ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

« Дослідження шляхів та розробка рекомендацій захисту та протидії фішинговим атакам електронної пошти корпоративної системи на базі рішення SpamAssassin »

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

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

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

_____ Максим КИРКАЧ
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
КИРКАЧ Максим
(прізвище, ім'я)

Керівник асистент БОЙКО Анна
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
"___" _____ 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Киркачу Максиму
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розробка рекомендацій захисту та протидії фішинговим атакам електронної пошти корпоративної системи на базі рішення Spam Assasin»

керівник кваліфікаційної роботи Бойко Анна, асистент
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2024 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.05.2024 р.

3. Вихідні дані до кваліфікаційної роботи
програмний комплекс для віртуалізації
рішення SpamAssasin
технічна література, експлуатаційна документація

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблематики виявлення фішингових атак
2. Аналіз наявних рішень напрямку протидії фішингу.
3. Розробка рекомендацій щодо розгортання антифішингових рішень

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 15.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми виявлення фішингу		
2.	Аналіз технічної літератури з питань теми кваліфікаційної роботи.		
3.	Аналіз проблематики виявлення фішингових атак		
4.	Аналіз наявних антифішингових рішень, детальний огляд рішення SpamAssassin		
5.	Розробка рекомендацій щодо розгортання SpamAssassin		
6.	Оформлення результатів дослідження.		
7.	Підготовка доповіді до захисту.	31.05.2024 р.	

Здобувач вищої освіти _____ Максим КИРКАЧ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Анна БОЙКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача КИРКАЧ Максим
на тему: «Дослідження шляхів та розробка рекомендацій захисту та протидії фішинговим атакам електронної пошти корпоративної системи на базі рішення Spam Assasin»

Актуальність: Захист корпоративної електронної пошти набуває особливої важливості в умовах зростання кіберзагроз. Фішингові атаки становлять значну небезпеку для компаній, оскільки можуть призвести до витоку конфіденційної інформації та фінансових втрат. Вибір теми дослідження є своєчасним, оскільки застосування рішення SpamAssassin сприяє ефективному виявленню та блокуванню фішингових атак, зменшуючи ризики несанкціонованого доступу до даних та забезпечуючи безпеку комунікацій. Це дослідження спрямоване на вдосконалення методів протидії фішинговим атакам, що є надзвичайно актуальним у сучасному кіберпросторі.

Позитивні сторони:

1. Дипломна робота містить детальний аналіз проблеми фішингових атак на корпоративні системи електронної пошти. Автор чітко формулює цілі та завдання, зосереджуючись на застосуванні інструменту SpamAssassin.
2. У роботі ретельно досліджені методи та засоби виявлення фішингових атак, акцентуючи увагу на можливостях SpamAssassin.
3. Представлені рекомендації щодо інтеграції SpamAssassin у корпоративні системи електронної пошти для підвищення рівня захисту є чіткими та практично значущими.
4. Текст роботи добре структурований, логічно та грамотно викладений.

Недоліки:

1. Аналіз практичного застосування SpamAssassin на прикладі конкретної організації міг би надати більш практичну перспективу та допомогти в кращому розумінні ефективності запропонованих методів.

Відзначене зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **Киркач Максим** – присвоєння кваліфікації бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Рецензент:

_____	_____	_____
(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач Киркач Максим до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розробка рекомендацій захисту та протидії фішинговим атакам електронної пошти корпоративної системи на базі рішення Spam Assasin».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***Киркач Максим*** обрав тему роботи, зосереджену на дослідженні методів захисту від фішингових атак електронної пошти корпоративних систем і розробці рекомендацій для їх виявлення та протидії. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***Киркач Максим*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***Киркача Максима*** на оцінку **"добре"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Анна БОЙКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **Киркач Максим** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)
_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 51 сторінку, 15 рисунків, 2 таблиці, 15 джерел.

Об'єкт дослідження – процеси захисту корпоративних систем електронної пошти від фішингових атак.

Предмет дослідження – методи та засоби виявлення та блокування фішингових атак на базі рішення Spam Assasin.

Методи дослідження – аналіз технічної літератури та наукових джерел для визначення основних принципів та переваг використання Spam Assasin; дослідження документації та випадків використання Spam Assasin для захисту корпоративних систем електронної пошти; проведення експериментального аналізу з використанням Spam Assasin на тестових даних для оцінки ефективності виявлення фішингових атак; порівняльний аналіз рішень для виявлення унікальних переваг Spam Assasin.

Захист електронної пошти є ключовим елементом у системі кібербезпеки будь-якої організації, особливо в умовах зростання кількості фішингових атак. Використовуючи різні методи аналізу електронних листів, Spam Assasin дозволяє виявляти та блокувати потенційні фішингові атаки, забезпечуючи захист конфіденційної інформації та зменшуючи ризики фінансових втрат. Особлива увага у дослідженні приділена застосуванню інструменту Spam Assasin, який інтегрується у корпоративні системи електронної пошти та забезпечує високий рівень безпеки комунікацій.

Дослідження охоплює методи і засоби застосування Spam Assasin, з особливим акцентом на його можливостях щодо виявлення та блокування фішингових атак. Аналізовано технічну літературу та наукові джерела, проведено експериментальний аналіз за допомогою Spam Assasin, і виявлено переваги застосування цього рішення порівняно з альтернативними методами.

В результаті дослідження розроблено рекомендації щодо інтеграції Spam Assasin у корпоративні системи електронної пошти, спрямовані на забезпечення вищого рівня захисту від фішингових атак. Практичне застосування результатів роботи може бути корисним у будь-якій організації, де критично важливо забезпечити надійність і безпеку комунікацій.

Галузь використання – кібербезпека інформаційних ресурсів організації.

АНАЛІЗ ФІШИНГОВИХ АТАК, SPAMASSASSIN, ЕЛЕКТРОННА ПОШТА,

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DOS – (denial-of-service) атака “відмови в обслуговуванні”

DMARC – Domain-based Message Authentication, Reporting & Conformance

DKIM – DomainKeys Identified Mail

SPF – Sender Policy Framework

2FA – two factor authentication

MitM – Man-in-the-Middle

DNSBL – Domain Name System Black List (“чорний” список доменних імен)

Sandbox – Пісочниця (система ізоляції для виконання та аналізування небезпечних та шкідливих файлів)

CRM – Customer relationship management

http – Hypertext Transfer Protocol

ВСТУП

Актуальність дослідження. У сучасному цифровому середовищі, де велика кількість бізнесових, наукових, освітніх та повсякденних процесів залежить від електронної пошти, питання її захисту набуває особливої ваги. Фішингові атаки можуть спричинити втрату важливої інформації, збитки в області фінансів чи репутації, а також створити серйозні загрози національній безпеці. Для України, забезпечення кібербезпеки є надзвичайно актуальним і це вимагає впровадження передових технологій захисту електронної пошти.

Технології виявлення та блокування фішингових атак є ключовими превентивними заходами, що дозволяють своєчасно ідентифікувати загрози. Використання рішення SpamAssassin суттєво знижує ризики несанкціонованого доступу до ресурсів організації, витоку конфіденційної інформації та інших кіберінцидентів. Програмне забезпечення SpamAssassin є одним із лідерів у цій галузі, що не лише дозволяє виявляти фішингові листи, але й забезпечує їх автоматичне блокування, інтегруючись із сучасними системами управління електронною поштою.

Дослідження цієї теми допоможе не тільки систематизувати наявні знання та передові практики застосування SpamAssassin у різних організаціях, але й виявити недоліки цих процесів, пропонуючи шляхи їх покращення та впровадження на різних етапах управління електронною поштою. Отже, це дослідження не тільки охоплює загальні аспекти кібербезпеки, але й орієнтоване на вирішення конкретних завдань, з якими стикаються адміністратори систем та фахівці з кібербезпеки в сучасних умовах.

Об'єкт дослідження – процеси захисту корпоративних систем електронної пошти від фішингових атак.

Предмет дослідження – методи та засоби виявлення та блокування фішингових атак на базі рішення Spam Assasin.

Мета роботи – розробити рекомендації щодо застосування на практиці рішення SpamAssassin

Наукові завдання:

дослідити сутність проблеми виявлення фішингових загроз;

проаналізувати основні методики виявлення загроз;

проаналізувати існуючі рішення для виявлення загроз;

проаналізувати методи та засоби пошуку загроз на базі базі рішення SpamAssassin;

розробити рекомендації щодо застосування рішення SpamAssassin на корпоративному рівні;

Методи дослідження – аналіз технічної літератури та наукових джерел, опрацювання стандартів та інтернет-джерел.

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування SpamAssassin для передбачення та усунення загроз.

1 АНАЛІЗ ПРОБЛЕМИ ПРОТИДІЇ ФІШИНГУ В ЕЛЕКТРОННИХ ПОШТАХ

1.1 Значення електронної пошти в корпоративних інформаційних системах

Електронна пошта є ключовим інструментом комунікації у корпоративних інформаційних системах. Вона забезпечує швидкий та ефективний обмін інформацією між співробітниками, партнерами та клієнтами, сприяючи координації діяльності та підвищенню продуктивності роботи.

Електронна пошта використовується для передачі важливих документів, обговорення проектів, організації зустрічей та збереження історії комунікацій, що є невід'ємною частиною бізнес-процесів. Крім того, вона служить важливим засобом для маркетингових кампаній та підтримки клієнтів, що робить її критичною складовою успішної діяльності будь-якої організації.

Важливість електронної пошти в корпоративних системах також визначається необхідністю захисту конфіденційної інформації та забезпечення безпеки даних, що обумовлює впровадження передових технологій захисту від кіберзагроз, зокрема фішингових атак.

Окрім цього, електронна пошта виконує роль платформи для інтеграції з іншими корпоративними системами, такими як системи управління проектами, CRM-системи та інші інструменти для підвищення ефективності роботи компанії. Це дозволяє створювати цілісне інформаційне середовище, де всі необхідні дані доступні в одному місці.

Електронна пошта також є важливим елементом у процесі прийняття рішень, оскільки дозволяє швидко отримувати необхідну інформацію, обмінюватися думками та узгоджувати дії. Зважаючи на її критичну роль, забезпечення безпеки електронної пошти стає першочерговим завданням для будь-якої організації. Це включає захист від спаму, фішингових атак, вірусів та інших кіберзагроз, які

можуть призвести до витоку конфіденційної інформації або порушення нормальної роботи компанії.

Важливість електронної пошти можна побачити в згадуванні її в “Положенні про Єдину базу даних електронних адрес, номерів факсів (телефаксів) суб`єктів владних повноважень”

Тобто, електронна пошта, як частина комунікаційної інфраструктури, використовується на рівні держави, а отже забезпечення безпеки є критично важливим для уникнення можливих витоків інформації та дискредитування структури як такої.

З основних складових важливості електронної пошти в компанії можна виділити наступні:

Основний засіб комунікації: Електронна пошта є основним засобом комунікації у більшості компаній. Вона дозволяє співробітникам швидко і ефективно обмінюватися інформацією як всередині компанії, так і з зовнішніми партнерами, клієнтами та постачальниками.

Офіційний канал зв'язку: Електронна пошта часто використовується для офіційних комунікацій, таких як надсилання важливих документів, угод, звітів та іншої офіційної кореспонденції. Це надає їй статусу офіційного каналу зв'язку.

