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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розроблення рекомендацій щодо запобіганню атак з використанням соціальної інженерії»

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

_____ Когут Дмитро
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
Когут Дмитро
(прізвище, ім'я)

Керівник к.т.н., доцент Борсуковський Ю.В.
(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

Когуту Дмитру Юрійовичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розроблення рекомендацій щодо запобігання атак з використанням соціальної інженерії »

керівник кваліфікаційної роботи к.т.н., доцент Борсуковський Ю.В.
(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 31.06.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення Cisco email security;
наукова та технічна література, експлуатаційна документація, нормативні

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми захисту кінцевих точок організації.
2. Аналіз методів та засобів захисту внутрішніх листуваннь на базі використання Cisco email security
3. Розроблення рекомендацій щодо захисту внутрішніх листуваннь на базі використання Cisco email security

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми атак з використанням соціальної інженерії.		
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.		
3.	Аналіз методів та засобів захисту внутрішніх листувань на базі використання Cisco email security.		
4.	Практична реалізація варіанту захисту внутрішніх листувань на базі використання Cisco email security.		
5.	Розроблення рекомендацій щодо застосування методів та засобів захисту від атак з використанням соціальної інженерії.		
6.	Оформлення результатів дослідження.		
7.	Підготовка доповіді до захисту.		

Здобувач вищої освіти _____ Когут Дмитро
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Юрій Борсуковський
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Когута Дмитра
на тему: «Дослідження шляхів та розроблення рекомендацій щодо запобіганню атак з використанням соціальної інженерії»

Актуальність: Соціальна інженерія є однією з найбільших загроз у сучасному кіберпросторі. Використовуючи психологічні маніпуляції, зловмисники можуть отримати доступ до конфіденційної інформації, обманюючи людей. Атаки соціальної інженерії є небезпечними через їхню простоту, ефективність і здатність обходити технічні засоби захисту. Це робить питання дослідження шляхів запобігання таким атакам особливо актуальним для захисту організацій і приватних осіб.

Позитивні сторони:

1. За допомогою проведеного аналізу встановлено проблематику захисту від загроз з викроситанням соціальної інженерії.
2. Досліджено методи та засоби захисту від загроз з використанням соціальної інженерії на базі Cisco email security.
3. Розроблено варіант системи захисту від загроз з використанням соціальної інженерії на базі Cisco email security.

Недоліки:

1. У кваліфікаційній роборі не було розкрито повних можливостей обраних програмних засобів.
2. Не було показано показано як обрані програмні засоби будут працювати в поєднанні з іншими для забезпечення більш надійного захисту
3. Запропонований варіант системи захисту було б бажано продемонструвати на прикладі конкретної організації .

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент:

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 53 сторінки, 17 рисунків, 12 джерел.

Об'єкт дослідження – захист від атак з використанням соціалної інженерії.

Предмет дослідження – методи та засоби захисту внутрнішніх листуваннь на базі CISCO EMAIL SECURITY(ESA).

Мета роботи розробити варіант системи на базі рішення ESA та рекомендації щодо застосування методів та засобів захисту внутрішніх листувань організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз загроз, практичне застосування.

Email security appliance відіграє важливу роль в захисті корпоративних листувань та підвищені рівня безпеки організації. Системи ESA призначені для для захисту організацій від загроз, пов'язаних з електронною поштою, таких як спам, шкідливе програмне забезпечення, фішингові атаки та витоки даних. Він забезпечує передові можливості захисту від загроз, щоб допомогти забезпечити безпеку електронних комунікацій.

В роботі досліджено проблему захисту внутрішніх листувань , визначено мету та завдання. Проведено аналіз існуючиз методів захисту внутрішніх листувань та електронних комунікацій. Досліджено методи захисту корпоративних листувань на базі CISCO EMAIL SECURITY(ESA). Визначено призначення, основні функції та склад рішення.

На основі проведених робіт запровоновано варіанти рішень на базі CISCO EMAIL SECURITY(ESA). Розроблено рекомендації щодо реалізації захисиу внутрішніх листувань.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ЗМІСТ

Вступ

Соціальна інженерія - це метод впливу на людей з метою отримання конфіденційної інформації або здійснення певних дій. Зазвичай цей термін використовується в контексті кібербезпеки і означає використання маніпуляцій та обману для отримання доступу до конфіденційної інформації чи впливу на поведінку людей.

Прикладами соціальної інженерії можуть бути шахрайські дзвінки, фішингові електронні листи, атаки в соціальних мережах тощо. Злоумисники можуть виглядати як довірливі особи, представляючися, наприклад, технічною підтримкою, інспекторами безпеки або іншими авторитетними особами, щоб викликати у потенційної жертви віру і отримати від неї інформацію.

Атаки з використанням соціальної інженерії можуть приймати різні форми та використовувати різні методи маніпуляцій для отримання неправомірного доступу чи конфіденційної інформації.

Ось деякі типові приклади атак, які використовують соціальну інженерію:

Фішинг: Атаки фішингу включають в себе надсилання шахрайських електронних листів або повідомлень, що намагаються обманути людей та надихнути їх відкрити зловмисний вміст або надати конфіденційну інформацію, таку як паролі чи дані кредитної картки.

Відгук на події: Зловмисники можуть виглядати як представники компаній, громадських служб або інших організацій та надсилати фальшиві повідомлення про події або кризові ситуації, щоб надихнути людей на реакцію та надання інформації.

