|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | |
| **НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ** | | | | | | | |
|  |  |  | | |  | |  |
| **КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ** | | | | | | | |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
| Пояснювальна записка | | | | | | | |
| до бакалаврської роботи | | | | | | | |
|  | на тему: | | | | | |  |
| **«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИЩЕНОГО ОБМІНУ ЕЛЕКТРОННОЮ ПОШТОЮ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ»** | | | | | | | |
|  | | | | | | | |
|  | | | | | | | |
|  | | | | | | | |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  |  | Виконав студент 4 курсу, групи БСД-41 | | | | | |
|  |  | спеціальності 125 Кібербезпека | | | | | |
|  |  | освітньо-професійної програми «Інформаційна та | | | | | |
|  |  | кібернетична безпека» | | | | | |
|  |  | (шифр і назва спеціальності) | | | | | |
|  |  | Шинкаренко В.А. | | | | | |
|  |  | (прізвище та ініціали) | | | | | |
|  |  | Керівник | Бойко А.О. | | | | |
|  |  |  | | | (прізвище та ініціали) | | |
|  |  | Рецензент | |  | | | |
|  |  | (прізвище та ініціали) | | | | | |
|  |  | Нормоконтролер | | | |  | |
|  |  |  | | | (прізвище та ініціали) | | |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  |  |  | | |  | |  |
|  | КИЇВ – 2023 | | | | | |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | | | |
| Інститут | ННІЗІ | | | | |  | |  | |  |
| Кафедра | Інформаційної та кібернетичної безпеки | | | | | | | | | |
| Ступінь вищої освіти | | | | Бакалавр | | | |  | |  |
| Спеціальність | | 125 Кібербезпека | | | | | |  | |  |
| Освітня програма | | | Інформаційна та кібернетична безпека | | | | | | | | |
|  |  | | | | |  | |  | |  |
|  |  | | | | |  | |  | |  |
|  |  | | | | |  | | ЗАТВЕРДЖУЮ | | |
|  |  | | | | |  | | Завідувач кафедри ІКБ | | |
|  |  | | | | |  | |  | | Гайдур Г.І. |
|  |  | | | | |  | | “\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | |
|  |  | | | | |  | |  | |  |
|  |  | | | | |  | |  | |  |
|  | **З А В Д А Н Н Я** | | | | | | | | |  |
|  | **НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ** | | | | | | | | |  |
|  |  | | | | |  | |  | |  |
| Шинкаренку Владиславу Анатолійовичу | | | | | | | | | | |
| (прізвище, ім’я, по батькові) | | | | | | | | | | |
| 1. Тема бакалаврської роботи: | | | | | «Дослідження шляхів та розробка | | | | | | |
| рекомендацій щодо захищеного обміну електронною поштою в корпоративній | | | | | | | | | | |
| інформаційній системі» | | | | | | | | | | |
| керівник бакалаврської роботи | | | | | | Дмітрієв Вячеслав Євгенович, ст.викладач | | | | |
|  |  | | | | | (прізвище, ім’я, по батькові, науковий ступінь, вчене звання) | | | | |
| затверджені наказом закладу вищої освіти від «\_\_\_ » \_\_\_\_\_\_\_\_2023 року № \_\_\_\_. | | | | | | | | | | |
|  |  | | | | |  | |  | |  |
| 2. Строк подання студентом бакалаврської роботи | | | | | | | | | 28.05.2023 р. | |
|  |  | | | | |  | |  | |  |
| 3. Вихідні дані до бакалаврської роботи | | | | | | |  | | |  |
| корпоративна інформаційна система; | | | | | | | |  | |  |
| захищений обмін електронною поштою; | | | | | | | | | |  |
| наукова та технічна література, експлуатаційна документація, нормативні | | | | | | | | | | |
| документи, міжнародні стандарти. | | | | | | | |  | |  |
|  |  | | | | |  | |  | |  |
| 4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) | | | | | | | | | | |
| 1. Актуальність проблеми захищеного обміну електронною поштою. | | | | | | | | | | |
| 2. Актуальні загрози електронної пошти. | | | | | | | | | | |
| 3. Методи та засоби захищеного обміну електронної пошти. | | | | | | | | | | |
| 4. Рекомендації щодо захисту корпоративної електронної пошти. | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. Перелік графічного матеріалу | | | | |  | |  | |
| 1. Тема бакалаврської роботи. | | | | | | | | |
| 2. Об’єкт, предмет, мета та наукові завдання дослідження. | | | | | | | | |
| 3. Результати аналізу проблеми захищеного обміну електронною поштою | | | | | | | | |
| 4. Результати аналізу методів та засобів захищеного обміну електронною поштою. | | | | | | | | |
| 5. Рекомендації щодо захисту корпоративної електронної пошти. | | | | | | | | |
| 7. Висновки за результатами роботи. | | | | | | | | |
|  | | | | | | | | |
| 6. Дата видачі завдання | | | 15.02.2023р. | | | | | |
|  | |  | |  |  | |  | |
|  | | **КАЛЕНДАРНИЙ ПЛАН** | | | | |  | |
|  | |  | |  |  | |  | |
| №  зп | Назва етапів  бакалаврської роботи | | | | | Строк виконання етапів бакалаврської роботи | | Примітка |
| 1. | Визначення актуальності проблеми захищеного обміну електронною поштою в корпоративній інформаційній системі. | | | | | 15.02.2023 р. | |  |
| 2. | Аналіз наукової та технічної літератури з питань теми бакалаврської роботи. | | | | | 01.03.2023 р. | |  |
| 3. | Аналіз методів та засобів захисту електронної пошти | | | | | 21.03.2023 р. | |  |
| 4. | Розроблення рекомендацій щодо захисту корпоративної електронної пошти. | | | | | 11.04.2023 р. | |  |
| 5. | Оформлення результатів дослідження. | | | | | 12.05.2023 р. | |  |
| 6. | Підготовка доповіді до захисту. | | | | | 28.05.2023 р. | |  |
|  | | | | | |  | |  |
|  | |  | | Студент | Шинкаренко В.А. | | | |
|  | |  | |  | (підпис) | | прізвище та ініціали | |
|  | |  | |  |  | |  | |
| Керівник бакалаврської роботи | | | | |  | | Бойко А.О. | |
|  | |  | |  | (підпис) | | прізвище та ініціали | |
|  | |  | |  |  | |  | |

**ВІДГУК РЕЦЕНЗЕНТА**

на бакалаврську роботу

студентаШинкаренка Владислава Анатолійовича

на тему: «Дослідження шляхів та розробка рекомендацій щодо захищеного обміну електронною поштою в корпоративній інформаційній системі»

**Актуальність:** Найбільш популярний спосіб ділового листування – електронна пошта. Месенджери та засоби візуальної комунікації поки що не можуть скласти їй конкуренцію, оскільки є насамперед інструментом зручного швидкого зв'язку та вирішення поточних питань. Замінити ділові електронні листи вони поки що не в змозі. Поштовими каналами щодня передаються сотні листів, багато з яких містять фінансову, конфіденційну інформацію або відомості про створення нових зразків продукції. Звичайно, все це може зацікавити конкурентів, і не лише їх. Електронна пошта приваблює хакерів, шахраїв та різноманітних аферистів. Тому у загальній стратегії захисту корпоративної інформації чимало місця займають заходи, спрямовані на те, щоб захистити поштову скриньку від злому.

**Позитивні сторони:**

1. Робота дозволяє досить повно оцінити загальний стан, характеристику, сутність та структуру поставленої проблеми.

2. Досліджено важливе питання розробки рекомендацій щодо забезпечення захищеного обміну електронною поштою.

3. Текст викладено достатньо грамотно, послідовно.

**Недоліки:**

1. У бакалаврській роботі не приведено детальний опис алгоритмів, за якими працюють протоколи поштових сервісів.

2. Слід було провести аналіз додаткової технічної літератури по темі бакалаврської роботи.

**Висновок:** Враховуючи недоліки, бакалаврська робота заслуговує оцінку **добре**, а студент **Шинкаренко В.А.** – присвоєння кваліфікації: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

|  |  |  |
| --- | --- | --- |
| Якість роботи | | Підпис рецензента (\_\_\_\_\_\_\_\_\_\_\_\_\_\_)  Підпис засвідчую  Підпис особи, що засвідчує (\_\_\_\_\_\_\_\_\_\_\_\_) |
| Виконано на замовлення підприємства |  |
| Виконано за тематикою НДР |  |
| Виконано з макетом |  |
| Виконано з застосуванням ЕОМ та МПТ | √ |
| Має практичну цінність | √ |
| Проект-частина комплексної теми |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | |
| **ПОДАННЯ**  **ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**  **ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ** | | | | | | | | |
| Направляється студент | | Шинкаренко В.А | | | до захисту бакалаврської роботи | | | |
|  | | (прізвище та ініціали) | | |  | | | |
| спеціальності 125 Кібербезпека | | |  | | |  | |  |
| освітньо-професійної програми | | | Інформаційна та кібернетична безпека | | | | | |
|  |  | | (шифр і назва спеціальності) | | | | | |
| на тему: | «Дослідження шляхів та розробка рекомендацій щодо захищеного обміну | | | | | | | |
| електронною поштою в корпоративній інформаційній системі». | | | | | | | | |
| Бакалаврська робота і рецензія додаються. | | | | | |  | |  |
| Директор інституту | | |  | | | Савченко В.А. | | |
| (підпис) (прізвище та ініціали) | | | | | | | | |
|  |  | |  | | |  | |  |
|  | **Довідка про успішність** | | | | | | |  |
| Шинкаренко В.А. | | | за період навчання в інституті | | | | | |
| (прізвище та ініціали студента) | | |  | | |  | |  |
| ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:  національною шкалою: відмінно \_\_\_\_%, добре \_\_\_\_%, задовільно \_\_\_\_%;  шкалою ECTS: А \_\_\_\_%; В \_\_\_\_%; С \_\_\_\_%; D \_\_\_\_%; Е \_\_\_\_%. | | | | | | | | |
| Секретар інституту, факультету (відділення) | | | | | |  | | Берестяна Т.В. |
|  |  | |  | | | (підпис) | | (прізвище та ініціали) |
|  | **Висновок керівника бакалаврської роботи** | | | | | | |  |
| Студент ***Шинкаренко В.А.*** обрав тему роботи, метою якої було дослідження методів та засобів захищеного обміну електронною поштою в корпоративній інформаційній системі. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Шинкаренко В.А. показав добру теоретичну та практичну підготовку. Роботу виконував сумлінно, акуратно та вчасно за планом.  Все це дозволяє оцінити виконану бакалаврську роботу студента Шинкаренка Владислава Анатолійовича на оцінку **«добре»** та присвоїти йому кваліфікацію: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека. | | | | | | | | |
| Керівник бакалаврської роботи | | | | | |  | | Бойко А.О. |
|  |  | |  | | | (підпис) | | (прізвище та ініціали) |
|  |  | |  | | | “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | |
|  | **Висновок кафедри про бакалаврську роботу** | | | | | | |  |
| Бакалаврська робота розглянута. Студент | | | | Шинкаренко В.А. | | | | |
|  |  | |  | (прізвище та ініціали) | | | | |
| Завідувач кафедри Інформаційної та кібернетичної безпеки | | | | | | |  |  |
| (назва) | | | | | | | | | |
|  |  | |  | | |  | | Гайдур Г.І. |
|  |  | | (підпис) | | | (прізвище та ініціали) | | |
| “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | |  | | |  | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **РЕФЕРАТ** | | | | |
|  |  |  |  |  |
|  |  |  |  |  |
| Текстова частина бакалаврської роботи: 49 сторінок, 10 джерел.  *Об’єкт дослідження* – забезпечення безпеки корпоративної електронної пошти.  *Предмет дослідження* – методи та засоби забезпечення безпеки електронної пошти.  *Мета роботи* – розробити рекомендації щодо застосування методів та засобів забезпечення безпеки корпоративної електронної пошти.  *Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.  В роботі приведено основні відомості про електронну пошту, загрози витоку конфіденційної інформації поштою та основні вектори атак.  Проаналізовано різні види загроз та наведено їх класифікацію.  Досліджено методи та засоби забезпечення безпеки корпоративної електронної пошти.  Досліджено можливості програмного комплексу Cisco Secure Email.  На основі досліджень проведених в роботі розроблено рекомендації щодо застосування методів та засобів для забезпечення безпеки корпоративної електронної пошти.  ЕЛЕКТРОННА ПОШТА, ПРОТОКОЛИ, МЕРЕЖА, ХМАРНІ ТЕХНОЛОГІЇ, ЗАГРОЗИ, ЗАХИСТ | | | | |

**ЗМІСТ**

[**ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 8**](#_Toc104132798)

[**ВСТУП 9**](#_Toc104132799)

[**1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕЛЕКТРОННОЇ ПОШТИ 11**](#_Toc104132800)