Інструмент для організації роботи: За допомогою електронної пошти можна планувати зустрічі, відправляти запрошення на заходи, організовувати робочі процеси та координувати діяльність різних відділів компанії.

Збереження історії комунікацій: Електронна пошта дозволяє зберігати історію комунікацій, що може бути корисним для відстеження ходу проектів, прийняття рішень та вирішення суперечок.

Швидкість і ефективність: Електронна пошта забезпечує швидкий обмін інформацією, що дозволяє зекономити час і підвищити продуктивність праці. Співробітники можуть оперативно отримувати відповіді на свої запити та швидко реагувати на зміни.

Глобальна доступність: Електронна пошта доступна з будь-якої точки світу, що робить її ідеальним інструментом для комунікації у міжнародних компаніях та для співробітників, які працюють віддалено.

Інтеграція з іншими системами: Електронна пошта може бути інтегрована з іншими корпоративними системами, такими як CRM, ERP, системами управління проектами та іншими інструментами. Це дозволяє створювати єдине інформаційне середовище і забезпечувати доступ до необхідних даних у будь-який час.

Маркетингові кампанії: Електронна пошта є важливим інструментом для проведення маркетингових кампаній. Вона дозволяє компаніям надсилати новини, рекламні матеріали, опитування та іншу інформацію безпосередньо до клієнтів, що сприяє підвищенню лояльності та залученню нових клієнтів.

Безпека інформації: Електронна пошта може бути налаштована з високим рівнем безпеки, включаючи шифрування даних та автентифікацію користувачів. Це забезпечує захист конфіденційної інформації та знижує ризики витоку даних.

1.2. Аналіз загроз для безпеки електронної пошти

Електронна пошта є одним з основних засобів комунікації в сучасних корпоративних інформаційних системах. Однак, з її широким використанням зростає і кількість загроз, спрямованих на порушення безпеки електронної пошти. Фішингові атаки, спам, шкідливе програмне забезпечення та інші кіберзагрози можуть призвести до значних фінансових втрат, компрометації конфіденційних даних та серйозних порушень у роботі компанії. Цей розділ присвячений огляду основних загроз для безпеки електронної пошти та методів їх нейтралізації, що є критично важливими для забезпечення надійності та безперебійної роботи корпоративних систем.

Фішингові атаки

Фішинг – це один з найпоширеніших видів кіберзлочинів, який спрямований на обман користувачів з метою отримання конфіденційної інформації, такої як логіни, паролі, або фінансові дані. Зловмисники надсилають шахрайські електронні

листи, що імітують повідомлення від довірених джерел, таких як банки або інші фінансові установи. Вони спонукають користувачів розкрити особисту інформацію або виконати шкідливі дії, такі як завантаження небезпечних файлів або переходи за посиланнями на підроблені вебсайти.

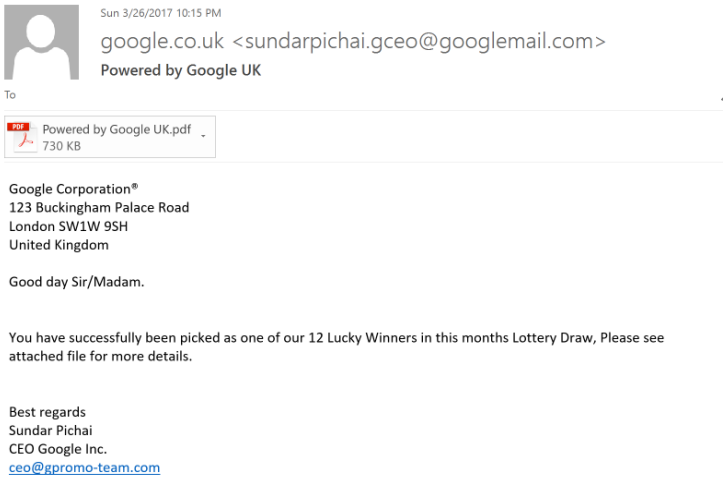

Рис. 1.1. Приклад фішингу на електронну пошту

Спам

Спам – це небажані та часто масово розіслані електронні листи, які можуть включати рекламні повідомлення, шахрайські пропозиції або шкідливе програмне забезпечення. Спам не тільки переповнює поштові скриньки і знижує продуктивність праці, але й може служити каналом для поширення шкідливих програм.

Subject: Waiting to hear from you

Hello

I am Mr Aziz maxwill secretary to my boss Alhiji Nkuruma Gold exporter manager in our branch company in Ghana.I need your assistant of transferring out $10.5 million US dollars and 250 kg of GOLD to a foreign account as our foreign investor or our foreign partner.we are doing it secretly without any member of our company knowing about it

We have a Gold mining company in Ghana owned by Mr GHALI Houcine originally from Switzerland but we normally sell most of our product in Switzerland ,Sudan,Asia during our yearly sales my boss Alhiji Nkuruma did over invoiced to come up with this amount $10.5 million US dollars and the GOLD 250 kg.If you are ready to work it out with us

Your share will be 30%,70%.for my boss and me This money and the GOLD has been deposited with Hassan Ahmad Financial Firm Consultant Limited here in Ghana. everything about this money will be put in your name for easy movement Now if you are interested,

let us discuss in details.

Waiting to hear from you

Mr Aziz maxwill secretary

Рис. 1.2. Приклад спаму на електронну пошту

Шкідливе програмне забезпечення (малваре)

Малваре – це шкідливе програмне забезпечення, яке може бути розповсюджене через вкладення або посилання в електронних листах. Віруси, трояни та інші види малваре можуть викрадати дані, знищувати файли, порушувати роботу системи та створювати бекдори для подальших атак.

Атаки на вразливості програмного забезпечення

Зловмисники можуть використовувати вразливості у поштових клієнтах або серверному програмному забезпеченні для компрометації системи. Такі атаки дозволяють отримати контроль над поштовими серверами або доступ до конфіденційної інформації.

Соціальна інженерія

Соціальна інженерія використовує психологічні маніпуляції для обману користувачів і примусу їх до виконання певних дій або розкриття конфіденційної

інформації. Зловмисники можуть підробляти адреси відправників (спуфінг) або створювати термінові ситуації, що змушують користувачів діяти необачно.

Атаки типу "людина посередині" (MitM)

Перехоплення комунікацій між двома сторонами з метою отримання або зміни переданої інформації. Зловмисники можуть перехоплювати електронні листи, читати або змінювати їх вміст, що може призвести до витоку конфіденційної інформації або інших серйозних наслідків.

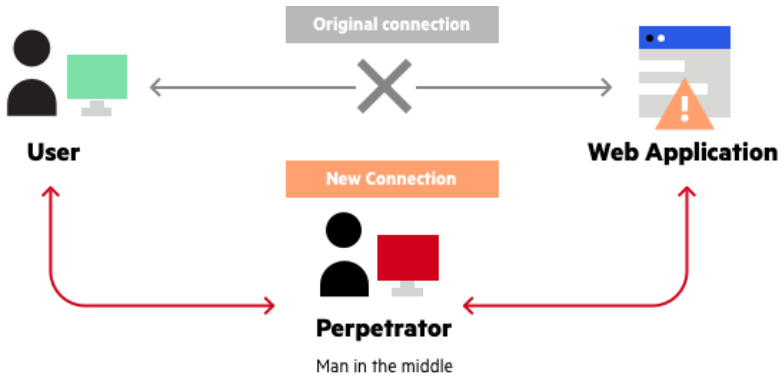

Рис.1.3. Принцип атаки “Людина посередині”

Брутфорс атаки на облікові записи

Використання автоматизованих інструментів для підбору паролів до облікових записів електронної пошти. Успішна атака може надати зловмисникам доступ до облікового запису, що дозволить їм читати, надсилати або видаляти електронні листи.

Атаки типу "DOS" (відмова в обслуговуванні)

Направлення великої кількості запитів на поштові сервери з метою перевантаження системи і зупинки її роботи. Атаки DDoS можуть зробити поштові сервери недоступними для легітимних користувачів, що перериває робочі процеси компанії.

Забезпечення безпеки електронної пошти є критично важливим аспектом функціонування будь-якої сучасної організації. Різноманітні загрози, такі як фішингові атаки, спам, шкідливе програмне забезпечення, атаки на вразливості

програмного забезпечення, соціальна інженерія, атаки типу "людина посередині", шкідливі вкладення, брутфорс атаки та атаки типу "дос", можуть призвести до серйозних наслідків, включаючи витік конфіденційної інформації, фінансові втрати та порушення нормальної роботи компанії.

Ефективна боротьба з цими загрозами вимагає використання передових інструментів та методик. Одним із таких інструментів є SpamAssassin, який надає потужні засоби для виявлення та блокування небажаних листів і захисту від фішингових атак. SpamAssassin дозволяє автоматизувати процеси фільтрації електронної пошти, інтегрується з існуючими системами і забезпечує високий рівень безпеки корпоративних комунікацій.

Розуміння та оцінка ризиків, пов'язаних з електронною поштою, а також впровадження відповідних заходів захисту, є ключовими для підтримки надійності та безпеки інформаційних систем організації. Це не лише допомагає запобігти потенційним атакам, але й сприяє збереженню довіри клієнтів і партнерів, підвищенню продуктивності праці та забезпеченню безперервності бізнес-процесів.

Отже, забезпечення безпеки електронної пошти повинно стати пріоритетним завданням для будь-якої компанії, яка прагне захистити свої інформаційні ресурси та забезпечити стійкість до кіберзагроз. Використання рішень на кшталт SpamAssassin є важливим кроком у цьому напрямку, забезпечуючи ефективний захист від сучасних загроз і підвищуючи загальний рівень кібербезпеки організації.

1.3. Дослідження існуючих методів боротьби з фішинговими атаками

Фішингові атаки є однією з найпоширеніших і найнебезпечніших загроз у сфері кібербезпеки. Вони спрямовані на обман користувачів з метою отримання конфіденційної інформації, такої як логіни, паролі або фінансові дані. Сучасні методи боротьби з фішингом включають комплекс підходів та інструментів, які допомагають виявляти, запобігати та реагувати на ці загрози. Нижче наведені основні методи, які використовуються для захисту від фішингових атак.

Фільтрація електронної пошти

Опис: Використання антиспам фільтрів, таких як SpamAssassin, для автоматичного виявлення та блокування підозрілих електронних листів.

Переваги: Допомагає знизити кількість фішингових листів, що доходять до користувачів.

Недоліки: Може пропустити деякі фішингові листи або помилково заблокувати легітимні повідомлення.

Аутентифікація електронної пошти

Методи: Використання технологій DMARC (Domain-based Message Authentication, Reporting & Conformance), DKIM (DomainKeys Identified Mail) та SPF (Sender Policy Framework).

Переваги: Забезпечує перевірку справжності відправника, що допомагає знизити ризик успішних фішингових атак.

Недоліки: Вимагає налаштування та підтримки з боку адміністраторів.

Шифрування електронної пошти

Опис: Використання протоколів шифрування, таких як SSL/TLS, для забезпечення конфіденційності та цілісності даних під час передачі електронної пошти.

Переваги: Захищає дані від перехоплення та модифікації.

Недоліки: Не запобігає доставці фішингових листів, але ускладнює їх використання.

