ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТАЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту корпоративної пошти на прикладі Barracuda Email Security Gateway»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

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

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

_____ Роман СУБОТЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62
СУБОТЕНКО Роман
(прізвище, ім'я)

Керівник к.держ.у. СКИБУН Олександр
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СУІБ – Система управління інформаційною безпекою

УЕП – Удосконалений електронний підпис

AES – Advanced Encryption Standard (Розширений стандарт шифрування)

AI – Artificial Intelligence (Штучний інтелект)

API – Application Programming Interface (Інтерфейс прикладного програмування)

ATO – Account Takeover (Захоплення облікового запису)

ATP – Advanced Threat Protection (Розширений захист від загроз)

BEC – Business Email Compromise (Компрометація ділової електронної пошти)

BESG – Barracuda Email Security Gateway (Шлюз безпеки електронної пошти Barracuda)

BIMI – Brand Indicators for Message Identification (Індикатори бренду для ідентифікації повідомлень)

BRBL – Barracuda Reputation Block List (Список блокування репутації Barracuda)

BRTS – Barracuda Real-Time System (Система реального часу Barracuda)

CPL – Cloud Protection Layer (Хмарний рівень захисту)

DDOS – Distributed Denial of Service (Розподілена відмова в обслуговуванні)

DKIM – DomainKeys Identified Mail (Ідентифікована пошта DomainKeys)

DLP – Data Loss Prevention (Запобігання витоку даних)

DMARC – Domain-based Message Authentication, Reporting and Conformance (Аутентифікація, звітність та відповідність повідомлень на основі домену)

DMZ – Demilitarized Zone (Демілітаризована зона)

DNS – Domain Name System (Система доменних імен)

DoS – Denial of Service (Відмова в обслуговуванні)

ESMTP – Extended Simple Mail Transfer Protocol (Розширений SMTP)

GDPR – General Data Protection Regulation (Загальний регламент про захист даних)

HIPAA – Health Insurance Portability and Accountability Act (Закон США про мобільність та підзвітність медичного страхування)

IEC – International Electrotechnical Commission (Міжнародна електротехнічна комісія)

IMAP – Internet Message Access Protocol (Протокол доступу до інтернет-повідомлень)

IP – Internet Protocol (Інтернет-протокол)

ISO – International Organization for Standardization (Міжнародна організація зі стандартизації)

LDAP – Lightweight Directory Access Protocol (Спрощений протокол доступу до каталогів)

MAPI – Messaging Application Programming Interface (Інтерфейс програмування додатків для обміну повідомленнями)

MDA – Mail Delivery Agent (Агент доставки пошти)

MFA – Multi-Factor Authentication (Багатофакторна автентифікація)

MTA – Mail Transfer Agent (Агент пересилання пошти)

MUA – Mail User Agent (Поштовий користувацький агент)

MX – Mail Exchange (Запис обміну поштою)

NIST – National Institute of Standards and Technology (Національний інститут стандартів і технологій)

PAN – Primary Account Number (Основний номер рахунку)

PCI DSS – Payment Card Industry Data Security Standard (Стандарт безпеки даних індустрії платіжних карток)

POP (POP3) – Post Office Protocol (Протокол поштового відділення)

RBL – Real-time Blackhole List (Чорний список у реальному часі)

SEG – Secure Email Gateway (Шлюз безпеки електронної пошти)

SMTP – Simple Mail Transfer Protocol (Простий протокол передачі пошти)

SOC – Security Operations Center (Центр операцій з безпеки)

SPF – Sender Policy Framework (Структура політики відправника)

SSL – Secure Sockets Layer (Рівень захищених сокетів)

TLS – Transport Layer Security (Безпека транспортного рівня)

ВСТУП

Актуальність теми дослідження зумовлена тим, що корпоративна електронна пошта залишається одночасно одним з найважливіших бізнес-інструментів та однією з найвразливіших точок входу для кібератак у сучасній організації. Незважаючи на появу нових платформ для спільної роботи, електронна пошта зберігає свою критичну роль як основний канал для офіційної комунікації, ведення переговорів, укладання угод, фінансових операцій та обміну конфіденційною документацією. Ця її повсюдність та високий рівень довіри з боку користувачів перетворюють її на головну мішень для зловмисників.

Ландшафт загроз, пов'язаних з електронною поштою, за останні роки кардинально еволюціонував. Якщо раніше основною проблемою був лише масовий спам, то сьогодні організації стикаються зі складними, цілеспрямованими та фінансово руйнівними атаками. Статистика підтверджує критичність проблеми: до 94% всіх шкідливих програм доставляються саме через електронну пошту. Такі загрози, як компрометація ділової пошти (BEC), цільовий фішинг (spear-phishing) та атаки програм-вимагачів (Ransomware), стали повсякденною реальністю. Атаки BEC призводять до багатомільйонних фінансових втрат через шахрайські перекази коштів, тоді як програми-вимагачі, потрапляючи в мережу через одне шкідливе вкладення, здатні повністю паралізувати операційну діяльність компанії.

Водночас, актуальність проблеми посилюється не лише через технічні, але й через юридичні та регуляторні чинники. Електронна пошта є одним з найбільших репозиторіїв персональних даних (ПД) та комерційної таємниці в організації. Такі регуляції, як європейський GDPR та український Закон "Про захист персональних даних", покладають на організації пряму юридичну відповідальність за забезпечення конфіденційності та цілісності цієї інформації. Галузеві стандарти, як-от PCI DSS, категорично забороняють передачу певних типів даних (номерів платіжних карток) через незахищені канали, до яких належить і електронна пошта.

Ця комбінація факторів — критична важливість для бізнесу, еволюція загроз від простого спаму до складних атак нульового дня, та жорсткі регуляторні вимоги — створюють нагальну потребу в аналізі та впровадженні сучасних, багаторівневих технологій захисту корпоративної пошти. Традиційні антивірусні сканери та спам-фільтри вже нездатні забезпечити належний рівень безпеки. Тому дослідження архітектури, методів та засобів, які пропонують передові рішення, такі як Barracuda Email Security Gateway, є надзвичайно актуальною задачею для забезпечення кіберстійкості та захисту інформаційних активів будь-якої сучасної організаці, що дозволить організаціям забезпечити відповідність вимогам регуляторних органів щодо захисту персональних та корпоративних даних.

Об’єкт дослідження – захист корпоративної пошти організації.

Предмет дослідження – технологія захисту корпоративної пошти на прикладі Barracuda Email security gateway.

Мета роботи – розробка варіанту технології захисту корпоративної пошти на прикладі Barracuda Email security gateway.

Наукові завдання:

дослідити сутність проблеми захисту корпоративної електронної пошти;

проаналізувати основні загрози корпоративної електронної пошти;

проаналізувати підходи та існуючі технології захисту корпоративної електронної пошти;

проаналізувати методи та засоби захисту корпоративної пошти на прикладі Barracuda Email Security;

розробити рекомендації щодо застосування технологія захисту корпоративної пошти.

Методи дослідження: опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, практичне використання засобів захисту віддалених користувачів.

Практичне значення одержаних результатів: запропоновано рекомендації щодо захисту корпоративної пошти організації.

Апробація результатів.

Суботенко Р.Р. Підходи до захисту корпоративної пошти організації. актуальні проблеми кібербезпеки. *Актуальні проблеми кібербезпеки:* матеріали всеукраїнської наук.-практ. конф., м. Київ: ДУІКТ, 29 жовт. 2025р. Київ. С 39-40.

1 АНАЛІЗ ПРОБЛЕМИ БЕЗПЕКИ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ

1.1. Вступ до безпеки електронної пошти

Електронна пошта залишається основним каналом зв'язку для бізнесу в усьому світі, що робить її критичним вектором для кібератак. Незважаючи на зростання популярності альтернативних комунікаційних платформ, електронна пошта продовжує бути основою організаційної комунікації та основною мішенню для зловмисників, які прагнуть скомпрометувати системи, викрасти дані або проникнути в мережі. Тому, необхідно створювати теоретичні основи, практичні методи, інструменти та технології, необхідні для захисту систем електронної пошти від складних загроз. Це надає можливість фахівцям з безпеки знання, необхідні для створення надійних програм безпеки електронної пошти, які захищають від найпоширеніших та найнебезпечніших загроз на основі електронної пошти, з якими стикаються організації сьогодні [3, 14].

Електронна пошта продовжує залишатися основним інструментом бізнес-комунікації, незважаючи на поширення альтернативних платформ обміну повідомленнями. Її повсюдність та важливість роблять її головною мішенню для зловмисників.

Електронна пошта займає критичну роль в діловому спілкуванні в організаціях та залишається центральною частиною організаційної комунікації з кількох причин [3, 14]:

Бізнес-критичні комунікації

- переговори та угоди щодо контрактів;
- комунікація з клієнтами та постачальниками;
- внутрішні корпоративні оголошення;
- фінансові операції та схвалення;
- обмін документами та співпраця.

Обмін файлами та розповсюдження документів

– комунікації з управління проектами;
– координація та планування зустрічей;
– сповіщення та оновлення робочого процесу;
– послуги автентифікації та облікових записів.

Підтвердження реєстрації облікового запису

– механізми скидання пароля;
– доставка багатофакторної автентифікації;
– сповіщення та оповіщення про послуги;
– маркетинг та взаємодія з клієнтами.

Управління взаємовідносинами з клієнтами

– маркетингові кампанії та розсилки;
– взаємодія зі службою підтримки клієнтів;
– оновлення та оголошення про продукти.

Ця критично важлива роль робить безпеку електронної пошти першорядною для управління організаційними ризиками та забезпечення безперервності операційної діяльності [3].

1.2 Еволюція проблем безпеки електронної пошти

З появою різних типів загроз електронної пошти, можна виділити основні етапи безпеки електронної пошти, які значно змінилювались з моменту її появи [3]:

Ранні етапи безпеки електронної пошти (1990-ті-2000-ті роки)

– базова фільтрація спаму;
– просте антивірусне сканування;
– рудиментарна автентифікація;
– ранні фішингові атаки, спрямовані на споживачів.

Середній етап (2005-2015)

– більш складні методи фішингу;
– цільові фішингові атаки;

– розповсюдження шкідливого програмного забезпечення через вкладення;

– ранні впровадження SPF, DKIM та DMARC.

Сучасний стан (2015 – дотепер)

– передові тактики соціальної інженерії;

– витончений компрометаційний захист ділової електронної пошти (BEC);

– цілеспрямовані атаки з розширеною розвідкою;

– фішинговий контент, згенерований штучним інтелектом;

– багатоетапні ланцюжки атак, що починаються з електронної пошти;

– проблеми безпеки хмарної електронної пошти.

Ця еволюція продовжується, оскільки зловмисники адаптуються до нових засобів захисту та використовують новітні технології.

Розглянемо основні концепції та безпеку архітектури електронної пошти [4].

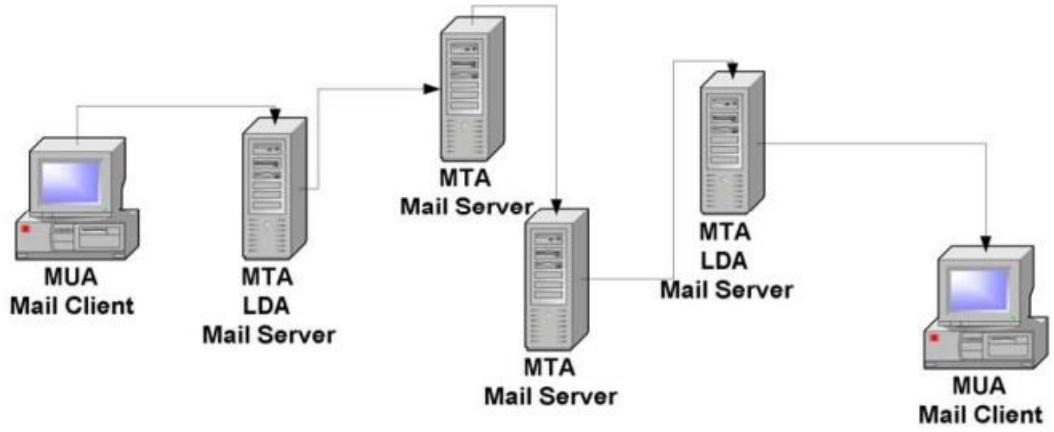

Рис.1.1. Архітектура та компоненти електронної пошти [4]

Розуміння архітектури електронної пошти є важливим для впровадження ефективної безпеки. Для аналізу цього питання розглянемо основні протоколи, компоненти та моделі безпеки, які складають основу безпеки електронної пошти.

Стандартні протоколи електронної пошти мають притаманні міркування безпеки:

Простий протокол передачі пошти (SMTP)

– спочатку розроблений без урахування безпеки;
– бракує вбудованих механізмів автентифікації;
– вразливий до перехоплення з'єднання без TLS;
– вразливий до підробки відправника та ретрансляційних атак;
– розширений SMTP (ESMTP) додає розширення безпеки.

Протокол поштового відділення (POP3)

– базова автентифікація часто використовує паролі у відкритому тексті;
– обмежена безпека сеансу без TLS;
– немає детального контролю доступу;
– обмежені можливості ведення журналу та аудиту.

Протокол доступу до інтернет-повідомлень (IMAP)

– більш складний, ніж POP3, але з подібними проблемами безпеки;
– кілька одночасних підключень збільшують поверхню атаки;
– спільний доступ до папок може призвести до несанкціонованого доступу;
– впровадження TLS є критично важливим для безпеки.

Розширення власних протоколів

– протокол MAPI Microsoft Exchange;
– власні протоколи Gmail від Google;
– розширені функції безпеки в сучасних реалізаціях;
– міркування безпеки, специфічні для постачальника.

Розуміння слабких місць протоколів допомагає визначити засоби контролю безпеки, необхідні для зменшення властивих їм вразливостей.

Компоненти інфраструктури доставки електронної пошти

Інфраструктура електронної пошти має кілька компонентів, що потребують контролю безпеки:

Агенти пересилання пошти (MTA)

– основні сервери, відповідальні за надсилання та отримання пошти;
– критичні вимоги до конфігурації безпеки;

– вразливий до DoS-атак та виснаження ресурсів;

– ключові цілі для початкового компромісу.

