ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ НА БАЗІ FORTIMAIL»

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

КИЇВ – 2021

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

APIs – Application Programming Interfaces

APT – Advanced Persistent Threat

BEC – Business Email Compromise

DNS – Domain Name System

IDS – Intrusion Detection System

IoT – Internet of Things

IP – Internet Protocol

IPsec – IP security

LDA – Local Delivery Agent

MUA – Mail User Agent

MTA – Mail Transfer Agent

SEG – Security Email Gateway

VPN – Virtual Private Networks

ВСТУП

Актуальність дослідження. Сьогодні корпоративна електронна пошта для більшості компаній є основним засобом комунікації. Листування необхідне як для спілкування всередині самих підприємств та організацій, так і для обміну даними з партнерами, клієнтами, постачальниками, державними органами тощо.

Ні для кого не секрет, що корпоративною електронною поштою пересилається великий об'єм конфіденційної інформації: договори, рахунки, інформація про продукцію та технології, ціни компанії, фінансові показники тощо. Якщо такі дані потрапляють до рук конкурентів, це може суттєво зашкодити підприємству, а бізнес може бути припиненим. Конкуренти, маючи в розпорядженні базу клієнтів, знаючи умови роботи і ціни, зможуть запропонувати їм кращі умови і, таким чином, нанесуть фінансові збитки.

Постійно спостерігається зростаюча тенденція до атак, які направлені на компрометацію ділової електронної пошти, коли зловмисник або захоплює, або ретельно імітує (підробляє) законний обліковий запис електронної пошти, щоб більш ефективно застосовувати соціальну інженерію в шахрайських діях та фінансових операціях. За оцінками фахівців, у 2020 році компрометація ділової електронної пошти була поширена у всіх галузях і розмірах бізнесу.

Одним словом, якщо в компанії постало питання про захист інформації, то, насамперед, необхідно захищати корпоративну пошту, так як основний об'єм документів пересилається через неї. При цьому треба закупляти, розгортати та застосовувати сучасні методи та засоби захисту корпоративної електронної пошти.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження методів та засобів захисту корпоративної електронної пошти.

Об'єкт дослідження – захист корпоративної електронної пошти.

Предмет дослідження – технологія захисту корпоративної електронної пошти.

Мета роботи – розробити порядок застосування технології захисту корпоративної електронної пошти та рекомендації щодо його реалізації.

Наукові завдання:

проаналізувати існуючі загрози корпоративній електронній пошті;

визначити зміст проблеми захисту корпоративної електронної пошти;

дослідити існуючі підходи до захисту корпоративної електронної пошти;

проаналізувати існуючі технології захисту корпоративної електронної пошти;

дослідити методи та засоби захисту корпоративної електронної пошти на базі FortiMail 200F;

розробити порядок застосування технології захисту корпоративної електронної пошти та рекомендації щодо захисту корпоративної електронної пошти.

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

Практичне значення одержаних результатів полягає в розробці рекомендацій щодо застосування технології захисту корпоративної електронної пошти.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференція «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2021 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ

1.1. Аналіз існуючих загроз корпоративній електронній пошті

Електронна пошта (e-mail), мабуть, найбільш широко використовувана система для обміну діловою інформацією через Інтернет (або будь-яку іншу комп'ютерну мережу). На самому базовому рівні процес електронної пошти можна розділити на два основних компоненти: (1) поштові сервери, які є хостами, які доставляють, пересилають і зберігають електронну пошту, та (2) поштові клієнти, які взаємодіють з користувачами і дозволяють користувачам читати, складати, відправляти і зберігати електронну пошту [1].

Розглянемо звіт PwC (PricewaterhouseCoopers, укр. ПрайсвотерхаусКуперс) щодо ландшафту загроз за 2020 рік [2]. PwC є авторитетною міжнародною мережою компаній, що пропонує професійні послуги у сфері консалтингу та аудиту.

Зазначається, що у 2020 році відбулося чітке зрушення в ландшафті кіберзагроз: програми-вимагачі стали найсерйознішою загрозою кібербезпеки, з якою стикаються організації, незалежно від галузі та місцезнаходження [2].

Пандемія COVID-19 також поширилася по кіберпростору, оскільки суб'єкти загроз використовували виникли в результаті цього страх і невпевненість. Більш широке використання віддаленої роботи працівників підприємств та організацій дозволило зосередити увагу на нових та існуючих загроз пов'язаних технологій та інфраструктури [2].

Істотні зміни в тактиці, що використовуються зловмисниками, які стоять за декількома родинами програм-вимагачів, привели до масової крадіжці даних до шифрування систем жертви. В результаті сайти з витоками набули розголосу, зробивши компроміс безпосередньо надбанням громадськості і посиливши тиск на жертв, щоб ті вимагали викупу [2].

Успіх таких операцій привернув на ринок нових гравців і навіть залучив

відомі кіберзлочинністю групи, які додали в свої портфелі програми-вимагачі. У міру зростання попиту на послуги програм-вимагачів партнерські програми і схеми Ransomware-as-a-Service (RaaS) знижували вхідний бар'єр для недосвідчених зловмисників.

Як і весь інший світ, суб'єкти загроз адаптувалися до змін, викликаних глобальною пандемією. І кіберзлочинці, і просунуті суб'єкти постійної загрози (APT) швидко включили цю тему в свої *фішингові електронні листи і документують приманки* [2].

Тема пандемії згодом еволюціонувала, щоб відобразити зміщення побоювань від доступності масок до схем фінансової допомоги і новин про вакцини, показуючи, що більшість суб'єктів загрози готові використовувати будь-які обставини, щоб зробити свої операції більш успішними. Здебільшого суб'єкти загроз використовували ці теми для виконання своєї звичайної діяльності, проте заходи реагування також були в центрі уваги досліджень, пов'язаних з вакцинами, які дуже затребувані декількома суб'єктами загроз [2].

Кілька тим, зазначених в 2019 році, продовжували грати свою роль в ландшафті загроз протягом усього 2020 року [2]:

діяльність зі збору розвідувальної інформації продовжувала відповідати геополітичному ландшафту, відображаючи події реального світу і стратегічні цілі національних держав;

також спостерігається зростаюча тенденція, коли суб'єкти загроз, історично пов'язані зі шпигунською діяльністю, зв'язуються з фінансово вмотивованою діяльністю, в операціях, які, ймовірно, мотивовані особистою вигодою;

ланцюжок поставок залишалася ключовою метою для зловмисників, які прагнуть скористатися привілейованим доступом і довірчими стосунками.

Група реагування на інциденти PwC у 2020 році відреагувала на численні кібератаки, що торкнулися ряд різних секторів промисловості. Переважна більшість, 86% інцидентів, сталися з вини кіберзлочинців [2].

З початку 2020 року дані близько 1330 жертв були розкриті, при цьому переважна більшість (79%) цих витоків відбулося в другій половині року. Це

відображає початок серії агресивних операцій з програмами-вимагачами, які збільшили кількість інцидентів. Але ця цифра спростовує мінливу долю деяких з найвідоміших операцій з програмами-вимагачами [2].

Група реагування на інциденти PwC відреагувала на інцидент, в ході якого було помічено, що зловмисник отримав доступ до середовища жертви всього за тиждень до виконання атаки програми-здирника Nefilim, причому половина цього часу була присвячена вилученню файлів з середовища жертви. Початковий доступ зловмисника здійснювався через скомпрометовані облікові дані постачальника програмного забезпечення, який надавав підтримку жертві щодо застосування постачальника [2].

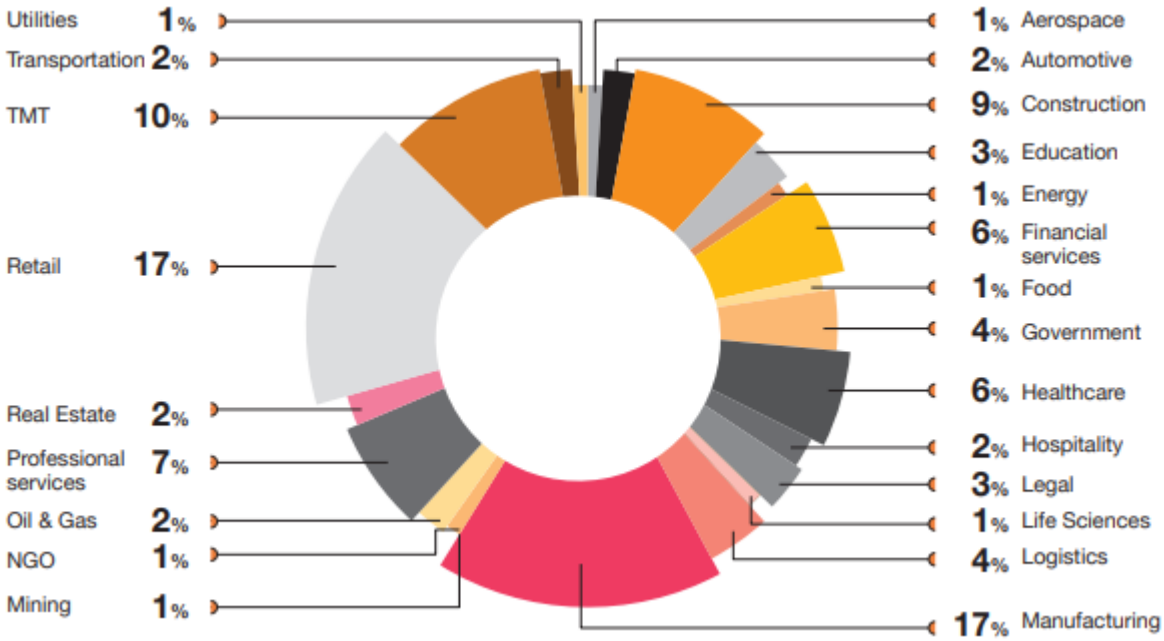

Рис. 1.1. Інциденти з програмами-вимагачами за секторами за 2020 [2]

Ці облікові дані використовувалися для отримання доступу до середовища жертви через рішення віддаленого доступу. Опинившись всередині, зловмисник використовував Cobalt Strike, щоб встановити наполегливість і C2, і використовував Mimikatz і Cobalt Strike, щоб розширити свій доступ і отримати доступ до більш привілейованих облікових записів [2].

Отримавши привілейований доступ, зловмисник ідентифікував файловий сервер і використовував його доступ для копіювання файлів з цього сервера, розміщення їх в інших скомпрометованих системах і завантаження їх в хмарні

служби, контрольовані зловмисником. Після вилучення цих даних зловмисник запустив програму-вимагач і пригрозив опублікувати вкрадені файли в Інтернеті, якщо не буде сплачено викуп. Після тижня несплати керівництву жертви прямо по електронній пошті пригрозили, що файли організації будуть опубліковані [2].

Компрометація ділової електронної пошти (Business Email Compromise, BEC): постійно спостерігається зростаюча тенденція до атак BEC, коли зловмисник або захоплює, або ретельно імітує (підробляє) законний обліковий запис електронної пошти, щоб більш ефективно застосовувати соціальну інженерію в шахрайських діях та фінансових операціях. У 2020 році BEC залишався поширеним у всіх галузях і розмірах бізнесу (рис. 1.1) [2].

За даними ФБР постійно зростаючі фінансові втрати від атак BEC склали 1,7 мільярда доларів в 2019 році, що зробило його найбільш прибутковою формою інтернет-злочинів в тому році. У той час як більшість атак BEC зосереджені на економії на масштабі, прагнучі отримати менші суми від цілей в декількох кампаніях, деяким зловмисникам вдалося вкрасти мільйони за одну атаку [2].

Атаки BEC стають все більш витонченими, в них використовується комбінація таких прийомів, як обман імен, захищений сервер і уособлення імені домена, компрометація електронної пошти постачальника (VEC) і атака типу «людина посередині» (PITM). Крім соціальної інженерії, дослідники безпеки відстежували експоненціальне зростання використання масових шкідливих програм (клавіатурних шпигунів і RAT) і фішингових методів серед учасників BEC в період з 2014 по 2020 рік, що свідчить про подальший розвиток TTP (Tactics, Techniques and Procedures) BEC для підвищення стійкості і масштабування можливостей крадіжки облікових даних (рис. 1.2) [2].

Серйозність BEC викликала посилення заходів правоохоронних органів на міжнародному рівні, що призвело до ряду гучних арештів у 2020 році. У червні 2020 року арешти Раймонда «Хушпуппі» Ігбалоде і Олалекана Якоба Понле (також відомого як «містер Вудберрі») притягнули увагу засобів масової інформації, після кримінальних скарг на людей, які стверджували, що їх розкішний спосіб життя, яким вони відкрито хвалилися в соціальних мережах більш ніж 2,4 мільйонам

передплатників, фінансується за рахунок доходів від онлайн-шахрайства. Стверджується, що один тільки Хушпуппі відмив близько 138 мільйонів доларів США в результаті атак BEC [2].

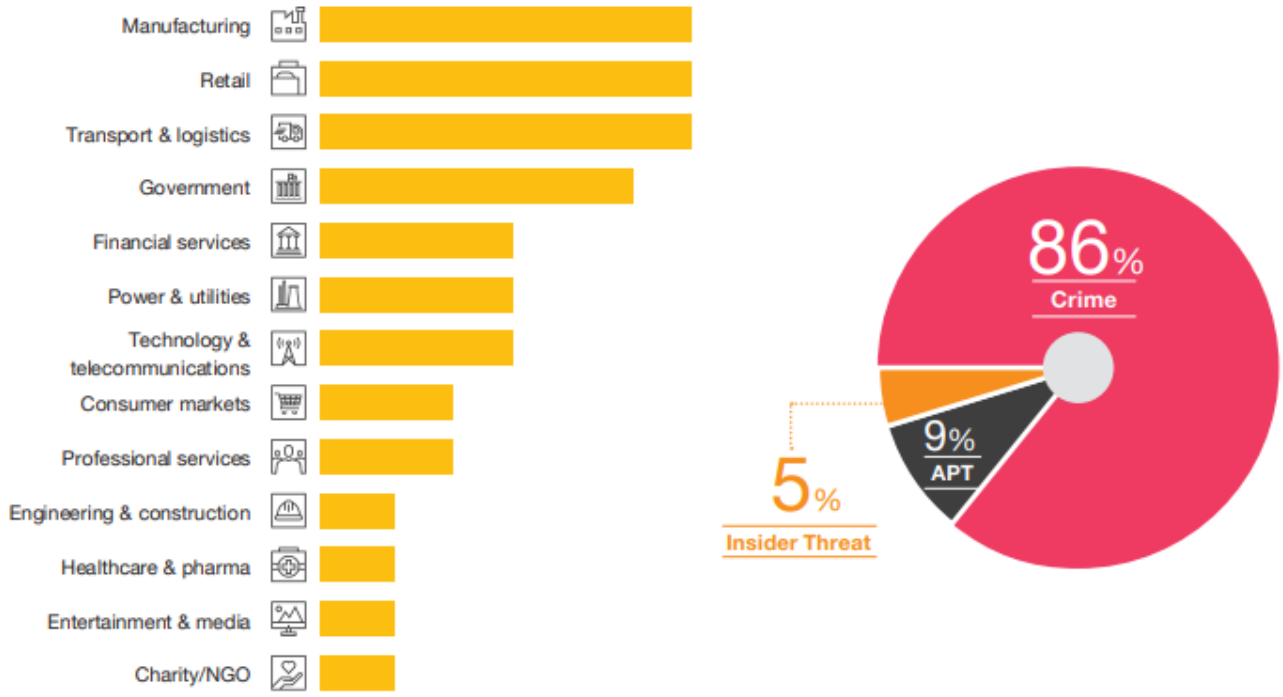

Рис. 1.2. Статистика команди реагування на інциденти PwC [2]

У листопаді 2020 року в рамках спільної операції Інтерпол, Group-IB і поліції Нігерії заарештували трьох осіб в Лагосі, обвинувачених в участі в BEC, а також в розробці та поширенні як мінімум *26 варіантів масового шкідливого ПЗ*, включаючи AgentTesla, Loki, Azorult, троянів віддаленого доступу Spartan, NanoCore і Remcos. PwC повідомила про діяльність 11 активних груп зловмисників, які базуються в Нігерії. Проте BEC також привертає більш витончених фінансово мотивованих зловмисників, таких як Cosmic Lynx, який базується в Росії [2].

З 2019 року російському зловмисникові приписують понад 200 кампаній проти цілей в 46 країнах, і, хоча в середньому зловмисники BEC запитують близько 55000 доларів США з кожної цілі, Cosmic Lynx запитує в середньому 1,27 мільйона доларів США [2].

Досить імовірно, що BEC продовжить залишатися дуже привабливою і прибутковою формою атаки, особливо в світлі збільшення числа співробітників, що працюють з дому через заходи ізоляції COVID-19. Дистанційна робота привела

до змін у функціонуванні багатьох підприємств, при цьому суб'єкти загроз продовжують отримувати вигоду з атмосфери невизначеності. Серйозність BEC викликала посилення заходів правоохоронних органів на міжнародному рівні, що призвело до ряду гучних арештів у 2020 році. Приклад з практики Norfund вкрав 100 мільйонів норвезьких крон в результаті злому ділової електронної пошти [2].

16 березня 2020 року Norfund перевів 9 888 055 доларів США на банківський рахунок в Banco Mercantil del Norte (Мексика), який, на думку Norfund, належав його клієнт – камбоджійській фінансовій установі LOLC Plc. Фактично банківський рахунок контролювався зловмисником, якому вдалося зламати обліковий запис електронної пошти, що належить співробітникові Norfund, зареєструвати підроблені домени і видати себе за співробітників Norfund і LOLC в розмові. До шахрайства, у вересні 2019 року, зловмисник зламав свій обліковий запис електронної пошти, що належить співробітникові Norfund, і протягом семи місяців контролював спілкування Norfund [2].