[1.1. Поняття та елементи електронної пошти 11](#_Toc104132801)

[1.2. Загрози електронної пошти 15](#_Toc104132802)

[1.3. Проблеми, які вирішує захист електронної пошти 18](#_Toc104132803)

[2 **ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОЧТИ** 21](#_Toc104132804)

[2.1. Безпечні протоколи 21](#_Toc104132805)

[2.2.1. PGP 21](#_Toc104132806)

[2.2.2. S/MIME 22](#_Toc104132807)

[2.2.3. HTTPS 22](#_Toc104132808)

[2.2. Рішення для захисту електронної пошти 23](#_Toc104132809)

[3 **РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ** 34](#_Toc104132810)

[3.1. Забезпечення безпеки електронної пошти 34](#_Toc104132811)

[3.2. Способи захисту електронної пошти 35](#_Toc104132812)

[3.3. Огляд Cisco Secure Email 40](#_Toc104132813)

[**ВИСНОВКИ 55**](#_Toc104132814)

[**ПЕРЕЛІК ПОСИЛАНЬ 57**](#_Toc104132815)

[**ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ) 58**](#_Toc104132816)

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

GSM – Global System for Mobile Communications

ЕОМ – Електронна обчислювальна машина

SMTP – Simple Mail Transfer Protocol

POP3 – Post Office Protocol

HTML – HyperText Markup Language

ЕЦП – Електронний цифровий підпис

DoES – Denial of Email Service

PGP – Pretty Good Privacy

S/MIME – Secure/Multipurpose Internet Mail Extension

HTTPS – HyperText Transfer Protocol Secure

DLP – Data Leak Prevention

URL – Uniform Resource Locator

# ВСТУП

Сьогодення відзначається проривною епохою злетів різноманітних технологій та інтелектуальних мобільних пристроїв, мережа Інтернет залишається основою комунікацій у повсякденній діяльності. Інтернет дає змогу цифровим пристроям, таким як смартфони та смарт-пристрої, підключатися до мережі доступу до віддалених ресурсів та хмарних середовищ, а отже – і до кінцевого користувача.

Сьогодні постійно зростаюча кількість взаємодій між кінцевими користувачами, такими організаціями як: банки та уряди, компанії та підприємства, навчальні заклади та школи здійснюється в електронному вигляді. Тому і не дивно, що найвидатнішим досягненням 21 століття вважається розширення мережі Інтернет по всьому світу та вражаюче зростання цифрових мобільних мереж (наприклад, GSM).

Кількість користувачів обох систем, які не існувало або обмежувались дослідницькими колами лише на початку 90-х років, зараз становить близько мільярда. Успіх цих нових технологій можна віднести до ряду властивих переваг цифрових систем: цифрова інформація практично нечутлива до шуму, вона може бути відправлена на великі відстані, скопійована або модифікована без втрати якості.

Проте ті самі властивості, які роблять настільки привабливими цифрові інформаційні системи, роблять їх особливо вразливими до широкого спектру зловживань. У традиційній поштовій системі одержувач листа може виконувати деякі прості тести, щоб переконатися в тому, що повідомлення не було скомпрометовано. Він може перевірити, що (герметичний) конверт не був відкритий, вивчати, чи відповідає рукопис чи підпис, а також шукати аномалії, які можуть вказувати на те, що частини були переписані. Всі ці тести будуються на припущенні, що будь-які маніпуляції з повідомленням обов'язково залишать деякі сліди на його фізичному носії.

На жаль, це саме те, що цифрові системи намагалися уникнути. Як скоро було зрозумілим, єдиний спосіб захистити цифрові системи, не жертвуючи їх перевагами, полягає в тому, щоб перетворити інформацію таким чином, щоб вона захищала себе незалежно від того, як вона передається або зберігається.

Слід зазначити, що багато питань безпеки, порушених сучасними інформаційними технологіями, не є новими. Швидко розширюючи мережі, з'єднуються все більше і більше пристроїв по всьому світу, збільшуючи як кількість цікавих цілей, так і кількість потенційних зловмисників. Крім того, прослуховування цих мереж набагато простіше за рахунок розповсюдження безпроводових точок доступу.

Нарешті, зростаюча складність засобів зв'язку та інформаційних систем робить їхню безпеку набагато складнішою, що призводить до ряду досить несподіваних нових проблем, таких як комп'ютерні віруси та хробаки, які здатні не просто ушкодити електронні документи, а і створити прецеденти для подальшого розповсюдження та зараження інших мереж спеціального призначення.

Тому тема роботи, яка присвячена дослідженню шляхів, а також розробці рекомендацій щодо організації захищеного обміну електронною поштою є актуальною.

# 1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕЛЕКТРОННОЇ ПОШТИ

## **1.1. Поняття та елементи електронної пошти**

Електронна пошта є одним із найстаріших сервісів глобальної мережі, доступний усім її користувачам. Електронна пошта є універсальним засобом віртуальної взаємодії не вимогливим до ресурсів, який дає можливість обмінюватися інформацією та спілкуватися практично на будь-якій ЕОМ, навіть на найстарішій. За допомогою електронної пошти можна легко писати листи, повідомлення, обмінюватися в мережі фотографіями та малюнками через звичайний веб-браузер або застосовуючи спеціальне програмне забезпечення. Вона дуже схожа на роботу звичайної пошти, але для використання електронної пошти користувачеві потрібен доступ до інтернету, електронна поштова скринька, обліковий запис на будь-якому поштовому сервері.

Електронна пошта (mail, e-mail, email від electronic mail – англійська) – це інформаційна технологія, що надає послуги користувачам з обміну електронними повідомленнями («електронними листами») по розподілених комп'ютерних мережах та у глобальній мережі Інтернет. Якщо розглянути склад та основні принципи функціонування електронної пошти, можна побачити велику кількість запозичень, та її принципи повторюють принципи функціонування традиційної пошти. Від звичайної пошти перейшла велика кількість термінів (лист, поштова скринька, конверт та інші), а крім цього вона успадкувала і великий набір позитивних та негативних характеристик - починаючи з простоти та надійності використання та закінчуючи відсутністю будь-яких гарантій.

Основне призначення електронної пошти – це обмін листами, повідомленнями. Повідомлення e-mail складається із трьох частин: заголовка; кодового конверту; тіла повідомлення: текст повідомлення з вкладенням. Заголовок листа містить тему листа, хто відправник, адресу відправника, тобто кому буде надіслано відповідь цього листа після натискання кнопки - /Відповісти/. Крім цього заголовок містить безліч іншої службової інформації, яка зазвичай прихована від очей простих користувачів за непотрібністю, а лист для нього представляється у легкочитаному вигляді. Заголовки оформляються за двома основними стандартами: RFC 822 та MIME.

Структура заголовка має такий вигляд:

From - від кого надійшло послання (електронна адреса)

To - кому адресовано (електронна адреса)

Cc - кому ще направлено (електронні адреси)

Subject - тема повідомлення (текст)

Date - дата та час відправлення повідомлення (DateTime)

Message-Id - унікальний ідентифікатор послання, який надає сервер автоматично

Reply-To - як правило адреса абонента, якому надійде відповідь на лист.

Електронна адреса є вказівкою на бажаного одержувача листа, і в побуті зазвичай і називається просто - e-mail. Він складається із двох частин, які відокремлені між собою символом @ («собака»). У другій частині адреси (після @) записується назва поштового сервера, де була зареєстрована електронна скринька користувача. Перша частина електронної поштової адреси містить безпосередньо саме облікове ім'я користувача даному поштовому сервері.

Електронна поштова скринька – це дисковий простір, що виділяється на поштовому сервері для зберігання листів користувача (вхідних, надісланих, чернеток та ін.). Розмір електронної поштової скриньки зазвичай обмежений, але подібні обмеження можуть і відсутні. Крім цього, багатьма поштовими сервісами передбачається можливість налаштувати сервер так, що одній поштовій скриньці будуть відповідати кілька адрес електронної пошти і навпаки, або просто прикріпити до однієї скриньки кілька інших незалежно від постачальника поштових послуг.

Обліковий запис користувача складається з набору особистої інформації про користувача (ім'я користувача, логін, пароль, інша службова інформація), яка має бути конфіденційною та надійно зберігатися на поштовому сервері у спеціалізованій базі даних. При цьому одного облікового запису цілком може відповідати теоретично кілька електронних адрес та поштових скриньок.

В даний час існує кілька способів отримати поштову скриньку в мережі Internet і увійти в безмежний світ електронного спілкування.

Так наприклад, багато провайдерів, коли реєструють нового клієнта, зазвичай, надають безкоштовну поштову скриньку, але можливо з деякими обмеженнями по місткості. Переважна більшість користувачів інтернету все-таки користуються послугами найбільших поштових сервісів. Вони дозволяють своїм користувачам реєструвати поштові скриньки в будь-якій кількості та безкоштовно, користуватися якими дуже зручно та просто хоч за допомогою поштових клієнтів (що використовують протоколи SMTP та POP3), хоч через звичайні Web-браузери.

Більшість користувачів під час роботи з електронною поштою користуються звичайними веб-браузерами. Цей спосіб має свої переваги, наприклад:

- листи можуть бути на сервері необмежений час без необхідності їх завантажувати;

- може працювати у будь-яких операційних системах;

- отримання листів «на лету», а чи не лише при підключенні до POP3-серверу;

- мають безліч додаткових «примочок» у вигляді будь-яких тулбарів, розташованих у вигляді панелей у вікні браузера з купою додаткових функцій, що дають можливість стежити за поштою в режимі реального часу;

- більшість Web-сервісів електронної пошти мають у своєму розпорядженні додаткові сервіси для зберігання файлів, новини, хостинг, інформація та інше;

- нема чого освоювати інтерфейс двох програм (і браузера, і поштового клієнта);

- можна перевіряти кореспонденцію у будь-якому місці, де є комп'ютер та доступ до Інтернету, без наявності додаткових поштових програм;

- автоматичні фільтри від спаму та засоби антивірусного захисту, що не потребують настроювання.

Поштовий клієнт - програма, що встановлюється на комп'ютері користувача, що взаємодіє з поштовими серверами за стандартними протоколами та служить для отримання, читання, створення, надсилання електронних листів в Інтернеті. Слід зазначити, що працювати з електронною поштою за допомогою поштового клієнта дуже зручно та швидко. Крім цього, він незамінний при обмеженому доступі до інтернету, коли дорога кожна хвилина. Отже, його перевагами є такі:

- значна економія інтернет-трафіку, оскільки немає завантаження самого сайту поштового сервісу з усім його візуальним оформленням, рекламою, презентаціями та іншим абсолютно непотрібним вмістом;

- підтримка автономної роботи, тобто. можна читати старі листи з відсутністю підключення до Інтернету;

- містять різноманітні інструменти для сортування повідомлень та перевірки орфографії, шаблони, вбудований текстовий редактор та ін.;

- можна організовувати роботу з електронною кореспонденцією так, як це подобається користувачеві, а не фантазії Web-дизайнера;

- можливість настроїти фільтри від спаму, тобто. можна ще більше берегти трафік та нерви;

- зручніше у використанні, коли багато скриньок різних поштових серверах, ніж прив'язувати в Web-інтерфейсі.

Сам процес реєстрації нової поштової скриньки дуже простий. Заходимо на поштовий сервіс і тиснемо /Реєстрація/. Спочатку треба вигадати собі логін. Логін є унікальним псевдонімом користувача, щоб його дізнавалися сервіси, де він зареєстрований. Логін повинен бути складений лише з цифр та букв латинського алфавіту (при цьому регістр букв не враховується). Логін також може містити точки та дефіси (які рівнозначні), але не допускаються пробіли та інші символи. Можна також використовувати своє ім'я, назву фірми, свій сайт чи блог тощо. Зазвичай поштові послуги радять користувачам можливі варіанти незайнятих електронних адрес. Оскільки на поштових серверах зареєстровані мільйони абонентів, можливо, доведеться деякий час попрацювати, щоб підібрати відповідний логін, так як він має бути унікальним. Далі в обов'язкових та необов'язкових полях реєстрації необхідно забити свої дані: ім'я, прізвище, рік народження та інші.

## **1.2. Загрози електронної пошти**

Практично кожна працююча людина в нашій країні має свою електронну поштову адресу. Електронна пошта – найлегший спосіб для своєчасної передачі інформації та ведення ділових переговорів. Однак надання співробітникам компанії доступу до Інтернету з можливістю обміну електронними поштовими повідомленнями незмінно спричинить і загрози, пов'язані з безпекою корпоративної мережі. Нижче наведено перелік деяких атак, яким схильні сьогодні організації, що використовують поштові e-mail-системи:

* трояни;
* цільовий та нецільовий спам;
* фішинг організацій;
* Backscatter – bounce-повідомлення;
* Email Bombing – поштове бомбардування;
* Denial of Email Service (DoES) - відмова поштової служби;
* експлуатація (експлойти) відкритих релеїв.

