ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ ВІД ШКІДЛИВИХ ПРОГРАМ ТА ПРОГРАМ-ВИМАГАЧІВ НА БАЗІ MICROSOFT 365»

Виконав студент 6 курсу, групи БСДМ-63
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Ларін О. Д.
(прізвище та ініціали)
Керівник Собчук А. В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н. С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …… 10

ВСТУП ……..…… 10

1 **АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ ВІД ШКІДЛИВИХ ПРОГРАМ** ……..… 12

1.1 Дослідження проблеми захисту інформаційних ресурсів організації від шкідливих програм та програм-вимагачів ……. 12
1.2 Аналіз підходів до захисту інформаційних ресурсів організації від шкідливих програм ……... 18
1.3 Аналіз існуючих рішень із захисту інформаційних ресурсів організації від шкідливих програм ……..…..... 26

2 **АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ ВІД ШКІДЛИВИХ ПРОГРАМ НА ПРИКЛАДІ MICROSOFT 365** ……..…..…. 41

2.1 Основні функції та зміст захисту від шкідливих програм і програм-вимагачів у Microsoft 365 …… 41
2.2 Призначення та основні функції захисту рішення Exchange Online Protection ……..…… 49
2.3 Призначення та основні функції рішення Microsoft Defender for Office 365 ……...…….. 52

3 **ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ ВІД ШКІДЛИВИХ ПРОГРАМ** ……..……. 56

3.1 Технологія захисту від програм-вимагачів для клієнта Microsoft 365 ……..…….…… 56
3.2 Технологія захисту від загроз у Microsoft Defender для Office 365 60

3.3 Рекомендації щодо застосування технології захисту інформаційних ресурсів організації від шкідливих програм ……. 66

ВИСНОВКИ …….. 73

ПЕРЕЛІК ПОСИЛАНЬ 75

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 77

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

ACL – Access Control List

API – Application Programming Interface

APT – Advanced Persistent Threat

CDN – Content Delivery Network

CRS – Core Rule Sets

DDoS – Distributed Denial of Service

DNS – Domain Name System

EOP – Exchange Online Protection

IaaS – Infrastructure as a Service

ICMP – Internet Control Message Protocol

MFA – Multi-Factor Authentication

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. Офіс залишається серцем повсякденної роботи компанії – його відповідне функціонування є абсолютно необхідним. Сьогодні більшість офісних процесів відбувається в цифровому середовищі, тож програмне забезпечення має бути надійним та безпечним. Працівники часто використовують різноманітне програмне забезпечення, що призводить до проблем з ефективністю та безпекою. Пов'язаний, цілісний програмний пакет необхідний компаніям для того, щоби відповідати потребам сучасних офісів та справлятися з будь-якими викликами та задачами, які постають перед працівниками у щоденній роботі.

Програмний продукт Microsoft 365 задовольняє всі потреби, пов'язані з виконанням офісних задач впродовж робочого дня: від підготовки документів, створення презентацій, роботи з таблицями та розрахунками до керування календарем, комунікації у команді тощо. Microsoft 365 також забезпечує прямий доступ до даних, електронної пошти та зустрічей у віддаленому режимі. Microsoft 365 дозволяє користувачам одночасно працювати з документами в режимі реального часу та безпечно комунікувати з колегами та клієнтами за допомогою текстових чатів та дзвінків.

Сьогодні інформаційні ресурси організації різного роду по всьому світу зазнають кібератак зловмисників із використанням шкідливих програм та програм-вимагачів. Microsoft 365 містить механізми захисту, які запобігають проникненню шкідливого програмного забезпечення в клієнти або сервери Microsoft 365.

Використання програмного забезпечення для захисту від шкідливого програмного забезпечення є основним механізмом захисту активів Microsoft 365 від нього. Програмне забезпечення для захисту від шкідливого програмного забезпечення виявляє та запобігає проникненню комп’ютерних вірусів, шкідливого програмного забезпечення, руткітів, черв’яків та іншого шкідливого програмного забезпечення в будь-які сервісні системи. Програмне забезпечення для захисту забезпечує як превентивний, так і детективний контроль над

шкідливим програмним забезпеченням.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження технології захисту інформаційних ресурсів організації від шкідливих програм на прикладі Microsoft 365.

Об'єкт дослідження – захист інформаційних ресурсів організації від шкідливих програм.

Предмет дослідження – технологія захисту інформаційних ресурсів організації від шкідливих програм на прикладі Microsoft 365.

Мета роботи – розробити порядок застосування технології захисту інформаційних ресурсів організації від шкідливих програм та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми захисту інформаційних ресурсів організації від шкідливих програм;

проаналізувати підходи до захисту інформаційних ресурсів організації від шкідливих програм;

проаналізувати існуючі рішення із захисту інформаційних ресурсів організації від шкідливих програм;

проаналізувати методи та засоби захисту інформаційних ресурсів організації від шкідливих програм на прикладі Microsoft 365;

розкрити порядок реалізації технології захисту інформаційних ресурсів організації від шкідливих програм в Microsoft 365.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології захисту інформаційних ресурсів організації від шкідливих програм, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ ВІД ШКІДЛИВИХ ПРОГРАМ

1.1. Дослідження проблеми захисту інформаційних ресурсів організації від шкідливих програм та програм-вимагачів

Офіс залишається серцем повсякденної роботи компанії – його відповідне функціонування є абсолютно необхідним. Сьогодні більшість офісних процесів відбувається в цифровому середовищі, тож програмне забезпечення має працювати на найвищому рівні. Працівники часто використовують різноманітне програмне забезпечення, що призводить до проблем з ефективністю та безпекою. Пов'язаний, цілісний програмний пакет необхідний компаніям для того, щоби відповідати потребам сучасних офісів та справлятися з будь-якими викликами та задачам, які постають перед працівниками у щоденній роботі [1].

Microsoft 365 задовольняє всі потреби, пов'язані з виконанням офісних задач впродовж робочого дня: від підготовки документів, створення презентацій, роботи з таблицями та розрахунками до керування календарем, комунікації у команді тощо. ПЗ також забезпечує прямий доступ до даних, електронної пошти та зустрічей у віддаленому режимі. Microsoft 365 дозволяє користувачам одночасно працювати з документами в режимі реального часу та безпечно комунікувати з колегами та клієнтами за допомогою текстових чатів та дзвінків. Всі ці рішення пов'язані одне з одним [1].

Будь-які офісні процеси мають бути захищеними. Microsoft 365 надає безпечний спосіб керування даними та процесами, що відповідає вимогам до захисту даних.

За словами директора з кібербезпеки «Київстар» Юрія Прокопенка [2], кібератаки здатні унеможливити надання компаніями своїх послуг, зупинка яких може обійтися великому бізнесу від 300 тисяч до понад 1 мільйона доларів (рис.1.1).

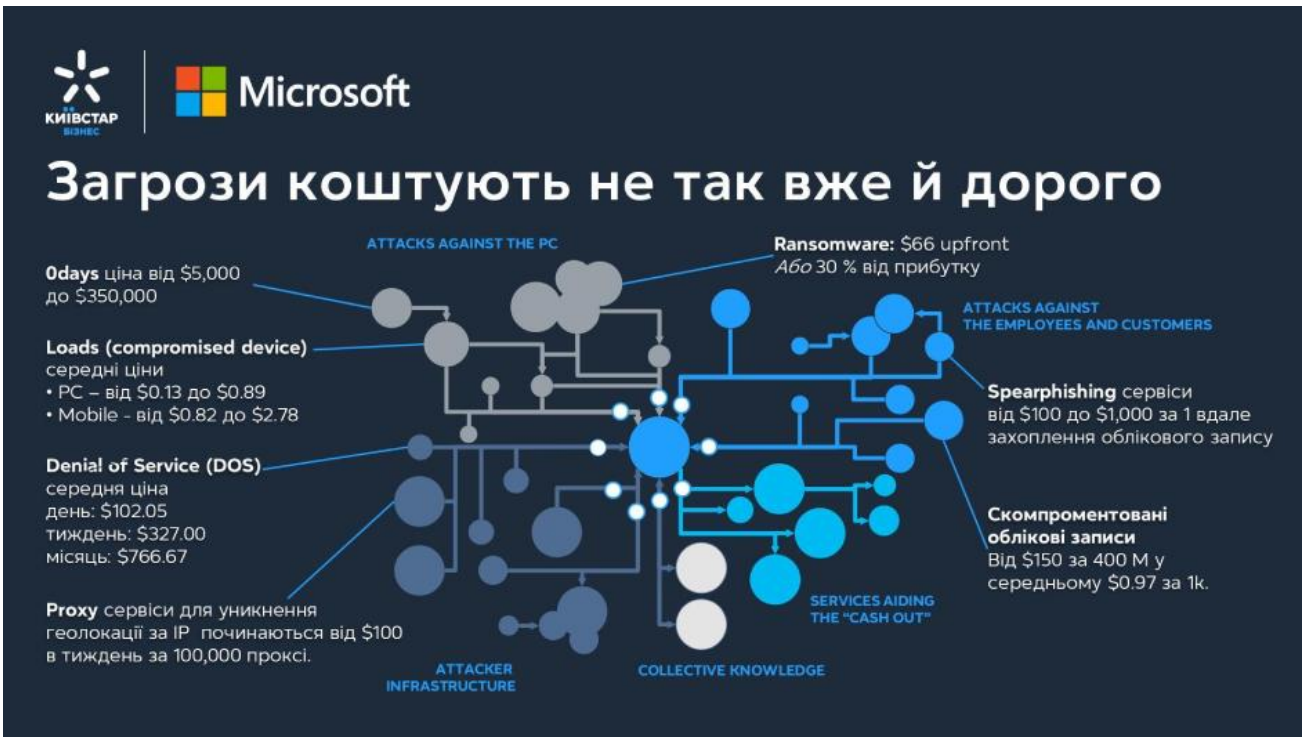

Рис. 1.1. Збитки організацій від кібератак [2]

Прикладами кібератак є фішингові листи, злам акаунтів і крадіжки особистих або корпоративних даних, програми, які приховують файли та блокують доступи. Під загрозою може опинитися будь-яка організація чи бізнес, не тільки великі компанії. Найчастіше хакерські атаки спрямовуються на державні установи, банки та інші фінансові організації, онлайн-магазини, IT-компанії, бізнес, що працює з персональними даними клієнтів, виробничі компанії, стартапи [2].

Програмне забезпечення-вимагач – це тип атаки здирництва, який знищує або шифрує файли та папки, запобігаючи доступу до критичних даних. Програмне забезпечення-вимагач зазвичай поширюється як вірус, який заражає пристрої та потребує лише усунення шкідливого програмного забезпечення. Програмне забезпечення-вимагач, яким керує людина, є результатом активної атаки кіберзлочинців, які проникають у локальну або хмарну IT-інфраструктуру організації, підвищують їхні привілеї та розгортають програмне забезпечення-вимагач на критично важливих даних [3].

Після завершення атаки зловмисник вимагає від жертви гроші в обмін на видалені файли, ключі для зашифрованих файлів або обіцянку не розкривати

конфіденційні дані. Програми-вимагачі, якими керує людина, також можуть використовуватися для зупинки критично важливих машин або процесів, таких як ті, що потрібні для промислового виробництва, зупиняючи звичайні бізнес-операції, доки не буде сплачено викуп і не буде виправлено збиток, або організація самостійно усуне збитки [3].

Атака програми-вимагача, яка керована людиною, може мати катастрофічні наслідки для підприємств будь-якого розміру. Її важко очистити, вимагаючи повного усунення зловмисника для захисту від майбутніх атак. На відміну від програм-вимагачів, керованих людьми, вони можуть продовжувати загрожувати діяльності бізнесу після початкового запиту викупу [3].

Шкідливий код – це небажані файли або програми, які можуть завдати шкоди комп’ютеру або скомпрометувати дані, що зберігаються на комп’ютері. Різні класифікації шкідливого коду включають віруси, хробаки та троянські програми [6].

Віруси мають здатність пошкоджувати або знищувати файли в комп’ютерній системі та поширюються шляхом спільного використання вже зараженого знімного носія, відкриття шкідливих вкладень електронної пошти та відвідування шкідливих веб-сторінок.

Хробаки – це тип вірусу, який самостійно поширюється від комп'ютера до комп'ютера. Його функція полягає у використанні всіх ресурсів вашого комп’ютера, що може призвести до того, що комп’ютер перестане відповідати.

Троянські коні – це комп’ютерні програми, які приховують вірус або потенційно шкідливу програму. Нерідко безкоштовне програмне забезпечення містить троянський кінь, який змушує користувача думати, що він використовує законне програмне забезпечення, натомість програма виконує шкідливі дії на вашому комп’ютері.

Шкідливі файли даних – це невиконувані файли, як-от документ Microsoft Word, Adobe PDF, ZIP-файл або файл зображення, які використовують слабкі місця програмного забезпечення, що використовується для їх відкриття. Зловмисники часто використовують шкідливі файли даних для встановлення

шкідливого програмного забезпечення в систему жертви, зазвичай розповсюджуючи файли електронною поштою, соціальними мережами та веб-сайтами [6].

У звіті Sophos [7] зазначалося, що кількість кібератак зростає, а їхня складність і вплив зростають. 66% організацій постраждали від програм-вимагачів минулого року (рис. 1.2), порівняно з 37% у 2020 році. Це зростання на 78% протягом року, що свідчить про те, що стало значно більше зловмисників здатних здійснювати найбільш масштабні атаки.

Зловмисники також стали більш успішними у шифруванні даних під час своїх атак. У 2021 році зловмисникам вдалося зашифрувати дані в 65% атак (рис. 1.2), що більше, ніж у 2020 році, коли рівень шифрування становив 54%. Проте відсоток жертв, які зазнали атаки лише з метою вимагання, зменшився з 7% до 4%. дані не були зашифровані, але організацію вимагали викуп із загрозою розкриття даних [7].

Збільшення кількості успішних атак програм-вимагачів є частиною дедалі складнішого ширшого середовища загроз: за останній рік 57% зазнали збільшення загального обсягу кібератак, 59% помітили збільшення складності атак, а 53% сказали, що вплив атак мав збільшився. 72% помітили зростання принаймні в одній із цих сфер (рис. 1.2) [7].

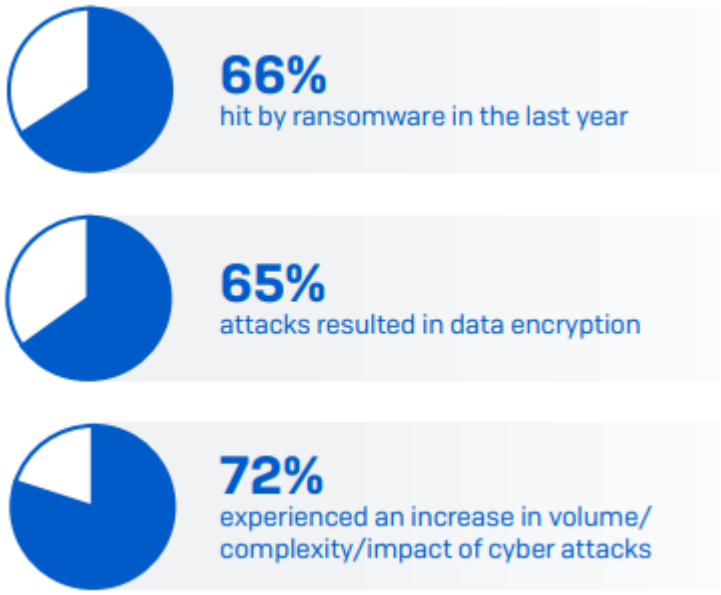

Рис. 1.2. Дані щодо атак програм-вимагачів [7]

Microsoft [8] підкреслює, що кіберзлочинці розробляють дедалі складніші схеми та методи, щоб знищити налаштування безпеки та націлитися на окремих осіб, компанії та організації.

Щоб зменшити ризик фішингу для організації, Microsoft [8] рекомендує адміністраторам запровадити такі політики та функції:

вимагати використання MFA для всіх облікових записів, щоб обмежити неавторизований доступ;

увімкнути функції умовного доступу для облікових записів із високим рівнем привілеїв, щоб заблокувати доступ із країн, регіонів та IP-адрес, які зазвичай не генерують трафік у вашій організації;

розглянути можливість використання фізичних ключів безпеки для керівників, співробітників, які беруть участь у платежах або купівлі, та інших привілейованих облікових записів;

примусово використовувати браузери, які підтримують такі служби, як Microsoft SmartScreen, для аналізу URL-адрес на наявність підозрілої поведінки та блокування доступу до відомих шкідливих веб-сайтів;

використовувати рішення безпеки на основі машинного навчання, яке поміщає в карантин високоймовірний фішинг і підриває URL-адреси та вкладення в пісочниці до того, як електронна пошта потрапить до папки "Вхідні", як-от Microsoft Defender для Office 365.

Однією з причин розповсюдження ботнетів є скомпрометовані маршрутизатори MikroTik.

Так, оператори Trickbot використовують скомпрометовані маршрутизатори MikroTik і переконфігурують їх, щоб діяти як частина їхньої інфраструктури C2. Популярність цих пристроїв посилює серйозність зловживань ними з боку Trickbot, а їх унікальне апаратне та програмне забезпечення дозволяє суб’єктам загроз уникати традиційних заходів безпеки, розширювати свою інфраструктуру та скомпрометувати більше пристроїв і мереж [8].