9 березня 2020 року зловмисник перехопив електронну переписку між Norfund і LOLC про майбутні транзакції. Він змінив реквізити банківського рахунку в повідомленні про виплату і переконав Norfund в тому, що використовувався мексиканський банк, щоб уникнути використання декількох банківських посередників в транзакції. Зловмисник використовував COVID-19 як фактор, щоб переконати LOLC в тому, що банківський переказ затримується. У той же час він відправив у Norfund електронні листи, що підтверджують, що кошти були отримані LOLC, щоб запобігти подальшому розслідування з боку Norfund [2].

24 квітня 2020 року зловмисник спробував маніпулювати транзакцією з іншим камбоджійським клієнтом, First Finance Plc, попросивши змінити реквізити банківського рахунку на Banco Mercantil del Norte. Інвестиційний менеджер Norfund звернувся в First Finance з проханням підтвердити зміну і згодом отримав підтвердження того, що рахунок їм не належить. 30 квітня 2020 року Norfund отримав електронного листа від LOLC, в якому говорилося, що реквізити банківського рахунку в переказі 16 березня 2020 року було невірними. Після виявлення спроби шахрайства Norfund звернувся до команди PwC з реагування на

інциденти, щоб впоратися з цим інцидентом у співпраці з норвезькими правоохоронними органами і постачальником IT-послуг Norfund [2].

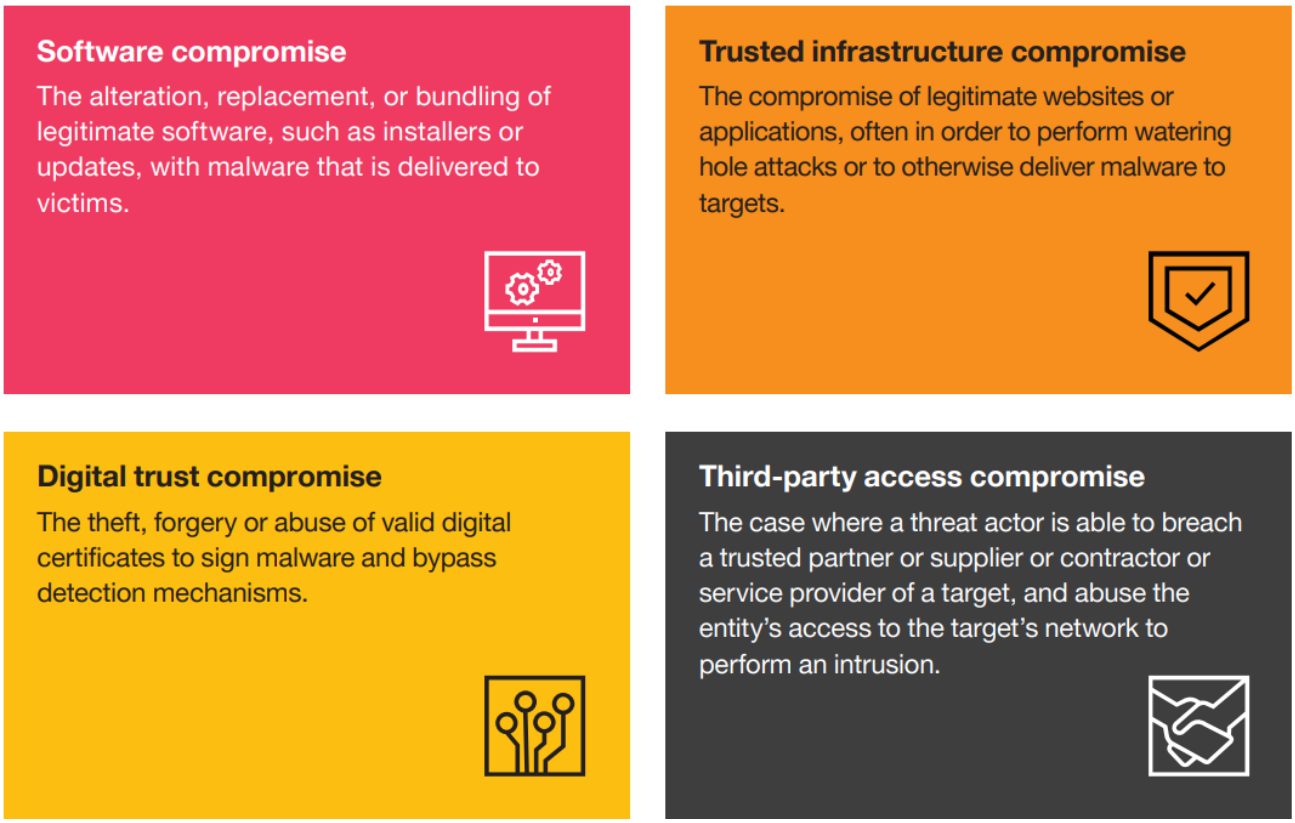

Рис. 1.3. Форми компрометацій інформаційних систем [2]

Щоб ускладнити зусилля щодо запобігання та виявлення, компрометація у ланцюгу поставок може приймати безліч різних форм, що може включати один або декілька з наступних прикладів (рис. 1.3) [2]:

компрометація програмного забезпечення – зміна, заміна або об'єднання законного ПЗ, такого як установники або поновлення, з шкідливим ПЗ, яке доставляється жертвам;

компрометація цифрової довіри – крадіжка, підробка або зловживання діючими цифровими сертифікатами для підпису шкідливих програм і обходу механізмів виявлення;

компрометація довіреної інфраструктури – компрометація законних веб-сайтів або додатків, часто з метою виконання атак watering hole або іншим способом доставки шкідливого ПЗ до цілей;

компрометація доступу третіх осіб – випадок, коли зловмисник може зламати довіреного партнера або постачальника, підрядника або постачальника

послуг цілі і зловжити доступом організації до мережі цілі для здійснення вторгнення.

Крім того, в деяких інцидентах компрометації ланцюжка поставок протягом 2020 року аналіз передбачає можливість того, що кілька суб'єктів загрози могли скомпрометувати одну і ту ж організацію «постачальника» одночасно або в різний час, що може ускладнити як визначення масштабів, так і реагування на інциденти , а також їх встановлення [2].

На місці кіберзлочинів переважають програми-вимагачі і поява сайтів з витоками інформації. Тепер жертви повинні мати справу з потенційним витоком конфіденційних даних і публічним розкриттям інцидентів, на додаток до впливу шкідливого шифрування на бізнес. Успіх цих операцій привів до появи нових гравців і розширенню існуючих кіберзлочинних угруповань. Це призвело до остаточного зсуву в ландшафті кіберзагроз, зробивши операції з програмами-вимагачами серйозною загрозою для організацій у всіх секторах і географічних регіонах, і ця тенденція, ймовірно, збережеться протягом 2021 року [2].

Стандарт [1] розглядає питання безпеки поштових серверів і поштових клієнтів, включаючи доступ до пошти через Інтернет.

Поштові сервери і робочі станції користувачів, на яких працюють поштові клієнти, часто стають об'єктами атак зловмисників. Оскільки обчислювальні і мережеві технології, що лежать в основі електронної пошти, широко поширені і добре зрозумілі для багатьох, зловмисники можуть розробити методи атаки, щоб використовувати слабкі місця в системі безпеки. Поштові сервери також стають мішенню, тому що вони (і загальнодоступні веб-сервери) повинні в деякій мірі взаємодіяти з ненадійними третіми сторонами. Крім того, поштові клієнти були націлені на ефективний засіб впровадження шкідливих програм на машини і поширення цього коду на інші машини [1].

В результаті поштові сервери, поштові клієнти і підтримуюча їх мережева інфраструктура повинні бути захищені. Нижче наведені приклади проблем з безпекою електронної пошти [1].

Необхідність обміну електронною поштою з зовнішнім світом, що є вимогою

для більшості організацій, дозволено за допомогою засобів захисту периметра мережі організації. На базовому рівні віруси і інші типи шкідливих програм можуть поширюватися по організації по електронній пошті. Однак все частіше зловмисники стають все більш витонченими і використовують електронну пошту для проведення цільових атак нульового дня в спробі скомпрометувати робочі станції користувачів у внутрішній мережі організації.

З огляду на природу електронної пошти, що дозволяє спілкуватися між людьми, її можна використовувати як засіб соціальної інженерії. Електронна пошта може дозволити зловмиснику використовувати користувачів організації для збору інформації або спонукати користувачів виконати дії, що сприяють атаці.

Недоліки в додатку поштового сервера можуть використовуватися як засіб компрометації базового сервера і, отже, приєднаної мережі. Приклади такого несанкціонованого доступу включають отримання доступу до файлів або папок, які не повинні були бути загальнодоступними, і можливість виконувати команди та/або встановлювати програмне забезпечення на поштовий сервер.

Атаки типу «відмова в обслуговуванні» (DoS) можуть бути спрямовані на поштовий сервер або його підтримувану мережеву інфраструктуру, забороняючи або перешкоджаючи дійсним користувачам використовувати поштовий сервер.

Конфіденційна інформація на поштовому сервері може бути прочитана неавторизованими особами або змінена несанкціонованим чином. Конфіденційна інформація, що передається між поштовим сервером і клієнтом в незашифрованому вигляді, може бути перехоплена.

Всі популярні стандарти електронної пошти за замовчуванням відправляють імена користувачів, паролі і електронні листи в незашифрованому вигляді. Інформація в електронному листі може бути змінена в якийсь момент між відправником і отримувачем.

Шкідливі об'єкти можуть отримати несанкціонований доступ до ресурсів в іншому місці мережі організації в результаті успішної атаки на поштовий сервер. Наприклад, після злому поштового сервера зловмисник може отримати паролі користувачів, які можуть надати зловмисникові доступ до інших вузлів в мережі

організації.

Шкідливі об'єкти можуть атакувати зовнішні організації в результаті успішної атаки на хост поштового сервера.

Невірна конфігурація може дозволити зловмисникам використовувати поштовий сервер організації для розсилки рекламних оголошень по електронній пошті (наприклад, спаму).

Користувачі можуть відправляти невідповідну, службову або іншу конфіденційну інформацію по електронній пошті. Це може привести до судового переслідування організації.

1.2. Дослідження існуючих підходів до захисту корпоративної електронної пошти

Розуміння того, як створюються, доставляються і зберігаються повідомлення електронної пошти, допомагає зрозуміти безпеку електронної пошти. Для більшості користувачів електронної пошти, коли повідомлення складено і відправлено, воно залишає комп'ютер і певним чином з'являється в поштовій скриньці одержувача. Це може здатися простим, але обробка і доставка повідомлення електронної пошти можуть вимагати не менше зусиль, як і доставка фізичної пошти, з обробкою і сортуванням, яка відбувається в декількох проміжних точках до прибуття в кінцевий пункт призначення [1].

Процес починається зі створення повідомлення. Найпростіші поштові клієнти зазвичай просять користувача вказати наступне: тему, вміст повідомлення і передбачуваних одержувачів. Коли ці поля заповнені і користувач відправляє повідомлення, повідомлення перетворюється в певний стандартний формат, зазначений в RFC 2822, Інтернет-формат повідомлення. На самому базовому рівні двома основними розділами повідомлення є заголовок і тіло. Розділ заголовка містить важливу інформацію про повідомлення, включаючи дату відправлення, відправника, одержувача(ів), шлях доставки, тему і інформацію про формат. Тіло повідомлення містить фактичний зміст повідомлення [1].

Як тільки повідомлення переведено в формат повідомлення RFC 2822, воно може бути передано. Використовуючи мережеве з'єднання, поштовий клієнт, званий поштовим призначеним для користувача агентом (MUA), підключається до агенту передачі пошти (MTA), що працює на поштовому сервері. Після ініціювання зв'язку поштовий клієнт надає серверу ідентифікаційні дані відправника. Потім, використовуючи команди поштового сервера, клієнт повідомляє серверу, ким є передбачувані одержувачі [1].

Хоча повідомлення містить список передбачуваних одержувачів, поштовий сервер не перевіряє повідомлення на наявність цієї інформації. Тільки після того, як на сервер буде відправлений повний список одержувачів, клієнт надає повідомлення. З цього моменту доставка повідомлень знаходиться під контролем поштового сервера [1].

Коли поштовий сервер обробляє повідомлення, відбувається кілька подій: ідентифікація сервера-одержувача, встановлення з'єднання і передача повідомлення. Використовуючи служби системи доменних імен (DNS), поштовий сервер відправника визначає поштовий сервер(и) для одержувача(ів). Потім сервер відкриває з'єднання з поштовим сервером(ами) одержувача і відправляє повідомлення, використовуючи процес, аналогічний тому, який використовується вихідним клієнтом [1].

У цей момент може статися одна з двох подій. Якщо поштові скриньки відправника і одержувача розташовані на одному поштовому сервері, повідомлення доставляється за допомогою локального агента доставки (LDA). Якщо поштові скриньки відправника і одержувача розташовані на різних поштових серверах, процес відправки повторюється від одного MTA до іншого, поки повідомлення не досягне поштової скриньки одержувача [1].

Коли LDA контролює повідомлення, може статися ряд можливих подій. Залежно від конфігурації LDA може доставити повідомлення або обробити повідомлення на основі попередньо визначеного фільтра повідомлень перед доставкою. Після доставки повідомлення поміщається в поштову скриньку одержувача, де воно зберігається до тих пір, поки одержувач не виконає з ним будь-

яку дію (наприклад, читання, видалення) за допомогою MUA. На рис. 1.4. показаний потік повідомлення через різні поштові компоненти, розглянуті раніше. Це загальний процес відправлення електронного листа.

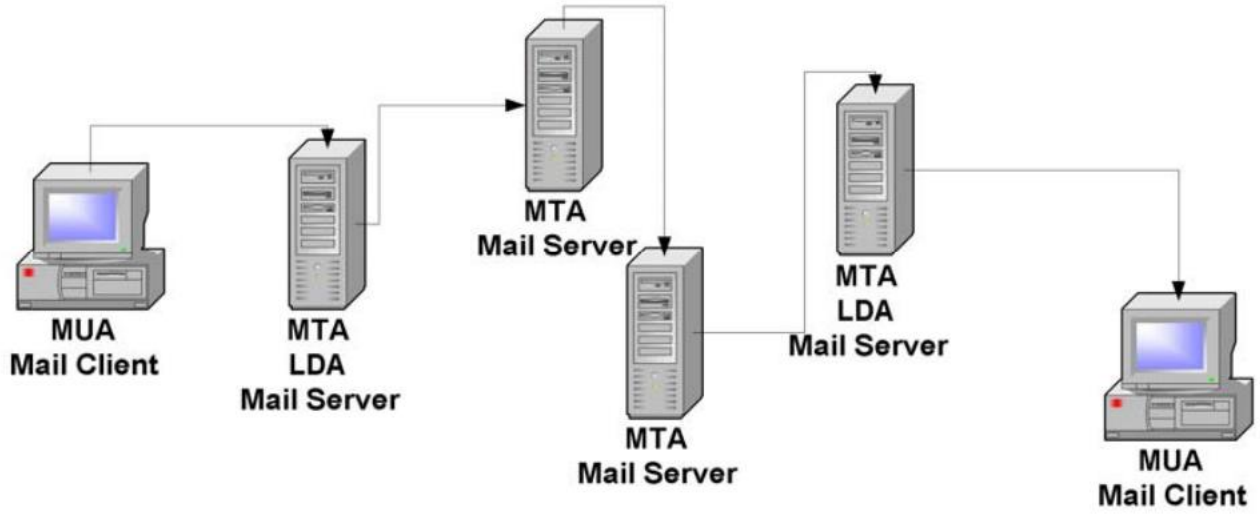

Рис. 1.4. Приклад потоку повідомлень [1]

Організації часто хочуть захистити конфіденційність і цілісність деяких своїх повідомлень електронної пошти, наприклад запобігти розкриттю особистої інформації у вкладеннях електронної пошти. Електронні листи можна захистити за допомогою криптографії різними способами, наприклад наступними [1]:

підпишіть цифровим підписом повідомлення електронної пошти, щоб переконатися в його цілісності і підтвердити особу відправника;

зашифруйте тіло повідомлення електронної пошти, щоб забезпечити його конфіденційність;

шифруйте обмін даними між поштовими серверами, щоб захистити конфіденційність як тіла повідомлення, так і заголовка повідомлення.

Перші два методи, підписання повідомлення і шифрування тексту повідомлення, часто використовуються разом. Наприклад, якщо повідомлення необхідно зашифрувати для захисту його конфіденційності, воно зазвичай також має цифровий підпис, щоб одержувач міг забезпечити цілісність повідомлення та перевірити особу яка підписала [1].

Повідомлення з цифровим підписом зазвичай не шифруються, якщо конфіденційність вмісту не вимагає захисту.

Третій метод криптографії, перерахований вище, шифрування передачі між поштовими серверами, зазвичай застосовується лише тоді, коли дві організації хочуть захистити електронні листи, які регулярно відправляються між ними. Наприклад, організації можуть створити віртуальну приватну мережу (VPN) для шифрування зв'язку між своїми поштовими серверами через Інтернет.