Простий погляд на Web-сайти більшості компаній може дати атакувальному зловмиснику список e-mail-адрес для реалізації, наприклад, фішинг-атаки, розсилки шкідливого вкладення або посилання на хакерський сайт, після відвідування якого на комп'ютери користувачів непомітно буде встановлено програмне забезпечення, яке їх краде паролі до корпоративних ресурсів або іншу не менш цінну персональну інформацію.

Якщо навіть електронна поштова адреса генерального директора не викладена на веб-сайті компанії, це ще не означає, що вона не може стати метою для атаки. Більшість компаній дотримуються стандартного формату e-mail-адрес - ім'я.прізвище@компанія.ш. Збираючи та порівнюючи цю інформацію з Web-сайту, різних документів, що випускаються компанією для публічного використання, прес-релізів, новин тощо, хакер легко вгадає легітимні поштові адреси, прийняті в тій чи іншій організації, включаючи адреси вищого керівництва.

Атака на МТА

Якщо зловмисники визначили мету, далі вони можуть діяти кількома шляхами. Найперша атака, що використовує функціонал e-mail-повідомлень, була націлена проти вразливостей так званого mail transfer agent (МТА), або поштового сервера, програми, що відповідає за доставку повідомлення на певний комп'ютер. Sendmail був першим і найпопулярнішим МТА на зорі виникнення Інтернету, і в 1988 р. некоректність у його роботі дозволила черв'ю Morris поширитися і наповнити собою значну частину Всесвітнього павутиння. Хтось скаже, що це було двадцять років тому і подібні загрози зжили себе як вигляд, проте не радимо поспішати з висновками. Досить зайти на офіційний сайт виробника будь-якого, навіть найсучаснішого, поштового сервера (наприклад, Microsoft Exchange), щоб виявити, що він може містити в собі вразливості.

Атаки на клієнтські поштові програми

Іншою мішенню для атаки можуть бути обрані поштові програми, такі як Microsoft Outlook або Lotus Notes. Поштовий клієнт, як і будь-яка інша програма, що обробляє вхідні дані, може містити в собі вразливість. З точки зору програмування можна впевнено сказати, що чим складніше розробляється програма і чим більше вона буде підтримувати різні для користувачів нововведення, тим більша ймовірність того, що в її програмному коді будуть допущені помилки. Можливості вкладень у текст поштових повідомлень графічних зображень, закодованої інформації, а також ускладнення функціоналу поштових клієнтів, хоч би якими цікавими вони здавалися пересічному користувачеві, фахівцям з інформаційної безпеки лише збільшують фронт робіт. У 2003 р. перегляд зібраного спеціальним чином поштового повідомлення у форматі html.

Атака через поштові вкладення

У 1999 р. Melissa (перший успішний черв'як, що використовував вкладення до e-mail) підірвав Інтернет і змусив усвідомити ІТ-департаменти компаній по всьому світу всю серйозність загроз, які таять у собі поштові вкладення. До цього лише деякі компанії обмежували пересилання виконуваних програм, тобто ехе-файлів поштою. Після черв'яка Melissa організації були змушені адаптувати свої системи безпеки до ще більш складної загрози - тепер вже навіть звичайний файл даних може потенційно містити в собі шкідливий код! В результаті - зараз будь-яке вкладення має бути проскановано, перш ніж воно потрапить до корпоративної мережі. У більшості випадків файли, що виконуються, можуть бути видалені з поштових повідомлень, але документи MS Office, PDF-файли, графічні зображення.

Фішинг

У ряді прикладів найпоширеніших способів атак на мережі компаній, як уже було згадано вище, можна навести використання технік соціальної інженерії або фішингу в поштових повідомленнях. При типовій фішинг-атаці зловмисник розсилає безліч підроблених поштових повідомлень, складених так, ніби вони відправлені від довіреного джерела: відомої всім торгової або фінансової компанії (наприклад, банку). У листі "жертву" всіляко підштовхують оновити його персональну інформацію, щоб нібито не втратити доступ до спеціальних сервісів (доступ до банківського on-line-рахунку тощо), і для цього йому підсувається посилання на офіційний Web-сайт, на вигляд не викликає жодних сумнівів.

Клацаючи на пропоноване посилання, користувач переправляється на підроблений сайт зловмисника, що нічим не відрізняється від оригінального сайту (зазвичай його клон). Таким чином, "жертва", нічого не підозрюючи, заповнює запропоновані форми та залишає всю свою персональну інформацію хакерам. Але навіть якщо користувач достатньо освічений, щоб не завантажувати і не запускати жодних файлів і не заповнювати форм, а він просто "клікне" за запропонованим у листі посиланням, то і в цьому випадку ніхто не дасть гарантії, що зловмисники не отримають усі його логіни та паролі. Хакер може провести атаку в цьому випадку на Web-браузер користувача, на комп'ютер якого будуть завантажені всі необхідні експлоїти, які почнуть свою роботу автоматично після кліка.

Спам

Разом із перерахованими вище загрозами не можна не згадати і про спам, який негативно впливає на продуктивність праці працівників, змушених щодня читати купу непотрібного їм рекламного сміття та витрачати на це свій робочий час. Крім того, технології спаму також широко використовуються хакерами для крадіжки та отримання прибутку. Найпопулярнішим на сьогодні способом розповсюдження спамерами їхніх листів є так звані бот-мережі, або "зомбі", тобто спільноти комп'ютерів, ресурси яких знаходяться під контролем хакерів. "Зомбі" можуть розсилати непомітно для їх користувачів величезні кількості спаму, тим самим забезпечуючи спамерам ефективність (середній обсяг атаки становить 70-200 млн повідомлень) та анонімність, адже розсилка здійснюється з IP-адрес легітимних користувачів або компаній. За деякими дослідженнями вельми шанованих аналітиків, майже одна чверть усіх комп'ютерів у світі є учасниками тієї чи іншої бот-мережі.

Сучасні системи захисту поштового трафіку

Наведена вище інформація дає деяке уявлення про те, наскільки важким і комплексним є на сьогоднішній день завдання захисту корпоративної e-mail-пошти від загроз, пов'язаних із доступом до громадських мереж та мережі Інтернет.

Як правило, за забезпечення безпеки корпоративної пошти від загроз ззовні у компанії повинен відповідати спеціалізований пристрій або комплекс.

## **1.3. Проблеми, які вирішує захист електронної пошти**

Найсерйознішою загрозою є витік комерційної інформації. Цінність конфіденційної інформації в середовищі бізнесу не підлягає сумніву. Вона є «ласим шматком» для конкурентів та зловмисників. При цьому мало хто замислюється, що електронні повідомлення пересилаються незашифрованими і можуть бути перехоплені або підроблені. Для цього потрібно лише мати можливість «слухати» трафік, перебуваючи або в офісі, або в мережі провайдера.

Тому захист електронної пошти, перш за все, має бути спрямований на зниження доступності інформації для сторонніх осіб.

Існують різні способи вирішення цього завдання. Наприклад, захист електронної пошти може бути забезпечений цифровим підписом (ЕЦП) або шифруванням повідомлень з використанням особистих та відкритих ключів. Конкретне вирішення завдання захисту повідомлень під час передачі залежить від специфіки переданої інформації та інших чинників.

Наступна загроза, на усунення якої спрямований захист електронної пошти – зовнішні атаки. Найнешкідливіша з них – це цільовий та нецільовий спам. За статистикою на спам-розсилки припадає понад 80% усієї кореспонденції, що передається через всесвітню павутину. Такі повідомлення як серйозно завантажують інформаційні системи, а й щодня відволікають співробітників від виконання службових обов'язків. З метою зниження потоку спаму захист електронної пошти використовує спеціальні програмні фільтри та антиспам-системи.

Більш серйозною загрозою є троянські та шкідливі програми, а також фішингові посилання, які у величезних кількостях розсилаються в електронних повідомленнях. Шкідливе ПЗ може завдати непоправної шкоди серверам, робочим станціям та інформації, що в них є – спотворити або знищити дані, блокувати роботу додатків та операційної системи в цілому.

Перехід за фішинговими посиланнями на сайти хакеру загрожує тим, що на комп'ютери користувачів будуть непомітно встановлені програми, що дозволяють отримати зловмисникам доступ до цінної персональної інформації, логінам і паролям від корпоративних ресурсів. Для усунення таких загроз захист електронної пошти використовує надійні антивірусні програми, які дозволяють сканувати поштові повідомлення, а також сповіщати про наявність фішингових посилань в отриманому листі.

Крім того, на корпоративний поштовий сервер можуть бути організовані зовнішні атаки, наслідком яких стане відмова поштової служби - DoES (Denial of Email Service). У ситуації, коли корпоративна пошта активно використовується в процесі роботи, це може стати серйозною проблемою.

Захист електронної пошти стосується також вихідної інформації. Йдеться про контроль відправок файлів, даних за важливими контрактами, автоматичну та ручну перевірку повідомлень. Захист електронної пошти у цій частині є прерогативою служби безпеки компанії. Недарма всі серйозні корпорації приділяють велику увагу контролю над вихідною поштою. Відсутність такого контролю незмінно тягне або випадковий, або навмисний витік важливих комерційних відомостей.

У випадку, зокрема, захист електронної пошти нами розглядається, як сукупність наступних заходів:

* Забезпечення високої відмовостійкості та продуктивності поштових серверів.
* Контентний та репутаційний захист від спаму.
* Встановлення сигнатурного та проактивного захисту від вірусів.
* Захист електронної пошти шляхом шифрування вихідних повідомлень за допомогою криптографічних програм.
* Використання адаптивної фільтрації вхідних електронних повідомлень.
* Захист від DDos атак на поштові сервери.
* Встановлення найнадійніших поштових клієнтів.
* Налаштування black/white списків та персонального карантину.
* Захист електронної пошти від витоку конфіденційних даних, контролюючи вихідні повідомлення.

Загалом захист електронної пошти потребує системного підходу. Використання різноманітних рішень для захисту електронної пошти ґрунтується на роботі комплексу спеціалізованих пристроїв та програмного забезпечення. Можна вважати, що захист електронної пошти - один з найважливіших компонентів забезпечення інформаційної безпеки.

# 2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОЧТИ

## **2.1. Безпечні протоколи**

### **2.2.1. PGP**

Перший протокол – протокол PGP – Pretty Good Privacy. PGP був винайдений Філом Цимерманном (Phil Zimmermann), щоб забезпечити секретність, цілісність та встановлення автентичності електронної пошти. PGP може використовуватися, щоб створити безпечне поштове повідомлення або зберегти файл для майбутнього вилучення.

Шифрування PGP здійснюється послідовно хешуванням, стиском даних, шифруванням з симетричним ключем, і, нарешті, шифруванням з відкритим ключем, причому кожен етап може здійснюватися одним з декількох алгоритмів, що підтримуються. Симетричне шифрування проводиться з використанням одного із семи симетричних алгоритмів (AES, CAST5, 3DES, IDEA, Twofish, Blowfish, Camellia) на сеансовому ключі. Сеансовий ключ генерується з використанням стійкого криптографічно генератора псевдовипадкових чисел. Сеансовий ключ зашифровується відкритим ключем одержувача за допомогою алгоритмів RSA або Elgamal (залежно від типу ключа одержувача). Кожен відкритий ключ відповідає імені користувача або адресі електронної пошти. Перша версія системи називалася Мережа Довіри та протиставлялася системі X.509, що використовувала ієрархічний підхід, заснованої на центрах, що засвідчують, доданий в PGP пізніше. Сучасні версії PGP включають обидва методи.

### **2.2.2. S/MIME**

Інша служба безпеки розроблена для електронної пошти Безпечне/багатоцільове розширення пошти (S/MIME - Secure/Multipurpose Internet Mail Extension). Цей протокол є розширенням багатоцільового розширення пошти (MIME - Multipurpose Internet Mail Extension).

MIME - це додаткові протоколи, які дозволяють даними, що не передаються за допомогою ASCII, проходити електронною поштою. MIME перетворює такі дані на стороні передавача даних NVT ASCII і поставляє їх клієнту MTA по мережі Інтернет. Повідомлення на приймальній стороні перетворюється знову на початковий вид.

S/MIME додає деякі нові типи заголовків вмісту, щоб увімкнути служби безпеки в MIME. Всі ці нові типи включають параметр "application/pkcsP-mime", у якому "pkcs (Public Key Cryptography Specification)" визначає "Специфікацію криптографії відкритого ключа".

Керування ключами

Керування ключами в S/MIME - це комбінація керування ключами, що використовується в X.509 та PGP. S/MIME використовує сертифікат відкритого ключа, який підписаний адміністрацією, що засвідчує X.509. Однак користувач несе відповідальність за підтримку мережі довіри для перевірки підпису, як визначено PGP.