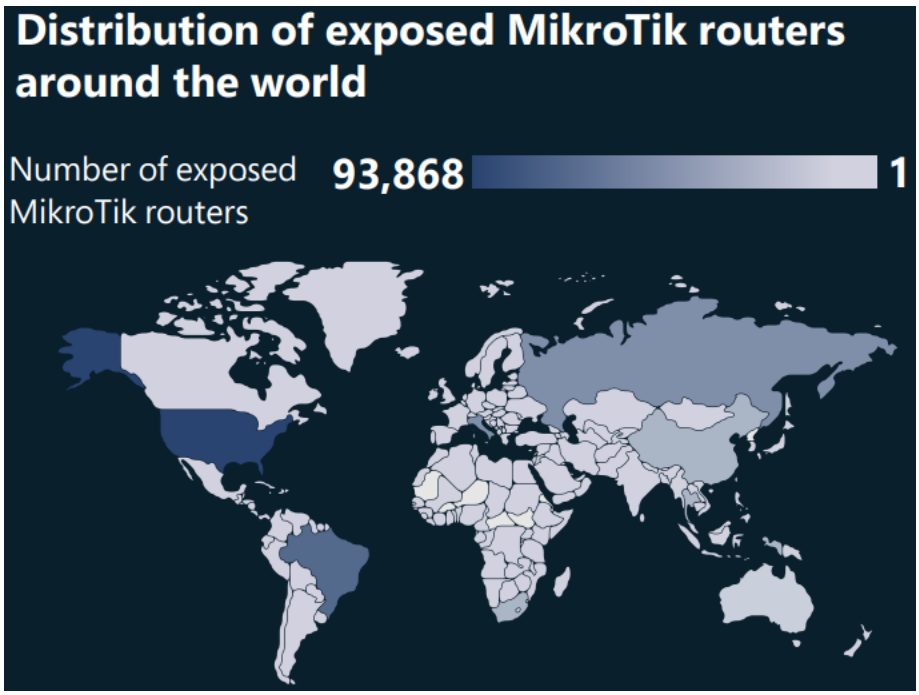

Рис. 1.3. Розповсюдження відкритих маршрутизаторів MikroTik [8]

Відстежуючи та аналізуючи трафік, що містить команди безпечної оболонки (Secure SHell, SSH), можна спостерігали, як зловмисники використовують маршрутизатори MikroTik для зв'язку з інфраструктурою Trickbot після отримання законних облікових даних для пристроїв.

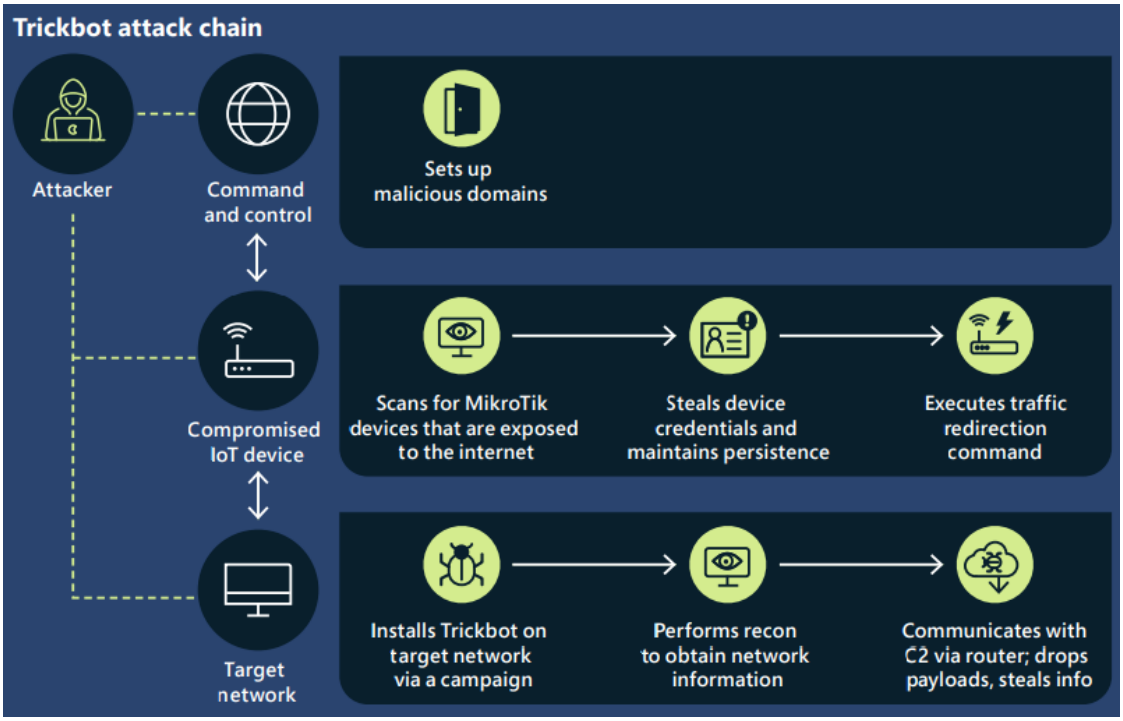

Рис. 1.4. Ланцюг атаки Trickbot [8]

Ці облікові дані можна отримати за допомогою атак грубої сили, використання відомих уразливостей за допомогою легкодоступних патчів і використання паролів за замовчуванням.

Після доступу до пристрою зловмисник видає унікальну команду, яка перенаправляє трафік між двома портами маршрутизатора, встановлюючи лінію зв'язку між ураженими Trickbot пристроями та C2. Ланцюжок атаки Trickbot показано на рисунку 1.4.

Отже, проблема захисту інформаційних ресурсів організації від шкідливих програм та програм-вимагачів немає остаточного вирішення.

1.2. Аналіз підходів до захисту інформаційних ресурсів організації від шкідливих програм

Антивірусне програмне забезпечення сканує комп'ютерні файли та пам'ять на наявність шаблонів, які вказують на можливу присутність шкідливого коду. Антивірусне сканування можна проводити автоматично або вручну [6].

Автоматичне сканування – більшість антивірусних програм можуть автоматично сканувати певні файли чи каталоги. Нова інформація про віруси додається часто, тому варто скористатися цією опцією.

Сканування вручну. Якщо ваше антивірусне програмне забезпечення не сканує автоматично нові файли, вам слід вручну сканувати файли та медіафайли, які ви отримуєте із зовнішнього джерела, перш ніж відкривати їх, зокрема вкладення електронної пошти, веб-завантаження, компакт-диски, DVD-диски та USB-диски [6].

Незважаючи на те, що антивірусне програмне забезпечення може бути потужним засобом захисту комп'ютера, іноді воно може спричиняти проблеми, перешкоджаючи роботі комп'ютера. Надлишок антивірусного програмного забезпечення може вплинути на продуктивність комп'ютера та ефективність програмного забезпечення.

Шкідливе програмне забезпечення, також відоме як зловмисний код, відноситься до програми, яка таємно вставлена в іншу програму з наміром знищити дані, запустити деструктивні чи нав’язливі програми або іншим чином порушити конфіденційність, цілісність або доступність даних жертви, програм або операційна система. Шкідливе програмне забезпечення є найпоширенішою зовнішньою загрозою для більшості хостів, спричиняючи значну шкоду та збої та потребуючи значних зусиль щодо відновлення в більшості організацій [5].

Організації також стикаються з подібними загрозами від кількох форм нешкідливого програмного забезпечення, які часто пов’язані зі зловмисним програмним забезпеченням. Однією з цих форм, що стала звичним явищем, є фішинг, який використовує оманливі комп’ютерні засоби, щоб обманом змусити людей розкрити конфіденційну інформацію.

На відміну від більшості загроз шкідливого програмного забезпечення кілька років тому, яке, як правило, швидко поширювалося та було легко помітити, багато сучасних загроз шкідливого програмного забезпечення більш приховані, спеціально розроблені для тихого, повільного поширення на інші хости, збираючи інформацію протягом тривалих періодів часу та зрештою призводячи до викрадання конфіденційних даних та інших негативних впливів.

Організації повинні мати надійні можливості процесу реагування на інциденти, які стосуються обробки інцидентів шкідливого програмного забезпечення. *Процес реагування на інциденти має чотири основні фази: підготовка, виявлення та аналіз, стримування/ліквідація/відновлення та діяльність після інциденту.*

Організації повинні виконати підготовчі заходи, щоб забезпечити ефективну реакцію на випадки шкідливого програмного забезпечення. Рекомендовані дії включають:

формування та підтримку навичок, пов’язаних зі зловмисним програмним забезпеченням, у групі реагування на інциденти;

сприяння комунікації та координації в усій організації;

придбання необхідних інструментів (апаратного та програмного

забезпечення) і ресурсів для допомоги в обробці інцидентів зі зловмисним програмним забезпеченням.

Організації повинні прагнути швидко виявляти та перевіряти інциденти зі зловмисним програмним забезпеченням, щоб мінімізувати кількість заражених хостів і розмір збитку, який зазнає організація. Рекомендовані дії включають:

аналіз будь-якого ймовірного інциденту шкідливого програмного забезпечення та підтвердження того, що шкідливе програмне забезпечення є причиною. Це включає визначення характеристик активності шкідливого програмного забезпечення шляхом вивчення джерел виявлення, таких як антивірусне програмне забезпечення, системи запобігання вторгненням і технології безпеки та керування подіями (SIEM);

визначення хостів, заражених шкідливим програмним забезпеченням, щоб хости могли пройти відповідні дії зі стримування, видалення та відновлення. Виявлення заражених хостів часто ускладнюється динамічною природою шкідливого програмного забезпечення та обчислень. Організаціям слід ретельно розглянути питання ідентифікації хостів до того, як станеться масштабний інцидент зі зловмисним програмним забезпеченням, щоб вони були готові використовувати кілька стратегій для ідентифікації заражених хостів у рамках своїх заходів із стримування. Організаціям слід вибрати достатньо широкий діапазон підходів до ідентифікації та розробити процедури та технічні можливості для ефективного виконання кожного вибраного підходу, коли відбувається серйозний інцидент шкідливого програмного забезпечення;

пріоритезація обробки кожного інциденту;

вивчення поведінки шкідливого програмного забезпечення шляхом його активного аналізу (виконання шкідливого програмного забезпечення) або криміналістичного (перевірка зараженого хоста на наявність шкідливих програм).

Стримування інцидентів шкідливого програмного забезпечення складається з двох основних компонентів: припинення поширення шкідливого програмного забезпечення та запобігання подальшому пошкодженню хостів.

Майже кожен інцидент зі зловмисним програмним забезпеченням потребує

стримування. При вирішенні інциденту важливо, щоб організація вирішила, які методи стримування застосувати спочатку, на початку реагування. Організації повинні мати стратегії та процедури для прийняття рішень щодо стримування, які відображають рівень ризику, прийнятний для організації. Стратегії стримування повинні підтримувати обробників інцидентів у виборі відповідної комбінації методів стримування на основі характеристик конкретної ситуації. Конкретні рекомендації, пов'язані зі стримуванням, включають наступне:

може бути корисно надати користувачам інструкції про те, як ідентифікувати інфекції та які заходи вжити, якщо хост інфікований; однак організації не повинні покладатися насамперед на користувачів у стримуванні інцидентів шкідливого програмного забезпечення;

якщо шкідливе програмне забезпечення не може бути виявлено та локалізовано за допомогою оновленого антивірусного програмного забезпечення, організації повинні бути готові використовувати інші інструменти безпеки для його стримування. Організації також повинні бути готові надіслати копії невідомого шкідливого програмного забезпечення своїм постачальникам програмного забезпечення безпеки для аналізу, а також зв'язатися з довіреними сторонами, такими як організації з реагування на інциденти та постачальники антивірусних програм, коли потрібні вказівки щодо обробки нових загроз;

організації повинні бути готові вимкнути або заблокувати служби, які використовують шкідливе програмне забезпечення для стримування інциденту, і повинні розуміти наслідки цього. Організації також повинні бути готові реагувати на проблеми, спричинені іншими організаціями, які відключають їхні власні служби у відповідь на інцидент шкідливого програмного забезпечення;

організації повинні бути готові накласти додаткові тимчасові обмеження на підключення до мережі, щоб стримати інцидент шкідливого програмного забезпечення, наприклад призупинення доступу до Інтернету або фізичне відключення хостів від мереж, усвідомлюючи вплив, який обмеження можуть мати на організаційні функції.

Основною метою викорінення є видалення шкідливих програм із заражених

хостів. Через потенційну потребу в значних зусиллях з ліквідації, організації повинні бути готові використовувати різні комбінації методів ліквідації одночасно для різних ситуацій.

Організаціям також слід розглянути можливість проведення заходів з підвищення обізнаності, які встановлюють очікування щодо зусиль з ліквідації та відновлення; ці дії можуть бути корисними для зменшення стресу, який можуть спричинити серйозні випадки шкідливого програмного забезпечення.

Двома основними аспектами відновлення після інцидентів шкідливого програмного забезпечення є відновлення функціональності та даних заражених хостів і скасування тимчасових заходів стримування. Організаціям слід ретельно розглянути можливі найгірші сценарії та визначити, як слід виконувати відновлення, включаючи відновлення скомпрометованих хостів з нуля або завідомо хороших резервних копій. Під час серйозних інцидентів зі зловмисним програмним забезпеченням часто важко визначити час скасування тимчасових заходів стримування, таких як призупинення послуг або з’єднання.

Групи реагування на інциденти повинні прагнути підтримувати заходи стримування, доки розрахункова кількість інфікованих хостів і хостів, вразливих до інфекції, не стане достатньо низькою, щоб наступні інциденти не мали великих наслідків. Однак, незважаючи на те, що група реагування на інциденти повинна оцінити ризики відновлення послуг або підключення, керівництво в кінцевому підсумку має нести відповідальність за визначення того, що слід зробити на основі рекомендацій групи реагування на інциденти та розуміння керівництвом впливу на бізнес збереження заходів стримування.

Оскільки обробка інцидентів зі зловмисним програмним забезпеченням може бути надзвичайно дорогою, для організацій особливо важливо проводити надійну оцінку уроків, отриманих після серйозних інцидентів зі зловмисним програмним забезпеченням, щоб запобігти виникненню подібних інцидентів. Отримання досвіду, отриманого під час обробки таких інцидентів, має допомогти організації покращити свої можливості обробки інцидентів і захисту від шкідливого програмного забезпечення, включаючи визначення необхідних змін у

політиці безпеки, конфігураціях програмного забезпечення та розгортанні програмного забезпечення для виявлення та запобігання зловмисному програмному забезпеченню.

Шкідливе програмне забезпечення, також відоме як зловмисний код, відноситься до програми, яка таємно вставлена в іншу програму з наміром знищити дані, запустити деструктивні чи нав'язливі програми або іншим чином порушити конфіденційність, цілісність або доступність даних жертви, програм або операційна система. Шкідливе програмне забезпечення є найпоширенішою зовнішньою загрозою для більшості хостів, спричиняючи значну шкоду та збої та потребуючи значних зусиль щодо відновлення в більшості організацій.

Розглянемо інструменти зловмисників.

Різні типи інструментів зловмисників можуть бути доставлені на хост через шкідливе програмне забезпечення. Ці інструменти дозволяють зловмисникам мати несанкціонований доступ або використовувати заражені хости та їхні дані, або здійснювати додаткові атаки. Популярні типи інструментів зловмисників:

бекдори. Бекдор – це шкідлива програма, яка прослуховує команди на певному порту TCP або UDP. Більшість бекдорів дозволяють зловмиснику виконувати певний набір дій на хості, наприклад отримувати паролі або виконувати довільні команди. Типи бекдорів включають зомбі (більш відомі як боти), які встановлюються на хост, щоб змусити його атакувати інші хости, і інструменти віддаленого адміністрування, які встановлюються на хості, щоб дозволити віддаленому зловмиснику отримати доступ до функцій хосту та дані за потреби;

реєстратори натискань клавіш. Реєстратор натискань клавіш відстежує та записує використання клавіатури. Деякі вимагають, щоб зловмисник отримав дані з хоста, тоді як інші реєстратори активно передають дані на інший хост через електронну пошту, передачу файлів або іншими способами;

руткіти. Руткіт – це набір файлів, які встановлюються на хості для зміни його стандартних функцій зловмисним і прихованим способом. Руткіт зазвичай вносить багато змін у хост, щоб приховати існування руткіта, що ускладнює

визначення наявності руткіта та визначення того, що руткіт змінив;

плагіни веб-браузера. Модуль веб-браузера надає спосіб відображення або виконання певних типів вмісту через веб-браузер. Шкідливі плагіни веб-переглядача можуть відстежувати використання браузера;

генератори електронної пошти. Програму генерації електронної пошти можна використовувати для створення та надсилання великої кількості електронних листів, таких як шкідливе програмне забезпечення та спам, на інші хости без дозволу або відома користувача;

набори інструментів для зловмисників. Багато зловмисників використовують набори інструментів, що містять кілька різних типів утиліт і сценаріїв, які можна використовувати для зондування та атаки на хости, наприклад сніфери пакетів, сканери портів, сканери вразливостей, зломщики паролів, а також програми та сценарії для атаки.

Розглянемо природу сучасного шкідливого програмного забезпечення.