Агенти доставки пошти (MDA)

– обробка остаточної доставки до поштових скриньок користувачів;

– проблеми контролю доступу та автентифікації;

– потенціал для локального підвищення привілеїв;

– наслідки для безпеки зберігання даних.

Поштові користувацькі агенти (MUA)

– поштові клієнти, що використовуються для читання та написання повідомлень

– підлягає вразливостям на стороні клієнта;

– часто стають мішенню для крадіжки облікових даних;

– міркування безпеки плагінів;

Допоміжна інфраструктура

– DNS-сервіси для записів MX та маршрутизації електронної пошти;

– служби каталогів для автентифікації користувачів;

– сервіси сертифікації для впровадження TLS;

– балансувальники навантаження та проксі-сервіси.

Кожен компонент вимагає спеціальних заходів безпеки для створення комплексної системи безпеки.

Системи автентифікації електронної пошти допомагають перевірити легітимність відправника:

Структура політики відправника (SPF)

– механізм авторизації серверів-відправників на основі DNS;

– запобігає базовій підміні доменів відправників;

– проблеми впровадження переадресації та надсилання з кількох джерел;

– різні рівні забезпечення дотримання (відсутність, карантин, відхилення).

Ідентифікована пошта DomainKeys (DKIM)

– криптографічний підпис повідомлень;
– зберігає цілісність під час транспортування;
– ключові управлінські виклики;
– потрібна правильна конфігурація DNS.

Аутентифікація, звітність та відповідність повідомлень на основі домену (DMARC)

– створено на основі SPF та DKIM;
– забезпечує механізми зворотного зв'язку та звітності;
– визначає політики власника домену щодо обробки повідомлень;
– критично важливо для захисту репутації домену.

Індикатори бренду для ідентифікації повідомлень (BIMI)

Новий стандарт для візуальних індикаторів бренду;

Потрібна потужна реалізація DMARC;

Сертифікати перевіреної марки (VMC);

Підвищує захист бренду та довіру користувачів;

Впровадження цих фреймворків створює основу для надійного електронного спілкування.

1.2. Загрози безпеці корпоративної електронної пошти

У 2025 році корпоративна електронна пошта залишається однією з найпоширеніших цілей кібератак. Особливістю є те, що 94% усіх шкідливих програм доставляються саме через електронну пошту. Електронні листи є критично важливим інструментом для комунікації працівників організацій, тому вони становлять значні ризики для безпеки інформаційної системи організації. Зловмисники використовують складні методи для використання поштових систем, що призводить до фінансових втрат, витоків даних та шкоди репутації. Розуміння найпоширеніших загроз безпеці електронної пошти та впровадження безпечних методів роботи з електронною поштою є важливим для запобігання кібератак.

Незважаючи на численні передові практики кібербезпеки, електронна пошта все ще не є повністю захищенною. Системи електронної пошти можуть бути вразливими до широкого спектру атак, від фішингу до шкідливого програмного забезпечення, оскільки вони ніколи не були розроблені з урахуванням надійної безпеки. Без належного захисту електронні листи можуть бути перехоплені, змінені або використані для розповсюдження шкідливого контенту. Навіть із сучасними технологіями безпеки, такими як шифрування, зловмисники продовжують знаходити способи обходу захисту та атакувати користувачів за допомогою шкідливих електронних листів.

Електронна пошта слугує основним засобом комунікації як для бізнесу, так і для приватних осіб, що робить її цінною ціллю для кіберзлочинців. Незахищені системи електронної пошти можуть наражати будь-яку організацію на низку кіберзагроз , включаючи фішингові атаки, програми-вимагачі та витік даних . Це може призвести до втрати конфіденційної інформації, порушень відповідності вимогам, фінансової шкоди та значної шкоди репутації вашої компанії. Посилення безпеки електронної пошти допомагає забезпечити цілісність комунікацій та захищає бізнес від дороговартісних інцидентів.

З найбільш відомих загроз можна виділити сім 7 найбільших загроз безпеці електронної пошти організації у 2025 році [1].

1. Захоплення домену (кіберсквотинг)

Кіберсквотинг домену відбувається коли зловмисники реєструють доменні імена, що дуже схожі на легітимні, щоб обдурити користувачів (рис.1.2). Цей метод часто використовується для імітації довірених організацій та надсилання шахрайських електронних листів. Наприклад, зловмисник може зареєструвати домен, такий як "micosoft.com", щоб видавати себе за Microsoft та надсилати фішингові електронні листи нічого не підозрюючим одержувачам.

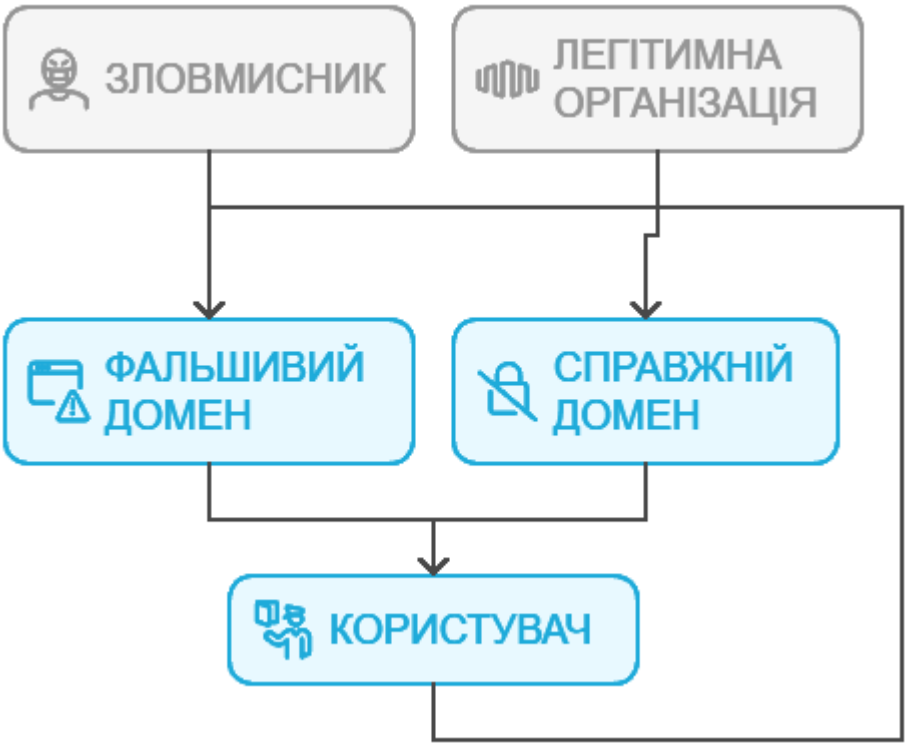

Рис. 1.2. Захоплення домену (кіберсквотинг)

Кіберсквотинг особливо небезпечний, оскільки він використовує довіру користувачів до знайомих доменів. Щойно користувачі вважають, що взаємодіють із законним джерелом, вони з більшою ймовірністю відкривають шкідливі вкладення або надають конфіденційну інформацію. Моніторинг підозрілих реєстрацій доменів та впровадження заходів захисту доменів можуть допомогти захиститися від цієї загрози.

2. Фішингові атаки

Фішингові атаки є однією з найпоширеніших загроз безпеці електронної пошти. Кіберзлочинці використовують фішингові електронні листи, щоб обманом змусити одержувачів розкрити особисту інформацію, перейти за шкідливими посиланнями або завантажити шкідливе програмне забезпечення. Ці атаки часто видають себе за відомі бренди або термінові повідомлення, щоб маніпулювати жертвами та змусити їх діяти без роздумів.

Оскільки методи фішингу стають дедалі складнішими, важливо підвищувати обізнаність у працівників організації виявляти фішинг та повідомляти

адміністратору про такі листи. Зловмисники тепер можуть використовувати кішинг — фішинг за допомогою QR-кодів — як і традиційні методи. Навчання співробітників розпізнаванню спроб фішингу та використання антифішингового програмного забезпечення є ключовими стратегіями запобігання кібератак.

3. Шкідливі вкладення

Шкідливі вкладення є серйозною проблемою для безпеки електронної пошти. Шкідливі вкладення можуть маскуватися під легітимні файли, такі як PDF-файли, документи Word або таблиці Excel. Після відкриття вони можуть встановлювати на пристрій користувача шкідливі програми, такі як трояни, програми-вимагачі або шпигунські програми, що ставить під загрозу конфіденційні дані та потенційно заражає всю мережу.

Організаціям слід впроваджувати інструменти, які сканують вхідні вкладення на наявність шкідливого контенту, та навчати співробітників про небезпеку відкриття небажаних вкладень.

4. Програми-вимагачі

Атаки програм-вимагачів продовжують зростати, а електронна пошта є одним із найпоширеніших векторів поширення цього руйнівного шкідливого програмного забезпечення (рис.1.3). Програма-вимагач шифрує файли жертви та вимагає викуп за їх розблокування. У багатьох випадках жертви втрачають критично важливі дані та стикаються з тривалим простоєм.

Рис.1.3. Вплив програм-вимагачів на роботу організації

Зростаюча частота та складність атак програм-вимагачів роблять їх значною загрозою для бізнесу будь-якого розміру. Захист від програм-вимагачів вимагає багаторівневого підходу, включаючи надійний захист електронної пошти, регулярне резервне копіювання та навчання співробітників.

У [2] зазначено найважливіші статистичні дані та тенденцій щодо шкідливого програмного забезпечення-вимагача, які підкреслюють масштаб та актуальність цієї кіберзагрози:

72% організацій повідомили про загальне зростання кіберризиків за останній рік, причому атака з використанням шкідливого програмного забезпечення з метою вимагання стала головною проблемою, згідно з «Global Cybersecurity Outlook 2025» [2].

Згідно з [2] зазначено, що 45% організацій визначили атаки з використанням шкідливого програмного забезпечення з метою викупу як свою основну кіберзагрозу.

Атаки з метою вимагання продовжують зростати в усьому світі, хоча й зі змінами в частоті та цілях. У 2024 році було зареєстровано понад 5400 атак шкідливого програмного забезпечення з метою вимагання на організації по всьому світу – на 11% більше, ніж у 2023 році. Незважаючи на репресії правоохоронних органів проти основних угруповань, що займаються атаками шкідливого програмного забезпечення з метою вимагання , екосистема була фрагментованою, а активні групи програм-вимагачів фактично зросли (95 груп у 2024 році, що на 40% більше , ніж у 2023 році) [2].

Фінансові збитки від шкідливого програмного забезпечення Ransom величезні та зростають. Загальна сума виплат викупу нещодавно досягла піку, а потім знизилася: жертви виплатили понад 1 мільярд доларів вимагачам, що займаються викупом шкідливих програм, у 2023 році [2].

Майже 63% вимог про викуп за минулий рік становили щонайменше 1 мільйон доларів , а близько 30% перевищували 5 мільйонів доларів.

В одній гучній справі хакери навіть вимагали 70 мільйонів доларів від підрядника компанії, що займається виробництвом напівпровідників (витік даних постачальника TSMC у 2023 році).

Ці цифри підкреслюють нагальну потребу в надійних заходах кібербезпеки для пом'якшення зростаючої загрози програм-вимагачів, які можуть бути за рахунок незахищенної корпоративної електронної пошти.

5. Компрометація ділової електронної пошти (Business Email Compromise - BEC)

Компрометація ділової електронної пошти (BEC) – це тип шахрайства, коли зловмисники видають себе за керівників або довірених партнерів, щоб обманом змусити співробітників переказати кошти або поділитися конфіденційною інформацією. Атаки BEC є вузько цілеспрямованими та часто не мають звичайних ознак фішингової атаки, таких як шкідливі посилання або вкладення.

Оскільки атаки BEC зазвичай добре досліджені та персоналізовані, їх може бути важко виявити. Працівників слід навчити перевіряти будь-які незвичайні запити на гроші або конфіденційну інформацію, особливо коли вони, здається, надходять від вищого керівництва.

6. Витік даних

Витік даних може статися, коли конфіденційна інформація випадково надсилається неправильному одержувачу або передається неавторизованим особам. Електронна пошта часто є причиною витоку даних, особливо коли співробітники не навчені належним методам обробки даних. У деяких випадках кіберзлочинці також можуть використовувати вразливості електронної пошти для крадіжки цінних даних.

Запобігання витокам даних вимагає дотримання суворих політик безпеки електронної пошти, включаючи шифрування конфіденційних листів та постійний моніторинг підозрілої активності.

7. Експлойти форматів файлів

Зловмисники часто використовують вразливості в популярних форматах файлів, таких як PDF-файли та документи Word, для розповсюдження шкідливого

програмного забезпечення. Ці файли можуть містити шкідливий код, який активується під час відкриття, що призводить до зараження пристрою або мережі користувача. Багато традиційних антивірусних рішень мають труднощі з виявленням цих загроз, особливо коли зловмисники використовують нові або модифіковані експлойти.

Підтримка програмного забезпечення в актуальному стані та обмеження типів вкладених файлів, дозволених у інформаційній системі електронної пошти, є важливими кроками для зменшення цього ризику.

Отже, визначена проблема загроз електронної пошти зумовлює визначити основні підходи, які дозволять організаціям захистити свої ресурси, недопустити витік конфіденційної інформації, що може призвести до компроментації організації.

1.3. Аналіз нормативного регулювання захисту корпоративної електронної пошти

Корпоративна електронна пошта є однією з найкритичніших IT-систем будь-якої організації. Вона слугує основним каналом ділової комунікації, засобом обміну документами (часто конфіденційними), точкою взаємодії з клієнтами та партнерами, а також, на жаль, головним вектором для кібератак (фішинг, програми-вимагачі, шахрайство).

Через це регуляторні вимоги до захисту пошти походять з трьох основних джерел:

Міжнародні стандарти (ISO/IEC). Добровільні стандарти та найкращі практики, які де-факто стали обов'язковими для ведення бізнесу на глобальному ринку (наприклад, серія ISO 27000).

Законодавство про захист даних. Юридично обов'язкові закони, що захищають персональні дані громадян (наприклад, GDPR в ЄС та відповідний закон в Україні).