Соціальний інженер у реальному житті:

Зловмисники можуть намагатися входити в довіру, використовуючи соціальну інженерію в особистому спілкуванні. Наприклад, вони можуть виглядати як співробітники компаній чи сервісних служб та намагатися отримати доступ до об'єктів або інформації в реальному середовищі.

Атаки в соціальних мережах: Зловмисники можуть створювати фальшиві профілі та взаємодіяти з користувачами в соціальних мережах, витягаючи важливу інформацію або розповсюджуючи шахрайський вміст.

Технічна підтримка: Атаки можуть включати в себе дзвінки або повідомлення від осіб, які виглядають як технічна підтримка, і які намагаються отримати доступ до комп'ютерів або інших пристроїв під виглядом вирішення технічних проблем.

На жаль, атаки з використанням соціальної інженерії залишаються дуже актуальними і представляють серйозну загрозу як для індивідуальних користувачів, так і для підприємств.

Деякі причини, що підтримують актуальність цих атак, включають:
Людський фактор: Слабкість в захисті від соціальної інженерії часто пов'язана з людським фактором. Зловмисники використовують психологічні методи, щоб викликати відповіді, які дозволяють їм отримати доступ до конфіденційної інформації.

Зростання інтернет-залежності: Зі зростанням використання інтернету та соціальних мереж, атаки з використанням соціальної інженерії отримують нові можливості для здійснення атак на користувачів в онлайн-середовищі.

Залучення великої кількості інформації: Зловмисники можуть використовувати доступну велику кількість особистої інформації в інтернеті для створення переконливих атак, виглядаючи як довірливі особи або використовуючи особисті подробиці.

Недостатній рівень освіти користувачів: Багато користувачів можуть бути недостатньо освіченими щодо ризиків та методів захисту від соціальної інженерії, що робить їх легкими мішенями для атак.

Стрімка еволюція атак: Зловмисники постійно вдосконалюють свої методи соціальної інженерії, щоб уникати виявлення та пристосовуватися до нових технологій та заходів безпеки.

1.1Аналіз проблеми атак з використанням соціальної інженерії

Проблема атак з використанням соціальної інженерії стає все більш актуальною в сучасному цифровому світі, де люди все більше залучаються до використання інтернету та соціальних мереж. Соціальна інженерія полягає у використанні маніпулятивних технік для отримання конфіденційної інформації або навіть зламу системи шляхом використання психологічних механізмів.

Основні аспекти цієї проблеми включають:

1. Маніпуляція довіри: Зловмисники можуть використовувати соціальну інженерію, щоб підібрати довірливість у потенційної жертви, шляхом підробки ідентифікаційних даних або створення ситуацій, де жертва відчуває необхідність допомогти.

2. Використання соціальних мереж: Соціальні мережі надають зловмисникам доступ до величезної кількості особистої інформації про людей, що дозволяє їм створювати правдоподібні атаки або фішингові повідомлення.

3. Фішинг: Це метод атак, який полягає у відправці фальшивих повідомлень (електронною поштою, повідомленнями в соціальних мережах тощо), з метою отримання конфіденційної інформації або виклику певних дій від жертви.

4. Технічна соціальна інженерія: Зловмисники можуть використовувати соціальну інженерію, щоб отримати фізичний доступ до приміщень або комп'ютерних систем, використовуючи маніпуляцію людьми, що мають доступ.

5. Брак освіти: Багато людей не розуміють повної міри загроз, які становить соціальна інженерія, і тому можуть стати легкою мішенню.

Соціальна інженерія в реальному житті

Соціальна інженерія в реальному житті представляє собою маніпулювання людьми з метою отримання конфіденційної інформації або здійснення інших шахрайських дій. Цей підхід базується на використанні психологічних та соціальних методів, а не технічних атак, для досягнення своїх цілей. Ось деякі приклади соціальної інженерії в реальному житті:

1. Фішингові атаки через електронну пошту: Зловмисники можуть надсилати електронні листи, що виглядають як офіційні повідомлення від компаній чи організацій, і просити отримати конфіденційну інформацію, таку як паролі чи номери кредитних карток.

2. Телефонні шахрайства (vishing): Атаки, під час яких зловмисники дзвонять людям, представляючись різними фігурами, такими як банківські

представники або технічна підтримка, і намагаються отримати особисту інформацію або переконати їх здійснити фінансові транзакції.

3. Атаки в соціальних мережах: Зловмисники можуть створювати фальшиві профілі, імітуючи друзів, колег чи інших користувачів соціальних мереж, для отримання доступу до особистої інформації або розповсюдження шахрайських повідомлень.

4. Фішинг через текстові повідомлення (smishing): Зловмисники можуть висилати текстові повідомлення, претендуючи на представників банків, компаній чи сервісів, і намагатися викликати у користувача реакцію, включаючи надання особистої інформації.

5. Атаки на відомість (pretexting): Зловмисники можуть створювати вигадані історії чи обставини, щоб обманом отримати довір'я інших осіб та використовувати це довір'я для отримання інформації.

6. Атаки в офісі: Зловмисники можуть намагатися проникнути в корпоративний офіс, вигадуючи себе службовцями, контрактниками чи іншими авторитетними особами.