Характерною рисою сучасного шкідливого програмного забезпечення, яка найбільше відрізняє його від попередніх поколінь шкідливого програмного забезпечення, є ступінь його налаштування. Для зловмисників стало тривіальним створення власного шкідливого програмного забезпечення, придбання наборів шкідливих програм, таких як Zeus, SpyEye і Poison Ivy, і налаштування шкідливого програмного забезпечення, створеного цими наборами інструментів, відповідно до їхніх індивідуальних потреб. Багато з цих наборів інструментів доступні для придбання, тоді як інші мають відкритий вихідний код, і більшість із них мають зручні інтерфейси, які дозволяють некваліфікованим зловмисникам легко створювати налаштоване шкідливе програмне забезпечення з високими можливостями.

Багато зловмисників додатково налаштовують своє шкідливе програмне забезпечення, пристосовуючи кожен екземпляр шкідливого програмного забезпечення до конкретної особи чи невеликої групи людей. Наприклад, багато зловмисників збирають інформацію через соціальні мережі, а потім використовують цю інформацію про приналежність і стосунки для створення

ефективних атак соціальної інженерії.

Налаштування шкідливого програмного забезпечення створює значні проблеми для виявлення шкідливого програмного забезпечення, оскільки воно значно збільшує різноманітність шкідливого програмного забезпечення, яке антивірусне програмне забезпечення та інші засоби захисту повинні виявляти та блокувати.

Коли зловмисники здатні надіслати унікальну атаку кожній потенційній жертві, не варто дивуватися тому, що засоби безпеки, які здебільшого базуються на сигнатурах, наприклад антивірусне програмне забезпечення, не встигають за ними. Пом’якшення передбачає підхід до глибокого захисту з використанням кількох різних методів виявлення, щоб збільшити ймовірність того, що принаймні один із них зможе виявити зловмисну поведінку налаштованого шкідливого програмного забезпечення.

Ще однією важливою характеристикою сучасного шкідливого програмного забезпечення є його прихований характер. Більшість сучасних зловмисних програм спеціально розроблено для тихого, повільного поширення на інші хости, збираючи інформацію протягом тривалих періодів часу та зрештою призводячи до викрадання конфіденційних даних та інших негативних наслідків.

Для позначення таких типів шкідливого програмного забезпечення зазвичай використовується термін «розширені стійкі загрози» (APT). APT можуть здійснювати стеження тижнями, місяцями чи навіть роками, потенційно завдаючи значної шкоди організації лише однією компрометацією.

Також відомо, що APT важко видалити з хостів, часто потрібно перевстановити операційну систему та програми хоста та відновити всі дані з відомих резервних копій.

Таким чином, сучасне шкідливе програмне забезпечення часто важче виявити, завдає більшої шкоди та важче видалити, ніж шкідливе програмне забезпечення попередніх поколінь. І немає жодних ознак того, що ця еволюція закінчилася. Коли найскладніші сучасні проблеми шкідливого програмного забезпечення стануть рутинною справою, очікуйте появи нових проблем.

1.3. Аналіз існуючих рішень із захисту інформаційних ресурсів організації від шкідливих програм

Шкідливе програмне забезпечення часто атакує хости, використовуючи вразливості в операційних системах, службах і програмах. Отже, пом’якшення вразливостей є дуже важливим для запобігання інцидентам зі зловмисним програмним забезпеченням, особливо коли шкідливе програмне забезпечення випускається незабаром після оголошення про нову вразливість або навіть до того, як уразливість визнається публічно [5].

Вразливість зазвичай можна пом’якшити одним або декількома методами, наприклад застосуванням патчів для оновлення програмного забезпечення або перенастроюванням програмного забезпечення (наприклад, вимкненням вразливої служби). З огляду на проблеми, пов’язані з пом’якшенням вразливості, включаючи постійне виявлення нових вразливостей, організації повинні мати задокументовану політику, процеси та процедури для пом’якшення вразливості. Організаціям слід розглянути можливість використання технологій автоматизації безпеки з контрольними списками конфігурації ОС і програм, щоб допомогти адміністраторам постійно й ефективно захищати хости [5].

Технології автоматизації безпеки можуть використовувати контрольні списки для застосування параметрів конфігурації, які покращують рівень безпеки за замовчуванням, і для постійного моніторингу параметрів хостів, щоб переконатися, що вони все ще відповідають параметрам контрольного списку.

Організаціям також слід розглянути можливість використання технологій автоматизації безпеки для управління виправленнями ОС і додатків – для виявлення, отримання, розповсюдження та встановлення виправлень, пов’язаних із безпекою, щоб пом’якшити вразливі місця, на які виправлення звертаються.

Організації повинні дотримуватися *принципу найменших привілеїв*, який стосується налаштування хостів для надання лише мінімально необхідних прав відповідним користувачам, процесам і хостам. Найменші привілеї можуть бути

корисними для запобігання інцидентам шкідливого програмного забезпечення, оскільки шкідливе програмне забезпечення часто потребує прав адміністратора для успішного використання вразливостей [5].

Якщо інцидент все ж трапиться, попереднє застосування найменших привілеїв може мінімізувати кількість збитків, які може завдати шкідливе програмне забезпечення. Організації також повинні впровадити інші заходи захисту хостів, які можуть ще більше зменшити ймовірність інцидентів шкідливого програмного забезпечення, наприклад [5]:

вимкнення або видалення непотрібних служб (зокрема мережевих), які є додатковими векторами, які шкідливі програми можуть використовувати для поширення;

усунення незахищених спільних файлів, які є поширеним способом розповсюдження шкідливого програмного забезпечення;

видалення або зміна імен користувачів і паролів за замовчуванням для ОС і програм, які можуть використовуватися зловмисним програмним забезпеченням для отримання неавторизованого доступу до хостів;

вимкнення автоматичного виконання двійкових файлів і сценаріїв, включаючи автозапуск на хостах Windows;

зміна асоціацій файлів за замовчуванням для типів файлів, які найчастіше використовуються зловмисним програмним забезпеченням, але не користувачами (наприклад, .pif, .vbs), щоб такі файли не запускалися автоматично, якщо користувачі намагаються їх відкрити.

Захист хосту також має включати програми, такі як клієнти електронної пошти, веб-браузери та текстові процесори, які часто є мішенню шкідливого програмного забезпечення.

Організаціям слід вимикати непотрібні функції та можливості цих програм, особливо ті, які зазвичай використовують шкідливе програмне забезпечення, щоб обмежити можливі вектори атак шкідливого програмного забезпечення. Одним із прикладів є використання макросів текстовими процесорами та електронними таблицями. Більшість поширених програм із можливостями макросів пропонують

функції захисту макросів, які дозволяють макроси лише з надійних місць або пропонують користувачеві схвалити чи відхилити кожну спробу запуску макросу, таким чином зменшуючи ймовірність інфікування макросами зловмисним програмним забезпеченням.

Іншим прикладом є запобігання інсталяції програмного забезпечення у веб-браузерах шляхом налаштування браузерів на заборону інсталяції плагінів або прохання користувачів схвалити встановлення кожного плагіна.

Можливість швидко змінювати налаштування конфігурації програми може бути дуже корисною для швидкого усунення вразливостей, включаючи тимчасові заходи з усунення. Наприклад, зміна конфігурації може тимчасово вимкнути вразливу службу, поки постачальник служби готує та випускає патч, який остаточно усуває вразливість. Коли виправлення стане доступним і розгорнуто, організація може скасувати зміну конфігурації, щоб повторно активувати службу, яка більше не є вразливою.

Організації повинні заздалегідь розглянути, як можна змінити параметри конфігурації у відповідь на надзвичайну ситуацію шкідливого програмного забезпечення, а також встановити та підтримувати відповідні процедури.

Організації повинні виконувати пом’якшення загроз, щоб виявити та зупинити шкідливе програмне забезпечення, перш ніж воно зможе вплинути на свої цілі. Навіть якщо практично всі вразливості в хості пом’якшено, пом’якшення загроз все ще є критично важливим, наприклад, для зупинки шкідливого програмного забезпечення, яке не використовує вразливості, наприклад атак, які покладаються на методи соціальної інженерії, щоб змусити користувачів запустити шкідливі файли.

Пом’якшення загрози також має вирішальне значення для ситуацій, коли велика ймовірність того, що нова загроза незабаром атакує організацію, і організація не має прийнятного варіанту пом’якшення вразливості. Наприклад, може не бути доступного патча для нової вразливості.

Існує кілька типів інструментів безпеки, які можуть пом’якшити загрози шкідливого програмного забезпечення: антивірусне програмне забезпечення,

системи запобігання вторгненням (IPS), брандмауери, фільтрація/перевірка вмісту та білий список програм.

Антивірусне програмне забезпечення є найпоширенішим технічним засобом захисту від шкідливих програм. Існує багато марок антивірусного програмного забезпечення, більшість з яких забезпечує подібний захист за допомогою таких рекомендованих можливостей [5]:

сканування критичних компонентів хоста, таких як файли запуску та завантажувальні записи;

перегляд дій на хостах у режимі реального часу для виявлення підозрілої активності. Поширеним прикладом є сканування всіх вкладень електронної пошти на наявність відомого шкідливого програмного забезпечення під час надсилання та отримання електронних листів. Антивірусне програмне забезпечення має бути налаштовано на виконання сканування кожного файлу в режимі реального часу під час його завантаження, відкриття або виконання, що називається скануванням під час доступу; відстеження поведінки звичайних програм, таких як клієнти електронної пошти, веб-браузери та програмне забезпечення для обміну миттєвими повідомленнями. Антивірусне програмне забезпечення має відстежувати активність програм, які, швидше за все, будуть використані для зараження хостів або розповсюдження шкідливого програмного забезпечення на інші хости;

сканування файлів на наявність шкідливих програм. Антивірусне програмне забезпечення на хостах має бути налаштовано на регулярне сканування всіх жорстких дисків для виявлення заражень файлової системи та, за бажанням, залежно від потреб організації в безпеці, сканування знімних носіїв, вставлених у хост, перш ніж дозволити їх використання. Користувачі також повинні мати можливість запускати сканування вручну за потреби, що називається скануванням за вимогою;

виявлення поширених типів шкідливих програм, а також інструментів зловмисників;

дезінфекція файлів, яка стосується видалення шкідливого програмного

забезпечення з файлу, і розміщення файлів на карантині, що означає, що файли, які містять шкідливе програмне забезпечення, зберігаються ізольовано для подальшої дезінфекції або перевірки. Лікувати файл, як правило, краще, ніж помістити його на карантин, оскільки шкідливе програмне забезпечення видаляється, а вихідний файл відновлюється; однак багато інфікованих файлів неможливо вилікувати. Відповідно, антивірусне програмне забезпечення має бути налаштовано на спробу вилікувати заражені файли та поміщати в карантин або видаляти файли, які не можна вилікувати.

Організації повинні використовувати антивірусне сканування як на базі хоста, так і на основі мережі. Організації повинні розгортати антивірусне програмне забезпечення на всіх хостах, для яких доступне відповідне антивірусне програмне забезпечення. Антивірусне програмне забезпечення слід установити якомога швидше після встановлення ОС, а потім оновити останніми сигнатурами та виправленнями антивірусного програмного забезпечення (щоб усунути будь-які відомі вразливості самого антивірусного програмного забезпечення).

Потім антивірусне програмне забезпечення має виконати повне сканування хоста, щоб виявити потенційні інфекції. Щоб підтримувати безпеку хоста, антивірусне програмне забезпечення має бути належним чином налаштовано та підтримувано, щоб воно й надалі було ефективним у виявленні та зупинці шкідливого програмного забезпечення. Антивірусне програмне забезпечення є найефективнішим, якщо його сигнатури повністю оновлені. Відповідно, антивірусне програмне забезпечення має підтримуватися в актуальному стані з останніми сигнатурами та оновленнями програмного забезпечення для покращення виявлення шкідливого програмного забезпечення.

Організації повинні використовувати антивірусне програмне забезпечення з централізованим керуванням, яке регулярно контролюється та контролюється антивірусними адміністраторами, які також зазвичай відповідають за отримання, тестування, затвердження та доставку антивірусних сигнатур і оновлень програмного забезпечення в усій організації. Користувачі не повинні мати можливість вимкнути або видалити антивірусне програмне забезпечення зі своїх

хостів, а також вони не повинні мати можливість змінювати критичні налаштування.

Адміністратори антивірусної програми повинні здійснювати постійний моніторинг, щоб підтвердити, що хости використовують поточне антивірусне програмне забезпечення та чи програмне забезпечення налаштоване належним чином. Реалізація всіх цих рекомендацій має суттєво підтримати організацію в забезпеченні надійного та послідовного розгортання антивірусної програми в усій організації.

Можливим заходом для покращення захисту від шкідливого програмного забезпечення є використання кількох антивірусних продуктів для ключових хостів, наприклад серверів електронної пошти. Наприклад, один постачальник антивірусної програми може мати нову сигнатуру, доступну за кілька годин до іншого постачальника, або організація може мати операційну проблему з певним оновленням сигнатури. Інша можливість полягає в тому, що сам антивірусний продукт може містити вразливість, яку можна використовувати; наявність альтернативного продукту в таких випадках може забезпечити захист, доки не буде вирішено проблему з основним продуктом.

Оскільки одночасний запуск кількох антивірусних продуктів на одному хості може спричинити конфлікти між продуктами, якщо декілька продуктів використовуються одночасно, їх слід інсталювати на окремих хостах. Наприклад, один антивірусний продукт можна використовувати на периметральних серверах електронної пошти, а інший – на внутрішніх серверах електронної пошти. Це могло б забезпечити більш ефективне виявлення нових загроз, але також вимагало б посиленого адміністрування та навчання, а також додаткових витрат на обладнання та програмне забезпечення.

Хоча антивірусне програмне забезпечення стало необхідністю для запобігання інцидентам шкідливого програмного забезпечення, антивірусне програмне забезпечення не може зупинити всі інциденти шкідливого програмного забезпечення.

Недоліком є те, що антивірусне програмне забезпечення не справляється з

невідомими раніше загрозами. Антивірусні програмні продукти виявляють шкідливе програмне забезпечення насамперед шляхом пошуку певних характеристик відомих екземплярів шкідливого програмного забезпечення. Це дуже ефективно для виявлення відомого шкідливого програмного забезпечення, але не настільки ефективне для виявлення настроюваного шкідливого програмного забезпечення, яке використовується все частіше.

Мережеві системи запобігання вторгненням (IPS) виконують перехоплення пакетів і аналізують мережевий трафік, щоб виявити та зупинити підозрілу активність. Мережеві продукти IPS зазвичай розгортаються вбудовано, що означає, що програмне забезпечення діє як мережевий брандмауер. Він приймає пакети, аналізує їх і пропускає прийнятні пакети.

Мережева архітектура IPS дозволяє виявляти деякі атаки в мережах до того, як вони досягнуть намічених цілей. Більшість мережевих продуктів IPS використовують комбінацію сигнатур атак і аналізу мережевих і програмних протоколів, що означає, що вони порівнюють мережеву активність програм, які часто атакуються (наприклад, сервери електронної пошти, веб-сервери), з очікуваною поведінкою, щоб визначити потенційно зловмисну активність.

Мережеві продукти IPS використовуються для виявлення багатьох типів зловмисної діяльності, окрім шкідливого програмного забезпечення, і зазвичай за замовчуванням можуть виявляти лише кілька екземплярів шкідливого програмного забезпечення, наприклад нещодавніх основних черв’яків. Однак деякі продукти IPS можна налаштувати, що дозволяє адміністраторам створювати та розгортати сигнатури атак для багатьох нових основних загроз шкідливого програмного забезпечення за лічені хвилини. Незважаючи на те, що це пов’язано з ризиком, наприклад, погано написана сигнатура викликає хибні спрацьовування, які ненавмисно блокують доброякісну активність, спеціальна сигнатура може блокувати нову загрозу шкідливого програмного забезпечення за години до того, як сигнатури антивірусу стануть доступними.

Мережеві продукти IPS можуть бути ефективними для припинення певних відомих загроз, таких як черв’яки мережевих служб і шкідливе програмне

забезпечення, що передається електронною поштою, з легко розпізнаваними характеристиками (наприклад, тема, назва файлу вкладення). Інша форма IPS, відома як система аналізу поведінки мережі (NBA), намагається зупинити атаки шляхом визначення незвичних потоків мережевого трафіку.

Хоча ці продукти в основному призначені для припинення розподілених атак типу «відмова в обслуговуванні» (DDoS) проти організації, їх також можна використовувати для виявлення активності хробаків та інших форм шкідливого програмного забезпечення, а також використання інструментів зловмисників, таких як бекдори та генератори електронної пошти.

Система NBA зазвичай працює шляхом моніторингу звичайних шаблонів мережевого трафіку, включно з тим, які хости спілкуються один з одним, використовуючи які протоколи, а також типовий і піковий обсяг активності, щоб встановити базові показники. Потім програмне забезпечення відстежує мережеву активність, щоб виявити значні відхилення від базових показників. Якщо шкідливе програмне забезпечення спричиняє особливо великий обсяг мережевого трафіку або використовує мережеві протоколи або протоколи додатків, які зазвичай не використовуються, система NBA повинна мати можливість виявити та, якщо розгорнуто вбудовано, заблокувати активність [5].

Ще один спосіб обмежити деякі інциденти шкідливого програмного забезпечення – налаштувати мережеві пристрої для обмеження максимальної пропускної здатності, яка може використовуватися окремими хостами або службами. Крім того, деякі типи програмного забезпечення для моніторингу мережі можуть виявляти значні відхилення від очікуваної мережевої активності та повідомляти про них, хоча це програмне забезпечення зазвичай не може конкретно позначати діяльність як пов’язану зі зловмисним програмним забезпеченням або блокувати її.