Національні та галузеві стандарти. Специфічні вимоги, що регулюють захист інформації в окремих секторах (наприклад, банківський, державний) або для певних типів даних (наприклад, платіжні картки).

Розглянемо кожну з цих категорій детально.

Міжнародні стандарти (ISO/IEC)

Це фундаментальний рівень, що формує основу для побудови системи управління інформаційною безпекою (СУІБ) в організації. Електронна пошта є ключовим активом у будь-якій СУІБ.

ISO/IEC 27001:2022 - цей стандарт не дає прямих вказівок «налаштуйте свій поштовий шлюз так», але він вимагає від організації впровадження процесів для ідентифікації, оцінки та обробки ризиків інформаційної безпеки.

Як це стосується електронної пошти:

Оцінка ризиків (Risk Assessment): Організація зобов'язана ідентифікувати ризики, пов'язані з корпоративною поштою. Наприклад:

Ризик витоку конфіденційної інформації через несанкціонований доступ.

Ризик компрометації системи через фішинговий лист.

Ризик втрати даних (видалення важливих листів) через відсутність резервного копіювання.

Вибір засобів контролю (Controls): На основі оцінки ризиків організація обирає відповідні заходи безпеки, описані в Додатку А (Annex A) стандарту.

ISO/IEC 27002:2022 (Заходи контролю інформаційної безпеки) є каталогом найкращих практик для реалізації контролів, згаданих у ISO 27001. Він надає детальні рекомендації «що і як» робити. Для захисту пошти релевантними є десятки контролів, ось ключові з них:

Організаційні заходи (Organizational Controls):

A.5.15 «Контроль доступу» (Access Control). Впровадження політики, що чітко визначає, хто має доступ до поштових скриньок (особливо спільних або системних), і як цей доступ надається та відкликається.

A.5.16 «Управління ідентифікацією» (Identity Management). Забезпечення унікальності ідентифікаторів (логінів) для кожного користувача пошти.

A.5.17 «Управління автентифікацією» (Authentication Management): Вимога складних паролів та, що критично важливо, багатофакторної автентифікації (MFA) для доступу до пошти, особливо веб-доступу.

A.5.23 «Безпека інформації при використанні хмарних послуг» (Information security for use of cloud services): Якщо компанія використовує M365 або Google Workspace, цей контроль вимагає оцінки безпеки провайдера, чіткого розмежування відповідальності та належних налаштувань безпеки в хмарі.

A.6.7 «Навчання та обізнаність» (Security Awareness Training): Пряма вимога регулярно навчати персонал розпізнавати фішинг, соціальну інженерію та інші загрози, що надходять електронною поштою.

Технічні заходи (Technological Controls):

A.8.2 «Маркування інформації» (Information Classification): Впровадження систем (часто інтегрованих з поштою), які дозволяють або вимагають від користувачів маркувати листи як "Публічні", "Внутрішні", "Конфіденційні".

A.8.3 «Запобігання витоку даних» (Data Loss Prevention, DLP): Використання технічних засобів (наприклад, функціонал Barracuda, Proofpoint), які сканують вихідну пошту на наявність чутливих даних (номери карток, персональні дані, комерційна таємниця) та блокують їх відправку.

A.8.7 «Захист від шкідливого програмного забезпечення» (Protection against Malware): Це пряма вимога до поштових шлюзів. Система повинна сканувати всі вхідні та вихідні листи та вкладення на наявність вірусів, програм-вимагачів, шпигунського ПЗ тощо. Це включає «пісочницю» (sandboxing) для аналізу невідомих файлів.

A.8.23 «Веб-фільтрація2 (Web Filtering): Багато поштових шлюзів (включно з Barracuda) пропонують "заміну URL" (URL rewriting). Цей контроль вимагає перевірки всіх посилань у листах у момент натискання, щоб заблокувати перехід на фішингові або шкідливі сайти.

A.8.16 «Моніторинг активності» (Monitoring Activities): Вимога збирати та аналізувати журнали (логи) поштової системи для виявлення підозрілої активності (наприклад, вхід з нетипової геолокації, масова розсилка спаму зі скомпрометованого акаунта).

Міжнародні та регіональні закони (GDPR)

Це юридично обов'язковий рівень. Навіть якщо організація знаходиться в Україні, вона повинна дотримуватися цих норм, якщо вона обробляє персональні дані резидентів ЄС (наприклад, має клієнтів в Європі, продає товари онлайн громадянам ЄС).

GDPR не містить технічних специфікацій, але встановлює жорсткі вимоги до захисту персональних даних (ПД), а електронна пошта є одним з найбільших репозиторіїв ПД в компанії (імена, прізвища, контакти, резюме, обговорення клієнтів).

Ключові статті, що стосуються електронної пошти.

Стаття 5. Принципи обробки персональних даних:

Конфіденційність та цілісність: Вимагає обробляти ПД у спосіб, що «забезпечує належну безпеку... включаючи захист від несанкціонованої або незаконної обробки та від випадкової втрати, знищення або пошкодження, шляхом вжиття відповідних технічних та організаційних заходів». Це пряма вимога до захисту пошти.

Стаття 25. Захист даних «за задумом» та «за замовчуванням» (Data Protection by Design and by Default):

За задумом. Вимагає "вбудовувати" заходи безпеки в саму архітектуру поштової системи з самого початку, а не додавати їх потім. Наприклад, одразу планувати шифрування, MFA та DLP.

За замовчуванням. Вимагає, щоб за замовчуванням налаштування системи були максимально приватними.

Стаття 32. Безпека обробки:

Це ключова стаття. Вона зобов'язує контролера (організацію) впроваджувати технічні та організаційні заходи для забезпечення рівня безпеки, що відповідає ризику. Стаття прямо пропонує такі заходи:

«Псевдонімізація та шифрування персональних даних». Це стосується як шифрування листів (S/MIME), так і шифрування каналів (TLS) та сховищ.

«Здатність забезпечити постійну конфіденційність, цілісність, доступність і стійкість систем... обробки»: Це вимога до відмовостійкості поштових серверів та їх захисту від зломів.

«Здатність своєчасно відновлювати доступність і доступ до персональних даних у разі фізичного або технічного інциденту»: Це пряма вимога до резервного копіювання (backup) поштових скриньок та серверів.

«Процес регулярної перевірки, оцінки та оцінювання ефективності технічних і організаційних заходів...»: Вимога до регулярних аудитів, тестів на проникнення (pentest) та симуляцій фішингу.

Статті 33-34. Повідомлення про витік даних:

Якщо відбувається витік ПД (наприклад, злом поштового сервера, масова фішингова атака, що призвела до компрометації акаунтів), організація зобов'язана повідомити про це регулятора протягом 72 годин. Це вимагає наявності потужних систем моніторингу та виявлення інцидентів (Detection & Response).

Національне законодавство України

Цей рівень є обов'язковим для всіх організацій, що діють на території України. Він багато в чому гармонізований з європейськими підходами, але має свою специфіку, особливо щодо державних стандартів.

Закон України «Про захист персональних даних»

Це український аналог GDPR. Він встановлює загальні вимоги до обробки та захисту ПД. Корпоративна пошта є «базою персональних даних», оскільки містить ПД співробітників, клієнтів та контрагентів.

Стаття 24. Захист персональних даних Закон України «Про захист персональних даних»:

Зобов'язує власників баз ПД (організації) вживати «належних технічних та організаційних заходів для захисту» даних від незаконної обробки, втрати, знищення, а також від несанкціонованого доступу.

Це означає, що компанія несе юридичну відповідальність за злом пошти, якщо не зможе довести, що вжила належних заходів (MFA, антивірус, антиспам, шифрування).

Закон України «Про основні засади забезпечення кібербезпеки України»

Цей закон є рамковим і визначає загальну стратегію держави у сфері кібербезпеки.

Об'єкти критичної інфраструктури (ОКІ): Якщо організація належить до ОКІ (енергетика, транспорт, банки, охорона здоров'я), вона підпадає під посилене регулювання. Її поштова система вважається частиною «критичної інформаційної інфраструктури».

Такі організації зобов'язані впроваджувати заходи кіберзахисту, проводити регулярний аудит та повідомляти про кіберінциденти (наприклад, злом пошти) до Державного центру кіберзахисту (ДЦКЗ) Держспецзв'язку.

Закон України "Про електронні документи та електронний документообіг"

Цей закон надає юридичної сили електронним документам, які часто пересилаються поштою. Він вимагає забезпечення цілісності та автентичності електронних документів. Це опосередковано вимагає захисту каналу передачі (e-mail) від модифікації (атаки «man-in-the-middle») та використання електронних цифрових підписів (КЕП/УЕП) для підтвердження авторства та незмінності вмісту.

Галузеві стандарти та найкращі практики

На додаток до загальних законів, багато галузей мають власні, часто суворіші, стандарти.

PCI DSS (Payment Card Industry Data Security Standard). Це обов'язковий стандарт для будь-якої організації, що приймає, обробляє, зберігає або передає дані платіжних карток (номери карток, імена, CVC2).

Правило №1. Стандарт категорично забороняє передачу нешифрованих даних платіжних карток (PAN) через незахищені канали, до яких належить звичайна електронна пошта (e-mail, SMS, чати).

Вимога 4.2: Чітко вказує, що «ніколи не слід надсилати нешифровані PAN через кінцеві користувацькі технології обміну повідомленнями (наприклад, електронну пошту, миттєві повідомлення, SMS, чат)».

Захист корпоративної електронної пошти в сучасній організації — це комплексна задача, що лежить на перетині чотирьох площин регулювання:

Міжнародні практики (ISO 27001/27002) - вимагають впровадження процесів управління ризиками та набір технічних контролів (MFA, DLP, Anti-Malware, Sandboxing, URL-filtering, шифрування).

Закони про приватність (GDPR, Закон "Про захист ПД") - покладають юридичну відповідальність за витік персональних даних, вимагаючи захисту «за задумом», шифрування та можливості відновлення (резервного копіювання).

Національні стандарти - встановлюють обов'язкові технічні вимоги (особливо для держсектору та об'єктів критичної інфраструктури) та вимагають атестації систем і сертифікації засобів захисту.

Галузеві норми (PCI DSS, НБУ) -накладають суворі, специфічні заборони та вимоги, що стосуються конкретних типів даних (наприклад, заборона передачі номерів карток поштою).

1.4. Аналіз технологій забезпечення захисту корпоративної електронної пошти

Зловмисники постійно розробляють нові методи атак, такі як соціальна інженерія, фішинг та компрометація ділової електронної пошти (BEC), щоб націлитися на конфіденційну інформацію. Зі зростанням обсягу та складності цих загроз очікується що комплексне рішення для безпеки корпоративної електронної пошти є критично важливим питанням.

Успіх організації залежить від захисту своїх співробітників та бізнесу від сучасних передових загроз електронної пошти. Саме тому у звіті Gartner Magic Quadrant для платформ безпеки електронної пошти за 2024 рік показано найкращі рішення, які реалізуються в організаціях для захисту корпоративної пошти (рис.1.4) [5].

Для порівняння та вибору рішення оберемо: Proofpoint, Check Point Software Technologies, Trend Micro та Barracuda.

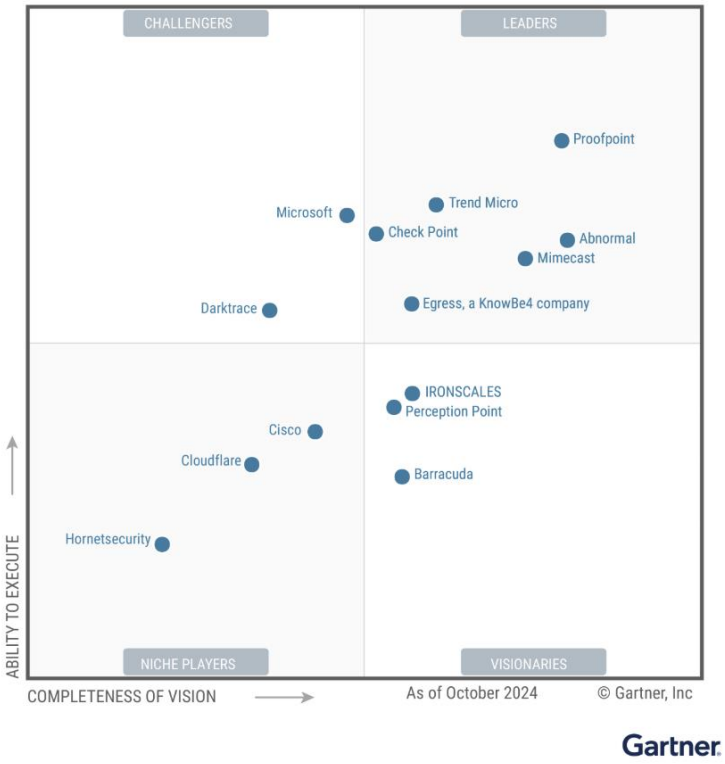

Рис. 1.4. Кращі рішення захисту корпоративної пошти [5]

Сучасний захист корпоративної пошти вимагає багаторівневої стратегії, що виходить за межі простого блокування спаму. Найкращі технології захисту корпоративної електронної пошти сьогодні зосереджені на наступних критеріях:

AI-керованому виявленні. Аналіз поведінки та контексту для виявлення фішингу та шахрайства (BEC).

API-інтеграції. Сканування внутрішнього трафіку та вже доставлених листів.

Захисті від Account Takeover (ATO). Моніторинг скомпрометованих облікових записів.

Автоматичному реагуванні. Видалення загроз після доставки (post-delivery remediation).

Навчанні користувачів. Інтегровані симуляції та тренінги.

Розглянемо, як кожен із провідних вендорів реалізує ці технології.

Надаймо короткий огляд кожної платформи, яку будемо порівнювати.

1. Proofpoint Email Security and Protection

Proofpoint вважається одним із лідерів ринку, особливо у великому корпоративному сегменті (Enterprise). Його потужність полягає у надзвичайно потужному та деталізованому шлюзі безпеки (Secure Email Gateway, SEG). Шлюз пропонує глибокий аналіз загроз, передові технології ізоляції браузера та надійні функції запобігання втраті даних (DLP). Рішення є модульним, що дозволяє компаніям обирати необхідні компоненти, тому це може збільшити складність та вартість.