### **2.2.3. HTTPS**

HTTPS (HyperText Transfer Protocol Secure) – розширення протоколу HTTP, що підтримує шифрування. Дані, що передаються за протоколом HTTPS, "упаковуються" у криптографічний протокол SSL або TLS. На відміну від HTTP, для стандарту HTTPS використовується TCP-порт 443.

HTTPS не є окремим протоколом. Це стандартний HTTP, що працює через шифровані транспортні механізми SSL і TLS. Він забезпечує захист від атак, заснованих на прослуховуванні мережного з'єднання - від сніфферських атак та атак типу man-in-the-middle, за умови, що будуть використовуватися шифруючі засоби та сертифікат сервера перевірений і йому довіряють.

За умовчанням HTTPS URL використовує 443 TCP-порт (для незахищеного HTTP - 80). Щоб підготувати веб-сервер для обробки https-з'єднань, адміністратор повинен отримати та встановити сертифікат для цього веб-сервера. Сертифікат складається з 2 частин (2 ключі) - public і private. Public-частина сертифіката використовується для зашифровування трафіку від клієнта до сервера в захищеному з'єднанні, private-частина - для розшифровування отриманого від клієнта зашифрованого трафіку на сервері. Після того як пара ключів приватний/публічний згенеровані, на основі публічного ключа формується запит на сертифікат до Центру сертифікації, у відповідь на який ЦС надсилає підписаний сертифікат. ЦС під час підписання перевіряє клієнта, що дозволяє йому гарантувати, що власник сертифіката є тим, за кого себе видає (зазвичай це платна послуга).

HTTPS для шифрування використовується довжина ключа 40, 56, 128 або 256 біт. Деякі старі версії браузерів використовують довжину ключа 40 біт, що пов'язане з обмеженнями експорту в США. Довжина ключа 40 біт не є надійною. Багато сучасних сайтів вимагають використання нових версій браузерів, що підтримують шифрування з довжиною ключа 128 біт, щоб забезпечити достатній рівень безпеки. Таке шифрування значно ускладнює зловмиснику пошук паролів та іншої особистої інформації.

## **2.2. Рішення для захисту електронної пошти**

SpamTitan

SpamTitan – це провідна платформа безпечного шлюзу електронної пошти, що забезпечує комплексний захист від загроз, пов'язаних з електронною поштою, включаючи спам, шкідливі програми, програми-вимагачі та фішингові атаки. SpamTitan побудований на потужній платформі фільтрації спаму з найкращим на ринку коефіцієнтом виявлення 99,99% та рівнем помилкових спрацьовувань 0,0003%. Поряд із фільтрацією спаму SpamTitan забезпечує розширений захист від витончених фішингових атак, скануючи всі вхідні електронні листи в режимі реального часу та відфільтровуючи шкідливий контент, включаючи посилання на фішингові веб-сторінки та шкідливі вкладення.

SpamTitan забезпечує максимальний захист від загроз як для вхідної, так і вихідної електронної пошти. Платформа забезпечує багаторівневий захист від загроз для вхідної електронної пошти, включаючи захист від уособлення генерального директора, фішинг та захист, аналіз URL-адрес, ізольоване програмне середовище для вкладень, захист від програм-вимагачів, перевірку та шифрування SPF/DKIM/DMARC. SpamTitan запобігає фішингові та китобійні атаки, скануючи вхідні електронні листи в режимі реального часу, забезпечуючи високий рівень захисту поштової скриньки. Поряд із вхідною електронною поштою SpamTitan дозволяє адміністраторам налаштовувати потужні правила запобігання витоку даних, які допомагають зупинити втрату даних вихідної електронної пошти.

SpamTitan – це доступна та проста в управлінні платформа з повним набором функцій SEG. Сервіс простий у використанні та розгортанні, легко інтегрується з існуючими системами електронної пошти. SpamTitan добре працює як додатковий рівень безпеки для облікових записів Office 365, забезпечуючи покращений захист від загроз та створення звітів для користувачів електронної пошти Office 365. Цей захист підтримується їхньою чуйною та знаючою командою технічної підтримки. SpamTitan користується популярністю у клієнтів, які хвалять сервіс за простоту розгортання, вигідні ціни та якісну технічну підтримку.

Proofpoint Essentials

Шлюз безпеки електронної пошти Proofpoint Essentials

Proofpoint — провідний на ринку шлюз безпеки електронної пошти та найбільший у світі постачальник засобів захисту електронної пошти з річним доходом понад 1 мільярд доларів. Proofpoint Essentials – це рішення Proofpoint для малих та середніх організацій. Essentials – це надійне рішення для захисту електронної пошти, шифрування, архівування та забезпечення безперервності, яке постачається як єдина платформа з єдиною консоллю адміністратора. Proofpoint має неперевершений огляд загроз електронної пошти за допомогою своєї глобальної платформи аналізу загроз, що охоплює електронну пошту, соціальні мережі та мобільні пристрої. Інші постачальники покладаються на сторонні аналітичні дані щодо загроз, які можуть бути менш точними. Proofpoint збирає та аналізує понад 100 мільярдів точок даних на день з більш ніж 100 мільйонів скриньок електронної пошти, 200 мільйонів облікових записів соціальних мереж та 7 мільйонів мобільних додатків. Proofpoint забезпечує більше 50% акцій Fortune 100,

Proofpoint забезпечує найкращий захист від загроз, пов'язаних з електронною поштою, з ефективним захистом та виявленням спаму, потужним захистом URL-адрес та динамічною фільтрацією контенту. Essentials — це економічне рішення з багатьма функціями, такими як архівування та шифрування, включеними до пакета Professional, які інакше були б дорогими надбудовами. Essentials надає ряд звітів та журналів, щоб дати більше контролю та поінформованості про мережу електронної пошти. Сучасна консоль адміністратора Proofpoint забезпечує детальний контроль та покращену звітність про загрози. З Essentials Proofpoint надає організаціям захист електронної пошти корпоративного класу за вигідною ціною. Це ідеальне рішення для підприємств та MSP з простим налаштуванням, розгортанням та конкурентоспроможними цінами.

Abnormal Security

Abnormal Security – це хмарна платформа електронної пошти, що забезпечує комплексний захист від погроз, пов'язаних з електронною поштою, включаючи компрометацію корпоративної електронної пошти, фішинг, шкідливі програми, програми-вимагачі та спроби видачі себе за іншу особу. Abnormal використовує технології машинного навчання для створення базового середовища електронної пошти, дозволяючи системам захисту від загроз точно виявляти та блокувати шкідливий вміст електронної пошти від доставки користувачам. Компанія Abnormal Security була заснована в 2018 році і в даний час захищає понад 5% компаній зі списку Fortune 1000 зі 100-відсотковою частотою оновлення для підприємств із 5 000–500 000 співробітників.

Платформа Abnormal використовує поведінковий ШІ для миттєвого виявлення шкідливого вмісту електронної пошти та блокування вхідних та внутрішніх поштових загроз. Abnormal також відстежує та захищає внутрішні облікові записи електронної пошти для виявлення та виправлення скомпрометованих облікових записів. Розуміючи відому хорошу поведінку особи, контент та тон, Abnormal може виявляти користувачів, які демонструють незвичайну поведінку, та виправляти облікові записи, виводячи користувачів з активних сеансів та вимагаючи скидання пароля.

Abnormal — це потужна платформа безпеки електронної пошти, розроблена як хмарна альтернатива, що добре зарекомендувала себе постачальникам шлюзів безпеки електронної пошти. Рішення, визнане "Переважним рішенням Microsoft" і обране Microsoft за його можливості захисту електронної пошти, розгортається через API і може бути запущено в хмарних середовищах електронної пошти за лічені хвилини. Платформа спочатку інтегрується з платформами Microsoft 365 та Google Workspace для забезпечення покращеного захисту та зручної взаємодії з користувачем. З цієї причини рекомендують цю послугу організаціям, які використовують Microsoft 365 або Google Workspace і потребують підвищеної безпеки електронної пошти.

IRONSCALES

IRONSCALES забезпечує швидкий та потужний захист від загроз у поштовій скриньці. Вони пропонують два платні пакети (Email Protect™ та Complete Protect™), які забезпечують захист від фішингу у поєднанні з інтегрованим навчанням безпеки та підвищення обізнаності, адміністрування яких здійснюється з єдиної консолі. IRONSCALES — це повністю хмарна платформа, яка ідеально підходить для використання з Office 365 та G Suite. Впровадження може бути завершено лише за два кліки, і жодні зміни запису MX ніколи не потрібні. Під час тестування він виявив фішингові загрози, які пропустили Office 365 та інші провідні рішення для захисту електронної пошти. IRONSCALES забезпечує потужний захист від витончених атак соціальної інженерії, таких як фішинг та компрометація корпоративної електронної пошти.

IRONSCALES використовує інструменти безпеки на основі ШІ у поєднанні з людським інтелектом кінцевих користувачів для виявлення шкідливих електронних листів та автоматичного видалення їх із поштових скриньок користувачів.

Крім того, IRONSCALES дозволяє підприємствам впроваджувати кнопку "повідомити про фішинг" безпосередньо в поштові клієнти кінцевих користувачів. Це працює на всіх пристроях і повністю настроюється. Це дозволяє користувачам повідомляти про підозрілі електронні листи, що скорочує час очікування. Відповідно до політики адміністратора, коли кінцевий користувач повідомляє про електронний лист, іншим користувачам, які отримали такий самий або схожий електронний лист, відображатиметься попередження, або, альтернативно, електронний лист буде поміщений до карантину. IRONSCALES також надає повний набір навчальних матеріалів з питань безпеки і моделювання фішингу з шаблонами фішингу, що настроюються, і захоплюючими навчальними матеріалами.

Клієнти хвалять IRONSCALES за те, що вони спростили управління фішинговими загрозами в широкому масштабі. Адміністратори повідомляють, що в багатьох випадках IRONSCALES дозволяє їм легко видаляти фішингові електронні листи з поштових скриньок, зупиняючи атаки до того, як вони відбудуться. Клієнти також хвалять простоту розгортання. IRONSCALES дуже добре інтегрується з хмарними постачальниками електронної пошти, такими як Office 365 та G-Suite. IRONSCALES — чудовий варіант для організацій, які задоволені своїм рівнем фільтрації спаму, але потребують додаткового захисту від складних загроз електронної пошти, таких як фішинг, внутрішні загрози та компрометація корпоративної електронної пошти. IRONSCALES тепер також пропонує захист від шкідливих посилань та вкладень у середовищі Microsoft Teams.

Безпечний поштовий шлюз Mimecast

Mimecast — один із найбільш повнофункціональних безпечних шлюзів електронної пошти на ринку. Він орієнтований насамперед на корпоративних користувачів, пропонуючи високий рівень захисту від загроз та деталізовані політики адміністрування. Платформа Mimecast є потужною та настроюваною. Mimecast забезпечує надійний захист від загроз електронної пошти, а адміністратори можуть налаштувати службу відповідно до конкретних потреб. Mimecast пропонує захист від уособлення, щоб допомогти запобігти атакам фішингу. Mimecast також пропонує такі функції, як захист вкладень та URL-адрес. Вони працюють у режимі реального часу, запобігаючи зараженню мережі загрозами.

Mimecast є одним з провідних постачальників у сфері дослідження загроз. Вони відстежують мільярди електронних листів та мають велику базу даних загроз. Це добре для клієнтів, оскільки означає, що вони завжди в курсі останніх загроз та готові захистити організацію від них. Клієнти хвалять звіти та аналітику, пропоновані Mimecast. Їх легко зрозуміти, що дозволяє відстежувати, наскільки захищена електронна пошта та наскільки добре працює Mimecast. Mimecast може похвалитися низьким рівнем легітимних електронних листів, хибно помічених як спам, та високим рівнем блокування спаму та вірусів. Mimecast — гарний варіант для корпоративних організацій, яким потрібний найпотужніший захист для їхньої електронної пошти.

Microsoft Defender для Office 365

Microsoft Defender для Office 365 – це хмарна служба фільтрації електронної пошти, яка спочатку працює з Office 365, як і слід очікувати від служби Microsoft. Це допомагає захистити організації від невідомих шкідливих програм та вірусів, включаючи антивірусне сканування та сканування URL-адрес для блокування шкідливих програм та шкідливих посилань у режимі реального часу.

Microsoft Defender надає ряд функцій, включаючи застосування політик захисту від фішингу, захист від шкідливих програм у SharePoint, OneDrive та Microsoft Teams, а також забезпечення безпеки вкладень. Клієнтам дуже легко розпочати роботу з Office 365. Як додаткову послугу, що забезпечує більш надійний захист Office 365, Захисник надає адміністраторам політики захисту від погроз, звіти та можливості розслідування та реагування, які інакше компанії не отримали б з Office 365. За допомогою Defender адміністратори можуть налаштовувати захист від загроз, переглядати звіти в режимі реального часу та використовувати інструменти для дослідження загроз та їх джерел. Це важлива функціональність, яка виходить за межі можливостей безпеки, які підприємства можуть реалізувати за допомогою Office 365.