Продукти IPS на основі хоста подібні за принципом і призначенням до інших IPS, за винятком того, що продукт IPS на основі хоста відстежує характеристики окремого хоста та події, що відбуваються в цьому хості. Приклади активності, яку можуть відстежувати IPS на основі хоста, включають

мережевий трафік, журнали хоста, запущені процеси, доступ до файлів і їх модифікацію, а також зміни конфігурації хоста та програми. Продукти IPS на основі хостів часто використовують комбінацію сигнатур атаки та знання очікуваної або типової поведінки для ідентифікації відомих і невідомих атак на хости. Наприклад, продукти IPS на основі хоста, які відстежують спроби змінити файли, можуть бути ефективними для виявлення вірусів, які намагаються заразити файли, і троянських коней, які намагаються замінити файли, а також використання інструментів зловмисника, таких як руткіти, які часто доставляють шкідливе програмне забезпечення. Якщо продукт IPS на основі хоста відстежує мережевий трафік хоста, він пропонує можливості виявлення, подібні до мережевих IPS.

Мережевий брандмауер – це пристрій, що розгортається між мережами для обмеження типів трафіку, який може проходити з однієї мережі в іншу. Брандмауер на основі хоста – це частина програмного забезпечення, що працює на одному хості та може обмежувати вхідну та вихідну мережеву активність лише для цього хоста. Обидва типи брандмауерів можуть бути корисними для запобігання інцидентам шкідливого програмного забезпечення.

Організації повинні налаштувати свої брандмауери з наборами правил заборони за замовчуванням, тобто брандмауери забороняють весь вхідний трафік, який явно не дозволений. За наявності таких наборів правил шкідливе програмне забезпечення не може поширюватися за допомогою служб, які вважаються непотрібними для організації. Організаціям також слід обмежити вихідний трафік до можливого ступеня, зосереджуючись на запобіганні використанню заборонених служб, які зазвичай використовуються шкідливим програмним забезпеченням.

У разі появи великої загрози шкідливого програмного забезпечення, націленої на мережеву службу, організаціям може знадобитися покладатися на брандмауери, щоб запобігти інциденту. Щоб підготуватися до найгірших ситуацій, організації повинні бути готові швидко додати або змінити правила брандмауера, щоб запобігти інциденту шкідливого програмного забезпечення на

основі мережевої служби. Правила брандмауера також можуть бути корисними для зупинки шкідливого програмного забезпечення, яке покладається на певні IP-адреси, наприклад хробака, який завантажує троянські програми з одного з п’яти зовнішніх хостів. Додавання правила, яке блокує всі дії, пов’язані з IP-адресами зовнішніх хостів, може перешкодити троянським програмам досягти організації.

Організаціям слід використовувати *технології перевірки та фільтрації вмісту*, щоб зупинити загрози шкідливого програмного забезпечення на основі електронної пошти. Організаціям слід використовувати технології фільтрації спаму, щоб зменшити кількість спаму, що надходить до користувачів. Спам часто використовується для доставки шкідливого програмного забезпечення, зокрема для фішингових атак, тому зменшення кількості спаму має призвести до відповідного зниження кількості інцидентів шкідливого програмного забезпечення, викликаних спамом.

Організаціям також слід розглянути можливість налаштування серверів електронної пошти та клієнтів для блокування вкладень із розширеннями файлів, які пов’язані зі шкідливим кодом (наприклад, .pif, .vbs), і підозрілими комбінаціями розширень файлів (наприклад, .txt.vbs, .htm.exe). Однак це також може ненавмисно заблокувати законну діяльність. Деякі організації змінюють підозрілі розширення файлів вкладень електронної пошти, щоб одержувач мав зберегти вкладення та перейменувати його перед запуском, що може бути хорошим компромісом між функціональністю та безпекою. Організаціям також слід використовувати технології перевірки вмісту та фільтрації для запобігання загрозам шкідливого програмного забезпечення в Інтернеті.

Програмне забезпечення для фільтрації веб-вмісту має кілька способів зробити це. Хоча це, як правило, розглядається як запобігання доступу до матеріалів, які є неприйнятними для робочого місця, воно також може містити інформацію про чорний список і репутацію. Він також може блокувати небажані типи файлів, наприклад, за розширенням файлу або типом мобільного коду. Для особливо високих ситуацій безпеки організаціям слід обмежити, які типи мобільного коду (наприклад, непідписаний ActiveX) можуть або не можуть

використовуватися з різних джерел (наприклад, внутрішні сервери, зовнішні сервери). Організації також повинні блокувати небажані спливаючі вікна веб-браузера як форму фільтрації вмісту. Деякі спливаючі вікна створені так, щоб вони виглядали як законні системні вікна повідомлень або веб-сайти, і можуть обманним шляхом змусити користувачів перейти на фальшиві веб-сайти, зокрема сайти, які використовуються для фішингу, або дозволити зміни їхніх хостів, серед інших шкідливих дій. Більшість веб-браузерів можуть блокувати спливаючі вікна, також доступні блокувальники спливаючих вікон сторонніх розробників.

І фільтрація електронної пошти, і веб-вмісту повинні використовувати чорні списки в реальному часі, служби репутації та інші подібні механізми, коли це можливо, щоб уникнути прийняття вмісту від відомих або ймовірно зловмисних хостів і доменів. Ці механізми використовують різні методи для ідентифікації певних IP-адрес, доменних імен або URI як імовірно зловмисних або ймовірно безпечних. Чорні списки в режимі реального часу, як правило, базуються на спостережуваній активності шкідливого програмного забезпечення, тоді як служби репутації можуть базуватися на думках користувачів або автоматичному аналізі веб-сайтів, електронних листів тощо без обов’язкового виявлення шкідливого програмного забезпечення.

Оскільки точність і точність цих механізмів значно відрізняються від однієї реалізації до іншої, організаціям слід ретельно оцінювати будь-які чорні списки в реальному часі, служби репутації чи інші подібні механізми, перш ніж розгортати їх у виробничих середовищах, щоб мінімізувати збої в роботі.

Технології створення білих списків програм, також відомі як програми керування додатками, використовуються для визначення того, які програми дозволено використовувати на хості. Більшість технологій створення білих списків програм можна запускати в двох режимах: аудит і примусове виконання.

У примусовому режимі технологія зазвичай забороняє виконання всіх програм, яких немає в білому списку. У режимі аудиту технологія реєструє всі випадки запуску на хості програм, які не входять до білого списку, але не зупиняє їх. Компроміс між режимом примусового виконання та режимом аудиту простий;

використання примусового режиму зупинить запуск шкідливого програмного забезпечення, але також може запобігти запуску нешкідливих програм, яких немає в білому списку.

Організаціям, які розгортають технології створення білих списків додатків, слід спочатку розглянути можливість їх розгортання в режимі аудиту, щоб визначити будь-які необхідні програми, яких немає в білому списку, перш ніж повторно налаштовувати їх для режиму примусового застосування. Запуск технологій білого списку додатків у режимі аудиту аналогічний програмному забезпеченню для виявлення вторгнень без можливостей запобігання вторгненням; це може бути корисно після того, як відбувається зараження, щоб визначити, які хости були уражені, але воно не має можливості запобігти зараженню. Організаціям з високими потребами в безпеці або середовищах з високим ризиком слід розглянути можливість використання технологій білого списку програм для своїх керованих хостів. Технології білого списку додатків вбудовані в багато операційних систем, а також доступні через утиліти сторонніх розробників.

Захисна архітектура. Незалежно від того, наскільки суворими були зусилля щодо пом’якшення вразливості та загроз, інциденти шкідливого програмного забезпечення все одно траплятимуться. Треба застосовувати захисну архітектуру програмного забезпечення хоста, щоб зменшити вплив інцидентів: *захист BIOS, ізольоване програмне середовище, розділення браузера та сегрегація за допомогою віртуалізації.*

Несанкціонована модифікація мікропрограми BIOS шкідливим програмним забезпеченням становить значну загрозу через унікальне та привілейоване положення BIOS в архітектурі ПК. Зловмисна модифікація BIOS може бути частиною складної цілеспрямованої атаки на організацію – або постійна відмова в обслуговуванні (якщо BIOS пошкоджено), або постійна присутність шкідливого програмного забезпечення (якщо BIOS імплантовано шкідливе програмне забезпечення).

Перехід від звичайних реалізацій BIOS до реалізацій на основі

уніфікованого розширюваного інтерфейсу мікропрограми (UEFI) може спростити шкідливе програмне забезпечення націлитися на BIOS широко поширеним способом, оскільки ці реалізації BIOS базуються на загальній специфікації.

Ізольоване програмне середовище відноситься до моделі безпеки, у якій програми запускаються в пісочному програмному середовищі – контрольованому середовищі, яке обмежує операції, які програми можуть виконувати, і яке ізолює їх від інших програм, що працюють на тому самому хості. У моделі безпеки пісочниці зазвичай лише авторизовані «безпечні» операції можуть виконуватися в пісочниці; пісочниця забороняє програмам у пісочниці виконувати будь-які інші операції. Пісочниця також обмежує доступ до системних ресурсів, таких як пам’ять і файлова система, щоб програми ізольовано від інших програм хоста.

Ізольоване програмне середовище надає кілька переваг щодо запобігання інцидентам шкідливого програмного забезпечення та обробки. Обмежуючи доступні операції, він може запобігти виконанню зловмисним програмним забезпеченням деяких або всіх зловмисних дій, які воно намагається виконати; це може запобігти успіху шкідливого програмного забезпечення або зменшити шкоду, яку воно завдає. А середовище ізольованого програмного середовища – ізоляція – може додатково зменшити вплив шкідливого програмного забезпечення, обмежуючи доступ до інформації та функцій шкідливого програмного забезпечення. Ще одна перевага пісочниці полягає в тому, що саму пісочницю можна скинути до завідомо справного стану кожного разу, коли її ініціалізують.

Розділення веб-браузерів. На одному хості можна встановити веб-браузери кількох марок (наприклад, Microsoft Edge, Mozilla Firefox, Google Chrome, Opera). Доступ до веб-сайтів, що містять зловмисний вміст, є одним із найпоширеніших способів атаки на хости, наприклад встановлення шкідливих плагінів у браузері. Щоб зменшити вплив таких атак, користувачі можуть використовувати одну марку браузера для корпоративних додатків і іншу марку браузера для всіх інших веб-сайтів.

Це відокремлює конфіденційні корпоративні дані в одному веб-браузері від

даних в іншому браузері, забезпечуючи кращий захист корпоративних даних (хоча лише це не може належним чином захистити дані веб-браузера) і зменшує ймовірність того, що шкідливе програмне забезпечення, яке зустрічається під час звичайного перегляду веб-сторінок, вплине на корпоративні програми.

Наявність окремого бренду браузера для корпоративних додатків також дозволяє надійніше захистити цей веб-переглядач, наприклад, вимкнути всі форми мобільного коду (наприклад, Java, ActiveX), які не потрібні для зазначених програм.

Відокремлення за допомогою віртуалізації. Розділення браузерів фактично відокремлює веб-браузери один від одного. Віртуалізацію можна використовувати для відокремлення програм або операційних систем одна від одної з набагато більшою суворістю, ніж може забезпечити просте відокремлення браузера. Наприклад, організація може мати один екземпляр ОС для корпоративних програм і інший екземпляр ОС для всіх інших дій, включаючи веб-перегляд.

Кожен екземпляр ОС – це завідомо справний віртуалізований образ, який містить відповідні програми та відповідно захищений. Користувач завантажує ці віртуалізовані образи та виконує свою роботу в цих образах гостьової ОС, а не безпосередньо в самій хост-ОС. Злом одного образу не вплине на інший образ, якщо компроміс не стосується самого програмного забезпечення віртуалізації.

Ще одна перевага полягає в тому, що кожного разу, коли образ перезапускається, його можна перезавантажувати з завідомо справного образу, забезпечуючи усунення будь-яких компромісів, які виникають в образі.

Альтернативною стратегією, більш зручною, але менш безпечною, є використання гостьової ОС для більш ризикованої поведінки (наприклад, звичайного перегляду веб-сторінок) і хост-ОС для корпоративних програм. Це допомагає ізолювати ризиковані дії від інших дій на хості. Основну ОС можна обмежити лише програмами з білого списку, щоб запобігти запуску в ній неавторизованих програм.

Таким чином, аналіз існуючих рішень із захисту інформаційних ресурсів

організації від шкідливих програм показав можливість широкого застосування різноманітних способів та засобів протидії впливу шкідливого коду.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ ВІД ШКІДЛИВИХ ПРОГРАМ НА ПРИКЛАДІ MICROSOFT 365

2.1. Основні функції та зміст захисту від шкідливих програм і програм-вимагачів у Microsoft 365

Першим напрямком є захист даних клієнтів Microsoft 365 від шкідливих програм.

Шкідливе програмне забезпечення складається з вірусів, шпигунського та іншого шкідливого програмного забезпечення. Microsoft 365 містить механізми захисту, які запобігають проникненню шкідливого програмного забезпечення в Microsoft 365 клієнтом або сервером Microsoft 365. Використання програмного забезпечення для захисту від шкідливого програмного забезпечення є основним механізмом захисту активів Microsoft 365 від шкідливого програмного забезпечення. Програмне забезпечення для захисту від шкідливого програмного забезпечення виявляє та запобігає проникненню комп'ютерних вірусів, шкідливого програмного забезпечення, руткітів, черв'яків та іншого шкідливого програмного забезпечення в будь-які сервісні системи. *Програмне забезпечення для захисту від шкідливого програмного забезпечення забезпечує як превентивний, так і детективний контроль над шкідливим програмним забезпеченням [3]*.

Кожне наявне рішення для захисту від шкідливих програм відстежує версію програмного забезпечення та запущені сигнатури. Автоматичне завантаження та застосування оновлень сигнатур щонайменше щодня з сайту визначення вірусів постачальника централізовано керується відповідним інструментом захисту від шкідливого програмного забезпечення для кожної служби обслуговування. Наступні функції централізовано керуються відповідним інструментом захисту від шкідливого програмного забезпечення на кожній кінцевій точці для кожної

служби обслуговування [3]:

автоматичне сканування середовища;

періодичне сканування файлової системи (принаймні щотижня);

сканування файлів у режимі реального часу під час їх завантаження, відкриття або виконання;

автоматичне завантаження та застосування оновлень сигнатур щонайменше щодня з сайту визначення вірусів постачальника;

попередження, очищення та пом’якшення виявлених шкідливих програм.

Коли засоби захисту від шкідливого програмного забезпечення виявляють шкідливе програмне забезпечення, вони блокують його та генерують сповіщення для персоналу служби обслуговування Microsoft 365, служби безпеки Microsoft 365 та/або групи безпеки та відповідності організації Microsoft, яка керує відповідними центрами обробки даних. Приймаючий персонал ініціює процес реагування на інцидент. Інциденти відстежуються та вирішуються, а також проводиться посмертний аналіз.

Другим напрямком є захист від шкідливого програмного забезпечення за допомогою рішення Exchange Online Protection.

Усі повідомлення електронної пошти для Exchange Online проходять через Exchange Online Protection (EOP), який поміщає в карантин і сканує в режимі реального часу всі електронні листи та вкладення електронної пошти, які надходять і залишають систему, на наявність вірусів та іншого шкідливого програмного забезпечення. Адміністраторам не потрібно налаштовувати або підтримувати технології фільтрації – вони ввімкнені за умовчанням. Однак адміністратори можуть налаштовувати фільтри для конкретної компанії за допомогою центру адміністрування Exchange [3].

Використовуючи кілька механізмів захисту від шкідливого програмного забезпечення, EOP пропонує багаторівневий захист, розроблений для виявлення всіх відомих шкідливих програм. Повідомлення, що передаються через службу, перевіряються на наявність шкідливого програмного забезпечення (включно з вірусами та шпигунським програмним забезпеченням). У разі виявлення

шкідливого програмного забезпечення повідомлення видаляється. Сповіщення також можуть надсилатися відправникам або адміністраторам, коли інфіковане повідомлення видалено та не доставлено. Ви також можете вибрати заміну заражених вкладень повідомленнями за замовчуванням або спеціальними повідомленнями, які сповіщають одержувачів про виявлення шкідливого програмного забезпечення.

Наведене нижче допомагає забезпечити захист від шкідливого програмного забезпечення [3]:

багаторівневий захист від шкідливого програмного забезпечення. Численні механізми сканування шкідливого програмного забезпечення, які використовуються в EOP, допомагають захистити як від відомих, так і від невідомих загроз. Ці механізми включають потужне евристичне виявлення, щоб забезпечити захист навіть на ранніх стадіях спалаху шкідливого програмного забезпечення. Доведено, що цей підхід із кількома механізмами забезпечує значно кращий захист, ніж використання лише одного механізму захисту від шкідливих програм;

реагування на загрози в режимі реального часу. Під час деяких спалахів група боротьби зі зловмисним програмним забезпеченням може мати достатньо інформації про вірус або іншу форму шкідливого програмного забезпечення, щоб написати складні правила політики, які виявляють загрозу ще до того, як буде доступне визначення з будь-якого механізму, який використовує обслуговування. Ці правила публікуються в глобальній мережі кожні дві години, щоб надати вашій організації додатковий рівень захисту від атак;

швидке розгортання визначення шкідливого програмного забезпечення. Команда захисту від шкідливого програмного забезпечення підтримує тісні стосунки з партнерами, які розробляють механізми захисту від шкідливого програмного забезпечення. Як наслідок, служба може отримувати та інтегрувати визначення шкідливого програмного забезпечення та виправлення до їх публічного випуску. Зв’язки Microsoft з партнерами часто дозволяють їм розробляти власні засоби захисту. Служба щогодини перевіряє наявність

оновлених визначень для всіх механізмів захисту від шкідливих програм.

