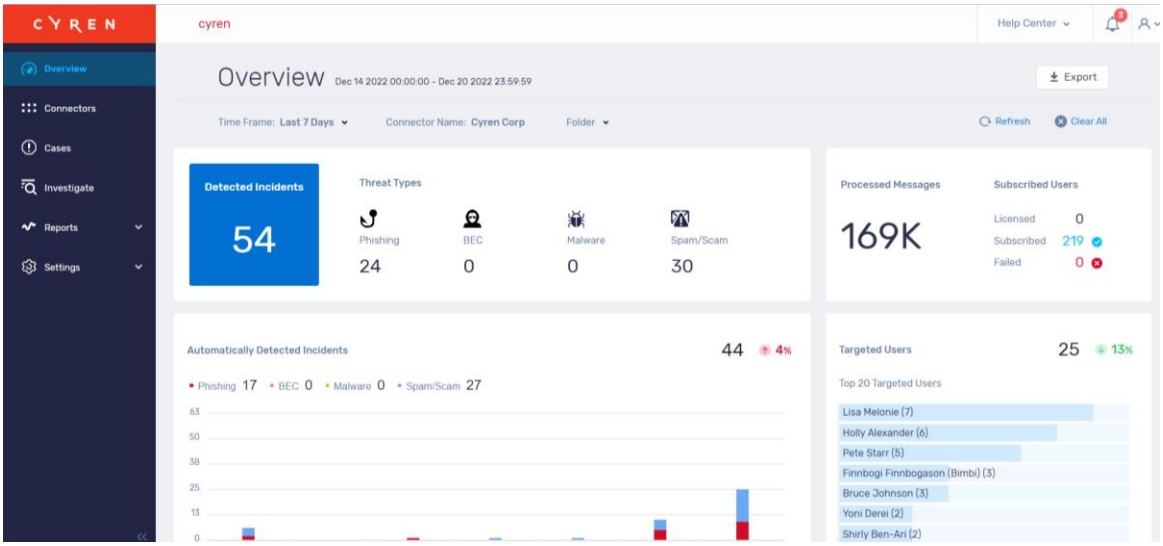


Рис.2.1. Головний екран Cyren Inbox Security

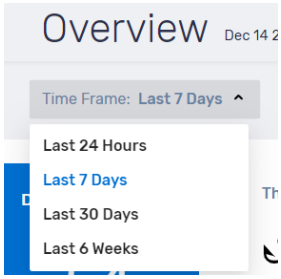


Рис.2.2. Час, для показу інцидентів за певний період

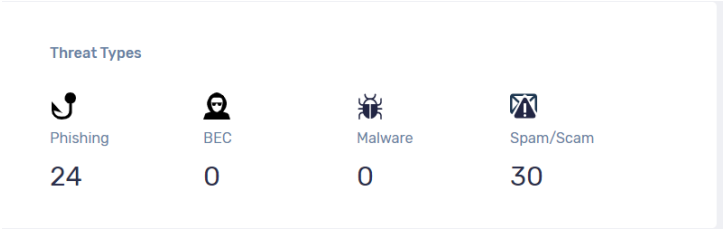


Рис.2.3. Виявлені загрози

У вкладці «Cases» надані всі інциденти які були виявлені самою системою або ж які були надіслані самими користувачами, які підозрювали лист на фішинг або ж BEC(рис.2.4). Тут надана детальна інформація про кожен кейс: який саме тип загрози, ким саме було виявлено(системою, користувачем або ж адміністратором), дата та ідентифікатор інциденту, чи закритий даний кейс чи потребує додаткового розслідування. Якщо аналітику потрібно знайти певний інцидент серед інших, він

може знайти його за відповідним ідентифікатором, статусом(закритий/відкритий) або ж за поштою користувача, який отримав даний лист.

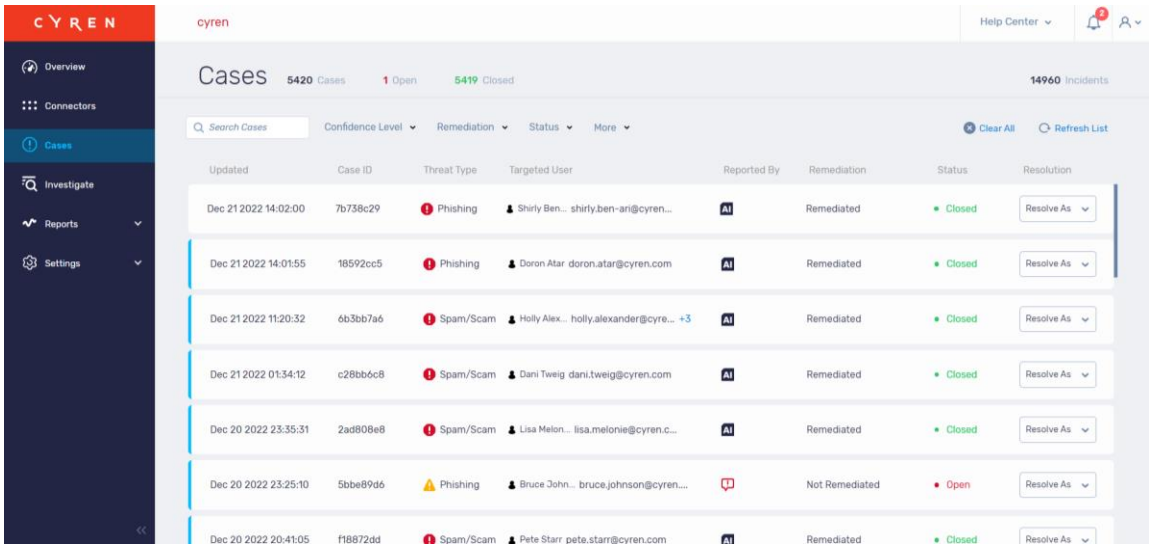


Рис.2.4. Вкладка «Cases»

У вкладці «Connectors» аналітик може створювати правила, за якими при отриманні шкідливого листа будуть працювати певні умови(рис.2.5). Наприклад, при отриманні повідомлення з фішингом або ж зловмисним додатком, лист не дійде до отримувача, адже система виявить його та одразу видалить, щоб користувач не зміг піддатись даній атаці. Також тут присутні такі варіанти як: переміщення листа до певної папки(наприклад, видалених), додання попереджального банеру, блокування шкідливих посилань та додатків.