Фішингові атаки через електронну пошту

Фішингові атаки через електронну пошту — це метод атаки, коли зловмисники відправляють шахрайські електронні листи, щоб обманом отримати конфіденційну інформацію від користувачів. Такі електронні листи можуть виглядати, ніби вони відомі або надійні джерела, такі як банки, компанії чи громадські служби. Ось деякі типові риси електронної пошти фішингу:

1. Імітація надійного джерела: Зловмисники стараються підробити логотипи, стилі оформлення та ім'я відомих компаній чи організацій, щоб зробити електронний лист схожим на офіційні повідомлення від цих джерел.

2. Створення термінової ситуації: Фішери можуть намагатися створити враження терміновості або небезпеки, щоб викликати спонтанну реакцію від одержувача.

3. Ланки на фальшиві веб-сайти: Електронні листи можуть містити ланки, які ведуть на фальшиві веб-сайти, що наочно імітують логін-сторінки або інші онлайн-ресурси. Метою цього може бути збір паролів або іншої конфіденційної інформації.

4. Запит на особисту інформацію: Фішери можуть намагатися отримати особисту інформацію, таку як паролі, номери кредитних карток, адреси та інше, використовуючи підступні запити в електронних листах.

5. Використання масового розсилання: Атаки можуть бути направлені на велику кількість користувачів шляхом масового розсилання фішингових електронних листів.

Атаки в офісі

Атаки в офісі можуть включати різні соціально-інженерні методи, що мають на меті отримання конфіденційної інформації або викликання інших негативних наслідків. Декілька прикладів атак в офісі включає:

- Фізичний доступ: Зловмисники можуть спробувати отримати фізичний доступ до приміщень офісу, вигадуючи, що вони є новими співробітниками, кур'єрами чи службовцями певних служб.

Фізичний доступ до офісних приміщень може стати точкою вразливості для безпеки інформації та активів компанії. Атаки, пов'язані з отриманням фізичного доступу, можуть призвести до втрати конфіденційної інформації, втрати обладнання чи інших потенційних ризиків. Ось деякі аспекти та стратегії атак в офісному середовищі:

1. Спостереження і підслуховування: Зловмисники можуть спостерігати за діяльністю в офісі або використовувати аудіо- та відеозаписи для отримання конфіденційної інформації.

2. Підміна пристроїв: Злоумисники можуть встановлювати фізично модифіковані пристрої (наприклад, USB-ключі, клавіатури, миші) для отримання доступу або крадіжки інформації.

3. Соціальна інженерія в офісі: Використання соціальної інженерії для отримання доступу в офіс шляхом вигадування різних сценаріїв або позначення під відомих працівників.

4. Викрадення або підміна ідентифікаційних карток: Зловмисники можуть красти або підмінювати картки доступу для нелегального входу в приміщення.

5. Фізична крадіжка обладнання: Атакувальники можуть викрадати комп'ютери, сервери або інші фізичні пристрої для отримання доступу до зберіганої інформації.

6. Використання неконтрольованих пристроїв: Введення в офіс непідконтрольованих пристроїв, таких як USB-ключі чи переносні комп'ютери, які можуть використовуватися для витоку інформації.

7. Підробка персоналу: Атакувальники можуть видачи себе за співробітників або представників інших організацій та намагатися отримати доступ до інформації або ресурсів.

8. Спілкування зі співробітниками: Зловмисники можуть намагатися взаємодіяти зі співробітниками офісу, вигадуючи різні причини, такі як опитування, перевірка безпеки, чи інші обставини.

9. Соціальна інженерія через телефонні дзвінки: Використання телефонних дзвінків для взаємодії зі співробітниками та вигадування сценаріїв для отримання інформації.

10. Фішингові атаки в офісі: Надсилання фішингових електронних листів або інших підступних повідомлень співробітникам офісу з метою отримання їхніх логінів, паролів або іншої конфіденційної інформації.

Використання пристроїв USB

Використання пристроїв USB: Зловмисники можуть залишати заражені USB-носії в офісі, на надію, що хтось їх підключить, і тим самим викличе інфікування систем.

Використання пристроїв USB може бути потенційною загрозою для безпеки інформації в офісному середовищі. Ось декілька аспектів, які слід враховувати щодо безпеки USB-пристроїв:

1. Інфікування вірусами та шкідливим ПЗ: USB-пристрої можуть містити віруси, троянці, чи інше шкідливе програмне забезпечення. Якщо співробітник вставляє такий пристрій у робочий комп'ютер, це може призвести до інфікування системи.

2. Витік конфіденційної інформації: Співробітники можуть використовувати USB-пристрої для копіювання чи вивезення конфіденційної інформації з офісу. Це може становити загрозу для безпеки даних та конфіденційності.

3. Атаки "BadUSB": "BadUSB" - це метод атаки, при якому атакувальник може перепрограмувати функції USB-пристрою, змінити його функціональність та використовувати для введення шкідливого коду.

Атаки "BadUSB" представляють собою метод, при якому атакувальники зловживають можливостями програмування вбудованих контролерів USB-пристроїв, щоб змінити їхню функціональність. Це може призвести до широкого спектру загроз, таких як введення шкідливого коду на систему, перепрограмування пристроїв для виконання небажаних дій або навіть фізичного збитку USB-пристроїв.

Основні особливості атак "BadUSB":

1. Фірмвар від атакувальника: Атакувальники можуть змінити фірмвар (програмне забезпечення вбудованого контролера) USB-пристроїв, перепрограмувавши його для виконання відомих їм команд.

2. Ховані функції: Атакувальники можуть приховати шкідливий код в стандартних функціях USB-пристрою, щоб обманути системи безпеки.