Третім напрямком є захист від шкідливого програмного забезпечення за допомогою рішення Microsoft Defender для Office 365.

Microsoft Defender для Office 365 – це служба фільтрації електронної пошти, яка забезпечує додатковий захист від певних типів розширених загроз, зокрема шкідливих програм і вірусів. Наразі Exchange Online Protection використовує надійний і багаторівневий антивірусний захист, який працює на основі кількох механізмів проти відомих шкідливих програм і вірусів. Microsoft Defender для Office 365 розширює цей захист за допомогою функції під назвою «Безпечні вкладення», яка захищає від невідомих зловмисних програм і вірусів і забезпечує кращий захист «нульового дня» для захисту вашої системи обміну повідомленнями. Усі повідомлення та вкладення, які не мають відомої сигнатури вірусу/шкідливого програмного забезпечення, направляються в спеціальне середовище гіпервізора, де виконується аналіз поведінки за допомогою різних методів машинного навчання та аналізу для виявлення зловмисних намірів.

Exchange Online Protection також сканує кожне повідомлення під час передавання в Microsoft 365 і забезпечує захист часу доставки, блокуючи будь-які шкідливі гіперпосилання в повідомленні. Іноді зловмисники намагаються приховати шкідливі URL-адреси за допомогою, здавалося б, безпечних посилань, які після отримання повідомлення перенаправляються на небезпечні сайти службою пересилання. Безпечні посилання проактивно захищають ваших користувачів, якщо вони вибирають таке посилання. Цей захист залишається щоразу, коли вони вибирають посилання, а шкідливі посилання динамічно блокуються, поки хороші посилання доступні.

Microsoft Defender для Office 365 також пропонує широкі можливості звітування та відстеження, тож ви можете отримати важливу інформацію про те, хто стає ціллю у вашій організації та категорії атак, з якими ви стикаєтесь. Звітування та відстеження повідомлень дозволяють досліджувати повідомлення, заблоковані через невідомий вірус або зловмисне програмне забезпечення, а функція відстеження URL-адрес дозволяє відстежувати окремі зловмисні

посилання в повідомленнях, які були натиснуті.

Четвертим напрямком є захист за допомогою рішення SharePoint Online і OneDrive для бізнесу від програм-вимагачів.

Існує багато форм атак програм-вимагачів, але однією з найпоширеніших є випадки, коли зловмисник шифрує важливі файли користувача, а потім вимагає від користувача щось, наприклад гроші чи інформацію, в обмін на ключ для їх розшифровки. Атаки програм-вимагачів зростають, особливо ті, які шифрують файли, що зберігаються в хмарному сховищі користувача.

Контроль версій допомагає захистити списки SharePoint Online і бібліотеки SharePoint Online і OneDrive для бізнесу від деяких, але не всіх, типів атак програм-вимагачів. Керування версіями ввімкнено за замовчуванням у OneDrive для бізнесу та SharePoint Online. Оскільки керування версіями ввімкнено в списках сайтів SharePoint Online, ви можете переглянути попередні версії та за потреби відновити їх. Це дає змогу відновлювати версії елементів, які передували їх шифруванню програмою-вимагачем. Деякі організації також зберігають кілька версій елементів у своїх списках з юридичних причин або з метою аудиту.

Адміністратори SharePoint Online можуть відновити видалену колекцію сайтів за допомогою центру адміністрування SharePoint Online. Користувачі SharePoint Online мають кошик, де зберігається видалений вміст. Вони можуть отримати доступ до кошика, щоб відновити видалені документи та списки, якщо їм це потрібно. Елементи в кошику зберігаються протягом 93 днів. Кошик захоплює такі типи даних: колекції сайтів, сайти, списки, бібліотеки, папки, список елементів, документи, веб-сторінки.

Контроль версій не захищає від атак програм-вимагачів, які копіюють файли, шифрують їх, а потім видаляють оригінальні файли. Однак кінцеві користувачі можуть використовувати кошик для відновлення файлів OneDrive для бізнесу після атаки програм-вимагачів.

Розглянемо засоби захисту та засоби контролю, які Microsoft використовує для зменшення ризику кібератаки на організацію та її активи.

Microsoft створила засоби захисту та засоби керування, які вона

використовує для зменшення ризиків атаки програм-вимагачів на організацію та її активи. Активи можна організовувати за доменами, причому кожен домен має власний набір засобів пом’якшення ризиків.

Домен 1: елементи керування на рівні орендаря.

Перший домен – це люди, які складають організацію, а також інфраструктура та служби, якими володіє та контролює організація. Наведені нижче функції в Microsoft 365 увімкнено за замовчуванням або їх можна налаштувати, щоб зменшити ризик і відновити активи в цьому домені після успішної компрометації.

Exchange Online. Завдяки відновленню окремих елементів і зберіганню поштової скриньки клієнти можуть відновлювати елементи в поштовій скриньці після ненавмисного або зловмисного передчасного видалення. Клієнти можуть відкочувати поштові повідомлення, видалені протягом 14 днів за замовчуванням, налаштовувати до 30 днів.

Exchange Online Protection сканує вхідну електронну пошту та вкладення в режимі реального часу під час входу в систему та виходу з неї. Це ввімкнено за замовчуванням і доступні налаштування фільтрації. Повідомлення, що містять програмне забезпечення-вимагач або інше відоме чи ймовірне шкідливе програмне забезпечення, видаляються. Ви можете налаштувати адміністраторів на отримання сповіщень, коли це відбувається.

SharePoint Online і OneDrive for Business Protection мають вбудовані функції, які допомагають захистити від атак програм-вимагачів, а саме:

Контроль версій: оскільки контроль версій зберігає щонайменше 500 версій файлу за замовчуванням і може бути налаштований на збереження більшої кількості, якщо програма-вимагач редагує та шифрує файл, попередню версію файлу можна відновити.

Кошик: якщо програмне забезпечення-вимагач створює нову зашифровану копію файлу та видаляє старий файл, клієнти мають 93 дні, щоб відновити його з кошика.

Бібліотека збереження: файли, що зберігаються на сайтах SharePoint або

OneDrive, можна зберегти, застосувавши параметри збереження. Якщо документ із версіями підпадає під параметри збереження, версії копіюються до бібліотеки збереження та існують як окремий елемент. Якщо користувач підозрює, що його файли зламано, він може дослідити зміни файлу, переглянувши збережену копію. Відновлення файлів можна використовувати для відновлення файлів протягом останніх 30 днів.

Чати Teams зберігаються в поштових скриньках користувачів Exchange Online, а файли зберігаються в SharePoint Online або OneDrive для бізнесу. Дані Microsoft Teams захищені засобами керування та механізмами відновлення, доступними в цих службах.

Домен 2: елементи керування рівнем обслуговування.

Другий домен – це люди, які входять до складу організації Microsoft, і корпоративна інфраструктура, якою володіє та контролює Microsoft для виконання організаційних функцій бізнесу.

Підхід Microsoft до захисту своєї корпоративної власності – це нульова довіра, реалізована за допомогою наших власних продуктів і послуг із захистом нашої цифрової власності. Додаткові функції в Microsoft 365 розширюють засоби зменшення ризиків, доступні в домені 1, щоб додатково захистити активи в цьому домені.

SharePoint Online і OneDrive для захисту бізнесу:

Контроль версій: якщо програма-вимагач зашифрувала файл на місці, як редагований, файл можна відновити до початкової дати створення файлу за допомогою можливостей історії версій, якими керує Microsoft.

Кошик: якщо програма-вимагач створила нову зашифровану копію файлу та видалила старий файл, користувачі мають 93 дні, щоб відновити його з кошика. Після 93 днів є 14-денне вікно, протягом якого Microsoft все ще може відновити дані. Після цього вікна дані видаляються остаточно.

Зменшення ризиків для Teams, описане в домені 1, також застосовується до домену 2.

Домен 3: Розробники та сервісна інфраструктура.

Третій домен – це люди, які розробляють і керують службою Microsoft 365, кодом та інфраструктурою, що надає службу, а також зберіганням і обробкою даних.

Інвестиції Microsoft, спрямовані на захист платформи Microsoft 365 і пом'якшення ризиків у цьому домені, зосереджені на таких сферах:

постійна оцінка та перевірка стану безпеки служби;

створення інструментів і архітектури, які захищають службу від компромісу;

створення спроможності виявляти загрози та реагувати на них, якщо атака все ж відбудеться;

постійна оцінка та перевірка стану безпеки.

Microsoft зменшує ризики, пов'язані з людьми, які розробляють і керують службою Microsoft 365, використовуючи принцип найменших привілеїв. Це означає, що доступ і дозволи до ресурсів обмежені лише тим, що необхідно для виконання необхідного завдання.

Модель Just-In-Time (JIT), Just-Enough-Access (JEA) використовується для надання інженерам Microsoft тимчасових привілеїв. Інженери повинні подати запит на конкретне завдання, щоб отримати підвищені привілеї. Запитами керують через Lockbox, який використовує керування доступом на основі ролей Azure (RBAC), щоб обмежити типи запитів на підвищення рівня JIT, які можуть надсилати інженери.

На додаток до вищезазначеного, усі кандидати Microsoft проходять попередню перевірку перед початком роботи в Microsoft. Співробітники, які обслуговують онлайн-сервіси Microsoft у Сполучених Штатах, повинні пройти Microsoft Cloud Background Check як передумову для доступу до систем онлайн-сервісів. Усі працівники корпорації Microsoft зобов'язані пройти базовий тренінг з питань безпеки разом із тренінгом зі стандартів ділової поведінки.

Інструменти та архітектура, які захищають сервіс. Життєвий цикл розробки безпеки (SDL) Microsoft зосереджується на розробці безпечного програмного забезпечення для покращення безпеки програм і зменшення

вразливостей. Microsoft 365 обмежує зв’язок між різними частинами інфраструктури служби лише тим, що необхідно для роботи.

Мережевий трафік захищається за допомогою додаткових мережевих брандмауерів у граничних точках, щоб допомогти виявляти, запобігати та пом’якшувати мережеві атаки.

Служби Microsoft 365 створені для роботи без інженерів, які потребують доступу до даних клієнта, за винятком випадків, коли клієнт чітко запитує та схвалює.

Можливості виявлення та реагування. Microsoft 365 здійснює постійний моніторинг безпеки своїх систем, щоб виявляти загрози Службам Microsoft 365 і реагувати на них.

Централізоване журналювання збирає та аналізує події журналу для дій, які можуть вказувати на інцидент безпеки. Дані журналу аналізуються, коли вони завантажуються в систему сповіщень, і створюють сповіщення майже в реальному часі.

Хмарні інструменти дозволяють швидко реагувати на виявлені загрози. Ці інструменти дозволяють виправити помилку за допомогою автоматично запущених дій. Якщо автоматичне усунення неможливе, сповіщення надсилаються відповідним інженерам за викликом, які оснащені набором інструментів, які дозволяють їм діяти в режимі реального часу для пом’якшення виявлених загроз.

2.2. Призначення та основні функції захисту рішення Exchange Online Protection

Exchange Online Protection (EOP) – це хмарна служба фільтрації, яка захищає організацію від спаму, шкідливого програмного забезпечення та інших загроз електронної пошти. EOP включено в усі різновиди Microsoft 365 із поштовими скриньками Exchange Online [9].

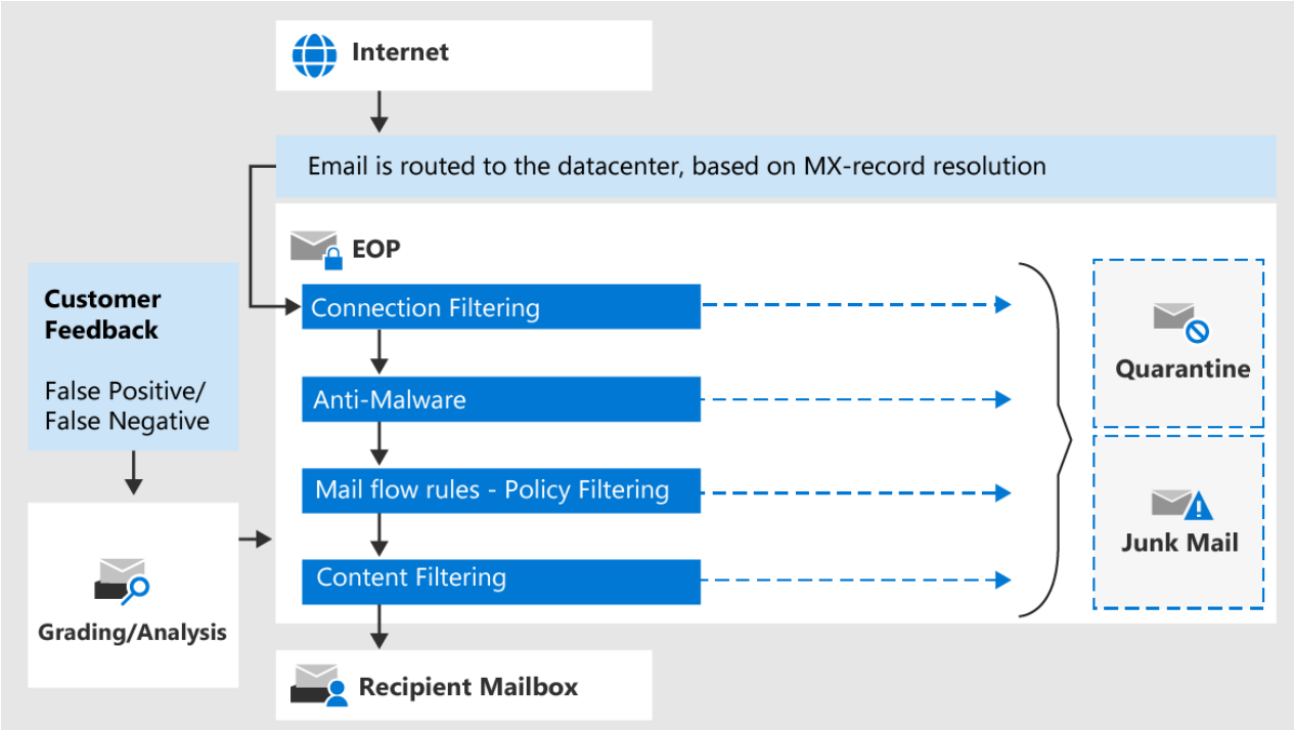

Рис. 2.1. Схема обробки вхідної електронної пошти EOP [9]

Порядок обробки вхідної електронної пошти EOP наступний [9]:

коли вхідне повідомлення потрапляє в EOP, воно спочатку проходить через фільтрацію підключення, яка перевіряє репутацію відправника. Більшість спаму зупиняється на цьому етапі та відхиляється EOP;

потім повідомлення перевіряється на наявність шкідливих програм. Якщо в повідомленні або у вкладеннях виявлено зловмисне програмне забезпечення, повідомлення доставляється на карантин. За замовчуванням лише адміністратори можуть переглядати та взаємодіяти з повідомленнями шкідливого програмного забезпечення в карантині. Але адміністратори можуть створювати та використовувати політики карантину, щоб указати, що користувачам дозволено робити з повідомленнями, розміщеними на карантині;

повідомлення продовжує фільтрацію політики, де воно оцінюється за будь-якими правилами потоку пошти (також відомими як правила транспортування), які ви створили. Наприклад, правило може надсилати сповіщення менеджеру, коли повідомлення надходить від певного відправника;

у локальній організації з клієнтською ліцензією Exchange Enterprise із

ліцензіями на служби перевірки запобігання втраті даних Microsoft Purview (DLP) у EOP також відбуваються на цьому етапі;

повідомлення проходить через фільтрацію вмісту (захист від спаму та спуфінгу), де шкідливі повідомлення ідентифікуються як спам, спам з високою достовірністю, фішинг, фішинг із високою достовірністю, масові повідомлення (політика захисту від спаму) або спуфінг (налаштування підробки в антифішингу). політики). Ви можете налаштувати дії для повідомлення на основі вердикту фільтрації (карантин, переміщення до папки небажаної електронної пошти тощо), а також те, що користувачі можуть робити з повідомленнями в карантині за допомогою політик карантину.

Повідомлення, яке успішно пройшло всі ці рівні захисту, доставляється одержувачам.

EOP працює у всесвітній мережі центрів обробки даних, розроблених для забезпечення найкращої доступності. Наприклад, якщо центр обробки даних стає недоступним, повідомлення електронної пошти автоматично спрямовуються до іншого центру обробки даних без перерви в обслуговуванні. Сервери в кожному центрі обробки даних приймають повідомлення від вашого імені, створюючи рівень відокремлення між вашою організацією та Інтернетом, тим самим зменшуючи навантаження на ваші сервери. Через цю високодоступну мережу Microsoft може гарантувати, що електронна пошта надходить до організації своєчасно.

EOP виконує балансування навантаження між центрами обробки даних, але лише в межах регіону. Якщо ви працюєте в одному регіоні, усі ваші повідомлення оброблятимуться за допомогою маршрутизації пошти для цього регіону.

