ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Комплексне рішення для захисту корпоративної електронної пошти на базі FortiMail»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Владислав ЛУКАШЕНКО
(підпис)

Виконав: здобувач(ка) вищої освіти групи БСД-43
ЛУКАШЕНКО Владислав
(прізвище, ім'я)

Керівник д.т.н., проф. КОЖУХІВСЬКИЙ Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

API – Application Programming Interface

APT – Advanced Persistent Threat

BEC – Business Email Compromise

DDoS – Distributed Denial of Service

DKIM – Domain Keys Identified Mail

DMARC – Domain-Based Message Authentication, Reporting and Conformance

DNS – Domain Name System

ESP – Email Security Platform

HTTP/HTTPs – Secured and non-secured HyperText Transfer Protocols

IaaS – Infrastructure as a Service

IMAP – Internet Message Access Protocol

MFA – Multifactor Authentication

MTA – Message Transfer Agent

MUA – Mail User Agent

MX – Mail Exchange

POP3 – Post Office Protocol version 3

SEGs – Secure Email Gateways

SMTP – Simple Mail Transfer Protocol

SPF – Sender Policy Framework

ВСТУП

Актуальність дослідження. Необхідність захисту корпоративної електронної пошти в сучасних умовах є критично важливою з кількох основних причин. Більшість кібератак на організації починаються саме через електронну пошту. Це найпоширеніший канал для доставки шкідливого програмного забезпечення (вірусів, програм-вимагачів), фішингових листів та спроб соціальної інженерії. Атаки можуть призвести до зупинки роботи поштових серверів, втрати важливої кореспонденції, зриву комунікацій як всередині компанії, так і з зовнішнім світом, що паралізує операційну діяльність.

Корпоративна пошта часто містить або використовується для передачі чутливих даних: комерційної таємниці, фінансової інформації, персональних даних клієнтів та співробітників, інтелектуальної власності, даних для входу в інші системи. Несанкціонований доступ до пошти може призвести до витоку цієї інформації. Витік даних або успішна атака через пошту може серйозно підірвати довіру клієнтів, партнерів та інвесторів до компанії. Багато країн (включаючи Україну з її Законом «Про захист персональних даних», а також міжнародні норми на кшталт GDPR) вимагають належного захисту персональних даних.

Також необхідно відмітити, що сучасні кіберзагрози стають все більш витонченими (цільовий фішинг, використання можливостей штучного інтелекту для створення переконливих шахрайських листів), що вимагає постійного вдосконалення засобів захисту.

Таким чином, захист корпоративної електронної пошти – це не просто технічна необхідність, а фундаментальний елемент загальної стратегії кібербезпеки, управління ризиками та забезпечення безперервності бізнесу в сучасному цифровому світі. Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження методів та засобів захисту корпоративної електронної пошти на базі FortiMail.

Об'єкт дослідження – захист корпоративної електронної пошти.

Предмет дослідження – методи та засоби захисту корпоративної електронної пошти на базі FortiMail.

Мета роботи – розробити варіант системи захисту корпоративної електронної пошти на базі FortiMail та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми захисту корпоративної електронної пошти;

проаналізувати підходи до захисту корпоративної електронної пошти;

проаналізувати існуючі рішення для захисту корпоративної електронної пошти;

проаналізувати методи та засоби захисту корпоративної електронної пошти на базі FortiMail;

розробити варіант системи захисту корпоративної електронної пошти на базі FortiMail.

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

Практичне значення одержаних результатів: запропоновано варіант системи захисту корпоративної електронної пошти на базі FortiMail, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ

1.1. Дослідження проблеми захисту корпоративної електронної пошти

За даними BEC Global Insights [1] обсяг атак на компрометацію бізнес-електронної пошти (Business Email Compromise, BEC) зменшився на 13% у лютому 2025 року порівняно з січнем 2025 року (рисунок 1.1).

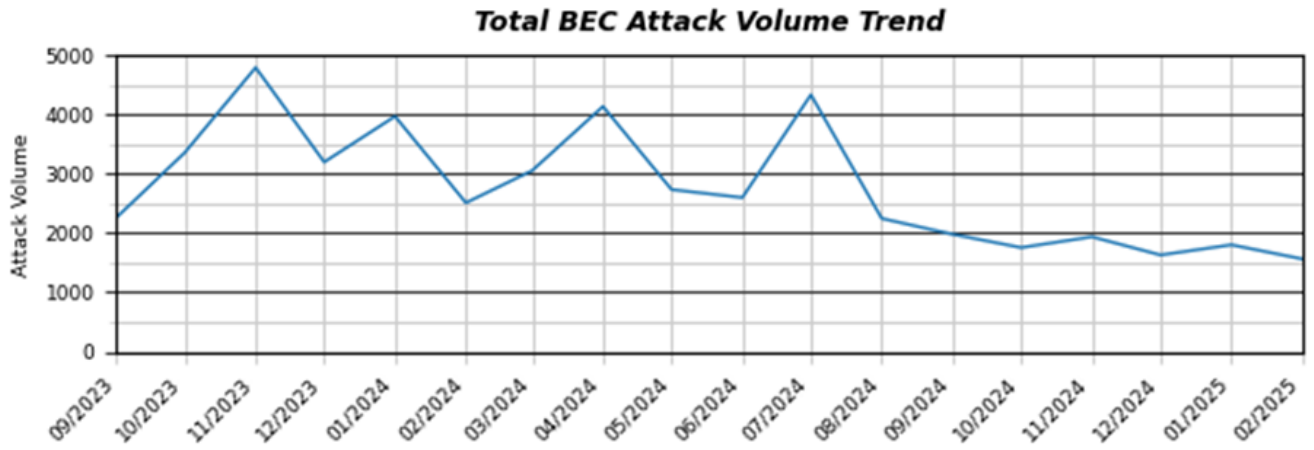

Рис. 1.1. Обсяг атак на компрометацію бізнес-електронної пошти [1]

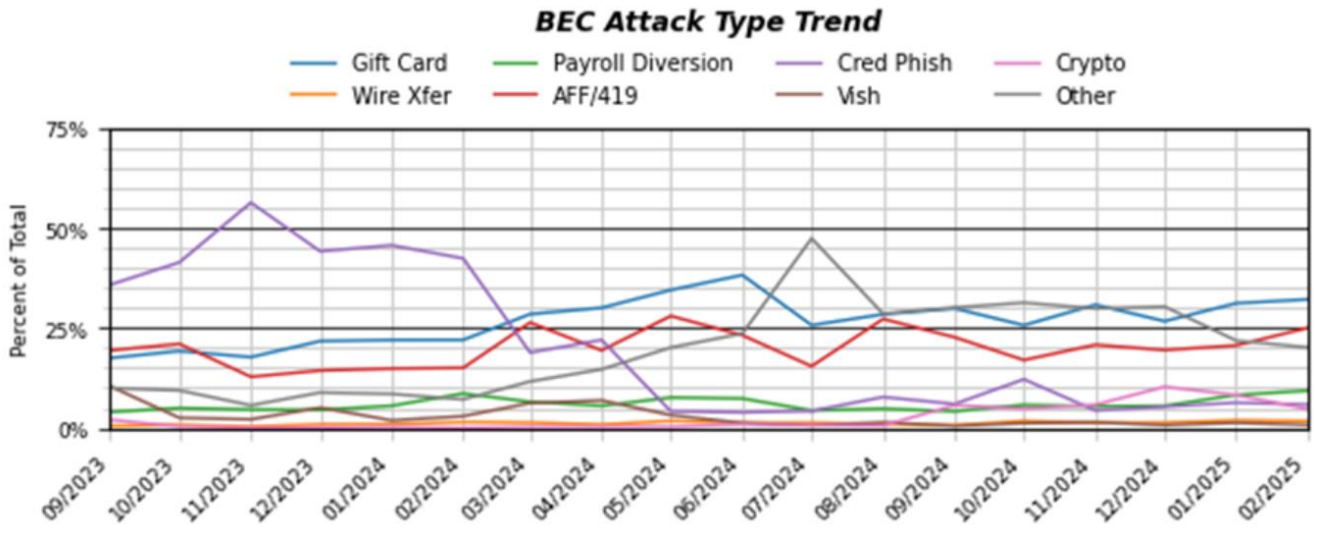

Рис. 1.2. Типи атак на компрометацію бізнес-електронної пошти [1]

У [1] зазначається, що подарункові картки були найпоширенішим методом виведення готівки (32,2%), далі йшли шахрайство з розширеними комісіями (25,1%), перенаправлення заробітної плати (9,4%), фішинг облікових даних (5,9%), криптовалюта (4,8%), банківські перекази (1,8%) та вішинг (0,8%). Двадцять відсотків атак у лютому 2025 року стосувалися запитів на різні інші види платежів (рисунок 1.2).

73% атак BEC було надіслано з адрес електронної пошти, розміщених на безкоштовних постачальниках веб-пошти, порівняно з 27% атак, надісланих зі зловмисно зареєстрованих доменів. Відсоток використовуваних постачальників безкоштовної веб-пошти зменшився у лютому порівняно з 72% у січні 2025 року [1] (рисунок 1.3).

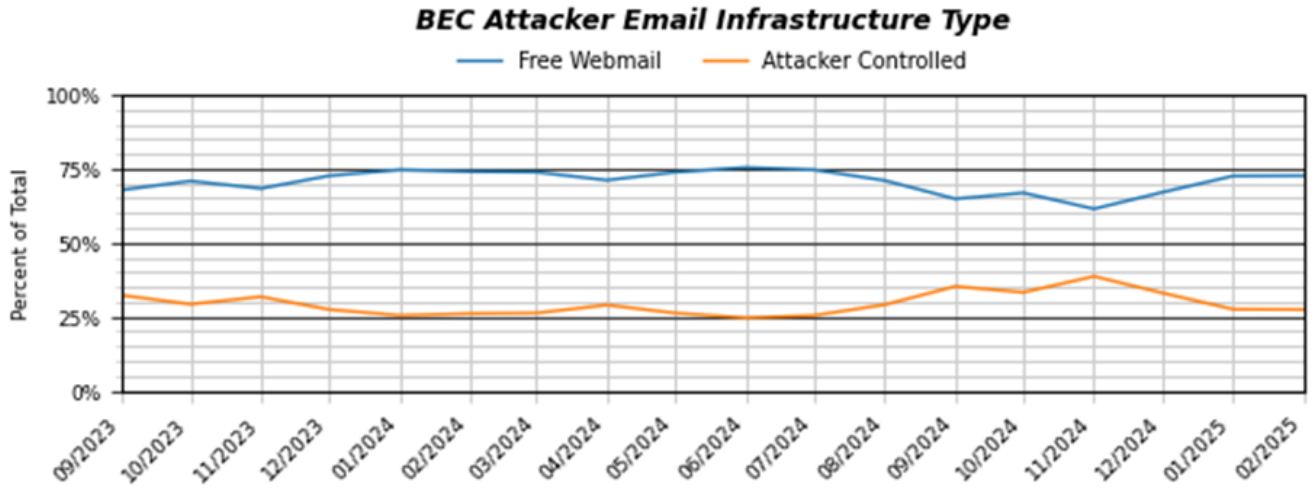

Рис. 1.3. Типи джерел атак на компрометацію бізнес-електронної пошти [1]

У лютому 2025 року Google був основним постачальником веб-пошти, який використовували актори для надсилання кампаній BEC, складаючи 76% з 1036 безкоштовних облікових записів веб-пошти, що використовувалися шахраями. Серед інших популярних постачальників веб-пошти були Microsoft та Verizon Media [1] (рисунок 1.4).

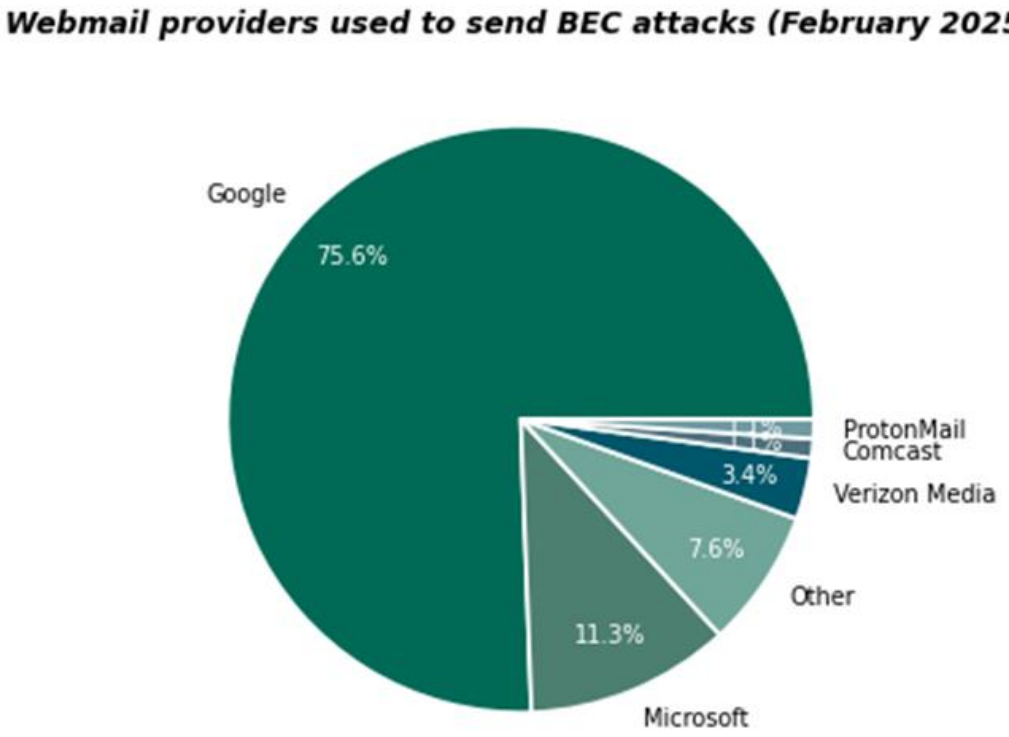

Рис. 1.4. Постачальники веб-пошти, який використовували актори для надсилання кампаній BEC [1]

У [2] зазначається, що компрометація ділової електронної пошти продовжує залишатися однією з найбільш фінансово збиткових кіберзагроз у 2025 році. Атаки на компрометацію ділової електронної пошти становили 73% усіх зареєстрованих кіберінцидентів у 2024 році.

У [2] визначається, що компрометація ділової електронної пошти (BEC) – це кіберзагроза фінансового характеру, яка передбачає атаку злочинців на існуючі ділові зв’язки. Ці зловмисники видають себе за довірених контактів або організації, щоб маніпулювати жертвами та змусити їх здійснювати несанкціоновані фінансові перекази. Зловмисники можуть змінювати законні рахунки-фактури або створювати переконливі підробки. А в деяких випадках ці шахрайства передбачають фактичне компрометування облікових записів електронної пошти для підвищення привілеїв та ефективності шахрайських повідомлень (рисунок 1.5).

У 2025 році ландшафт загроз демонструє тривожну тенденцію до атак BEC – з розвитком тактики та посиленням атак на певні галузі [2].

Рис. 1.5. Приклад змісту атаки на компрометацію бізнес-електронної пошти [2]

Приблизно 66% спроб фішингу були зосереджені на ресурсах організації, переважно з використанням методів крадіжки облікових даних та підроблених платіжних документів. Решта 34% атак були спрямовані на особисту інформацію, зокрема фінансові дані, причому зловмисники часто маскувалися під служби доставки або банківські установи [2].

Дослідження [2] показують 30% зростання атак BEC станом на березень 2025 року. Атаки BEC є другим найдорожчим типом порушення, їхня вартість у середньому становить 4,89 мільйона доларів. Атаки BEC становлять понад 50% усіх інцидентів соціальної інженерії . Навіть організації з менш ніж 1000 співробітниками мають 70% ймовірність щотижня зіткнутися з принаймні однією атакою BEC. Середній запит на банківський переказ BEC на початку 2025 року становив 24 586 доларів США. Дані Verizon також показують, що частота використання претензійних текстових повідомлень (тактика, що лежить в основі BEC) минулого року зросла майже вдвічі.