3. Автоматичне запускання атак: Шкідливий USB-пристрій може автоматично запускати атаки на комп'ютер, вставлений в USB-порт, без будь-якого втручання користувача.

4. Сховані атаки: Атакувальники можуть використовувати "BadUSB" для впровадження різноманітних атак, таких як відправлення клавіатурних команд, імітація мережевих адаптерів та інші.

5. Підробка пристроїв: Атакувальники можуть використовувати підроблені USB-пристрої, щоб отримати фізичний або логічний доступ до системи.

1.2Аналіз підходів до захисту від атак з використанням соціальної інженерії

Підходи до захисту від атак з використанням соціальної інженерії можна розділити на кілька основних категорій:

1. Освіта та навчання: Один з найважливіших підходів - це освіта та навчання персоналу та користувачів. Працівникам слід надавати регулярні інструкції щодо ризиків соціальної інженерії та викладати їм стратегії виявлення та запобігання атакам. Користувачам також слід надавати освітні матеріали та тренування з виявлення фішингових атак та інших маніпуляційних методів.

2. Мультіфакторна аутентифікація: Використання мультіфакторної аутентифікації може значно ускладнити завдання зловмисникам, оскільки вони не зможуть отримати доступ до облікового запису без додаткового підтвердження, навіть якщо вони отримали доступ до логіну та паролю.

3. Використання технологічних засобів безпеки: Використання антивірусного програмного забезпечення, програм для виявлення фішингу, фільтрів спаму та інших інструментів безпеки може допомогти виявляти та блокувати атаки з використанням соціальної інженерії.

4. Створення культури безпеки: Важливо створити культуру безпеки в організації, де працівники розуміють важливість безпекових практик і відповідальні за дотримання цих практик. Це може включати регулярні нагадування про правила безпеки, шкільні тренування та стимулювання виконання безпекових процедур.

5. Впровадження строгих правил безпеки: Компанії та організації повинні розробляти та впроваджувати строгі правила безпеки, щоб захистити конфіденційну інформацію та обмежити доступ до неї тільки для авторизованих користувачів.

6. Стеження за вразливостями та оновлення програмного забезпечення: Постійне стеження за вразливостями та оновлення програмного забезпечення допоможе уникнути використання вразливостей зловмисниками для отримання доступу.

Мультіфакторна аутентифікація

Мультіфакторна аутентифікація (MFA) - це метод аутентифікації, що вимагає від користувача надання двох або більше незалежних факторів для підтвердження своєї особи перед наданням доступу до системи або облікового запису. Цей підхід до захисту дозволяє ускладнити завдання зловмисникам, які намагаються отримати несанкціонований доступ, навіть якщо вони володіють одним з факторів аутентифікації.

Основні компоненти мультіфакторної аутентифікації включають:

1. Щось, що ви знаєте: Це може бути пароль, ПІН-код або відповідь на контрольне питання. Цей фактор зазвичай є єдиним, який користувач вводить вручну.

2. Щось, що ви маєте: Це може бути фізичний пристрій, такий як смартфон або ключ-USB, який генерує одноразові паролі (OTP) або здійснює підпис підтвердження. Фізичний токен або мобільний додаток можуть використовуватися як другий фактор аутентифікації.

3. Щось, що ви є: Цей фактор включає біометричні дані користувача, такі як відбиток пальця, розпізнавання обличчя або сканування радужки.

Переваги мультіфакторної аутентифікації включають:

• Підвищена безпека: Навіть якщо один з факторів аутентифікації компрометовано, доступ до системи все одно буде захищено, оскільки зловмисники не матимуть доступу до інших факторів.

• Захист від фішингу та парольних атак: Зловмисники, які намагаються викрасти паролі або провести фішингові атаки, зазвичай не зможуть отримати доступ до другого фактора аутентифікації.

• Забезпечення відповідності нормативам безпеки: Використання мультіфакторної аутентифікації може відповідати вимогам регуляторних організацій та стандартам безпеки даних.

Використання технологічних засобів безпеки

Використання технологічних засобів безпеки є ключовим компонентом стратегії захисту від атак з використанням соціальної інженерії. Ці технологічні інструменти допомагають виявляти, блокувати та реагувати на потенційні загрози, забезпечуючи безпеку інформації та систем. Ось деякі ключові технологічні засоби безпеки:

1. Антивірусне програмне забезпечення: Ці програми виявляють, блокують та видаляють шкідливе програмне забезпечення, включаючи програми-шпигуни, віруси та троянські коні.

2. Брандмауери: Брандмауери встановлюють периметральні бар'єри, щоб контролювати потік даних між внутрішніми мережами та зовнішніми мережами Інтернету, захищаючи мережеві ресурси від несанкціонованого доступу.

3. Системи виявлення вторгнень (IDS) та системи управління використанням загроз (SIEM): IDS виявляють аномальну або зловмисну активність в мережі, тоді

як SIEM збирає та аналізує дані з різних джерел, щоб виявляти вторгнення та реагувати на них.

4. Системи захисту електронної пошти: Ці системи використовують фільтри та аналізатори для виявлення та блокування спамових повідомлень, фішингових атак та інших загроз, пов'язаних з електронною поштою.

5. Шифрування даних: Шифрування даних забезпечує конфіденційність інформації, що передається по мережі, а також зберіганої на пристроях, унеможливлюючи несанкціонований доступ до них.

6. Системи управління правами доступу: Ці системи дозволяють адміністраторам керувати правами доступу користувачів до різних ресурсів, обмежуючи доступ тільки до необхідної інформації та функцій.