У вкладці «Settings» можливо здійснити налаштування акаунтів, визначити головних адміністраторів, а також налаштувати попереджувальні банери, які будуть вказувати та попереджувати користувача про можливу загрозу.

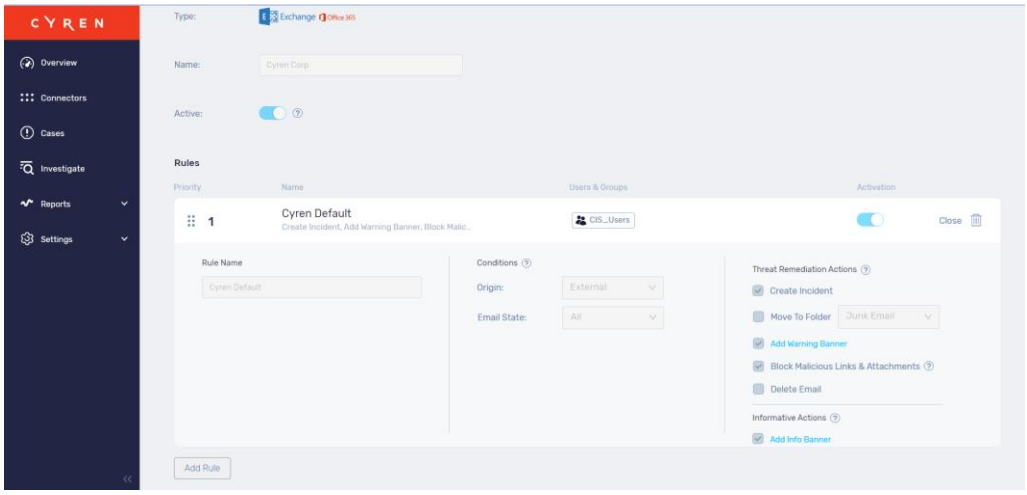


Рис.2.5. Вкладка «Connectors»

У Cyren Inbox Security є декілька типів таких банерів, звернувши увагу на які користувач буде обережно ставитись до даного листа і повідомить про загрозу аналітика. Банера можуть налаштовуватись під кожну організацію окремо, з будь-яким текстом та умовами, при яких він буде з'являтись. На рисунку нижче наведений приклад банеру, який попереджає користувача про посилання з фішингом та рекомендує не переходити на ту чи іншу сторінку(рис.2.6).

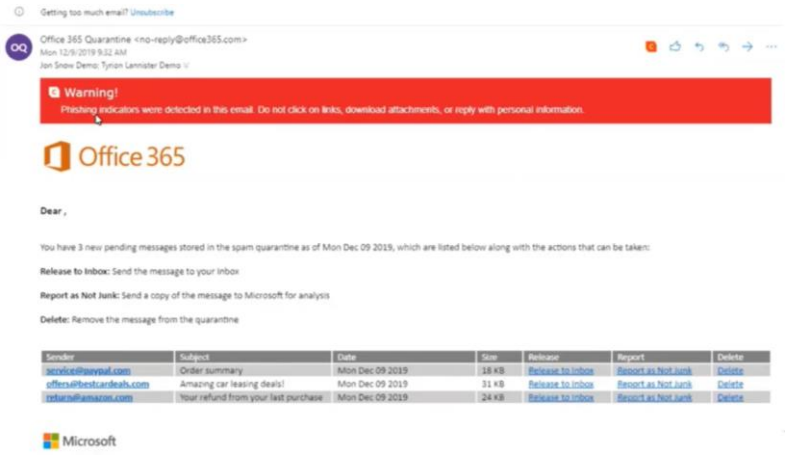


Рис.2.6. Попередження про фішинг

Також можна налаштувати інформаційний банер, який буде попереджувати про підозру листа, який був надісланий від зовнішнього невідомого системі користувача, якщо отримувач погоджується та підозрює даний лист, то він може повідомити про це аналітика, який в свою чергу вже проведе розслідування(рис.2.7).

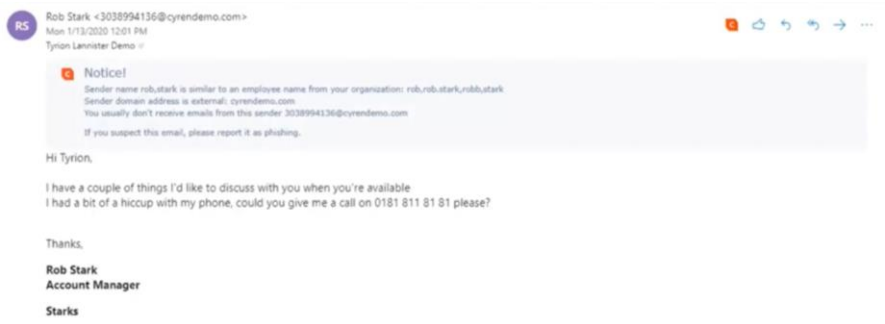
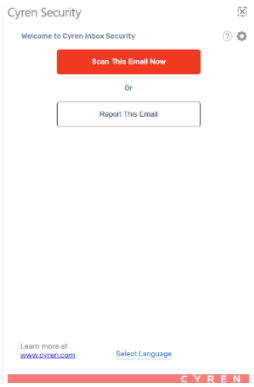


Рис.2.7. Приклад інформаційного банера

В деяких випадках, як було зазначено вище, користувач може сам виявити підозрілий лист та через встановлений плагін повідомити про це аналітика(рис.2.8). Після сканування користувач може бути не згоден з результатом і надіслати дане повідомлення з поміткою phishing/spam/malware. Такий відгук отримує аналітик і перевіряє лист на наявність тієї чи іншої загрози, після розслідування закриває даний кейс з відповідним лейблом(рис.2.9).



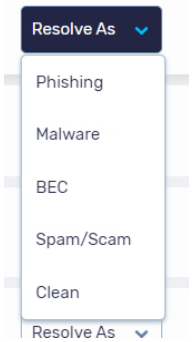


Рис.2.8. Плагін для сканування листів Рис.2.9. Рішення, як саме закрити кейс

Після закриття, до користувача приходить лист з результатом, чи це був шкідливий лист чи все ж таки чистий.

3 РОЗРОБЛЕННЯ ТЕХНОЛОГІЇ ЗАХИСТУ ЕЛЕКТРОННИХ ПОШТ ПРАЦІВНИКІВ З ВИКОРИСТАННЯМ CYREN INBOX SECURITY

За останній час все більше і більше компаній піддаються атакам, які реалізуються через електронну пошту рядового співробітника компанії. Результатом такої атаки може бути як викрадення даних облікового запису, для отримання доступу до ресурсів та конфіденційної інформації організації, так і порушення звичайного робочого процесу.