Дослідження [2] свідчать про те, що зловмисники використовують дедалі просунутіші технології для створення переконливих імітацій. Злочинці, що використовують фішингові електронні листи, чудово вміють використовувати

претексти – вони видають себе за генеральних директорів, фінансових директорів, інших керівників або зовнішніх партнерів/постачальників. У понад 60% фішингових електронних листів зловмисники видають себе за відомий бренд або організацію, щоб скористатися існуючою довірою.

У багатьох електронних листах BEC змінюється ім’я, щоб представити високопоставлену особу – це спостерігалося в 36% електронних листів BEC в одному дослідженні. Атаки з використанням методу вішингу стають все більш поширеними, і 30% організацій повідомляють про випадки, коли зловмисники використовували фальшиві дзвінки, щоб видавати себе за посадовців або керівників. Зловмисники зараз використовують інструменти штучного інтелекту для полірування своїх повідомлень, пов’язаних із фішингом BEC. До другого кварталу 2024 року близько 40% фішингових листів BEC позначалися як контент, створений штучним інтелектом [2].

Palo Alto Networks [4] визначає компрометацію ділової електронної пошти (BEC) як цілеспрямовану кібератаку з використанням соціальної інженерії, яка використовує довіру до корпоративних поштових систем, щоб маніпулювати співробітниками та змушувати їх ініціювати несанкціоновані транзакції або розголошувати конфіденційну інформацію. Зловмисники часто захоплюють або підробляють облікові записи електронної пошти керівників, використовуючи крадіжку облікових даних, імітацію доменів або методи втоми багатофакторної автентифікації (MFA). Потрапивши в ланцюжок зв’язку, зловмисники проводять розвідку, щоб імітувати стилі письма, посилатися на реальні проекти та перенаправляти платежі або дані на контрольовані зловмисниками місця призначення [4].

Компрометація ділової електронної пошти (BEC) спрямована на людський та процедурний рівні електронного спілкування. Замість того, щоб використовувати технічні слабкі місця в інфраструктурі електронної пошти, вона намагається маніпулювати легітимними каналами зв’язку, щоб обдурити цілі та перенаправити довірені дії – найчастіше пов'язані з коштами, обліковими даними або конфіденційними даними [4].

Згідно з фреймворком MITRE ATT&CK, BEC відповідає T1586.002 (Компрометація інфраструктури: домен) і часто перетинається з T1566.002 (Фішинг: Підшвидкісний фішинговий зв'язок) та T1556.002 (Зміна процесу автентифікації: Модифікація довіри домену) залежно від етапу та способу доставки [4].

Компрометація ділової електронної пошти досягається завдяки імітації легітимного листування, позиціонуванню себе саме в потрібний момент бізнес-процесу та надсиланню запиту, який є процедурно обґрунтованим, але стратегічно шкідливим [4].

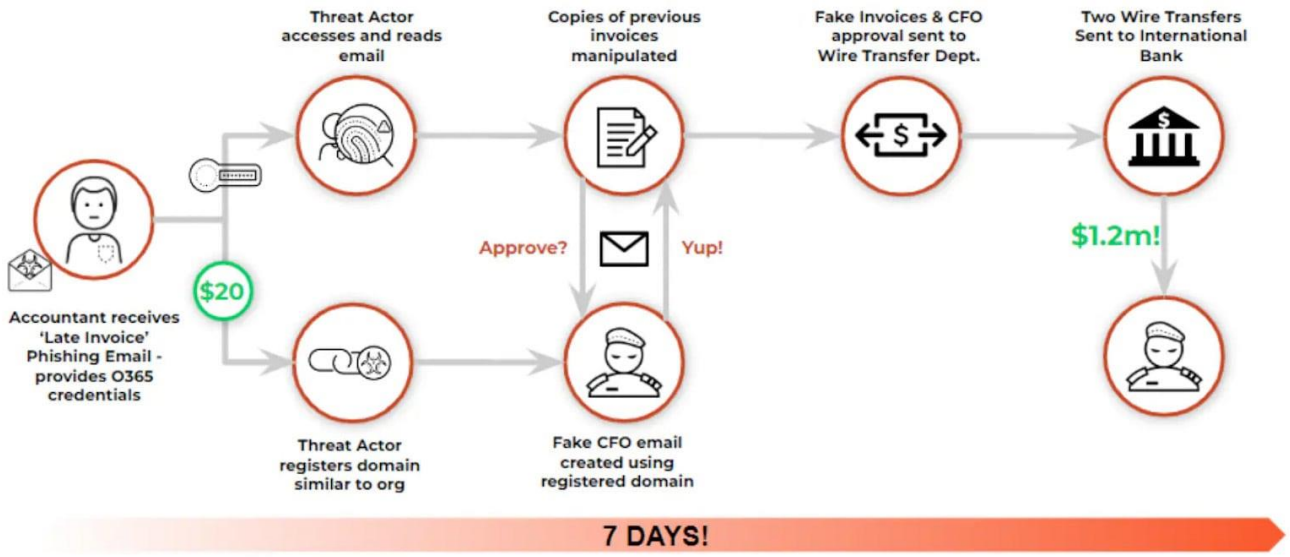

Рис. 1.6. Схема соціальної інженерії компрометації ділової електронної пошти [4]

Необхідно підкреслити, що компрометація ділової електронної пошти виступає в ролі засобу сприяння розвитку проміжного ланцюга в зловмисних кампаніях. Вона рідко є точкою входу і не є кінцевою метою. Натомість, компрометація ділової електронної пошти забезпечує точку повороту, яка перетворює цифровий доступ на операційний вплив. У разі успішного виконання вона дозволяє кіберзлочинцям обходити засоби контролю автентифікації, забезпечення дотримання політик та виявлення аномалій, працюючи в рамках довіреної бізнес-логіки [4].

Низький технічний профіль та високий вплив BEC роблять його привабливим як для державно-орієнтованих груп, так і для фінансово мотивованих суб'єктів. Його гнучкість дозволяє йому функціонувати в різних вертикалях та на різних етапах розвитку атаки [4].

Слід звернути увагу на те, що компрометація ділової електронної пошти не генерує традиційних індикаторів компрометації. Немає хешу шкідливого програмного забезпечення, немає ланцюжка експлойтів і часто немає аномальної активності файлів. Виявлення залежить від розпізнавання ледь помітних змін у поведінці в довірених системах. Проблема полягає в тому, що BEC зазвичай працює в межах автентифікованих сеансів, використовуючи легітимну інфраструктуру [4].

Визначення BEC вимагає нашарування сигналів ідентифікації, поведінки повідомлень та телеметрії доступу. Системи повинні співвідносити контекст користувача з шаблонами зв'язку, щоб виявити зловживання, які виглядають авторизованими на рівні протоколу, але явно не відповідають бізнес-логіці.

1.2. Аналіз підходів до захисту корпоративної електронної пошти

Microsoft [3] визначає такі основні стратегії запобігання та виявлення атак BEC: щоб зупинити атаку BEC на ранніх стадіях, потрібне поєднання проактивних заходів, технологічного захисту та чіткого плану реагування на проблеми.

Необхідно проводити організаційні заходи та навчання співробітників [3]. Перша лінія захисту – це співробітники, а обізнаність перетворює потенційні слабкі ланки на союзників у кібербезпеці. Співробітники повинні знати, як розпізнати:

фішингові посилання;

невідповідність домену та адреси електронної пошти;

підозріло термінові запити.

Розгортання та застосування безпечних шлюзів електронної пошти та інші

технічні рішення [3].

Методи та засоби, які можуть посилити корпоративний захист. Інструменти, призначені для виявлення та блокування шкідливих електронних листів, включають [3]:

шлюзи безпечної електронної пошти (SEG) – вони діють як фільтр, аналізуючи вхідні повідомлення на наявність ознак шахрайства або підробки;

багатофакторна автентифікація (MFA) – навіть якщо шахраї отримують доступ до облікових даних, MFA додає додатковий рівень безпеки;

автентифікація, звітування та відповідність повідомлень на основі домену (DMARC) – цей протокол допомагає запобігти підміні електронного домену зловмисниками.

Впровадження цих інструментів може значно знизити ризик успішної атаки BEC.

Приблизні дії щодо реагування на підозрювану атаку BEC [3]:

припинення транзакції — якщо було ініційовано банківський переказ, негайно зверніться до свого банку, щоб зупинити або скасувати платіж;

повідомлення служби захисту – вони можуть дослідити джерело електронного листа та заблокувати подальше спілкування від зловмисника;

перегляд та оновлення процесів – пошук вразливостей у існуючих протоколах безпеки та усунення їх, щоб запобігти майбутнім інцидентам.

Наявність Плану реагування на інциденти безпеки є недохідною умовою протидії атакам BEC.

Microsoft [3] зазначає, що зростання штучного інтелекту для кібербезпеки та машинного навчання змінює правила гри в безпеці електронної пошти. Ці технології можна застосовувати для:

аналізу моделі поведінки електронної пошти, щоб виявити аномалії, такі як раптовий запит на банківський переказ;

визначення ледь помітних ознак підробки, такі як незначні варіації в адресах електронної пошти;

постійного адаптування до нових загроз, що ускладнює шахраям

випередження інструментів виявлення.

Microsoft [3] зазначає, що атаки BEC не є загрозою типу «налаштував і забув». Шахраї постійно вдосконалюють свої методи обходу існуючих інструментів безпеки, тому потрібно бути пильними та звертати увагу на:

проведення регулярних аудитів безпеки для виявлення слабких місць у корпоративному захисті.

проведення оновлення програмного забезпечення для виправлення вразливостей та забезпечення захисту від нових експлойтів;

постійний моніторинг загроз для виявлення незвичайної активності в режимі реального часу, від підозрілих шаблонів електронної пошти до спроб несанкціонованого доступу.

DMARC (Domain-based Message Authentication, Reporting and Conformance – автентифікація, звітність та відповідність повідомлень на основі домену) – це протокол автентифікації електронної пошти, який базується на SPF та DKIM для запобігання підробці домену. Якщо встановлено значення «відхилити», він повідомляє поштовим серверам-отримувачам про необхідність блокувати неавтентифіковані повідомлення, які, здається, надходять з вашого домену. Без застосування DMARC зловмисники можуть підробити домен вашого бренду в кампаніях BEC, не викликаючи помилок доставки повідомлень або сповіщень.

DMARC – це метод, який використовується для перевірки електронних листів, що надсилаються та одержуються корпоратвиними поштовими доменами. DMARC – один з кращих способів захисту організацій від спуфінгу домену, фішингу та інших кібератак на основі електронної пошти.

Стандарт DMARC було розроблено у 2012 році провідними галузевими організаціями, включаючи PayPal, Google, Microsoft. DMARC використовує існуючі методи автентифікації електронної пошти для захисту підприємств від підроблених доменів [5].

DMARC – дві важливі функції безпеки електронної пошти [5]:

дозволяє організаціям наочно відстежувати свої канали електронної пошти. Організації можуть бачити надіслані та отримані електронні листи, а також їхню

репутацію;

організації можуть блокувати шкідливі електронні листи, які надсилаються через їхні домени, щоб захистити своїх клієнтів та замовників від підроблених доменних повідомлень та фішингових атак.

DMARC використовує методи автентифікації електронної пошти Sender Policy Framework (SPF) та Domain Keys Identified Mail (DKIM).

SPF – це метод перевірки автентичності електронної пошти, який використовується для запобігання використанню вашого домену кіберзлочинцями для масового розсилання спаму. Використовуючи SPF, організація може публікувати авторизовані поштові сервери, які повідомляють приймаючим системам, наскільки надійним є джерело електронної пошти. SPF використовує DNS (службу доменних імен), щоб дати користувачам можливість вказати, яким поштовим серверам дозволено надсилати електронні листи з ваших доменів [5].

DKIM – це метод автентифікації електронної пошти, який дозволяє одержувачам переконатися, що електронні листи були надіслані та авторизовані власником домену, з якого було надіслано електронного листа. Це допомагає користувачам уникнути атак фішингу, які видають себе за відомі домени електронної пошти. Це досягається шляхом надання електронній пошті цифрового підпису DKIM, який додається до справжніх електронних листів і шифрується [5].

Використання DMARC означає, що електронні листи, які правильно налаштовані та автентифіковані, не будуть помічені одержувачами електронної пошти як спам або зловмисне програмне забезпечення. Це допомагає підвищити ймовірність того, що ваші повідомлення електронної пошти побачать одержувачі, і вони (листи) не потраплять до папки небажаної пошти або спаму [5].

Політика DMARC дозволяє відправнику вказати, що його повідомлення захищені SPF та/або DKIM, і повідомляє одержувачу, що робити, якщо жоден із цих методів автентифікації не пройде – наприклад, відхилити повідомлення або відхилити його. DMARC усуває здогадки з обробки одержувачем цих невдалих повідомлень, обмежуючи або усуваючи вплив потенційно шахрайських та

шкідливих повідомлень на користувача. DMARC також надає одержувачу електронної пошти спосіб повідомляти відправнику про повідомлення, які пройшли та/або не пройшли оцінку DMARC [6] (рисунок 1.7).

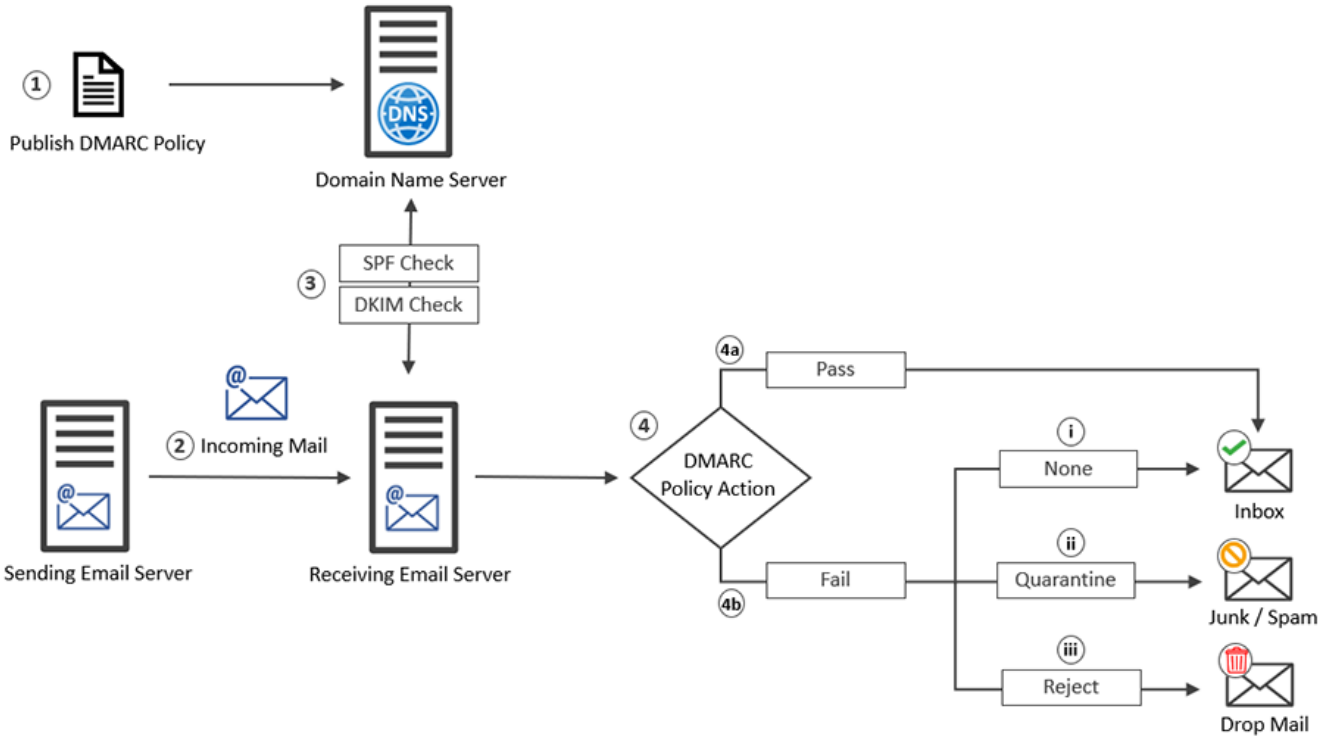

Рис. 1.7. Схема роботи за протоколом DMARC [6]

Основні кроки за протоколом DMARC (рисунок 1.7) [6]:

1. власник домену публікує політику DMARC на відповідному сервері доменних імен;

2. поштовий сервер-отримувач отримує вхідну пошту від поштового сервера-відправника;

3. поштовий сервер, що приймає, виконує перевірки DKIM/SPF відповідно до політики DMARC власника домену;

4. поштовий сервер, що приймає, оцінює результати перевірок DKIM/SPF відповідно до політики DMARC власника домену:

a. Pass: пряма поштова розсилка до поштової скриньки одержувача;

b. Fail: застосувати дію політики DMARC (None, Quarantine, Reject);

None: пряма розсилка до поштової скриньки одержувача.