7. Системи моніторингу та аналізу активності користувачів: Ці системи відстежують та аналізують дії користувачів у системі, щоб виявляти підозрілу або несанкціоновану активність.

Створення культури безпеки

Створення культури безпеки в організації є важливим елементом ефективної стратегії захисту від атак з використанням соціальної інженерії. Це означає виховання свідомості та усвідомлення персоналом безпекових практик і створення середовища, в якому безпека даних і інформації стає пріоритетом. Ось кілька ключових аспектів створення культури безпеки:

1. Лідерство та залучення керівництва: Підтримка верхівки управління є ключовою для успіху будь-якої ініціативи щодо безпеки. Керівництво повинно виявити свою зобов'язаність до безпеки даних, активно просуваючи та підтримуючи програми безпеки.

2. Освіта та навчання персоналу: Регулярні тренування та навчання персоналу щодо безпекових практик і виявлення потенційних загроз є важливим елементом створення культури безпеки. Це включає навчання персоналу розпізнавати фішингові атаки, управляти паролями, а також поводитися з конфіденційною інформацією.

3. Залучення всіх рівнів персоналу: Культура безпеки має бути розповсюджена на всіх рівнях організації, від керівництва до робітників. Кожен працівник повинен розуміти свою роль у забезпеченні безпеки інформації та дотримуватися відповідних політик і процедур.

4. Створення політик безпеки: Організації повинні розробити і впровадити конкретні політики безпеки, які визначають правила та вимоги щодо обробки, зберігання та передачі конфіденційної інформації.

5. Постійне оновлення та аналіз інцидентів: Важливо постійно оновлювати політики та процедури безпеки, враховуючи нові загрози та вразливості. Також необхідно аналізувати інциденти безпеки, щоб виправляти помилки та запобігати їх повторенню.

6. Системи винагородження та стимулювання: Створення систем винагородження та стимулювання може підтримати відповідальну поведінку персоналу в галузі безпеки, що сприяє створенню позитивної культури безпеки.

Впровадження строгих правил безпеки

Впровадження строгих правил безпеки є ключовим елементом захисту від атак з використанням соціальної інженерії, оскільки допомагає уникнути небажаних ситуацій та забезпечити безпеку даних та систем. Ось кілька важливих аспектів впровадження строгих правил безпеки:

1. Розробка політик безпеки: Організація повинна розробити докладні політики безпеки, які визначають правила та вимоги щодо захисту даних та інформації. Ці політики повинні включати в себе вимоги щодо паролів, доступу до систем, обміну інформацією та інші аспекти безпеки.

2. Сильні паролі та аутентифікація: Встановлення вимог до складності паролів, регулярне їх оновлення та використання мультіфакторної аутентифікації можуть значно зменшити ризик несанкціонованого доступу до систем та даних.

3. Обмеження доступу: Встановлення принципу найменших привілеїв та обмеження доступу до чутливої інформації тільки на необхідний час і тільки авторизованим користувачам.

4. Шифрування даних: Важливо шифрувати дані під час їх передачі по мережі та зберігання на пристроях, щоб уникнути несанкціонованого доступу до них у разі втрати чи крадіжки.

5. Регулярні оновлення та патчі: Постійне оновлення програмного забезпечення та вчасне встановлення патчів та оновлень допомагають уникнути використання вразливостей зловмисниками для атак.

6. Моніторинг та аудит безпеки: Проведення регулярного моніторингу систем безпеки, виявлення аномальних активностей та проведення аудиту безпеки дозволяють своєчасно виявляти та реагувати на можливі загрози.

7. Санкції за порушення правил безпеки: Встановлення правил та санкцій за їх порушення допомагає стимулювати персонал до дотримання безпекових норм і зменшити можливість внутрішніх загроз.

1.3 Аналіз існуючих рішень із захисту від атак з використанням соціальної інженерії

Існує безліч рішень для захисту від атак з використанням соціальної інженерії, які включають в себе технологічні інструменти, стратегії освіти та навчання персоналу, культурні підходи та інші заходи безпеки. Ось кілька існуючих рішень:

1. Фільтри електронної пошти: Використання фільтрів електронної пошти для виявлення та блокування спаму, фішингових атак та шкідливих вкладень може значно зменшити ризик успішної атаки з використанням соціальної інженерії через електронну пошту.

2. Системи мультіфакторної аутентифікації: Впровадження систем мультіфакторної аутентифікації зміцнює безпеку входу до систем, ускладнюючи завдання для зловмисників, які намагаються отримати несанкціонований доступ.

3. Технології управління доступом: Використання технологій управління доступом, які базуються на правилах та політиках безпеки, дозволяє обмежити доступ до конфіденційної інформації тільки авторизованим користувачам.

4. Системи моніторингу та аналізу активності користувачів: Впровадження систем, які відстежують та аналізують активність користувачів у системі, може допомогти вчасно виявляти підозрілі дії та запобігати атакам з використанням соціальної інженерії.

5. Навчання та тренінги персоналу: Організація регулярних навчань та тренінгів для персоналу з питань безпеки допомагає підвищити їхню осведомленість та навички виявлення та запобігання соціальній інженерії.

6. Створення культури безпеки: Розвиток культури безпеки, в якій кожен працівник відчуває відповідальність за безпеку інформації та систем, може стати ефективним захистом від атак з використанням соціальної інженерії.