Освіта та підвищення обізнаності користувачів

Опис: Регулярне проведення тренінгів та інформаційних кампаній для співробітників щодо розпізнавання фішингових листів та безпечного користування електронною поштою. **Переваги:** Зменшує ймовірність успішних фішингових атак за рахунок підвищення обізнаності користувачів. **Недоліки:** Вимагає постійних зусиль і може бути неефективним без регулярного оновлення інформації.

Використання двофакторної аутентифікації (2FA) Опис: Впровадження двофакторної аутентифікації для доступу до електронної пошти та інших корпоративних систем. **Переваги:** Значно ускладнює доступ зловмисників до

облікових записів навіть у разі компрометації пароля. **Недоліки:** Може вимагати додаткових витрат на впровадження та підтримку.

Антивірусне та антифішингове програмне забезпечення Опис: Використання сучасних антивірусних програм та спеціалізованих антифішингових інструментів для виявлення та блокування шкідливих вкладень та посилань. **Переваги:** Допомагає знизити ризик зараження шкідливим програмним забезпеченням та переходу за фішинговими посиланнями. **Недоліки:** Потребує регулярного оновлення баз даних та налаштувань.

Моніторинг та аналіз аномалій Опис: Використання систем моніторингу та аналізу для виявлення підозрілої активності в мережі та поштових скриньках. **Переваги:** Допомагає оперативно виявляти та реагувати на потенційні загрози. **Недоліки:** Вимагає наявності відповідних інструментів та кваліфікованого персоналу для аналізу.

Використання пісочниць (sandboxing) Опис: Запуск підозрілих вкладень та програм у ізольованому середовищі для перевірки їх поведінки перед тим, як вони зможуть вплинути на основну систему. **Переваги:** Ефективний спосіб виявлення нових та невідомих загроз. **Недоліки:** Потребує додаткових ресурсів та часу на аналіз. Ці методи, у поєднанні з використанням передових технологій, таких як SpamAssassin, створюють надійний багаторівневий захист від фішингових атак та інших загроз, пов’язаних з електронною поштою.

Згідно вищезазначених методів можна виділити такі програми(черга програм згідно методів) :

SpamAssassin

Опис роботи:

SpamAssassin є одним із найпопулярніших інструментів для фільтрації спаму. Він використовує багатокомпонентний підхід для аналізу вмісту електронної пошти, включаючи байєсову фільтрацію, чорні списки, білі списки, DNS-базовані списки блокування (DNSBL) та інші евристичні методи. Кожен електронний лист оцінюється за шкалою на основі виявлених ознак спаму, і якщо сума балів

перевищує встановлений поріг, лист позначається як спам і відповідно обробляється.

Переваги: Висока точність виявлення спаму. Гнучкість у налаштуванні фільтрів під конкретні потреби організації. **Недоліки:** Може вимагати додаткового налаштування для досягнення оптимальної ефективності.

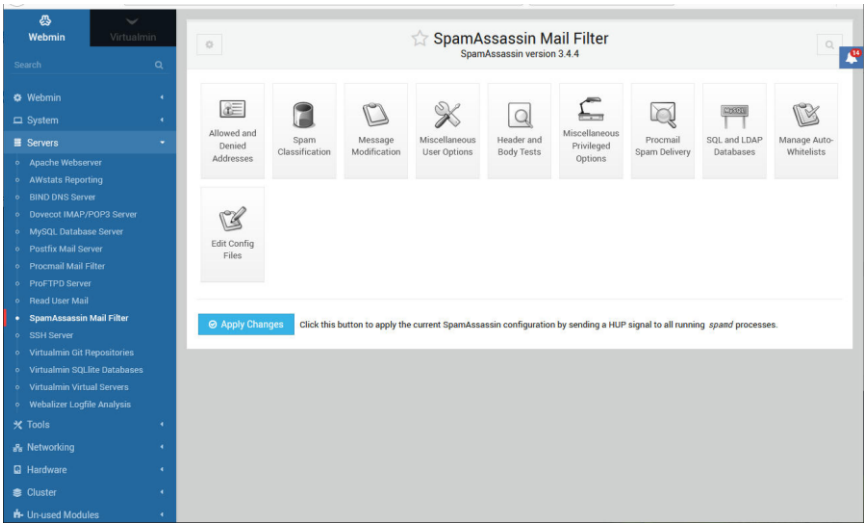

Рис.1.4. Графічний інтерфейс SpamAssassin

DKIM, SPF та DMARC

Опис роботи: SPF (Sender Policy Framework): Дозволяє власникам доменів визначати, які сервери мають право надсилати електронні листи від їхнього імені. Перевірка здійснюється шляхом порівняння IP-адреси відправника з записами в DNS. **DKIM (DomainKeys Identified Mail):** Використовує цифрові підписи для перевірки, що електронний лист не було змінено під час передачі. Підпис додається до заголовків листа і перевіряється приймаючим сервером. **DMARC (Domain-based Message Authentication, Reporting & Conformance):** Працює на базі SPF та DKIM, дозволяючи власникам доменів задавати політику обробки невідповідних листів та отримувати звіти про їх перевірку.

Переваги: Забезпечує перевірку справжності відправника. Підвищує рівень захисту від фішингових атак. **Недоліки:** Вимагає налаштування та постійного моніторингу.

ProtonMail Опис роботи:

ProtonMail пропонує автоматичне шифрування електронної пошти з використанням відкритих криптографічних стандартів. Кожен лист шифрується на пристрої відправника перед відправкою і розшифровується на пристрої отримувача. Це забезпечує високий рівень конфіденційності та цілісності даних.

Переваги: Високий рівень безпеки та конфіденційності. Простота використання. **Недоліки:** Можливі обмеження у функціональності порівняно з традиційними поштовими клієнтами.

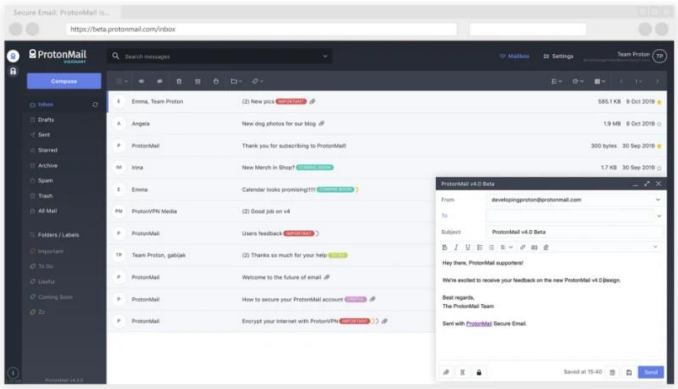

Рис.1.5. Графічний інтерфейс ProtonMail

KnowBe4

Опис роботи:

KnowBe4 пропонує комплексну платформу для навчання співробітників методам захисту від фішингових атак. Включає симуляції фішингових атак, інтерактивні навчальні модулі та оцінку рівня обізнаності. Платформа також надає можливість створення та проведення тестів для перевірки знань користувачів.

Переваги: Підвищує обізнаність користувачів про кіберзагрози. Знижує ризик успішних фішингових атак. **Недоліки:** Вимагає постійних інвестицій у навчання та оновлення програм.

Google Authenticator Опис роботи: Google Authenticator генерує одноразові коди для двофакторної аутентифікації (2FA). Ці коди використовуються як додатковий рівень захисту під час входу в облікові записи. Кожен код дійсний лише протягом короткого проміжку часу, що ускладнює доступ зловмисникам навіть у разі компрометації пароля.

Переваги: Підвищує безпеку облікових записів. Ускладнює несанкціонований доступ. **Недоліки:** Вимагає доступу до мобільного пристрою.

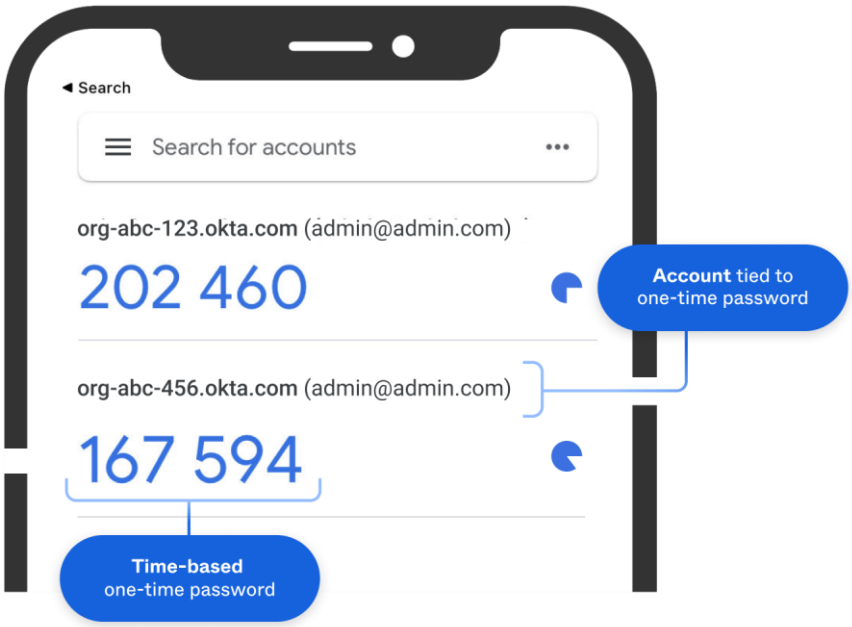

Рис.1.6. Графічний інтерфейс Google Authenticator

Norton 360 Опис роботи:

Norton 360 пропонує всебічний захист від вірусів, шкідливого ПЗ, фішингу та інших загроз. Пакет включає в себе фільтрацію електронної пошти, брандмауер,

захист від фішингових атак та інші засоби захисту. Програма також забезпечує регулярні оновлення баз даних для виявлення нових загроз.

Переваги: Комплексний захист від різних видів загроз. Регулярні оновлення баз даних. **Недоліки:** Може сповільнювати роботу системи. Потребує регулярного оновлення.

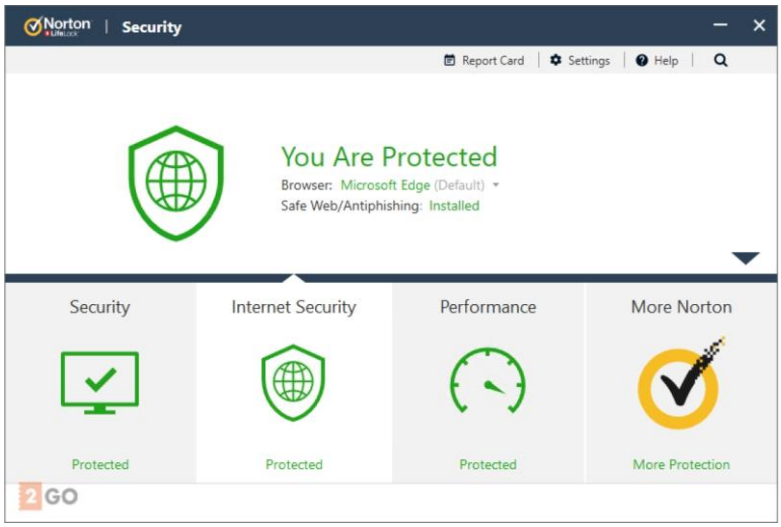

Рис.1.7. Графічний інтерфейс Norton 360

Splunk

Опис роботи:

Splunk надає інструменти для моніторингу, аналізу та візуалізації даних з різних джерел, включаючи електронну пошту. Він допомагає виявляти підозрілу активність, аналізувати її та реагувати на неї. Splunk може інтегруватися з іншими системами для забезпечення повного контролю над інформаційною безпекою.