На відміну від методів, які можуть шифрувати тільки тіло повідомлення, VPN може шифрувати всі повідомлення, включаючи заголовки повідомлень електронної пошти, таку як відправники, одержувачі та теми. У деяких випадках організаціям може знадобитися захистити інформацію заголовка. Однак одне тільки рішення VPN не може забезпечити механізм підпису повідомлень і не може забезпечити захист повідомлень електронної пошти на всьому шляху від відправника до одержувача [1].

Більшість повідомлень електронної пошти захищаються індивідуально за допомогою цифрового підпису та, при необхідності, їх шифрування. Найбільш широко розповсюдженими стандартами для підпису повідомлень та шифрування повідомлень є Open Pretty Good Privacy (OpenPGP) і Secure/Multipurpose Internet Mail Extensions (S/MIME) [1].

Обидва вони частково засновані на концепції криптографії з відкритим ключем, яка передбачає, що у користувача є пара пов'язаних ключів: відкритий ключ, який може володіти будь-хто, і закритий ключ, який належить виключно його власнику. Оскільки криптографія з відкритим ключем вимагає великих обчислень, вона рідко використовується в захисті електронної пошти. Криптографія з симетричним ключем, яка набагато ефективніша, використовується набагато частіше [1].

Криптографія з симетричним ключем вимагає, щоб один ключ був загальним для взаємодіючих сторін, відправника та одержувача повідомлення електронної пошти. В процесі відправник генерує випадковий ключ і шифрує їм повідомлення з використанням алгоритму шифрування з симетричним ключем. Потім відправник шифрує симетричний ключ за допомогою відповідного алгоритму шифрування з відкритим ключем, використовуючи відкритий ключ одержувача, і відправляє

одержувачу зашифроване повідомлення і зашифрований симетричний ключ. Цей гібридний процес використовує шифрування з відкритим ключем тільки для шифрування симетричного ключа. Оскільки тільки передбачуваний одержувач повідомлення має закритий ключ, необхідний для відновлення симетричного ключа, ніяка інша сторона не може розшифрувати повідомлення і прочитати його. Методи цифрового підпису засновані на створенні дайджесту або відбитка інформації (тобто відправляти повідомлення) з використанням криптографічного хеша, який може бути підписаний більш ефективно, ніж всі повідомлення [1].

Існують проблеми з шифруванням електронної пошти. Хоча шифрування електронної пошти забезпечує додаткову безпеку, воно вимагає певних витрат, тому організаціям слід ретельно зважити проблеми, пов'язані з шифруванням повідомлень електронної пошти [1]:

сканування на віруси та інші шкідливі програми, а також фільтрація вмісту електронної пошти на брандмауері і поштовому сервері значно ускладнюються через шифрування.

Якщо у брандмауера або поштового сервера немає методу дешифрування електронної пошти, він не може прочитати його вміст і діяти відповідно до нього. Деякі сканери шкідливих програм можуть розшифрувати електронні листи, якщо сканер є одержувачем електронних листів або якщо відправник спеціально шифрує електронні листи для сканера, але такі рішення технічно складні і часто важко застосовувати. Крім того, надання сканера шкідливих програм можливості розшифровувати багато або всі електронні листи може мати серйозні наслідки, якщо хост сканера шкідливих програм сам заражений або іншим чином скомпрометований.

Якщо використання сканера шкідливих програм для розшифровування електронних листів неможливо, можливо, буде потрібно виконати сканування на вузлах поштових клієнтів, що виконують дешифрування;

шифрування і дешифрування вимагають процесорного часу. Організаціям може знадобитися оновити або замінити обладнання, яке не здатне підтримувати навантаження шифрування і дешифрування;

використання шифрування в масштабах всієї організації може зажадати значних адміністративних витрат. Приклади цього включають поширення ключів, відновлення ключів та відкликання ключів шифрування;

шифрування електронної пошти може ускладнити перевірку повідомлень електронної пошти правоохоронними органами та іншими слідчими сторонами.

Зашифровані електронні листи, відправлені або отримані від інших організацій, можуть бути недостатньо захищені, якщо ці організації не підтримують використання надійних алгоритмів шифрування і розмірів ключів. Організації повинні гарантувати, що поштові додатки їх користувачів повідомляють їх, коли вони отримують слабо зашифроване повідомлення або коли вони намагаються відправити зашифроване повідомлення одержувачу, який підтримує тільки слабкі методи шифрування. Потім користувачі можуть зв'язатися з відповідною стороною, щоб повідомити їх про проблему і попросити або використовувати більш надійний алгоритм шифрування, або передати інформацію, яка потребує захисту, за допомогою механізму, відмінного від електронної пошти.

1.3. Аналіз існуючих методів та засобів захисту корпоративної електронної пошти

Безпека електронної пошти повинна бути головним пріоритетом для будь-якої компанії. Електронна пошта – це найголовніша ціль, яку хакери використовують для отримання доступу до конфіденційних даних компанії, а атаки на електронну пошту, такі як фішинг та компрометація ділової електронної пошти, зростають. Тому першою лінією захисту повинен бути шлюз електронної пошти – платформа, яка захищає електронні листи від хакерів, спаму та вірусів [3].

Доступно багато рішень шлюзу електронної пошти. Деякі орієнтовані на корпоративних користувачів, які шукають детальний контроль адміністратора та розширену функціональність. Деякі з них краще підходять для невеликих підприємств, які шукають зручну платформу з вигідною ціною [3].

Відповідно до The Top 11 Email Security Gateways [3] розглянемо лідерів даного дослідження, а саме рішення SpamTitan, Avanan та Proofpoint Essentials.

SpamTitan Gateway – це комплексне рішення для фільтрації електронної пошти, яке захищає бізнес, співробітників та клієнтів. Продукт шлюзу гарантує виявлення спаму на 99,97%, захист від вірусів та шкідливих програм, контроль автентифікації, вихідне сканування, а також надійне звітування [5].

SpamTitan Gateway розроблений спеціально, щоб дозволити компаніям легко захистити своїх користувачів та мережу від електронної пошти, вірусів та шкідливих програм. Рішення шлюзу легко інтегрується в існуючу інфраструктуру і розгортання дуже просте [5].

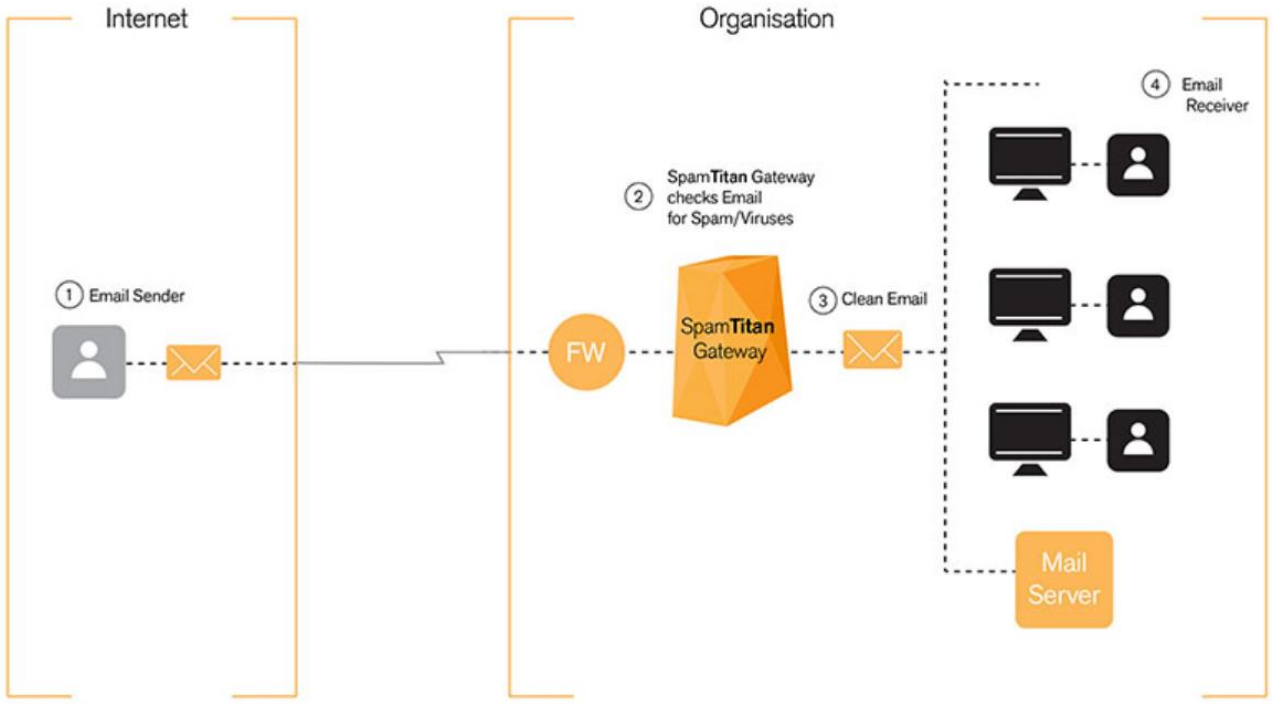

Рис. 1.6. Архітектура SpamTitan Gateway [5]

Особливості SpamTitan Gateway [5]:

фільтрування спаму – SpamTitan Gateway фільтрує електронний трафік організації, щоб запобігти поширенню електронної пошти до користувачів. Рішення гарантує 99,97% виявлення спаму за допомогою багатошарового аналізу спаму, включаючи; в режимі реального часу чорні списки (RBLs), списки сайтів, які були виявлені в небажаних повідомленнях електронної пошти (SURBLs), рамки політики відправника і байєсівський аналіз, це в поєднанні з низьким рівнем false positive спрацьовувань 0,03% дозволяє не втрачати справжньої електронної пошти та бути захищеними від небажаної електронної пошти;

блокування вірусів та шкідливих програм – рішення, яке отримало багато нагород, містить подвійний антивірусний захист: BitDefender та Clam AV, які служать для блокування вірусів та шкідливих програм, які намагаються проникнути у корпоративну мережу електронною поштою;

білий список / чорний список – рішення дозволяє вносити в білий / чорний список адреси електронної пошти відправника для дозволу / блокування пошти з певної адреси електронної пошти;

звітність – шлюз SpamTitan може надсилати користувачам звіти про карантин у визначений час та інтервали. Звіт про карантин містить список електронних листів, які не були надіслані користувачеві, оскільки вони потенційно містять спам або віруси. Кінцевий користувач може вирішити доставити, дозволити або видалити електронні листи у звіті про карантин;

перевірка одержувача – SpamTitan пропонує декілька типів перевірки одержувачів: це динамічна перевірка одержувачів (DRV), LDAP, заснована на списку та вказує перевірку регулярних виразів. Після доставки пошти до SpamTitan він перевіряє адресу електронної пошти на поштовому сервері, відхиляючи таким чином фальшиві електронні листи та спам;

вихідне сканування – сьогодні вихідне сканування електронної пошти є життєво важливим. Він блокує розсилку спаму та вірусів з організації, тим самим запобігаючи потраплянню IP-адрес у чорний список як спамерів однією з багатьох глобальних служб чорного списку. Чорний список IP-адрес запобігає доставці електронної пошти, заважає бізнес-процесам, а вирішення продуктивності важко та вимагає багато часу. Шлюз SpamTitan допомагає запобігти потраплянню до чорного списку до корпоративної IP;

автентифікація – налаштування веб-автентифікації дозволяють контролювати для кожного домену, який метод автентифікації використовуватиметься, коли користувач намагатиметься ввійти. Підтримуються такі методи автентифікації: внутрішня (за замовчуванням), LDAP, SQL-сервер, POP3 та IMAP. Підтримка зовнішніх модулів автентифікації гарантує, що, коли це

можливо, користувачам не доведеться запам'ятовувати кілька паролів. Усі спроби входу будуть спрямовані на відповідний сервер автентифікації для цього домену;

масштабування – шлюз SpamTitan є масштабованим, щоб задовольнити потреби організації.

Оскільки Avanan запатентував підхід на основі API до захисту електронної пошти в 2019 році, низка інших постачальників API вийшла на ринок. Існує багато відмінностей між рішеннями Avanan та іншими API. Але це ключове: Avanan може запобігти потраплянню шкідливих електронних листів до вхідних; інші можуть відповісти лише згодом [6].

Запатентоване рішення безпеки електронної пошти Avanan поєднує в собі всі переваги хмарного додатку безпеки електронної пошти та справжню безпеку попереднього вхідного повідомлення Secure Email Gateway (SEG).

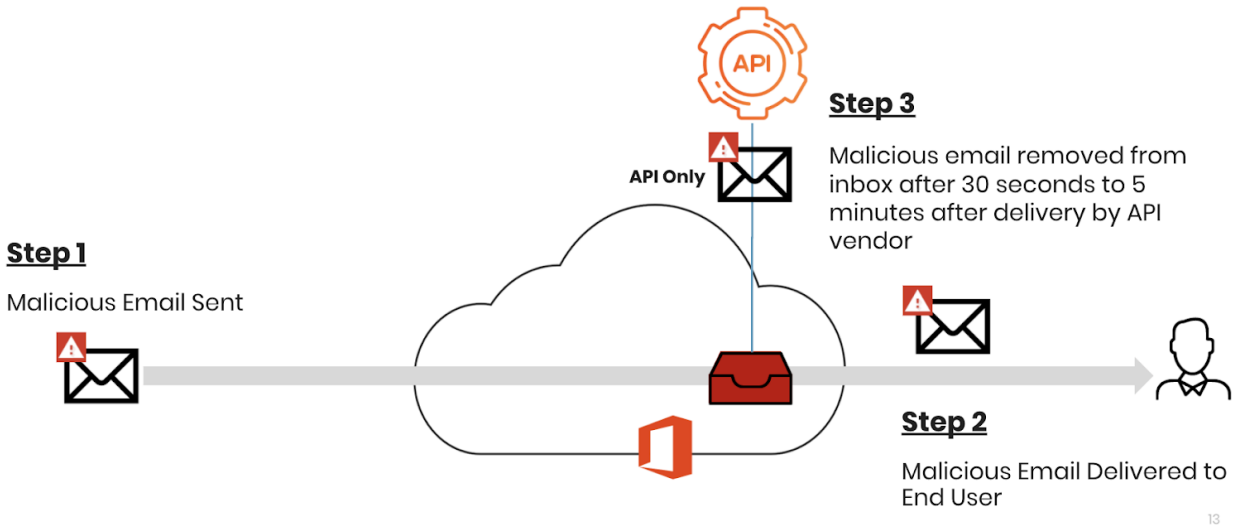

Рис. 1.7. Виявлення шкідливого повідомлення рішенням Avanan з API [6]

Інфраструктура Avanan підтримує API із запатентованими технологіями, що пропонують унікальні переваги перед постачальниками SEG та CESS. Зокрема, патент Avanan дозволяє запобігти доставці шкідливих електронних листів перед папкою Вхідні, а також забезпечити всі переваги внутрішнього захисту електронної пошти та забезпечення після доставки (рис. 1.7, 1.8) [6].

Ця архітектура не тільки блокує шкідливу електронну пошту перед папкою Вхідні, вона може робити це в масштабі, захищаючи компанії будь-якого розміру (від 25 до 250 000 користувачів або більше) [6].

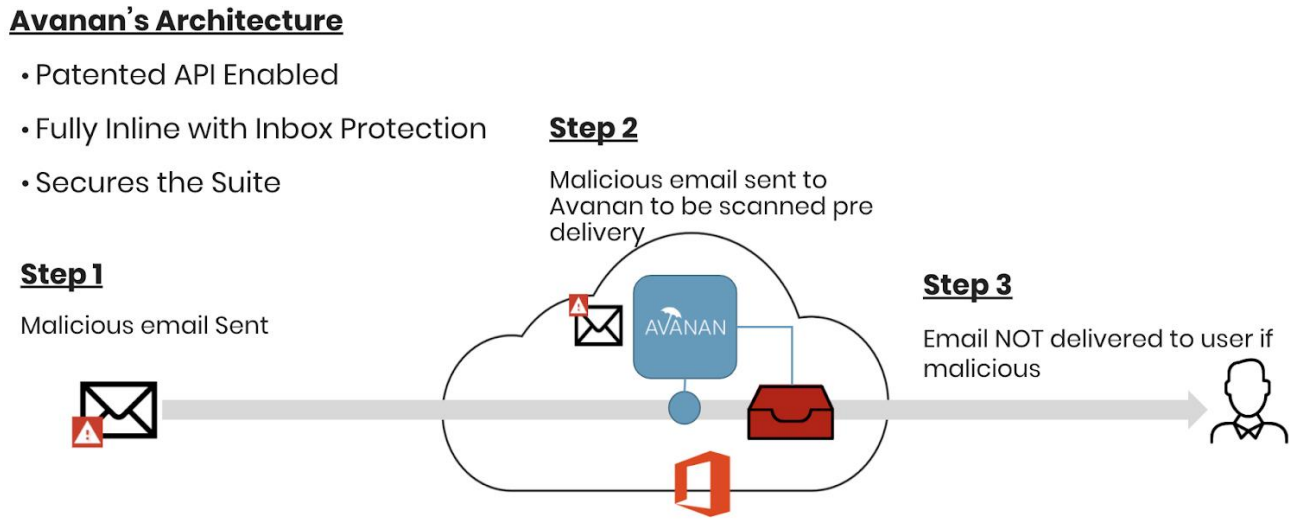

Рис. 1.8. Архітектура рішення Avanan [6]

Пакет Proofpoint Essentials Professional надає малому і середньому бізнесу захист електронної пошти нового покоління і відповідність вимогам. Він допомагає захистити співробітників від загроз, заснованих на шкідливих програмах, таких як шкідливі вкладення або посилання, від загроз, що не містять шкідливих програм, таких як шахрайство по електронній пошті або фішингові електронні листи з обліковими даними. Це також допомагає захищатися від атак через канали соціальних мереж. Захист від втрати даних (DLP) і шифрування електронної пошти ідентифікують і захищають конфіденційну інформацію, що відправляється по електронній пошті. А безперервність електронної пошти допомагає підтримувати бізнес-комунікації в постійному робочому стані. Хмарний архів електронної пошти допомагає підприємствам малого та середнього бізнесу управляти даними і забезпечувати їх безпеку, забезпечуючи відповідність вимогам і скорочуючи витрати на зберігання і управління [7].