7. Системи миттєвого повідомлення та реагування на інциденти: Впровадження систем, які швидко виявляють та реагують на інциденти безпеки, може зменшити час відновлення після атак та мінімізувати наслідки.

Фільтри електронної пошти

Фільтри електронної пошти - це технологічні інструменти, які використовуються для виявлення та блокування небажаних повідомлень електронної пошти, таких як спам, фішингові атаки, віруси та інші шкідливі повідомлення, що містять віруси або шкідливі посилання. Вони допомагають зберегти чистоту та безпеку

електронної пошти користувачів та організацій. Ось кілька ключових функцій фільтрів електронної пошти:

1. Виявлення спаму: Фільтри електронної пошти використовують різні методи, такі як аналіз ключових слів, співставлення патернів та аналіз заголовків, для виявлення повідомлень, що містять спам.

2. Виявлення фішингу: Вони також виявляють повідомлення, що намагаються використати соціальну інженерію для отримання конфіденційної інформації, такі як логіни, паролі або фінансові дані.

3. Аналіз вкладень: Фільтри електронної пошти перевіряють вкладені файли на наявність вірусів, троянських програм та інших шкідливих кодів.

4. Білий та чорний список: Вони можуть використовувати списки електронних адрес або доменів для блокування або допуску повідомлень від певних адрес або доменів.

5. Налаштування правил: Користувачі можуть налаштовувати правила фільтрації для автоматичної обробки повідомлень відповідно до їх власних потреб.

6. Сповіщення про підозрілі повідомлення: Деякі фільтри можуть надсилати сповіщення користувачам про повідомлення, які містять підозрілі елементи або вважаються потенційно шкідливими.

Системи мультіфакторної аутентифікації

Системи мультіфакторної аутентифікації (MFA) - це методи перевірки ідентичності користувача, які вимагають двох або більше методів аутентифікації перед наданням доступу до системи чи послуги. Це важлива стратегія захисту від атак з використанням соціальної інженерії, оскільки ускладнює завдання для зловмисників, які намагаються отримати несанкціонований доступ до облікових записів або систем.

Ось деякі ключові компоненти систем мультіфакторної аутентифікації:

1. Щось, що ви знаєте: Це може бути пароль, PIN-код, відповідь на контрольний питання або будь-яка інша інформація, яка відома тільки користувачу.

2. Щось, що ви маєте: Це може бути фізичний об'єкт, такий як токен, смарт-карта або USB-ключ, який користувач повинен мати при собі для аутентифікації.

3. Те чим ви є: Це використання біометричних даних, таких як відбиток пальця, розпізнавання обличчя, розпізнавання голосу або інші унікальні фізичні характеристики користувача.

Переваги систем мультіфакторної аутентифікації включають:

• Підвищена безпека: Навіть якщо один метод аутентифікації стає компромісним, інші методи залишаються для захисту облікового запису.

• Зменшення ризику доступу зловмисників: Ускладнюється завдання для зловмисників, оскільки вони повинні мати доступ до кількох елементів аутентифікації.

• Покращене відчуття безпеки користувачів: Користувачі відчувають себе захищеними, знаючи, що їх облікові записи захищені не лише паролем, а й додатковими шарами безпеки.

• Відповідність з вимогами безпеки: Багато галузей, таких як фінанси або медицина, вимагають використання мультіфакторної аутентифікації для забезпечення відповідності стандартам безпеки.

Системи моніторингу та аналізу активності користувачів

Системи моніторингу та аналізу активності користувачів (User Activity Monitoring, UAM) - це інструменти, які використовуються для збору, аналізу і візуалізації даних про дії користувачів у системі. Вони дозволяють організаціям виявляти ненормальну або підозрілу активність, виявляти загрози безпеці та вчасно реагувати на потенційні інциденти безпеки. Ось кілька ключових аспектів систем моніторингу та аналізу активності користувачів:

1. Логування дій користувачів: Системи UAM збирають дані про дії користувачів, такі як вхід в систему, взаємодія з файлами та документами, доступ до мережевих ресурсів тощо.

2. Аналіз поведінки користувачів: Шляхом аналізу зібраних даних системи UAM можуть виявляти зміни в звичайному патерні поведінки користувачів, що може свідчити про потенційні загрози або компроміс облікового запису.

3. Виявлення підозрілих дій: Системи UAM використовують різні алгоритми та правила для виявлення незвичайних або підозрілих дій, таких як спроби несанкціонованого доступу, спроби підйому привілеїв, аномальний обсяг даних, що передається тощо.

4. Сповіщення та реагування на інциденти: При виявленні підозрілої активності системи UAM можуть генерувати сповіщення адміністраторам безпеки або

автоматично запускати процедури реагування, такі як блокування облікового запису, відключення від мережі або запуск інцидентної відповіді.

5. Аудит та звітність: Системи UAM можуть створювати детальні звіти про активність користувачів для аудиту та відповідності стандартам безпеки, що допомагає організаціям виконувати регуляторні вимоги та внутрішні політики.

6. Інтеграція з іншими системами безпеки: Системи UAM можуть інтегруватися з іншими системами безпеки, такими як системи виявлення вторгнень (IDS/IPS), системи запобігання витокам даних (DLP) або системи управління подіями і журналами (SIEM), для забезпечення комплексного захисту.