Однак, незважаючи на ці функції, функціональність Office 365, особливо з точки зору фільтрації спаму, функцій адміністрування та захисту від фішингу, не така розвинена, як у інших сторонніх рішень. Microsoft Defender – популярний вибір серед клієнтів як комплексне рішення, яке працює безпосередньо із Office 365.

Avanan

Avanan – це інноваційне хмарне рішення для захисту електронної пошти з повним пакетом захисту від загроз для Office 365 та Google Workspace (раніше GSuite). Платформа Avanan захищає підприємства від витончених атак електронної пошти, таких як фішинг, шкідливе програмне забезпечення, компрометація облікового запису та втрата даних. На відміну від традиційних безпечних шлюзів електронної пошти, Avanan знаходиться всередині середовища електронної пошти і розгортається лише за кілька хвилин, не вимагаючи жодних змін записів MX. Ця інтеграція на основі API дозволяє Avanan аналізувати всі історичні електронні листи, що дозволяє йому виявляти видачу себе за користувача і шахрайство з електронною поштою.

Avanan забезпечує багаторівневий захист від загроз для захисту електронних листів у поштовій скриньці. Оскільки Avanan знаходиться в середовищі електронної пошти, він може захищати вхідні, вихідні та внутрішні листи. Avanan використовує машинне навчання для виявлення фішингових атак нульового дня, використовуючи більше 300 індикаторів компрометації, включаючи час відправлення, місцезнаходження та домен, щоб помічати підозрілі електронні листи. Avanan також використовує машинні алгоритми для виявлення компрометації корпоративної електронної пошти, помічаючи входи в систему в кількох країнах та попереджаючи адміністраторів про незвичайну поведінку, яка вказує на захоплення облікових записів.

Avanan також забезпечує покращений захист електронної пошти від шкідливих програм. Це включає захист від шкідливих вкладень та URL-адрес з розширеними звітами для всіх вхідних, вихідних та внутрішніх повідомлень електронної пошти. Всередині мережі електронної пошти Avanan забезпечує в режимі реального часу та історичні дані про всіх користувачів та загрози, пов'язані з електронною поштою. Avanan – це надійне рішення для користувачів Office 365 та Google Workspace, яким потрібний потужний захист від фішингу, адресного фішингу та компрометації облікового запису.

Безпека електронної пошти Trustifi

Trustifi — це постачальник послуг з безпеки та шифрування електронної пошти, який допомагає організаціям захищати свої вхідні та вихідні повідомлення електронної пошти від таких загроз, як фішинг, захоплення облікових записів та зловмисне програмне забезпечення, що доставляється електронною поштою. Trustifi поєднує в собі розширений захист від вхідних загроз, що сканує електронні листи на наявність шкідливого вмісту, з шифруванням вихідної електронної пошти, що забезпечує захист конфіденційних даних у стані спокою, у сховищі та передачі. Сумісний з локальними поштовими клієнтами, Office 365 Outlook і Google Workspace, Trustifi допомагає організаціям захищати свої поштові скриньки та дотримуватися вимог, незалежно від того, яку платформу вони використовують для зв'язку.

Технологія захисту вхідної електронної пошти Trustifi сканує всі повідомлення електронної пошти на наявність шкідливого вмісту, такого як спам, віруси, зловмисне програмне забезпечення та спроби фішингу. Платформа ранжує кожен електронний лист відповідно до його рівня загрози та типу загрози, починаючи від «Аутентифіковано» і закінчуючи такими попередженнями, як «Атака з використанням уособлення». Потім рішення поміщає до карантину або видаляє шкідливі електронні листи відповідно до політик, налаштованих адміністратором. Trustifi також пропонує білий та чорний списки адрес, щоб допомогти організаціям уникнути повторних атак з боку відомих зловмисників та гарантувати, що електронні листи відомих зовнішніх відправників не будуть помилково поміщені до карантину.

Рішення Trustifi розгортається через інтеграцію з API, тому його можна швидко та легко налаштувати. Він постачається з попередньо налаштованими параметрами за замовчуванням, тому після розгортання він миттєво забезпечує захист від загроз. Потім адміністратори можуть увійти до системи, щоб налаштувати більш детальні налаштування безпеки вхідної та вихідної електронної пошти. Клієнти хвалять Trustifi за простоту використання як з погляду адміністратора, так і з погляду кінцевого користувача, і рекомендують його як потужне та зручне рішення для організацій будь-якого розміру, які хочуть захистити свої поштові скриньки від таких загроз, як фішинг, а також як зашифрувати їх найбільш конфіденційний контент електронної пошти.

Barracuda

Barracuda надає багатофункціональну систему захисту електронної пошти без великих витрат. Barracuda пропонує сканування на віруси та захист від спаму в режимі реального часу. Його легко розгорнути за допомогою Office 365, що робить його ідеальним варіантом для невеликої компанії, яка хоче перенести свою мережу електронної пошти на хмару. Незважаючи на низьку ціну, Barracuda вклала у цю платформу безліч функцій. Він пропонує розширений захист із скануванням URL-адрес та фільтрацією вихідної електронної пошти. Це додаткові платні функції для багатьох сервісів-конкурентів. Завдяки цим функціям не дивно, що сервіс дуже популярний серед малих підприємств та MSP.

Клієнти хвалять Barracuda Essentials за підтримку, і багато користувачів кажуть, що їхня команда швидко реагує і добре обізнана. Як глобальний постачальник систем безпеки, Barracuda має великий підрозділ з аналізу загроз, який постійно шукає нові загрози і розробляє заходи для захисту від них.

Barracuda Essentials пропонує багато інших послуг у комплекті із захистом електронної пошти. Це включає рішення для архівування, а також шифрування і резервне копіювання. Цей набір функцій дозволяє легко рекомендувати цю послугу невеликій компанії або MSP, які шукають комплексне рішення.

Безпека хмарної електронної пошти Cisco

Cisco створила надійний захищений шлюз електронної пошти, що забезпечує надійний захист від компрометації корпоративної електронної пошти та фішингових атак. Їхня дослідницька група, що вивчає загрози електронної пошти, є величезною, що гарантує, що у завжди буде доступ до передового захисту від загроз. Платформа Cisco забезпечує надійний захист від компрометації корпоративної електронної пошти та програм-вимагачів. Це пов'язано з функцією, яка автоматично блокує посилання, які вважає небезпечними, що захищає від електронних листів, навіть якщо вони є справжніми. Ця платформа надає ряд функцій адміністратора, що настроюються. Пропоновані звіти та ведення журналів надійні та дають уявлення про безпеку електронної пошти.

Cisco пропонує ефективну фільтрацію спаму, яка гарантує, що в папку «Вхідні» потраплять лише ті листи, які потрібні. Платформа також має захист від втрати даних за допомогою методів, які забезпечують захист електронних листів за допомогою шифрування.

Одна з ключових переваг цієї платформи полягає в тому, що як продукт Cisco вона легко інтегрується в низку інших послуг безпеки. Це означає, що організація отримує доступ до надійного багаторівневого захисту.

Libraesva ESG

Libraesva ESG – це інтегроване рішення для забезпечення безпеки електронної пошти, яке використовує кілька рівнів захисту для захисту Microsoft 365, Exchange та Google Workspace як на рівні шлюзу, так і на рівні API, тому загрози електронної пошти, такі як шахрайство з електронною поштою, BEC і фішингові атаки, запобігають ще до того, як вони досягнуть намічених ними цілей.

Це повнофункціональне рішення, що пропонує користувачам низку корисних можливостей. Існує захист від спуфінгу, який дозволяє виявляти та блокувати самозванців, а також запобігати спуфінгу за допомогою комбінації методів автентифікації SPF, DKIM та DMARC, а також усунення загроз, що полегшує видалення шкідливих повідомлень електронної пошти з поштових скриньок користувачів, що означає, що електронний лист або видалені або збережені для подальшого аналізу.

Портал аналізу загроз являє собою універсальну інформаційну панель, що надає покращену інформацію про атаки електронною поштою та дані про тенденції для організацій у порівнянні з глобальними даними Libraesva. Рішення також запобігає доставці шкідливих файлів за допомогою ретельної перевірки та очищення документації, забезпечує захист одним клацанням миші, яка інтелектуально сканує всі посилання на наявність ухильної поведінки, щоб відвернути користувачів від небезпечних веб-сайтів, та забезпечує наскрізне шифрування електронної пошти. Безперервність електронної пошти запобігає впливу простоїв на продуктивність, а доступна мобільна програма дозволяє користувачам керувати Microsoft 365, Exchange і Google Workspace, навіть якщо вони знаходяться далеко від свого робочого місця.

Libraesva ESG забезпечує розширений захист для хмарних поштових платформ з повним захистом від складних загроз та атак, простоту розгортання та детальне налаштування. Рішення добре підходить для середніх та великих підприємств або клієнтів зі сфери освіти, зацікавлених в економічному захисті електронної пошти з високим рівнем видимості та налаштування.

# 3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ

## **3.1. Забезпечення безпеки електронної пошти**

Рішення для захисту електронної пошти запобігають доставці шкідливих електронних листів, їх розповсюдженню всередині або надсилання з мережі електронної пошти. Безпека електронної пошти — це широке зонтичне поняття, яке може використовуватися для позначення кількох технологій, програмних рішень та середовищ, призначених для захисту мереж електронної пошти.

Усім організаціям важливо мати ефективну систему безпеки електронної пошти для захисту користувачів, клієнтів та партнерів від витончених загроз електронної пошти, таких як спам, шкідливе програмне забезпечення, фішинг та компрометація корпоративної електронної пошти. Безпека електронної пошти також важлива для забезпечення та демонстрації дотримання правил безпеки даних.

Шлюзи безпеки електронної пошти призначені для захисту мережі електронної пошти, блокуючи потрапляння шкідливого вмісту електронної пошти в поштові скриньки користувачів і запобігаючи надсиланню вихідного шкідливого вмісту електронної пошти.

Багато шлюзів безпеки електронної пошти використовують поєднання інструментів сканування вмісту електронної пошти, сканування репутації домену, сканування URL-адрес та пісочниці вкладень для проведення детермінованої оцінки вхідного повідомлення електронної пошти. Якщо повідомлення є шкідливим, воно блокується; якщо він вважається безпечним, він доставляється.

Адміністратори повинні мати можливість настроювати політики, що регулюють роботу цієї фільтрації. Вони можуть захотіти заблокувати електронні листи з певних доменів або дозволити електронні листи від відомих надійних відправників. Крім того, шлюзи безпеки електронної пошти повинні надавати докладні звіти, щоб допомогти організаціям відстежувати вхідні загрози електронної пошти.

Сучасні шлюзи безпеки електронної пошти часто повністю засновані на хмарі, але можуть бути розгорнуті локально або у вигляді гібридних рішень. Розгортання має бути простим, особливо з хмарними системами електронної пошти, такими як Microsoft 365 або Google Workspace.

Цей список також містить хмарні рішення для забезпечення безпеки електронної пошти, які не є традиційними шлюзами, але належать до категорії, яку Gartner визначає як «Доповнення до хмарної безпеки електронної пошти» (CESS). Ці постачальники часто повністю хмарні і інтегруються з O365 і Google через інтеграцію API, при цьому не потрібні жодні зміни в записах MX.

Перевага цих рішень полягає в тому, що вони можуть забезпечити більший захист в мережі електронної пошти, ніж SEG, які зазвичай забезпечують посилений захист мережі електронної пошти на її кордоні. Це означає, що хмарні рішення для захисту електронної пошти можуть ефективно виявляти ознаки фішингу та компрометації облікового запису.

## **3.2. Способи захисту електронної пошти**

Комплексний захист інформації, для передачі якого використовується електронна поштова скринька, ставить перед собою такі завдання:

Забезпечення безперешкодного отримання листів адресатом, без можливості їх перехоплення, розтину, прочитання, а також запобігання можливому підробленню.

Захист інформації, надісланої через e-mail, від її розповсюдження зловмисником без відома відправника.

Захист листів від перехоплення

Досягнення цього завдання, яка рано чи пізно вимагатиме свого вирішення, ґрунтується на застосуванні традиційних методів криптографії – використанні певних шифрів. Захист від можливого підроблення передбачає застосування ЕЦП (електронного цифрового підпису).

Технічна сторона забезпечення безпеки найчастіше передбачає встановлення спеціального незалежно компілюваного програмного модуля (plug-in) для поштового клієнта. Зазвичай цього цілком достатньо, оскільки цей невеликий за розмірами додатковий софт в автоматичному режимі зашифровує листи і підписує їх. Якщо користувач застосовує веб-інтерфейс для входу у власну пошту, цей процес виконується поштовим сервером або спеціальним скриптом, що забезпечує більш високий рівень безпеки. Для первинного обміну ключами передбачається застосування спеціальних ресурсів.