Відмінними рисами Proofpoint Essentials є [7]:

багатошарова захист – Proofpoint Essentials Professional використовує ту ж безпеку і прозорість корпоративного класу як і найбільші організації в світі, що піклуються про безпеку;

розширений захист від загроз – більшість атак націлені на людей. Вони спонукають їх вибрати посилання в електронному листі або відкрити вкладення. Для захисту співробітників застосовуються передові можливості Targeted Attack Protection – провідного в галузі рішення для аналізу електронної пошти. Ця

унікальна технологія дозволяє аналізувати ізольоване програмне середовище URL-адрес і вкладень;

запобігання втрати даних і фільтрація контенту – Essentials Professional допоможе відповідати вимогам. Фільтр DLP на основі політик допомагає знизити ризик, коли співробітники приймають рішення про політику безпеки і розкриття інформації. Система автоматично ідентифікує і захищає вихідну конфіденційну інформацію. Сюди входять PII, PHI, фінансова інформація, умови GDPR і багато іншого з вбудованими словниками термінів та ідентифікаторами SmartSearch;

автоматичне шифрування електронної пошти – захист електронних листів, що містять конфіденційні дані є головним пріоритетом. Автоматичне шифрування електронної пошти допомагає знизити потенційні негативні наслідки втрати даних;

безперервність бізнесу – екстрена поштова скринька, миттєве відтворення втрачених або видалених листів за останні 30 днів і буферизація електронної пошти допомагають підтримувати бізнес;

захист облікового запису в соціальних мережах –контроль кожного облікового запису, щоб запобігти його злом і захистити від спаму і шкідливих програм, що розміщуються на ваших каналах;

хмарний архів електронної пошти – покращує управління сховищем електронної пошти і підвищує продуктивність. Всі повідомлення електронної пошти зберігаються в централізованому архіві. Можна отримати до них доступ з браузера і Microsoft Outlook або Outlook Web Access (OWA). Корпоративні користувачі також можуть отримати доступ до своїх архівів. І вони можуть шукати і читати свою повну історію електронної пошти. Вони також можуть отримувати повідомлення електронної пошти, які вони відправляли в минулому, і пересилати їх. Архів електронної пошти має необмежену сховище з політикою зберігання до 10 років і юридичним утриманням.

базові пакети – Proofpoint Essentials доступний в трьох спеціально розроблених пакетах, створених з урахуванням потреб бізнесу, вимог до функцій і бюджету.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ НА БАЗІ FORTIMAIL 200F

2.1. Призначення та основні функції рішення FortiMail 200F

FortiMail – високорейтинговий шлюз захисту електронної пошти, який використовується для протидії просунутим таргетованим кіберзагрозам, забезпечує захист від динамічних видів атак на підприємство, запобігає втраті конфіденційної інформації і сприяє дотриманню норм і правил. Високопродуктивні фізичні та віртуальні пристрої можуть бути розгорнуті на робочому місці або в загальнодоступному хмарному сервісі. Вони призначені для будь-яких організацій – від підприємств малого бізнесу до операторів зв'язку, провайдерів послуг і великих підприємств [8].

Засіб FortiMail 200F, який розглядається у даній роботі, призначений для підприємств малого бізнесу, відділень філій і організації.

Засіб FortiMail 200F виконує наступні основні функції захисту корпоративної електронної пошти [8]:

захист від загроз. Потужний засіб захисту від спаму і шкідливих програм включає в себе такі передові технології як протидія поширенню вірусів, знешкодження та реконструкція контенту, аналіз за допомогою технології «пісочниця», захист від імперсонації та інші технології для запобігання небажаної масової розсилки, атаки з метою вимагання викупу , компрометації корпоративної електронної пошти і націлених атак;

захист даних. Передбачені надійні функції запобігання втрати даних, шифрування електронної пошти на основі ідентифікації та архівування, які сприяють запобіганню ненавмисної втрати конфіденційної інформації та дотримання корпоративних і галузевих правил;

інтеграція з Fortinet Security Fabric. Інтеграція з продуктами Fortinet, а також з компонентами сторонніх організацій забезпечує упереджувальний підхід замовника до безпеки за допомогою спільного використання індикаторів

компрометації (IoC) з сумісним середовищем Fortinet Security Fabric. Він також забезпечує розширений і додатковий захист електронної пошти для середовищ Microsoft 365 за рахунок інтеграції на рівні API.

Fortinet лідирує в галузі щодо високої продуктивності, виміряної сторонніми тестувальниками по всьому світу. FortiMail усуває весь спектр ризиків, які електронна пошта являє для організацій, завдяки забезпеченню FortiGuard Labs аналітичними даними про загрози нульового дня [8].

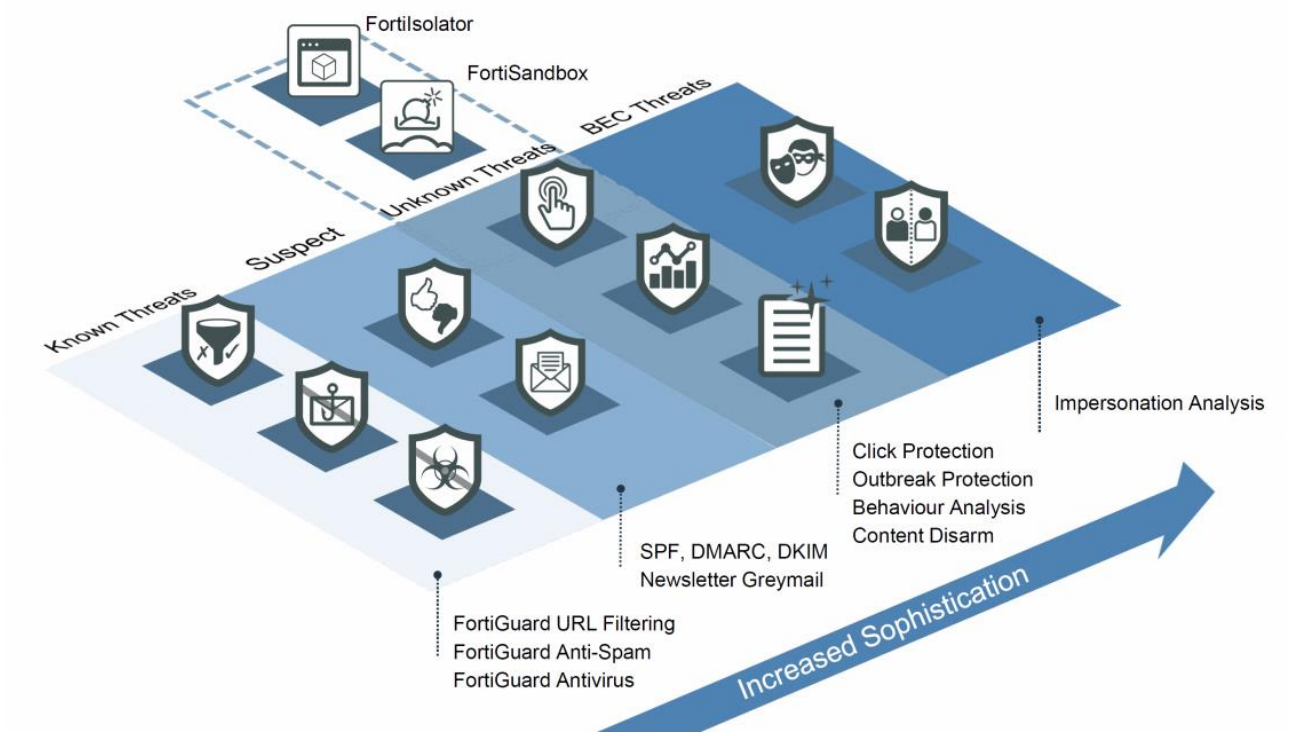

Рис. 2.1. Технології FortiMail [8]

Особливостями рішень FortiMail є:

багаторівневий захист від спаму. Більше десятка методів перевірки відправників, протоколів та вмісту захищають мережі та користувачів від небажаної масової електронної пошти. Він починається з оцінки IP, домену та інших репутацій і продовжується різними методами перевірки, такими як перевірка відмов у доставці, автентифікація та перевірка одержувача, а також перевірка SPF (інфраструктура політики відправника), DKIM (e-mail з доменними ключами) та DMARC (Domain-based Message Authentication, Reporting & Conformance, політика перевірки автентичності відправника електронного листа, заснована на протоколах DKIM і SPF). Нарешті, структура та вміст повідомлень аналізуються на основі

цифрового підпису, ключових слів у контексті, аналізу зображень, вбудованих URI (Uniform Resource Identifier) та більш досконалих методів, таких як аналіз поведінки та захист від спаму. Спільно працюючи, ці методи послідовно ідентифікують і блокують перевірені 99,7% спаму в реальних умовах;

інтегрований захист даних. Надійний набір можливостей для запобігання втрати даних, шифрування електронної пошти та архівування електронної пошти для безпечної доставки конфіденційних електронних листів та захисту від випадкової втрати даних. Ці особливості сприяють дотриманню корпоративної політики та галузевих норм;

висока продуктивність, гнучке розгортання. Легко масштабуючи для обробки більше двох мільйонів повідомлень на годину з повною фільтрацією антиспаму та антизловмисного програмного забезпечення, FortiMail обслуговує організації будь-якого розміру, з можливістю розгортання в шлюзному, прозорому або серверному режимах. Інтуїтивне управління електронною поштою в режимі реального часу, інформаційні панелі, розширені звіти, центральні карантини та засоби керування кінцевим користувачем, а також повні можливості MTA (Mail Transfer Agent) та обробки пошти забезпечують організаціям повну видимість та легкий контроль над трафіком електронної пошти;

потужний захист від шкідливих програм. Поєднуючи різні статичні та динамічні технології, що включають сигнатурні, евристичні та поведінкові прийоми, а також запобігання спалаху вірусів, FortiMail захищає від широкого кола загроз, які постійно розвиваються;

розширений захист від загроз. Для ще сильнішого захисту від найновіших класів загроз, таких як компрометація ділової електронної пошти та цілеспрямовані атаки, FortiMail пропонує необов’язкове роззброєння та реконструкцію вмісту, аналіз пісочниці, складне виявлення підробки тощо;

інтеграція API. Використовуючи API Microsoft 365 в Exchange Online, FortiMail може легко захистити внутрішню електронну пошту, а також вхідні скриньки користувачів від останніх загроз.

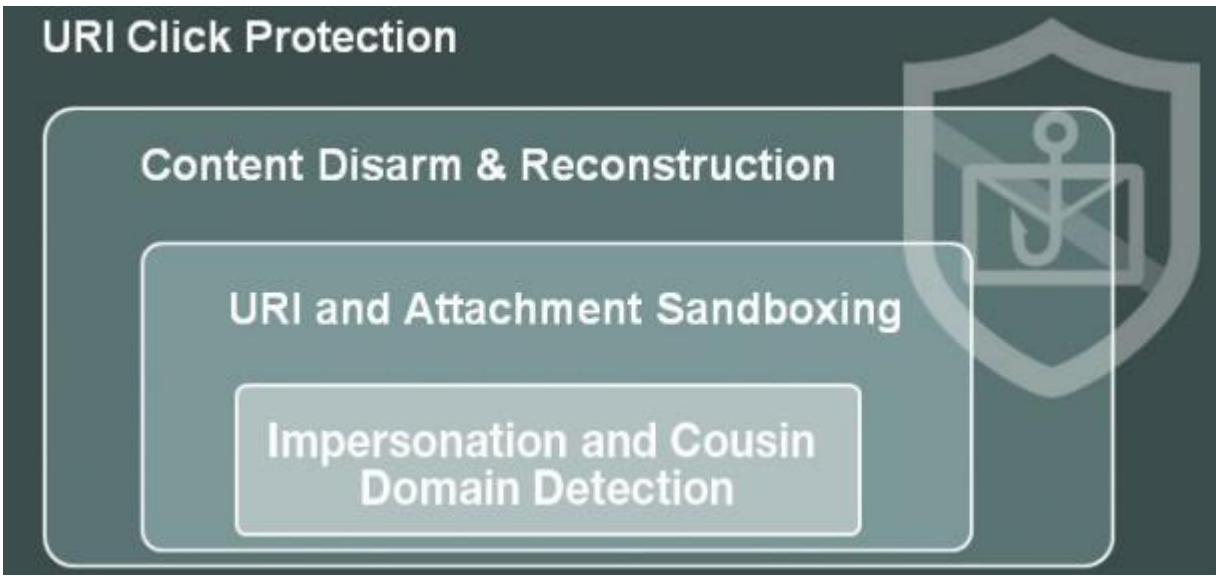

Рис. 2.2. Сучасні методи захисту електронної пошти [4]

Можливості FortiGuard Labs забезпечують найновіші методи захисту електронної пошти [4]:

визначення веб-сайтів, які були озброєні після доставки електронної пошти;

роззброєння та реконструкція вмісту, що видаляє вбудований активний код для доставки безпечних файлів;

застосування FortiSandbox для виявлення абсолютно нових шкідливих атак, вкладень та веб-сайтів;

аналіз уособлення для виявлення підробки та інших показників шахрайства з електронною поштою.

Ці методи доповнюють усталені функції повнофункціонального рішення безпечного шлюзу електронної пошти [4].

Особливостями системи рішень FortiMail є [8]:

широкий діапазон можливостей розгортання: прозорий режим, режим шлюзу і сервера; локальне розгортання, розгортання в загальнодоступному або приватному хмарному сервісі; служби управління хмарними середовищами;

перевірка вхідного і вихідного контенту;

підтримка декількох доменів електронної пошти та окремо настроює кожного домена: розрахована на багато користувачів підтримка MSSP (провайдера послуг управління безпекою) з підтримкою за концепцією «White label»

(використання продукції однієї компанії під брендом іншої); багаторівневе адміністрування;

підтримка адрес по протоколам IPv4 і IPv6;

віртуальний хостинг з використанням вихідного адреси та / або пулів цільових IP-адрес;

підтримка автентифікації SMTP по протоколам LDAP, RADIUS, POP3 і IMAP;

маршрутизація електронної пошти на основі протоколу LDAP;

перевірка кожного користувача з використанням атрибутів LDAP на основі політики (домену);

універсальний інтерфейс Webmail (веб-пошти) для розгортання режиму сервера та управління карантином;

управління чергою поштових повідомлень;

багатомовна підтримка додатку Webmail і інтерфейсу адміністратора;

відповідність RFC протоколу SMTP;

сучасний графічний інтерфейс користувача (GUI) на основі HTML 5;

незалежне тестування VBSpam, NSS, ICSA;

сумісність з хмарними сервісами, наприклад Office365, Google G-Suite.

Особливостями захисту від спаму рішень FortiMail є [8]:

служба захисту від спаму FortiGuard: репутація відправника в глобальній мережі; контрольні суми об'єктів спаму; евристичні правила з динамічними характеристиками;

захист від масової розсилки спаму в реальному часі FortiGuard;

фільтрація URL-адрес всіх категорій з використанням служби FortiGuard, включаючи URL-адреси спаму, шкідливих програм і фішингових URL-адрес;

щодо компрометація корпоративної електронної пошти (BEC): багаторівневий захист від спуфинга та виявлення самозванців;

застосування технології Greylisting (сірі списки) для IPv4, IPv6- адрес і облікових записів електронної пошти;

локальна репутація відправника (на основі протоколів IPv4, IPv6 і ідентифікатора кінцевих точок);

аналіз поведінки;

поглиблена перевірка заголовків електронної пошти;

інтеграція зі сторонніми URI-адресами спаму і чорними списками в реальному часі (SURBL/RBL);

інформаційний бюлетень (greymail) і виявлення підозрілих інформаційних бюлетенів;

сканування PDF і аналіз зображень;

чорні/безпечні списки на рівні глобальної мережі, домену або на рівні користувача;

підтримка стандартів підприємства по ідентифікації відправника: інфраструктура політики відправника (SPF), пошта з доменними ключами (DKIM) та ідентифікація повідомлень по доменному імені (DMARC);

гнучкі профілі дій і повідомлень;

множинні карантини системи і індивідуальних користувачів;

динамічний аналіз зображень для дорослих;

Особливостями захисту від шкідливих програм рішень FortiMail є [8]:

виявлення за допомогою FortiGuard Antivirus: перевірка сигнатур CPRL; визначення поведінки на основі евристики; виявлення потенційно небезпечного ПЗ;

протидія поширенню вірусів FortiGuard Virus Outbreak: надання та аналіз даних про глобальні загрози;

захищений паролем архів і дешифрування PDF;

виявлення активного контенту (документів PDF і Office);

повторне сканування загроз при випуску з карантину;

перевірка хешування призначених для користувача файлів.