Переваги: Висока ефективність виявлення аномалій. Гнучкість у налаштуванні та інтеграції.

Недоліки: Висока вартість. Потребує кваліфікованого персоналу для аналізу даних.

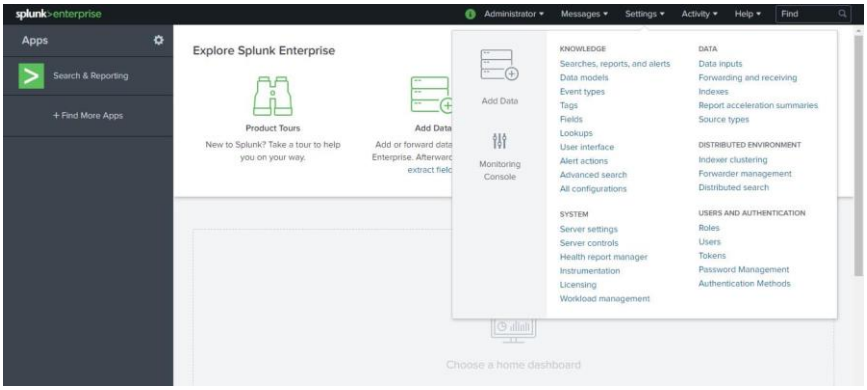

Рис.1.8. Графічний інтерфейс Splunk

FireEye

Опис роботи:

FireEye пропонує рішення для ізоляції та аналізу підозрілих файлів у безпечному середовищі (sandbox). Це дозволяє визначити їх шкідливий потенціал до того, як вони можуть вплинути на систему. FireEye аналізує поведінку файлів і надає детальні звіти про можливі загрози.

Переваги: Ефективний захист від нових та невідомих загроз. Висока точність аналізу. **Недоліки:**

Висока вартість. Потребує додаткових ресурсів.

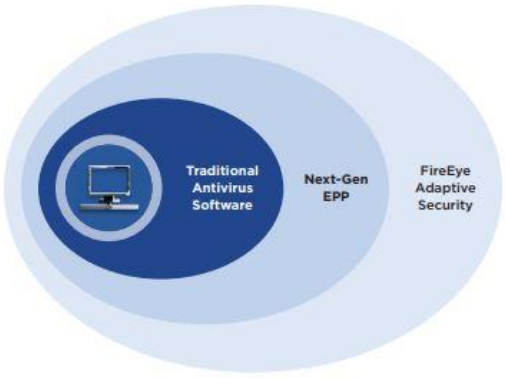

Рис.1.9. Місце FireEye в системі захисту персонального комп’ютера

Ці програми забезпечують багаторівневий захист від фішингових атак та інших загроз, пов'язаних з електронною поштою, і допомагають підтримувати високий рівень кібербезпеки в організаціях.

2. АНАЛІЗ МЕТОДІВ ТА ІНСТРУМЕНТІВ ПРОТИДІЇ ФІШИНГУ В ЕЛЕКТРОННИХ ПОШТАХ НА БАЗІ SPAMASSASIN

2.1. Принципи роботи SpamAssassin

SpamAssassin є потужним інструментом для фільтрації небажаних електронних листів (спаму). Він використовує різноманітні методи аналізу та виявлення спаму, об'єднуючи їх у багаторівневий підхід для досягнення високої точності.

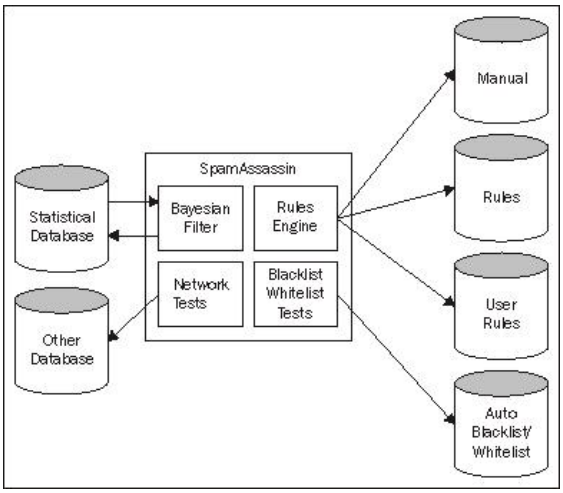

Рис.2.1. Структура SpamAssassin

Ось основні принципи роботи SpamAssassin:

Байєсова фільтрація

SpamAssassin використовує байєсовий алгоритм для аналізу вмісту електронних листів. Байєсова фільтрація заснована на ймовірнісному підході, який визначає, чи є лист спамом, на основі частоти появи певних слів або фраз у спам-листах і легітимних листах. Принцип роботи: Система навчається на базі прикладів спаму[1] та легітимних листів, а потім використовує цю інформацію для оцінки нових листів.

Додано примітку [1]: https://cwiki.apache.org/confluence/display/SPAMASSASSIN/BayesInSpamAssassin

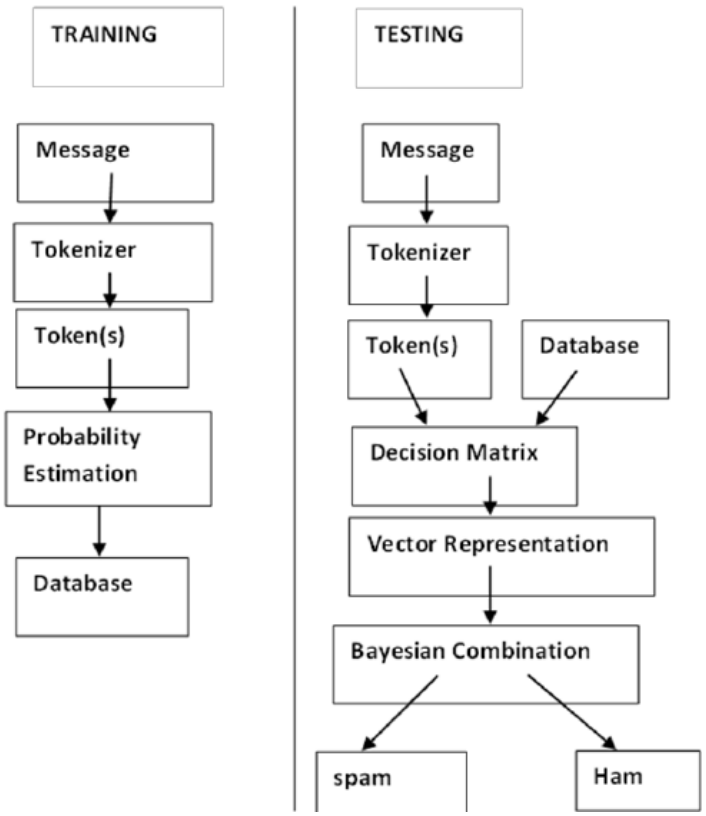

Рис.2.2. Процеси навчання та тестування байєсового фільтра.

Чорні та білі списки (Blacklists and Whitelists)

Чорні списки містять IP-адреси, домени або адреси електронної пошти, відомі як джерела спаму. Білі списки містять довірені адреси або домени, які ніколи не повинні бути позначені як спам. Принцип роботи: При отриманні нового листа SpamAssassin перевіряє його відправника за чорними та білими списками, щоб швидко визначити, чи є лист потенційно небажаним.

DNS-базовані списки блокування (DNSBL)

DNSBL – це онлайн-сервіси, які надають списки IP-адрес, пов'язаних зі спамом. SpamAssassin використовує ці списки для додаткової перевірки відправників. Принцип роботи: При отриманні нового листа SpamAssassin

перевіряє IP-адресу відправника через DNSBL-сервіси. Якщо адреса знайдена в списку, лист отримує додаткові бали спаму.[2]

Додано примітку [2]: https://cwiki.apache.org/confluence/display/SPAMASSASSIN/DnsBlocklists

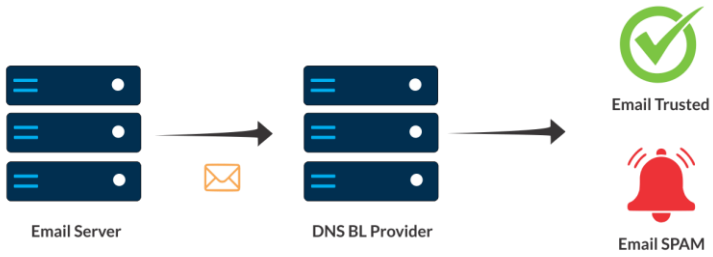

Рис.2.3. Схема використання DNSBL сервісу для перевірки електронних листів на предмет спаму чи фішингу.

Евристичний аналіз Евристичний аналіз включає використання правил і шаблонів для виявлення ознак спаму у вмісті листів. Ці правила можуть перевіряти наявність підозрілих посилань, певних слів, фраз або форматування.

Принцип роботи: Кожне правило має певну вагу, і при виявленні ознаки спаму до листа додаються бали[3]. Якщо сума балів перевищує встановлений поріг, лист позначається як спам.

Додано примітку [3]: https://cwiki.apache.org/confluence/display/SPAMASSASSIN/WritingRules

Аналіз заголовків

Аналіз заголовків електронних листів включає перевірку полів заголовка на предмет підозрілих або неправомірних значень.

Принцип роботи: SpamAssassin перевіряє, чи відповідають заголовки листа стандартам і чи містять вони ознаки підробки або спамової активності.

Перевірка автентичності відправника

SpamAssassin може використовувати технології SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) та DMARC (Domain-based Message Authentication, Reporting & Conformance) для перевірки автентичності відправника.

Принцип роботи: Ці технології допомагають підтвердити, що лист надсилається з довіреного джерела і не був змінений під час передачі.

Підрахунок балів (Scoring System)

SpamAssassin використовує систему підрахунку балів для оцінки кожного листа. Різні методи аналізу додають або віднімають бали залежно від виявлених ознак спаму.

Принцип роботи: Якщо сумарний бал перевищує заданий поріг, лист позначається як спам. Адміністратори можуть налаштовувати поріг та вагу окремих правил для підвищення точності фільтрації.

Навчання та адаптація

SpamAssassin може бути налаштований для постійного навчання на нових даних, що дозволяє йому адаптуватися до нових загроз і тенденцій у спамі.

Принцип роботи: Адміністратори можуть вручну або автоматично оновлювати бази даних фільтрів, щоб покращити ефективність виявлення спаму.

У підсумку, SpamAssassin є ефективним рішенням для забезпечення безпеки електронної пошти, яке може значно знизити ризики, пов'язані з небажаними листами та кіберзагрозами, і забезпечити надійну та безперебійну роботу корпоративних інформаційних систем. Важливо зазначити, що SpamAssassin не тільки фільтрує спам, але й інтегрується з іншими інструментами та технологіями кібербезпеки, що дозволяє створити комплексну систему захисту. Завдяки своїй модульній архітектурі та широким можливостям налаштування, SpamAssassin може бути адаптований до специфічних потреб кожної організації, забезпечуючи оптимальний баланс між продуктивністю та безпекою. Крім того, постійне навчання та адаптація SpamAssassin дозволяють йому залишатися актуальним у боротьбі з новими та еволюціонуючими загрозами. Це особливо важливо в умовах постійно змінюваного ландшафту кіберзагроз, де швидкість реакції на нові атаки може бути вирішальним фактором. Використання SpamAssassin у поєднанні з іншими методами захисту, такими як багатофакторна аутентифікація та регулярне навчання персоналу, може суттєво підвищити загальний рівень кібербезпеки організації.