Використовувані з цією метою криптографічні технології відпрацьовані, їх застосування надійно захищає інформацію від перехоплення або підробки. Зазвичай таких заходів захисту цілком достатньо. Можливі вразливості такого комплексу заходів безпеки виявляються лише у таких випадках:

- встановлення явно «слабких» криптоалгоритмів, хоча вибір такого софту може бути визначений і національною законодавчою базою країни, оскільки забезпечує можливість спецслужбам отримати доступ до електронної пошти шляхом злому криптоалгоритмів;

- збої функціональності криптографічних алгоритмів чи задіяних протоколів;

- спочатку зроблені зловмисником «Закладки» у криптоалгоритми, які уможливлюють зламування захисту e-mail;

- "дії" вірусу, здатного перехопити вже розшифроване повідомлення на пристрої адресата або отримав доступ до ключів "машини" відправника або адресата.

Здебільшого відомі наразі вразливості мають або зовнішній характер, або продиктовані обраним способом реалізації системи безпеки. При комплексному підході до захисту пошти ці вразливості виявляються і усуваються.

Захист відправленої поштою інформації від дій несумлінного адресата

Завдання захисту відправленого поштою листа від його розповсюдження зловмисником, який втерся в довіру, здійснюється шляхом використання певних коштів, що дозволяють створити ситуацію, коли «адресат має можливість лише прочитати листа». Решта дій з отриманою через пошту інформацією йому недоступні. Застосовується при цьому невелика за обсягом програма, що називається або власний переглядач листи, або спеціальний переглядач, або спеціальний браузер.

Цей софт виключає можливість використання зовнішніх компонентів, які зазвичай використовуються для демонстрації вмісту листів. В результаті, у відправника з'являються власні труднощі - не підтримується більшість програмно-апаратних платформ, а також форматів документів, що надсилаються через e-mail.

Професіонали зазначають, що, на відміну від засобів захисту листів від перехоплення, використання спецпроглядача листів не дозволяє забезпечити бажаного рівня захисту, оскільки це неможливо в принципі. Зловмисник може просто зробити скріншот отриманої в листі інформації, а потім сформувати з нього документ. Не маючи можливості повністю запобігти небажаному поширенню інформації, софт, що захищає пошту від поширення листів зловмисником, лише кардинально обмежує потенційний обсяг витоку.

Ефективність заходів щодо обмеження можливого несанкціонованого поширення інформації залежить від стійкості застосовуваних засобів захисту до існуючих методів автоматичного зчитування інформації з отриманого листа, а саме:

- злом ззовні спецпереглядача листів для того, щоб витягти з нього документ;

- копіювання документів з екрана, зміна формату копій та перетворення їх у документ.

Навіть набір наявних засобів захисту e-mail може виявитися безглуздим, якщо немає чіткого розуміння, що потрібно захистити, від яких дій, для чого це необхідно і наскільки надійною має бути побудована система захисту. Тільки наявність комплексного розуміння завдань і способів їх вирішення дозволяє вибрати оптимальну систему з існуючих на ринку пропозицій.

Засоби захисту

Безпечна функціональність e-mail створюється застосуванням:

- Поштового Антивірусу, який автоматично проводить сканування листів, інформаційних фалів на присутність шкідливого софту;

- Анти-спаму, що відповідає за виявлення звичайних розсилок, на отримання яких користувач не підписувався.

Обидва дані компонента отримують доступ до повідомлень, що надходять на пошту, шляхом:

- своєчасне перехоплення, дослідження поштового трафіку в автоматичному режимі за протоколами POP3, SMTP, NNTP, IMAP;

- використання спеціальних plug-in, що є у поштових клієнтах.

Інсталяція додаткових програм Поштового «антивірусника» (в Microsoft Office Outlook і The Bat!) та Анти-Спама (в Microsoft Office Outlook, Outlook Express та The BAT!) здійснюється автоматично, при установці програми-антивірус.

Параметри функціонування Поштового Антивірусу

Заводською установкою передбачається, що Поштовий Антивірус досліджуватиме як листи, що надходять, так і надсилаються. Користувач, за своїм бажанням, може не перевіряти "надіслані", відключивши цю функцію.

Передбачені і додаткові обмеження, які може встановити сам клієнт, скасувавши сканування вкладених файлів, наприклад:

- пропускати без сканування архіви, що не рекомендується, оскільки наголошувалися випадки виявлення вірусів, що розсилаються у вигляді архівів;

- Обмежити максимальну тривалість процесу сканування, що часто використовується для прискорення процесу отримання листів. Заводська установка передбачає трихвилинне сканування повідомлення.

Крім «ручного» вибору налаштувань функціональності Поштового антивірусника, споживач має можливість використовувати один із заздалегідь встановлених рівнів захисту:

- високий;

- рекомендований;

- низький.

Алгоритм функціональності Поштового Антивірусу

Софт Поштовий Антивірус, використовуючи сигнатурний аналіз, практично однаковий з Файловим Антивірусом, проводить обробку листів як заражених, так і підозрілих. Як і під час роботи звичайного антивірусника, об'єкти або видаляються, або лікуються, або вирушають у карантин.

Порядок обробки мають вірус або підозрілих об'єктів

Поштовий антивірусник запитує власника пристрою дозвіл на проведення певних дій або об'єкт обробляється на основі параметрів, вибраних у налаштуваннях.

Програма захисту пошти від вірусу виводить повідомлення про свої дії, супроводжуючи їх виконання певним текстом:

- Message has been disinfected — видалені/виліковані об'єкти, що загрожують;

- Suspicious part has been quarantined – підозрілі файли, отримані з листом, відправлені до карантину;

- Message is infected або Message has a suspicious part — не знешкоджено виявлені заражені або потенційно небезпечні об'єкти.

Софт Поштового Антивірусу, страхуючи користувача від помилкового запуску файлу, де потенційно знаходиться вірус, самостійно змінює назви або видаляє файли, що мають розширення ".com", ".exe". Якщо вкладений файл перейменовано, замість останньої літери з'являється нижнє підкреслення.

Алгоритм дій Анти-спаму

Софт Анти-Спам, здійснивши перевірку отриманого листа, визначає його статус - спам, можливий спам, а також спам.

Застосовуються по черзі такі критерії оцінки:

Список відправників, від яких дозволено отримувати пошту, а також перелік фраз, наявність яких зацікавить власника e-mail - якщо відправник включений до "зеленого списку" або є заздалегідь обумовлена ​​фраза, лист оцінюється як "не спам".

Список відправників, від яких заборонено отримання листів або перелік фраз, наявність яких не цікавить власника поштової скриньки - якщо відправник значиться в «чорному списку» або загальна оцінка небажаних фраз, що використовуються в листі, перевищує 100%, лист визнається «спамом».

Аналізуються заголовки, використовуючи алгоритм, що самонавчається Байєса (аналіз тексту), оцінка вкладених зображень.

Шляхом аналізу структури визначається статус листа.

Після проведеної Анти-Спамом оцінки, у темі листа може з'явитися повідомлення:

- [!! SPAM] - листу надано статус «спам»;

- [?? Probable spam] - лист визнаний можливим спамом.

Як мають бути налаштовані порти

Перехоплення мережних інформпакетів, подальший контроль поштового трафіку із застосуванням протоколів POP3, SMTP, NNTP, IMAP, проводиться прийому пошти через стандартні порти.

Якщо використовуються нестандартні порти – вони додаються до списку, який перевіряються цими протоколами. Для перевірки, які порти контролюються, слід зайти в розділ налаштувань антивіруса Налаштування мережі.

## **3.3. Огляд Cisco Secure Email**

Клієнти стикаються з однією і тією ж страшною проблемою: електронна пошта одночасно є найважливішим інструментом ділового спілкування та провідним вектором атак для порушень безпеки. Cisco Email Security дозволяє користувачам безпечно спілкуватися та допомагає організаціям боротися з компрометацією ділової електронної пошти, програмами-вимагачами, сучасними шкідливими програмами, фішингом, спамом та втратою даних за допомогою багаторівневого підходу до безпеки.

Cisco Secure Email включає розширені можливості захисту від загроз для швидшого виявлення, блокування та усунення загроз, запобігання втраті даних та захисту важливої інформації при передачі за допомогою наскрізного шифрування.

Cisco Secure Email клієнти можуть:

* Виявляти та блокувати більше загроз за допомогою чудової аналітики загроз від Talos™, групи з дослідження загроз.
* Боротьба з програмами-вимагачами, прихованими у вкладеннях, які не виявляються при початковому виявленні, за допомогою Cisco Secure Email Malware Defense та Cisco Threat Grid.
* Автоматично видаляти електронні листи з небезпечними посиланнями або блокувати доступ до нещодавно заражених сайтів за допомогою аналізу URL-адрес в режимі реального часу для захисту від фішингу та BEC.
* Запобігання зловживанню торговельною маркою та витонченим атакам на електронну пошту за допомогою ідентифікаційних даних за допомогою Cisco Secure Email Domain Protection та Cisco Secure Email Phishing Defense.
* Захист конфіденційного вмісту вихідних повідомлень електронної пошти за допомогою функції запобігання втраті даних (DLP) та простого використання шифрування електронної пошти — все в одному вирішенні.
* Навчання користувачів за допомогою Cisco Secure Awareness Training, щоб допомогти користувачам працювати ефективніше та безпечніше.
* Гнучкість розгортання за допомогою хмарного, віртуального, локального або гібридного розгортання або поетапного переходу до хмари.
* Забезпечення інтеграцію з зростаючим числом продуктів Cisco Security та прискоріть ключові функції безпеки, такі як видимість, виявлення, автоматизація, розслідування та усунення за допомогою SecureX.

Характеристики та переваги

Сьогоднішні загрози безпеці електронної пошти складаються з програм-вимагачів, передових шкідливих програм, BEC, фішингу та спаму. Технологія Cisco Secure Email блокує загрози, тому компанії отримують лише легальні повідомлення. Cisco використовує декілька рівнів, щоб забезпечити максимальну комплексну безпеку електронної пошти, включаючи превентивні та відповідні заходи для посилення захисту.

Інформація про глобальні загрози

Отримайте швидкий комплексний захист електронної пошти за допомогою Talos, однієї з найбільших у світі мереж виявлення загроз. Talos забезпечує широку видимість та велику площу, в тому числі:

● 600 мільярдів електронних листів на день

● 16 мільярдів веб-запитів на день.

● 1,5 мільйона зразків шкідливих програм.

Talos надає 24-годинний огляд глобальної дорожньої активності. Він аналізує аномалії, виявляє нові загрози та відстежує тенденції трафіку. Talos допомагає запобігти атакам нульової години, постійно створюючи правила, які передають оновлення рішенням безпеки електронної пошти клієнтів. Ці оновлення відбуваються кожні три-п'ять хвилин, забезпечуючи найкращий у галузі захист від загроз.

Репутаційна фільтрація

Блокуйте небажану електронну пошту за допомогою фільтрації репутації на основі інформації про загрози від Talos. Для кожного вбудованого гіперпосилання виконується перевірка репутації для підтвердження цілісності джерела. Веб-сайти з поганою репутацією автоматично блокуються. Репутаційна фільтрація зупиняє 90 відсотків спаму ще до того, як він потрапить до мережі, що дозволяє масштабувати рішення за рахунок аналізу набагато меншого корисного навантаження.

Захист від спаму

Спам – складна проблема, що потребує складного вирішення. Cisco робить це легко. Cisco Secure Email блокує небажані електронні листи, використовуючи багаторівневу архітектуру сканування, що забезпечує найвищий рівень виявлення спаму, що перевищує 99 відсотків, із частотою неправдивих спрацьовувань менше одного на мільйон.

Функція захисту від спаму в Cisco Secure Email використовує механізм контекстноадаптивного сканування Cisco (CASE). Цей двигун перевіряє повний контекст повідомлення, у тому числі зміст повідомлення, структуру повідомлення, відправника повідомлення та куди веде заклик до дії повідомлення. Поєднуючи ці елементи, Cisco Secure Email блокує найширший спектр загроз з найкращою в галузі точністю.

Виявлення підробленої електронної пошти

Виявлення підробленої електронної пошти захищає від BEC-атак, спрямованих на керівників, які вважаються важливими цілями. Виявлення підробленої електронної пошти допомагає блокувати ці індивідуальні атаки та надає докладні журнали про всі спроби та вжиті дії.

Захист електронної пошти Cisco від фішингу

CAPP зупиняє атаки на основі обману особистих даних, таких як соціальна інженерія, шахраї та BEC, поєднуючи глобальну аналітику загроз Cisco Talos з локальною аналітикою електронної пошти та передовими методами машинного навчання для моделювання надійної поведінки електронної пошти в Інтернеті, всередині організацій та між окремими особами.