Тому керівники, адміністратори безпеки компаній, при створенні політики безпеки, приділити значну увагу захисту корпоративних пошт працівників. Адже згідно зі статистиками, які були представленні у роботі, більшість атак основані на надсиланні шкідливого листа звичайному працівнику і через незнання та слабкий рівень захисту, співробітник може надати ту чи іншу критичну інформацію зловмиснику.

3.1. Робота з Cyren Inbox Security, розслідування інцидентів.

Робота експерта з розслідування інцидентів полягає в перевірці вмісту листа, репутації відправника, а також всіх посилань та вкладень, які надійшли разом з повідомленням. В деяких випадках система може не виявити ту чи іншу загрозу, частіше за все це трапляється через те, що кожного дня з’являються нові типи та способи доставки фішингу чи зловмисного ПЗ до користувача. Через це, використовуючи послуги Cyren Inbox Security, організації можуть додатково посилити свій рівень безпеки, адже кожен виявлений користувачем інцидент, буде розглянутий експертами з безпеки та будуть вжиті ті чи інші міри для забезпечення безпеки компанії.

В даній частині роботи буде розглянутий принцип роботи експерта, кожен крок, та як саме в даному випадку працює Cyren Inbox Security.

При отриманні листа, співробітник може просканувати його, за допомогою влаштованого плагіну, результат сканування буде наданий через декілька секунд(рис.3.1). В даному випадку результат сканування «Phishing not found», тобто надіслана інформація не має шкідливого вмісту. Якщо ж просканований лист має протилежний результат, тобто знайдений фішинг чи зловмисний додаток, то результат буде «Phishing found»(рис.3.2). В даному випадку система попереджає користувача не натискати на посилання та не відповідати на нього.

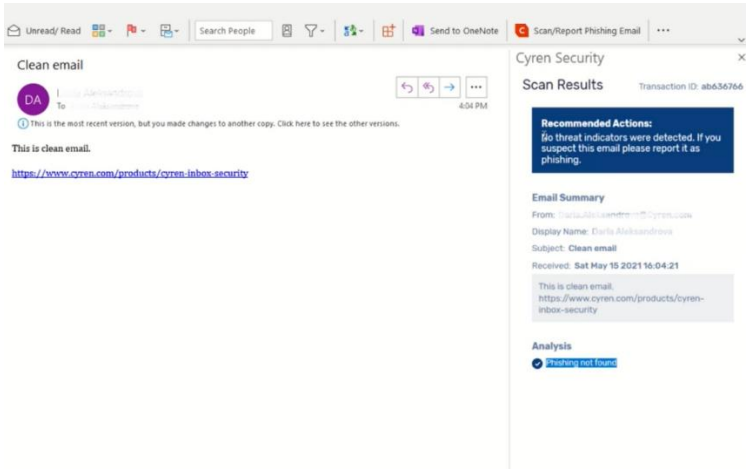


Рис.3.1. Результат сканування. Лист чистий

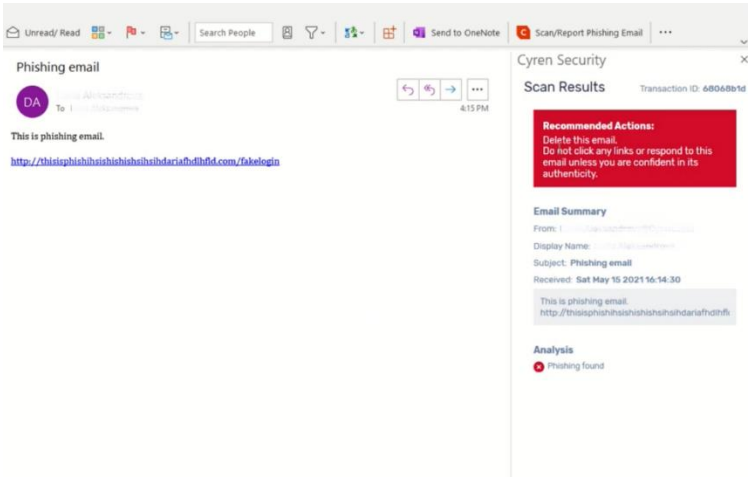


Рис.3.2. - Результат сканування. Лист з фішингом

Після користувач може повідомити експерта з безпеки про даний лист, надіславши відгук, де буде вказано, що саме є індикатором загрози(відправник, додаток, посилання чи сам текст). Для цього потрібно натиснути на кнопку «Report as

phishing» та обрати індикатори, за побажанням написати детальну інформацію щодо листа(рис.3.3).

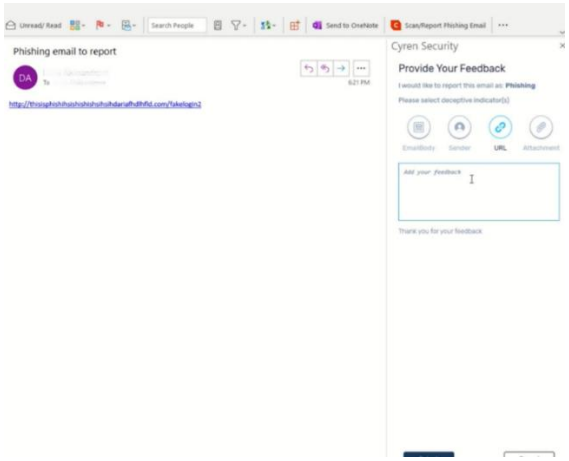


Рис.3.3. – Створення відгуку на отриманий лист

Даний відгук отримає експерт з безпеки в CIS UI та починає розслідування інциденту(рис.3.4). Для цього перш за все перевіряються всі посилання на наявність фішингу або автоматично завантажувального зловмисного додатку, після перевіряється відправник та його активність, чи було надіслані шкідливі листи до цього. Після того як все було перевірено, аналітик робить висновок та закриває кейс з відповідним висновком(фішинг, шкідливе ПЗ, BEC, спам/скам або чистий).