2. Check Point Harmony Email & Collaboration

Check Point пропонує інноваційний підхід, який значною мірою покладається на API-інтеграцію, а не на традиційний шлюз (хоча шлюз також доступний). Harmony підключається безпосередньо до хмарних сервісів, таких як Microsoft 365 та Google Workspace. Це дозволяє йому аналізувати не лише зовнішній, але й внутрішній поштовий трафік (east-west traffic) та захищати додатки для спільної роботи (Teams, Slack, OneDrive), що є його унікальною перевагою.

3. Trend Micro Email Security

Trend Micro пропонує багаторівневий захист, який поєднує традиційний шлюз з передовими технологіями. Сильною стороною є використання машинного навчання та спеціалізованої "пісочниці" (sandbox) для глибокого аналізу вкладень та URL-адрес. Trend Micro також використовує унікальну технологію "Writing Style DNA" (аналіз стилю письма), яка за допомогою AI допомагає виявляти цільові атаки та шахрайство з боку керівництва (BEC).

4. Barracuda Total Email Protection

Barracuda пропонує найбільш інтегрований підхід "все-в-одному". Платформа Total Email Protection — це комплексний пакет, що поєднує кілька ключових технологій:

Gateway Defense. Потужний шлюз для фільтрації спаму та вірусів на вході.

Sentinel (AI). «Мозок» системи. Це рішення на базі AI, що інтегрується через API безпосередньо в M365. Воно вивчає унікальні патерни спілкування компанії, щоб виявляти загрози, які пропускають шлюзи (BEC, ATO, фішинг).

Security Awareness Training. Повністю інтегрована платформа для навчання та симуляції фішингу.

Impersonation Protection. Розширений захист від усіх 13 типів поштових загроз, включаючи шахрайство.

У таблиці 1.1 представлено порівняння обраних вендорів за сучасними критеріями захисту.

Таблиця 1.1.

Порівняння рішень за обраними критеріями

Критерій захисту	**Proofpoint Email Security**	**Check Point Harmony Email**	**Trend Micro Email Security**	**Barracuda Total Email Protection**
Основний підхід	Потужний шлюз (SEG) з глибоким аналізом. Сильний акцент на DLP та відповідність нормам.	API-інтеграція ("in-box defense"). Захист не лише пошти, але й додатків для спільної роботи.	Багаторівневий шлюз (SEG) з використанням машинного навчання та "пісочниці" (sandboxing).	Інтегрована платформа: Поєднує Шлюз + API-захист (AI) + Навчання + Архівацію в єдиному рішенні.

AI-захист (BEC/Phishing)	Високоефективний, але більше покладається на аналіз на рівні шлюзу.	Дуже сильний. Аналізує понад 300 індикаторів фішингу; бачить внутрішній трафік.	Сильний. Використовує "Writing Style DNA" для виявлення BEC.	Винятково сильний (Sentinel). API-модуль Sentinel вивчає унікальні патерни спілкування компанії та виявляє аномалії, які пропускають шлюзи.
Захист від Account Takeover (ATO)	Пропонується як окремий модуль. Вимагає додаткової інтеграції та налаштування.	Вбудований в платформу Harmony, виявляє підозрілий вхід в систему та внутрішні загрози.	Присутній, але фокус більше на вхідних загрозах, ніж на моніторингу скомпрометованих акаунтів.	Вбудований (Sentinel). Активно моніторить поштові скриньки на предмет підозрілої активності, автоматично блокує скомпрометовані акаунти.
Пост-доставка (Retraction)	Присутня (TRAP - Threat Response Auto-Pull), але часто вимагає ручного втручання або складних налаштувань.	Так, API-підхід дозволяє миттєво видаляти загрози, виявлені	Так, дозволяє видаляти листи, які були визнані шкідливими після аналізу.	Повністю автоматизовано. Sentinel автоматично знаходить і видаляє всі копії шкідливого листа з поштових

		після доставки.		скриньок користувачів.
Інтегроване навчання (Awareness)	Пропонується (раніше Wombat Security), але це окремий продукт, що вимагає окремої ліцензії та інтеграції.	Не є основним фокусом платформи Harmony, зазвичай вимагає сторонніх рішень.	Пропонує інструмент симуляції фішингу (Phish Insight), але він не так тісно інтегрований у загальний цикл захисту.	Повністю інтегровано. Платформа Total Email Protection включає модуль Security Awareness Training "з коробки".

Аналіз показує, що хоча всі рішення пропонують потужний захист, Barracuda Total Email Protection виділяється як найкращий вибір завдяки своїй комплексній та тісно інтегрованій стратегії.

Конкуренти, як-от Proofpoint і Trend Micro, історично покладалися на підхід "фортеці" (шлюз). Barracuda визнає, що загрози (особливо BEC та ATO) часто виникають всередині мережі. Її модуль Sentinel (AI), що працює через API, є найкращим інструментом для боротьби з цими сучасними атаками, оскільки він аналізує внутрішній трафік і поведінкові патерни, що є невидимим для традиційних шлюзів.

Barracuda пропонує не просто «продукт», а «платформу». Замість того, щоб купувати окремий шлюз, окремий інструмент для захисту від ATO та окрему платформу для навчання персоналу, Barracuda об’єднує всі три стовпи захисту (Шлюз, AI-захист пошти та Навчання) в одному пакеті Total Email Protection. Це значно спрощує управління та знижує загальну вартість володіння.

Інструменти Barracuda, особливо в частині видалення загроз після доставки та реагування на компрометацію облікових записів (ATO), є високо

автоматизованими. Це звільняє час IT-команд, дозволяючи їм зосередитись на стратегічних завданнях, а не на ручному «полюванні» за загрозами.

У той час як Proofpoint є лідером для великих підприємств зі складними вимогами DLP, а Check Point пропонує інноваційний API-захист, Barracuda надає найбільш збалансоване, повне та інтегроване рішення, яке ідеально підходить для організацій, що прагнуть отримати максимальний рівень захисту від усіх типів поштових загроз без зайвої складності.

Висновки до розділу 1

1. Аналіз показав, що корпоративна електронна пошта залишається критично важливим інструментом для бізнес-комунікацій. Водночас вона є домінуючим вектором кібератак — 94% шкідливих програм доставляються саме через e-mail, що створює фундаментальну проблему безпеки для сучасних організацій.

2. Ландшафт загроз значно еволюціонував від простого спаму до складних, фінансово руйнівних атак. Сучасні загрози, такі як компрометація ділової пошти (BEC), програми-вимагачі (Ransomware) та цільовий фішинг, вимагають захисту, що виходить далеко за межі базової антивірусної фільтрації.

3. Захист корпоративної пошти є не лише технічною необхідністю, але й суворою юридичною та регуляторною вимогою. Міжнародні (ISO 27001/27002, GDPR) та галузеві (PCI DSS) стандарти вимагають від організацій впровадження конкретних технічних і організаційних контролів (MFA, DLP, шифрування, аудит, резервне копіювання).

4. Порівняльний аналіз провідних технологій (Proofpoint, Check Point, Trend Micro, Barracuda) показав, що традиційні шлюзи безпеки є недостатніми для боротьби з сучасними загрозами. Найбільш ефективною є комплексна, інтегрована платформа, яка поєднує захист шлюзу з AI-аналізом (для BEC), API-інтеграцією (для ATO) та інтегрованим навчанням персоналу.

2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ BARRACUDA EMAIL SECURITY GATEWAY

2.1. Архітектура Barracuda Email security gateway

Barracuda Email security gateway захищає як вхідну, так і вихідну електронну пошту від найновіших спамів, вірусів, черв'яків, фішингу, атак типу «відмова в обслуговуванні» та загроз «нульового дня». Barracuda Email security gateway — це служба, яка діє як фільтр перед розміщеною поштовою службою або серверами.

У Barracuda Email security gateway доступні такі функції :

Отримує вхідну електронну пошту від імені вашої організації, захищаючи ваш поштовий сервер від отримання прямих інтернет-з’єднань та пов’язаних із ними загроз.

Використовує фільтрацію контенту для виявлення та блокування небажаних електронних листів, перш ніж прийняти їхнє тіло для подальшої обробки.

Використовує засоби контролю вхідної та вихідної пошти для захисту вашої поштової інфраструктури від автоматизованого програмного забезпечення для розсилки спаму, а потім виконує подальший аналіз IP-адрес електронних листів.

Забезпечує автентифікацію відправника, таку як Sender Policy Framework (SPF), для вхідної пошти з метою перевірки відправників; застосовує політики та прогнозне профілювання відправників для визначення поведінки відправника та відхилення з’єднань та/або повідомлень від спамерів.

Використовує три рівні сканування на віруси: вірусні визначення з відкритим кодом від спільноти розробників відкритого коду, власницькі вірусні визначення від Barracuda Central та систему реального часу Barracuda (BRTS), яка забезпечує аналіз відбитків пальців, захист від вірусів та аналіз намірів.

Використовує запатентовану антивірусну суперкомп'ютерну сітку Barracuda Antivirus, захищаючи вашу мережу від поліморфних вірусів.

Пропонує розширений захист від загроз (ATP) на основі підписки для аналізу вхідних вкладень електронної пошти в окремому захищеному хмарному середовищі з метою виявлення нових загроз.

Надсилає користувачам сповіщення про карантин та блокування контенту.

Забезпечує кілька типів шифрування для вхідного та вихідного трафіку повідомлень.

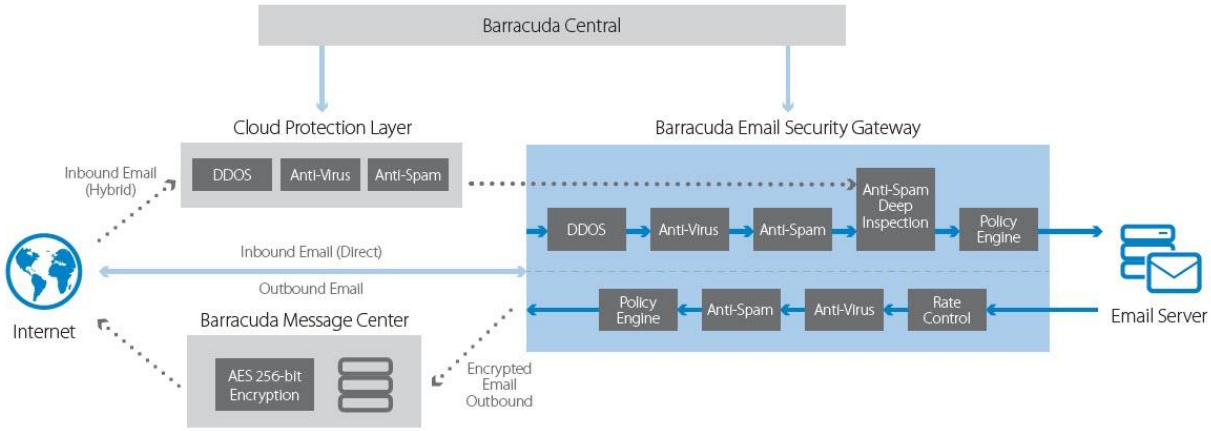

Рис. 2.1. Архітктура Barracuda Email Security Gateway

Надана архітектурна схема на рис.2.1. Barracuda Email Security Gateway ілюструє ключовий принцип захисту, а саме багаторівневу оборона. Замість того, щоб покладатися на один механізм, Barracuda Email Security Gateway створює ешелоновану систему безпеки, де кожен наступний шар призначений для виявлення та блокування загроз, які могли б (теоретично) пройти крізь попередній шар [8,9].

До складу архітектури Barracuda Email Security Gateway входить чотири основних, логічно відокремлених компонентів, які працюють узгоджено між собою:

1. Barracuda Central. «Мозок» системи, що працює в режимі реального часу.

2. Хмарний рівень захисту (Cloud Protection Layer -CPL). Необов'язковий, але рекомендований хмарний фільтр першого проходу електронної пошти.

3. Шлюз безпеки (Barracuda Email Security Gateway). Основний пристрій (фізичний, віртуальний або хмарний), що виконує глибоку інспекцію корпоративної електронної пошти.

4. Центр повідомлень (Barracuda Message Center). Зовнішня хмарна служба для шифрування, буферизації та запобігання втраті даних (DLP).

Аналіз архітектури показує два основних потоки обробки пошти - вхідний (inbound) та вихідний (outbound), кожен з яких має свій унікальний ланцюжок фільтрації для вирішення специфічних завдань.

Реалізація концепції архітектури Barracuda Email Security Gateway може бути за двома підходами:

Гібридний підхід. Рис.2.1 чітко показує можливість гібридного розгортання. Тобто вхідний трафік «Inbound Email (Hybrid)» пошти спочатку проходить через Cloud Protection Layer, який відфільтровує основну масу спаму та вірусів, зменшуючи навантаження на локальний шлюз. Це також забезпечує захист від DDOS-атак на рівні хмари, не даючи їм дістатися до інфраструктури компанії [8-9].

Прямий підхід. Вхідний потік "Inbound Email (Direct)" пошти може працювати і автономно, приймаючи пошту безпосередньо з Інтернету.

Розділення потоків. Вхідний та вихідний потоки (inbound/outbound) всередині самого шлюзу Barracuda Email Security Gateway обробляються різними конвеєрами. Це критично важливо, оскільки завдання в них різні:

– Вхідний потік. Захист компанії від зовнішнього світу (фішинг, віруси, спам).

– Вихідний потік. Захист репутації компанії та запобігання витоку даних (DLP, шифрування, блокування спаму зі скомпрометованих акаунтів).

Перейдемо до опису основних компонент Barracuda Email Security Gateway, який представимо у вигляді таблиці 2.1. Основними компонентами Barracuda Email Security Gateway є Barracuda Central, Cloud Protection Layer, Barracuda Email Security Gateway, Barracuda Message Center, Email Server.