Системи миттєвого повідомлення та реагування на інциденти

Системи миттєвого повідомлення та реагування на інциденти (Incident Response and Instant Messaging Systems) - це інструменти, які використовуються для швидкого сповіщення та координації дій у випадку інцидентів безпеки або інших надзвичайних ситуацій. Вони грають важливу роль у реагуванні на загрози безпеки та мінімізації можливих наслідків. Ось кілька ключових характеристик і переваг таких систем:

1. Швидке сповіщення: Ці системи дозволяють швидко сповістити відповідні відділи чи особи про виявлення потенційної загрози або інциденту безпеки.

2. Координація дій: Вони допомагають забезпечити ефективну координацію дій між членами команди реагування на інциденти та іншими відповідальними особами.

3. Збір та обробка інформації: Системи можуть автоматично збирати та обробляти інформацію про інцидент, що допомагає аналізувати ситуацію та приймати відповідні рішення.

4. Підтримка комунікації: Вони надають засоби для ефективної комунікації між учасниками реагування на інциденти, включаючи можливість обміну повідомленнями, файлами та іншою інформацією.

5. Автоматизація процесів: Деякі системи можуть автоматизувати певні аспекти процесу реагування на інциденти, такі як реєстрація подій, розподіл завдань та виконання певних дій.

6. Аналіз та звітність: Вони дозволяють проводити аналіз інцидентів, визначати їхні причини та наслідки, а також створювати звіти для подальшого вдосконалення процесів безпеки.

2.1 Архітектура та компоненти рішення Cisco email security

Рішення Cisco Email Security - це комплексна платформа для захисту електронної пошти від різних загроз, таких як спам, фішинг, віруси, атаки з використанням вбудованих посилань та інші види загроз. Основні компоненти цього рішення включають наступне:

1. Cisco Email Security Appliance (ESA): Це апаратне або програмне забезпечення, яке відповідає за фільтрацію трафіку електронної пошти. Воно виявляє й блокує спам, фішингові атаки, віруси, а також провіряє вбудовані посилання та вкладення на предмет шкідливих або небезпечних вмістів.

2. Cisco Content Security Management Appliance (SMA): Це програмне забезпечення для керування рішенням Cisco Email Security. Воно дозволяє адміністраторам налаштовувати правила фільтрації, моніторити та аналізувати трафік електронної пошти, а також надає засоби для звітності.

3. Cisco Security Management Appliance (SMA): Це програмне забезпечення для керування безпекою, яке включає в себе інструменти для управління Cisco Email Security, а також іншими рішеннями безпеки від Cisco.

4. Cisco Security Intelligence Operations (SIO): Це сервіс, який забезпечує постійне оновлення бази даних інформації про загрози для рішення Cisco Email Security. Це дозволяє швидко реагувати на нові загрози та захищати користувачів від них.

5. Інтеграція з іншими продуктами Cisco: Рішення Cisco Email Security може інтегруватися з іншими продуктами безпеки від Cisco, такими як Cisco Advanced Malware Protection (AMP), для забезпечення більш широкого захисту від загроз.

Cisco Email Security Appliance (ESA)

Cisco Email Security Appliance (ESA) - це апаратне або програмне забезпечення, яке використовується для захисту і керування трафіком електронної пошти в організаціях. Основні функції ESA включають:

1. Фільтрація спаму і небажаних повідомлень: ESA виявляє і блокує спам, фішингові атаки, небажані повідомлення та інші форми небажаного трафіку електронної пошти.

2. Антивірусний захист: ESA виявляє і блокує віруси та інші шкідливі вкладення в електронних листах.

3. Аналіз та фільтрація контенту: ESA проводить аналіз тексту та вкладень електронної пошти для виявлення можливих загроз або небажаного вмісту.

4. Захист від витоку інформації: ESA може виявляти і блокувати відправку конфіденційної інформації через електронну пошту, щоб запобігти витоку даних.

5. Шифрування електронної пошти: ESA надає можливість шифрування електронних листів для забезпечення конфіденційності інформації.

6. Моніторинг та аналіз трафіку : ESA забезпечує інструменти для моніторингу та аналізу трафіку електронної пошти з метою виявлення несправностей, аналізу трендів та виявлення потенційних загроз.

Cisco Content Security Management Appliance (SMA)

Cisco Content Security Management Appliance (SMA) - це компонент інфраструктури безпеки електронної пошти, який відповідає за управління та моніторинг рішення безпеки пошти від Cisco. Основна мета SMA полягає в забезпеченні адміністраторам зручного і ефективного інтерфейсу для керування політиками безпеки, аналізу загроз та виявлення подій, пов'язаних з електронною поштою.

Основні функції та можливості Cisco SMA включають:

1. Управління політиками безпеки: SMA надає інтерфейс для налаштування та управління політиками безпеки електронної пошти. Це включає в себе встановлення правил фільтрації, керування списками блокування та дозволу, налаштування антивірусного сканування тощо.

2. Моніторинг та аналіз: SMA дозволяє адміністраторам моніторити потік поштових повідомлень, виявляти загрози, такі як спам, фішингові атаки, віруси, шкідливі вкладення тощо, та аналізувати їхні характеристики.

3. Автоматизована реакція на загрози: SMA може автоматично реагувати на виявлені загрози згідно з налаштованими правилами та політиками безпеки. Наприклад, відправляти повідомлення про блокування загроз, пересилати їх до систем інцидентного реагування або автоматично виконувати інші дії.

4. Звітність та аналітика: SMA надає інструменти для створення звітів про ефективність рішення безпеки електронної пошти, а також аналізу виявлених загроз та використання ресурсів.

5. Інтеграція з іншими системами: SMA може інтегруватися з іншими продуктами та системами безпеки для забезпечення цілісності та комплексності захисту корпоративної мережі.