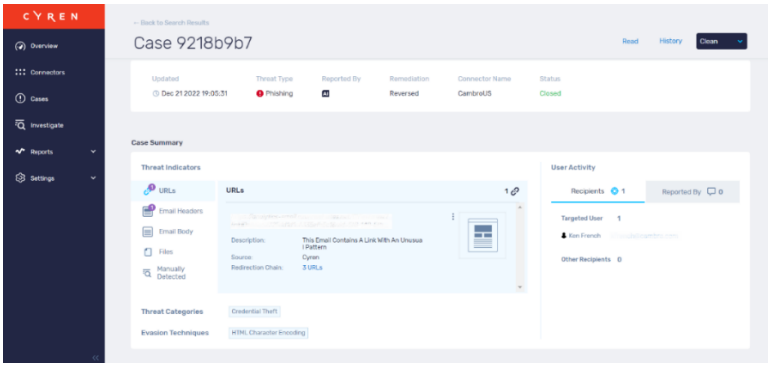


Рис.3.4. Приклад закритого кейсу, як «Clean»

Найчастіше зловмисники надсилають фішинг у вигляді вкладення, яке на перший погляд має вигляд чеку для оплати з назвою «Invoice for …», де в назві буде вказано номер замовлення чи ім’я отримувача, або у вигляді PDF-файлу з певною інформацією. Далі буде розглянуто приклад даної атаки на співробітника однієї компанії, який надіслав відгук з підозрою на BEC(рис.3.7)

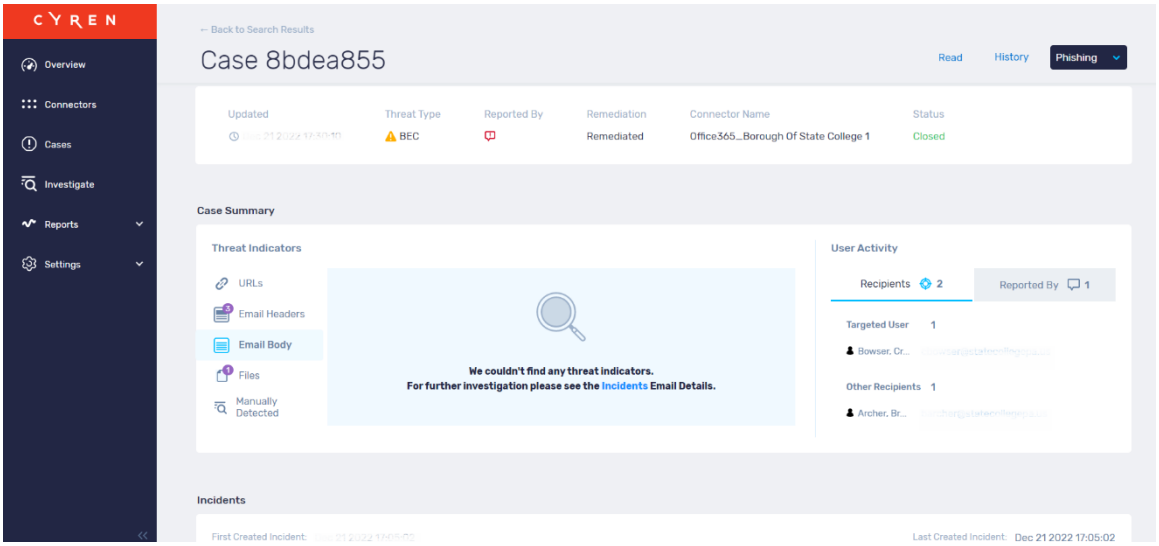


Рис.3.5. Відгук користувача

В даному кейсі повідомлення було надіслано від внутрішнього користувача компанії, без додаткового тексту, тільки з попередженням про те, що лист надісланий ззовні компанії, але електронна адреса схожа на працівника організації(рис.3.6).

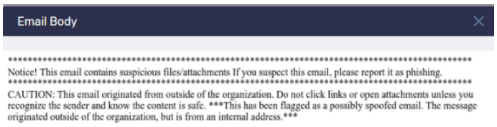


Рис.3.6. Надісланий лист

Тому наступним кроком буде перевірка вкладення на вміст шкідливого ПЗ чи фішингової сторінки(рис.3.7). В даному випадку, система автоматично виявила та надала категорію Phishing для надісланого файлу, при відкритті автоматично завантажується браузер та відображається підроблена сторінка для входу в обліковий запис Microsoft(рис.3.8).