Таблиця 2.1:

Основні компоненти архітектури та їх призначення

Компонент	Розташування	Основна функція
Barracuda Central	Глобальна хмара (Зовнішнє)	Надання розвідки про загрози в реальному часі (IP-репутація, сигнатури вірусів, спам-патерни).
Cloud Protection Layer	Глобальна хмара (Зовнішнє)	Фільтрація першого проходу: блокування DDOS-атак та масового спаму/вірусів до того, як вони досягнуть мережі.
Barracuda Email Security Gateway	Локально / Приватна хмара (Внутрішнє)	Основний механізм глибокої інспекції, застосування політик, DLP та розширеного захисту.
Barracuda Message Center	Глобальна хмара (Зовнішнє)	Безпечний портал для обміну зашифрованими листами, буферизація вихідної пошти.
Email Server	Локально / Приватна хмара (Внутрішнє)	Кінцева точка доставки пошти (напр., Microsoft Exchange, M365, Google Workspace).

Успіх будь-якого сучасного шлюзу безпеки залежить не лише від його власних обчислювальних потужностей, але й від якості та швидкості отримання даних про загрози. Архітектура Barracuda робить на цьому сильний акцент.

1. Barracuda Central (Глобальний центр розвідки)

Як показано на рис.2.1, Barracuda Central є "парасольковою" структурою, яка надає дані як хмарному рівню (CPL), так і локальному шлюзу (Barracuda Email Security Gateway - BESG). Це критично важливий компонент.

Це глобальний SOC, який працює 24/7/365. Він збирає та аналізує дані про загрози з мільйонів точок збору по всьому світу (інших пристроїв Barracuda, "медових пасток", аналітичних систем).

Функції Barracuda Central:

– Репутація IP. Barracuda Central веде динамічний список IP-адрес, помічених у розсилці спаму або зловмисній активності. CPL та BESG використовують цей список, щоб відхиляти з'єднання від відомих поганих джерел ще до прийому самого листа.

– Сигнатури спаму (Spam Signatures). Центр миттєво створює "відбитки" нових спам-кампаній і розсилає їх на всі пристрої.

– Сигнатури вірусів (Virus Definitions). Забезпечує оновлення для антивірусних механізмів.

– Аналіз намірів (Intent Analysis). Barracuda Central аналізує URL-адреси в режимі реального часу, щоб ідентифікувати нові фішингові сайти.

2. Cloud Protection Layer (CPL) (Хмарний рівень захисту)

Рис.2.1.показує, що CPL є першим бастіоном в гібридному сценарії. Він діє як буфер між Інтернетом та інфраструктурою клієнта.

Призначення CPL полягає в зменшенні навантаження та забезпечення безперервності бізнесу. CPL приймає 100% вхідного трафіку. Він виконує три основні операції:

– DDOS-захист -поглинає масивні атаки на рівні з'єднань, які могли б «покласти» локальний шлюз або інтернет-канал компанії.

– Anti-Virus - перший прохід антивірусного сканування, відсіює відомі загрози.

– Anti-Spam: Блокує 80-90% очевидного спаму на основі репутації та сигнатур від Barracuda Central.

Лише "чистий" або "підозрілий" трафік, який потребує глибшого аналізу пересилається далі на локальний Barracuda Email Security Gateway. Barracuda Email Security Gateway

Додаткова функція CPL полягає у буферізації, тобто виконання функцію буферизації пошти (spooling). Якщо локальний Email Server або сам BESG стають недоступними (наприклад, збій живлення, падіння інтернет-каналу), CPL буде приймати та зберігати вхідну пошту (до 96 годин) і доставить її, щойно з'єднання відновиться. Це забезпечує нульову втрату листів під час збоїв [10].

3. Barracuda Email Security Gateway

На рис.2.1. детально показано процес обробки листів, що надходять до організації. Розглянемо кожен етап. Після того, як лист пройшов CPL (або надійшов напряму), він потрапляє у ланцюжок фільтрів на самому шлюзі. Цей процес часто називають "12-рівневим захистом", і рис.2.1 ілюструє його ключові етапи [9,8].

Eman 1: DDOS (Захист від відмови в обслуговуванні). Якщо CPL не використовується, шлюз сам має вбудовані механізми захисту від атак на рівні поштових протоколів (наприклад, атаки на SMTP-автентифікацію).

Eman 2: Anti-Virus (Антивірусне сканування). Це не один механізм, а три рівні антивірусного захисту:

– Власний антивірусний механізм Barracuda.

– Ліцензований механізм (наприклад, Avira або Sophos).

– Сканування всередині архівів (ZIP, RAR, 7-Zip), блокування за типами файлів.

Цей етап відсіює відомі віруси, трояни та шкідливе ПЗ на основі сигнатур.

Eman 3: Anti-Spam (Базовий захист від спаму). На цьому етапі відбувається перевірка на основі репутації (з Barracuda Central), перевірка SPF, DKIM та DMARC для автентифікації відправника.

Eman 4: Anti-Spam Deep Inspection (Глибока інспекція). Це найважливіший етап для боротьби з сучасними загрозами (нульового дня та фішингом). Він включає три перевірки:

Advanced Threat Protection (ATP). Це хмарна "пісочниця" (sandbox). Якщо антивірус не виявив загрози, але файл виглядає підозріло (наприклад, .docx з макросами, невідомий .exe), він відправляється в ізольоване хмарне середовище Barracuda, де файл "підривається" (запускається) і система спостерігає за його поведінкою (чи намагається він зашифрувати файли, з'єднатися зі шкідливим C&C-сервером тощо) [11].

Link Protection (Захист посилань). Усі URL-адреси в тілі листа переписуються, щоб вказувати на проксі-сервер Barracuda. Коли користувач натискає на посилання (навіть через тиждень), він спочатку потрапляє на сервер Barracuda, який в режимі реального часу перевіряє репутацію цільового сайту. Якщо сайт фішинговий, користувач блокується.

Аналіз намірів (Intent Analysis). Пошук ознак шахрайства (BEC) – аналіз заголовків, виявлення спроб видати себе за керівника (impersonation), пошук підозрілих ключових слів ("терміново", "переказ коштів").

Eman 5: Policy Engine (Механізм політик) Це фінальний фільтр, де застосовуються власні правила організації, такі як:

Content Filtering. Блокування листів за ключовими словами в темі або тілі.

Attachment Filtering. Блокування певних типів файлів (напр., .exe, .bat), навіть якщо вони не є вірусами.

DLP (Data Loss Prevention). Сканування вхідної пошти на наявність чутливих даних (наприклад, номери кредитних карток), хоча DLP більш критичний для вихідного потоку.

Recipient Verification. Перевірка, чи існує одержувач в LDAP або Azure AD, для блокування атак підбору адрес (Directory Harvest Attack).

Лише після проходження всіх цих етапів лист доставляється на Email Server.

3. Barracuda Message Center (Центр обміну повідомленнями). Цей компонент, винесений в хмару, вирішує проблему безпечної передачі конфіденційних даних. Звичайна електронна пошта за своєю природою не є безпечною [12,13].

Розглянемо, як це працює у вигляді основних кроків:

1. Вихідний лист потрапляє в Policy Engine на BESG.

2. Політика (DLP або правило) визначає, що лист потребує шифрування.

3. BESG не відправляє лист одержувачу. Замість цього він безпечним каналом передає його до Barracuda Message Center.

4. Message Center зберігає лист у зашифрованому вигляді (наприклад, AES 256-bit Encryption).

5. Одержувачу в Інтернеті надсилається звичайний, чистий e-mail (сповіщення) з текстом: «Ви отримали безпечне повідомлення від [Ім'я Співробітника]. Натисніть тут, щоб переглянути».

6. Одержувач натискає на посилання, потрапляє на захищений веб-портал Message Center, де він (після простої реєстрації або введення пароля) може прочитати лист і безпечно завантажити вкладення.

Переваги:

– Конфіденційний вміст ніколи не залишає захищений периметр (BESG -> Message Center).

– Відповідає вимогам GDPR, HIPAA, PCI-DSS щодо захисту даних «в русі».

– Простота для кінцевих користувачів (як відправника, так і одержувача).

2.2. Ключові характеристики Barracuda Email security gateway

Розглянемо основні сервіси, які надає Barracuda Email security gateway.

1. Шари управління з'єднаннями

Шари упралінняя з’єднаннями визначають та блокують небажані електронні листи, перш ніж прийняти їхнє тіло для подальшої обробки. Фільтрація з’єднань дозволяє блокувати або дозволяти:

– IP-адреси відправника
– Адреси електронної пошти / домени відправника
– Повідомлення електронної пошти, написані певними мовами
– Повідомлення електронної пошти, надіслані з певних країн/регіонів

2. Захист від відмови в обслуговуванні (DoS)

Email Gateway отримує вхідну електронну пошту від імені організації, захищаючи поштовий сервер вашої організації від отримання прямих інтернет-з’єднань та пов’язаних із ними загроз. Цей рівень не застосовується до вихідної пошти.

3. Контроль швидкості

Автоматизоване програмне забезпечення для боротьби зі спамом може використовуватися для надсилання великих обсягів електронної пошти на один поштовий сервер. Щоб захистити інфраструктуру електронної пошти від цих атак на основі флуду, Email Gateway Defense підраховує кількість одержувачів від відправника до домену протягом 30-хвилинного інтервалу та відкладає з’єднання після перевищення певного порогу. Контроль вхідної швидкості – це поріг для кількості одержувачів, яких домен бажає отримати від відправника (однієї IP-адреси) протягом 30-хвилинного інтервалу. Контроль вхідної швидкості налаштовується, тоді як контроль вихідної швидкості встановлюється автоматично Email Gateway Defense.

4. Моніторинг підозрілої електронної пошти

Моніторинг підозрілої електронної пошти перевіряє вхідну пошту з усього світу, шукаючи листи зі спільними темами та підозрілим вмістом. Якщо такі виявляються, Email Gateway Defense відкладає цей лист, змушуючи відправника повторити спробу надіслати його пізніше. Зазвичай лист буде дозволено після

повторної спроби. Однак може знадобитися кілька повторних спроб, особливо якщо вони зроблені занадто швидко. Клієнти можуть додати адресу відправника до політики дозволу відправників, щоб обійти фільтрацію підозрілих повідомлень, або звернутися до служби технічної підтримки Barracuda Networks, щоб вимкнути політику підозрілих повідомлень.

5. Аналіз IP-адрес

Після застосування контролю швидкості на основі IP-адреси, Email Gateway виконує аналіз IP-адреси електронної пошти на основі репутації Barracuda, зовнішніх списків блокування, а також списків дозволених і заблокованих IP-адрес.

6. Автентифікація відправника

Оголошення недійсної адреси «відправника» – поширена практика, яку використовують спамери. Рівень автентифікації відправника Email Gateway використовує низку методів для вхідної пошти, щоб перевірити відправника електронного повідомлення та застосувати політику. Sender Policy Framework (SPF) відстежує автентифікацію відправника, змушуючи домени публікувати зворотні записи MX, щоб відобразити, які машини призначені як машини відправника пошти для цього домену. Одержувач може перевірити ці записи, щоб переконатися, що пошта надходить із призначеної машини відправника.

7. Шари сканування пошти

Найбазовішим рівнем сканування пошти є сканування на віруси. Email Gateway використовує три рівні сканування на віруси та автоматично розпаковує архіви для комплексного захисту. Використовуючи визначення вірусів, клієнти Email Gateway отримують найкращий та найповніший захист від вірусів та шкідливих програм. Три рівні сканування на віруси вхідної та вихідної пошти включають:

– Потужні визначення вірусів з відкритим кодом від спільноти відкритого коду допомагають відстежувати та блокувати найновіші вірусні загрози.

– Власні вірусні визначення, зібрані та підтримувані Barracuda Central, нашим передовим центром безпеки, який працює цілодобово та безперервно відстежує та блокує найновіші інтернет-загрози.

– Система реального часу Barracuda (BRTS). Ця функція забезпечує аналіз відбитків пальців, захист від вірусів та аналіз намірів. Після ввімкнення будь-який новий спалах вірусу або спаму може бути зупинений у режимі реального часу, що забезпечує відмінний час реагування на загрози, що передаються електронною поштою. BRTS дозволяє клієнтам повідомляти про активність поширення вірусів та спаму на ранній стадії до Barracuda Central. Сканування на віруси має пріоритет над усіма іншими методами сканування пошти та застосовується навіть тоді, коли пошта проходить через рівні керування підключеннями. Таким чином, навіть електронні листи, що надходять з виключених IP-адрес, доменів відправників, адрес електронної пошти відправників або одержувачів, все одно скануються на наявність вірусів та поміщаються в карантин, якщо виявлено вірус.

Крім того, Barracuda Networks пропонує послугу розширеного захисту від загроз (ATP) на основі підписки – хмарну службу захисту від вірусів, яка застосовується до вхідних повідомлень. ATP аналізує вкладення електронної пошти в окремому захищеному хмарному середовищі, щоб виявляти нові загрози та визначати, чи блокувати такі повідомлення.

8. Суперкомп'ютерна мережа Barracuda Antivirus

Додатковим рівнем захисту від вірусів, що очікує на отримання патенту, що пропонує Email Gateway, є Barracuda Antivirus Supercomputing Grid, яка може захистити мережу від поліморфних вірусів. Вона не лише виявляє нові спалахи, схожі на відомі віруси, але й ідентифікує нові загрози, для яких ніколи не існувало сигнатур, за допомогою технології «передбачень».

9. Аналіз намірів

Усі спам-повідомлення мають «намір» – спонукати користувача відповісти на електронний лист, відвідати веб-сайт або зателефонувати за номером телефону.

Аналіз намірів включає дослідження адрес електронної пошти, веб-посилань та номерів телефонів, вбудованих у повідомлення електронної пошти, щоб визначити, чи пов’язані вони з легітимними особами. Часто аналіз намірів є захисним рівнем, який виявляє фішингові атаки. Коли його ввімкнено, Email Gateway застосовує різні форми аналізу намірів як до вхідної, так і до вихідної пошти, включаючи аналіз намірів (або «контенту») у режимі реального часу та багаторівневий аналіз. Багаторівневий намір – це процес ідентифікації URL-адрес у тілі повідомлення електронної пошти, які перенаправляють на відомі сайти зі спамом або шкідливим програмним забезпеченням.