Quarantine: пряма пошта надсилається до папки небажаної пошти або спаму одержувача.

Reject: блокує отримання некваліфікованих електронних листів одержувачем.

Захист ділової електронної пошти є критично важливим для безпеки будь-якої організації. Існує багато підходів, які часто використовуються комплексно для створення багатошарової системи захисту.

Для *фільтрації спаму та шкідливого програмного забезпечення* використовуються потужні спам-фільтри та антивірусні сканери для блокування небажаних листів, фішингу та листів із шкідливими вкладеннями чи посиланнями.

Шифрування при передачі (TLS) забезпечує захист даних під час їх передачі між поштовими серверами. Більшість сучасних серверів підтримують TLS.

Шифрування вмісту листа (End-to-End Encryption, E2EE) – використання технологій типу S/MIME або PGP – для шифрування самого тіла листа та вкладень так, що прочитати їх може лише отримувач з відповідним ключем.

Пісочниця (Sandboxing) застосовується для автоматичного аналізу підозрілих вкладень та посилань у безпечному ізольованому середовищі перед тим, як вони потраплять до користувача.

Захист від фішингу та цільових атак забезпечують спеціалізовані рішення, які використовують машинне навчання та аналіз поведінки для виявлення складних фішингових атак, BEC та інших загроз, які можуть обійти стандартні фільтри.

Перевірка репутації IP-адрес та доменів застосовується для блокування листів з відомих шкідливих джерел.

URL Rewriting / Link Protection захищають від переписування посилань у листах так, щоб вони проходили через службу безпеки для перевірки в момент натискання.

Контроль доступу та автентифікація користувачів забезпечується наступним:

використовуються надійні паролі та політика паролів. Висувається вимога використання складних паролів та їх регулярна зміна;

застосування багатофакторної автентифікації (MFA/2FA). Обов'язкове використання другого фактору (код з додатку, SMS, апаратний ключ) окрім пароля для входу в поштову скриньку. Це один з найефективніших способів захисту від несанкціованого доступу;

контроль доступу на основі ролей (RBAC). Надання користувачам лише тих прав доступу до поштових ресурсів, які необхідні для виконання їхніх обов'язків;

реалізація політики умовного доступу (Conditional Access). Обмеження доступу до пошти на основі геолокації, стану пристрою, IP-адреси тощо.

Застосування систем DLP (Data Loss Prevention) – сканування вихідної пошти, впровадження політик DLP для автоматичного виявлення та блокування/попередження відправки листів, що містять конфіденційну інформацію (номери кредитних карток, персональні дані тощо).

1.3. Аналіз існуючих рішень для захисту корпоративної електронної пошти

Платформи безпеки електронної пошти забезпечують захист від спаму, фішингу та компрометації ділової електронної пошти [7].

Gartner [7] визначає платформу безпеки електронної пошти як продукт, що захищає інфраструктуру електронної пошти. Її основна мета – видалення шкідливих (фішинг, соціальна інженерія, віруси) або небажаних повідомлень (спам, маркетинг). Інші функції включають захист даних електронної пошти, автентифікацію повідомлень на основі домену, звітність та відповідність (DMARC), розслідування та виправлення через спеціальну консоль. Вони можуть інтегруватися як безпечний шлюз електронної пошти (SEG) для захисту перед доставкою або як інтегроване хмарне рішення для безпеки електронної пошти (ICES) для захисту після доставки.

Платформи безпеки електронної пошти захищають інфраструктуру

електронної пошти організації від соціальної інженерії, фішингу, компрометації ділової електронної пошти, спаму, атак шкідливого програмного забезпечення та крадіжки даних. Платформи безпеки електронної пошти розгортаються незалежно, але інтегруються з іншими засобами контролю безпеки мережі та кінцевих точок для покращення загального стану безпеки організації. Платформи безпеки електронної пошти пропонують командам кібербезпеки видимість інцидентів безпеки, пов'язаних з електронною поштою, для розслідування та усунення наслідків [7].

Gartner [7] визначає наступні обов’язкові функції платформи безпеки електронної пошти:

сканування повідомлень, тіла та заголовків на наявність фішингу та спаму;

перевірка вкладень та їх карантин або деактивація;

аналіз та захист URL-адрес;

захист даних електронної пошти, включаючи функції шифрування та запобігання втраті даних.

Загальні характеристики платформи безпеки електронної пошти включають [7]:

управління DMARC/ідентифікованою поштою з ключами домену (DKIM)/ фреймворком політики відправника (SPF);

запобігання захопленню облікового запису;

захист інструментів для співпраці/продуктивності;

навчання з питань обізнаності;

агент передачі повідомлень (MTA).

Рис. 1.8. Магічний квадрант для платформ безпеки електронної пошти [7]

Abnormal Security є лідером за Gartner [7]. Платформа штучного інтелекту Abnormal Human Behavior аналізує поведінку користувачів, щоб виявляти та усувати загрози. Вона також підтримує власну базу даних постачальників для відстеження моделей бізнес-комунікацій та виявлення атак на ланцюги поставок.

Abnormal покращила інтеграцію зі сторонніми інструментами, включаючи інструменти SIEM, ITSM та EPP, що дозволяє проводити розслідування та виправлення з-за меж своєї платформи. Компанія також інтегрувала

функціональність чат-бота зі штучним інтелектом для покращення попереднього звітування про фішингові випадки [7].

Платформа штучного інтелекту для аналізу аномальної людської поведінки підходить для широкого кола організацій, що зосереджені на основній безпеці електронної пошти та вищому рівні автоматизованих функцій захисту електронної пошти [7].

Відповідність Abnormal Security вимогам ринку підкріплюється потужними циклами зворотного зв’язку з клієнтами та розробкою функцій, що відповідають вимогам клієнтів та ринку. Abnormal впроваджує інновації шляхом швидкого впровадження нових функцій, внутрішніх процесів та структур підтримки [7].

Основні можливості рішення Abnormal Security [8]:

забезпечує цілісний захист електронної пошти. Поведінковий штучний інтелект додає глибоке розуміння того, що є нормальним, виявляє тонкі загрози та ідентифікує аномалії у моделях комунікації;

прискорює автоматизацію за допомогою штучного інтелекту. Повністю автоматизує безпеку на хмарній платформі електронної пошти за допомогою передового штучного інтелекту для виявлення та усунення загроз;

забезпечує рівномірний кросплатформний захист. Розширює багаторівневі заходи безпеки для послідовного захисту на всіх каналах зв'язку та усуває необхідність у надлишкових SEG.

Як хмарна платформа безпеки електронної пошти на основі API, Abnormal використовує поведінкову науку про дані, щоб зупинити невідомі атаки, які обходять традиційні інструменти безпеки. Там, де застарілі рішення для безпеки електронної пошти покладаються на правила та політики для виявлення атак, Abnormal пропонує принципово інший підхід, який точно виявляє та автоматично усуває загрози електронної пошти [8]. Trend Micro є лідером за Gartner [7]. Її флагманський продукт ESP, Trend Vision One Email and Collaboration Security, можна поєднувати з широким набором додаткових рішень постачальника в сегменті ESP, таких як XDR for Email.

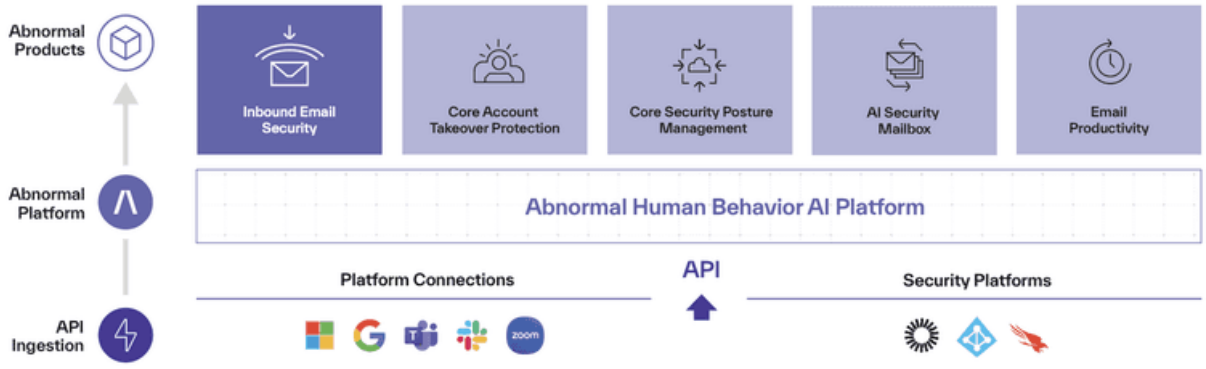

Рис. 1.9. Основні можливості рішення Abnormal Security [8]

Trend Micro пропонує додаткові можливості безпеки електронної пошти, такі як DLP та шифрування, а також функції навчання з безпеки та обізнаності. Флагманський продукт Trend Micro, ESP, підходить для широкого кола організацій по всьому світу, включаючи клієнтів, які прагнуть консолідації постачальників рішень безпеки, та тих, хто шукає інтегровані можливості безпеки робочого простору.

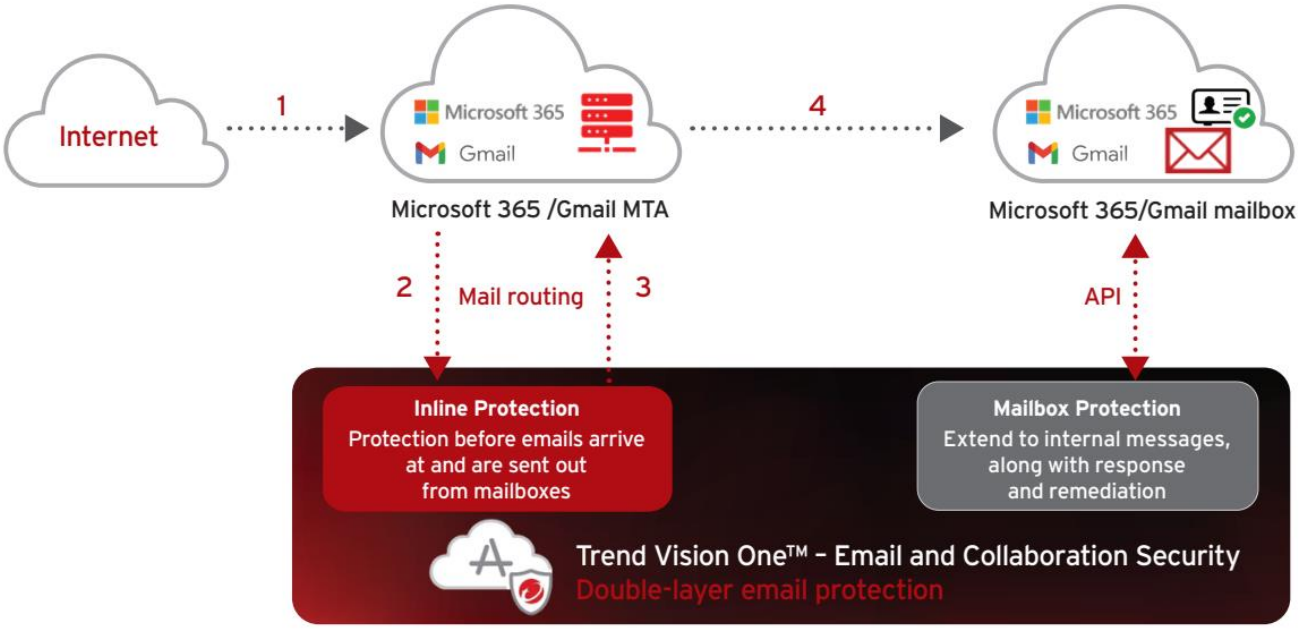

Рис. 1.10. Схема роботи Trend Vision One – Email and Collaboration Security [9]

Trend Micro пропонує універсальні можливості впровадження, проектування архітектури та адміністрування, зберігаючи при цьому високий

ступінь зручності використання. Trend Micro має чіткий процес збору та впровадження відгуків клієнтів для покращення функцій.

Proofpoint є лідером за Gartner [7]. Його флагманський продукт ESP, Proofpoint Threat Protection, включає панелі керування ризиками, захист від шахрайства електронною поштою та функції DLP, які є одними з найповніших пропозицій на ринку у відповідних категоріях.

Proofpoint Threat Protection підходить широкому колу організацій, особливо великим підприємствам та тим, хто шукає повнофункціональну платформу безпеки. Proofpoint пропонує широкий набір інструментів платформи та потужні можливості виявлення. Розширення функцій Proofpoint, такі як впровадження захисту від неправильно спрямованої пошти, відповідають новим загрозам та вимогам клієнтів [7].

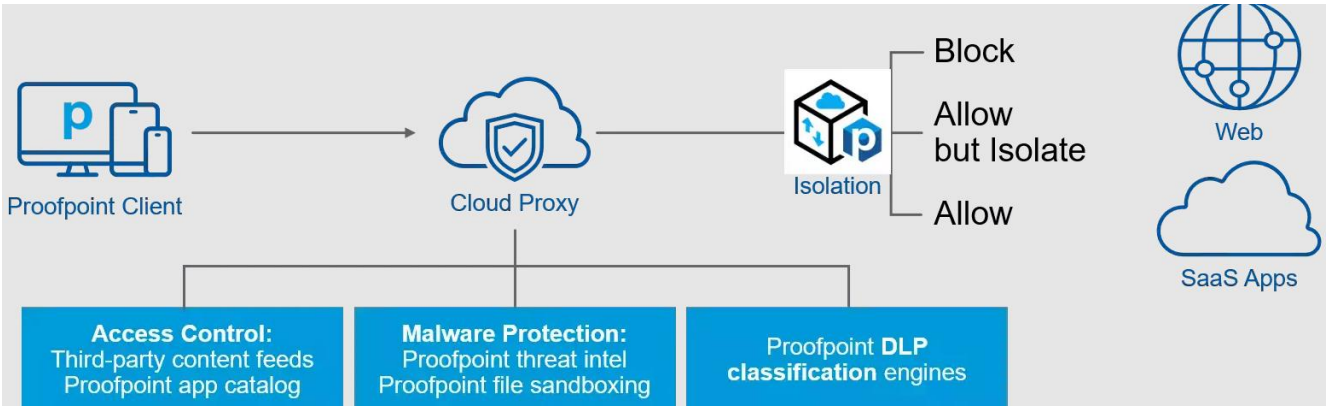

Рис. 1.11. Основні можливості рішення Proofpoint Threat Protection [10]

Gartner [7] зазначає, що інфраструктура електронної пошти переважно перейшла в хмару, що збільшує ринковий потенціал для постачальників, які в першу чергу забезпечують безпеку поза межами традиційного впровадження шлюзів безпечної електронної пошти (SEG). Досягнення в технологіях, що використовуються в платформах безпеки електронної пошти (ESP), значно змінилися за останнє десятиліття, особливо щодо трьох областей: впровадження, виявлення соціальної інженерії та варіації можливостей продукту.