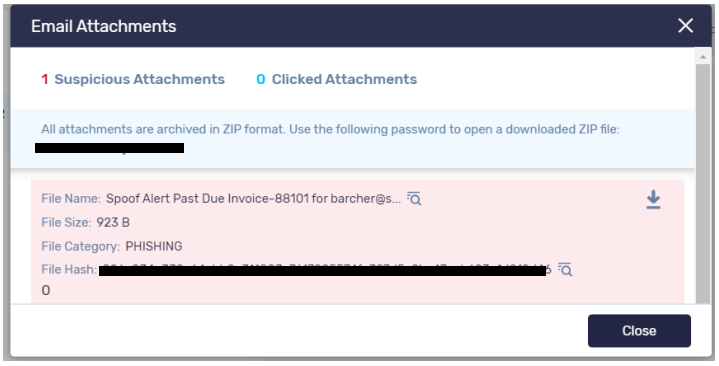


Рис.3.7. Перевірка вкладення

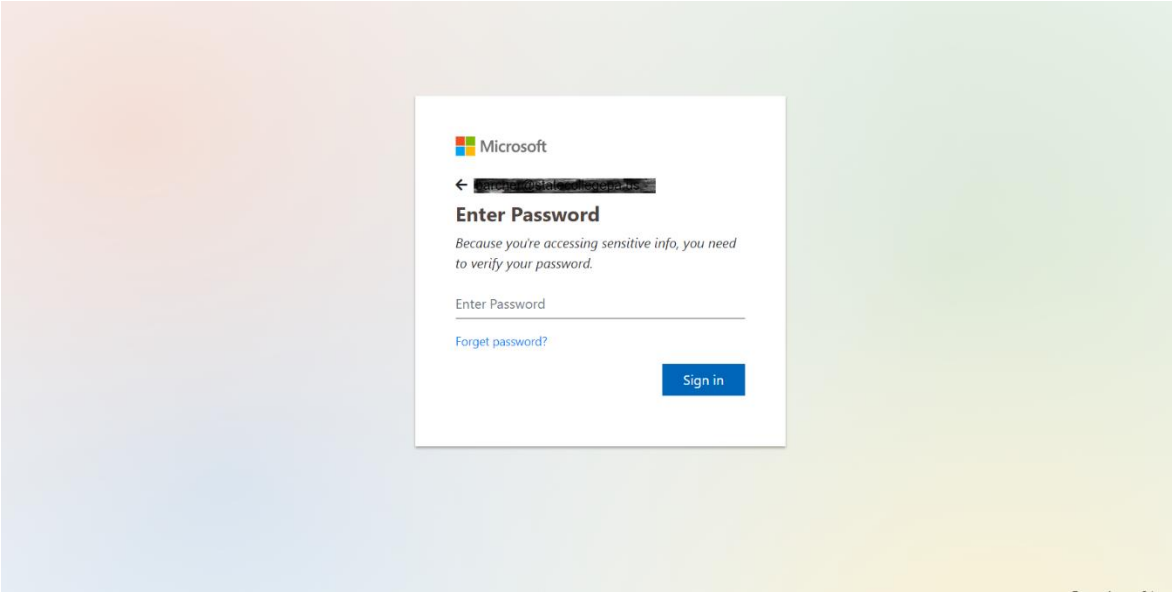


Рис.3.8. Сторінка з фішингом

На даній сторінці користувача просять ввести пароль для отримання доступу до надісланої інформації, при введенні паролю, користувача просять ввести його ще раз, бо вказаний пароль не вірний, користувач буде намагатись ввести пароль, але все одно доступу до інформації не отримає, адже головна задача зловмисника, що отримати саме пароль(рис.3.9). Таким чином зловмисник отримує пароль від облікового запису та доступ до нього.

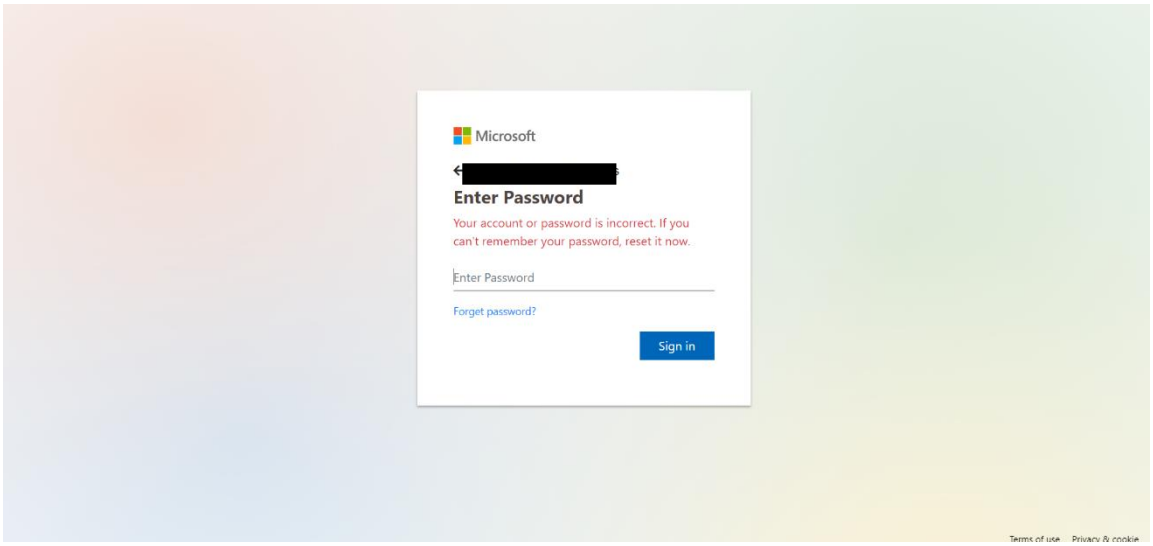


Рис.3.9. Спроба ввести пароль

Для того щоб надалі система не пропускала листи з таким вкладенням адміністратору або ж експерту з безпеки потрібно заблокувати відправника з типом Phishing, якщо ж лист був відправлений з електронної адреси співробітника(тобто з підробленої пошти), то слід заблокувати хеш вкладення, який надалі буде ідентифікуватись системою як шкідливий.

Як тільки всі потрібні дії були проведені, адміністратору чи експерту з безпеки потрібно закрити кейс з відповідним рішенням, в даному випадку «Phishing» і після будуть задіяні обрані попередньо правила для шкідливих листів, в даному випадку блокування вкладення, перенесення листа у папку «Видалені»(рис.3.10).

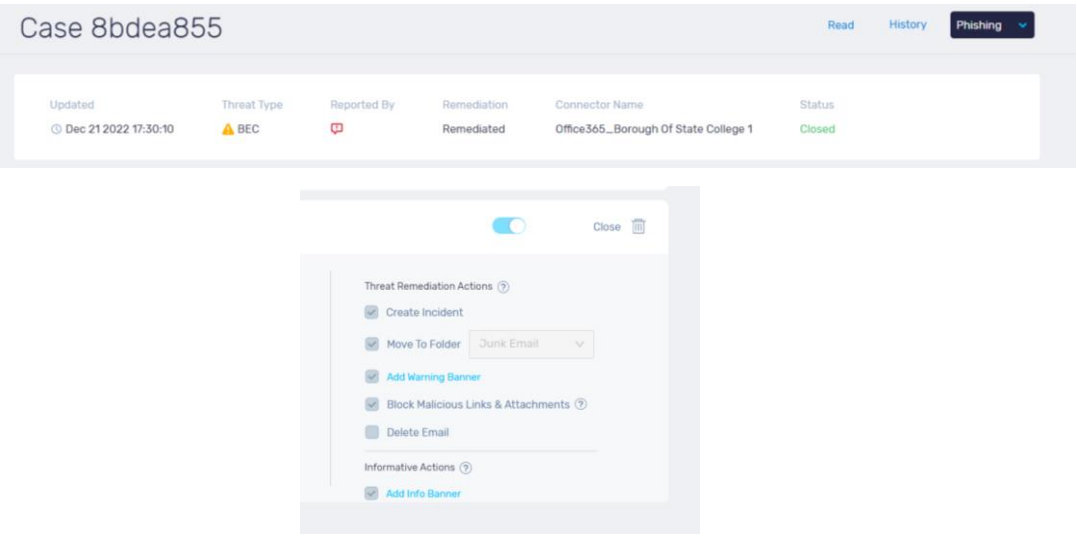


Рис.3.10. Закриття кейсу та встановлені правила

Ще один варіант інциденту, коли співробітнику надсилають лист з посиланням на сховище, де знаходиться потрібний файл для огляду(рис.3.11). Найчастіше такі посилання містяться на доменах my.sharepoint.com, де сторінка виглядає як інтернет версія OneNote. Для того, щоб передивитись файл, користувачу потрібно натиснути на кнопку «View Documents Online Here», після він буде перенаправленний на сторінку схожу на вхід до облікового запису Microsoft(рис.3.12). Але якщо подивитись на посилання, то можна впевнитись, що даний сайт не є офіційним Microsoft:

```
https://06-0-1-bryjh-0lkgf-9ejt-fgkw-9j6thg90jen-0g9jnrjg.obs.ap-southeast-1.myhuaweicloud.com/vryh6-0g9et5k6-6g90njmewr-9g8hbnw-rfmkj-r9jhg-9gnjmg.htm
```

Також спробувавши ввести будь-які дані(недійсну електронну адресу та будь-яке поєднання символів у графу «пароль»), результатом буде нібито проводиться перенаправлення до облікового запису, хоча насправді, отримані дані відсилаються зловмиснику(рис.3.13).