10. Розширене виявлення спаму

Ви можете налаштувати виявлення спаму для користувацьких категорій, встановивши оцінку типу вмісту. Ця оцінка коливається від 0 (точно не спам) до 10 (точно спам). На основі цієї оцінки Email Gateway блокує повідомлення, які виглядають як спам. Ці повідомлення відображаються в журналі повідомлень користувача з категорією, що відповідає за блокування.

11. Прогнозне профілювання відправника

Коли спамери намагаються приховати свою особу, Email Gateway може використовувати прогнозне профілювання відправників, щоб визначити поведінку всіх відправників та відхилити з’єднання та/або повідомлення від спамерів. Це передбачає врахування репутації очевидного відправника повідомлення, так само, як банк повинен враховувати репутацію дійсного власника кредитної картки, якщо вона втрачена або вкрадена та використана для шахрайства. Деякі приклади поведінки спамерів, які намагаються сховатися за дійсним доменом, та функції Email Gateway Defense, які вирішують цю проблему, включають наступне:

– Надсилання занадто великої кількості електронних листів з однієї мережевої адреси – автоматизоване програмне забезпечення для розсилки спаму може використовуватися для надсилання великої кількості електронних листів з одного поштового сервера. Завдяки функції контролю швидкості передачі даних (Rate Control) функція Email Gateway Defense обмежує кількість підключень, здійснених з будь-якої IP-адреси протягом 30-хвилинного періоду. Порушення

реєструються для виявлення спамерів. Контроль швидкості вхідних повідомлень можна налаштувати, тоді як контроль швидкості вихідних повідомлень встановлюється автоматично функцією Email Gateway Defense.

– Спроба надсилання занадто великому числу недійсних одержувачів – багато спамерів атакують поштові інфраструктури, збираючи електронні адреси. Перевірка одержувача в Email Gateway Defense дозволяє системі автоматично відхиляти спроби SMTP-з'єднання від відправників електронної пошти, які намагаються надсилати листи занадто великій кількості недійсних одержувачів, що свідчить про атаки на збирання адрес каталогів або словникові атаки.

– Реєстрація нових доменів для спам-кампаній – оскільки реєстрація нових доменних імен є швидкою та недорогою, багато спамерів змінюють доменні імена, що використовуються в кампанії, та надсилають електронні листи-розсилки в перший день реєстрації домену. Аналіз намірів у реальному часі в Email Gateway Defense зазвичай використовується для нових доменних імен і включає виконання DNS-пошуку та порівняння конфігурації DNS нових доменів з конфігураціями DNS відомих доменів спамерів.

– Використання безкоштовних інтернет-сервісів для перенаправлення на відомі спам-домени – використання безкоштовних веб-сайтів для перенаправлення на відомі спамерські веб-сайти – це поширена практика, яку використовують спамери для приховування або маскування своєї особи від методів сканування пошти, таких як аналіз намірів. За допомогою багаторівневого аналізу намірів Email Gateway Defense перевіряє результати веб-запитів до URI відомих безкоштовних веб-сайтів на наявність перенаправлень на відомі спамерські сайти.

12. Сповіщення

Email Gateway надсилає два типи сповіщень:

– Дайджест карантину – для одержувачів електронної пошти, перелічених у базі даних Email Gateway Defense, на їхню адресу електронної пошти з інтервалом, який ви вказуєте для користувачів, надсилається електронний лист зі зведеною інформацією про електронні листи, що перебувають у карантині.

– Блокування вкладень для контенту – відправнику повідомлення надсилається сповіщення, коли його заблоковано через фільтрацію вмісту вкладень.

13. Обсяг відстежуваної вихідної електронної пошти

Захист шлюзу електронної пошти контролює обсяг вихідної електронної пошти із системи до Інтернету. Якщо обсяг перевищує звичайні порогові значення протягом будь-якого 30-хвилинного інтервалу, активується функція контролю швидкості, в результаті чого вся вихідна пошта відкладається до кінця 30-хвилинного періоду. Потік вихідної пошти продовжується, якщо обсяг не буде перевищено знову протягом наступного 30-хвилинного інтервалу. Якщо це так, знову спрацьовує функція контролю швидкості, і вихідна пошта відкладається до кінця періоду часу.

14. Шифрування

Щоб запобігти витоку даних і забезпечити дотримання політик щодо інформації у фінансовій, медичній та інших федерально регульованих установах, Email Gateway пропонує кілька типів шифрування для вхідного та вихідного повідомного трафіку.

15. Зашифрований канал

Забезпечує безпечну передачу вмісту електронної пошти, як вхідної, так і вихідної, через зашифрований канал за допомогою протоколу Secure Sockets Layer (SSL), також відомого як TLS.

Щоб вимагати надсилання вихідної пошти з Email Gateway через TLS-з’єднання, увімкніть функцію «Примусово надсилати TLS» для кожного домену на сторінці «Налаштування вихідної пошти» > «Захист від втрати даних/шифрування» . Пошта, надіслана на ці домени, має передаватися через TLS-з’єднання. Якщо TLS-з’єднання не вдається встановити, пошта не буде доставлена.

Щоб вимагати використання TLS-з’єднання для вхідної пошти, що надходить до Email Gateway, установіть для параметра SMTP через TLS значення « Обов’язково» на сторінці «Домени» > «Налаштування» для кожного домену. Якщо встановлено значення «Обов’язково» , і TLS доступний на поштовому

сервері вашої організації, вхідна пошта надсилатиметься через канал TLS. Якщо ні, пошта надсилатиметься у відкритому тексті.

16. Шифрування вихідної пошти

Для гарантованого шифрування повідомлень та гарантованої доставки вихідних повідомлень використовуйте Центр повідомлень Barracuda для шифрування вмісту певних вихідних повідомлень. Створіть політики щодо шифрування вихідних повідомлень на сторінці «Налаштування вихідних повідомлень» > «Політики вмісту» для домену.

Висновки 2 розділу

1. Гібридна модель виявлення загроз: Технологія поєднує традиційні сигнатурні методи (бази вірусів, RBL, SPF-автентифікація) з передовими евристичними та поведінковими механізмами. Такі функції, як "Суперкомп'ютерна мережа Barracuda Antivirus" для поліморфних вірусів, "Прогнозне профілювання відправника" та "Аналіз намірів" дозволяють виявляти нові, раніше невідомі (zero-day) загрози, фішинг та спам-кампанії, які не мають відомих сигнатур.

2. Ефективність багатьох функцій Barracuda Email Security Gateway напряму залежить від постійного оновлення даних у режимі реального часу. Це перетворює шлюз з ізольованого пристрою на частину глобальної мережі виявлення загроз.

3. Комплексний захист вхідних та вихідних потоків, які захищають інфраструктуру компанії від атак, захищають репутацію компанії від розсилки спаму зі скомпрометованих акаунтів та запобігають витоку конфіденційних даних, забезпечуючи їх передачу через захищені канали.

4. Розглянутий набір сервісів Email Gateway створює цілісну, глибоко інтегровану систему безпеки, що здатна протидіяти широкому спектру загроз на кожному етапі життєвого циклу електронного повідомлення — від початкової спроби з'єднання до фінальної доставки чи шифрування.

3 ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНОЇ ПОШТИ BARRACUDA EMAIL SECURITY GATEWAY

3.1. Варіанти технології розгортання та налаштуваяння електронної пошти Barracuda

Barracuda Email Security Gateway пропонує декілька варіантів розгортання технології для захисту електронооі пошти корпоративної інформаційної системи.

Крок 1. Вибір варіанту розгортання.

Шлюз безпеки електронної пошти Barracuda в демілітаризованій зоні

На рис.3.1. показано Barracuda Email Security Gateway, який встановлюється перед корпоративним брандмауером у демілітаризованій зоні (DMZ). У цьому прикладі поштовий сервер має IP-адресу 64.5.5.6, а шлюз безпеки електронної пошти Barracuda має IP-адресу 64.5.5.5.

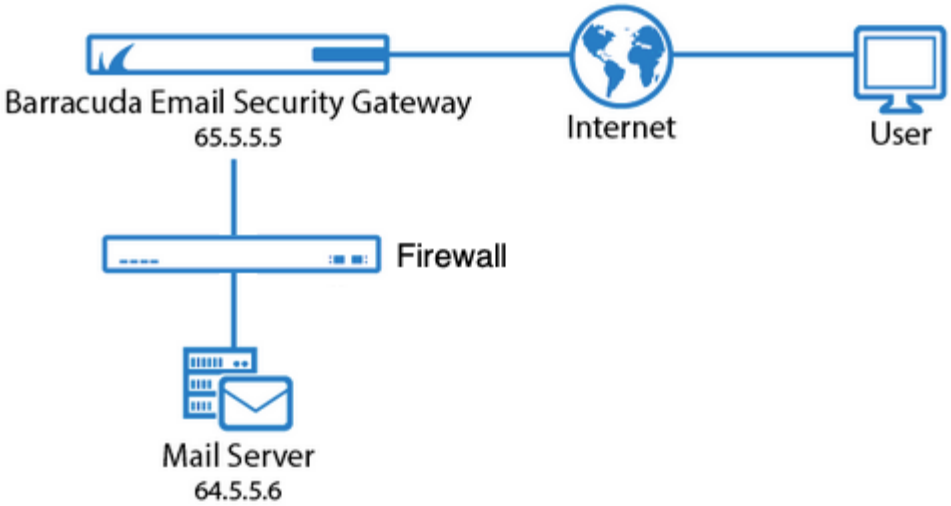

Рис.3.1. Barracuda Email Security Gateway в демілітаризованій зоні

В цьому варіанті налаштування необхідно виконайте такі завдання:

1. Призначте доступну зовнішню IP-адресу шлюзу безпеки електронної пошти Barracuda.

2. Змініть записи MX на DNS), щоб спрямувати трафік на шлюз безпеки електронної пошти Barracuda.

Розгортання за корпоративним брандмауером

На рис 3.2 показано Barracuda Email Security Gateway за корпоративним брандмауером. У цьому прикладі поштовий сервер має IP-адресу 10.10.10.2, а шлюз безпеки електронної пошти Barracuda має IP-адресу 10.10.10.3.

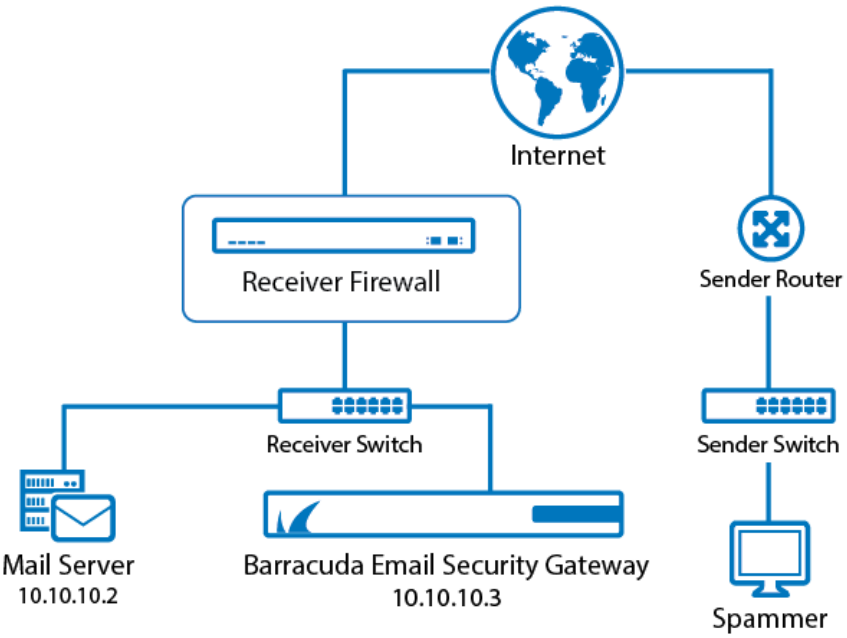

Рис.3.2. Barracuda Email Security Gateway за корпоративним брандмауером

Для цього варіанту налаштування необхідно виконайте такі завдання:

1. Переадресація (перенаправлення порту) вхідного SMTP-трафіку на порту 25 до шлюзу безпеки електронної пошти Barracuda о 10.10.10.3.

2. Налаштувати Barracuda Email Security Gateway для пересилання відфільтрованих повідомлень на поштовий сервер призначення 10.10.10.2.

Крок 2. Встановлення шлюзу безпеки електронної пошти Barracuda.

Крок 3 – Початкова конфігурація.

Крок 4. Активація продукту та оновлення прошивки.

Крок 5 – Налаштування веб-інтерфейсу.

Крок 6 – Маршрутизація вхідної пошти.

Метою налаштування шлюзу безпеки електронної пошти Barracuda є виявлення спаму без блокування дійсних повідомлень. Розглянемо використання власної політики фільтрації спаму для вхідної пошти, а також додаткові, більш складні методи ідентифікації спаму.

Основний перелік налаштувань Barracuda Email Security Gateway включає:

– Розширений захист від загроз.
– Захист від шахрайства та фішингу.
– Контроль швидкості вхідного сигналу.
– Аналіз IP-адрес вхідного зв'язку.
– Вхідний аналіз контенту.
– Вхідний баєсівський аналіз.
– Виявлення масової розсилки електронною поштою.
– Регіональна політика.

Розширений захист від загроз

Розширений захист від загроз (ATP) пропонує хмарний захист від складних шкідливих програм, експлойтів нульового дня та цілеспрямованих атак, які не виявляються функціями сканування на віруси Barracuda Email Security Gateway. Barracuda Email Security Gateway надає доступ до рівня захисту Barracuda Cloud Protection Layer (CPL) за наявності активної підписки ATP.

ATP аналізує вкладення вхідних електронних листів з більшістю типів MIME та загальнодоступними посиланнями для прямого завантаження в окремій захищеній хмарній пісочниці, виявляючи нові загрози та визначаючи, чи блокувати такі повідомлення (рис.3.3). ATP пропонує захист від складного шкідливого програмного забезпечення, експлойтів нульового дня та цілеспрямованих атак, які не виявляються функціями сканування на віруси Barracuda Email Security Gateway.