Основні функції захисту, які доступні у EOP [9]:

EOP використовує кілька списків заблокованих URL-адрес, які допомагають виявляти відомі шкідливі посилання в повідомленнях;

EOP використовує величезний список доменів, які, як відомо, надсилають спам;

EOP використовує кілька механізмів захисту від шкідливого програмного

забезпечення, які допомагають автоматично захищати клієнтів у будь-який час;

EOP перевіряє активне корисне навантаження в тілі повідомлення та всі вкладення повідомлення на наявність шкідливих програм;

EOP застосовує визначені політики захисту.

Основними елементами політики захисту від шкідливих програм в EOP є:

політика фільтра шкідливого програмного забезпечення: визначає сповіщення одержувача, сповіщення відправника та адміністратора, ZAP і загальні налаштування фільтра вкладень;

правило фільтра шкідливого програмного забезпечення: визначає пріоритет і фільтри одержувачів (до кого застосовується політика) для політики фільтрування шкідливого програмного забезпечення.

2.3. Призначення та основні функції рішення Microsoft Defender for Office 365

Microsoft 365 Defender – це уніфікований пакет корпоративного захисту до та після злому, який безпосередньо координує виявлення, запобігання, розслідування та реагування на кінцеві точки, ідентифікатори, електронну пошту та програми для забезпечення інтегрованого захисту від складних атак.

Завдяки інтегрованому рішенню Microsoft 365 Defender спеціалісти з безпеки можуть об’єднати сигнали про загрози, які отримує кожен із цих продуктів, і визначити повний масштаб і вплив загрози; як воно потрапило в середовище, на що воно вплинуло та як воно зараз впливає на організацію. Microsoft 365 Defender виконує автоматичні дії, щоб запобігти або зупинити атаку та самостійно відновити уражені поштові скриньки, кінцеві точки та ідентифікаційні дані користувачів.

Microsoft Defender для Office 365 захищає вашу організацію від зловмисних загроз, створених електронними повідомленнями, посиланнями (URL-адресами) та інструментами для співпраці. Defender для Office 365 містить [10]:

інсталяція за допомогою попереднього налаштування може налаштувати все

за вас: найпростіше та рекомендоване налаштування автоматизує розгортання безпечного середовища (якщо у вашій організації можливі автоматичні політики);

політики захисту від загроз: визначте політики захисту від загроз, щоб установити належний рівень захисту для організації;

звіти: переглядайте звіти в реальному часі для моніторингу продуктивності Defender для Office 365 в організації;

розслідування загроз і можливості реагування: використовуйте передові інструменти для дослідження, розуміння, моделювання та запобігання загрозам.

можливості автоматизованого розслідування та реагування: заощаджуйте час і зусилля на розслідуванні та пом’якшенні загроз.

На рисунку 2.2 показано базову архітектуру Microsoft Defender для Office, яка може включати шлюз SMTP стороннього виробника або локальну інтеграцію.

1. Хост-сервер для зовнішнього відправника зазвичай виконує загальнодоступний DNS-пошук для запису MX, який забезпечує цільовому серверу ретрансляцію повідомлення. Цим рефералом може бути безпосередньо Exchange Online (EXO) або шлюз SMTP, налаштований для ретрансляції на EXO.

2. Exchange Online Protection узгоджує та перевіряє вхідне з’єднання та перевіряє заголовки та вміст повідомлень, щоб визначити, які додаткові політики, теги чи обробка потрібні.

3. Exchange Online інтегрується з Microsoft Defender для Office 365, щоб запропонувати розширеніший захист від загроз, їх пом’якшення та виправлення.

4. Повідомлення, яке не є зловмисним, не заблокованим або поміщеним на карантин, обробляється та доставляється одержувачу в EXO, де оцінюються та активуються налаштування користувача, пов’язані з небажаною поштою, правилами поштової скриньки чи іншими налаштуваннями.

5. Інтеграцію з локальною Active Directory можна ввімкнути за допомогою Azure AD Connect для синхронізації та надання поштових об’єктів і облікових записів для Azure Active Directory і, зрештою, Exchange Online.

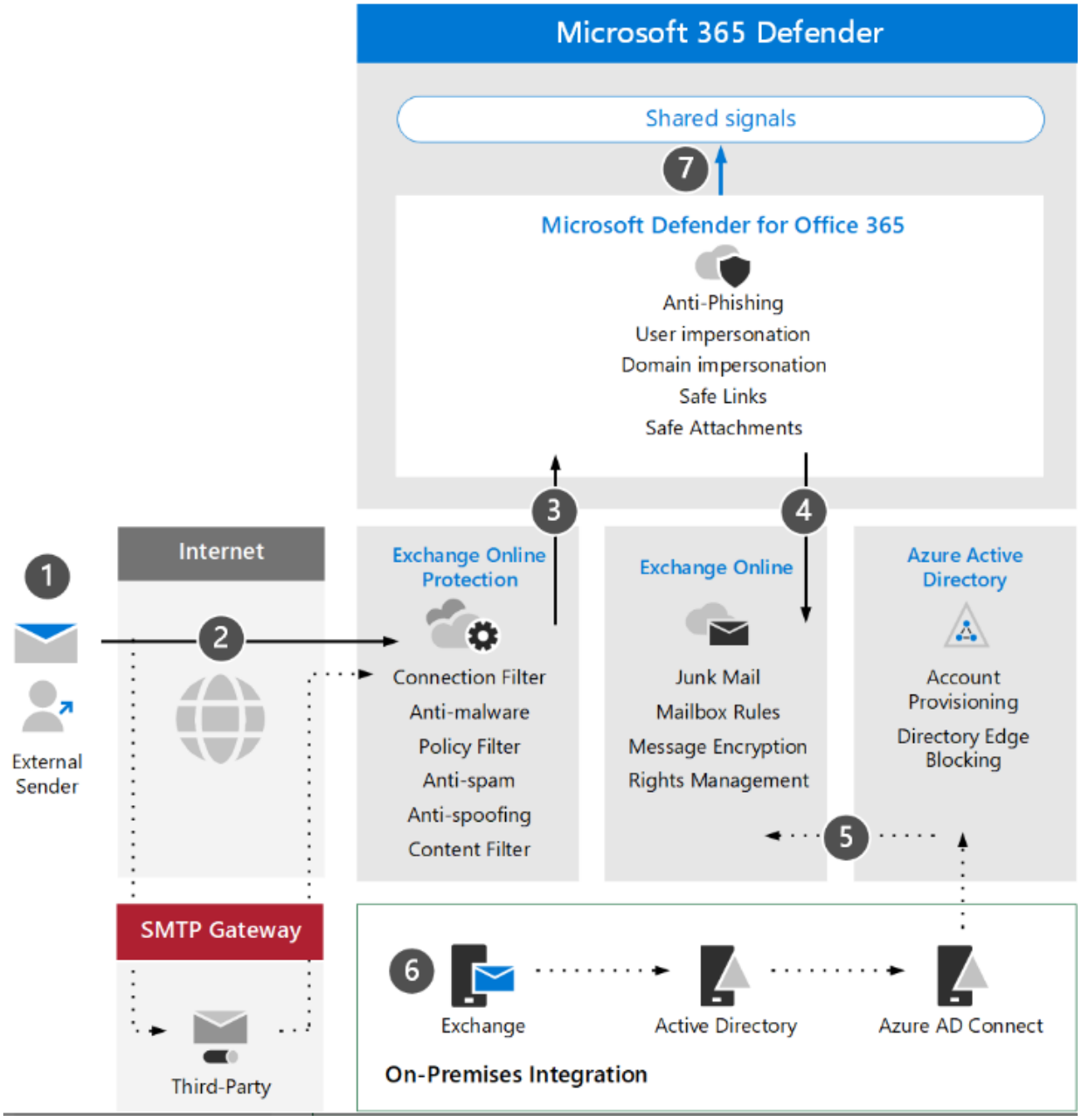

Рис. 2.2. Базова архітектура Microsoft Defender для Office [11]

6. Під час інтеграції локального середовища рекомендується використовувати сервер Exchange для підтримуваного керування та адміністрування атрибутів, параметрів і конфігурацій, пов’язаних із поштою.

7. Microsoft Defender для Office 365 передає сигнали Microsoft 365 Defender для розширеного виявлення та реагування (XDR).

Успішна оцінка або пілотна робота Defender для Office 365 передбачає наявність таких попередніх умов:

усі корпоративні поштові скриньки одержувачів зараз знаходяться в Exchange Online;

корпоративний загальнодоступний запис MX передається безпосередньо в EOP або сторонній шлюз SMTP, який потім передає вхідну зовнішню електронну пошту безпосередньо в EOP;

корпоративний основний домен електронної пошти налаштовано як авторитетний в Exchange Online;

успішно розгорнуто та налаштовано граничне блокування на основі каталогу (DBEB).

Також можна інтегрувати Microsoft Defender для Office 365 із Microsoft Sentinel, щоб більш детально аналізувати події безпеки у організації та створювати посібники для ефективного та негайного реагування. Microsoft Defender для Office 365 також можна інтегрувати в інші рішення безпеки та управління подіями (SIEM) за допомогою Office 365 Activity Management API.

3 ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ ВІД ШКІДЛИВИХ ПРОГРАМ

3.1. Технологія захисту від програм-вимагачів для клієнта Microsoft 365

Програмне забезпечення-вимагач – це тип атаки здирництва, який знищує або шифрує файли та папки, запобігаючи доступу до критичних даних. Програмне забезпечення-вимагач зазвичай поширюється як вірус, який заражає пристрої та потребує лише усунення шкідливого програмного забезпечення. Програмне забезпечення-вимагач, яким керує людина, є результатом активної атаки кіберзлочинців, які проникають у локальну або хмарну IT-інфраструктуру організації, підвищують їхні привілеї та розгортають програмне забезпечення-вимагач на критично важливих даних.

Після завершення атаки зловмисник вимагає від жертви гроші в обмін на видалені файли, ключі розшифровки для зашифрованих файлів або обіцянку не передавати конфіденційні дані в темну мережу чи публічний Інтернет. Програми-вимагачі, якими керує людина, також можуть використовуватися для зупинки критично важливих машин або процесів, таких як ті, що потрібні для промислового виробництва, зупиняючи звичайні бізнес-операції, доки не буде сплачено викуп і не буде виправлено збиток, або організація самостійно усуне збитки.

Атака програми-вимагача, керована людиною, може мати катастрофічні наслідки для підприємств будь-якого розміру, і її важко очистити, вимагаючи повного вигнання зловмисника для захисту від майбутніх атак. На відміну від програм-вимагачів, керованих людьми, вони можуть продовжувати загрожувати діяльності бізнесу після початкового запиту викупу.

Атака програми-вимагача на клієнта Microsoft 365 передбачає, що зловмисник має дійсні облікові дані облікового запису користувача для клієнта та має доступ до всіх файлів і ресурсів, які дозволені для облікового запису

користувача. Зловмиснику без жодних дійсних облікових даних облікового запису користувача доведеться розшифрувати дані в стані спокою, зашифровані Microsoft 365 за замовчуванням і розширене шифрування [3].

Microsoft 365 містить механізми захисту, які запобігають проникненню шкідливого програмного забезпечення в клієнти або сервери Microsoft 365. Використання програмного забезпечення для захисту від шкідливого програмного забезпечення є основним механізмом захисту активів Microsoft 365 від нього. Програмне забезпечення для захисту від шкідливого програмного забезпечення виявляє та запобігає проникненню комп'ютерних вірусів, шкідливого програмного забезпечення, руткітів, черв'яків та іншого шкідливого програмного забезпечення в будь-які сервісні системи. Програмне забезпечення для захисту від шкідливого програмного забезпечення забезпечує як превентивний, так і детективний контроль над шкідливим програмним забезпеченням [3].

В Microsoft 365 кожне наявне рішення для захисту від шкідливих програм відстежує версію програмного забезпечення та запущені сигнатури. Автоматичне завантаження та застосування оновлень сигнатур щонайменше щодня з сайту визначення вірусів постачальника централізовано керується відповідним інструментом захисту від шкідливого програмного забезпечення для кожної служби обслуговування. Наступні функції централізовано керуються відповідним інструментом захисту від шкідливого програмного забезпечення на кожній кінцевій точці для кожної служби обслуговування [3]:

автоматичне сканування середовища;

періодичне сканування файлової системи (принаймні щотижня);

сканування файлів у режимі реального часу під час їх завантаження, відкриття або виконання;

автоматичне завантаження та застосування оновлень сигнатур щонайменше щодня з сайту визначення вірусів постачальника;

попередження, очищення та пом'якшення виявлених шкідливих програм.

Коли засоби захисту від шкідливого програмного забезпечення виявляють шкідливе програмне забезпечення, вони блокують його та генерують сповіщення

для персоналу служби обслуговування Microsoft 365, служби безпеки Microsoft 365 та/або групи безпеки та відповідності організації Microsoft, яка керує нашими центрами обробки даних. Приймаючий персонал ініціює процес реагування на інцидент. Інциденти відстежуються та вирішуються, а також проводиться наступний їх аналіз [4].

Процес розгортання функції захисту та пом'якшення Microsoft 365, встановлення конфігурації та поточних операцій показано на рисунку 3.1.

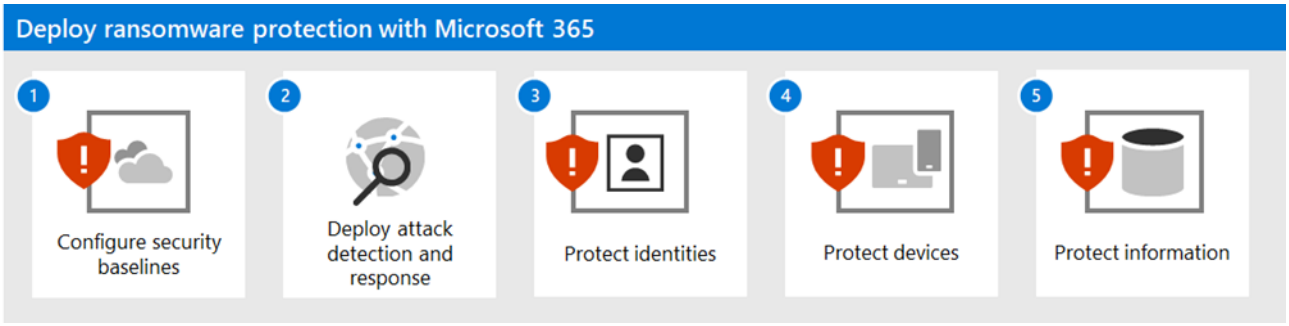

Рис. 3.1. Технологія захисту від програм-вимагачів для клієнта Microsoft 365 [4]

Розглянемо зміст технології захисту від програм-вимагачів для клієнта Microsoft 365 більш детальніше [3].

Перший етап – налаштування базових параметрів. Спочатку здійснюється оцінка і вимірюється рівень безпеки за допомогою Microsoft Secure Score та дотримання інструкцій, щоб покращити його за потреби. Далі застосовуються правила зменшення поверхні атаки, щоб блокувати підозрілу активність і вразливий вміст.

Другий етап – розгортання виявлення атак і реагування. Настійно рекомендований початковий крок для виявлення атак програм-вимагачів і реагування на них у клієнті Microsoft 365. Налаштовується пробне середовище, щоб оцінити функції та можливості Microsoft 365 Defender.

Третій етап – захист ідентифікації. Вживаються заходи від компрометації облікових даних, що зазвичай є першим етапом великої атаки програм-вимагачів.

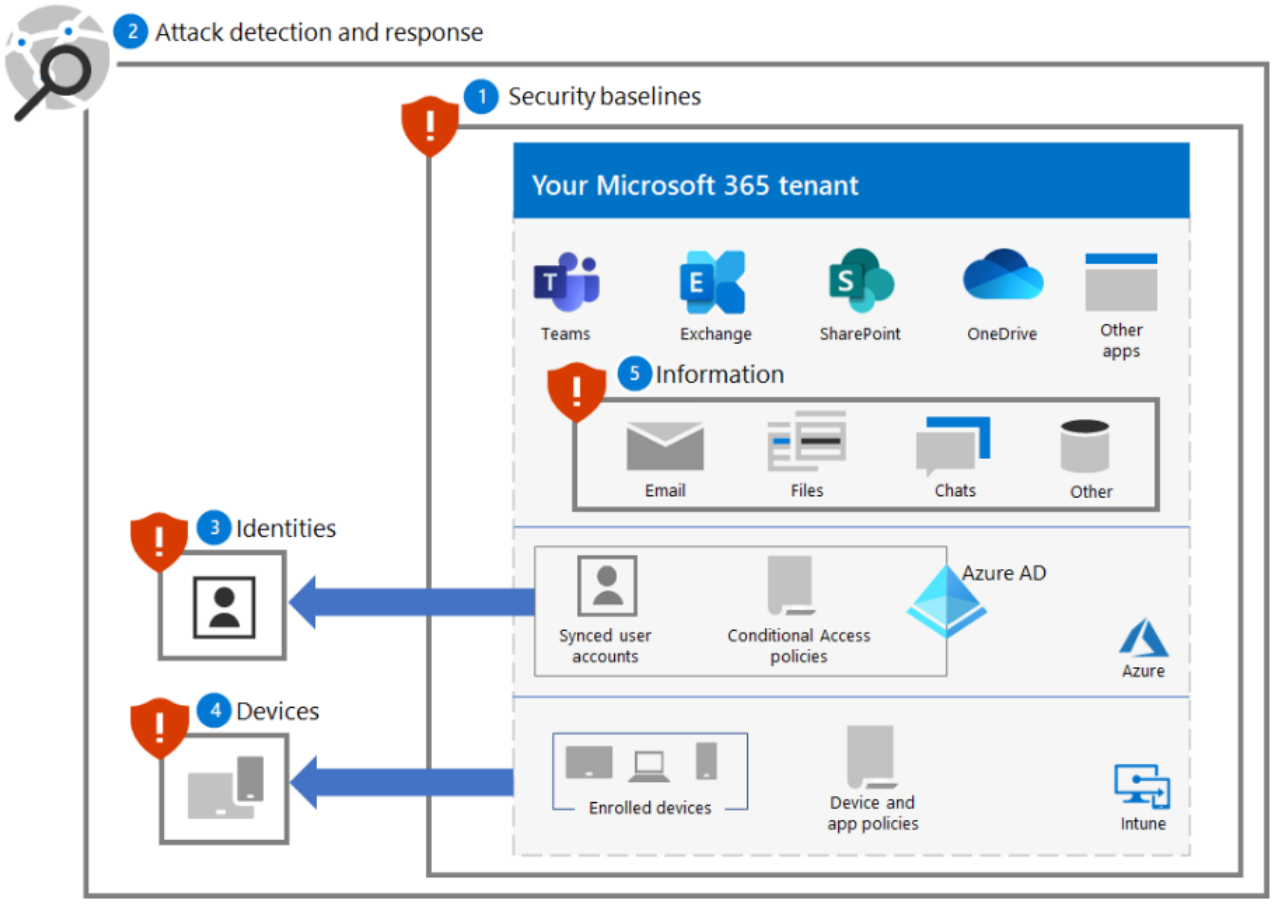

Рис. 3.2. Схема розгортання рішення для клієнта Microsoft 365 [4]

Четвертий етап – захист пристроїв. Вживаються заходи захисту пристроїв (кінцевих точок) від початкового доступу під час атаки програм-вимагачів.