* Інтегрує методи машинного навчання для щоденного оновлення моделей, підтримуючи розуміння поведінки електронної пошти в режимі реального часу, щоб запобігти обману особистих даних.
* Поєднує в собі швидку звітність і відповідність автентифікації повідомлень домену (DMARC), розширений захист імен, що відображаються, і виявлення за допомогою самозванця домену для запобігання атак BEC.
* Моделює поведінку загрози захоплення облікового запису, щоб блокувати атаки, що виходять із скомпрометованих облікових записів електронної пошти.
* Розгортання в якості полегшеного датчика в хмарі або локально в середовищі замовника у вигляді розміщеної віртуальної машини (ВМ) на вибір або встановлення на «голе залізо». Будь ласка, зверніться до таблиці 7 для технічних характеристик обладнання віртуальної машини. Хмарний датчик надається як частина розгортання Cisco Cloud Email Security.
* Підтримує режим подвійної доставки. У цьому режимі датчик приймає копії повідомлень електронної пошти за простим протоколом передачі пошти (SMTP) та витягує метадані в потоковому режимі.

Захист домену електронної пошти Cisco Secure

CDP для зовнішньої електронної пошти допомагає запобігти надсиланню фішингових листів за допомогою домену (доменів) клієнта. Він автоматизує процес впровадження стандарту автентичності електронної пошти DMARC для кращого захисту співробітників, клієнтів та постачальників від фішингових атак з використанням домену(ів) клієнта. Це захищає ідентичність бренду клієнтів, а також підвищує ефективність маркетингу електронною поштою за рахунок зменшення влучення фішингових повідомлень до поштових скриньок.

Захист від вірусів

Пропонуючи високопродуктивне рішення для сканування вірусів, інтегроване в шлюз, Cisco Secure Email забезпечує багаторівневий підхід до фільтрації вірусів від різних постачальників.

Виявлення сірої пошти та безпечна відписка

Сіра пошта складається з маркетингу, соціальних мереж та масових повідомлень. Функція виявлення сірої пошти точно класифікує та відстежує сіру пошту, що надходить до організації. Потім адміністратор може вжити відповідних дій для кожної категорії. Часто в сірій пошті є посилання на відмову від підписки, за якою кінцеві користувачі можуть вказати відправнику, що вони хотіли б відмовитися від отримання таких електронних листів. Оскільки імітація механізму відписки є популярною технікою фішингу, користувачі повинні обережно натискати на ці посилання для відписки.

Безпечне рішення для відмови від підписки забезпечує:

* Захист від шкідливих загроз, що маскуються під посилання відписки.
* Єдиний інтерфейс для керування підписками.

Найкраща видимість таких листів для адміністраторів електронної пошти та кінцевих користувачів.

Захист від шкідливих програм та Cisco Threat Grid

Malware Defense та Threat Grid забезпечують оцінку та блокування репутації файлів, ізольоване програмне середовище та ретроспекцію файлів для безперервного аналізу загроз. Користувачі можуть блокувати більше атак, відстежувати підозрілі файли, зменшувати масштаб епідемії та швидко усувати її. Cisco Secure Email також інтегрується із захистом від шкідливих програм для кінцевих точок. Захист від шкідливих програм для кінцевих точок надає інформацію про загрози для всього середовища клієнта, забезпечуючи уніфікацію безпеки кінцевих точок, мережі, електронної пошти, хмар та Інтернету.

Завдяки цим інтеграціям захист від шкідливих програм автоматично зіставляє файли, дані телеметрії, поведінку та активність для проактивного захисту від складних загроз у всіх можливих напрямках.

Автоматичне виправлення поштових скриньок для клієнтів Microsoft 365 допомагає усувати порушення швидше та з меншими зусиллями. Клієнти просто налаштовують своє рішення для захисту електронної пошти на виконання автоматичних дій із цими зараженими електронними листами.

Клієнти можуть придбати додаткову ліцензію для повністю локального розгортання системи захисту від шкідливих програм за допомогою приватної хмари захисту від шкідливих програм. Це, поряд із Threat Grid, забезпечує повний локальний захист від шкідливих програм.

SecureX

Архітектурний підхід до інтегрованих продуктів безпеки означає ефективний обмін інформацією про загрози та багато іншого. Реагування на загрози SecureX забезпечує більш швидку та синхронізовану реакцію по всьому портфоліо.

Захист та контроль, пов'язані з URL

Користувачі захищені від шкідливих URL-адрес за допомогою фільтрації URL-адрес, сканування URL-адрес у вкладеннях та керованих (скорочених) URL-адрес. До повідомлень застосовуються відповідні політики залежно від репутації або категорії URL-адрес.

Фільтри спалахів

Фільтри епідемій захищають від нових загроз та змішаних атак. Вони можуть створювати правила для будь-якої комбінації шести параметрів, включаючи тип файлу, ім'я файлу, розмір файлу та URL-адресу в повідомленні. У міру того, як Talos дізнається більше про спалах, він може відповідним чином змінювати правила та звільняти повідомлення з карантину. Фільтри епідемій також можуть переписувати URL-адреси, пов'язані з підозрілими повідомленнями. При натисканні нові URL-адреси перенаправляють одержувача через проксі-сервер Cisco Web Security.

Потім вміст веб-сайту активно сканується, і фільтри епідемій відображають користувачеві екран блокування, якщо сайт містить зловмисне програмне забезпечення.

Відстеження веб-взаємодії

Відстеження веб-взаємодії – це повністю інтегроване рішення, яке дозволяє ІТ-адміністраторам відслідковувати кінцевих користувачів, які натискають на URL-адреси, які були переписані Cisco Secure Email. Звіти показують:

● Найпопулярніші користувачі, які натискали на шкідливі URL-адреси.

● Найчастіше використовувані кінцевими користувачами шкідливі URL-адреси.

Дату і час, щоб переписати причину та дію, зроблену для URL-адрес.

Cisco Secure Email пропонує ефективне DPL та шифрування електронної пошти. Централізоване управління та звітність спрощують захист даних.

DLP

Захист вихідних повідомлень за допомогою Cisco Secure Email DLP. Вибір з великої бібліотеки політик, що містить понад 100 експертних політик, що охоплюють правила уряду, приватного сектору та компаній. Передбачені політики захисту від втрати даних включені до Cisco Secure Email та спрощують застосування політики вихідної електронної пошти з урахуванням вмісту. Варіанти виправлення включають шифрування, додавання нижніх колонтитулів та заяв про відмову від відповідальності, додавання сліпих копій (BCC), повідомлення та поміщення в карантин. Для компаній, яким потрібна складна політика користувача, стандартні блоки визначених політик легко доступні, щоб зробити процес швидким і легким.

Шифрування

Завдяки шифруванню електронної пошти відправники не бояться друкарських помилок в адресах одержувачів, помилок у змісті або термінових електронних листів, оскільки вони завжди можуть заблокувати повідомлення. Відправник зашифрованого повідомлення отримує повідомлення прочитання, як тільки одержувач відкриває повідомлення, а високозахищені відповіді та переадресація автоматично шифруються для забезпечення наскрізної конфіденційності та контролю. Додаткова інфраструктура для розгортання не потрібна. З метою підвищення безпеки вміст повідомлення передається прямо від шлюзу до одержувача, а в хмарі зберігається тільки ключ шифрування.

Вимоги до шифрування для таких нормативних актів, як Стандарт безпеки даних індустрії платіжних карток (PCI DSS), Закон про переносимість та підзвітність медичного страхування (HIPAA), Закон Гремма-Ліча-Блайлі (GLBA) або Закон Сарбейнса-Окслі (SOX) - а також державні правила конфіденційності та європейські директиви - не обтяжуючи відправників, одержувачів або адміністраторів електронної пошти.

Керованість

Універсальна підтримка пристроїв

Всі користувачі можуть отримувати доступ до повідомлень, коли це необхідно, незалежно від того, чи вони використовують смартфони, планшети, ноутбуки або настільні комп'ютери. Універсальна підтримка пристроїв призначена для того, щоб повідомлення з високим ступенем захисту могли бути прочитані будь-яким одержувачем, незалежно від того, який пристрій використовується для відкриття повідомлення. Спеціалізовані програми, що підключаються, забезпечують розширений інтерфейс для Microsoft Outlook, а також для смартфонів і планшетів Apple iOS і Google Android.

Панель огляду системи

Відстеження та повідомлення про вихідні повідомлення з централізованої панелі огляду системи, що настроюється. Уніфікована бізнес-звітність пропонує єдину виставу для всебічного аналізу організації.

Детальне відстеження повідомлень

Слідкування за повідомленням одержувача конверта, відправника конверта, теми, вкладень та подій повідомлення, включаючи політику захисту від втрати даних або ідентифікатори. Коли надсилається повідомлення до Cisco Secure Email, база даних відстеження повідомлень заповнюється протягом хвилини або двох, і можна бачити, що сталося з повідомленнями, що проходять через систему, на кожному етапі обробки.

Навчання безпеки

Забезпечує гнучкість та підтримку для ефективного розгортання моделювання фішингу та підвищення обізнаності, а також для вимірювання та складання звітів про результати. Він фокусується на навчанні поведінки користувачів для внесення довгострокових змін та дає групі операцій із забезпечення безпеки можливість усувати загрози у реальному часі.

Високоякісний контент, який включає конструктор курсів з більш ніж 150 навчальними модулями на вибір, навчання на основі ролей і високоінтерактивний контент з гейміфікацією для залучення користувачів.

Інтуїтивно зрозумілий фішинговий симулятор, що пропонує готові сценарії фішингу, що відображають реальні кібер- та фішингові загрози, які інтегровані з навчанням для своєчасного зворотного зв'язку.

Багатомовний контент та платформа з підтримкою понад 40 мов (озвучення та текст) для забезпечення доступності програм підвищення безпеки по всьому світу.

Комунікаційні та допоміжні матеріали, що надаються великими бібліотеками попередньо розробленого контенту та шаблонів для просування внутрішньої кампанії та посилення контенту (включаючи відео, плакати та інформаційні бюлетені).

Консультативний підхід з унікальними пропозиціями, включаючи інструктаж з інформаційної безпеки, керовані послуги та налаштування контенту, щоб допомогти організаціям розробити та оптимізувати стратегію забезпечення безпеки.

Ліцензії на програмне забезпечення Cisco для безпечної електронної пошти

Існує три пакети програмного забезпечення для забезпечення безпеки електронної пошти: Cisco Secure Email Inbound Essentials, Cisco Secure Email Outbound Essentials та Cisco Secure Email Premium; також доступні додаткові автономні опції (див. Таблицю 2). Просто придбайте відповідні ліцензії для кількості поштових скриньок, які необхідно підтримувати. Для хмарних та віртуальних пристроїв просто замовте ліцензії на програмне забезпечення, щоб отримати права.

* Термінові ліцензії на підписку
* Ліцензії є терміновими підписками на 1, 3 або 5 років.
* Ліцензії на підписку на основі кількості

Портфоліо Cisco Secure Email використовує багаторівневе ціноутворення залежно від кількості поштових скриньок. Представники відділу продажу та партнерів допоможуть визначити правильне розгортання клієнтів.

Основи безпечної вхідної електронної пошти Cisco

Пакет Cisco Secure Email Inbound Essentials забезпечує захист від загроз, пов'язаних з електронною поштою, і включає захист від спаму, виявлення сірої пошти, антивірусне рішення Sophos, фільтри епідемій і виявлення підробленої електронної пошти.

Microsoft 365 Cisco Secure Email Inbound Essentials

Пакет Cisco Secure Email Inbound Essentials забезпечує захист від загроз, пов'язаних з електронною поштою, і включає захист від спаму, виявлення сірої пошти, фільтри епідемій та виявлення підробленої електронної пошти.

Cisco Secure Email Inbound Essentials плюс захист від шкідливих програм та Cisco Threat Grid

Пакет Cisco Secure Email Inbound Essentials забезпечує захист від загроз, пов'язаних з електронною поштою, і включає захист від спаму, виявлення сірої пошти, антивірусне рішення Sophos, фільтри епідемій і виявлення підробленої електронної пошти.

Захист від шкідливих програм можна придбати разом із будь-яким пакетом програмного забезпечення Cisco Secure Email.

Threat Grid and Malware Defense розширює можливості виявлення та блокування шкідливих програм, які вже пропонуються в Cisco Secure Email, за рахунок оцінки та блокування репутації файлів, пісочниці та ретроспекції файлів для безперервного аналізу загроз навіть після того, як вони пройшли через шлюз електронної пошти. Malware Defense та Threat Grid тепер можна повністю розгорнути локально за допомогою віртуального пристрою Malware Defense Private Cloud Virtual Appliance.

Основи вихідної електронної пошти Cisco Secure

Пакет Cisco Secure Email Outbound Essentials захищає від втрати даних завдяки відповідності DLP та шифруванню електронної пошти.