2.2. Порівняння SpamAssasin з іншими антиспам та антивірусними інструментами

Таблиця 2.1

Таблиця порівняння основних деталей SpamAssasin з іншими подібними інструментами

Характеристика	SpamAssassin	Mimecast	Proofpoint	Norton 360	Barracuda Email Security
Методи фільтрації	Байєсова фільтрація, чорні та білі списки, DNS-базовані списки блокування, евристичний аналіз, аналіз заголовків, SPF, DKIM, DMARC, система підрахунку балів, навчання та адаптація	Аналіз вмісту, машинне навчання, евристичний аналіз, чорні та білі списки, захист від фішингових атак, шкідливих URL та вкладень	Машинне навчання, аналіз вмісту, евристичний аналіз, захист від фішингу, шкідливих URL та вкладень, чорні та білі списки	Байєсова фільтрація, аналіз вмісту, захист від фішингу, шкідливих URL та вкладень	Аналіз вмісту, чорні та білі списки, евристичний аналіз, захист від фішингу, шкідливих URL та вкладень
Переваги	Висока точність виявлення спаму, гнучкість налаштувань, модульна архітектура, інтеграція з іншими інструментам	Інтегровані рішення для захисту електронної пошти, архівування та безперервності бізнесу, висока	Високий рівень захисту, детальна аналітика, інтеграція з іншими інструментами кібербезпеки, захист	Комплексний захист від різних видів загроз, регулярні оновлення баз даних, проста інтеграція	Простота використання, інтеграція з іншими рішеннями Barracuda, висока ефективність фільтрації

	и кібербезпеки	точність, автоматичні оновлення	від розширених загроз		
Недоліки	Вимагає технічних знань для налаштування, потребує постійного моніторингу та оновлення правил	Вартість, залежність від хмарного сервісу	Висока вартість, потребує налаштування та підтримки	Може сповільнювати роботу системи, потребує регулярного оновлення	Вартість, складність налаштування для малих компаній
Ціна	Безкоштовний (Open Source)	Платний (вартість залежить від обсягу послуг)	Платний (вартість залежить від обсягу послуг)	Платний (вартість залежить від обсягу послуг)	Платний (вартість залежить від обсягу послуг)
Інтеграція	Підтримка багатьох поштових серверів та клієнтів	Інтеграція з популярними поштовими серверами та хмарними сервісами	Інтеграція з популярними поштовими серверами та хмарними сервісами	Інтеграція з основними поштовими клієнтами та сервісами	Інтеграція з рішеннями Barracuda та основними поштовими серверами

Таблиця порівняння антиспам та антивірусних інструментів, таких як SpamAssassin, Mimecast, Proofpoint, Norton 360 та Barracuda Email Security, виявляє ключові відмінності у підходах до забезпечення безпеки електронної пошти. SpamAssassin, як безкоштовне рішення з відкритим вихідним кодом, виділяється своєю гнучкістю та модульною архітектурою, яка дозволяє інтегрувати його з багатьма поштовими серверами та клієнтами. Його методи фільтрації включають байєсову фільтрацію, чорні та білі списки, DNS-базовані списки блокування, евристичний аналіз, аналіз заголовків та перевірку автентичності відправника за допомогою SPF, DKIM та DMARC. Це забезпечує високу точність виявлення

спаму, проте вимагає технічних знань для налаштування та постійного моніторингу.

Mimecast та Proofpoint пропонують інтегровані хмарні рішення з високим рівнем захисту, які використовують машинне навчання, аналіз вмісту та евристичний аналіз для виявлення фішингових атак, шкідливих URL та вкладень. Ці інструменти забезпечують високу точність та автоматичні оновлення, але їх основними недоліками є висока вартість та залежність від хмарних сервісів.

Norton 360 пропонує комплексний захист від різних видів загроз, включаючи віруси та фішингові атаки, з регулярними оновленнями баз даних, але може сповільнювати роботу системи і також вимагає регулярного оновлення.

Barracuda Email Security, з іншого боку, забезпечує високу ефективність фільтрації з простотою використання і можливістю інтеграції з іншими рішеннями Barracuda. Водночас, його вартість та складність налаштування можуть бути бар'єром для менших компаній. Усі розглянуті інструменти мають свої унікальні переваги та недоліки, і вибір конкретного рішення залежить від специфічних потреб та ресурсів організації.

Таблиця 2.2.

Таблиця порівняння технічних характеристик антиспам та антивірусних інструментів

Характеристика	**SpamAssassin**	**Mimecast**	**Proofpoint**	**Norton 360**	**Barracuda Email Security**
Тип рішення	Open Source	Хмарне рішення	Хмарне рішення	Локальне/Хмарне рішення	Локальне/Хмарне рішення
Точність виявлення	Висока	Висока	Висока	Висока	Висока
Гнучкість налаштувань	Висока	Середня	Середня	Низька	Середня
Автоматичні	Ні	Так	Так	Так	Так

оновлення					
Потреба у технічних знаннях	Висока	Середня	Середня	Низька	Середня
Основні функції	Фільтрація спаму, аналіз заголовків, перевірка автентичності відправника, навчання та адаптація	Фільтрація спаму, захист від фішингу, шкідливих URL та вкладень, архівування	Фільтрація спаму, захист від фішингу, шкідливих URL та вкладень, детальна аналітика	Фільтрація спаму, захист від фішингу, шкідливих URL та вкладень, антивірусний захист	Фільтрація спаму, захист від фішингу, шкідливих URL та вкладень, інтеграція з іншими рішеннями Barracuda
Підтримка	Спільнота	Професійна	Професійна	Професійна	Професійна

Таблиця порівняння технічних характеристик антиспам та антивірусних інструментів показує суттєві відмінності між ними, підкреслюючи сильні та слабкі сторони кожного рішення. SpamAssassin, як безкоштовне рішення з відкритим вихідним кодом, виділяється своєю високою гнучкістю налаштувань та підтримкою багатьох поштових серверів і клієнтів. Воно забезпечує високу точність виявлення спаму завдяки використанню байєсової фільтрації, чорних та білих списків, DNS-базованих списків блокування, евристичного аналізу, аналізу заголовків та перевірки автентичності відправника. Проте, SpamAssassin вимагає значних технічних знань для налаштування та постійного моніторингу, що може бути викликом для деяких організацій.

Mimecast та Proofpoint пропонують хмарні рішення з високою точністю виявлення спаму, захистом від фішингових атак, шкідливих URL та вкладень. Ці інструменти забезпечують автоматичні оновлення та інтеграцію з популярними поштовими серверами та хмарними сервісами, що робить їх зручними для

організацій, які прагнуть мінімізувати витрати на технічне обслуговування. Однак, висока вартість та залежність від хмарних сервісів можуть бути обмежуючими факторами для деяких компаній.

Norton 360 пропонує комплексний захист від різних видів загроз, включаючи спам, фішингові атаки та віруси. Він забезпечує регулярні оновлення баз даних, але його інтеграція з основними поштовими клієнтами та сервісами менш гнучка порівняно з іншими рішеннями. Крім того, Norton 360 може сповільнювати роботу системи, що є важливим аспектом для великих організацій з високими вимогами до продуктивності.

Barracuda Email Security виділяється своєю простотою використання та інтеграцією з іншими рішеннями Barracuda, забезпечуючи високу ефективність фільтрації спаму та захисту від фішингових атак. Це рішення підходить для організацій, які вже використовують продукти Barracuda, але його вартість і складність налаштування можуть бути перешкодою для менших компаній.

Загалом, вибір оптимального антиспам та антивірусного рішення залежить від специфічних потреб і ресурсів організації. Кожне з розглянутих рішень має свої унікальні переваги та обмеження, які слід враховувати при розробці стратегії кібербезпеки.

Порівняння технічних характеристик та функціональних можливостей антиспам і антивірусних інструментів показує суттєві відмінності між ними, що дозволяє зробити висновки про їх відповідність різним потребам і ресурсам організацій.

SpamAssassin виділяється серед інших інструментів своєю безкоштовністю, відкритим вихідним кодом та високою гнучкістю налаштувань. Його сильні сторони включають використання багатокомпонентного підходу до фільтрації спаму, який включає байєсову фільтрацію, чорні та білі списки, DNS-базовані списки блокування, евристичний аналіз, аналіз заголовків та перевірку автентичності відправника за допомогою SPF, DKIM та DMARC. Це дозволяє SpamAssassin забезпечувати високу точність виявлення спаму, що є значною перевагою порівняно з іншими інструментами. Можливість навчання та адаптації

також підвищує ефективність його роботи у боротьбі з новими та еволюціонуючими загрозами.

Проте, SpamAssassin має і певні слабкі сторони. Він вимагає значних технічних знань для налаштування та постійного моніторингу, що може бути викликом для деяких організацій. Крім того, відсутність автоматичних оновлень означає, що адміністратори повинні самостійно підтримувати актуальність правил і фільтрів, що може вимагати додаткових ресурсів.

Інші інструменти, такі як Mimecast, Proofpoint, Norton 360 та Barracuda Email Security, мають свої унікальні переваги. Mimecast і Proofpoint пропонують інтегровані хмарні рішення з високою точністю виявлення спаму, автоматичними оновленнями та зручною інтеграцією з популярними поштовими серверами та хмарними сервісами. Однак, вони можуть бути дорогими і залежними від хмарних сервісів. Norton 360 забезпечує комплексний захист від різних видів загроз і пропонує регулярні оновлення баз даних, але може сповільнювати роботу системи. Barracuda Email Security виділяється своєю простотою використання та ефективністю, особливо для організацій, які вже використовують продукти Barracuda, хоча його вартість і складність налаштування можуть бути перешкодою для менших компаній.

Загалом, вибір оптимального антиспам та антивірусного рішення залежить від специфічних потреб і ресурсів організації. SpamAssassin може бути ідеальним для організацій, які мають технічні знання та ресурси для його налаштування та підтримки, і потребують високої гнучкості та адаптивності. Інші інструменти можуть бути більш підходящими для організацій, які шукають інтегровані та автоматизовані рішення з мінімальними вимогами до технічного обслуговування. Ретельний аналіз потреб та можливостей організації є ключовим для вибору найбільш підходящого рішення для забезпечення надійного захисту електронної пошти від спаму та інших кіберзагроз.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИКОРИСТАННЯ МЕТОДІВ ТА ІНСТРУМЕНТІВ ПРОТИДІЇ ФІШИНГУ В ЕЛЕКТРОННИХ ПОШТАХ

3.1. Впровадження Spam Assasin в корпоративні системи електронної пошти

В сучасному цифровому середовищі, де велика кількість бізнесових процесів залежать від електронної пошти, захист від спаму та фішингових атак стає критично важливим для кожної організації. Спам не лише знижує продуктивність праці співробітників, але й може стати каналом для поширення шкідливого програмного забезпечення та фішингових атак, які загрожують конфіденційності корпоративних даних. Впровадження ефективного рішення для фільтрації спаму, такого як SpamAssassin, допомагає захистити корпоративні системи електронної пошти від цих загроз. У даному розділі буде розглянуто процес впровадження SpamAssassin у корпоративні системи електронної пошти, що включає підготовчий етап, налаштування серверного середовища, встановлення та конфігурацію інструменту, а також інтеграцію з існуючими поштовими серверами.