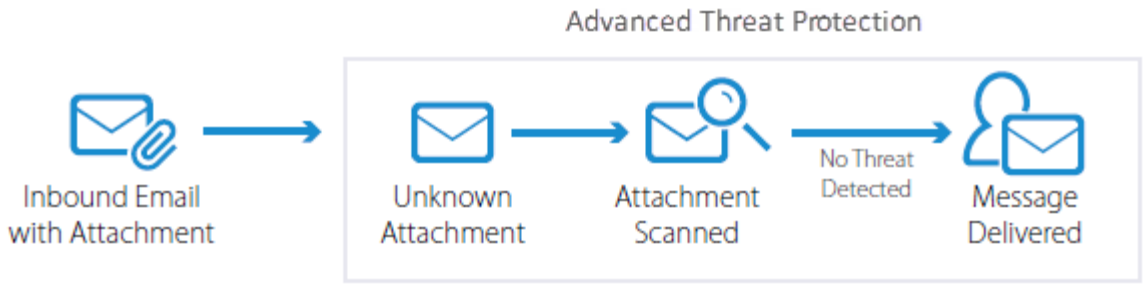

Рис. 3.3. Технологія захисту від розширених атак

ATP аналіз відбувається у компоненті, або модулі CPL. Це надає можливість визначати як і коли сканувати вкладення, на вкладці НАЛАШТУВАННЯ ATP.

1. *Спочатку доставити, потім сканувати* – якщо вибрано цей режим, то служба ATP намагається сканувати пошту в режимі реального часу. Якщо сканування ATP завершується в режимі реального часу і виявлено вірус, повідомлення блокується та не доставляється. Якщо сканування ATP не завершується в режимі реального часу, повідомлення доставляється. Якщо служба ATP визначає, що вкладення є підозрілим або зараженим вірусом після завершення, одержувач отримує сповіщення, а якщо для параметра «Повідомити адміністратора» встановлено значення «Так» , сповіщення електронною поштою надсилається на вказану адресу адміністратора.

Цей параметр не затримує обробку електронної пошти, проте одержувач електронного листа може потенційно відкрити заражене вкладення.

2. *Спочатку сканувати, а потім доставляти* – якщо вибрано цей режим, служба ATP сканує повідомлення з вкладеннями перед доставкою. Якщо у вкладенні виявлено вірус, повідомлення блокується, інакше повідомлення доставляється одержувачу.

Цей параметр забезпечує підвищений рівень безпеки та запобігає відкриттю заражених вкладень одержувачем електронного листа. Треба розуміти, що повідомлення з вкладеннями можуть бути тимчасово відкладені, поки вони стоять у черзі на сканування. Ці повідомлення відображаються в журналі повідомлень, а «Очікування сканування» відображається у стовпці «Причина» . Поштовий сервер

повторює спроби, доки сканування не завершиться, і у вкладенні не буде виявлено вірусів, після чого повідомлення доставляється.

3. Ні – якщо вибрано цей режим, ATP вимкнено.

Захист від шахрайства та фішингу

Фішингові шахрайства – це зазвичай шахрайські електронні листи, які виглядають як повідомлення від законних відправників, наприклад, університету, інтернет-провайдера або фінансової установи. Ці повідомлення зазвичай містять URL-адресу, яка після натискання перенаправляє користувача на підроблений веб-сайт або іншим чином обманює користувача, щоб розкрити особисту інформацію, таку як логін, пароль або інші конфіденційні дані. Ця інформація потім використовується для крадіжки особистих даних та/або грошей.

Щоб скористатися функціями, спочатку потрібно налаштувати службу Cloud Protection Layer (CPL) разом із вашим шлюзом безпеки електронної пошти Barracuda. Ви можете налаштувати Cloud Protection Layer для оцінки та перезапису шахрайських URL-адрес, щоб після натискання користувач безпечно перенаправлявся на дійсний домен або на домен Barracuda з попередженням про шахрайство.

Щоб налаштувати дану функцію, необхідно перейти на сторінку НАЛАШТУВАННЯ ВХІДНИХ ПОШТІВ > Антифішинг та обрати необхідні функції:

Розвідка проти шахрайства – ця функція виявлення фішингу від Barracuda Networks використовує спеціальну байєсівську базу даних для виявлення фішингових шахрайств.

Попередження про зовнішнього відправника – якщо для цього параметра встановлено значення Увімкнено, у верхній частині всіх вхідних електронних листів, що надходять з-за меж вашої організації, з’являється банер, який попереджає користувачів про відкриття вкладень і натискання посилань.

Аналіз намірів – якщо встановлено значення Увімкнено , шар захисту хмари сканує документи, надіслані як вкладення в електронних листах, на наявність посилань. Сканування відбувається під час обробки та доставки повідомлення. Цей

процес перевіряє посилання у вкладеннях на наявність шкідливого вмісту. Якщо в повідомленні виявлено шкідливий вміст, до повідомлення виконується дія « Намір вмісту». Після цього необхідно обрати блокувати чи відкладати повідомлення, що містять шкідливий вміст.

Захист посилань – якщо встановлено значення «Так» , служба автоматично перезаписує оманливу URL-адресу в електронному повідомленні на безпечну URL-адресу Barracuda та доставляє це повідомлення користувачеві.

Користувач натискає URL-адресу, служба оцінює її на дійсність та репутацію та надає інформацію про шкідливий вміст. Якщо домен визначено дійсним, користувача перенаправляють на цей веб-сайт. Якщо URL-адреса підозріла, користувача перенаправляють на сторінку попередження служби захисту посилань Barracuda, яка відображає деталі про заблоковану URL-адресу (рис.3.4).

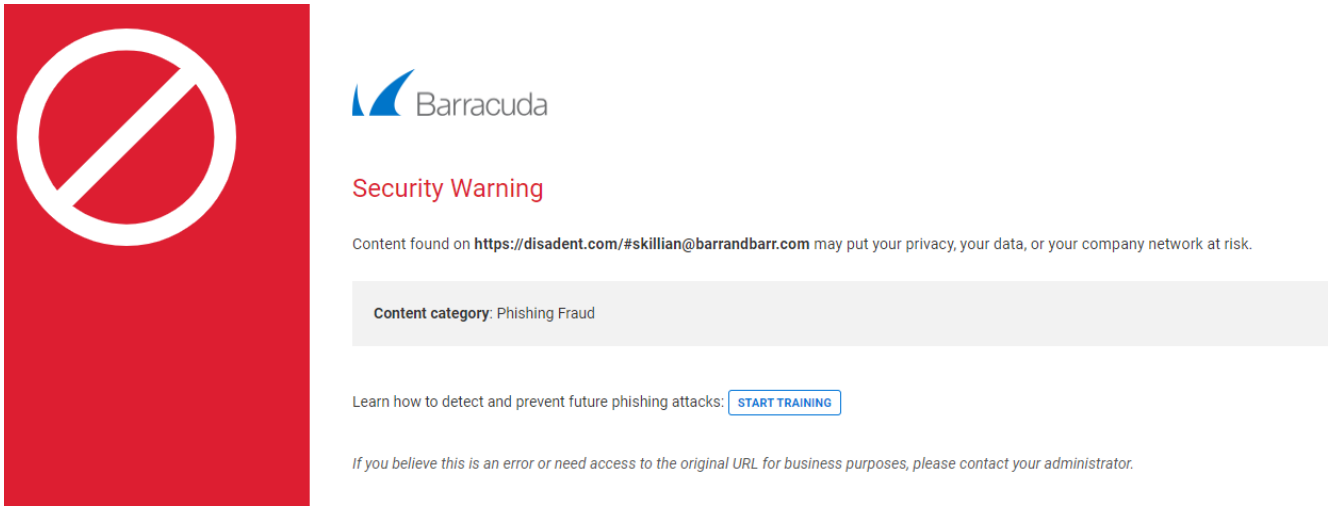

Рис.3.4. Повідомлення шкідливий вміст повідомлення

Контроль швидкості вхідного сигналу

Функція контролю швидкості розсилки Barracuda Email Security Gateway захищає систему від спамерів або спам-програм (також відомих як «спам-боти»), які надсилають великі обсяги електронної пошти на сервер за короткий проміжок часу. Контроль швидкості розсилки налаштовується на сторінці БЛОКУВАННЯ/ПРИЙНЯТТЯ > Контроль швидкості розсилки (рис 3.4).

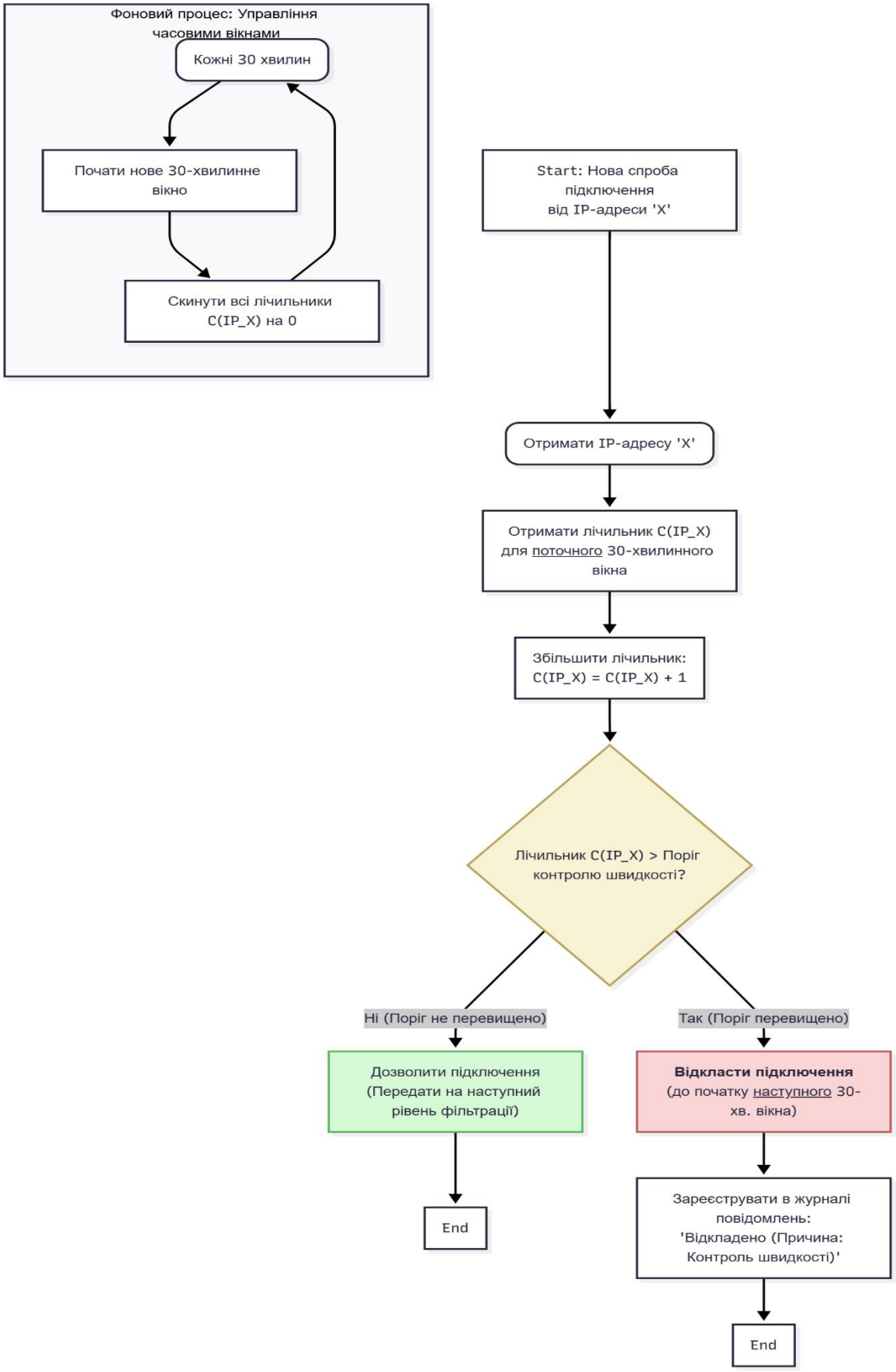

Рис. 3.5. Контроль швидкості вхідного сигналу

Як частина рівня керування підключеннями, механізм контролю швидкості підраховує кількість підключень до шлюзу безпеки електронної пошти Barracuda протягом півгодинного періоду та порівнює це число з порогом контролю швидкості, який є максимальною кількістю підключень, дозволених з будь-якої IP-адреси протягом цього півгодинного періоду. Якщо кількість підключень з однієї IP-адреси перевищує поріг контролю швидкості протягом півгодинного періоду, шлюз безпеки електронної пошти Barracuda відкладає будь-які подальші спроби підключення з цієї конкретної IP-адреси до наступного півгодинного періоду та реєструє кожну спробу як відкладену в журналі повідомлень з причиною контролю швидкості.

Аналіз IP-адрес вхідного зв'язку

Після застосування контролю швидкості, шлюз безпеки електронної пошти Barracuda виконує аналіз IP-адреси, застосовуючи політики тегів, карантину або блокування, які ви налаштовуєте на сторінках БЛОКУВАННЯ / ПРИЙНЯТТЯ .

Після того, як справжнього відправника електронного листа визначено, слід визначити його репутацію та наміри, перш ніж вважати повідомлення дійсним або «не спамом». Найкращий спосіб вирішити обидві проблеми – це знати IP-адреси надійних відправників та пересилачів електронної пошти та додати їх до списку дозволених відомих надійних відправників на шлюзі безпеки електронної пошти Barracuda.

Barracuda Reputation – це база даних, що підтримується Barracuda Central і містить список IP-адрес відомих надійних відправників, а також відомих спамерів або IP-адрес з «поганою» репутацією. Ці дані збираються зі спам-пасток та інших систем в Інтернеті. Історія надсилання, пов’язана з IP-адресами всіх поштових серверів відправника, аналізується для визначення ймовірності надходження легітимних повідомлень з цих адрес. Barracuda Central постійно оновлює Barracuda Reputation.