Інтегровані рішення для хмарної безпеки електронної пошти (ICES)

найчастіше стосуються ESP, які використовують API-з’єднання з існуючою поштовою інфраструктурою для моніторингу вхідних повідомлень. Хоча деякі з них також можуть використовувати ведення журналу для мінімізації часу виявлення, функція виправлення залишається такою ж. Рішення ICES значно зменшують складність впровадження, терміни та, як наслідок, можливість конкурентного порівняння ефективності різних ESP. Вони дедалі більше кидають виклик стандарту вбудованої безпеки електронної пошти, а це означає, що організації тепер повинні розглянути ідеальну схему впровадження, перш ніж остаточно вибрати постачальника.

Одночасно з розвитком рішень ICES, досягнення в обробці природної мови (NLP) та поява моделей великих мов (LLM) змінили як те, як організації атакуються, так і те, як постачальники електронних послуг (ESP) захищаються від атак соціальної інженерії. Люди дедалі менше здатні виявляти атаки соціальної інженерії, оскільки LLM удосконалюються зловмисниками для конкретних цілей. ESP дедалі більше розвивають можливості програмного зчитування та розуміння вмісту електронної пошти в контексті соціальної інженерії. Деякі постачальники включають аналіз соціальних графів для виявлення шаблонів обміну повідомленнями серед соціальних груп та контекст ідентифікації для підвищення точності обробки підозрілої пошти. Gartner [7] вважає це важливими компонентами майбутнього безпеки електронної пошти.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ НА БАЗІ FORTIMAIL

2.1. Призначення та основні функції рішення FortiMail

Завдяки найкращій у своєму класі ефективності, рішення FortiMail забезпечує багаторівневий захист від усього спектру загроз, що передаються електронною поштою. FortiMail допомагає виявляти та запобігати атакам через електронну пошту, включаючи спам, фішинг, розсилку шкідливих програм та посилань, заміну відправника та компрометацію ділової електронної пошти (BEC) [12].

Рішення FortiMail забезпечує захист від загроз, що передаються електронною поштою. Ефективний засіб захисту від спаму і шкідливого ПЗ включає технології захисту від масових розсилок і вірусних кампаній, реконструкції листів і вкладень з видаленням (знешкодженням) небезпечного вмісту, аналізу поведінки в «пісочниці», захисту від підміни [12].

Відмічається, що Fortinet є одним із небагатьох виробників, які регулярно підтверджують ефективність своїх рішень у рамках незалежних тестувань галузевими лабораторіями. FortiMail присвоєно рейтинг AAA лабораторією SE Labs, а Virus Bulletin підтвердив ефективність в 99.78% проти спаму [12].

FortiMail є частиною екосистеми безпеки. FortiMail також дозволяє забезпечити захист електронної пошти для Microsoft 365 за рахунок інтеграції на рівні API. За підтримки FortiGuard Labs FortiMail використовує індикатори компрометації від Fortinet FortiGuard Labs. спам листів на день, 136 тис. фішингові листи в хвилину і є однією з провідних груп з дослідження загроз [12].

Основними функціями рішення FortiMail є (рисунок 2.1) [12]:

проактивна безпека електронної пошти. FortiMail дозволяє компенсувати весь спектр ризиків інформаційної безпеки, з якими стикається організація під час використання електронної пошти;

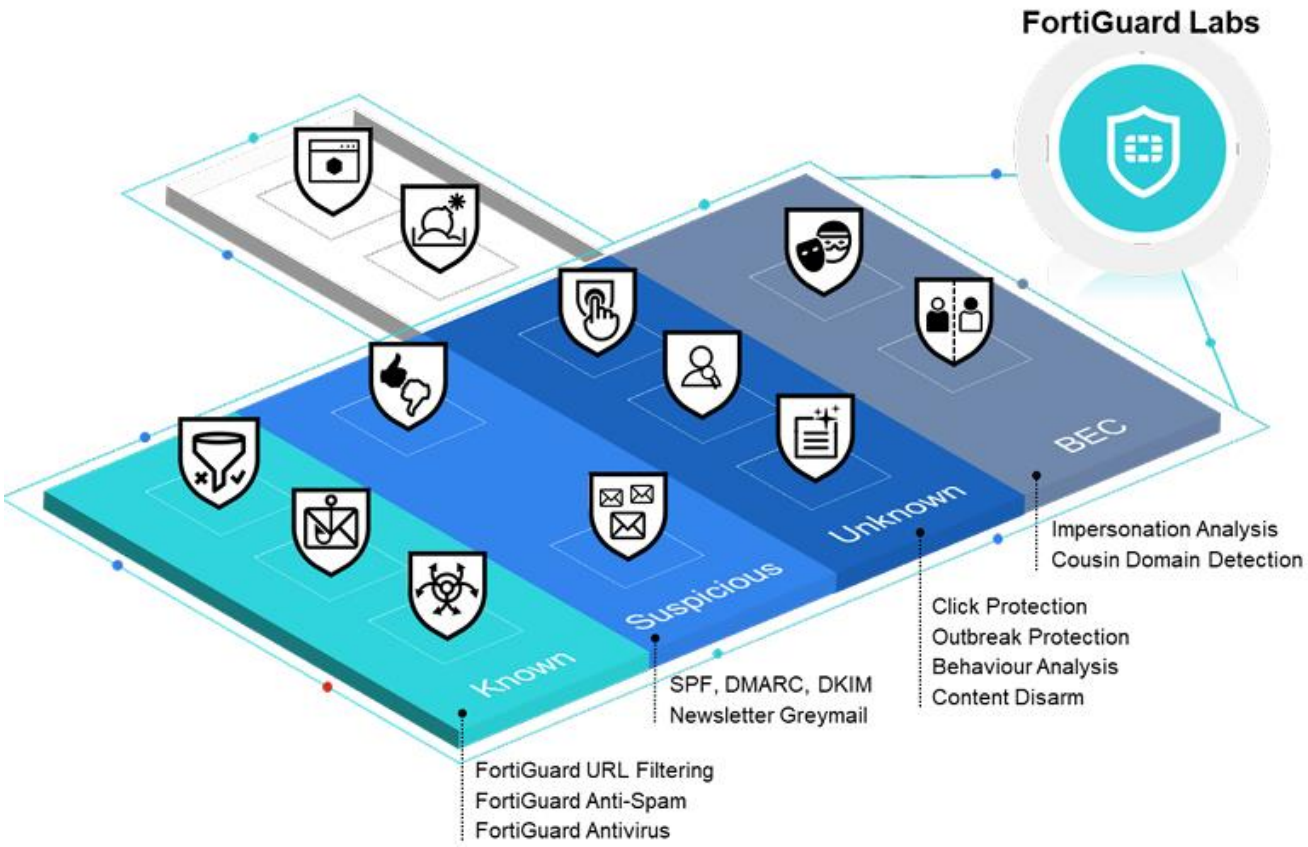

Рис. 2.1. Основні функції рішення FortiMail [12]

багаторівневий захист від спаму. Для захисту користувачів від спаму та небажаної пошти використовуються різні техніки перевірки відправника, інспекції SMTP протоколу та контенту, що пересилається. Для забезпечення безпеки та виключення помилкових спрацьовувань FortiMail комбінує аналіз репутації, автентифікацію відправника (SPF, DKIM, DMARC), верифікацію одержувача, географічне розташування відправника. Вкладення та структура повідомлень аналізуються на наявність шкідливого програмного забезпечення, посилань на небезпечні та небажані ресурси, ключових слів, зображень. Ці техніки дозволяють відсікти 99,7% спаму;

захист від шкідливого програмного забезпечення. За допомогою спільного використання технік статичного та динамічного аналізу, а також сигнатур, евристики та аналізу поведінки підозрілих файлів FortiMail захищає від усіх типів шкідливого програмного забезпечення;

захист від просунутих атак. Для ще більш надійного захисту від цільових

атак та компрометації ділової пошти FortiMail використовує технології знешкодження та реконструкції контенту, аналіз у «пісочниці», додаткові алгоритми захисту від заміни відправника та багато іншого;

вбудований захист даних. Широкий набір вбудованих засобів захисту від втрати даних, включаючи шифрування електронної пошти та архівацію, дозволяють захистити важливу інформацію від ненавмисної втрати. Ця функція забезпечує дотримання корпоративної політики безпеки та галузевих норм та правил;

інтуїтивно зрозуміле управління. Інтерактивні дашборди, вбудовані шаблони звітів, централізований карантин та користувальницькі дайджести, інтуїтивно зрозумілий інтерфейс управління функціями безпеки дозволяють організаціям мінімізувати витрати на впровадження та експлуатацію;

інтеграція з Fortinet Security Fabric. Інтеграції дозволяють відстежити атаку на всіх етапах і рубежах, а також дивитися не тільки туди, де зараз зловмисник, але й визначати, куди він прямує. FortiGuard Labs поширює індикатори компрометації, що детектуються, по всіх елементах Fortinet Security Fabric, дозволяючи ефективно протистояти зловмисникам на всіх вузлах розподіленого периметра безпеки.

2.2. Режими роботи рішення FortiMail

Розглянемо протоколи електронної пошти, які реалізовано в рішенні FortiMail. Існує кілька поширених стандартних протоколів електронної пошти [12]:

SMTP-адреса;

POP3;

IMAP;

HTTP та HTTPS.

Простий протокол передачі пошти (SMTP) – це стандартний протокол для надсилання електронної пошти між:

двома агентами з пересилання пошти (MTA);

поштовим агентом користувача (MUA) та MTA.

Коли користувач електронної пошти надсилає електронного листа, його MUA використовує SMTP для надсилання листа на MTA, який часто є їхнім поштовим сервером. Потім MTA використовує SMTP для прямої або опосередкованої доставки електронного листа на поштовий сервер призначення, який розміщує електронну пошту для користувача електронної пошти одержувача.

Коли MTA підключається до сервера електронної пошти призначення, він визначає, чи існує одержувач на цьому сервері. Якщо адреса електронної пошти одержувача є дійсною, MTA доставляє електронний лист на сервер електронної пошти, з якого користувачі електронної пошти можуть використовувати протокол, такий як POP3 або IMAP для отримання електронної пошти. Якщо адреса електронної пошти одержувача не існує, MTA зазвичай надсилає окреме повідомлення електронної пошти відправнику, повідомляючи його про невдалу доставку [12].

Хоча базовий протокол SMTP є простим, багато SMTP-серверів підтримують низку розширень протоколу для таких функцій, як автентифікація, шифрування, багаточастинні повідомлення та вкладення, і їх можна називати розширені SMTP-сервери (ESMTP) [12].

Пристрої FortiMail можуть сканувати SMTP-трафік на наявність спаму та вірусів, а також підтримувати кілька розширень SMTP.

Протокол поштового відділення версії 3 (POP3) – це стандартний протокол, який використовується поштовими клієнтами для отримання електронної пошти, доставленої та збереженої на поштовому сервері.

На відміну від IMAP, після того, як клієнт POP3 завантажує електронний лист на комп’ютер користувача електронної пошти, копія листа зазвичай не залишається на жорсткому диску поштового сервера. Перевагою цього є те, що це звільняє місце на жорсткому диску сервера. Недоліком цього є те, що завантажена електронна пошта зазвичай знаходиться лише на одному персональному

комп’ютері. Якщо всі їхні клієнти POP3 не налаштовані на постійне залишання копій електронної пошти на сервері, користувачі електронної пошти, які використовують кілька комп’ютерів для перегляду електронної пошти, наприклад, настільний комп’ютер і ноутбук, не зможуть переглядати з одного комп’ютера будь-які електронні листи, попередньо завантажені на інший комп’ютер [12].

Пристрої FortiMail не сканують POP3-трафік на наявність спаму та вірусів.

Протокол доступу до повідомлень в Інтернеті (IMAP) – це стандартний протокол, який використовується поштовими клієнтами для отримання електронної пошти, доставленої та збереженої на поштовому сервері.

Якщо клієнти IMAP не налаштовані для доступності офлайн, вони зазвичай спочатку завантажують лише заголовок повідомлення. Вони завантажують тіло повідомлення та вкладення лише тоді, коли користувач електронної пошти вирішує прочитати електронний лист.

На відміну від POP3, коли клієнт IMAP завантажує електронний лист на комп’ютер користувача електронної пошти, копія листа залишається на жорсткому диску поштового сервера. Перевага цього полягає в тому, що користувачі електронної пошти можуть переглядати електронні листи з кількох комп’ютерів. Це особливо корисно в ситуаціях, коли папку «Вхідні» може переглядати кілька осіб, наприклад, коли всі співробітники відділу контролюють спільну папку «Вхідні». Недоліком цього є те, що, якщо користувачі електронної пошти не видаляють електронні листи, IMAP може швидше використовувати місце на жорсткому диску сервера [12].

Пристрої FortiMail не сканують IMAP-трафік на наявність спаму та вірусів, але можуть використовувати IMAP під час роботи в режимі сервера, коли користувач електронної пошти отримує свою електронну пошту.

Захищені та незахищені протоколи передачі гіпертексту (HTTP/HTTPS), хоча й не лише для передачі електронної пошти, часто використовуються веб-поштові додатки для перегляду електронної пошти, що зберігається віддалено.

Пристрої FortiMail не сканують HTTP- або HTTPS-трафік на наявність

спаму чи вірусів, але використовують їх для відображеннякарантини та, якщо пристрій FortiMail працює в режимі сервера, FortiMail веб-пошта [12].

Рішення FortiMail легко масштабується для обробки мільйонів повідомлень за годину. Спроектоване для інфраструктур будь-якої складності, поставляється у різних варіантах виконання, підтримує чотири режими роботи [12].

Фізичні та віртуальні пристрої FortiMail призначені для організацій, які вважають за краще самостійно керувати інфраструктурою безпеки електронної пошти в рамках ЦОД, приватних чи публічних хмар.

програмно-апаратні комплекси;

віртуальні пристрої для популярних середовищ віртуалізації, включаючи:

VMWare;

Citrix XenServer;

Hyper-V;

KVM;

AWS;

Azure.

Рішення FortiMail Cloud призначене для організацій, які воліють використовувати сервіси безпеки як послугу (SaaS). Підходить як для хмарних, так і локальних варіантів виконання сервісу електронної пошти.

Розглянемо режими роботи рішення FortiMail.

Режим шлюзу (Gateway Mode). У режимі шлюзу FortiMail виконує роль поштового агента (MTA) для вхідної та вихідної електронної пошти. Проста зміна запису MX в DNS перенаправляє пошту на аналіз на FortiMail. Після фільтрації FortiMail надсилає безпечну пошту на поштовий сервер.

Інтеграція з Microsoft 365 на рівні API. При використанні Microsoft 365 як сервіс електронної пошти FortiMail може бути розгорнутий осторонь маршруту доставки електронної пошти. Функції безпеки в цьому режимі реалізуються за допомогою інтеграції FortiMail з Microsoft 365 на рівні API. Перевірка вхідного, вихідного та внутрішнього корпоративного листування здійснюється без необхідності зміни MX записів у DNS. FortiMail забезпечує виконання

корпоративних політик безпеки щодо захисту електронної пошти, відповідності вимогам галузевих стандартів, істотно доповнюючи вбудований функціонал безпеки Microsoft 365.

Прозорий режим (Transparent Mode). Прозорий режим не вимагає змін у маршрутизації електронної пошти або конфігурації поштових серверів. Особливо привабливий для операторів зв'язку, сервіс-провайдерів та постачальників послуг безпеки електронної пошти.