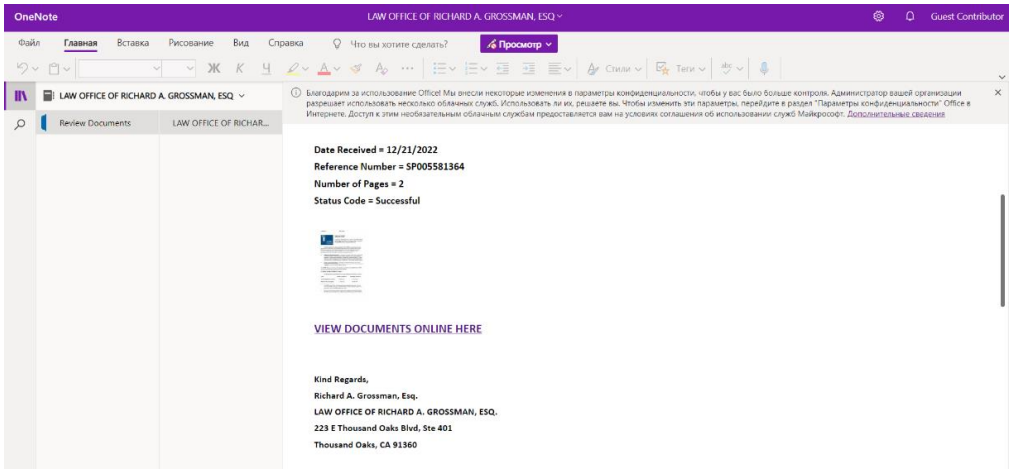


Рис.3.10. Сховище з файлом

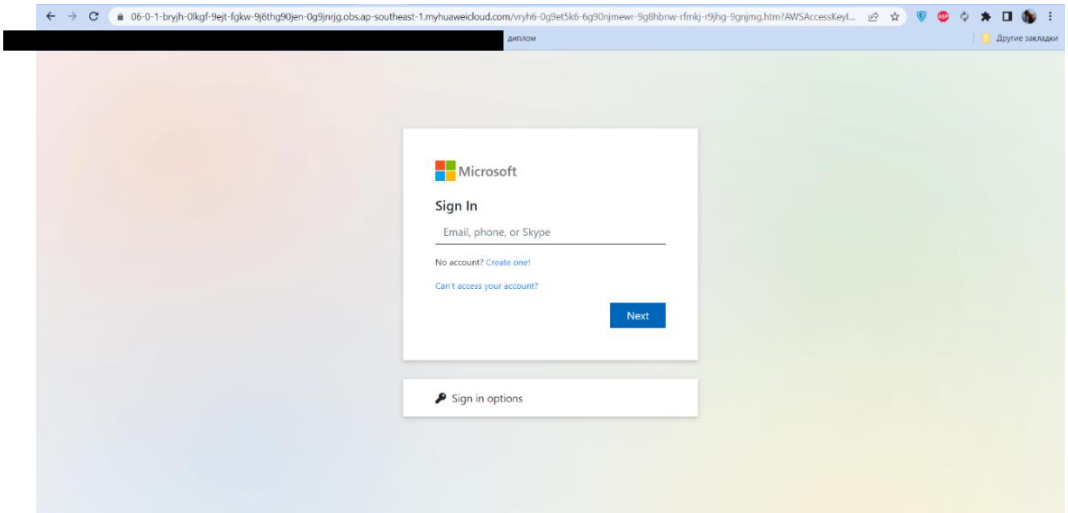


Рис.3.12 – Сторінка з фішингом

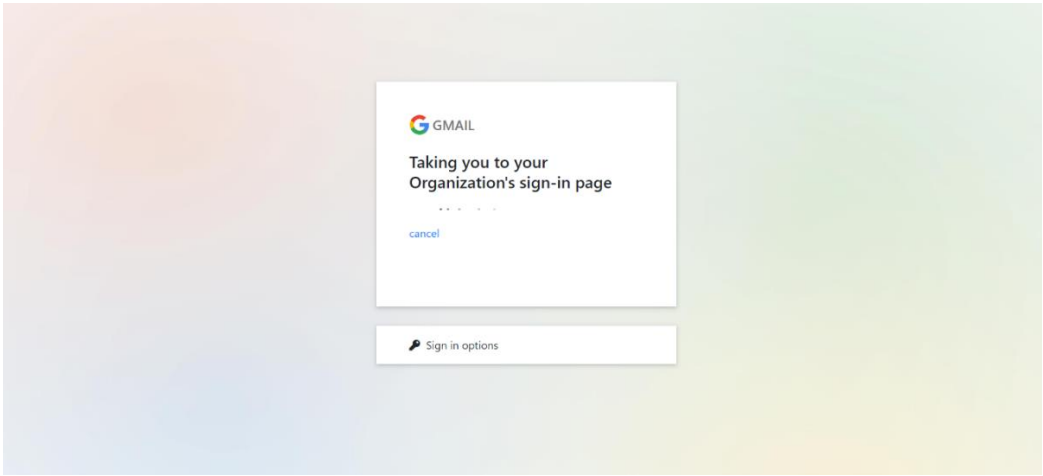


Рис.3.13. Результат введення недійсних даних(адреса та пароль)

При даному інциденті, адміністратор отримує відгук на даний лист від співробітника, перевіряє всі посилання та репутацію відправника. Результат дослідження буде наступним: посилання з фішингом, а також сторінка з кнопкою, яка перенаправляє, будуть заблоковані з категорією Phishing, кейс буде закритий з висновком Phishing та будуть застосовані вказані у налаштуваннях для організації правила(перенесення листа у папку «Видалені», додання попереджального банеру, блокування посилань).