П’ятий етап – захист інформації. Оскільки зловмисники також переглядатимуть локальні дані, розташовані у файлах, базах даних та інших типах серверів, один із найкращих способів захистити ці дані – перенести їх на клієнта Microsoft 365. Опинившись там, дані можна захистити вбудованими функціями пом’якшення та відновлення, такими як керування версіями, кошик і відновлення файлів.

Як висновок, програми-вимагачі та здирництво – це високоприбутковий і недорогий бізнес, який має виснажливий вплив на цільові організації. Програмне забезпечення-вимагач розрослося до різноманітних методів вимагання, спрямованих на всі типи корпоративних мереж і хмарних платформ. Щоб клієнти, які використовують продукти Microsoft, були захищені від атак програм-

вимагачів необхідно максимально підвищити стійкість в умовах впливу програм-вимагачів за допомогою рішень безпеки Microsoft. Ці рішення містять рекомендовані найкращі практики захисту, впровадження яких гарантує, що організація максимізує як профілактичні, так і захисні можливості для подолання атак програм-вимагачів.

3.2. Технологія захисту від загроз у Microsoft Defender для Office 365

Стек захисту або фільтрації Microsoft Defender для Office 365 можна розбити на чотири етапи. Загалом, вхідна пошта проходить усі ці фази перед доставкою, але фактичний шлях електронної пошти залежить від конфігурації Defender для Office 365 організації [12].

Фаза перша – Edge захист.

На жаль, Edge блоки, які колись були критичними, тепер відносно легко подолати для зловмисників. З часом тут блокується менше трафіку, але він залишається важливою частиною стека.

Edge блоки сконструйовані як автоматичні. У разі хибного спрацьовування відправники отримають сповіщення та розкажуть, як вирішити проблему. З'єднувачі від надійних партнерів із обмеженою репутацією можуть забезпечити доступність або тимчасові перевизначення можна застосувати під час підключення нових кінцевих точок.

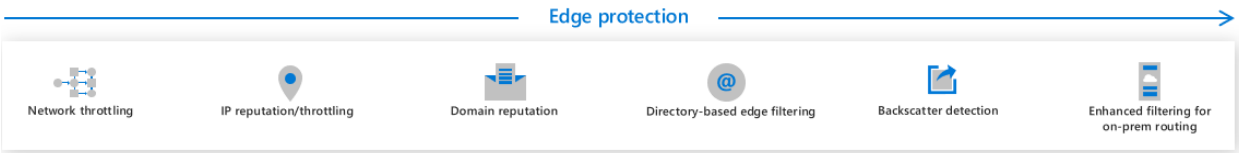

Рис. 3.3. Схема Edge захисту [12]

1. Регулювання мережі захищає інфраструктуру та клієнтів Office 365 від атак типу «Відмова в обслуговуванні» (DOS), обмежуючи кількість повідомлень, які може надсилати певний набір інфраструктури.

2. Репутація IP-адреси та обмеження блокують повідомлення, які надсилаються з завідомо поганих IP-адрес підключення. Якщо конкретна IP-адреса надсилає багато повідомлень за короткий проміжок часу, їх буде придушено.

3. Репутація домену блокуватиме будь-які повідомлення, надіслані з завідомо поганого домену.

4. Гранична фільтрація на основі каталогу блокує спроби отримати інформацію з каталогу організації через SMTP.

5. Виявлення зворотного розсіювання запобігає атаці на організацію через недійсні звіти про недоставку (non-delivery reports, NDR).

6. Покращена фільтрація для з'єднувачів зберігає інформацію автентифікації, навіть якщо трафік проходить через інший пристрій, перш ніж він досягне Office 365. Це покращує точність стеку фільтрації, включаючи моделі машинного навчання евристичної кластеризації, захисту від спуфінгу та захисту від фішингу, навіть у складних або гібридних сценаріях маршрутизації. .

Фаза друга – Інформація про відправника.

Функції розвідки відправників мають вирішальне значення для виявлення спаму, масових повідомлень, повідомлень, що видають себе за іншу особу, і несанкціонованих підроблених повідомлень, а також впливають на виявлення фішингу. Більшість із цих функцій можна налаштувати окремо.

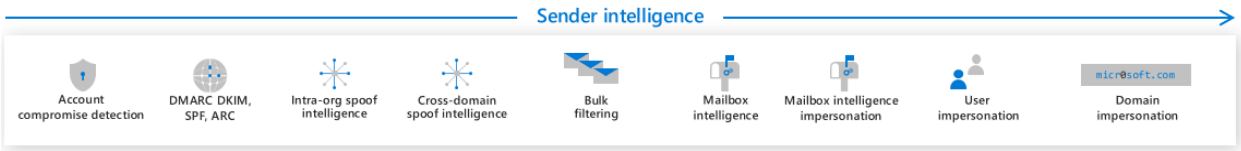

Рис. 3.4. Схема етапу Інформація про відправника [12]

1. Тригери виявлення зламаного облікового запису та сповіщення запускаються, коли обліковий запис має аномальну поведінку, що відповідає компрометації. У деяких випадках обліковий запис користувача блокується, і йому забороняється надсилати будь-які повідомлення електронної пошти, доки

проблему не вирішить команда безпеки організації.

2. Автентифікація електронної пошти включає як налаштовані клієнтом методи, так і методи, налаштовані в хмарі, спрямовані на те, щоб переконатися, що відправники є авторизованими автентичними розсилками. Ці методи протистоять спуфінгу.

SPF (Sender Policy Framework) може відхиляти пошту на основі записів DNS TXT, у яких перелічено IP-адреси та сервери, яким дозволено надсилати пошту від імені організації.

DKIM (DomainKeys Identified Mail) надає зашифрований підпис, який ідентифікує відправника.

DMARC (Domain-based Message Authentication, Reporting, and Conformance) дозволяє адміністраторам позначати SPF і DKIM як потрібні в їхньому домені та забезпечує узгодження результатів цих двох технологій.

ARC базується на DMARC для роботи з пересиланням у списках розсилки під час запису ланцюжка автентифікації.

3. Аналітика спуфінгу здатна відфільтровувати тих, кому дозволено "підробляти" (тобто тих, хто відправляє пошту від імені іншого облікового запису або пересилає для списку розсилки) від зловмисних відправників, які імітують організаційні або відомі зовнішні домени. Він відокремлює законну пошту від імені відправників, які підробляють розсилку спаму і фішингових повідомлень.

Інтелектуальні засоби спуфінгу всередині організації виявляють та блокують спроби спуфінгу з домену всередині організації.

4. Інтелект міждоменної підробки виявляє та блокує спроби підробки з домену за межами організації.

5. Масова фільтрація дозволяє адміністраторам налаштувати рівень достовірності масової розсилки (BCL), що вказує, чи надіслано повідомлення відправником масового розсилання. Адміністратори можуть використовувати повзунок «Масове розсилання» у політиці захисту від спаму, щоб вирішити, який рівень масового розсилання вважати спамом.

6. Аналітика поштових скриньок навчається на стандартній поведінці

користувачів електронної пошти. Він використовує графік спілкування користувача, щоб визначити коли відправник тільки здається тим, з ким користувач зазвичай спілкується, але насправді є зловмисником. Цей метод виявляє уособлення.

7. Уособлення аналітики поштових скриньок включає або вимикає покращені результати уособлення на основі індивідуальної картки відправника кожного користувача. Коли цю функцію увімкнено, вона допомагає ідентифікувати уособлення.

8. Уособлення користувача дозволяє адміністратору створити список важливих цілей, які можуть бути уособлені. Якщо надходить повідомлення, в якому відправник має те саме ім'я та адресу, що й захищений високодохідний обліковий запис, повідомлення позначається або позначається. (Наприклад, trαcye@contoso.com для tracye@contoso.com).

9. Уособлення домену виявляє домени, схожі на домен одержувача і намагаються виглядати як внутрішній домен. Наприклад, це уособлення tracye@liwαre.com для tracye@litware.com.

Фаза третя – Фільтрування вмісту

На цьому етапі стек фільтрації починає обробляти конкретний вміст пошти, включаючи гіперпосилання та вкладення.

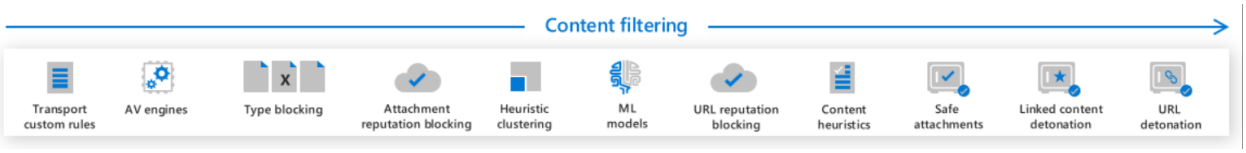

Рис. 3.5. Схема етапу Фільтрування вмісту [12]

1. Правила транспорту (також відомі як правила потоку обробки пошти або правила транспорту Exchange) дозволяють адміністратору виконувати широкий спектр дій, коли для повідомлення виконується такий же широкий діапазон умов. Всі повідомлення, що проходять через вашу організацію, оцінюються щодо відповідності включеним правилам обробки пошти/правилам транспорту.

2. Антивірусна програма Microsoft Defender та сторонній антивірусний модуль використовуються для виявлення всіх відомих шкідливих програм у вкладеннях.

3. Антивірусні (AV) механізми також використовуються для типів вкладень істинного типу, що підтримуються, що дозволяє блокувати тип для правильного блокування типів файлів, зазначених адміністраторами.

4. Щоразу, коли Microsoft Defender для Office 365 виявляє шкідливе вкладення, хеш файлу та хеш його активного вмісту додаються до репутації Exchange Online Protection (EOP). Блокування репутації вкладення заблокує цей файл у всіх Office 365 та на кінцевих точках через хмарні дзвінки MSAV.

5 Евристична кластеризація може визначити, що файл є підозрілим на основі евристики доставки. У разі виявлення підозрілого вкладення вся кампанія припиняється, а файл поміщається в пісочницю. Якщо файл виявляється шкідливим, вся кампанія блокується.

6. Моделі машинного навчання впливають на заголовок, основний текст та URL-адресу повідомлення для виявлення спроб фішингу.

7. Microsoft використовує визначення репутації з пісочниці URL-адрес, а також репутацію URL-адрес із сторонніх каналів у блокуванні репутації URL-адрес , щоб заблокувати будь-яке повідомлення з відомою шкідливою URL-адресою.

8. Евристика вмісту може виявляти підозрілі повідомлення з урахуванням структури і частоти слів у тілі повідомлення з допомогою моделей машинного навчання.

9. Безпечні вкладення ізолюють кожне вкладення для клієнтів Defender для Office 365, використовуючи динамічний аналіз для виявлення раніше невідомих загроз.

10. Детонація зв'язаного вмісту обробляє кожну URL-адресу, яка посилається на файл в електронному листі, як вкладення, асинхронно поміщаючи файл у пісочницю під час доставки.

11. Детонація URL-адреси відбувається, коли попередня технологія захисту

від фішингу вважає повідомлення або URL-адресу підозрілими. Детонація URL-адрес ізолює URL-адресу в повідомленні під час доставки.

Фаза четверта – Захист після доставки.

Останній етап відбувається після доставки пошти або файлу, впливаючи на пошту, яка знаходиться в різних поштових скриньках, а також файли та посилання, які з'являються у клієнтах, таких як Microsoft Teams.

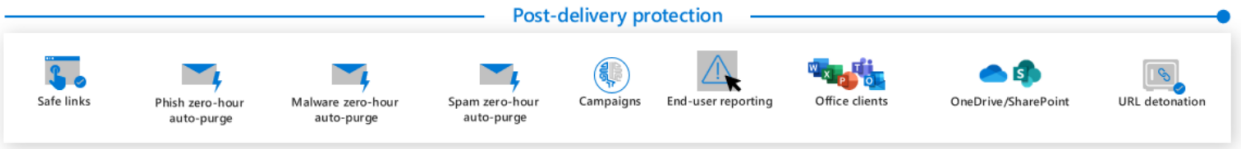

Рис. 3.6. Схема етапу Захист після доставки [12]

1. Безпечні посилання – це захист часу натискання Defender для Office 365. Кожна URL-адреса в кожному повідомленні упакована так, щоб вказувати на сервери Microsoft Safe Links. При натисканні URL-адреси він перевіряється на відповідність останньої репутації, перш ніж користувач буде перенаправлений на цільовий сайт. URL-адреса асинхронно ізольована для оновлення своєї репутації.

2. Автоматичне очищення нульової години (Zero-hour auto purge, ZAP) від фішингу заднім числом виявляє та нейтралізує шкідливі фішингові повідомлення, які вже були доставлені до поштових скриньок Exchange Online.

3. ZAP для шкідливих програм заднім числом виявляє та нейтралізує повідомлення про шкідливі програми, які вже були доставлені до поштових скриньок Exchange Online.

4. ZAP для спаму заднім числом виявляє та нейтралізує шкідливі спам-повідомлення, які вже були доставлені до поштових скриньок Exchange Online.

5. Подання кампанії дозволяють адміністраторам побачити загальну картину атаки швидше та повніше, ніж будь-яка команда без автоматизації. Microsoft використовує величезні обсяги даних про захист від фішингу, спаму та шкідливих програм у всій службі, щоб допомогти ідентифікувати кампанії, а потім дозволяє адміністраторам досліджувати їх від початку до кінця, включаючи

цілі, впливи та потоки, які також доступні в описі кампанії, який можна завантажити.

6. Надбудови Report Message дозволяють людям легко повідомляти про помилкові спрацьовування (хороший електронний лист, помилково позначений як поганий) або хибнонегативний (невірний електронний лист, позначений як хороший) до корпорації Microsoft для подальшого аналізу.

7. Безпечні посилання для клієнтів Office пропонують той самий захист часу кліка, що й безпечні посилання в підтримуваних програмах Office, таких як Word, PowerPoint і Excel.

8. Захист для OneDrive, SharePoint та Teams пропонує однаковий захист безпечних вкладень від шкідливих файлів, вбудований у OneDrive, SharePoint та Microsoft Teams.

9. Коли URL-адреса, яка вказує на файл, вибрана після доставки, детонація зв'язаного вмісту відображає сторінку з попередженням, поки пісочниця файлу не буде завершена і URL-адреса не буде визнана безпечною.

3.3. Рекомендації щодо застосування технології захисту інформаційних ресурсів організації від шкідливих програм

Реалізація наведених нижче рекомендацій має сприяти більш ефективним і ефективним реагуванням на інциденти шкідливого програмного забезпечення для федеральних департаментів і агентств.