Режим сервера (Server Mode). FortiMail виконує функції поштового сервера з підтримкою протоколів SMTP, POP3, IMAP та доступу до поштових скриньок через веб-інтерфейс.

2.3. Основні можливості рішення FortiMail

Клієнт-серверні з'єднання та спрямованість з'єднання в SMTP відрізняються від того, як це реалізується в інших протоколах. Наприклад, у протоколі SMTP, SMTP-клієнт підключається до SMTP-сервера. Це, здається, узгоджується з традиційною клієнт-серверною моделлю зв'язку. Однак, через поняття ретрансляція в SMTP, SMTP-клієнт може бути одним із таких:

додаток електронної пошти на персональному комп'ютері користувача;

інший SMTP-сервер, який діє як агент доставки для користувача електронної пошти, пересилаючи електронний лист на сервер призначення.

Розміщення клієнтів та серверів у корпоративній мережі може вплинути на режим роботи, який обирається під час встановлення пристрою FortiMail. Якщо пристрій FortiMail працюватиме в режимі шлюзу або у режимі сервера SMTP-клієнти, включаючи SMTP-сервери, що підключаються як клієнти, мають бути налаштовані для підключення до пристрою FortiMail [12].

Такі терміни, як MTA та MUA, описують взаємозв'язки між сервером і клієнтом, специфічні для протоколів електронної пошти.

Агент передачі пошти (Mail Transfer Agent MTA) – це SMTP-сервер, який передає електронні листи на інший SMTP-сервер.

Не всі MTA є повноцінними поштовими серверами: деякі MTA існують виключно для ретрансляції електронної пошти та не розміщують облікові записи користувачів електронної пошти.

Компоненти FortiMail, що працюють у режимі шлюзу функціонують як MTA. Пристрої FortiMail, що працюють у режимі сервера як MTA та повний (SMTP, IMAP, POP3, веб-пошта) поштовий сервер.

Щоб доставити електронну пошту, якщо тільки вона не є вхідною, а поштовий сервер не має доменного імені та доступ до нього здійснюється лише за IP-адресою, MTA повинен запросити DNS-сервер для запису MX та відповідний запис.

Агент користувача пошти (Mail User Agent, MUA) або поштовий клієнт – це програмне забезпечення, таке як Microsoft Outlook, яке дозволяє користувачам надсилати та отримувати електронну пошту.

Підтримка пристроїв FortiMail SMTP- з’єднання для надсилання електронної пошти за допомогою MUA.

Пристрої FortiMail, що працюють у режиму сервера POP3 та IMAP-з’єднання для отримання електронної пошти за допомогою агента користувача пошти (MUA). Для користувачів електронної пошти, які надають перевагу використанню веб-браузерів для надсилання та отримання електронної пошти замість традиційного агента користувача пошти, пристрої FortiMail, що працюють у режимі сервера, також забезпечують веб-пошту FortiMail.

Багато функцій FortiMail, такі як проксі-сервери та політики, діють на основі спрямованості SMTP-з’єднання або електронного повідомлення. Вхідні SMTP-з’єднання складаються з тих, що призначені для SMTP-серверів, що є захищеними доменами пристрою FortiMail. Наприклад, якщо пристрій FortiMail налаштовано на захист SMTP-сервера, IP-адреса якого 192.168.0.1, пристрій FortiMail обробляє всі SMTP-з’єднання, призначені для 192.168.0.1, як вхідні.

Вихідні з’єднання складаються з тих, що призначені для SMTP-серверів, для захисту яких пристрій FortiMail не налаштовано. Наприклад, якщо пристрій FortiMail не налаштовано для захисту SMTP-сервера, IP-адреса якого 10.0.0.1, усі

SMTP-з’єднання, призначені для 10.0.0.1, будуть вважатися вихідними, незалежно від їхнього походження.

Вхідна та вихідна електронна пошта

Вхідні електронні листи складаються з повідомлень, надісланих одержувачам захищеного домену (RCPT TO:). Наприклад, якщо пристрій FortiMail налаштовано на захист SMTP-сервера з доменним ім’ям example.com, пристрій FortiMail обробляє всі електронні листи, надіслані на example.com, як вхідні.

Вихідні електронні листи складаються з повідомлень, надісланих одержувачам (RCPT TO:) у доменах, для захисту яких пристрій FortiMail не налаштовано. Наприклад, якщо пристрій FortiMail не налаштовано для захисту домену example.com, усі електронні листи, надіслані одержувачам на example.com, будуть розглядатися як вихідні, незалежно від їхнього походження.

Спрямованість на рівні з’єднання може відрізнятися від спрямованості на рівні електронних листів, що містяться в цьому з’єднанні. Можливо, що вхідне з’єднання може містити вихідне повідомлення електронної пошти, і навпаки.

Наприклад, на рисунку 2.2 з’єднання від внутрішніх поштових ретрансляторів до внутрішніх поштових серверів є вихідними з’єднаннями, але вони містять вхідні електронні листи. І навпаки, з’єднання від віддалених MUA до внутрішніх поштових ретрансляторів є вхідними з’єднаннями, але можуть містити вихідні електронні листи, якщо адреси електронної пошти одержувачів (RCPT TO:) є зовнішніми.

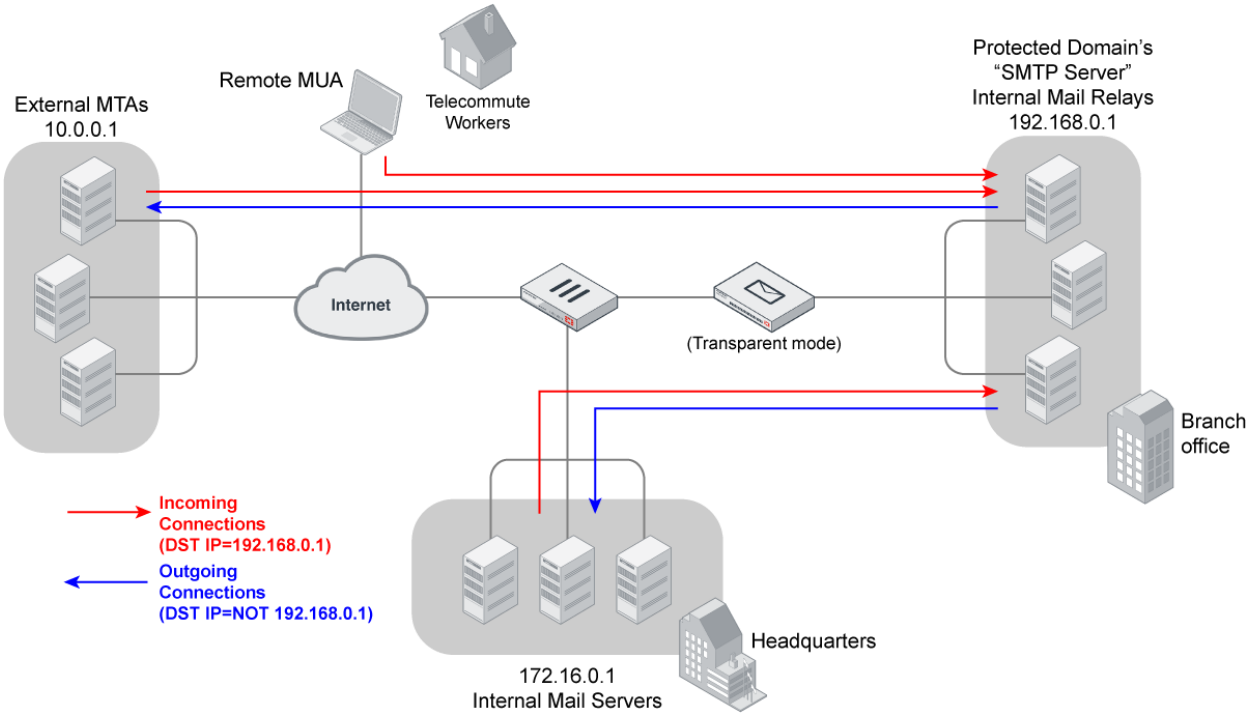

Рис. 2.2. Вхідні та вихідні SMTP-з'єднання [12]

Оскільки спрямованість розглядається окремо на мережевому рівні та рівні додатка, спрямованість SMTP-з'єднання може бути протилежною спрямованості електронного повідомлення: з'єднання може бути призначене для SMTP-сервера, який не пов'язаний із захищеним доменом, тоді як адреса електронної пошти одержувача пов'язана із захищеним доменом, або навпаки [12].

Розглянемо, як FortiMail обробляє електронну пошту. Пристрої FortiMail отримують електронну пошту для визначених доменів електронної пошти та керують ретрансляцією електронної пошти до інших доменів. Електронну пошту, що проходить через пристрій FortiMail, можна сканувати на наявність вірусів та спаму. Політики та профілі визначають, як пристрій FortiMail сканує електронну пошту та що він робить з повідомленнями електронної пошти, що містять віруси або спам. Окрім політик і профілів, інші налаштовані елементи, такі як домени електронної пошти, можуть впливати на обробку електронної пошти корпоративним пристроєм FortiMail.

Домен електронної пошти – це набір облікових записів електронної пошти, що знаходяться на певному поштовому сервері. Ім'я домену електронної пошти – це частина адреси електронної пошти користувача після @символу. Пристрої

FortiMail можна налаштувати для захисту доменів електронної пошти (які називаються «захищені домени») шляхом визначення політик і профілів для сканування та ретрансляції вхідної та вихідної електронної пошти.

Якщо пристрій FortiMail працює в режимі шлюзу або прозорому режимі, існує один локальний домен електронної пошти, який представляє сам пристрій FortiMail. Якщо пристрій FortiMail працює в режимі сервера, захищені домени знаходяться локально на вбудованому сервері електронної пошти пристрою FortiMail.

У прозорому режимі кожен мережевий інтерфейс містить проксі-сервер та/або неявний MTA, який отримує та передає електронну пошту. За замовчуванням проксі-сервер/неявний MTA відповідає на SMTP-вітання (HELO/ EHLO) з використанням імені хоста SMTP-сервера захищеного домену. Цей «маскарад» приховує існування пристрою FortiMail.

Правила контролю доступу дозволяють контролювати, як електронні листи переміщуються до, з та через пристрій FortiMail. Використовуючи правила контролю доступу, пристрій FortiMail може аналізувати електронні листи та вживати заходів на основі результату. Повідомлення можна перевіряти відповідно до адреси електронної пошти відправника, адреси електронної пошти одержувача та IP-адреси або імені хоста системи, яка доставляє електронне повідомлення.

Кожне правило контролю доступу визначає дію, яку потрібно виконати для відповідного електронного листа.

Перевірка адреси одержувача. Перевірка адреси одержувача гарантує, що пристрій FortiMail відхилить електронні листи з недійсними одержувачами та не скануватиме й не надсилатиме їх на захищений поштовий сервер. Ця перевірка може зменшити навантаження на пристрій FortiMail, коли спамер намагається надсилати повідомлення всім можливим одержувачам на поштовому сервері.

Якщо використовується перевірка адреси одержувача, то потрібно перевірити адреси одержувачів електронної пошти за допомогою поштового сервера або сервера LDAP.

Зазвичай можна використовувати поштовий сервер для перевірки адреси.

Це працює з більшістю поштових серверів, які надають відповідь *User unknown* на недійсні адреси.

Повідомлення про застереження та налаштований зовнішній вигляд. Ми можемо налаштувати як повідомлення про відмову від відповідальності, так і повідомлення про заміну, а також зовнішній вигляд інтерфейсу модуля FortiMail. Повідомлення із застереженням додається до всіх електронних листів, зазвичай попереджаючи одержувача, що вміст може бути конфіденційно.

Повідомлення-замінники – це повідомлення, які одержувачі отримують замість своєї електронної пошти. Вони можуть містити попередження про надіслані повідомлення та вхідні повідомлення, які є спамом або заражені вірусом.

Ми можемо налаштувати зовнішній вигляд веб-сторінок модуля FortiMail, видимих для адміністраторів пошти, щоб вони краще відповідали зовнішньому вигляду та стилю компанії.

Розширені функції доставки. Обробка електронної пошти потребує часу. Затримки обробки можуть призвести до тайм-ауту клієнтів і серверів. Щоб зменшити цю проблему, ми можемо:

відкласти доставку для обробки електронної пошти великого розміру в той час, коли очікується невеликий трафік;

відправити сповіщення про статус доставки (DSN).

Методи боротьби зі спамом. Виявлення спаму є ключовою функцією пристрою FortiMail. Ця функція базується на двох рівнях захисту від спаму [12]:

методи захисту від спаму FortiMail;

антиспам-сервіс FortiGuard.

Кожен рівень відіграє важливу роль у відокремленні спаму від легітимної електронної пошти. FortiGuard Antispam надає високоналаштований керований сервіс для класифікації спаму, тоді як модуль FortiMail пропонує передові технології виявлення та контролю спаму.

Окрім сканування вхідних електронних листів, пристрої FortiMail також можуть перевіряти вміст вихідних повідомлень. Це може допомогти усунути

можливість розсилання спаму співробітником або скомпрометованим комп’ютером, що призведе до внесення поштових серверів вашої організації до списку блокування.

Служба захисту від спаму FortiGuard – це керована служба Fortinet, яка забезпечує триетапний підхід до перевірки електронних листів.

Перший елемент – це список блокування DNS (DNSBL), який є «живим» списком відомих джерел спаму.

Другий елемент – це поглиблена перевірка електронної пошти на основі URL-адреси (Uniform Resource Identifier, URL), що міститься в тілі повідомлення, – широко відомої як списки блокування спаму в режимі реального часу (SURBL).

Третій елемент – це список блокування спаму контрольної суми FortiGuard Antispam (Функція SHASH. Використовуючи SHASH, пристрій FortiMail надсилає хеш електронного листа на сервер FortiGuard Antispam, який порівнює хеш із хешами відомих спам-повідомлень, що зберігаються в базі даних FortiGuard Antispam. Якщо результати хешування збігаються, електронний лист позначається як спам.

Результати запитів FortiGuard можна кешувати в памяті для економії пропускної здатності мережі.

3 РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ НА БАЗІ FORTIMAIL

3.1. Варіанти системи захисту корпоративної електронної пошти на базі FortiMail

Початкове налаштування FortiMail включає такі кроки [12]:

підключення до графічного інтерфейсу або командного рядка;

вибір режиму роботи;

запуск майстра швидкого запуску;

підключення до сервісів FortiGuard;

розгортання режиму шлюзу;

розгортання прозорого режиму;

розгортання в режимі сервера;

тестування установки;

резервне копіювання конфігурації.

Після встановлення та ввімкнення пристрою FortiMail, а також завершення початкового налаштування, ми можемо налаштувати режим роботи пристрою FortiMail за допомогою інтерфейсу командного рядка (CLI) або графічного інтерфейсу користувача (GUI).

Пристрої FortiMail можуть працювати в одному з трьох режимів роботи: режим шлюзу, прозорий режим або режим сервера. Зазвичай ми обираємо режим роботи, який відповідає корпоративній топології та вимогам, і налаштовуємо його лише один раз, одразу після фізичної установки та початкового налаштування, а також перед використанням майстра швидкого запуску.

Загалом кажучи, режим шлюзу підходить для більшості середовищ розгортання. Зазвичай його легше реалізувати та краще зрозуміти. Винятками є ситуації, коли ні записи MX DNS, ні IP-адреси не можна змінити.

Прозорий режим було розроблено з метою впровадження FortiMail в

середовищах операторів зв’язку для боротьби зі спамом. Він підходить для певних середовищ, але потребує ретельнішого керування маршрутизацією та гарного розуміння прозорості мережевого та прикладного рівнів.

Прозорий режим – найкращий вибір для боротьби з вихідним спамом у середовищах операторів зв'язку.

Режим сервера використовується для налаштування окремого поштового сервера або для заміни існуючого поштового сервера.

Після встановлення режиму роботи запустіть майстер швидкого запуску, щоб налаштувати базову систему. Потім розгортаємо свій пристрій FortiMail. Деталі залежать від обраного режиму роботи.