Принцип впровадження

Підготовчий етап

Перш ніж впроваджувати SpamAssassin, необхідно провести ретельний аналіз існуючих систем електронної пошти та визначити основні загрози, з якими стикається організація. Важливо зрозуміти обсяг та характер спаму, який отримує компанія, а також врахувати специфічні потреби користувачів. Наприклад, деякі підрозділи можуть мати особливі вимоги до фільтрації електронної пошти, які потрібно врахувати при налаштуванні SpamAssassin. Важливо також скласти план впровадження, який включатиме етапи тестування та оцінки ефективності.

Вибір та налаштування серверного середовища

SpamAssassin може бути встановлений на різні операційні системи, такі як Linux, Unix або Windows. Першим кроком є вибір відповідного серверного

середовища та його налаштування. Для кращої продуктивності та безпеки рекомендується використовувати сучасні версії операційних систем і забезпечити їх своєчасне оновлення.

Встановлення SpamAssassin

Встановлення SpamAssassin може здійснюватися за допомогою пакетних менеджерів (наприклад, apt для Debian/Ubuntu або yum для CentOS/RHEL) або шляхом завантаження вихідного коду і його компіляції. Ось базові кроки для встановлення на системах Linux(будемо розглядати його інсталяцію саме на цих системах):

Виконання команди для встановлення SpamAssassin:

sudo apt-get install spamassassin -y

або

sudo yum install spamassassin -y

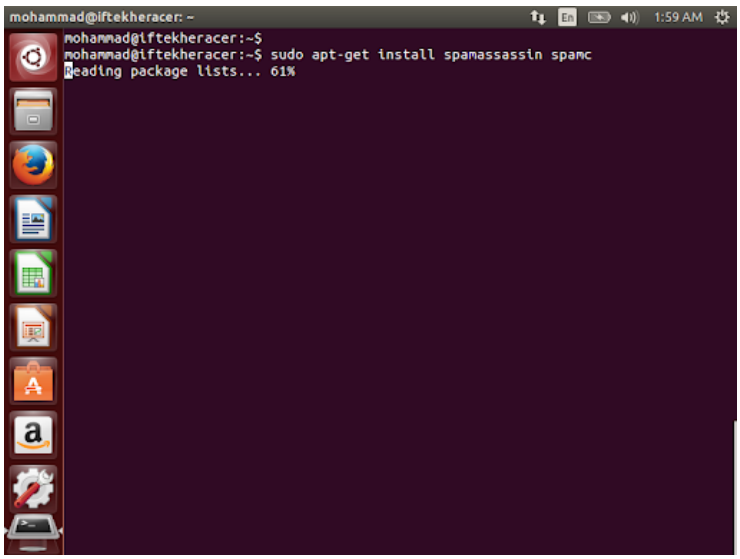

Рис.3.1. Процес інсталяції SpamAssassin

Налаштування SpamAssassin

Після встановлення SpamAssassin необхідно провести його налаштування відповідно до вимог організації. Це включає конфігурацію основних параметрів,

налаштування правил фільтрації, визначення порогів для підрахунку балів спаму, а також налаштування чорних та білих списків. Основні конфігураційні файли знаходяться в директорії `/etc/spamassassin/`.

Відредагуйте файл `local.cf` для налаштування основних параметрів:

sudo nano /etc/spamassassin/local.cf

Додайте або змініть наступні параметри:

required_score 5.0
rewrite_header Subject SPAM
report_safe 0
whitelist_from your_trusted@domain.com
blacklist_from spammer@domain.com

Інтеграція з поштовим сервером

SpamAssassin може бути інтегрований з різними поштовими серверами, такими як Postfix, Sendmail або Exim. Для інтеграції з Postfix, необхідно встановити та налаштувати `Amavisd-new` або `SpamAss-Milter`. Приклад інтеграції з Postfix:

Встановлення `Amavisd-new`:

sudo apt-get install amavisd-new -y

Налаштування Postfix для використання `Amavisd-new`:

sudo nano /etc/postfix/main.cf

Додайте або змініть наступні параметри:

content_filter = smtp-amavis:[127.0.0.1]:10024

Перезапуск Postfix:

sudo systemctl restart postfix

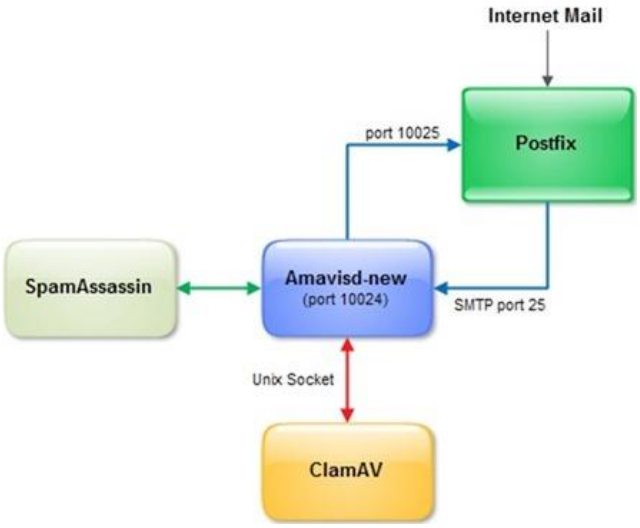

Рис 3.2. Інтеграція поштових сервісів для перевірки вхідної пошти на предмет спаму,фішингу чи вірусів.

Тестування та моніторинг

Після налаштування та інтеграції SpamAssassin необхідно провести тестування його роботи. Надішліть кілька тестових листів, включаючи як звичайні, так і відомі спам-повідомлення, щоб перевірити ефективність фільтрації. Використовуйте лог-файли та інструменти моніторингу для оцінки роботи SpamAssassin та внесення необхідних коригувань.

Постійне обслуговування та оновлення

Для підтримання високої ефективності фільтрації спаму необхідно регулярно оновлювати правила та бази даних SpamAssassin. Адміністратори повинні періодично перевіряти налаштування, аналізувати лог-файли та оновлювати конфігурації у відповідь на нові загрози.

Впровадження SpamAssassin у корпоративні системи електронної пошти дозволяє значно підвищити рівень захисту від спаму та фішингових атак,

забезпечуючи безпеку та продуктивність організації. Використовуючи гнучкі можливості налаштування та інтеграції, організації можуть адаптувати SpamAssassin до своїх специфічних потреб, що сприяє ефективному захисту від постійно змінюваних загроз у сфері кібербезпеки.

Для більш ефективного захисту від загроз, можна виділити такі додаткові аспекти впровадження:

Підвищення продуктивності та масштабування

Для великих організацій з великим обсягом електронної пошти може бути необхідно налаштувати масштабовану інфраструктуру для підтримки SpamAssassin. Це може включати використання декількох серверів або кластерів для розподілу навантаження та забезпечення високої продуктивності. Використання балансувальників навантаження дозволить рівномірно розподіляти вхідні повідомлення між серверами, що забезпечить безперебійну роботу системи та зменшить час обробки повідомлень.

Інтеграція з системами звітності та аналітики

SpamAssassin може бути інтегрований з системами звітності та аналітики для покращення моніторингу та аналізу ефективності фільтрації спаму. Це дозволяє адміністраторам отримувати детальні звіти про обсяг і типи заблокованих повідомлень, аналізувати тенденції спаму та визначати нові загрози. Такі інтеграції можуть включати використання інструментів, таких як Splunk або ELK Stack, для збору та аналізу логів SpamAssassin.

Підтримка різних мов та кодувань

SpamAssassin підтримує фільтрацію спаму на різних мовах та з різними кодуваннями, що є важливим для міжнародних організацій. Налаштування правил для різних мов дозволяє підвищити точність виявлення спаму в багатомовному середовищі. Це включає налаштування специфічних байєсових фільтрів та правил для кожної мови, що використовується в організації.

Використання додаткових плагінів та модулів

SpamAssassin підтримує використання різних плагінів та модулів, які розширюють його функціональність. Наприклад, можна використовувати плагіни

для інтеграції з антивірусними програмами, такими як ClamAV, для додаткової перевірки вкладень на наявність шкідливого програмного забезпечення. Інші плагіни можуть включати додаткові методи аналізу вмісту, такі як перевірка URL-адрес на наявність фішингових сайтів.

Впровадження політик збереження та видалення спаму

Організація повинна розробити політики збереження та видалення спаму, які відповідатимуть її потребам та вимогам безпеки. Це включає налаштування термінів зберігання заблокованих повідомлень, автоматичне видалення старих спам-листів та регулярний огляд і очищення спам-папок. Впровадження таких політик допомагає забезпечити відповідність нормативним вимогам і знижує ризик випадкового видалення важливих повідомлень.

Взаємодія з іншими системами кібербезпеки

SpamAssassin може бути частиною комплексної системи кібербезпеки, що включає інші інструменти та рішення. Взаємодія з системами захисту кінцевих точок, міжмережевими екранами та системами виявлення вторгнень (IDS/IPS) дозволяє створити багаторівневий захист від кіберзагроз. Інтеграція з цими системами забезпечує спільне використання даних про загрози та підвищує загальний рівень безпеки організації.

Постійне вдосконалення та тестування

Організація повинна постійно вдосконалювати та тестувати свою систему захисту від спаму. Це включає регулярне тестування ефективності SpamAssassin, оцінку нових методів фільтрації та адаптацію до змін у характері спам-атак. Впровадження циклу безперервного вдосконалення допомагає підтримувати високий рівень захисту та швидко реагувати на нові загрози.

Ці додаткові аспекти дозволяють забезпечити більш ефективне впровадження SpamAssassin в корпоративні системи електронної пошти, підвищуючи рівень захисту від спаму та інших кіберзагроз.

3.2. Налаштування та підвищення ефективності Spam Assasin для виявлення фішингових загроз

Виявлення та блокування фішингових загроз є одним із найважливіших аспектів забезпечення безпеки корпоративної електронної пошти. SpamAssassin, завдяки своїй гнучкій архітектурі та можливостям налаштування, може бути ефективним інструментом для виявлення фішингових листів. У цьому розділі розглянемо основні кроки для налаштування та підвищення ефективності SpamAssassin у боротьбі з фішинговими загрозами.

Налаштування основних правил та конфігурацій

Для початку необхідно налаштувати базові параметри SpamAssassin, щоб забезпечити ефективне виявлення фішингових повідомлень. Це включає редагування конфігураційних файлів, таких як `local.cf`, де ви можете налаштувати порогові значення для виявлення спаму, визначити правила для чорних і білих списків, та налаштувати загальні параметри.

Відредагуйте файл `local.cf`:

```
sudo nano /etc/spamassassin/local.cf
```

Додайте або змініть наступні параметри для посилення виявлення фішингових листів:

```
required_score 4.0
rewrite_header Subject [SPAM]
report_safe 0
trusted_networks 192.168.0.0/24
whitelist_from your_trusted@domain.com
blacklist_from spammer@domain.com
```

Використання правил для виявлення фішингових загроз

SpamAssassin підтримує використання додаткових правил, які допомагають виявляти специфічні ознаки фішингових атак. Ви можете завантажити та

налаштувати додаткові правила, розроблені спільнотою, такі як правила SARE (SpamAssassin Rules Emporium), які спеціально створені для боротьби з фішингом.