Особливостями захисту від націлених атак рішень FortiMail є [8]:

знешкодження та нейтралізація контенту: нейтралізація документів Office і PDF (видалення макросів, активного контенту, додатків тощо); нейтралізація

HTML-контенту електронної пошти; видалення URL-гіперпосилань; перезапис URL-адрес;

URL Click Protect (підміна сумнівних посилань) для перезапису;

URL-адрес і повторне сканування при доступі;

аналіз імперсонації;

інтеграція хмарної і локальної пісочниці, що підтримує аналіз файлів і URL адрес.

Особливостями управління, ведення журналів і складання звітів рішень FortiMail є [8]:

основні / поліпшені режими управління;

облікові записи адміністрування на основі ролей для кожного домена;

повномасштабна активність, зміна конфігурацій, ведення журналів і звітність;

вбудований модуль генерації звітів;

централізований карантин для великомасштабних розгортань;

додаткове централізоване ведення журналів і складання звітів за допомогою FortiAnalyzer;

підтримка SNMP-протоколу з використанням стандартної і захищеною MIB (інформаційної бази управління) з пастками на основі порогових значень;

підтримка локального або зовнішнього сервера зберігання, включаючи пристрої iSCSI;

підтримка зовнішнього журналу системних повідомлень;

відкритий архітектурний стиль REST на базі інтерфейсу API для налаштування і управління.

Особливостями щодо забезпечення високої доступності (HA) рішень FortiMail є [8]:

Висока доступність підтримується для всіх сценаріїв розгортання: режим активний-пасивний; режим синхронізації налаштування активний-активний;

синхронізація карантину і черги поштових повідомлень;

виявлення та повідомлення про несправності пристрою;

підтримка статусу посилання, самовідновлення та резервного інтерфейсу.

Особливостями рішень FortiMail щодо вдосконалених функцій є [8]:

архівування електронної пошти на основі політик з можливістю віддаленого зберігання: підтримка архівації журналу обміну;

універсальний захист від втрати даних за допомогою фінгерпрінтінга файлів і виявлення конфіденційної інформації: автоматичний фінгерпрінтінг CIFS (загальна файлова система Інтернету) і завантаження вручну; виявлення інформації про медичний контроль, фінанси і персональну інформацію;

шифрування на основі ідентифікації та S/MIME;

набір вдосконалених функцій сервера електронної пошти: універсальний інтерфейс веб-пошти; доступ до електронної пошти за протоколами POP3, IMAP; функції календарного планування; скасування відправлень;

інтеграція протоколу SAML 2.0 для SSO (Single Sign-On) і ADFS (Служби федерації Active Director) для доступу до веб-пошти і карантину.

Особливостями рішень FortiMail щодо підтримки є [8]:

прості можливості підтримки, що включають пакети підписок;

удосконалена підтримка повернення неякісних або несправних виробів (RMA);

кваліфікована допомога і можливість підтримки при установці.

2.2. Архітектура та основні компоненти рішення FortiMail 200F

Існує кілька поширених стандартних протоколів електронної пошти: SMTP, POP3, IMAP, HTTP та HTTPS. Розглянемо їх відповідно до [9].

Простий протокол пересилання пошти (Simple Mail Transfer Protocol, SMTP) – це стандартний протокол для надсилання електронної пошти між:

двома агентами пересилання пошти (mail transfer agent, MTA);

поштовий агент користувача (mail user agent, MUA) та MTA.

Зв'язок SMTP зазвичай відбувається на TCP номер порту 25 та SMTPS, як правило, відбувається на порту TCP номер 465.

Коли користувач електронної пошти надсилає електронне повідомлення,

його MUA використовує SMTP для надсилання електронного листа на MTA, який часто є їхнім сервером електронної пошти. Потім MTA використовує SMTP для прямої або непрямої доставки електронної пошти на кінцевий сервер електронної пошти, на якому розміщується електронна пошта для одержувача електронної пошти.

Коли MTA підключається до цільового сервера електронної пошти, він визначає, чи існує одержувач на цільовому сервері електронної пошти. Якщо адреса електронної пошти одержувача є законною, тоді MTA доставляє електронне повідомлення на сервер електронної пошти, з якого користувачі електронної пошти можуть потім використовувати протокол, такий як POP3 або IMAP для отримання електронного листа. Якщо адреса електронної пошти одержувача не існує, MTA зазвичай надсилає окреме повідомлення електронної пошти відправнику, повідомляючи його про помилку доставки.

Хоча основний протокол SMTP простий, багато серверів SMTP підтримують ряд розширень протоколу для таких функцій, як автентифікація, шифрування, багаточастинні повідомлення та вкладення, і їх можна називати розширені SMTP (ESMTP) сервери.

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

Протокол поштового відділення версії 3 (Post Office Protocol version 3, POP3) – це стандартний протокол, який використовується поштовими клієнтами для отримання електронної пошти, яка була доставлена та збережена на сервері електронної пошти. Зв'язок POP3 зазвичай відбувається на TCP номер порту 110.

На відміну від IMAP, після того, як клієнт POP3 завантажує електронне повідомлення на комп'ютер користувача електронної пошти, копія електронного листа, як правило, не залишається на жорсткому диску сервера електронної пошти. Перевага цього полягає в тому, що це звільняє місце на жорсткому диску на сервері. Недоліком цього є те, що завантажена електронна пошта зазвичай знаходиться лише на одному персональному комп’ютері. Якщо всі їх клієнти POP3 не налаштовані завжди залишати копії електронних листів на сервері, користувачі

електронної пошти, які використовують кілька комп’ютерів для перегляду електронної пошти, наприклад, як на робочому столі, так і на ноутбуці, не зможуть переглядати з одного комп’ютера будь-яку електронну пошту, яка раніше була завантажена на інший комп'ютер.

Блоки FortiMail не сканують трафік POP3 на наявність спаму та вірусів.

Протокол доступу до повідомлень в Інтернеті (Internet Message Access Protocol, IMAP) – це стандартний протокол, який використовується поштовими клієнтами для отримання електронної пошти, яка була доставлена та збережена на сервері електронної пошти.

Зв'язок IMAP зазвичай відбувається на TCP номер порту 143.

Якщо клієнти IMAP не налаштовані на доступ у режимі офлайн, спочатку клієнти завантажують лише заголовок повідомлення. Вони завантажують тіло повідомлення та вкладення, лише коли користувач електронної пошти вирішив прочитати електронне повідомлення.

На відміну від POP3, коли клієнт IMAP завантажує електронне повідомлення на комп'ютер користувача електронної пошти, копія електронного листа залишається на жорсткому диску сервера електронної пошти. Перевага цього полягає в тому, що він дозволяє користувачам електронної пошти переглядати електронні листи з більш ніж одного комп’ютера. Це особливо корисно в ситуаціях, коли більше ніж одній людині може знадобитися переглянути папку Вхідні, наприклад, коли всі члени відділу контролюють колективну папку Вхідні. Недоліком цього є те, що, якщо користувачі електронної пошти не видаляють електронну пошту, IMAP може швидше витрачати місце на жорсткому диску сервера.

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

Протоколи передачі гіпертексту (Secured and non-secured HyperText Transfer Protocols, HTTP/HTTPS), хоча і не є суто для транспортування електронної пошти, часто використовуються програми веб-пошти для перегляду електронної пошти,

яка зберігається віддалено.

Зв'язок HTTP зазвичай відбувається на TCP порт номер 80; Зв'язок HTTPS зазвичай відбувається на TCP-порту номер 443.

Блоки FortiMail не сканують трафік HTTP або HTTPS на наявність спаму чи вірусів, але використовують їх для відображення карантину і, якщо блок FortiMail працює в режим сервера, FortiMail веб-пошта.

Клієнт-серверні з'єднання в SMTP

З'єднання клієнт-сервер та спрямованість з'єднання в SMTP відрізняються від інших протоколів. Наприклад, у даному протоколі клієнт SMTP підключається до сервера SMTP. Це, здається, відповідає традиційній моделі комунікації клієнт-сервер. Однак завдяки поняттю ретрансляції в SMTP, клієнт SMTP може бути:

програма електронної пошти на персональному комп'ютері користувача;

інший SMTP-сервер, який виступає в ролі агента доставки для користувача електронної пошти, передаючи електронне повідомлення на його цільовий сервер електронної пошти.

Розміщення клієнтів та серверів у топології мережі може вплинути на режим роботи, який обирається під час встановлення пристрою FortiMail. Якщо пристрій FortiMail буде працювати в режимі шлюзу або серверному режимі, SMTP-клієнти (включаючи SMTP-сервери, що підключаються як клієнти) повинні бути налаштовані для підключення до блоку FortiMail.

Такі терміни, як MTA та MUA, описують взаємозв'язок сервера та клієнта, характерні для протоколів електронної пошти.

Mail Transfer Agent (MTA) – це SMTP-сервер, який передає повідомлення електронної пошти іншому SMTP-серверу. Не всі MTA є повноцінними серверами електронної пошти. Деякі MTA існують виключно для ретрансляції електронної пошти та не містять облікових записів користувачів електронної пошти.

Одиниці FortiMail, що працюють у шлюзового режиму як MTA. Одиниці FortiMail, що працюють у режиму сервера як MTA і повний (SMTP, IMAP, POP3, сервер електронної пошти).

Для доставки електронної пошти, якщо електронна пошта не входить і сервер

електронної пошти не має доменного імені та доступ до неї здійснюється лише за IP-адресою, MTA повинен запитати DNS-сервер для запис MX та передачу відповідного запису.

Mail User Agent (MUA) або поштовий клієнт – це програмне забезпечення, таке як Microsoft Outlook, яке дозволяє користувачам надсилати та отримувати електронні листи.

Підтримка одиниць FortiMail SMTP-з'єднання для надсилання електронної пошти MUA.

Одиниці FortiMail, що працюють в режимі сервера POP3 та з’єднання IMAP для отримання електронної пошти за допомогою MUA. Для користувачів електронної пошти, які вважають за краще використовувати свої веб-браузери для надсилання та отримання електронної пошти замість традиційного MUA, блоки FortiMail, що працюють у серверному режимі, також надають FortiMail веб-пошта [9].

Багато функцій FortiMail, такі як проксі-сервери та правила, впливають на спрямованість з'єднання SMTP або повідомлення електронної пошти.

Вхідні SMTP-з'єднання складаються з тих, призначених для SMTP-серверів, які є захищеними доменами блоку FortiMail. Наприклад, якщо блок FortiMail налаштований на захист SMTP-сервера, IP-адреса якого 192.168.0.1, блок FortiMail розглядає всі підключення SMTP, призначені для 192.168.0.1, як вхідні.

Вихідні з'єднання складаються з тих, призначених для SMTP-серверів, які блок FortiMail не налаштовано захищати. Наприклад, якщо блок FortiMail не налаштований на захист SMTP-сервера, IP-адреса якого 10.0.0.1, усі підключення SMTP, призначені для 10.0.0.1, будуть розглядатися як вихідні, незалежно від їх походження [9].

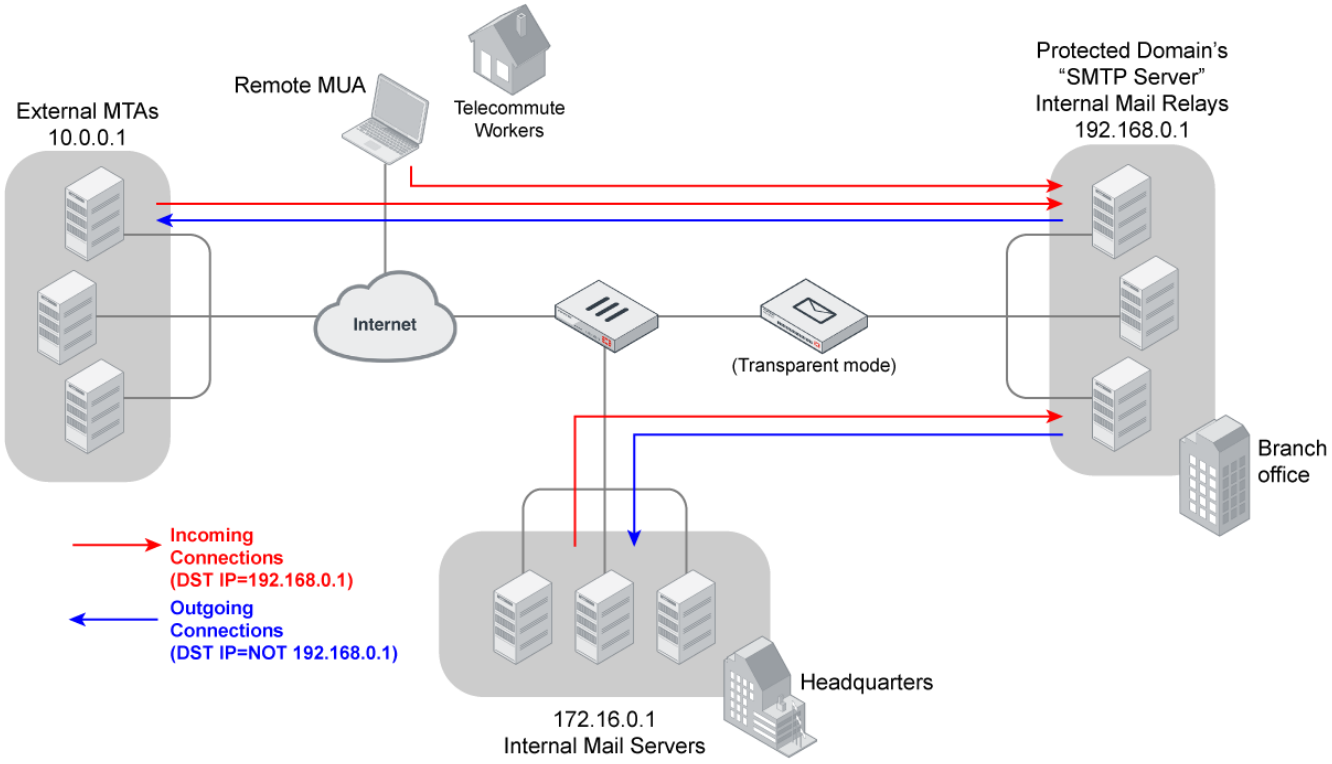

Рис. 2.3. Вхідні та вихідні з'єднання SMTP [9]

Вхідний та вихідний електронний лист

Вхідні повідомлення електронної пошти складаються з повідомлень, надісланих захищеним одержувачам домену (RCPT TO:). Наприклад, якщо блок FortiMail налаштований на захист SMTP-сервера, ім'я домену якого є example.com, блок FortiMail розглядає всі повідомлення електронної пошти, надіслані на example.com, як вхідну електронну пошту [9].

Вихідні повідомлення електронної пошти складаються з повідомлень, надісланих одержувачам (RCPT TO:) на домени, які блок FortiMail не налаштовано захищати. Наприклад, якщо блок FortiMail не налаштований на захист домену example.com, усі повідомлення електронної пошти, надіслані одержувачам на example.com, будуть розглядатися як вихідні повідомлення електронної пошти, незалежно від їх походження [9].

Спрямованість на рівні з'єднання може відрізнятися від спрямованості на рівні повідомлень електронної пошти, що містяться в з'єднанні. Можливо, що вхідне з'єднання може містити вихідне повідомлення електронної пошти, і навпаки [9].

Наприклад, на наведеному малюнку підключення від внутрішніх поштових

ретрансляторів до внутрішніх поштових серверів є вихідними, але вони містять вхідні повідомлення електронної пошти. І навпаки, підключення від віддалених MUA до внутрішніх реле пошти є вхідними, але можуть містити вихідні повідомлення електронної пошти, якщо адреси електронної пошти одержувачів (RCPT TO:) є зовнішніми.

Оскільки спрямованість розглядається окремо на мережевому та прикладному рівнях, спрямованість з'єднання SMTP може бути протилежною спрямованості повідомлення електронної пошти: 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 [9].

Роль DNS у доставці електронної пошти

SMTP можна налаштувати на роботу без DNS, використовуючи IP-адреси замість доменних імен для SMTP-клієнтів, SMTP-серверів та електронних адрес одержувачів. Однак така конфігурація зустрічається рідко.

SMTP, як він зазвичай використовується, покладається DNS для визначення сервера поштового шлюзу (MX) для доменного імені та для перетворення імен доменів на IP-адреси. Таким чином, зазвичай треба налаштувати сервери електронної пошти та блоки FortiMail, щоб мати можливість запитувати DNS-сервер.

Крім того, вам також може знадобитися налаштувати DNS-сервер за допомогою запис MX, запис і зворотний запис DNS для захищених доменних імен та доменного імені самого блоку FortiMail.

Компоненти FortiMail отримують електронну пошту для визначених доменів електронної пошти та керують передачею електронної пошти в інші домени. Електронну пошту, що проходить через блок FortiMail, можна сканувати на наявність вірусів та спаму. Політики та профілі визначають, як блок FortiMail сканує електронну пошту та що робить із повідомленнями електронної пошти, що містять віруси або спам.

На додаток до політик та профілів, інші налаштовані елементи, такі як домени електронної пошти, можуть впливати на те, як блок FortiMail обробляє

електронну пошту.

Блоки FortiMail можуть працювати в одному з трьох режими роботи: режим шлюзу, прозорий режим, і режим сервера.

Таблиця 2.1. Порівняння шлюзового, прозорого та серверного режимів роботи FortiMail [9]

	Gateway	Transparent	Server
SMTP role	MTA/relay	Transparent proxy/relay	Server
FortiMail unit is hidden	No	Yes, if enabled	No
Email user accounts	Preferences and per-recipient quarantine only	Preferences and per-recipient quarantine only	Yes
Requires DNS record change	Yes	No, if hidden with no per-recipient quarantines or Bayesian scan	Yes
May require changes to SMTP client configurations or other infrastructure	Yes	No	Yes
Requires FortiMail unit located between external MTAs and protected email servers	No	Yes	N/A (FortiMail unit acts as email server)
Protected email servers	Separate	Separate	Integrated (FortiMail unit acts as email server)

Крім того, деякі функції FortiMail специфічні для режиму роботи. Як результат, зміна режиму роботи може скинути конфігурацію FortiMail.