Під час роботи в режимі шлюзу пристрій FortiMail діє як агент передачі пошти (MTA), іноді відомий як шлюз або ретранслятор електронної пошти. Пристрій FortiMail отримує електронні листи, сканує їх на віруси та спам, а потім пересилає їх на поштовий сервер призначення для доставки. Зовнішні MTA підключаються до пристрою FortiMail, а не безпосередньо до захищеного поштового сервера.

Пристрої FortiMail, що працюють у режимі шлюзу, надають веб-інтерфейс користувача, через який користувачі електронної пошти можуть отримати доступ до особистих налаштувань та електронної пошти, поміщеної в карантин для кожного одержувача. Однак пристрої FortiMail, що працюють у режимі шлюзу, не розміщують локально поштові скриньки, такі як папка «Вхідні» кожного користувача електронної пошти. Поштові скриньки зберігаються на захищених серверах електронної пошти.

Режим шлюзу вимагає деяких змін у існуючій мережі. Вимоги включають записи MX на публічних DNS-серверах для кожного захищеного домену, які повинні посилатися на пристрій FortiMail, а не на захищені поштові сервери. Нам також може знадобитися налаштувати брандмауери або маршрутизатори для спрямування SMTP-трафіку на пристрій FortiMail, а не на корпоративні поштові сервери.

Приклад топології режиму шлюзу наведено на рисунку 3.1.

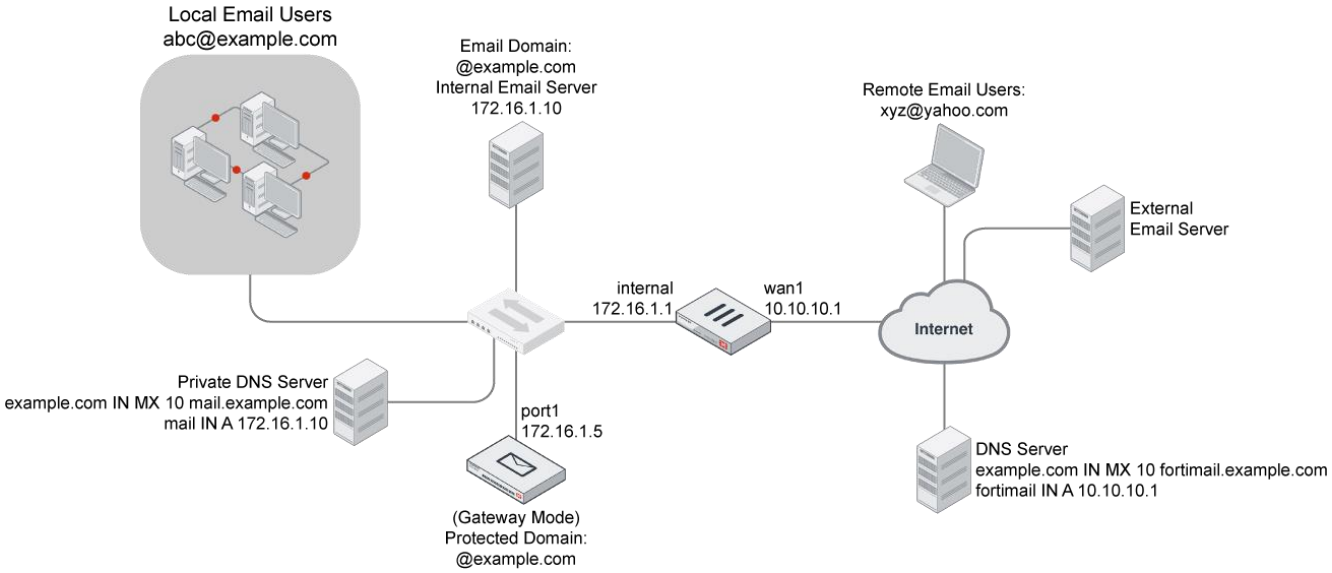

Рис. 3.1. Приклад топології режиму шлюзу пристрою FortiMail

Наприклад, інтернет-провайдер (ISP) може розгорнути пристрій FortiMail для захисту поштових серверів своїх клієнтів. З міркувань безпеки клієнти не хочуть, щоб їхні поштові сервери були безпосередньо видимі для зовнішніх MTA. Тому інтернет-провайдер встановлює пристрій FortiMail у режимі шлюзу та налаштовує свою мережу таким чином, щоб весь електронний трафік проходив через пристрій FortiMail, перш ніж досягти поштових серверів клієнтів.

У прозорому режимі FortiMail діє або як неявний ретранслятор, або як проксі-сервер. Пристрій FortiMail перехоплює електронні листи, сканує їх на віруси та спам, а потім передає їх на поштовий сервер призначення для доставки. Зовнішні MTA підключаються через пристрій FortiMail до захищеного поштового сервера.

Прозорий режим як на мережевому, так і на прикладному рівнях налаштовується, але не є обов'язковою. Під час приховування модуль FortiMail зберігає IP-адресу та доменне ім'я SMTP-клієнта в IP-заголовках, конверті SMTP та заголовках повідомлень, а не замінює їх своїми власними.

Пристрої FortiMail, що працюють у прозорому режимі, надають веб-інтерфейс користувача, через який користувачі електронної пошти можуть отримати доступ до особистих налаштувань та електронної пошти, поміщеної в карантин для кожного одержувача. Однак пристрої FortiMail, що працюють у

прозорому режимі, не розміщують локально поштові скриньки, такі як папка «Вхідні» кожного користувача електронної пошти. Ці поштові скриньки зберігаються на захищених серверах електронної пошти.

За замовчуванням пристрої FortiMail, що працюють у прозорому режимі, налаштовані як міст, з усіма мережевими інтерфейсами в одній підмережі. Ми можемо налаштувати мережеві інтерфейси поза мостом, якщо нам це потрібно, наприклад, якщо у нас є деякі захищені поштові сервери, які не розташовані в одній підмережі. Якщо ми встановлюємо інтерфейс у режим маршрутизації, ми повинні призначити інтерфейсу локальну IP-адресу, яка належить до іншої підмережі, ніж IP-адреса керування.

Прозорий режим зазвичай не вимагає змін до існуючої мережі. Вимоги включають фізичне розташування пристрою FortiMail між захищеним поштовим сервером та всіма SMTP-клієнтами, на відміну від режиму шлюзу. Оскільки пристрої FortiMail, що працюють у прозорому режимі, невидимі, клієнтів не можна налаштувати для маршрутизації електронної пошти безпосередньо до пристрою FortiMail, тому він має бути фізично розміщений там, де може перехоплювати з’єднання.

Приклад топології прозорого режиму наведено на рисунку 3.2.

Наприклад, школа може захотіти встановити пристрій FortiMail для захисту свого поштового сервера, але не хоче вносити жодних змін до існуючих конфігурацій DNS- та SMTP-клієнтів чи іншої топології мережі. Тому школа встановлює пристрій FortiMail у прозорому режимі.

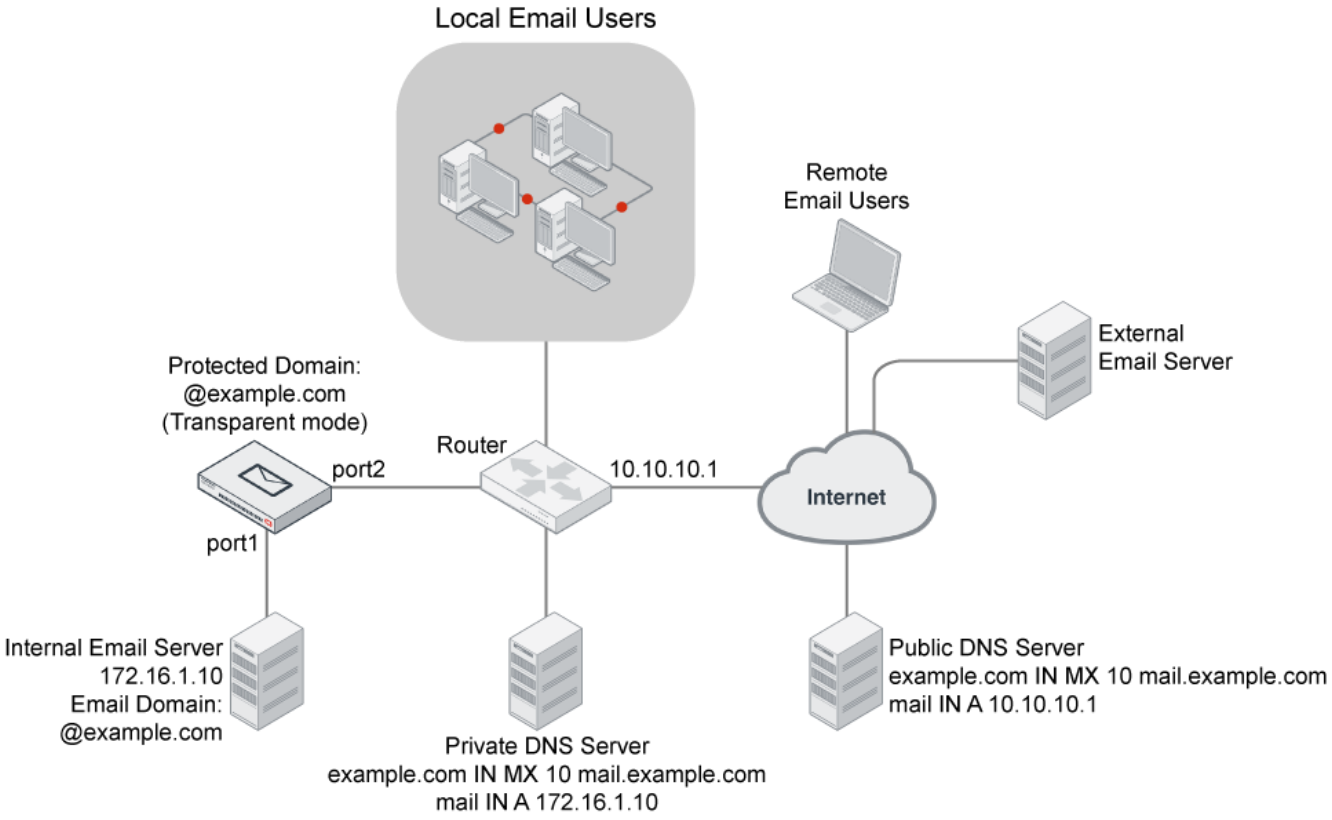

Рис. 3.2. Приклад топології прозорого режиму пристрою FortiMail

У режимі сервера пристрій FortiMail є автономним поштовим сервером. Пристрій FortiMail отримує електронні листи, сканує їх на віруси та спам, а потім доставляє електронні листи до поштових скриньок своїх користувачів. Зовнішні MTA підключаються до пристрою FortiMail, який також є захищеним поштовим сервером.

Пристрої FortiMail, що працюють у режимі сервера, забезпечують веб-інтерфейс користувача, через який користувачі електронної пошти можуть отримати доступ до:

особистих вподобань;

електронних листів, які переміщено до карантину для кожного одержувача;

їхніх локально розміщених поштових скриньок, такі як поштова скринька кожного користувача електронної пошти.

Крім того, користувачі електронної пошти можуть отримувати електронні листи за допомогою POP3 або IMAP.

Режим сервера вимагає деяких змін у існуючій мережі. Вимоги включають

записи MX на публічних DNS-серверах для кожного захищеного домену. Записи повинні стосуватися пристрою FortiMail. Нам також може знадобитися налаштувати брандмауери або маршрутизатори для спрямування SMTP-трафіку до пристрою FortiMail.

Приклад топології режиму сервера наведено на рисунку 3.3.

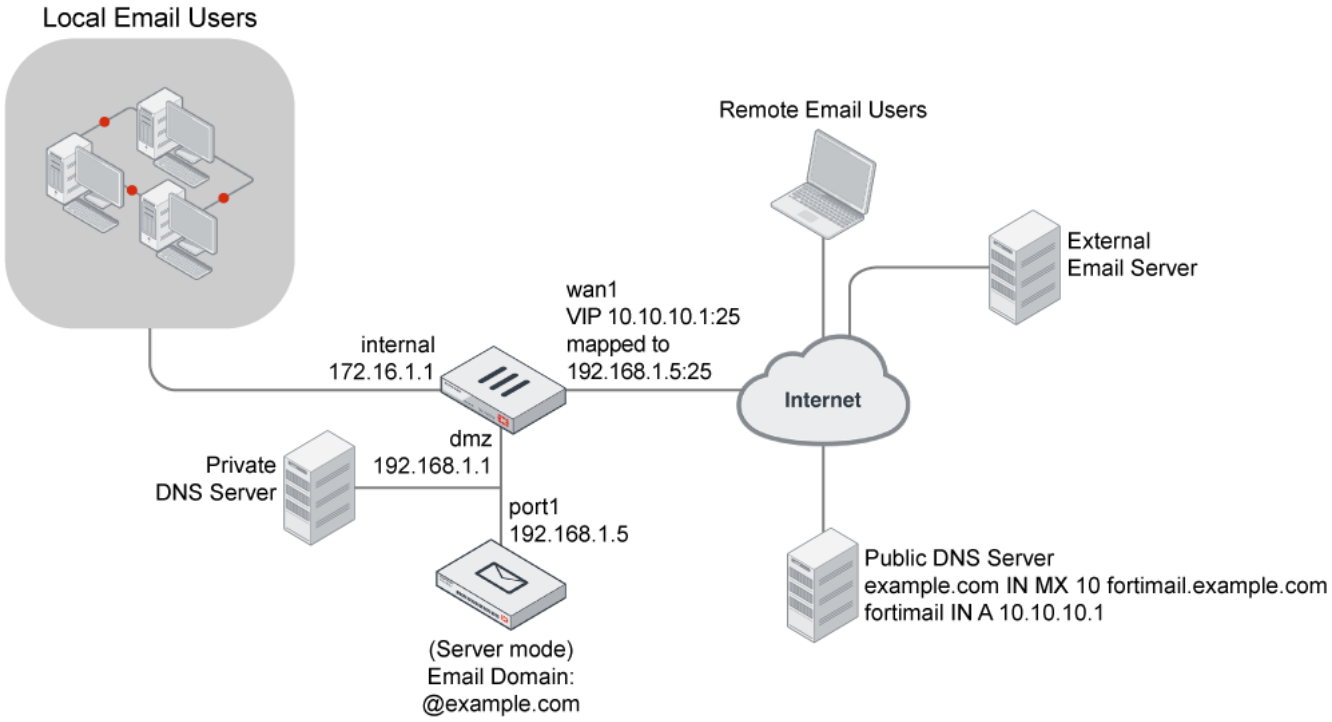

Рис. 3.3. Приклад топології режиму сервера пристрою FortiMail

Наприклад, компанія може створювати мережу і не мати існуючого поштового сервера. Компанія хоче зручно керувати як своїм поштовим сервером, так і системою безпеки електронної пошти на одному мережевому пристрої. Тому компанія розгортає пристрій FortiMail у режимі сервера.

3.2. Порядок застосування рішення FortiMail

Панель керування > Стан відображається першим після входу в графічний інтерфейс користувача. Вона містить приладову панель з віджетами, кожен з яких показує рівень продуктивності або іншу статистику.

За замовчуванням віджети відображають серійний номер та поточний

системний стан пристрою FortiMail, зокрема час безвідмовної роботи, використання системних ресурсів, сповіщення, ім’я хоста, версія прошивки, системний час та електронна пошта пропускна здатність.