Завантажте додаткові правила:

```
wget -P /etc/spamassassin/ https://www.rulesemporium.com/rules/70_sare_phish.cf
```

Додайте нові правила до конфігурації SpamAssassin:

```
sudo nano /etc/spamassassin/local.cf
```

Додайте рядок:

```
include /etc/spamassassin/70_sare_phish.cf
```

Налаштування SPF, DKIM та DMARC

Налаштування та перевірка автентичності відправників за допомогою SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) та DMARC (Domain-based Message Authentication, Reporting & Conformance) допоможуть запобігти підробці електронних адрес та знизити кількість фішингових листів.

Переконайтеся, що SPF, DKIM та DMARC налаштовані правильно на вашому поштовому сервері.

Додайте відповідні налаштування до SpamAssassin:

```
sudo nano /etc/spamassassin/local.cf
```

Додайте або змініть наступні параметри:

```
loadplugin Mail::SpamAssassin::Plugin::SPF
loadplugin Mail::SpamAssassin::Plugin::DKIM
loadplugin Mail::SpamAssassin::Plugin::DMARC
```

Використання плагінів та додаткових модулів

SpamAssassin підтримує різні плагіни та модулі, які можуть значно підвищити його ефективність у боротьбі з фішингом. Наприклад, плагін Razor

дозволяє обмінюватися інформацією про спам між користувачами, що допомагає швидше виявляти нові загрози.

Встановлення та налаштування плагіну Razor:

```
sudo apt-get install razor
sudo nano /etc/spamassassin/local.cf
```

Додайте або змініть наступні параметри:

```
use_razor2 1
razor_config /etc/razor/razor-agent.conf
```

Навчання та адаптація (Bayesian Learning)

SpamAssassin використовує байєсову фільтрацію для підвищення точності виявлення спаму, включаючи фішингові листи. Навчання байєсових фільтрів на прикладах легітимних та фішингових листів дозволяє системі адаптуватися до нових загроз.

Навчання байєсових фільтрів:

```
sa-learn --spam /path/to/phishing_emails/
sa-learn --ham /path/to/legitimate_emails/
```

Моніторинг та оцінка ефективності

Постійний моніторинг ефективності SpamAssassin допомагає виявляти слабкі місця та вносити необхідні корективи. Аналіз лог-файлів та звітів про фільтрацію дозволяє оцінити, наскільки добре система справляється з виявленням фішингових загроз.

Аналіз лог-файлів:

```
sudo cat /var/log/mail.log | grep spamassassin
```

Регулярні оновлення та підтримка

Для підтримання високої ефективності необхідно регулярно оновлювати правила та бази даних SpamAssassin. Адміністратори повинні стежити за новими версіями та оновленнями, щоб забезпечити захист від новітніх загроз.

Оновлення SpamAssassin:

```
sudo apt-get update
sudo apt-get upgrade spamassassin
```

Впровадження цих кроків допоможе налаштувати та підвищити ефективність SpamAssassin для виявлення фішингових загроз, забезпечуючи надійний захист корпоративної електронної пошти.

Спостереження та звітування про безпеку електронної пошти з використанням SpamAssasin

Одним із ключових аспектів забезпечення безпеки електронної пошти є постійний моніторинг і звітування про ефективність антиспам-фільтрів. SpamAssassin пропонує інструменти для детального спостереження за роботою системи та створення звітів, що допомагає адміністраторам оцінювати рівень захисту та оперативно реагувати на нові загрози. У цьому розділі розглянемо методи спостереження та звітування про безпеку електронної пошти з використанням SpamAssassin.

Моніторинг логів

SpamAssassin веде детальні журнали (логи) про всі оброблені електронні листи, що включають інформацію про виявлені спам-повідомлення та дії, вжиті для їх блокування. Аналіз цих логів дозволяє отримати розуміння про ефективність системи та виявити потенційні проблеми.

Перегляд логів SpamAssassin:

```
sudo tail -f /var/log/mail.log | grep spamassassin
```

Аналіз логів для оцінки виявлення спаму та фішингових загроз:

```
grep "spam" /var/log/mail.log
```

Використання систем моніторингу

Інтеграція SpamAssassin з системами моніторингу, такими як Nagios або Zabbix, дозволяє автоматизувати спостереження за роботою антиспам-фільтрів та оперативно реагувати на виявлені проблеми.

Налаштування моніторингу за допомогою Nagios:

Встановіть Nagios:

```
sudo apt-get install nagios-nrpe-server nagios-plugins
```

Налаштуйте перевірки SpamAssassin у файлі конфігурації Nagios:

```
sudo nano /etc/nagios/nrpe.cfg
```

Додайте наступний рядок для моніторингу SpamAssassin:

```
command[check_spamassassin]=/usr/lib/nagios/plugins/check_procs -c 1: -C spamd
```

Перезапустіть службу Nagios:

```
sudo systemctl restart nagios-nrpe-server
```

Створення звітів про фільтрацію спаму

Регулярне створення звітів про роботу SpamAssassin дозволяє адміністраторам оцінювати ефективність фільтрації та виявляти тенденції в спам-атак. Звіти можуть включати інформацію про кількість заблокованих повідомлень, типи виявлених загроз та рівень точності фільтрації.

Використання утиліт для створення звітів, таких як pflogsumm:

Встановіть pflogsumm:

```
sudo apt-get install pflogsumm
```

Створення звіту про роботу SpamAssassin:

```
sudo pflogsumm /var/log/mail.log > spamassassin_report.txt
```

Автоматичне сповіщення про інциденти

Для забезпечення оперативного реагування на загрози, SpamAssassin можна налаштувати на автоматичне сповіщення адміністраторів про виявлені інциденти. Це може включати надсилання повідомлень електронною поштою або інтеграцію з системами керування інцидентами.

Приклад налаштування автоматичних сповіщень через Postfix:

Налаштуйте Postfix для пересилання сповіщень на конкретну адресу

```
sudo nano /etc/postfix/aliases
```

Додайте рядок для сповіщення адміністратора:

```
spamassassin_alerts: your_email@domain.com
```

Оновіть базу даних Postfix:

```
sudo newaliases
```

Використання графічних інтерфейсів

Для зручності спостереження та звітування можна використовувати графічні інтерфейси, такі як MailWatch, які забезпечують візуалізацію даних та створення детальних звітів.

Встановлення MailWatch для SpamAssassin:

Завантажте та встановіть MailWatch:

```
git clone https://github.com/mailwatch/mailwatch.git
cd mailwatch
./install.sh
```

Налаштуйте інтеграцію з SpamAssassin та Postfix:

```
sudo nano /etc/mailwatch.conf
```

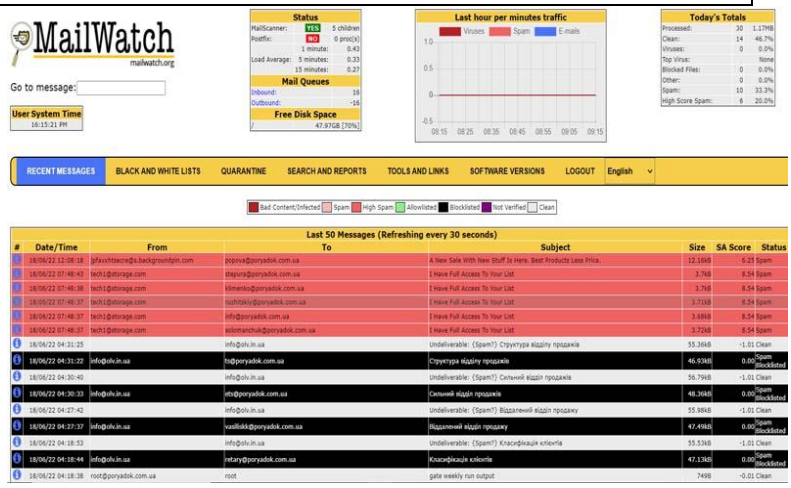

Рис.3.3. Вигляд MailWatch

Аудит та аналіз ефективності

Регулярний аудит системи дозволяє оцінювати ефективність SpamAssassin та вносити необхідні корективи для покращення фільтрації. Це включає аналіз помилково заблокованих (false positives) та пропущених (false negatives) повідомлень, а також внесення змін до правил та конфігурацій на основі отриманих результатів.

Аналіз помилкових позитивних та негативних спрацьовувань:

Перегляд звітів про помилково заблоковані повідомлення:

```
grep "false positive" /var/log/mail.log
```

Перегляд звітів про пропущені спам-повідомлення:

```
grep "false negative" /var/log/mail.log
```

Спостереження та звітування про безпеку електронної пошти з використанням SpamAssassin є важливим аспектом підтримки високого рівня кібербезпеки в корпоративних інформаційних системах. Ефективне впровадження та налаштування SpamAssassin дозволяє не тільки виявляти та блокувати спам і фішингові загрози, але й забезпечувати постійний моніторинг і оцінку ефективності роботи системи.

Першим кроком у цьому процесі є налаштування базових параметрів та правил, які визначають, які електронні листи будуть позначатися як спам. Важливо налаштувати порогові значення, що забезпечують баланс між мінімізацією помилкових позитивних спрацьовувань і ефективним блокуванням небажаних листів. Додатково, використання додаткових правил і плагінів, таких як правила SARE та плагін Razor, дозволяє розширити можливості виявлення спаму та фішингових загроз.

Налаштування та перевірка автентичності відправників за допомогою SPF, DKIM та DMARC допомагають запобігти підробці електронних адрес, що є важливим елементом захисту від фішингу. Використання цих технологій у комбінації з іншими методами фільтрації значно підвищує ефективність системи.

Моніторинг логів є важливим інструментом для відстеження роботи SpamAssassin. Аналіз лог-файлів дозволяє адміністраторам отримувати актуальну інформацію про оброблені електронні листи, виявлені спам-повідомлення та дії, вжиті для їх блокування. Інтеграція з системами моніторингу, такими як Nagios або Zabbix, дозволяє автоматизувати процес спостереження та забезпечити оперативне реагування на потенційні проблеми.

Створення звітів про роботу SpamAssassin є критичним для оцінки ефективності фільтрації та виявлення тенденцій у спам-атак. Використання утиліт, таких як pflogsumm, допомагає адміністраторам створювати детальні звіти, що включають інформацію про кількість заблокованих повідомлень, типи виявлених загроз та рівень точності фільтрації.

Автоматичне сповіщення про інциденти дозволяє адміністраторам оперативно реагувати на загрози, знижуючи ризик компрометації системи. Налаштування автоматичних сповіщень через поштовий сервер або інтеграція з системами керування інцидентами забезпечує своєчасне інформування про виявлені загрози.

Використання графічних інтерфейсів, таких як MailWatch, забезпечує зручну візуалізацію даних та створення детальних звітів. Це дозволяє адміністраторам легше інтерпретувати дані та приймати обґрунтовані рішення щодо налаштувань і оптимізації системи.

Регулярний аудит і аналіз ефективності системи є ключовими для підтримки високого рівня захисту. Це включає оцінку помилково заблокованих та пропущених спам-повідомлень, а також внесення необхідних змін до правил і конфігурацій. Постійне вдосконалення та адаптація системи до нових загроз допомагає підтримувати актуальність і ефективність SpamAssassin.