Методи управління FortiMail

Після встановлення блоку FortiMail треба налаштувати та керувати пристроєм одним із наступних двох методів [9]:

веб-менеджер;

інтерфейс командного рядка (CLI).

CLI доступний лише для облікових записів адміністраторів, домен яких - система. Він недоступний для домену (багаторівневий) облікові записи адміністратора.

Веб-менеджер дозволяє налаштувати пристрій FortiMail, підключившись до блоку FortiMail через веб-браузер. Веб-інтерфейс має два режими: стандартний

режим і розширений режим.

Стандартний режим забезпечує просту навігацію за допомогою спрощеного набору параметрів меню, які дозволяють використовувати багато, але не всі типові конфігурації блоку FortiMail. Менш часто використовувані параметри приховані, а деякі конфігурації спрощуються, надаючи заздалегідь визначені набори конфігурації [9].

Розширений режим надає повний набір опцій меню, що дозволяє досягти більш складних конфігурацій. Можна будь-коли перемикатись між основним режимом та розширеним режимом веб-інтерфейсу, не втрачаючи при цьому конфігурації. Наприклад, якщо надається перевага стандартному режиму, але потрібно налаштувати елемент, доступний лише в розширеному режимі, то можна перейти в розширений режим, налаштувати елемент, а потім повернутися до стандартного режиму. Щоб перемикатися між двома режимами, виберіть Стандартний режим або Розширений режим зі спадного списку у верхньому правому куті веб-інтерфейсу [9].

2.3. Варіанти розгортання та застосування рішення FortiMail 200F

При розгортанні та застосуванні рішення FortiMail необхідно обрати один із можливих варіантів: прозорий режим, режим шлюзу або режим сервера, який відповідає певним вимогам до безпеки електронної пошти, мінімізуючи зміни інфраструктури та переривання обслуговування [8].

Розглянемо режим шлюзу (Gateway Mode) (рис. 2.4). Надає служби агента пересилання пошти (MTA) вхідного і вихідного проксі-сервера для існуючих шлюзів захисту електронної пошти. Простою зміною запису DNS MX електронна пошта перенаправляється в FortiMail для сканування на наявність спаму і вірусів. FortiMail отримує повідомлення, сканує їх на наявність вірусів і спаму, а потім відправляє електронну пошту на цільової сервер електронної пошти для доставки.

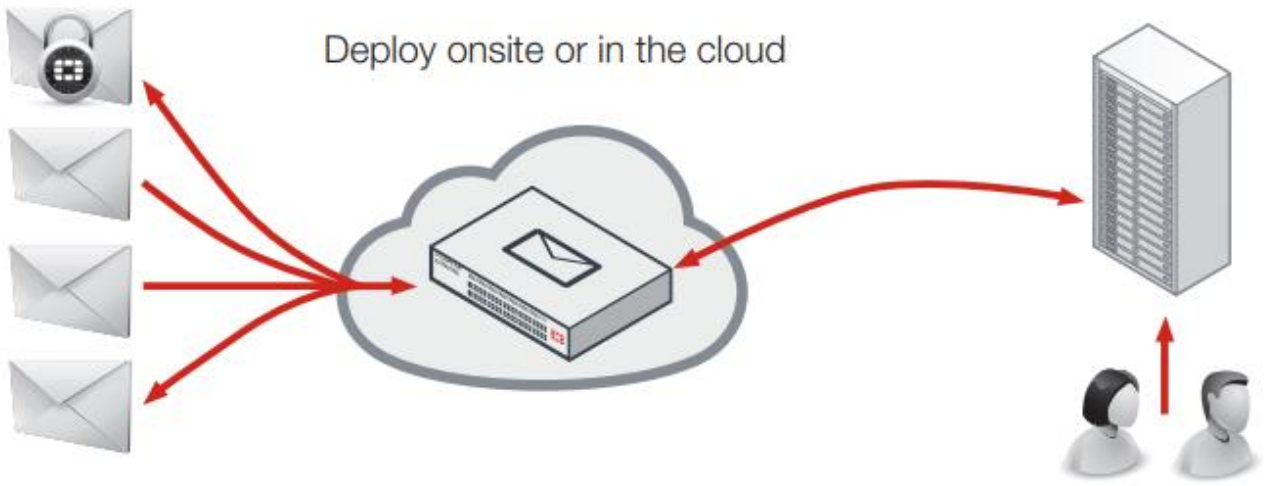

Рис. 2.4. Розгортання на робочому місці або в хмарі

Розглянемо прозорий режим (Transparent Mode) (рис. 2.5). Кожен мережевий інтерфейс включає в себе проксі-сервер, який отримує і надсилає корпоративну електронну пошту. Кожен проксі-сервер може перехоплювати сеанси SMTP (простий протокол передачі пошти), навіть якщо цільової IP-адреса не належить до FortiMail. FortiMail сканує повідомлення на наявність вірусів і спаму, а потім відправляє електронну пошту на цільової сервер електронної пошти для доставки. У цьому випадку відпадає необхідність зміни записи DNS MX або зміни існуючої конфігурації мережі сервера електронної пошти.

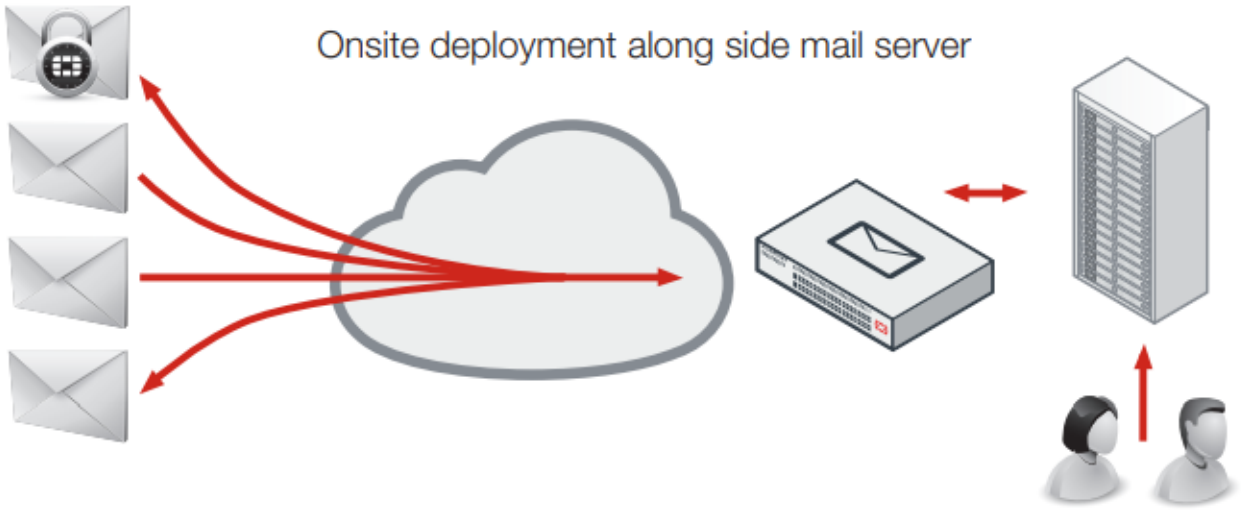

Рис. 2.5. Розгортання на робочому місці поряд з сервером електронної пошти

Розглянемо режим сервера (Server Mode) (рис. 2.5). FortiMail функціонує як автономний сервер обміну повідомленнями з повною функціональністю SMTP-сервера електронної пошти, включаючи гнучку підтримку безпечного доступу до

протоколів POP3, IMAP і з додатком WebMail (веб-пошта). FortiMail сканує електронну пошту на наявність вірусів і спаму перед доставкою. У режимі сервера зовнішні агенти пересилання пошти (MTA) приєднуються до FortiMail, дозволяючи йому функціонувати як захищений сервер.

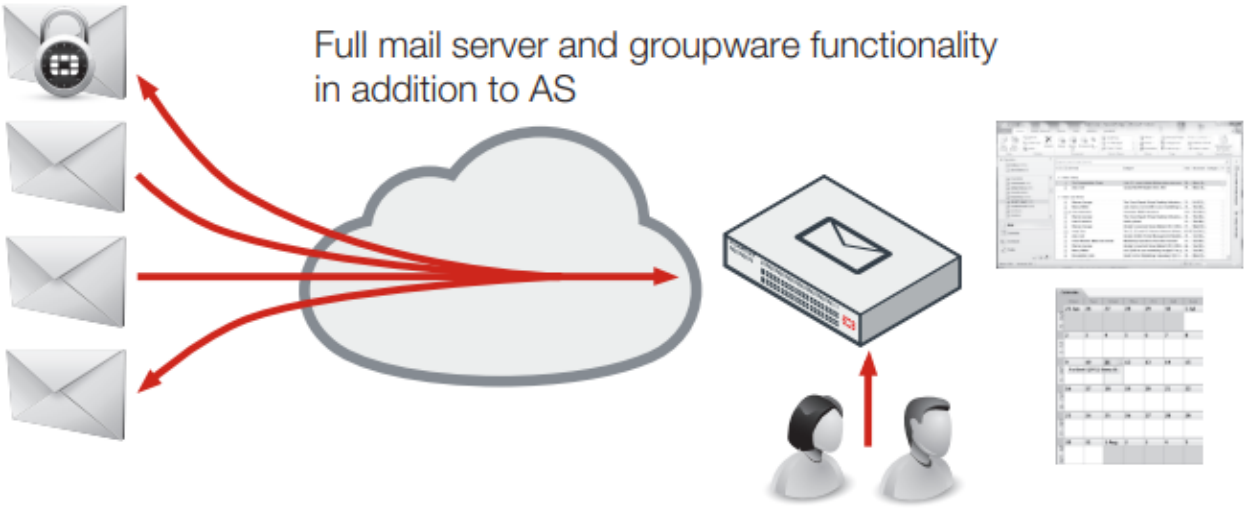

Рис. 2.6. Повна функціональність сервера електронної пошти і ПЗ для робочих груп на додаток до сервера автентифікації (AS)

Розглянемо інтеграцію з Microsoft 365 API: FortiMail можна розгорнути поза мережею, щоб спростити розгортання, тому не потрібно змінювати записи MX, а використовувати рідний API Microsoft 365 для забезпечення виявлення загроз та повернення повідомлень після доставки. Широка гнучкість можлива завдяки поверненню заявок на створення політик, що стосуються відповідності або унікальних бізнес-вимог, таких як побудова параметрів пошуку на основі ключових слів, імені файлу або типу вмісту. Ці можливості можуть слугувати потужним доповненням до власних функцій безпеки Microsoft, щоб підвищити загальну ефективність та зменшити ризик. Крім того, майбутні вдосконалення інтеграції API підтримуватимуть розширені можливості сканування поштової скриньки в режимі реального часу та внутрішньої пошти.

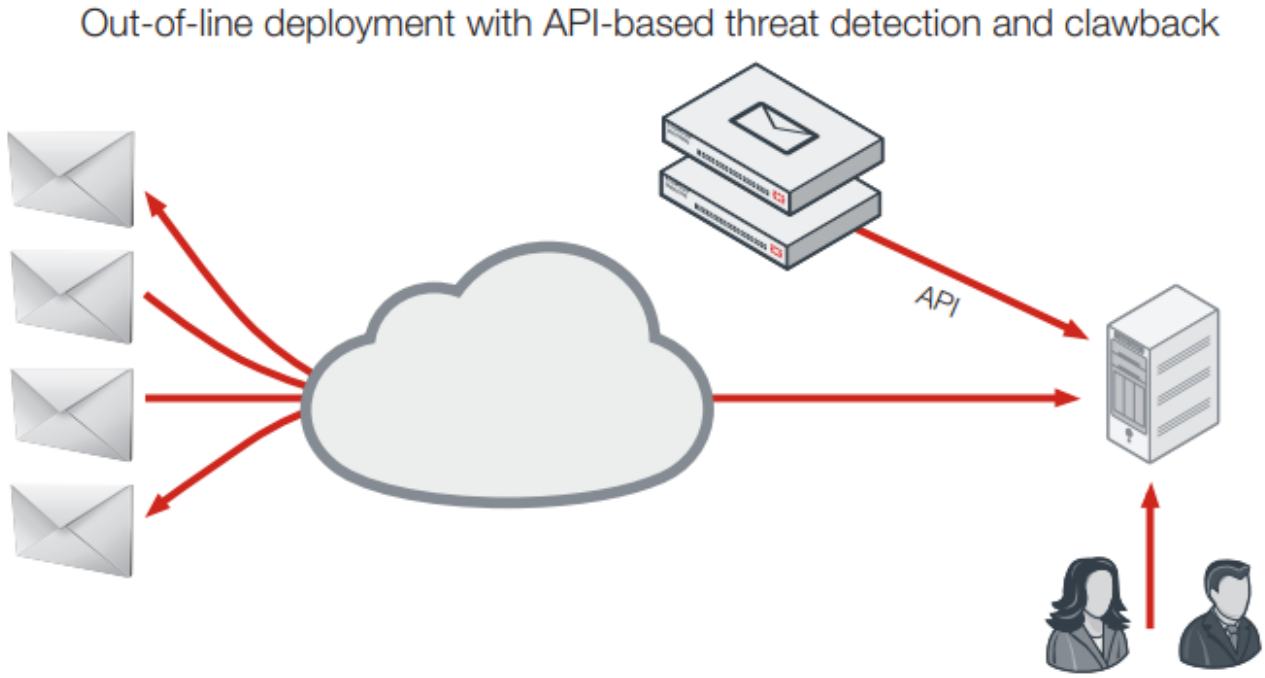

Рис. 2.7. Розгортання поза мережею з виявленням загрози та поверненням на основі API

Шифрування на основі ідентифікації (Identity-Based Encryption, IBE) дозволяє FortiMail доставляти електронну пошту з конфіденційною або піднаглядною інформацією в безпечному режимі, без необхідності використання додаткового апаратного забезпечення, надання ПЗ користувачеві або оплати додаткових ліцензій. Шифрування на основі ідентифікації (IBE) використовується для припинення паперового листування і зниження вартості.

Шифрування на основі політик. Автоматичне шифрування повідомлень відповідно контентом або одержувачем.

Технологія Push або Pull. Використання технології Push (дані формуються на сервері і доставляються клієнтові), Pull (запит проводиться клієнтом, відповідь породжується сервером) або їх комбінації відповідно до конкретних вимог.

Простота розгортання, використання та управління. Розгортання шифрування на основі ідентифікації в будь-якому режимі, в тому числі в прозорому режимі, без підготовки облікових записів користувача або без використання додаткового апаратного або програмного забезпечення.

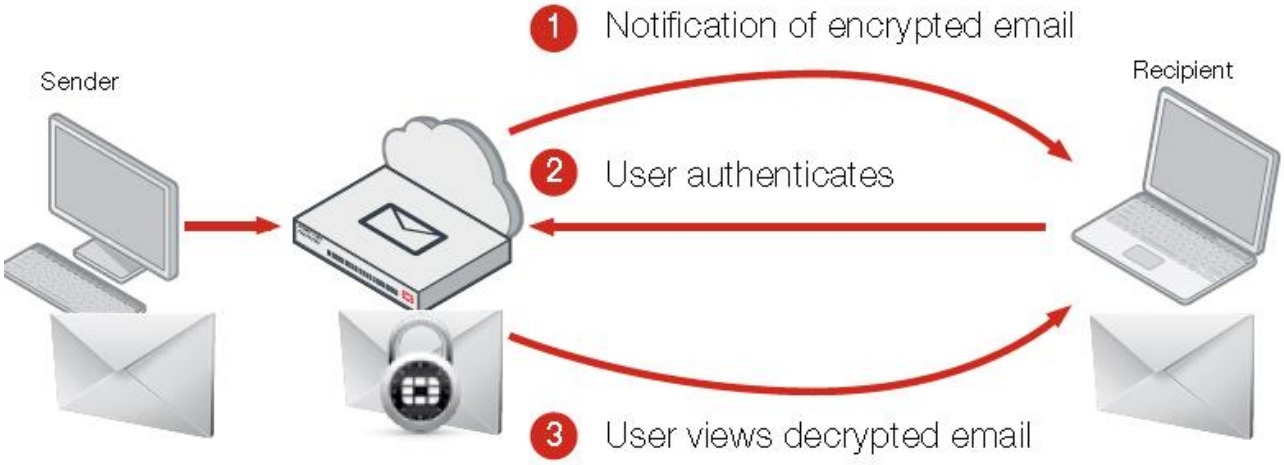

Рис. 2.8. Шифрування на основі ідентифікаційних даних (IBE)

3 ПОРЯДОК ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ

3.1. Рекомендації з планування і управління поштовими серверами

Найбільш важливим аспектом розгортання безпечного поштового сервера є ретельне планування перед установкою, налаштуванням і розгортанням. Ретельне планування забезпечить максимальну безпеку поштового сервера і відповідність всім відносним політикам організації. Багато проблем з безпекою і продуктивністю поштового сервера можуть бути пов'язані з відсутністю контролю планування або управління. Важливість управлінського контролю важко переоцінити. У багатьох організаціях структура підтримки інформаційних технологій сильно фрагментована. Ця фрагментація призводить до невідповідностей, які можуть призвести до вразливостей безпеки [1].