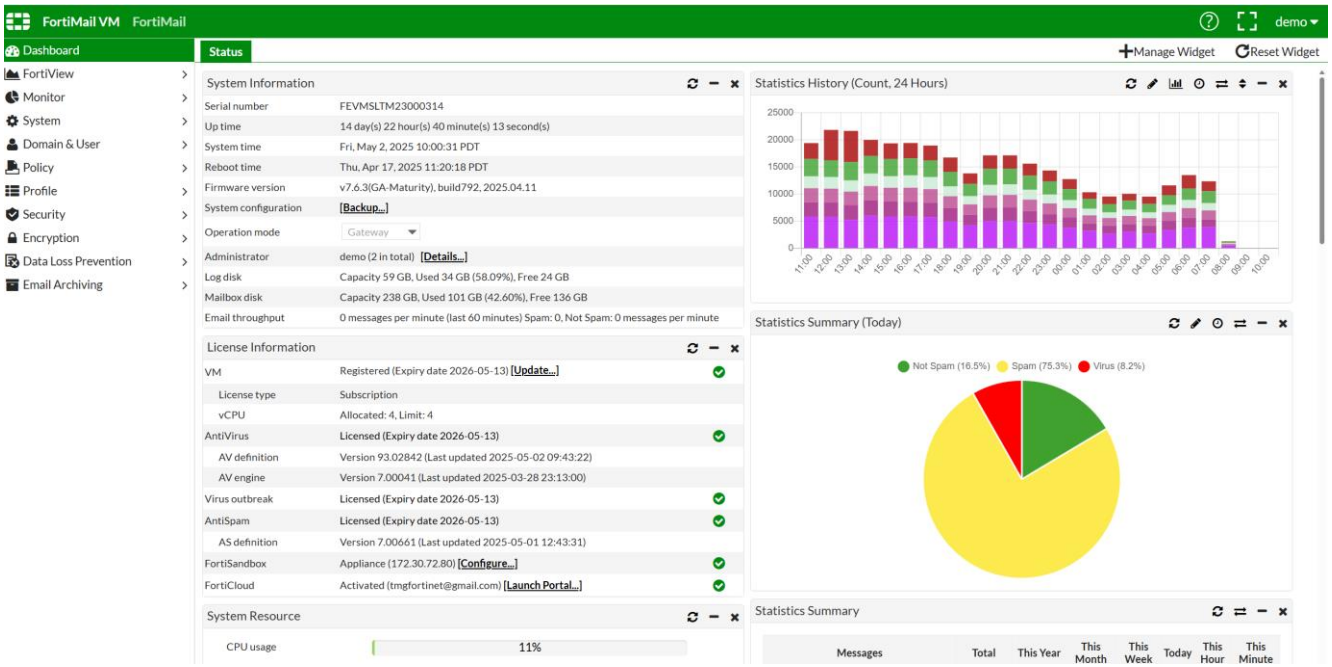

Рис. 3.4. Панель приладів пристрою FortiMail

Пристрій FortiMail може показувати дані про кількість електронних листів за кожен період часу, в яких пристрій FortiMail виявив віруси, спам або жодне з них. Він також може відстежувати розміри файлів електронної пошти, швидкість сканування та швидкість передачі (рисунок 3.5).

Для електронних листів, класифікованих як спам, статистика пошти включає інформацію про те, яка функція FortiMail класифікувала електронний лист як спам, наприклад, правила контролю доступу, список блокування для всієї системи або списки блокування для кожного користувача.

Електронні листи, які не класифікуються як спам жодним антиспам-скануванням, у статистиці пошти позначаються як Не спам .

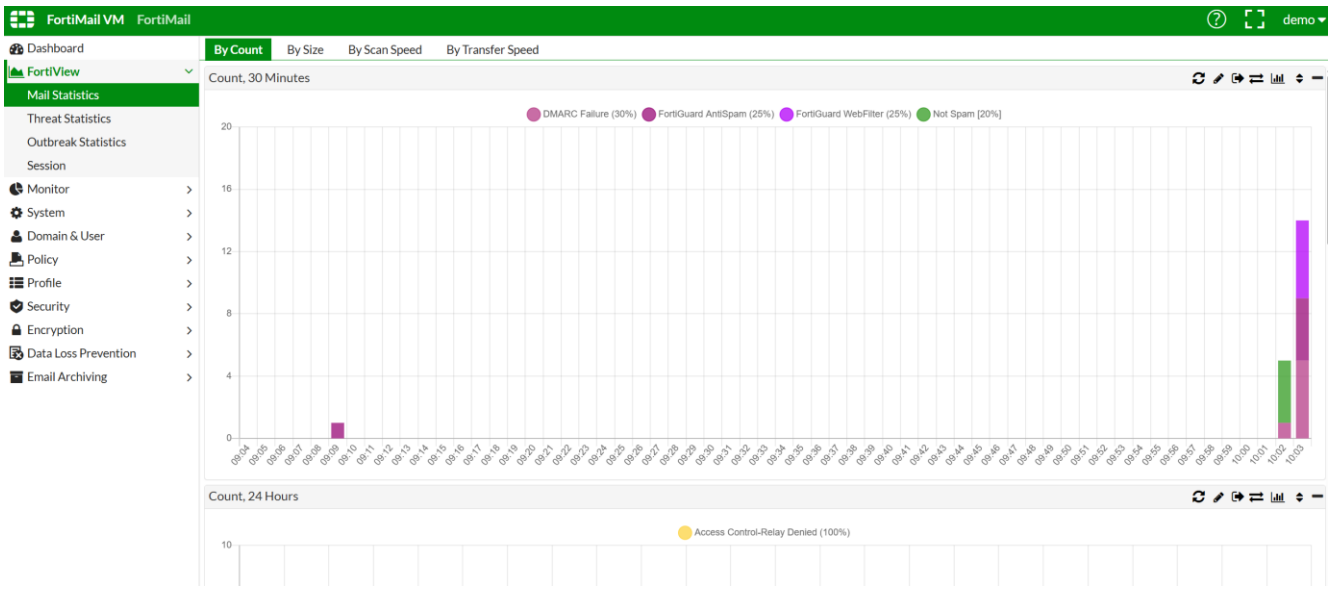

Рис. 3.5. Панель Mail Statistics

Панель Threat Statistics показує зведення щодо спаму та вірусних пошт, а також детальний розгляд загроз.

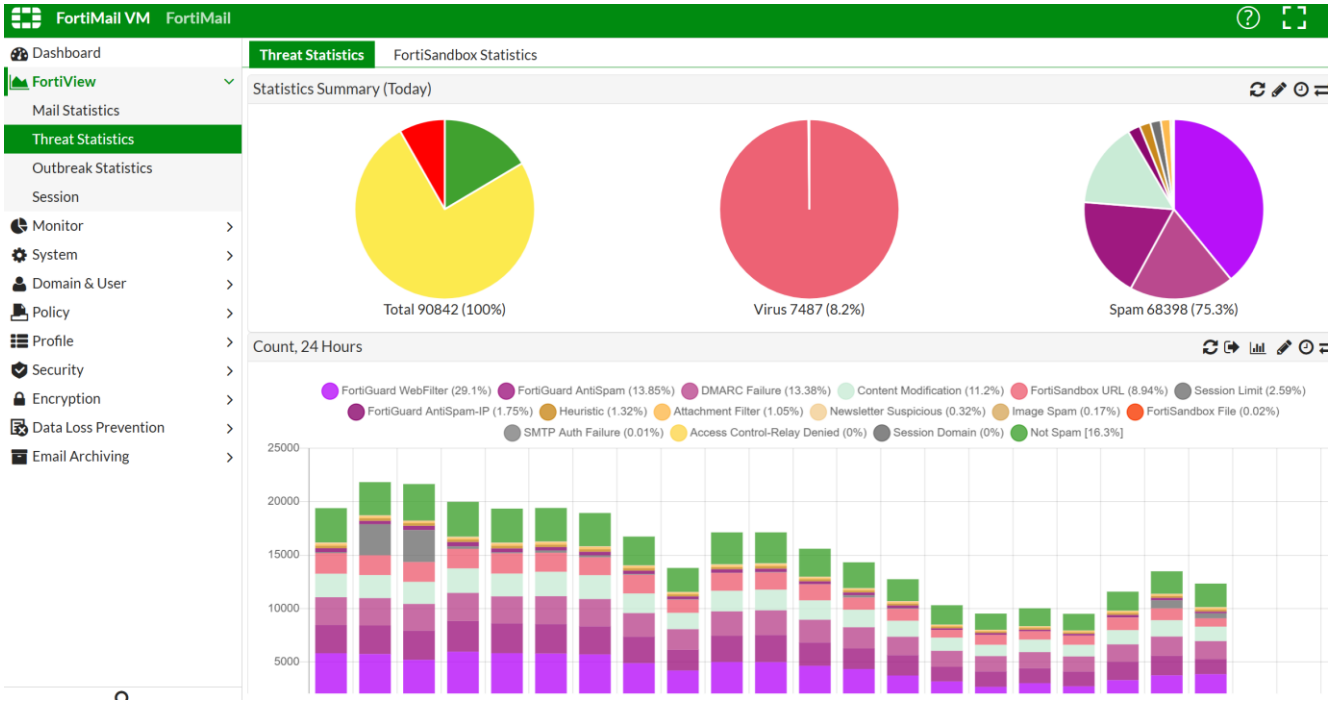

Рис. 3.6. Панель Threat Statistics

Меню Policy дозволяє створювати політики, які використовують профілі для фільтрації електронної пошти. Це також дозволяє контролювати, хто може надсилати електронні листи через пристрій FortiMail, і визначати правила

доставки електронних листів, які він проксі-серверує або ретранслює.

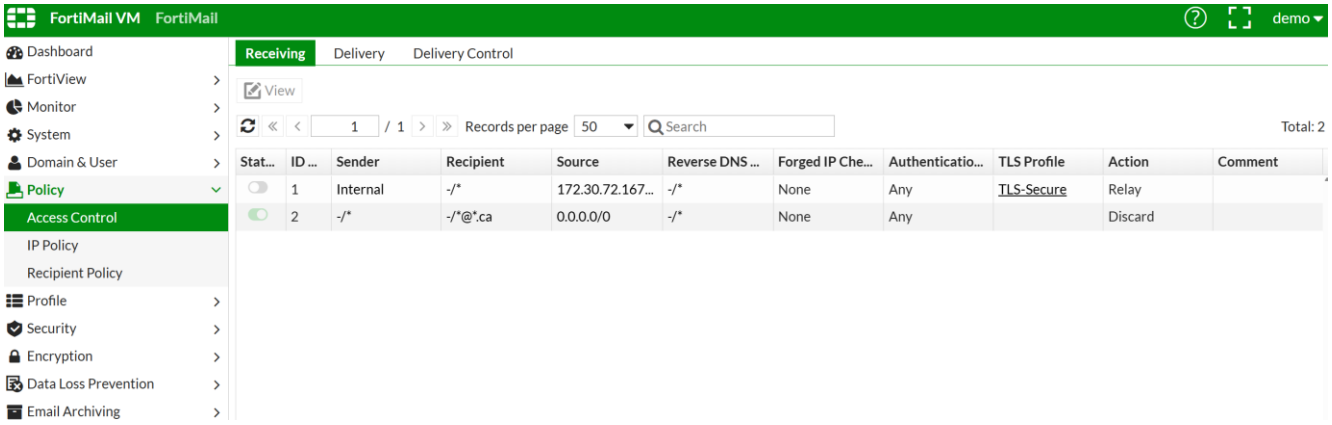

Рис. 3.7. Меню Policy

Політика визначає, яким чином буде фільтруватися трафік. Він також може визначати налаштування облікового запису користувача, такі як тип автентифікації, дискова квота та доступ до веб-пошти.

Після створення профілів захисту від спаму, антивіруса, контенту, автентифікації, TLS або ресурсів, потрібно застосувати їх до політик, щоб вони набули чинності.

Пристрої FortiMail підтримують три типи політик [12]:

правила контролю доступу та доставки, типові для SMTP-ретрансляторів та серверів;

політики на основі одержувачів;

політики на основі IP-адрес.

FortiMail має кілька типів політик:

Правила отримання та доставки контролю доступу контролюють, які SMTP-клієнти можуть надсилати електронні листи через FortiMail, а також як доставляти електронні листи, які він проксі-серверує або ретранслює.

Політики на основі IP-адрес контролюють сеанси SMTP на основі IP-адреси клієнта SMTP та, якщо пристрій FortiMail працює в прозорому режимі, SMTP-сервер. Вони можуть застосовувати різні функції, такі як захист від спаму.

Політики на основі одержувачів контролюють окремі повідомлення

електронної пошти на основі адреси електронної пошти одержувача та, для вихідної електронної пошти, адреси електронної пошти відправника. Вони можуть застосовувати різні функції, такі як захист від спаму.

Залежно від кожного електронного листа та конфігурації може застосовуватися кілька політик. Наслідки залежать від порядку виконання політик та того, які політики відповідають один одному.

Меню Profile (рисунок 3.8) дозволяє налаштувати багато типів профілів. Це набір налаштувань для захисту від спаму, антивіруса, автентифікації або інших функцій.

Після створення та налаштування профілю його можна застосувати безпосередньо в політиці або опосередковано, включивши до іншого профілю, вибраного в політиці. Політики застосовують кожен вибраний профіль до всіх повідомлень електронної пошти та SMTP-підключень, якими керує політика.

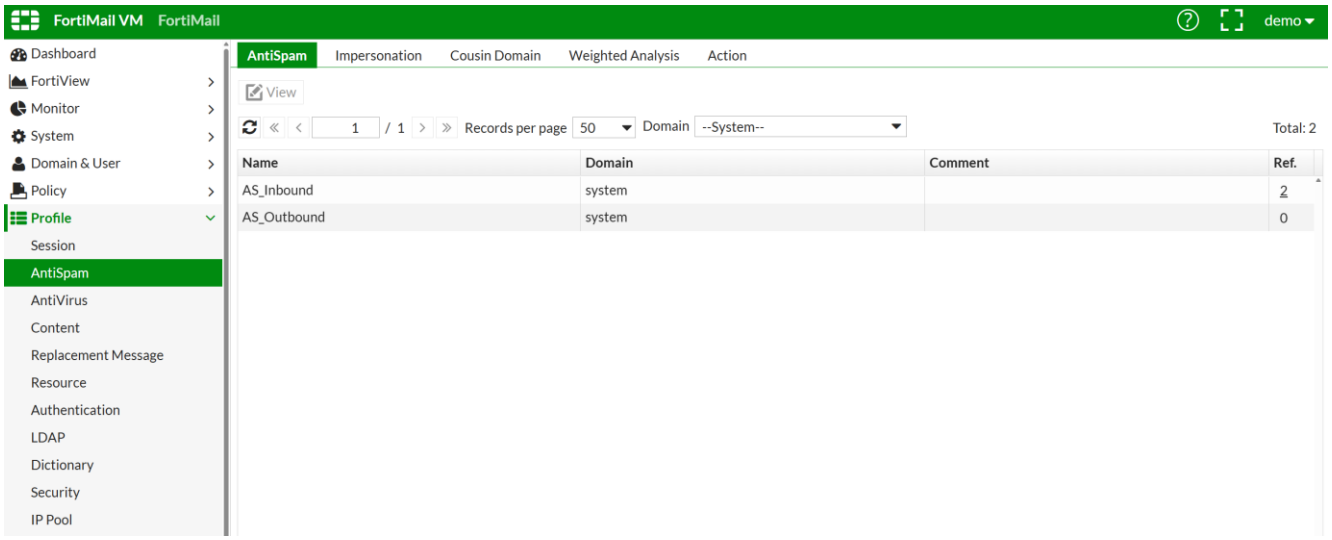

Рис. 3.8. Меню Profile

Створення кількох профілів для кожного типу політики дозволяє налаштувати службу електронної пошти, застосовуючи різні профілі до політик, що керують різними SMTP-з'єднаннями або користувачами електронної пошти. Наприклад, якщо ми є постачальником інтернет-послуг (ISP), ми можемо створювати та застосовувати антивірусні профілі лише до політик, що регулюють

користувачів електронної пошти, які платять вам за надання антивірусного захисту.