Загалом, комплексний підхід до спостереження та звітування про безпеку електронної пошти з використанням SpamAssassin дозволяє забезпечити надійний захист від спаму та фішингових загроз, підвищуючи загальний рівень кібербезпеки організації. Регулярний моніторинг, детальні звіти, автоматичне сповіщення та

постійне вдосконалення системи є ключовими елементами, які допомагають підтримувати ефективність і надійність захисту корпоративної електронної пошти.

3.3 Розробка рекомендацій щодо використання методів та інструментів протидії фішингу

Для успішної протидії фішинговим атакам були розроблені рекомендації для спеціалістів . Ключовими елементами є впровадження технологій аутентифікації електронної пошти, навчання користувачів, використання двофакторної аутентифікації, постійний моніторинг та звітування, налаштування фільтрів та антивірусного програмного забезпечення. Комплексний підхід до протидії фішинговим атакам дозволить значно підвищити рівень безпеки корпоративної електронної пошти та мінімізувати ризики компрометації інформації.

Технології аутентифікації електронної пошти

SPF (Sender Policy Framework):

SPF дозволяє адміністраторам доменів визначити, які сервери мають право надсилати електронні листи від імені їхнього домену. Це допомагає запобігти спуфінгу (підробці відправника) шляхом перевірки IP-адреси відправника з переліком дозволених серверів. Налаштування SPF запису в DNS є першим кроком для забезпечення автентичності відправника.

DKIM (DomainKeys Identified Mail):

DKIM використовує криптографічні підписи для перевірки автентичності повідомлення. Підписуючи повідомлення приватним ключем, DKIM дозволяє отримувачам перевіряти, чи було повідомлення змінено під час передачі, і чи дійсно воно надійшло від зазначеного відправника. Це забезпечує додатковий рівень захисту від підробки вмісту електронних листів.

DMARC (Domain-based Message Authentication, Reporting & Conformance):

DMARC об'єднує SPF і DKIM, дозволяючи власникам доменів визначати політику обробки повідомлень, які не пройшли аутентифікацію за допомогою SPF

або DKIM. DMARC також надає механізм для отримання звітів про спроби підробки повідомлень, що дозволяє адміністраторам аналізувати і реагувати на потенційні загрози.

Навчання користувачів

Освіта та підвищення обізнаності співробітників є важливим елементом боротьби з фішингом:

Регулярні тренінги з кібербезпеки: Проведення регулярних тренінгів, на яких співробітники навчаються виявляти фішингові повідомлення та правильно на них реагувати. Це може включати тренінги з розпізнавання підозрілих посилань, невідомих відправників і підозрілих вкладень.

Симуляції фішингових атак: Використання симуляцій фішингових атак для практичного навчання співробітників. Це допомагає підготувати їх до реальних атак, підвищуючи їх обізнаність та готовність до реагування.

Інформаційні кампанії: Проведення регулярних інформаційних кампаній, що включають розсилки електронною поштою, плакати та інші засоби інформування, щоб підтримувати високу обізнаність про загрози фішингу.

Використання двофакторної аутентифікації (2FA)

Двофакторна аутентифікація забезпечує додатковий рівень захисту облікових записів, що значно знижує ризик несанкціонованого доступу навіть у разі компрометації пароля. Впровадження 2FA може включати використання:

Одноразових паролів (OTP), які надсилаються на мобільний телефон користувача або генеруються спеціальними додатками.

Аппаратних токенів, які генерують одноразові паролі.

Біометричних методів, таких як відбитки пальців або розпізнавання обличчя.

Моніторинг та звітування

Постійний моніторинг та звітування про безпеку електронної пошти допомагають виявляти та швидко реагувати на нові загрози:

Інструменти моніторингу: Використання спеціалізованих інструментів для моніторингу підозрілої активності в системах електронної пошти. Ці інструменти

можуть виявляти аномальну активність та спроби фішингових атак у режимі реального часу.

Регулярні звіти: Створення регулярних звітів про безпеку електронної пошти, що містять інформацію про виявлені загрози, кількість фішингових атак та ефективність засобів захисту. Це дозволяє адміністраторам аналізувати дані та вносити необхідні корективи до політики безпеки.

Застосування фільтрів та засобів фільтрації

Фільтри електронної пошти є ефективним засобом для виявлення та блокування фішингових повідомлень:

Антифішингові фільтри: Використання спеціалізованих фільтрів для виявлення фішингових повідомлень на основі аналізу вмісту, заголовків та інших характеристик листів.

Чорні та білі списки: Ведення чорних списків для блокування відомих шкідливих відправників та білих списків для дозволу надійних контактів.

Аналіз вмісту: Застосування засобів аналізу вмісту для виявлення підозрілих посилань, вкладень та інших елементів, які можуть свідчити про фішингову атаку.

Використання антивірусного програмного забезпечення

Антивірусні програми забезпечують додатковий рівень захисту, виявляючи та блокуючи шкідливі вкладення у фішингових повідомленнях:

Регулярне оновлення антивірусного програмного забезпечення для забезпечення захисту від новітніх загроз та шкідливих програм.

Налаштування антивірусного програмного забезпечення для автоматичної перевірки всіх вхідних та вихідних листів.

ВИСНОВКИ

В ході виконання бакалаврської роботи мною було проведено дослідження методів захисту та протидії фішинговим атакам електронної пошти корпоративної системи на базі рішення SpamAssassin. Основною метою дослідження було визначення ефективних способів і засобів виявлення фішингових атак та розробка рекомендацій для підвищення рівня захисту корпоративної електронної пошти. Ця тема є надзвичайно актуальною у світлі зростання кількості та складності кіберзагроз.

Проведено глибокий аналіз сучасних методів захисту електронної пошти та інструментів фільтрації спаму. Було встановлено, що традиційні методи захисту електронної пошти не завжди забезпечують достатній рівень безпеки, оскільки фішингові атаки стають все більш витонченими. Використання SpamAssassin дозволяє автоматизувати процес виявлення та блокування фішингових повідомлень, що значно знижує ризики компрометації корпоративної інформації.

Досліджено методи налаштування та оптимізації SpamAssassin для підвищення ефективності виявлення фішингових атак. Налаштування включають використання байєсових фільтрів, чорних та білих списків, а також технологій SPF, DKIM та DMARC для перевірки автентичності відправника. Це дозволяє не тільки знижувати кількість фальшивих позитивів, але й підвищувати точність виявлення реальних загроз.

Розроблено детальні рекомендації щодо впровадження SpamAssassin у корпоративні системи електронної пошти. Ці рекомендації включають кроки з налаштування та інтеграції SpamAssassin з існуючими поштовими серверами, а також з використання додаткових правил та плагінів для підвищення ефективності фільтрації. Особлива увага приділена питанням моніторингу та звітування про роботу системи, що дозволяє адміністраторам оперативно реагувати на нові загрози.

Запропоновані рекомендації включають опис кроків для налаштування основних параметрів SpamAssassin, інтеграцію з поштовими серверами, використання додаткових плагінів та модулів, а також навчання користувачів методам виявлення фішингових повідомлень. Використання цих рекомендацій дозволяє значно підвищити рівень безпеки корпоративної електронної пошти, зменшуючи ризики компрометації та забезпечуючи ефективний захист від фішингових атак.

Впровадження розроблених методів та рекомендацій дозволить організаціям значно знизити ризики, пов'язані з фішинговими атаками, забезпечуючи високий рівень захисту корпоративної інформації. Оптимізація роботи SpamAssassin, налаштування його правил та плагінів, а також навчання користувачів сприятимуть створенню надійної системи захисту електронної пошти. Інтеграція з іншими засобами кібербезпеки дозволить забезпечити комплексний підхід до захисту інформаційних ресурсів організації.

Таким чином, дослідження методів захисту та протидії фішинговим атакам електронної пошти корпоративної системи на базі рішення SpamAssassin є важливим кроком до забезпечення кібербезпеки в сучасних умовах зростаючих кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. DNS Blocklists in SpamAssasin. URL: https://cwiki.apache.org/confluence/display/SPAMASSASSIN/DnsBlocklists (date of access: 10.05.2024).
2. BayesInSpamAssassin - SPAMASSASSIN - Apache Software Foundation. *Dashboard - Apache Software Foundation*. URL: https://cwiki.apache.org/confluence/display/SPAMASSASSIN/BayesInSpamAssassin (date of access: 31.05.2024).
3. *Enterprise Cybersecurity Solutions, Services & Training | Proofpoint US*. URL: https://www.proofpoint.com/sites/default/files/proofpoint-email-protection-solution-brief.pdf (дата звернення: 07.05.2024).
4. Phishing Protection | Phishing Email Protection. *Mimecast*. URL: https://www.mimecast.com/content/phishing-protection/ (date of access: 07.05.2024).
5. What is Anti-Phishing? | Anti-Phishing Solution. *Mimecast*. URL: https://www.mimecast.com/content/anti-phishing/ (date of access: 07.05.2024).
6. Inc P. Proofpoint's 2024 State of the Phish Report: 68% of Employees Willingly Gamble with Organizational Security. *Yahoo Finance*. URL: https://finance.yahoo.com/news/proofpoint-2024-state-phish-report-094900568.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAHhONi8Jwywd-25NEF5ou5k2KyhKurmjymjxe2eIboYdTaQrfZz3PbD7UfiB-14vIrJMatExn_gLW-42T386y1ryC9q0JxV5Uuvmwg5IVz5dr935RCOoiDgbwKilM2XR3Fg81rD7IJX5VzvnRAMz3t33a8BQKfpOJEITlQy2k4ab (date of access: 07.05.2024).
7. Apache SpamAssassin: Welcome. *Apache SpamAssassin: Welcome*. URL: https://spamassassin.apache.org/ (date of access: 14.05.2024).
8. Home - SPAMASSASSIN - Apache Software Foundation. *Dashboard - Apache Software Foundation*. URL:

https://cwiki.apache.org/confluence/display/SPAMASSASSIN/ (date of access: 14.05.2024).

9. Norton 360 Standard: Sicherheit für Desktop oder Smartphone. *Offizielle Website | Norton™ - Antivirus und Anti-Malware-Software*. URL: https://norton.com/products/norton-360-standard (date of access: 14.05.2024).

10. Top 13 Email Threat Types. *Barracuda Networks*. URL: https://www.barracuda.com/solutions/13-email-threat-types (date of access: 14.05.2024).

11. Regional Policies. *Barracuda Campus*. URL: https://campus.barracuda.com/product/emailgatewaydefense/doc/96023019/regional-policies/ (date of access: 14.05.2024).

12. How to send Password-protected Emails in Proton Mail | Proton. *Proton*. URL: https://proton.me/support/ru/password-protected-emails (date of access: 14.05.2024).

13. Spam, block, and allow lists | Proton. *Proton*. URL: https://proton.me/support/ru/spam-filtering (date of access: 14.05.2024).

14. Скибун О. ФІШИНГ ТА ФІШЕРИ В СУЧАСНОМУ СВІТІ. *Grail of Science*. 2023. № 23. С. 259–264. URL: https://doi.org/10.36074/grail-of-science.23.12.2022.38 (дата звернення: 30.05.2024).

15. Танашкіна М. Д. Фішинг - як вид шахрайства в Інтернеті. *Правникъ*. 2018. № 2 (весна). С. 87–89.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)