Завдання експерта з безпеки/адміністратора ретельно перевіряти кожен інцидент, який був виявлений самою системою або ж користувачем. Часто, через не знання, користувачі можуть надсилати відгук і на чистий лист, але при цьому задача експерта детально вивчити кожне посилання, вкладення та відправника, щоб правильно зробити висновок та закрити кейс як чистий чи шкідливий з відповідним типом. На схемі нижче представлений процес розслідування інцидентів(рис.3.14), де вказані при яких результатах, які саме дії повинен зробити експерт з безпеки/адміністратор.

Рис.3.14. – Процес розслідування інциденту

3.2. Розроблення загальних рекомендацій для забезпечення захисту корпоративних пошт.

Для забезпечення безпеки корпоративних пошт працівників та попередження атак типу фішинг, BEC, спам, тощо, користувачам та адміністраторам безпеки потрібно дотримуватись певних рекомендацій.

– *Шифрування вмісту листа.*

При надсиланні листа через електронну пошту, дані, що містяться у повідомленні, можуть потрапити під контроль зловмисника, таким чином конфіденційність та цілісність інформації буде порушена. В даному випадку рекомендується шифрувати дані при відправці. При цьому відправник шифрує лист особистим ключем, а отримувач, маючи свій ключ, розшифровує отримане повідомлення.

– *Ретельна перевірка вмісту листів та відправника.*

При отриманні повідомлення користувач повинен перевірити лист на наявність підозрілих посилань або ж впевнитись, що лист надісланий від надійного відправника. В даному випадку, щоб спростити перевірку та бути певним у легітимності листа, можна використовувати допоміжні утиліти або ж послуги компаній, які в свою чергу будуть проводити моніторинг надісланих повідомлень та блокувати небезпечний контент. Зазвичай деякі поштові сервери мають свій «чорний» список відомих відправників спаму та фішингу, які були визначені та зафіксовані раніше, також можна фільтрувати повідомлення та дозволяти відправку тільки від надійних та перевірених джерел.

– *Спам-фільтри.*

Постачальники послуг електронної пошти зазвичай вже відфільтровують певну кількість електронних листів, щоб вони взагалі не потрапляли до папки "Вхідні" (або папки спаму). Але компанії можуть особисто додатково налаштувати дані фільтри, так щоб ще більше обмежити доступ до своїх співробітників. Наприклад, можна

налаштувати білий список, коли будь-який контакт, який не входить до схваленого списку, буде заблоковано.

– *Встановлення антивіруса електронної пошти.*

Ще однин можливий метод захисту, це встановлення антивірусу, на корпоративних ПК, якими користуються працівники, яким часто доводиться надсилити/отримувати зовнішні електронні листи.

– *Використання аутентифікації та авторизації користувачів.*

Аутентифікація та авторизація користувачів є одним з найбільш важливих моментів в управлінні поштовим сервером. Багатофакторна аутентифікація, також допоможе попередити несанкціонований доступ до облікових записів. В даному випадку, ідентифікація особистості здійснюється через використання одноразового ключа, що відправляється в SMS-повідомленні.

– *Навчання співробітників.*

Даний метод захисту, є більше спробою попередження здійсненню атаки, адже в даному випадку найбільшою уразливістю є людський фактор. Якщо співробітник не буде ознайомлений з різними типами загроз, то при отримання листа з фішингом чи шкідливим ПЗ, працівник з легкістю може піддатись атаці та надати доступ до конфіденційної інформації.

В даному випадку керівники компаній мають забезпечити регулярні тренінги, де буде викладена основна інформація про той чи інший тип загрози та атаки, наведені приклади та як саме і що має зробити співробітник, при отриманні шкідливого або підозрілого листа.

Дуже важливо, щоб дані тренінги проводились за розкладом та декілька разів на рік, де кожен раз буде оновлюватись інформація про останні види загроз.[3]

3.3. Розроблення рекомендацій, щодо застосування Cyren Inbox Security, для захисту пошт працівників.

Для підвищення рівню захисту корпоративної електронної пошти керівники компаній можуть скористатись послугами хмарного додатку Cyren Inbox Security.

При встановлені даного продукту, користувач отримує можливість сканувати та перевіряти вміст листа самостійно, а також надсилати повідомлення, щодо підозри на шкідливий лист. Даний відгук отримує експерт безпеки чи адміністратор, який повинен провести детальне розслідування та закрити інцидент як чистий або ж як шкідливий, з відповідним типом загрози.

Першим кроком експерта при розслідуванні інциденту через Cyren Inbox Security, повинна бути перевірка вмісту листа на посилання або ж вкладення. При знаходженні шкідливого посилання, яке може містити сторінку з фішингом або ж автоматично завантажувальне ПЗ, наступним кроком має бути блокування посилання та закриття кейсу з відповідним типом атаки, при цьому застосовуючи правила, які визначені для організації при отриманні шкідливого листа. На рисунку нижче(рис.3.15) представлений приклад листа з фішингом. В даному випадку експерт з безпеки має звернути увагу на електронну адресу відправника, яка не відповідає компанії і є підозрілою. Також слід звернути увагу на те, що посилання на вхід до персонального акаунту банку має зовсім інший домен, який не відповідає тому, який вказаний в листі.

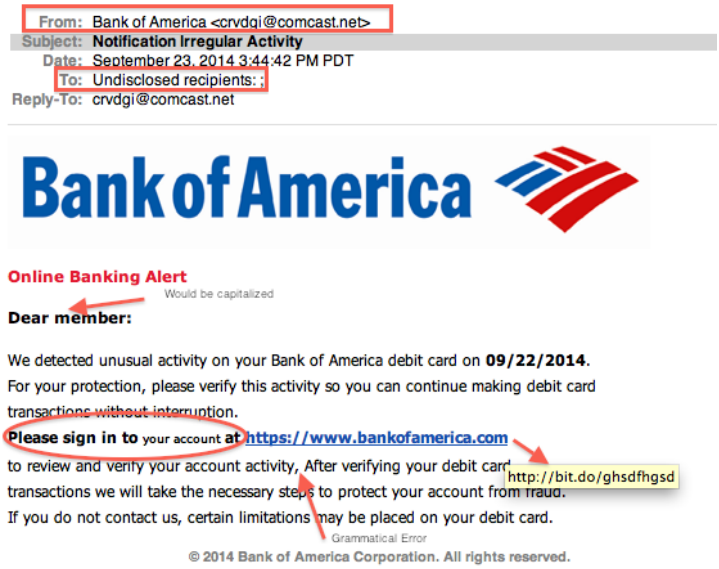


Рис.3.15. Лист з фішингом

Тобто користувач перейшовши по даному посиланню буде переведений на неофіційну сторінку, яка буде дуже схожа на звичайну форму входу в акаунт банку.