Розглянемо загальний список методів та стратегій, які рекомендуються для покращення безпеки пристрою FortiMail.

Необхідно встановити пристрій FortiMail у безпечному місці, наприклад, у замкненій кімнаті з обмеженим доступом. Заборона доступу до пристрою підвищить його безпеку, оскільки неавторизовані користувачі можуть порушити роботу всієї корпоративної мережі через ненавмисне та навмисне втручання.

Необхідно регулярно здійснювати оновлення прошивки до останньої версії.

Необхідно не дозволяти адміністративний доступ до зовнішнього інтерфейсу та використовуйте внутрішні методи доступу, такі як IPsec VPN або SSL VPN. Якщо вам потрібен віддалений доступ і ви не можете використовувати IPsec або SSL VPN, дозвольте лише HTTPS та SSH і використовуйте безпечні методи доступу, такі як довірені хости та двофакторна автентифікація.

Обов’язково необхідно налаштувати довірені хости для адміністраторів, щоб обмежити кількість комп’ютерів, з яких адміністратор може входити до пристрою. Визначення довіреного будинку призведе до того, що пристрій прийматиме вхід адміністратора лише з налаштованої IP-адреси або підмережі.

Необхідно змінити адміністративний порт за замовчуванням на нестандартний порт.

Необхідно зареєструватися у службах підтримки, щоб активувати гарантію на пристрій.

Щоб уникнути можливості того, що адміністратор відійде від комп’ютера керування та залишить його без доступу, можна додати автоматичний тайм-аут простою. Якщо графічний інтерфейс не використовується протягом певного часу, пристрій автоматично виведе адміністратора з системи.

Необхідно увімкнути автоматичну синхронізацію годинника для спрощення аудиту та узгодження дат закінчення терміну дії, що використовуються для визначення терміну дії сертифікатів та протоколів безпеки.

Програмне забезпечення для перебору паролів методом грубої сили може

запускати не лише словникові атаки. Воно може виявляти поширені паролі, де літера замінена цифрою. Наприклад, якщо як пароль використовується «p4ssw0rd», його можна зламати. Тому, необхідно створити політику безпечніших паролів, якої адміністратори повинні дотримуватися для забезпечення безпечнішого з'єднання.

Встановіть тривалість блокування, якщо адміністратор введе неправильний пароль певну кількість разів, за допомогою команди CLI *set admin-lockout-durationma set admin-lockout-threshold* в розділі *config system global*.

3.3. Рекомендації щодо захисту корпоративної електронної пошти

Впровадження надійних заходів безпеки корпоративної електронної пошти є важливим для захисту бізнесу від кібератак. Дотримуючись найкращих практик безпеки корпоративної електронної пошти, включаючи регулярне навчання та впровадження функцій безпеки, співробітники можуть допомогти запобігти витокам даних та іншим загрозам. Основними рекомендаціями щодо захисту корпоративної електронної пошти, яких повинні дотримуватися як фахівці з безпеки, так і співробітники організацій:

Необхідно впроваджувати та використовувати двофакторну автентифікацію користувачів. Двофакторна автентифікація (багатофакторна автентифікація), додає додатковий рівень безпеки, вимагаючи, окрім пароля, другу форму підтвердження, наприклад, текстовий код або сповіщення додатка. Це важливо, оскільки навіть якщо зловмисник викраде пароль, він не зможе отримати доступ до корпоративної електронної пошти без другого фактора.

Наприклад, без двофакторної автентифікації викрадений пароль може дозволити хакерам отримати доступ до конфіденційних електронних листів компанії, викрасти дані або розпочати подальші атаки. Завдяки двофакторній автентифікації цей додатковий крок забезпечує безпеку облікових записів, значно знижуючи ризик несанкціонованого доступу.

Необхідно створювати та використовувати надійні паролі для входу до

корпоративної пошти.

Створення надійних паролів є фундаментальною частиною захисту корпоративної електронної пошти. Слабкі або повторно використані паролі хакерам легко вгадати або зламати, що дає їм доступ до конфіденційних даних. Надійний пароль має бути довгим, складним і містити комбінацію літер, цифр і символів.

Щоб захистити паролі, співробітникам слід уникати використання легко вгадуваної інформації, такої як імена чи дати. Також важливо використовувати менеджер паролів для безпечного зберігання та створення складних паролів. Це гарантує, що кожен обліковий запис матиме унікальний пароль, зменшуючи ризик компрометації в кількох системах.

Необхідно впроваджувати та використовувати шифрування змісту електронних листів. Шифрування електронної пошти гарантує, що повідомлення не зчитуються ніким, окрім передбачуваного одержувача, захищаючи конфіденційну інформацію від несанкціонованого доступу під час передачі. Це особливо важливо для захисту конфіденційного ділового спілкування та запобігання витокам даних.

Щоб налаштувати шифрування електронної пошти, необхідно виконати такі дії:

увімкнути шифрування у поштовому клієнті. Більшість платформ, таких як Outlook або Gmail, пропонують вбудовані опції шифрування;

можна використовувати сторонні інструменти шифрування. Для розширеного шифрування такі сервіси, як ProtonMail або Mailvelope, забезпечують додатковий захист;

треба переконатися, що одержувачі підтримують шифрування. Для ефективної роботи шифрування має бути ввімкнено в обох сторонах.

Шифрування електронних листів є важливим кроком у забезпеченні безпеки корпоративного спілкування.

Необхідно впроваджувати та використовувати безпечний Wi-Fi. Використання незахищеного публічного Wi-Fi для бізнес-комунікацій наражає

організації на значні ризики. Хакери можуть перехоплювати дані, що надсилаються через публічні мережі, отримуючи доступ до конфіденційних електронних листів та облікових даних для входу.

Щоб захистити свою організацію, необхідно уникати публічних Wi-Fi під час доступу до корпоративної електронної пошти. Щоб підвищити безпеку корпоративної електронної пошти необхідно:

використовувати віртуальну приватну мережу (VPN) для захисту з'єднань, якщо необхідна віддалена робота;

переконайтеся, що Wi-Fi організації захищений надійним шифруванням (WPA3) та безпечним паролем;

регулярно оновлювати прошивку маршрутизатора та змінювати налаштування за замовчуванням, щоб запобігти несанкціонованому доступу.

Необхідно вкладати ресурси в програмне забезпечення для захисту корпоративної електронної пошти. Інвестування в програмне забезпечення безпеки є критично важливим для захисту систем організації від потенційних порушень. Однак ринок програмного забезпечення безпеки може бути величезним, з незліченними варіантами, що обіцяють різні рівні захисту. Ця складність може призвести до плутанини для покупців, які намагаються визначити, яке рішення найкраще відповідає їхнім потребам.

Зрештою, мета полягає у виборі програмного забезпечення, яке доповнює існуючого постачальника послуг електронної пошти, покращуючи його функції безпеки, не ускладнюючи робочий процес. Необхідно обирати рішення, які легко інтегруються, забезпечуючи додаткові рівні захисту від загроз електронної пошти, зберігаючи при цьому простоту використання. Правильно підібране програмне забезпечення для захисту пошти може значно посилити захист організацій від кіберризиків.

Необхідно постійно навчати співробітників безпечному використанню корпоративної електронної пошти. Найслабшою ланкою в кібербезпеці часто є людська помилка, тому вкрай важливо навчати співробітників безпечним методам роботи з електронною поштою. Регулярні тренінги з підвищення обізнаності

можуть допомогти розпізнавати потенційні загрози безпеці, такі як фішингові електронні листи або підозрілі вкладення, та реагувати на них належним чином.

Під час навчальних занять зосередьтеся на навчанні співробітників розпізнавати тривожні сигнали в електронних листах, перевіряти автентичність відправника та безпечно обробляти конфіденційну інформацію. Заохочуйте відкриті обговорення питань безпеки та створюйте культуру пильності. Інвестуючи в навчання співробітників, можна покращити загальний рівень безпеки організації та зменшити ймовірність помилок, які можуть поставити під загрозу безпеку електронної пошти.

Необхідно використовувати протоколи безпеки електронної пошти. Протоколи безпеки електронної пошти, такі як Domain Keys Identified Mail (DKIM) та Sender Policy Framework (SPF), відіграють вирішальну роль у захисті корпоративних листів від спуфінгу та фішингових атак. DKIM додає цифровий підпис до вихідних листів, що дозволяє серверу одержувача перевірити особу відправника та переконатися, що повідомлення не було підроблено.

Аналогічно, SPF визначає, які поштові сервери мають право надсилати електронні листи від імені корпоративного домену, допомагаючи запобігти несанкціонованому використанню. Впроваджуючи ці протоколи, можна підвищити безпеку електронної пошти, зміцнити довіру до своїх комунікацій та значно знизити ризик шкідливої діяльності, спрямованої на організацію.

Хоча такі протоколи, як DKIM та SPF, значно підвищують безпеку електронної пошти, зловмисники все ще можуть знайти способи уникнути виявлення. Наприклад, вони можуть підробити адресу відправника, щоб вона виглядала справжньою, або скомпрометувати авторизовані сервери для надсилання шкідливих електронних листів. Крім того, складні методи фішингу можуть обманом змусити одержувачів надати конфіденційну інформацію, обходячи технічні засоби захисту.

Розвинені організації усвідомлюють, що покладатися виключно на ці протоколи недостатньо. Вони шукають постачальників послуг безпеки, які пропонують комплексні рішення, включаючи виявлення загроз у режимі

реального часу, можливості машинного навчання та аналіз поведінки. Такий багаторівневий підхід гарантує, що потенційні загрози будуть виявлені та пом'якшені, перш ніж вони зможуть вплинути на організацію, створюючи надійніший захист від кіберризиків, що постійно змінюються.

Необхідно відмітити, що кібербезпека – це галузь, що швидко розвивається, де щодня з’являються нові загрози. Тому важливо постійно оновлювати свої заходи безпеки, щоб залишатися на крок попереду кіберзлочинців. Регулярне оновлення програмного забезпечення, включаючи протоколи та програми безпеки електронної пошти, допомагає виправляти вразливості та захищатися від найновіших векторів атак.

Крім того, організації повинні проводити періодичні аудити безпеки та навчальні сесії для оцінки та покращення свого захисту. Інформація про останні тенденції та передові практики в галузі кібербезпеки гарантує, що організація зможе ефективно адаптуватися до постійно мінливого середовища, зрештою захищаючи конфіденційну інформацію та підтримуючи довіру з клієнтами та партнерами.

ВИСНОВКИ

В роботі досліджено проблему захисту корпоративної електронної пошти. Компрометація корпоративної електронної пошти продовжує залишатися однією з найбільш фінансово збиткових кіберзагроз у 2025 році. Атаки на компрометацію корпоративної електронної пошти становили 73% усіх зареєстрованих кіберінцидентів у 2024 році. Необхідність захисту корпоративної електронної пошти в сучасних умовах є критично важливою з кількох основних причин. Більшість кібератак на організації починаються саме через електронну пошту. Це найпоширеніший канал для доставки шкідливого програмного забезпечення (вірусів, програм-вимагачів), фішингових листів та спроб соціальної інженерії. Атаки можуть призвести до зупинки роботи поштових серверів, втрати важливої кореспонденції, зриву комунікацій як всередині компанії, так і з зовнішнім світом, що паралізує операційну діяльність.

Визначено існуючі підходи до захисту корпоративної електронної пошти. Сьогодні широко застосовуються інструменти, призначені для виявлення та блокування шкідливих електронних листів такі, як:

шлюзи безпечної електронної пошти (SEG) – вони діють як фільтр, аналізуючи вхідні повідомлення на наявність ознак шахрайства або підробки;

багатофакторна автентифікація (MFA) – навіть якщо шахраї отримують доступ до облікових даних, MFA додає додатковий рівень безпеки;

автентифікація, звітування та відповідність повідомлень на основі домену (DMARC) – цей протокол допомагає запобігти підміні електронного домену зловмисниками.

Проаналізовано існуючі рішення для захисту корпоративної електронної пошти. Платформи безпеки електронної пошти є рішеннями, які захищають інфраструктуру електронної пошти. Їх основна мета – видалення шкідливих (фішинг, соціальна інженерія, віруси) або небажаних повідомлень (спам, маркетинг). Інші функції включають захист даних електронної пошти,

автентифікацію повідомлень на основі домену, звітність та відповідність (DMARC), розслідування та виправлення через спеціальну консоль. Вони можуть інтегруватися як безпечний шлюз електронної пошти (SEG) для захисту перед доставкою або як інтегроване хмарне рішення для безпеки електронної пошти (ICES) для захисту після доставки.

В роботі розглянуто методи та засоби захисту корпоративної електронної пошти на прикладі рішення FortiMail. Рішення FortiMail забезпечує захист від загроз, що передаються електронною поштою. Ефективний засіб захисту від спаму і шкідливого ПЗ включає технології захисту від масових розсилок і вірусних кампаній, реконструкції листів і вкладень з видаленням (знешкодженням) небезпечного вмісту, аналізу поведінки в «пісочниці», захисту від підміни тощо.

В роботі розглянуто варіанти подубови системи захисту корпоративної електронної пошти на базі FortiMail. Пристрої FortiMail можуть працювати в одному з трьох режимів роботи: режим шлюзу, прозорий режим або режим сервера. Зазвичай обирається режим роботи, який відповідає корпоративній топології та вимогам. В роботі розглянуто порядок застосування рішення FortiMail.

Розроблено рекомендації фахівцям з кібербезпеки щодо захисту корпоративної електронної пошти. Впровадження надійних заходів безпеки корпоративної електронної пошти є важливим для захисту бізнесу від кібератак. Дотримуючись найкращих практик безпеки корпоративної електронної пошти, включаючи регулярне навчання та впровадження функцій безпеки, співробітники можуть допомогти запобігти витокам даних та іншим загрозам.

Таким чином, правильне застосування методів та засобів захисту корпоративної електронної пошти має забезпечити ефективний захист інформаційних ресурсів організації під час обробки та обміну повідомленнями та документами.

ПЕРЕЛІК ПОСИЛАНЬ

1. John Farina. BEC Global Insights Report: February 2025. Fortra, Posted on March 7, 2025. URL: https://www.fortra.com/blog/bec-global-insights-report-february-2025

2. Maxime Cartier. Business Email Compromise Statistics 2025. Hoxhunt, March 3, 2025. URL: https://hoxhunt.com/blog/business-email-compromise-statistics

3. What is business email compromise (BEC)? Microsoft. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec

4. What Is Business Email Compromise (BEC)? Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-business-email-compromise-bec-tactics-and-prevention

5. DMARC для безпеки електронної пошти. Softprom, 15.04.2022. URL: https://softprom.com/ua/dmarc-dlya-bezpeki-elektronnoyi-poshti

6. Domain-based Message Authentication, Reporting & Conformance (DMARC). CSA, Last updated 7 February 2025. URL: https://www.csa.gov.sg/resources/internet-hygiene-portal/information-resources/dmarc

7. Max Taggett, Nikul Patel, Franz Hinner, Deepak Mishra. Magic Quadrant for Email Security Platforms. Gartner, 16 December 2024 - ID G00806896. URL: https://www.gartner.com/doc/reprints?id=1-2J20K7ZF&ct=241010&st=sb

8. Abnormal Cloud Email Security. URL: https://abnormal.ai/resources/cloud-email-security

9. Trend Vision One – Email and Collaboration Security. DataSheet. URL: https://device.report/m/a16aec617d4f0880a3fad1f44304fcc0513a674805ad4f07c05a4d7af56bf9f9.pdf

10. Stay ahead of attackers with adaptive email threat intelligence. URL: https://www.proofpoint.com/uk/products/cloud-security/web-security

11. FortiMail For Email Security. Data Sheet. Fortinet. URL:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiMail.pdf

12. FortiMail 7.6.3. Administration Guide. URL: https://docs.fortinet.com/document/fortimail/7.6.3/administration-guide/313415/email-concepts-and-process-workflow

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)