Організації повинні розробити та впровадити підхід до запобігання інцидентам шкідливого програмного забезпечення. Організації повинні планувати та впроваджувати підхід до запобігання інцидентам шкідливого програмного забезпечення на основі векторів атак, які, найімовірніше, будуть використані зараз і в найближчому майбутньому. Оскільки ефективність методів запобігання може відрізнятися залежно від середовища (тобто техніка, яка добре працює в керованому середовищі, може бути неефективною в некерованому середовищі),

організації повинні обирати методи запобігання, які добре підходять для їх середовища та хостів. Підхід організації до запобігання інцидентам зі зловмисним програмним забезпеченням має включати політичні міркування, програми підвищення обізнаності для користувачів і персоналу інформаційних технологій (IT), заходи щодо пом'якшення вразливості та загроз, а також міркування щодо захисної архітектури. Організації повинні переконатися, що їхні політики спрямовані на запобігання інцидентам шкідливого програмного забезпечення. Заяви про політику організації слід використовувати як основу для додаткових заходів із запобігання зловмисному програмному забезпеченню, таких як обізнаність користувачів і IT-персоналу, пом'якшення вразливостей, пом'якшення загроз і захисна архітектура. Якщо організація не викладає чітко міркування щодо запобігання зловмисному програмному забезпеченню у своїй політиці, вона навряд чи зможе виконувати дії із запобігання зловмисному програмному забезпеченню послідовно та ефективно в усій організації. Політика, пов'язана із запобіганням зловмисному програмному забезпеченню, має бути якомога загальнішою, щоб забезпечити гнучкість реалізації політики та зменшити потребу в частих оновленнях політики, але також має бути достатньо конкретною, щоб чітко пояснювати мету та сферу дії політики. Політика щодо запобігання зловмисному програмному забезпеченню повинна включати положення щодо віддалених працівників – як тих, хто використовує хости, які контролюються організацією, так і тих, хто використовує хости поза контролем організації (наприклад, комп'ютери підрядників, домашні комп'ютери працівників, комп'ютери ділових партнерів, мобільні пристрої) [5].

Організації повинні включити запобігання інцидентам шкідливого програмного забезпечення та обробку у свої програми інформування. Організації повинні впроваджувати програми підвищення обізнаності, які включають вказівки для користувачів щодо запобігання інцидентам шкідливого програмного забезпечення. Усі користувачі повинні бути обізнані про шляхи проникнення та зараження шкідливого програмного забезпечення на хостах, ризики, які створює шкідливе програмне забезпечення, нездатність технічного контролю запобігти

всім інцидентам і важливість користувачів у запобіганні інцидентам, з наголосом на уникненні атак соціальної інженерії. Програми підвищення обізнаності також повинні інформувати користувачів про політику та процедури, які застосовуються до обробки інцидентів шкідливого програмного забезпечення, наприклад, як визначити, чи може хост бути зараженим, як повідомити про підозрілий інцидент і що користувачам може знадобитися зробити, щоб допомогти в обробці інциденту. Крім того, організація повинна проводити заходи з підвищення обізнаності для IT-персоналу, який бере участь у запобіганні інцидентам зі зловмисним програмним забезпеченням, і проводити навчання щодо конкретних завдань. Організації повинні мати можливості пом’якшення вразливості, щоб запобігти інцидентам із шкідливим програмним забезпеченням. Організації повинні мати задокументовану політику, процеси та процедури для пом’якшення відомих уразливостей, якими може скористатися шкідливе програмне забезпечення. Оскільки вразливість зазвичай можна пом’якшити одним або декількома методами, організації повинні використовувати відповідну комбінацію методів, включаючи технології автоматизації безпеки з контрольними списками конфігурації безпеки та керуванням виправленнями, а також додаткові заходи зміцнення хоста, щоб ефективні методи були легко доступні для різних типів уразливості. Організації повинні мати можливості пом’якшення загроз, щоб допомогти у стримуванні інцидентів шкідливого програмного забезпечення.

Організації повинні виконувати пом’якшення загроз, щоб виявити та зупинити шкідливе програмне забезпечення, перш ніж воно зможе вплинути на свої цілі.

Найпоширенішим технічним засобом запобігання загрозам шкідливого програмного забезпечення є антивірусне програмне забезпечення; організації повинні розгортати антивірусне програмне забезпечення на всіх хостах, для яких доступне задовільний антивірусне програмне забезпечення.

Додаткові технічні засоби контролю, які допомагають запобігти загрозам шкідливого програмного забезпечення, включають системи запобігання вторгненням, брандмауери, фільтрацію та перевірку вмісту, а також білий список

програм.

Рекомендується втілювати механізми захисту від шкідливого програмного забезпечення на різних типах хостів, включаючи робочі станції, сервери, мобільні комп'ютерні пристрої, брандмауери, сервери електронної пошти, веб-сервери та сервери віддаленого доступу. Організаціям слід розглянути можливість використання методів оборонної архітектури, щоб зменшити вплив шкідливих програм.

Незалежно від того, наскільки суворими є зусилля щодо запобігання вразливості та загроз, інциденти шкідливого програмного забезпечення все одно траплятимуться. Організації повинні розглянути можливість зміни захисної архітектури програмного забезпечення своїх хостів, щоб допомогти пом'якшити ті інциденти, які все ще трапляються. Одним з методів є пісочниця, яка є моделлю безпеки, коли програми запускаються в контрольованому середовищі, яке обмежує операції, які програми можуть виконувати, і ізолює їх від інших програм. Інша техніка – це поділ браузерів, який передбачає використання різних веб-браузерів для різних типів доступу до веб-сайтів (корпоративні програми, загальний доступ тощо). Нарешті, поділ за допомогою методів віртуалізації відокремлює програми або операційні системи одна від одної за допомогою віртуалізації, наприклад мати один екземпляр ОС для корпоративних додатків і інший екземпляр ОС для всіх інших дій.

Як захистити себе від шкідливого коду? Використаємо рекомендації Cybersecurity and Infrastructure Security Agency (CISA) [6]. Дотримання цих заходів безпеки може допомогти вам зменшити ризики, пов'язані зі шкідливим кодом.

Необхідно встановлювати та підтримувати антивірусне програмне забезпечення. Антивірусне програмне забезпечення розпізнає шкідливе програмне забезпечення та захищає ваш комп'ютер від нього. Встановлення антивірусного програмного забезпечення від перевіреного постачальника є важливим кроком у запобіганні та виявленні інфекцій. Завжди відвідуйте сайти постачальників безпосередньо, а не натискайте рекламні оголошення чи

посилання в електронних листах. Оскільки зловмисники постійно створюють нові віруси та інші форми шкідливого коду, важливо постійно оновлювати антивірусне програмне забезпечення.

Будьте обережні з посиланнями та вкладеннями. Вживайте відповідних запобіжних заходів під час використання електронної пошти та веб-браузерів, щоб зменшити ризик зараження. Будьте обережні з небажаними вкладеннями електронної пошти та будьте обережні, натискаючи посилання електронної пошти, навіть якщо здається, що вони надійшли від людей, яких ви знаєте.

Необхідно блокувати спливаючу рекламу. Блокувальники спливаючих вікон відключають вікна, які потенційно можуть містити шкідливий код. Більшість браузерів мають безкоштовну функцію, яку можна ввімкнути для блокування спливаючих рекламних вікон.

Необхідно використовувати обліковий запис з обмеженими правами. Під час навігації в Інтернеті корисною практикою безпеки є використання облікового запису з обмеженими дозволами. Якщо ви інфікуєтеся, обмежені дозволи запобігають поширенню зловмисного коду та перенесенню його на обліковий запис адміністратора.

Необхідно вимикати функції AutoRun і AutoPlay на зовнішніх носіях. Вимкнення функцій AutoRun і AutoPlay запобігає автоматичному запуску зовнішнього носія, зараженого шкідливим кодом, на вашому комп’ютері.

Необхідно періодично змінювати свої паролі. Якщо ви вважаєте, що ваш комп’ютер заражений, змініть паролі. Це включає будь-які паролі для веб-сайтів, які могли бути кешовані у вашому веб-переглядачі. Створюйте та використовуйте надійні паролі, щоб зловмисникам було важко вгадати їх.

Необхідно постійно оновлювати програмне забезпечення. Установіть програмні виправлення на свій комп’ютер, щоб зловмисники не скористалися відомими вразливими місцями. Увімкніть автоматичні оновлення, якщо вони доступні.

Необхідно впроваджувати резервне копіювання даних. Регулярно створюйте резервні копії документів, фотографій і важливих електронних листів у

хмарі або на зовнішньому жорсткому диску. У разі зараження ваша інформація не буде втрачена.

Необхідно встановлювати або ввімкнути брандмауер. Брандмауери можуть запобігти деяким типам зараження, блокуючи шкідливий трафік до того, як він потрапить на ваш комп'ютер. Деякі операційні системи містять брандмауер; якщо операційна система, яку ви використовуєте, включає його, увімкніть його.

Використовуйте засоби захисту від шпигунського ПЗ. Шпигунське програмне забезпечення є поширеним джерелом вірусу, але ви можете звести до мінімуму зараження за допомогою програми, яка визначає та видаляє шпигунське програмне забезпечення. Більшість антивірусного програмного забезпечення містить опцію захисту від шпигунського програмного забезпечення; переконайтеся, що ви його ввімкнули.

Необхідно керувати обліковими записами. Слідкуйте за будь-яким несанкціонованим використанням або незвичною діяльністю ваших облікових записів, особливо банківських. Якщо ви виявите несанкціоновану або незвичну діяльність, негайно зв'яжіться зі своїм постачальником облікового запису.

Уникайте використання публічного Wi-Fi. Незахищений публічний Wi-Fi може дозволити зловмиснику перехопити мережевий трафік вашого пристрою та отримати доступ до вашої особистої інформації.

Вивчіть доступне антивірусне та антишпигунське програмне забезпечення, щоб визначити найкращий вибір для вас. Зверніть увагу на кількість шкідливого коду, яке розпізнає програмне забезпечення, і на те, як часто оновлюються визначення вірусів. Також перевірте наявність відомих проблем із сумісністю з іншим програмним забезпеченням, яке, можливо, працює на вашому комп'ютері.

Обмежте кількість встановлених програм. Тепер доступні пакети, які об'єднують одночасно антивірусні та антишпигунські можливості. Якщо ви вирішите вибрати окремі програми, вам знадобляться лише одна антивірусна та одна антишпигунська програма. Встановлення більшої кількості програм збільшує ризик виникнення проблем.

Використання антивірусного програмного забезпечення – найкращий спосіб

захистити комп’ютер від шкідливого коду. Якщо ви вважаєте, що ваш комп’ютер заражений, необхідно запустити антивірусну програму. В ідеалі антивірусна програма визначить будь-який шкідливий код на вашому комп’ютері та помістить його в карантин, щоб він більше не впливав на вашу систему. Ви також повинні розглянути ці додаткові кроки:

мінімізуйте шкоду. Якщо ви на роботі та маєте доступ до відділу інформаційних технологій (IT), негайно зверніться до нього. Чим швидше вони дослідять і «очистять» ваш комп’ютер, тим менша ймовірність завдати додаткової шкоди вашому комп’ютеру та іншим комп’ютерам у мережі. Якщо ви використовуєте домашній комп’ютер або ноутбук, від’єднайте комп’ютер від Інтернету; це завадить зловмиснику отримати доступ до вашої системи;

видаліть шкідливий код. Якщо на вашому комп’ютері встановлено антивірусне програмне забезпечення, оновіть програмне забезпечення та виконайте сканування всієї системи вручну. Якщо у вас немає антивірусного програмного забезпечення, ви можете придбати його в Інтернеті або в комп’ютерному магазині. Якщо програмне забезпечення не може знайти та видалити зараження, вам може знадобитися перевстановити операційну систему, як правило, за допомогою диска відновлення системи. Зауважте, що перевстановлення або відновлення операційної системи зазвичай стирає всі ваші файли та будь-яке додаткове програмне забезпечення, яке ви інсталювали на своєму комп’ютері. Після перевстановлення операційної системи та будь-якого іншого програмного забезпечення встановіть усі відповідні патчі для усунення відомих уразливостей.

Загрози для вашого комп’ютера продовжуватимуть розвиватися. Хоча ви не можете усунути кожну небезпеку, виявляючи обережність, встановлюючи та використовуючи антивірусне програмне забезпечення та дотримуючись інших простих заходів безпеки, ви можете значно зменшити ризик і посилити захист від шкідливого коду.

ВИСНОВКИ

В роботі проведено дослідження проблеми захисту інформаційних ресурсів організації від шкідливих програм та програм-вимагачів як складової частини забезпечення кібербезпеки її інформаційних ресурсів.

Рішення Microsoft 365 задовольняє всі потреби, пов'язані з виконанням офісних задач впродовж робочого дня: від підготовки документів, створення презентацій, роботи з таблицями та розрахунками до керування календарем, комунікації у команді тощо. ПЗ також забезпечує прямий доступ до даних, електронної пошти та зустрічей у віддаленому режимі. Microsoft 365 дозволяє користувачам одночасно працювати з документами в режимі реального часу та безпечно комунікувати з колегами та клієнтами за допомогою текстових чатів та дзвінків.

Програмне забезпечення-вимагач – це тип атаки здирництва, який знищує або шифрує файли та папки, запобігаючи доступу до критичних даних. Програмне забезпечення-вимагач зазвичай поширюється як вірус, який заражає пристрої та потребує лише усунення шкідливого програмного забезпечення. Програмне забезпечення-вимагач, яким керує людина, є результатом активної атаки кіберзлочинців, які проникають у локальну або хмарну IT-інфраструктуру організації, підвищують їхні привілеї та розгортають програмне забезпечення-вимагач на критично важливих даних.

Шкідливе програмне забезпечення часто атакує хости, використовуючи вразливості в операційних системах, службах і програмах. Отже, пом’якшення вразливостей є дуже важливим для запобігання інцидентам зі шкідливим програмним забезпеченням.

Проаналізовано основні функції та зміст захисту від шкідливих програм і програм-вимагачів у Microsoft 365. Першим напрямком є захист даних клієнтів Microsoft 365 від шкідливих програм. Microsoft 365 містить механізми захисту, які запобігають проникненню шкідливого програмного забезпечення в Microsoft 365

клієнтом або сервером Microsoft 365. Використання програмного забезпечення для захисту від шкідливого програмного забезпечення є основним механізмом захисту активів Microsoft 365 від шкідливого програмного забезпечення. Програмне забезпечення для захисту від шкідливого програмного забезпечення виявляє та запобігає проникненню комп'ютерних вірусів, шкідливого програмного забезпечення, руткітів, черв'яків та іншого шкідливого програмного забезпечення в будь-які сервісні системи. Програмне забезпечення для захисту від шкідливого програмного забезпечення забезпечує як превентивний, так і детективний контроль над шкідливим програмним забезпеченням.

Проаналізовано призначення та основні функції захисту рішення Exchange Online Protection. Exchange Online Protection – це хмарна служба фільтрації, яка захищає організацію від спаму, шкідливого програмного забезпечення та інших загроз електронної пошти. EOP включено в усі різновиди Microsoft 365 із поштовими скриньками Exchange Online.

Проаналізовано призначення та основні функції рішення Microsoft Defender for Office 365. Microsoft 365 Defender – це уніфікований пакет корпоративного захисту до та після злому, який безпосередньо координує виявлення, запобігання, розслідування та реагування на кінцеві точки, ідентифікатори, електронну пошту та програми для забезпечення інтегрованого захисту від складних атак.

Розглянуто технологію захисту від програм-вимагачів для клієнта Microsoft 365, а також технологію захисту від загроз у Microsoft Defender for Office 365.

Розроблено рекомендації фахівцям з кібербезпеки щодо застосування технології захисту інформаційних ресурсів організації від шкідливих програм.

Таким чином, правильна реалізація технології захисту інформаційних ресурсів організації від шкідливих програм має забезпечити ефективний захист корпоративних даних та кібербезпеку інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Microsoft 365 – цифровий офіс майбутнього вже сьогодні. Konica Minolta. [Електронний ресурс] – Режим доступу: https://www.konicaminolta.ua/uk-ua/software/it-services/microsoft-365.

2. Євгенія Підгайна. Кібербезпека для бізнесу під час війни: як завадити шкідливому трафіку, фішинговим атакам, зараженню вірусами та іншим загрозам та як кібертероризм набирає обертів. Mind. 22 березня 2022, 16:00. [Електронний ресурс] – Режим доступу: https://mind.ua/publications/20238234-kiberbezpeka-dlya-biznesu-pid-chas-vijni-yak-zavaditi-shkidlivomu-trafiku-fishingovim-atakam-zarazhennyu.

3. Malware and ransomware protection in Microsoft 365. Article 09/22/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection.

4. Deploy ransomware protection for your Microsoft 365 tenant. Article 23/09/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/microsoft-365/solutions/ransomware-protection-microsoft-365?view=o365-worldwide.

5. Murugiah Souppaya, Karen Scarfone. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. NIST Special Publication 800-83 Revision 1. [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-83r1.pdf.

6. Security Tip (ST18-004). Protecting Against Malicious Code. CISA. [Електронний ресурс] – Режим доступу: https://www.cisa.gov/uscert/ncas/tips/ST18-271.

7. The State of Ransomware 2022. A Sophos Whitepaper. April 2022. [Електронний ресурс] – Режим доступу: https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf.

8. Microsoft Digital Defense Report 2022. [Електронний ресурс] – Режим доступу: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us.

9. Exchange Online Protection overview. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/eop-about?view=o365-worldwide.

10. Microsoft Defender for Office 365. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/defender-for-office-365?view=o365-worldwide.

11. Review Microsoft Defender for Office 365 architecture requirements and key concepts. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/microsoft-365/security/defender/eval-defender-office-365-architecture?view=o365-worldwide.

12. Step-by-step threat protection in Microsoft Defender for Office 365. Article 11/17/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/protection-stack-microsoft-defender-for-office365?view=o365-worldwide.

13. Ларін О. Д. Технологія захисту інформаційних ресурсів організації від шкідливих програм та програм-вимагачів на базі Microsoft 365. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний Університет Телекомунікацій. 27 жовтня 2022. Тези доповідей. С. 14-18. [Електронний ресурс] – Режим доступу: https://dut.edu.ua/uploads/p_2121_20358827.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)