На наступному прикладі, експерту слід звернути увагу на текст самого листа(рис.3.16). В даному випадку лист надісланий співробітнику від нібито керівника компанії, але перевіривши електрону адресу відправника через утиліти Cyren Inbox Security, експерт отримає результат, що дана адреса не співпадає ні з однією внутрішньою, а також має зовсім інший домен, на відміну від того, який наявний у співробітників компанії. Після аналізу тексту листа, буде зрозуміло, що дане повідомлення це BEC, адже відправник підписався как CEO компанії та просить швидкої відповіді.

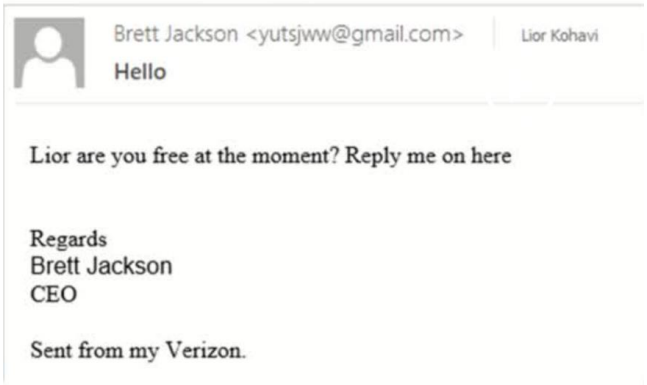


Рис.3.16. Лист з типом загрози BEC

У результаті дослідження експерту слід заблокувати відправника, закрити кейс як BEC та застосувати визначені правила для шкідливих листів, наприклад, перенесення повідомлення у папку «Видалені» та додати попереджувальний банер.

ВИСНОВКИ

Під час виконання магістерської роботи, була проаналізована проблема захисту корпоративної електронної пошти працівників організації.

Для даного аналізу були розглянуті всі можливі та найбільш розповсюджені типи атак на електронні пошти та наслідки, до яких їхнє успішне завершення може призвести. Були досліджені всі можливі методи захисту та попередження атак типу фішинг, BEC, шкідливого програмного забезпечення. Також у роботі були наведені приклади можливих атак, як саме вони реалізуються та як їх можна уникнути.

У роботі було розглянуте рішення для підвищення рівня захисту корпоративних електронних пошт від компанії Cyren, а саме Cyren Inbox Security. Проведено ознайомлення з інтерфейсом даного рішення та процесами роботи, аналіз всіх можливих функцій та наведені приклади, як саме експерт з безпеки або ж адміністратор може проводити розслідування тих чи інших інцидентів на основі використання продукту.

В останній частині роботі були описані рекомендації щодо електронних пошт. Надані загальні поради як саме можна попередити атаки на поштові скриньки, рекомендації були вказані як для керівників компаній, так і для рядових співробітників. Також були наведені поради з використання продукту Cyren Inbox Security при розслідуванні інцидентів, з чого почати і як правильно закрити той чи інший кейс.

Таким чином розроблені рекомендації допоможуть керівникам компаній та фахівцям з безпеки правильно організувати систему захисту конфіденційної інформації та забезпечити цілісність даних, які передаються через електронні пошти співробітників компанії.

ПЕРЕЛІК ПОСИЛАНЬ

1. What is email security? [Електронний ресурс] – Режим доступу: https://www.cloudflare.com/learning/email-security/what-is-email-security/
2. Що таке захист електронної пошти? [Електронний ресурс] – Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-email-security
3. How to Secure Email in Your Business with an Email Security Policy [Електронний ресурс] – Режим доступу: https://carbidesecure.com/resources/how-to-secure-email-in-your-business-with-an-email-security-policy/
4. The top 9 threats to your email security and how to protect your mailbox [Електронний ресурс] – Режим доступу: https://www.pinnacaretail.com/blog/email-security-top-mailbox-threats
5. Why Email Security is Important? [Електронний ресурс] – Режим доступу: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/why-email-security-is-important/
6. Types of Email Attacks Every Business Should Prepare For [Електронний ресурс] – Режим доступу: https://www.tessian.com/blog/email-attack-types/
7. The Latest 2022 Phishing Statistics (updated December 2022) [Електронний ресурс] – Режим доступу: https://aag-it.com/the-latest-2022-phishing-statistics-updated-october-2022/
8. APWG 1Q 2022: Phishing reaches record high; APWG observes one million attacks within the quarter – for the first time – in the first quarter of 2022 [Електронний ресурс] – Режим доступу: https://apwg.org/apwg-1q-2022-phishing-reaches-record-high-apwg-observes-one-million-attacks-within-the-quarter-for-the-first-time-in-the-first-quarter-of-2022/

9. What is spam? [Електронний ресурс] – Режим доступу: https://www.malwarebytes.com/spam
10. The top phishing statistics to know in 2023 [Електронний ресурс] – Режим доступу: https://blog.usecure.io/the-top-phishing-statistics-to-know-in-2022
11. Безпека пошти: основні рекомендації для захисту скриньок від онлайн-загроз [Електронний ресурс] – Режим доступу: https://eset.ua/ua/news/view/659/bezopasnost-pochty-vneshniye-i-vnutrenniye-faktory-zashchity-pochty
12. We are Cyren [Електронний ресурс] – Режим доступу: https://www.cyren.com/company/about-cyren
13. Protect your Office 365 users and yourbusiness against evasive phishing attacks [Електронний ресурс] – Режим доступу: https://www.cyren.com/tl_files/downloads/Cyren_Datasheet_InboxSecurity_200421_v1.4.1.pdf
14. Phishing and Fraud URL Intelligence [Електронний ресурс] – Режим доступу: https://www.cyren.com/tl_files/downloads/Phishing%20and%20Fraud%20URL%20Intelligence%20DS-FINAL.pdf
15. Cyren Threat InDepth. Malware File Intelligence [Електронний ресурс] – Режим доступу: https://www.cyren.com/tl_files/downloads/Cyren_Malware%20File%20Intelligence_Datasheet_12282020_Web.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)