Безпечна електронна пошта Cisco Premium

Пакет Cisco Secure Email Premium поєднує засоби захисту вхідного та вихідного трафіку, включені до згаданих вище ліцензій Cisco Secure Email Inbound та Outbound Essentials для захисту від загроз, пов'язаних з електронною поштою, а також необхідні DLP та шифрування.

Microsoft 365 Cisco Secure Email Premium

Пакет Cisco Secure Email Premium поєднує засоби захисту вхідного та вихідного трафіку, включені до ліцензій Cisco Secure Email Inbound та Cisco Secure Email Outbound Essentials для Office 365, згадані вище, для захисту від загроз, пов'язаних з електронною поштою, а також необхідні DLP та шифрування.

Cisco Secure Email Premium плюс захист від шкідливих програм та Cisco Threat Grid

Пакет Cisco Secure Email Premium поєднує засоби захисту вхідного та вихідного трафіку, включені до згаданих вище ліцензій Cisco Secure Email Inbound та Outbound Essentials для захисту від загроз, пов'язаних з електронною поштою, а також необхідні DLP та шифрування.

Захист від шкідливих програм можна придбати разом із будь-яким пакетом програмного забезпечення Cisco Secure Email.

Threat Grid та Malware Defense розширюють можливості виявлення та блокування шкідливих програм, які вже пропонуються у Cisco Secure Email, за рахунок оцінки та блокування репутації файлів, пісочниці та ретроспекції файлів для безперервного аналізу загроз, навіть після того, як вони пройшли через поштовий шлюз. Malware Defense та Threat Grid тепер можна повністю розгорнути локально за допомогою віртуального пристрою Malware Defense Private Cloud Virtual Appliance.

Захист від шкідливих програм та Cisco Threat Grid

Захист від шкідливих програм можна придбати разом із будь-яким пакетом програмного забезпечення Cisco Secure Email.

Threat Grid and Malware Defense розширює можливості виявлення та блокування шкідливих програм, які вже пропонуються в Cisco Secure Email, за рахунок оцінки та блокування репутації файлів, пісочниці та ретроспекції файлів для безперервного аналізу загроз навіть після того, як вони пройшли через шлюз електронної пошти. Malware Defense та Threat Grid тепер можна повністю розгорнути локально за допомогою віртуального пристрою Malware Defense Private Cloud Virtual Appliance.

Інтелектуальне мультисканування

Intelligent Multi-Scan (IMS) – це високопродуктивне багаторівневе рішення для захисту від спаму, в якому використовується комбінація механізмів захисту від спаму, у тому числі Cisco Anti-Spam, для збільшення швидкості виявлення спаму.

Graymail

Graymail тепер можна помітити справді безпечною опцією відмови від передплати. Цей тег керує безпечною дією скасування підписки від імені кінцевого користувача. Він також відстежує різні запити на скасування підписки сірої пошти. Усім цим можна управляти лише на рівні групи політики полегшеного протоколу доступу до каталогів (LDAP).

Захист електронної пошти Cisco від фішингу

CAPP можна придбати разом із будь-яким пакетом програмного забезпечення Cisco Secure Email. CAPP зупиняє атаки, що базуються на обмані особистих даних, такі як соціальна інженерія, самозванці та BEC. Він забезпечує локальну аналітику електронної пошти та передові методи машинного навчання для моделювання надійної поведінки електронної пошти в Інтернеті, всередині організацій та між окремими особами. CAPP також інтегрує методи машинного навчання для щоденного оновлення моделей, підтримуючи розуміння поведінки електронної пошти в режимі реального часу, щоб запобігти обману особистості. Пропонується лише для підписки на один та три роки.

Захист домену електронної пошти Cisco Secure

CDP можна придбати разом із будь-яким пакетом програмного забезпечення Cisco Secure Email. CDP для зовнішньої електронної пошти допомагає запобігти надсиланню фішингових листів за допомогою домену (доменів) клієнта. Служба CDP автоматизує процес впровадження стандарту автентифікації електронної пошти DMARC, щоб краще захистити співробітників, клієнтів та постачальників від фішингових атак з використанням домену(ів) клієнта. Це захищає ідентичність бренду клієнтів, а також підвищує ефективність маркетингу електронною поштою за рахунок зменшення влучення фішингових повідомлень до поштових скриньок. Пропонується лише для підписки на один та три роки.

Аналізатор зображень

Виявляє незаконний контент у вхідній та вихідній електронній пошті, дозволяючи клієнтам виявляти, відстежувати та навчати користувачів-порушників.

Навчання безпеки Cisco

Навчання Cisco Secure Awareness можна придбати разом із будь-яким пакетом програмного забезпечення Cisco Secure Email. Він розроблений, щоб допомогти просувати і застосовувати здоровий глузд ефективної кібербезпеки, змінюючи поведінку кінцевих користувачів і надаючи співробітникам можливість працювати ефективніше і безпечніше. Ця хмарна підписка забезпечує всебічне моделювання, навчання та звітність, тому прогрес співробітників можна постійно відстежувати та відстежувати. Це допомагає організаціям залишатися в безпеці з привабливим та актуальним комп'ютерним контентом з різними методами імітації атак та дозволяє людям у організації відігравати вирішальну роль у її спільній безпеці за допомогою Cisco Secure Awareness Training.

Всі варіанти розгортання Cisco Secure Email мають найпростіший підхід до реалізації. Майстер налаштування системи може працювати навіть зі складними середовищами та забезпечить захист всього за кілька хвилин, що зробить безпеку швидше. Ліцензування засноване на унікальному користувачі, а не на пристрої, тому можнавикористовувати його для кожного унікального користувача, а не для кожного пристрою, щоб забезпечити захист шлюзу вхідної та вихідної електронної пошти без додаткових витрат.

Хмара

Cisco Secure Email у хмарі надає гнучку модель розгортання для захисту електронної пошти. Це допоможе скоротити витрати завдяки спільному управлінню та відсутності локальної інфраструктури безпеки електронної пошти. Виділені системи безпеки електронної пошти в кількох центрах обробки даних Cisco відмовляються від високого рівня доступності послуг та захисту даних. Клієнти зберігають доступ до хмарної інфраструктури (і видимість її), а комплексна звітність та відстеження повідомлень допомагають забезпечити гнучкість адміністрування. Ця послуга включає комплексне програмне забезпечення, обчислювальну потужність і підтримку для простоти.

Віртуальний пристрій Cisco Secure Email Virtual Appliance значно знижує вартість розгортання системи безпеки електронної пошти, особливо в розподілених мережах. Цей пристрій дозволяє мережному адміністратору створювати екземпляри там, де і коли вони необхідні, використовуючи існуючу мережну інфраструктуру. Програмна версія фізичного пристрою працює поверх гіпервізора VMware ESXi та серверів Cisco Unified Computing System™ (Cisco UCS®).

За допомогою віртуального пристрою можна миттєво реагувати на зростання трафіку завдяки спрощеному плануванню ємності. Не потрібно купувати та доставляти пристрої, тому можна підтримувати нові можливості для бізнесу, не ускладнюючи центр обробки даних та не наймаючи додатковий персонал.

Локально

Cisco Secure Email Appliance – це шлюз, який зазвичай розгортається на межі мережі за межами брандмауера (так звана демілітаризована зона). Вхідний SMTP-трафік надсилається на інтерфейс даних пристрою відповідно до специфікацій, встановлених записами поштового обміну. Пристрій фільтрує його та повторно доставляє на мережевий поштовий сервер. Поштовий сервер також надсилає вихідну пошту на інтерфейс даних, де вона фільтрується відповідно до вихідних політик, а потім доставляється зовнішнім адресатам.

Гібридний

Гібридне рішення забезпечує максимальну гнучкість. Можна комбінувати будь-які варіанти розгортання відповідно до потреб. Наприклад, можна скористатися перевагою захищеної електронної пошти Cisco у хмарі для захисту від загроз у вхідних повідомленнях, а також впровадити контроль над конфіденційними повідомленнями на місці. Також можна розгорнути захист від вхідних загроз локально та у хмарі, щоб перейти у хмару у зручному темпі.

Можна запустити локальну та віртуальну Cisco Secure Email в тому самому розгортанні. Таким чином, невеликі філії або віддалені офіси можуть мати той самий захист, який отримується у штаб-квартирі, без необхідності встановлювати та підтримувати обладнання у цих місцях. Можна легко керувати розгортаннями користувача за допомогою Cisco Secure Email and Web Manager або Cisco Secure Email and Web Manager Virtual.

# ВИСНОВКИ

Електронна пошта — найпопулярніший канал ділового спілкування, яким кожен день проходять десятки і сотні тисяч листів з важливою і часто конфіденційною інформацією. Тому дуже часто корпоративна пошта піддається різним атакам.

Оскільки електронні листи зараз широко використовуються, вони стали засобом поширення вірусів, спаму, фішингових атак, таких як використання використання хибних повідомлень для того, щоб спонукати одержувачів розголосити конфіденційну інформацію, відкрити вкладення або перейти за небезпечним посиланням. Безпека електронної пошти користувача – співробітника компанії – часто є вразливим місцем, яким користуються зловмисники для отримання доступу до корпоративної мережі та важливих внутрішніх даних компанії. Також може бути атакований корпоративний поштовий сервер до повної зупинки його роботи. У ситуації, наприклад, інтернет-магазину, який приймає поштою замовлення, або будь-якого сервісу, для якого потрібне підтвердження реєстрації поштою, це може спричинити серйозні збитки та репутаційні втрати.

Способи та засоби захисту електронної пошти

На жаль, єдиного надійного способу захисту електронної пошти немає. Безпеку систем електронної пошти можна забезпечити лише за допомогою комплексу заходів, які включають:

* Вибір розташування сервера, забезпечення мережної безпеки
* Використання міжмережевого екрану або спеціалізованого Email Security Appliance
* Контроль доступу до корпоративної пошти, визначення привілеїв кожної категорії користувачів на поштовий та інші сервера забезпечення
* Використання шифрування для захисту повідомлень електронної пошти — навіть якщо вони будуть перехоплені, їх буде неможливо прочитати.
* Використання спеціалізованих антивірусів
* Засобів захисту електронної пошти для фільтрації спаму
* Навчання співробітників основ інформаційної безпеки
* Захист email від злому та хакерів

Необхідно мінімізувати ймовірність того, що хтось сторонній отримає доступ до корпоративної мережі та пошти. Для цього використовуються міжмережеві захисні екрани та політики безпеки мережі. Щоб захистити вміст листів та вкладень, застосовується шифрування, тоді їх неможливо буде прочитати навіть у разі перехоплення.

Налаштування безпеки пошти має включати SSL-шифрування для взаємної автентифікації сервера та клієнта; використання VPN для підключення до віддалених поштових клієнтів; захист від DDos-атак на поштові сервери; захист електронної пошти від вірусів У захисті корпоративної пошти допоможе установка спеціалізованого апаратного та програмного забезпечення, яке порівнюватиме нове ПЗ з відомим списком вірусів, аналізувати його "поведінку" - чи воно є загрозливим - і блокуватиме атаки.

Захист пошти від спаму та фішингу зазвичай реалізується за допомогою багаторівневої системи фільтрів, які перевіряють репутацію сервера-відправника, фільтрів на основі записів SPF (список серверів, з яких дозволено приймати пошту), DKIM (перевірка, що вміст листа не змінювався), DMARC, “чорних” та “білих” списків заборонених/дозволених відправників. Програми для захисту Існує безліч програм для забезпечення безпеки електронної пошти:

* PGP для шифрування та цифрового підпису повідомлень, зараз існують плагіни для браузерів та поштових клієнтів, що реалізують цю технологію
* Захищені поштові сервери
* Поштові антивіруси,
* Комплексні рішення, такі як захист електронної пошти Cisco.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Steven Furnell, Paul Dowland. Email Security: A Pocket Guide. IT Governance Publishing. Released November 2010. – 64 c.
2. Email Security with Cisco IronPort. Cisco Press. Released April 2012. – 10 c.
3. 7 Common Email Security Protocols Explained [Електронний ресурс]. – Режим доступу: <https://www.makeuseof.com/tag/common-email-security-protocols-explained/>
4. Email Security Software Reviews 2022 [Електронний ресурс]. – Режим доступу: <https://www.gartner.com/reviews/market/email-security>
5. The Top 11 Email Security Gateways [Електронний ресурс]. – Режим доступу: <https://expertinsights.com/insights/top-11-email-security-gateways/>
6. What Is Email Security? [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/c/en/us/products/security/what-is-email-security.html>
7. Cisco Secure Email Cloud Mailbox At-A-Glance [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/cloud-mailbox-defense-aag.html>
8. Cisco Secure Emai [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/c/en/us/products/security/email-security/index.html>
9. Cisco Secure Email Cloud Mailbox [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/c/en/us/products/security/cloud-mailbox-defense/index.html>
10. Cisco Secure Email Advanced Email Protection Data Sheet [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/datasheet-c78-742868.html>

# ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)