Безпеку поштового сервера слід враховувати на початковому етапі планування на початку життєвого циклу розробки системи, щоб максимізувати безпеку і мінімізувати витрати. Після впровадження і розгортання забезпечити безпеку набагато складніше і дорожче. Організації з більшою ймовірністю приймуть рішення про правильне і послідовне налаштування хостів, коли вони почнуть з розробки та використання докладного, добре продуманого плану розгортання. Розробка такого плану дозволяє організаціям приймати обґрунтовані рішення про компроміс між зручністю використання і продуктивністю, а також ризиками. План розгортання дозволяє організаціям підтримувати безпечні конфігурації і допомагає виявляти вразливості безпеки, які часто виявляються як відхилення від плану [1].

На етапах планування поштового сервера слід враховувати наступні моменти [1]:

визначте призначення поштового сервера та вимоги до нього: категорії інформації будуть зберігатися, оброблятися або передаватися через поштовий сервер; вимоги безпеки до цієї інформації; перелік послуг, які будуть надаватися

поштовим сервером (як правило, виділення хоста тільки в якості поштового сервера є найбільш безпечним варіантом) та вимоги безпеки для цих додаткових послуг; вимоги до безперервності поштових послуг, наприклад, зазначені в планах безперервності операцій і планах аварійного відновлення; визначення місця в мережі, де буде знаходитися поштовий сервер;

визначте мережеві служби, які будуть надаватися на поштовому сервері (на додаток до стандартних служб організації, що надаються кожним сервером для резервного копіювання, віддаленого адміністрування тощо), наприклад, надаються через стандартні протоколи електронної пошти (наприклад, SMTP, POP, IMAP) і пропрієтарні протоколи електронної пошти;

визначте програмне забезпечення мережевих служб, як клієнтське, так і серверне, яке буде встановлено на поштовому сервері і будь-яких інших серверах підтримки;

визначте користувачів або категорії користувачів поштового сервера і будь-яких вузлів підтримки, включаючи сервери, що забезпечують доступ до пошти через Інтернет;

визначте привілеї, які кожна категорія користувачів матиме на поштовому сервері і хостах підтримки;

визначте як буде управлятися поштовий сервер (наприклад, локально, віддалено з внутрішньої мережі, віддалено з зовнішніх мереж);

вирішіть чи будуть і як користувачі проходити автентифікацію і як будуть захищені дані автентифікації;

визначте будь-які вимоги до безпеки або конфіденційності для інформації, пов'язаної з адресою, такий як ім'я користувача, ідентифікаційні дані користувача і асоціація з організацією;

визначте як буде забезпечуватися відповідний доступ до інформаційних ресурсів;

визначте, які програми поштового сервера відповідають вимогам організації.

Розглянемо сервери, які можуть запропонувати більш високий рівень безпеки, хоча в деяких випадках і з меншою функціональністю.

Адміністраторам поштового сервера слід вибирати операційну систему, яка забезпечує наступні можливості [1]:

мінімальна схильність до вразливостей, які можуть бути виявлені у всіх операційних системах;

можливість обмежити дії адміністратора або кореневого рівня тільки авторизованими користувачами;

можливість заборонити доступ до інформації на сервері, крім тієї, яка повинна бути доступна;

можливість відключити непотрібні мережеві служби, які можуть бути вбудовані в операційну систему або серверне програмне забезпечення;

можливість реєструвати відповідні дії сервера для виявлення вторгнень та їх спроб.

Крім того, організаціям слід враховувати наявність навченого, досвідченого персоналу для адміністрування серверів і серверних продуктів. Багато організацій засвоїли важкий урок про те, що здатний і досвідчений адміністратор для одного типу операційного середовища автоматично не так ефективний для іншого [1].

З огляду на чутливий характер поштового сервера, вкрай важливо, щоб він розташовувався в зоні, що забезпечує безпечну фізичну середу. При плануванні розташування поштового сервера слід враховувати наступні моменти [1]:

надійний фізичний захист – наприклад, замки, доступ до кард-рідера, охорона і системи виявлення фізичних вторгнень (наприклад, датчики руху, камери) тощо;

контроль навколишнього середовища для підтримки необхідної вологості і температури;

резервне джерело живлення;

резервна ділянка за межами потенційної зони стихійного лиха.

Належні заходи управління мають вирішальне значення для роботи і обслуговування безпеки поштової сервера. Практика забезпечення безпеки тягне за собою ідентифікацію активів інформаційної системи організації, а також розробку, документування та впровадження політик, стандартів, процедур та настанов, що

забезпечують конфіденційність, цілісність і доступність ресурсів інформаційної системи [1].

Для забезпечення безпеки поштового сервера і підтримання мережевої інфраструктури організаціям слід застосовувати такі методи [1]:

політика безпеки інформаційної системи організації повинна визначати основні принципи і правила безпеки інформаційної системи, а також їх внутрішнє призначення. В політиці також слід вказати, хто в організації відповідає за певні галузі інформаційної безпеки (наприклад, впровадження, забезпечення дотримання, аудит, аналіз). Щоб політика була ефективною, вона повинна застосовуватися послідовно у всій організації. Як правило, IT-директор і вище керівництво несуть відповідальність за розробку політики безпеки організації;

конфігурація/контроль і управління змінами – процес управління модифікаціями системи, обладнання, мікропрограмами і програмним забезпеченням, що забезпечує достатню впевненість в тому, що система захищена від внесення неправильних модифікацій до, під час і після впровадження системи. Контроль конфігурації призводить до узгодженості з політикою безпеки інформаційної системи організації;

оцінка і управління ризиками – це процес аналізу та інтерпретації ризиків. Він включає визначення обсягу та методології оцінки, збір і аналіз даних, пов'язаних з ризиками, інтерпретацію результатів аналізу ризиків. Збір і аналіз даних про ризики вимагає виявлення активів, загроз, вразливостей, засобів захисту, наслідків та ймовірності успішної атаки. Управління ризиками – це процес вибору і впровадження засобів контролю для зниження ризику до рівня, прийнятного для організації;

стандартизовані конфігурації. Організації повинні розробити стандартизовані безпечні конфігурації для широко використовуваних операційних систем і додатків. Це надасть керівництво для поштових серверів і мережевих адміністраторів про те, як безпечно налаштувати свої системи і забезпечити узгодженість і відповідність політиці безпеки організації. Оскільки для компрометації мережі потрібно тільки один небезпечно налаштований хост,

організаціям зі значною кількістю хостів особливо рекомендується застосовувати цю рекомендацію;

поінформованість про безпеку і навчання. Програма навчання безпеки має вирішальне значення для загального стану безпеки в організації. Інформування користувачів і адміністраторів про їхні обов'язки щодо забезпечення безпеки та навчання правильним методам роботи допомагає їм змінити свою поведінку відповідно до кращих практик безпеки. Навчання також підтримує індивідуальну підзвітність, що є важливим методом підвищення безпеки інформаційної системи;

непередбачені обставини, безперервність операцій і планування аварійного відновлення. Плани на випадок непередбачених обставин, плани безперервності операцій і плани аварійного відновлення розробляються заздалегідь, щоб дозволити організації або підприємству підтримувати операції в разі збою;

сертифікація та акредитація. Сертифікація в контексті безпеки інформаційних систем означає, що система була проаналізована на предмет того, наскільки добре вона відповідає всім вимогам безпеки організації. Акредитація відбувається, коли керівництво організації погоджується з тим, що система відповідає вимогам безпеки організації.

Метою *планування безпеки системи* є поліпшення захисту ресурсів інформаційної системи [1].

Плани, що забезпечують адекватний захист інформаційних активів, вимагають, щоб менеджери і власники інформації, безпосередньо порушені і зацікавлені в інформації та/або можливості обробки, були переконані, що їх інформаційні активи адекватно захищені від втрати, неправомірного використання, несанкціонованого доступу або модифікації, недоступності і невиявлених дій [1].

Мета плану забезпечення безпеки системи – надати огляд вимог до безпеки та конфіденційності системи і описати існуючі або заплановані засоби управління для задоволення цих вимог. План забезпечення безпеки системи також визначає обов'язки і очікувану поведінку всіх осіб, що мають доступ до системи. План забезпечення безпеки системи слід розглядати як документацію структурованого процесу планування адекватного і рентабельного захисту системи [1].

Для державних організацій всі інформаційні системи повинні бути охоплені планом безпеки системи. Іншим організаціям також слід серйозно подумати про створення плану безпеки для кожної зі своїх систем. Власник інформаційної системи, як правило, є стороною, відповідальною за забезпечення розробки та підтримки плану безпеки, а також за розгортання і експлуатацію системи відповідно до узгоджених вимог безпеки.

Як правило, ефективний план забезпечення безпеки системи повинен включати наступне [1]:

системна ідентифікація. Перші розділи плану безпеки системи надають основну ідентифікаційну інформацію про систему. Вони містять загальну інформацію, таку як ключові точки дотику з системою, мета системи, рівень чутливості системи і середовище, в якому вона розгорнута;

елементи управління. У цьому розділі плану описуються заходи контролю (існуючі або плановані), які призначені для задоволення вимог захисту інформаційної системи.

Засоби управління діляться на три основні категорії – управлінський контроль, який зосереджений на управлінні системою комп'ютерної безпеки та управлінні ризиками для системи; операційні засоби контролю, які в основному реалізуються і виконуються людьми (на відміну від систем). Вони часто вимагають технічних або спеціалізованих знань і часто покладаються на управлінську діяльність, а також на технічний контроль; процедури контролю, які представляють собою механізми безпеки, які використовуються комп'ютерною системою.

Елементи управління можуть забезпечувати автоматичну захист від несанкціонованого доступу або неправомірного використання, полегшувати виявлення порушень безпеки і підтримувати вимоги безпеки для додатків і даних. Однак впровадження технічних засобів управління завжди вимагає значних експлуатаційних міркувань і має узгоджуватися з управлінням безпекою в організації.

Загальні принципи безпеки інформаційної системи

При вирішенні проблем безпеки поштового сервера рекомендується

пам'ятати про деякі загальні принципи інформаційної безпеки [1]:

простота – механізми безпеки (та інформаційні системи в цілому) повинні бути максимально простими. Складність лежить в основі багатьох проблем безпеки;

відмовостійкість – в разі збою система повинна вийти з ладу безпечним способом, при цьому засоби управління безпекою та налаштування залишаються в силі і застосовуються. Зазвичай краще втратити функціональність, ніж безпеку;

повне посередництво – замість надання прямого доступу до інформації слід використовувати посередників, що забезпечують дотримання політики доступу. Загальні приклади включають дозволи файлової системи, проксі, брандмауери і поштові шлюзи;

відкритий дизайн – безпека системи не повинна залежати від секретності реалізації або її компонентів;

поділ привілеїв – функції, наскільки це можливо, повинні бути розділені і забезпечувати максимально можливу деталізацію. Концепція може застосовуватися як до систем, так і до операторів/користувачів. Стосовно систем такі функції, як читання, редагування, запис і виконання, повинні бути окремими. Стосовно системних операторів і користувачів ролі повинні бути по можливості розділені. Наприклад, якщо дозволяють ресурси, роль системного адміністратора повинна бути відокремлена від ролі адміністратора безпеки;

найменші привілеї – цей принцип диктує, що кожній задачі, процесу або користувачеві надаються мінімальні права, необхідні для виконання своєї роботи. При послідовному застосуванні цього принципу, якщо задача, процес або користувач будуть скомпрометовані, обсяг збитку буде обмежений ресурсами, доступними скомпрометованому об'єкту;

психологічна прийнятність. Користувачі повинні розуміти необхідність безпеки. Це може бути забезпечено через навчання і освіту. Крім того, існуючі механізми безпеки повинні надавати користувачам розумні можливості, що забезпечують зручність використання, яке їм потрібно на щоденній основі. Якщо користувачі вважатимуть механізми безпеки занадто громіздкими, вони можуть

знайти способи їх обійти або скомпрометувати їх. Мета полягає не в тому, щоб послабити безпеку, щоб вона була зрозумілою і прийнятною, а в тому, щоб навчити і розробити механізми і політики безпеки, які будуть зручними і ефективними;

найменш поширений механізм – при наданні функції системі найкраще, щоб процес або послуга отримали деяку функцію, котрі дають ту ж функцію іншим частинам системи. Можливість доступу процесу поштового сервера до серверної базі даних, наприклад, не повинна також дозволяти іншим додаткам в системі звертатися до серверної бази даних;

глибокий захист – організації повинні розуміти, що єдиного механізму безпеки, як правило, недостатньо. Механізми безпеки (захисту) повинні бути багаторівневими, щоб компрометація одного механізму безпеки була недостатньою для компрометації хоста або мережі. Для безпеки інформаційних систем не існує «срібної кулі»;

фактор роботи. Організації повинні розуміти, що потрібно для злому функцій безпеки системи або мережі. Обсяг роботи, необхідний зловмиснику для злому системи або мережі, повинен перевищувати цінність, яку зловмисник отримає від успішного злому;

запис компрометації – записи і журнали повинні підтримуватися, щоб в разі компрометації докази атаки були доступні для організації. Ця інформація може допомогти в захисті мережі і хоста після злому, а також в ідентифікації методів і експлойтів, які використовуються зловмисником. Ця інформація може бути використана для кращого захисту хоста або мережі в майбутньому. Крім того, це може допомогти організаціям у виявленні та переслідуванні зловмисників.

Забезпечення безпеки операційної системи поштового сервера

Захист поштового сервера від злому включає посилення захисту базової операційної системи, додатків поштового сервера і мережі, щоб запобігти прямої атаку зловмисників на поштовий сервер [1].

Всі загальнодоступні поштові сервери працюють під управлінням універсальної операційної системи. Багато проблем безпеки можна уникнути, якщо правильно налаштувати операційні системи, що лежать в основі поштових серверів

[1].

Конфігурації обладнання та програмного забезпечення за замовчуванням зазвичай встановлюються виробниками, щоб підкреслити особливості, функції та простоту використання на шкоду безпеці. Оскільки виробники не обізнані про потреби кожної організації в безпеці, кожен адміністратор поштового сервера повинен налаштувати нові сервери, щоб відобразити вимоги безпеки своєї організації, і переналаштувати їх у міру зміни цих вимог. Рекомендовані тут методи розроблені, щоб допомогти адміністраторам поштових серверів налаштувати і розгорнути поштові сервери, які задовольняють вимогам безпеки їх організації. Адміністратори поштових серверів, що керують існуючими поштовими серверами, повинні підтвердити, що їх системи вирішують обговорювані проблеми [1].

Для забезпечення базової безпеки операційної системи необхідно виконати п'ять основних кроків [1]:

планування установки і розгортання операційної системи хоста і інших компонентів для поштового сервера;

виправлення і оновлення операційної системи хоста в міру необхідності;

посилення захисту та налаштування операційної системи хоста для адекватного забезпечення безпеки;

встановлення та налаштування додаткових заходів безпеки при необхідності;

тестування операційної системи хоста, щоб переконатися, що попередні чотири кроки адекватно вирішують всі проблеми безпеки.

Захист електронної пошти від шкідливих програм

Електронна пошта всі частіше використовується як засіб для відправки додадткових файлів у вигляді вкладень. Спочатку це не представляло особливої загрози безпеки, оскільки вкладення були в основному невеликими текстовими документами або фотографіями. У міру того як все більше організацій почали використовувати електронну пошту для повсякденної співпраці, розмір і типи вкладень електронної пошти збільшилися. Сьогодні багато таких повідомлень електронної пошти відправляються з вкладеннями, такими як виконувані файли програм, зображення, музика тощо [1].

Багато видів шкідливих програм, включаючи віруси, черв'яки, троянські коні та шпигунське ПЗ (шкідливе ПЗ, призначене для порушення конфіденційності користувача) часто передаються у вкладеннях. Все частіше зловмисники використовують електронну пошту для проведення атак нульового дня на цільові організації до того, як про ці вразливості стане відомо публічно. Ці атаки часто націлені на офісне програмне забезпечення та дають зловмисникові контроль над робочими станціями користувачів. Цей елемент управління може використовуватися для підвищення привілеїв, отримання доступу до конфіденційної інформації, відстеження дій користувачів (наприклад, натискань клавіш) і виконання інших шкідливих дій [1].

Визначення того, чи дозволяти певні типи вкладень може бути важким рішенням для організації. Заборона будь-яких вкладень спростить систему і зробить її більш безпечною, однак це різко знизить його корисність і користувачі можуть використовувати прийоми кодування, щоб обійти обмеження, щоб «виконати свою роботу». В кінцевому підсумку організації вважають за краще дозволити хоча б деякі вкладення до електронних листів [1].

Організації повинні визначити, які типи вкладень дозволити. Найпростіший підхід – дозволити всі типи вкладень. Якщо це так, то на шляху проходження пошти слід встановити якийсь сканер шкідливих програм (наприклад, антивірусне програмне забезпечення, анти-шпигунське програмне забезпечення), щоб відфільтрувати відомі шкідливі програми і, можливо, навіть деяку утиліту блокування поведінки, встановлену на клієнті. щоб запобігти будь-які небажані операції з виконуваними вкладеннями [1].