Виключення IP-адрес із Список блокування репутації Barracuda (BRBL) та інших списків блокування

BRBL та інші списки блокування, які ви вказуєте на сторінці БЛОКУВАННЯ/ПРИЙНЯТТЯ> Репутація IP-адрес, можна змінити, перерахувавши IP-адреси або адреси електронної пошти:

У розділі «Репутація Barracuda», «Діапазон винятків зовнішніх RBL IP-адрес» на сторінці «БЛОКУВАТИ/ПРИЙМАТИ» > «Репутація IP-адрес» . Тут ви можете виключити певні IP-адреси з перевірок RBL, зокрема зі списку блокування репутації Barracuda. Повідомлення з цих IP-адрес підлягатимуть усім іншим перевіркам на спам і віруси.

Вхідний аналіз контенту

Шлюз безпеки електронної пошти Barracuda дозволяє адміністраторам встановлювати власні фільтри вмісту на основі теми листа, заголовків повідомлення, тіла повідомлення та вмісту вкладених файлів. Загалом, адміністраторам не потрібно встановлювати власні фільтри для блокування спаму, оскільки ці форми правил автоматично надсилаються до шлюзу безпеки електронної пошти Barracuda через оновлення Barracuda Energize. Онлайн-довідка для сторінки БЛОКУВАННЯ/ПРИЙНЯТТЯ > Фільтрація вмісту містить посилання на сторінку довідки з регулярних виразів, яка охоплює вирази, які можна використовувати для розширеної фільтрації. HTML-коментарі та теги, вбудовані між символами у вихідному HTML-коді повідомлення, також фільтруються.

Ви можете вказати дії, які потрібно виконувати з повідомленнями, на основі попередньо створених шаблонів у темі або тілі повідомлення. Кредитні картки, номери соціального страхування, конфіденційна інформація, така як номери водійських посвідчень, номери телефонів або терміни дії, а також дані HIPAA можуть автоматично перевірятися та реагуватися шляхом блокування, позначання тегами або карантину вхідних повідомлень.

Виявлення масової розсилки електронною поштою

Для використання цієї функції потрібне використання додаткового шару захисту хмари (CPL) разом із шлюзом безпеки електронної пошти Barracuda .

Багато користувачів підписуються на веб-сайти та списки розсилки, а потім забувають, що вони підписалися, або підписалися несвідомо. Повідомлення електронної пошти, що містять щось, що схоже на посилання для скасування підписки чи інструкцію, можуть вважатися спамом одержувачем, а можуть і ні. Ви можете блокувати ці масові електронні листи, тим самим зменшуючи навантаження на свій поштовий сервер. Налаштуйте виявлення масової розсилки на сторінці НАЛАШТУВАННЯ ВХІДНИХ ПОШТ > Антиспам/Антивірус вашого CPL .

Регіональна політика

Щоб скористатися функцією, потрібно налаштувати безкоштовну службу Cloud Protection Layer за допомогою вашого шлюзу безпеки електронної пошти Barracuda.

Ви можете вибрати опцію «Блокувати повідомлення на основі країни походження» на сторінці «Налаштування вхідних повідомлень» > «Регіональні політики» , що дозволить вам зменшити кількість небажаних вхідних електронних листів. Після вибору країни з випадаючого меню та натискання кнопки «Додати » у таблиці відобразиться код ISO вибраної країни.

Отже, описаний процес захисту електронної пошти дозволив створити технологію захисту корпоративної електронної пошти від сучасних загроз (рис.3.6).

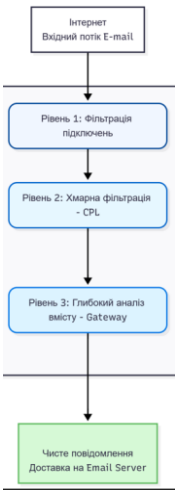

Рис.3.6. Технологія захисту корпоративної пошти

3.2. Рекомендації щодо впровадження заходів захисту корпоративної електронної пошти

Безпека електронної пошти допомагає захистити поверхню атаки організаціївід кіберзагроз, які використовують вектори атаки на облікові записи електронної пошти , такі як фішинг та спам, для отримання несанкціонованого доступу до мережі. Дотримуючись найкращих практик безпеки електронної пошти для кібербезпеки, включаючи облікові записи електронної пошти, організації можуть зменшити поширення шкідливого програмного забезпечення , такого як програми-вимагачі та віруси , щоб запобігти успішним кібератакам.

Електронна пошта є критично важливим компонентом організаційної комунікації, оскільки вона дозволяє користувачам швидко, легко та за допомогою різноманітних пристроїв спілкуватися. Крім того, електронну пошту можна використовувати для надсилання різних типів медіафайлів, а комунікації можна відстежувати, зберігати та організовувати за такими атрибутами, як позначки часу та дати, а також розмір.

Безпека електронної пошти важлива, оскільки вона містить конфіденційну інформацію, використовується всіма співробітниками організації та тому є однією з найбільших цілей атак компанії.

Безпека електронної пошти є важливою через її життєво важливу роль у діловому спілкуванні. Недостатній захист електронної пошти може серйозно вплинути на бізнес, починаючи від втрати критично важливих даних і закінчуючи проблемами з дотриманням вимог. Безпека електронної пошти є життєво важливою для підтримки цілісності організації та якомога раннього виявлення загроз і потенційних порушень для захисту бізнесу.

Забезпечення надійної безпеки електронної пошти передбачає проактивний підхід до захисту конфіденційної та чутливої інформації. Деякі найкращі практики для підвищення безпеки електронної пошти включають:

1. Впровадження багатофакторної автентифікації. Додавання надійної багатофакторної автентифікації додає додатковий рівень безпеки, оскільки ускладнює доступ неавторизованих користувачів до облікових записів електронної пошти, навіть якщо вони мають пароль.

2. Регулярні оновлення та виправлення. Для захисту від найновіших загроз важливо підтримувати системи електронної пошти в актуальному стані, встановлюючи виправлення безпеки та оновлення програмного забезпечення, щойно вони стають доступними.

3. Проводити перевірки безпеки та навчання. Регулярно оцінюйте поточні заходи безпеки електронної пошти та проводьте навчання з безпеки для співробітників. Це допомагає їм розпізнавати потенційні загрози, такі як спроби фішингу та шкідливі вкладення.

4. Розробити план дій. Розробіть чітку стратегію реагування на порушення безпеки. Ця стратегія повинна включати кроки щодо стримування, зменшення та усунення загроз, а також комунікації з постраждалими сторонами.

З вище сказаного можна виділити декілька найкращих практик для посилення безпеки електронної пошти з боку користувача:

- навчання персоналу з питань кібербезпеки;
- використовувати двофакторну автентифікацію;
- покращення керування паролями;
- шифрувати електронні листи;
- впровадження потужних спам-фільтрів для блокування шкідливих електронних листів
- будити обережні з фішинговими електронними листами.

Висновки до розділу 3

1. Barracuda Email Security Gateway забезпечує гнучкість у впровадженні, пропонуючи щонайменше два основні варіанти розгортання — у демілітаризованій

зоні або за корпоративним брандмауером. Це дозволяє організаціям інтегрувати шлюз у свою існуючу мережеву інфраструктуру з мінімальними змінами, обираючи між прямим прийомом трафіку або перенаправленням портів.

2. Технологія захисту Barracuda реалізує фундаментальний принцип кібербезпеки — ешелоновану оборону. Замість того, щоб покладатися на один механізм, шлюз створює послідовну "воронку" фільтрів.

3. Технологія фільтрації є неефективною без підтримки організаційних політик та навчання користувачів. Впровадження Barracuda Email Security Gateway (технічний захід) повинно невід'ємно супроводжуватися впровадженням MFA, регулярним навчанням персоналу розпізнаванню фішингу та розробкою плану реагування на інциденти.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні результати:

1. Аналіз показав, що корпоративна електронна пошта залишається критично важливим інструментом для бізнес-комунікацій. Водночас вона є домінуючим вектором кібератак — 94% шкідливих програм доставляються саме через e-mail, що створює фундаментальну проблему безпеки для сучасних організацій.

2. Ландшафт загроз значно еволюціонував від простого спаму до складних, фінансово руйнівних атак. Сучасні загрози, такі як компрометація ділової пошти (BEC), програми-вимагачі (Ransomware) та цільовий фішинг, вимагають захисту, що виходить далеко за межі базової антивірусної фільтрації.

3. Захист корпоративної пошти є не лише технічною необхідністю, але й суворою юридичною та регуляторною вимогою. Міжнародні (ISO 27001/27002, GDPR) та галузеві (PCI DSS) стандарти вимагають від організацій впровадження конкретних технічних і організаційних контролів (MFA, DLP, шифрування, аудит, резервне копіювання).

4. Порівняльний аналіз провідних технологій (Proofpoint, Check Point, Trend Micro, Barracuda) показав, що традиційні шлюзи безпеки є недостатніми для боротьби з сучасними загрозами. Найбільш ефективною є комплексна, інтегрована платформа, яка поєднує захист шлюзу з AI-аналізом (для BEC), API-інтеграцією (для ATO) та інтегрованим навчанням персоналу.

5. Технологія поєднує традиційні сигнатурні методи (бази вірусів, RBL, SPF-автентифікація) з передовими евристичними та поведінковими механізмами. Такі функції, як "Суперкомп'ютерна мережа Barracuda Antivirus" для поліморфних вірусів, "Прогнозне профілювання відправника" та "Аналіз намірів" дозволяють виявляти нові, раніше невідомі (zero-day) загрози, фішинг та спам-кампанії, які не мають відомих сигнатур.

6. Ефективність багатьох функцій Barracuda Email Security Gateway напряму залежить від постійного оновлення даних у режимі реального часу. Це перетворює шлюз з ізольованого пристрою на частину глобальної мережі виявлення загроз.

7. Комплексний захист вхідних та вихідних потоків, які захищають інфраструктуру компанії від атак, захищають репутацію компанії від розсилки спаму зі скомпрометованих акаунтів та запобігають витоку конфіденційних даних, забезпечуючи їх передачу через захищені канали.

8. Розглянутий набір характеристик Email Gateway Defense створює цілісну, глибоко інтегровану систему безпеки, що здатна протидіяти широкому спектру загроз на кожному етапі життєвого циклу електронного повідомлення — від початкової спроби з'єднання до фінальної доставки чи шифрування.

9. Barracuda Email Security Gateway забезпечує гнучкість у впровадженні, пропонуючи щонайменше два основні варіанти розгортання — у демілітаризованій зоні або за корпоративним брандмауером. Це дозволяє організаціям інтегрувати шлюз у свою існуючу мережеву інфраструктуру з мінімальними змінами, обираючи між прямим прийомом трафіку або перенаправленням портів.

10. Технологія захисту Barracuda реалізує фундаментальний принцип кібербезпеки — ешелоновану оборону. Замість того, щоб покладатися на один механізм, шлюз створює послідовну "воронку" фільтрів.

11. Технологія фільтрації є неефективною без підтримки організаційних політик та навчання користувачів. Впровадження Barracuda Email Security Gateway (технічний захід) повинно невід'ємно супроводжуватися впровадженням MFA, регулярним навчанням персоналу розпізнаванню фішингу та розробкою плану реагування на інциденти.

Таким чином, Barracuda Email Security Gateway являє собою комплексну, гнучку та багаторівневу технологічну платформу. Її ефективність базується на комбінації фільтрів різного рівня (від IP-репутації до "пісочниці") та тісній інтеграції з хмарними сервісами. У поєднанні з надійними організаційними політиками та навчанням персоналу, ця технологія дозволяє створити цілісний та потужний захист корпоративної електронної пошти від широкого спектру сучасних кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Email Security: 7 Biggest Threats. Keepnet Labs. URL: https://keepnetlabs.com/blog/email-security-7-biggest-threats (дата звернення: 07.11.2025).

2. Global Cybersecurity Outlook 2025: Digest. World Economic Forum, 2025. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/digest/ (дата звернення: 07.11.2025).

3. Introduction to Email Security. SecureDebug. URL: https://securedebug.com/email-security-protect-organization-communication/ (дата звернення: 07.11.2025).

4. Trustworthy Email : Special Publication (NIST SP) 800-177 Rev. 1. National Institute of Standards and Technology, 2022. URL: https://csrc.nist.gov/publications/detail/sp/800-177/rev-1/final (дата звернення: 07.11.2025).

5. Leader in the 2024 Gartner® Magic Quadrant™ for Email Security. Gartner, 2024.

6. Gartner Magic Quadrant for Email Security Platforms. Gartner, 2024. URL: https://www.gartner.com/en/documents/ 6019335 (дата звернення: 07.11.2025).

7. Захист електронної пошти Barracuda Email Gateway. Barracuda Campus. URL: https://campus.barracuda.com/product/emailgatewaydefense/ (дата звернення: 10.11.2025).

8. Barracuda Email Security Gateway: Datasheet / Barracuda Networks, Inc. 2024. URL: https://www.barracuda.com/products/email-protection/email-security-gateway/resources (дата звернення: 10.11.2025).

9. Архітектура та технології Barracuda Total Email Protection : White Paper / Barracuda Networks, Inc. 2023. 12 с.

10. Barracuda Cloud Protection Layer (CPL) Overview / Barracuda Campus: Documentation. URL:

https://campus.barracuda.com/product/emailsecuritygateway/doc/74954005/barracuda-cloud-protection-layer/ (дата звернення: 05.12.2025).

11. Advanced Threat Protection (ATP) / Barracuda Campus: Technology. URL: https://campus.barracuda.com/product/emailsecuritygateway/doc/74953930/advanced-threat-protection-atp/ (дата звернення: 05.12.2025).

12. Outbound Mail Filtering and Encryption / Barracuda Email Security Gateway Administrator Guide. Barracuda Networks, Inc., 2024.

13. Understanding the Barracuda Email Security Gateway Architecture / Barracuda Technical Library. 2023. URL: https://www.barracuda.com/resources/library (дата звернення: 05.12.2025).

14. Суботенко Р.Р. Підходи до захисту корпоративної пошти організації. актуальні проблеми кібербезпеки. *Актуальні проблеми кібербезпеки:* матеріали всеукраїнської наук.-практ. конф., м. Київ: ДУІКТ, 29 жовт. 2025р. Київ. С 39-40.