Кращим підходом є фільтрація потенційно небезпечних типів вкладень (наприклад, файлів з розширеннями .vbs, .ws, .wsc) на поштовому сервері або поштовому шлюзі при одночасному скануванні на наявність шкідливих програм дозволених типів файлів. Хоча фільтрація таких розширень є хорошим першим кроком, її ефективність обмежена, оскільки зловмисники можуть змінювати розширення. Замість того, щоб просто перевіряти розширення, при фільтрації слід перевіряти заголовок, нижній колонтитул або інші ідентифікуючі аспекти файлу,

якщо це можливо, щоб ідентифікувати вкладення [1].

Організації можуть також мати бажання розглянути можливість установки різних правил для електронної пошти внутрішнього і зовнішнього походження або довірених і ненадійних організацій (наприклад, довірених доменів .gov/.mil), хоча цей останній варіант може бути підробленою адресою електронної пошти.

Фільтрація вкладень не буде повністю ефективною, якщо не заблоковані всі вкладення, а це неможливо. Деякі з найбільш корисних типів вкладень, наприклад, з офісних пакетів для підвищення продуктивності, також є одними з найбільш ризикованих. Крім того, витончені зловмисники можуть різними способами приховати справжню природу своїх шкідливих вкладень. Наприклад, зловмисники іноді відправляють електронні листи, що містять гіперпосилання на шкідливий файл на віддаленому веб-сайті. Якщо користувач натискає на гіперпосилання і воно використовує HTTPS замість HTTP, шкідливий файл буде завантажений, поки захищений HTTPS, що приховає його від виявлення засобами контролю мережевої безпеки [1].

Організації можуть фільтрувати активні гіперпосилання в повідомленнях електронної пошти, щоб запобігти цьому, але це знизить зручність використання повідомлень електронної пошти для користувачів. Крім того, організація може вважати бажаним, щоб користувачі поміщали гіперпосилання на файли в свої повідомлення електронної пошти замість того, щоб прикріплювати файли до своїх повідомлень, оскільки це знижує навантаження на поштові сервери.

Організаціям також слід розглянути можливість обмеження максимально допустимого розміру вкладень електронної пошти. Це приносить користь поштових серверів декількома способами, включаючи зменшення затримки черги пошти, вимог до сховища і вимог до процесора сервера. Поєднання цих переваг знижує ймовірність успішної атаки відмови в обслуговуванні, викликаної потоком повідомлень великого розміру. Однак установка низького максимального розміру для вкладень може ненавмисно привести до блокування легітимного вмісту, що знизить зручність використання і цінність поштової системи [1].

Шифрування електронної пошти, як правило, робить фільтрацію складнішою

або неефективною. Після того, як повідомлення зашифровано, фільтрація на поштовому сервері та/або периферійних пристроях стає неефективною, якщо вони не можуть розшифрувати повідомлення, відсканувати його і повторно зашифрувати. Це проблематично через величезні вимоги до продуктивності. Конфіденційність і інші проблеми з такого роду рішенням також існують. Взагалі кажучи, якщо шифрування використовується широко, тоді фільтрація повинна відбуватися в кінцевій точці (робоча станція користувача поштового клієнта), яку можна обійти [1].

Ще один вектор поширення шкідливих програм по електронній пошті, який часто не береться до уваги, – це особисті поштові акаунти, доступ до яких здійснюється через веб-браузери. Організаціям необхідно визначити, чи доречний доступ до особистих поштових облікових записів з комп'ютерів організації, і якщо так, то вжити заходів, щоб користувачі не піддавали ризику активи організації при доступі до своїх особистих облікових записів.

Крім вкладень до електронних листів, шкідливі програми можуть передаватися по електронній пошті іншими способами. Наприклад, багато поштових клієнтів підтримують повідомлення в форматі HTML. Ці повідомлення часто містять активний вміст у вигляді клієнтської мови сценаріїв або керуючих об'єктів, які можуть вплинути на клієнта. Найпопулярнішими типами активного вмісту є ActiveX, Java, JavaScript і Visual Basic Script (VBScript) [1].

Організації повинні визначити, чи слід дозволяти або блокувати активний вміст або форми активного вмісту в повідомленнях електронної почти. Повідомлення на основі HTML також часто містять інший небажаний вміст, такий як спам-повідомлення і спроби фішінга. Під фішингом розуміється використання оманливих комп'ютерів, засновані на засобах обману для розкриття конфіденційної особистої інформації. Наприклад, зловмисник може відправити жертвам повідомлення електронної пошти, яке виглядає так, як якщо б воно було відправлено від відомої організації, такий як онлайн-бізнес, компанія, що випускає кредитні карти або фінансова установа. Електронний лист призначений для того, щоб обманним шляхом змусити користувачів відповісти на електронний лист і

розкрити особисті дані [1].

Якщо на поштовому сервері не встановлено програмне забезпечення для сканування шкідливих програм (наприклад, антивірусне програмне забезпечення, анти-шпигунське програмне забезпечення) або програмне забезпечення неефективно, потенційна загроза безпеки, створювана шкідливими програмами, зростає для кінцевих користувачів. Деякі популярні поштові клієнти мають конфігурації за замовчуванням, які використовуються шкідливими програмами для зараження клієнтських хостів і передачі шкідливих програм іншим користувачам [1].

Крім розгортання і налаштування технологій захисту, організація повинна також проводити навчання та інформаційні заходи для користувачів, особливо для віддалених співробітників, які використовують комп'ютери поза контролем організації, щоб користувачі могли краще розпізнавати шкідливі повідомлення електронної пошти та вкладення і обробляти їх належним чином.

3.2. Рекомендації щодо захисту корпоративної електронної пошти

Наступні основні рекомендації рекомендуються організаціям та підприємствам для підтримки безпеки поштового сервера на основі [1].

Організації повинні ретельно планувати і враховувати аспекти безпеки розгортання поштового сервера.

Оскільки після розгортання і впровадження забезпечити безпеку набагато складніше, безпеку слід враховувати на початковому етапі планування. Організації з більшою ймовірністю приймуть рішення про правильну і послідовної налаштування комп’ютерів, якщо вони розроблять і використовують детальний, добре продуманий план розгортання. Розробка такого плану допоможе адміністраторам поштових серверів прийняти неминучий компроміс між зручністю використання, продуктивністю і ризиками.

Організації часто не приймають до уваги потреби в людських ресурсах як на етапах розгортання, так і на етапах експлуатації поштового сервера і допоміжної інфраструктури. Організації повинні враховувати наступні моменти в плані

розгортання:

типи необхідного персоналу (наприклад, системні адміністратори і поштові сервери, мережеві адміністратори, співробітники служби безпеки інформаційних систем);

навички та навчання, необхідні призначеному персоналу;

наявність персоналу.

При обслуговуванні та експлуатації захищеного поштового сервера організаціям слід впровадити відповідні методи і засоби управління безпекою.

Відповідні методи управління необхідні для роботи і обслуговування безпечної поштової сервера.

Практика забезпечення безпеки тягне за собою ідентифікацію активів інформаційної системи організації, а також розробку, документування та впровадження політик, стандартів, процедур та настанов, які допомагають забезпечити конфіденційність, цілісність і доступність ресурсів інформаційної системи.

Щоб забезпечити безпеку поштового сервера і підтримуваної мережевої інфраструктури, необхідно реалізувати наступні методи:

політика безпеки інформаційної системи в масштабах всієї організації;

конфігурація/контроль і управління змінами;

оцінка і управління ризиками;

стандартизовані конфігурації програмного забезпечення, відповідні політиці безпеки інформаційної системи;

поінформованість про безпеку і навчання;

планування непередбачених обставин, безперервності операцій і аварійного відновлення;

сертифікація та акредитація.

Організації повинні гарантувати, що операційна система поштового сервера розгорнута, налаштована і управляється відповідно до вимог безпеки організації.

Першим кроком у захисті поштового сервера є захист базової операційної системи. Найчастіше доступні поштові сервери працюють під управлінням

операційної системи загального призначення. Багато проблем безпеки можна уникнути, якщо правильно налаштувати операційні системи, що лежать в основі поштових серверів.

Конфігурації обладнання та програмного забезпечення за замовчуванням зазвичай встановлюються виробниками, щоб підкреслити особливості, функції та простоту використання на шкоду безпеці. Оскільки виробники не обізнані про потреби кожної організації в області безпеки, кожен адміністратор поштового сервера повинен налаштувати нові сервери, щоб відобразити вимоги безпеки своєї організації, і переналаштувати їх у міру зміни цих вимог. Використання посібників з налаштування безпеки або контрольних списків може допомогти адміністраторам забезпечити послідовну і ефективну захист систем. Захист операційної системи зазвичай включає наступні кроки:

встановлення патчів і оновлення операційної системи;

видалення або вимкнення непотрібних сервісів і додатків;

налаштування автентифікації користувачів операційної системи;

налаштування управління ресурсами;

установка і настройка додаткових заходів безпеки при необхідності;

виконання тестів безпеки в операційній системі.

Організації повинні гарантувати, що додаток поштового сервера розгорнуто, налаштоване і управляється відповідно до вимог безпеки організації.

Багато в чому безпечна установка і настройка програми поштового сервера відображає процес операційної системи, описаний вище. Загальний принцип, як і раніше, полягає в установці мінімальної необхідної кількості служб поштового сервера і усунення будь-яких відомих вразливостей за допомогою виправлень або оновлень. Якщо програма установки встановлює будь-які непотрібні додатки, служби або сценарії, їх слід видалити відразу після завершення процесу установки.

Захист додатку поштового сервера зазвичай включає наступні кроки:

виправіть і обновіть додаток поштового сервера;

видаліть або вимкніть непотрібні служби, додатки та зразки вмісту;

налаштуйте автентифікацію користувачів поштового сервера і контроль

доступу;

налаштуйте елементи управління ресурсами поштового сервера;

перевірте безпеку додатку поштового сервера.

Організації повинні розглянути можливість впровадження криптографічних технологій для захисту автентифікації користувачів і даних електронної пошти.

Більшість стандартних протоколів електронної пошти за замовчуванням використовують незашифровану автентифікацію користувача і відправляють дані електронної пошти в незашифрованому вигляді. Відправлення цих даних у відкритому вигляді може дозволити зловмиснику легко зламати обліковий запис користувача та/або перехопити і змінити незашифровані електронні листи. Як мінімум, більшості організацій слід зашифрувати сеанс автентифікації користувача, навіть якщо вони не шифрують самі дані електронної пошти. Зашифрована автентифікація користувачів тепер підтримується більшістю стандартних і пропрієтарних протоколів поштових скриньок.

Проблеми, пов'язані з зашифрованими і підписаними даними електронної пошти, більш складні. Шифрування і підпис електронної пошти створюють велике навантаження на мережеву інфраструктуру організації, можуть ускладнити сканування шкідливих програм і фільтрацію вмісту електронної пошти і часто вимагають значних адміністративних витрат. Однак для багатьох організацій переваги шифрування електронної пошти і підписів переважують витрати.

Організації повинні використовувати свою мережеву інфраструктуру для захисту своїх поштових серверів.

Мережева інфраструктура (наприклад, брандмауери, маршрутизатори, системи виявлення вторгнень), що підтримує поштовий сервер, грає критично важливу роль у безпеці поштового сервера. У більшості конфігурацій мережева інфраструктура буде першою лінією захисту між Інтернетом і поштовим сервером. Однак сама по собі конструкція мережі не може захистити поштовий сервер. Частота, витонченість і різноманітність атак на поштовий сервер, що здійснюються сьогодні, підтверджують ідею про те, що безпека поштового сервера повинна бути реалізована за допомогою багаторівневих і різноманітних механізмів захисту.

Організації повинні гарантувати, що поштові клієнти розгорнуті, налаштовані і використовуються належним чином відповідно до вимог безпеки організації.

Багато в чому клієнтська сторона електронної пошти являє більший ризик для безпеки ніж поштовий сервер.

Щоб забезпечити належний рівень безпеки для поштових клієнтів, необхідно ретельно розглянути і вирішити безліч проблем. Безпечна установка, настройка і використання поштових клієнтських додатків зазвичай включає наступні кроки:

встановити патчі і оновлення поштової клієнтської програми;

налаштувати функції безпеки поштового клієнта, такі як відключення автоматичного відкриття повідомлень і включення функцій захисту від спаму і фішингу;

налаштувати автентифікацію і доступ до поштової скриньки;

налаштувати захист операційної системи клієнтського хоста.

Треба розуміти, що збереження безпеки поштового сервера є безперервним процесом. Підтримка безпеки поштового сервера вимагає від організації постійних зусиль, ресурсів і пильності. Щоденне адміністрування безпеки поштового сервера є важливим аспектом. Забезпечення безпеки поштового сервера зазвичай включає наступні кроки:

налаштування, захист і аналіз файлів журналів;

часте резервне копіювання даних;

захист від шкідливих програм (наприклад, вірусів, хробаків, троянських коней);

встановлення та дотримання процедур відновлення після компрометації;

своєчасне тестування і застосування патчів;

періодична перевірка безпеки.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми захисту корпоративної електронної пошти. Постійно спостерігається зростаюча тенденція до атак, які направлені на компрометацію корпоративної електронної пошти, коли зловмисник або захоплює, або ретельно імітує (підробляє) законний обліковий запис електронної пошти, щоб більш ефективно застосовувати соціальну інженерію в шахрайських діях та фінансових операціях. За оцінками фахівців, у 2020 році компрометація ділової електронної пошти була поширена у всіх галузях і розмірах бізнесу. Тому, постає проблема захисту корпоративної електронної пошту, так як основний об'єм документів пересилається через неї. При цьому треба закупляти, розгортати та застосовувати сучасні методи та засоби захисту корпоративної електронної пошти.

Проаналізовано існуючі загрози корпоративній електронній пошті. Атаки BEC стають все більш витонченими. Крім соціальної інженерії, дослідники безпеки відстежували експоненціальне зростання використання масових шкідливих програм (клавіатурних шпигунів і RAT) і фішингових методів серед учасників BEC в період з 2014 по 2020 рік, що свідчить про подальший розвиток TTP (Tactics, Techniques and Procedures) BEC для підвищення стійкості і масштабування можливостей крадіжки облікових даних.

Визначено зміст проблеми захисту корпоративної електронної пошти. Безпека електронної пошти повинна бути головним пріоритетом для будь-якої компанії. Тому першою лінією захисту повинен бути шлюз електронної пошти – платформа, яка захищає електронні листи від хакерів, спаму та вірусів.

Проаналізовано існуючі методи та засоби захисту корпоративної електронної пошти. FortiMail – високорейтинговий шлюз захисту електронної пошти, який використовується для протидії просунутим таргетованим кіберзагрозам, забезпечує захист від динамічних видів атак на підприємство, запобігає втраті конфіденційної інформації і сприяє дотриманню норм і правил. Високопродуктивні

фізичні та віртуальні пристрої можуть бути розгорнуті на робочому місці або в загальнодоступному хмарному сервісі. Вони призначені для будь-яких організацій – від підприємств малого бізнесу до операторів зв'язку, провайдерів послуг і великих підприємств.

Рішення FortiMail є потужним засобом захисту від спаму і шкідливих програм та включає в себе такі передові технології як протидія поширенню вірусів, знешкодження та реконструкція контенту, аналіз за допомогою технології «пісочниця», захист від імперсонації та інші технології для запобігання небажаної масової розсилки, атаки з метою вимагання викупу, компрометації корпоративної електронної пошти і націлених атак тощо.

Розроблено рекомендації керівникам підприємств та фахівцям з кібербезпеки щодо захисту корпоративної електронної пошти. Рекомендації направлені на забезпечення якісного планування і управління поштовими серверами та їх захистом, а також на ефективний захист корпоративної електронної пошти та суворе дотримання вимог з безпеки.

Таким чином, запропоновані в роботі рекомендації мають сприяти ефективному створенню та функціонуванню системи захисту корпоративної електронної пошти.

ПЕРЕЛІК ПОСИЛАНЬ

1. Guidelines on Electronic Mail Security. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-45 Version 2. Miles Tracy, Wayne Jansen, Karen Scarfone, Jason Butterfield – 139 p. [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-45/version-2/final.

2. Cyber Threats 2020: A Year in Retrospect. PwC [Електронний ресурс] – Режим доступу: https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf.

3. Joel Witts. The Top 11 Email Security Gateways. Expert Insights / Mar 01, 2021 [Електронний ресурс] – Режим доступу: https://expertinsights.com/insights/top-11-email-security-gateways/.

4. Protect digital business with a unique email security approach. Fortinet [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protect-digital-business-with-a-unique-email-security-approach.pdf.

5. SpamTitan Gateway [Електронний ресурс] – Режим доступу: https://cee.bakotech.com/product/spamtitan-gateway/.

6. Jeremy Fuchs. One Minute is One Minute Too Late When It Comes to Malicious Emails. December 14, 2020 [Електронний ресурс] – Режим доступу: https://www.avanan.com/blog/one-minute-is-one-minute-too-late-when-it-comes-to-malicious-emails.

7. Proofpoint Essentials Professional Package. Data Sheet [Електронний ресурс] – Режим доступу: https://www.proofpoint.com/sites/default/files/pfpt-uk-ds-essentials-professional-package.pdf.

8. FortiMail. Data Sheet [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiMail.pdf.

9. Administration Guide FortiMail 6.4.4 [Електронний ресурс] – Режим доступу: https://docs.fortinet.com/document/fortimail/6.4.4/administration-guide/245732/fortimail-operation-modes.

10. Дяченко Максим Миколайович. Технологія захисту корпоративної електронної пошти на базі FortiMail. ВСЕУКРАЇНСЬКА НАУКОВА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ». Державний Університет Телекомунікацій. 27 жовтня 2021. Тези доповідей. С. 75, 76. http://www.dut.edu.ua/uploads/p_2099_79407917.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)