Cisco Security Intelligence Operations (SIO)

Cisco Security Intelligence Operations (SIO) - це сервіс, який надається компанією Cisco і має на меті надання інформації про поточні загрози та вразливості у мережевих пристроях та програмному забезпеченні. Основна мета Cisco SIO - це забезпечити користувачів актуальною інформацією, яка допоможе їм вчасно реагувати на потенційні загрози та зменшити ризики безпеки мережі.

Основні характеристики та функціональність Cisco SIO включають:

1. Збір та аналіз інформації про загрози: Cisco SIO надає постійний моніторинг мережі та аналізує дані про виявлені загрози, включаючи нові види вірусів, шкідливе програмне забезпечення, вразливості систем і т. д.

2. Оновлення бази даних загроз: На основі зібраної інформації Cisco SIO оновлює базу даних загроз, що дозволяє користувачам мати доступ до актуальних даних про потенційні небезпеки.

3. Виявлення та блокування загроз: На основі інформації від Cisco SIO, безпекові продукти та рішення Cisco можуть виявляти та блокувати потенційні загрози автоматично або за допомогою конфігурацій користувачів.

4. Постійне оновлення: Cisco SIO працює постійно, щоб надати користувачам найновішу інформацію про загрози та вразливості. Це дозволяє підтримувати високий рівень безпеки мережі в реальному часі.

5. Інтеграція з іншими продуктами Cisco: Cisco SIO інтегрується з іншими продуктами та рішеннями безпеки Cisco, що дозволяє створювати цілісні та комплексні захисні стратегії.

2.2 Призначення та основні функції компонентів Cisco email security(ESA)

Cisco Email Security Appliance (ESA)

Cisco Email Security Appliance (ESA) - це апаратне або програмне забезпечення, яке використовується для захисту і керування трафіком електронної пошти в організаціях. Основні функції ESA включають:

1. Фільтрація спаму і небажаних повідомлень: ESA виявляє і блокує спам, фішингові атаки, небажані повідомлення та інші форми небажаного трафіку електронної пошти.

2. Антивірусний захист: ESA виявляє і блокує віруси та інші шкідливі вкладення в електронних листах.

3. Аналіз та фільтрація контенту: ESA проводить аналіз тексту та вкладень електронної пошти для виявлення можливих загроз або небажаного вмісту.

4. Захист від витоку інформації: ESA може виявляти і блокувати відправку конфіденційної інформації через електронну пошту, щоб запобігти витоку даних.

5. Шифрування електронної пошти: ESA надає можливість шифрування електронних листів для забезпечення конфіденційності інформації.

6. Захист від фішингу: ESA надає широкий спектр заходів для захисту від фішингу, який є однією з найпоширеніших загроз через електронну пошту.

Фільтрація спаму і небажаних повідомлень: ESA

Фільтрація спаму і небажаних повідомлень є однією з основних функцій Cisco Email Security Appliance (ESA). Ця функція включає в себе ряд технологій і методів, які допомагають виявляти та блокувати небажаний трафік електронної пошти перед тим, як він потрапить до поштової скриньки користувача. Основні аспекти фільтрації спаму і небажаних повідомлень в ESA включають наступне:

1. Сигнатурний аналіз: ESA використовує базу даних з відомими сигнатурами спаму і шкідливих вірусів для виявлення відомих видів небажаної пошти.

2. Машинне навчання і інтелектуальні алгоритми: ESA використовує методи машинного навчання для аналізу характеристик повідомлень та ідентифікації небажаної пошти на основі великої кількості показників.

3. Аналіз заголовків і вмісту повідомлень: ESA аналізує заголовки та вміст електронних листів для виявлення підозрілих або небажаних елементів, таких як неправильно сформовані заголовки, небажані слова або фрази, або шкідливі вкладення.

4. Перевірка IP-адрес і доменів відправників: ESA перевіряє IP-адреси та домени відправників на предмет включення до чорних списків спаму або відомих джерел небажаних повідомлень.

5. Блокування спам-ботів і зловмисних мереж: ESA виявляє та блокує повідомлення від комп'ютерів, які можуть бути зражені спам-ботами або які діють в якості зловмисних серверів.

Мал.2.2.1

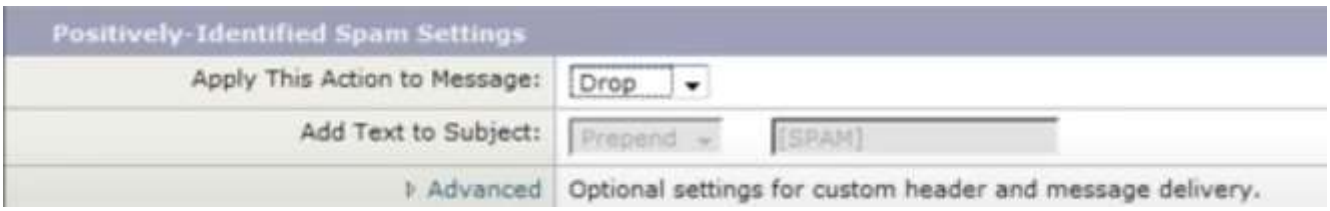
Для налаштування політик вхідних листів переходимо в розділ політики пошти (Mail Policies).

Мал.2.2.2

В розділі (Default Policies) переходимо за гіперпосиланням для налаштування політик фільтрації спаму та небажаних повідомлень.

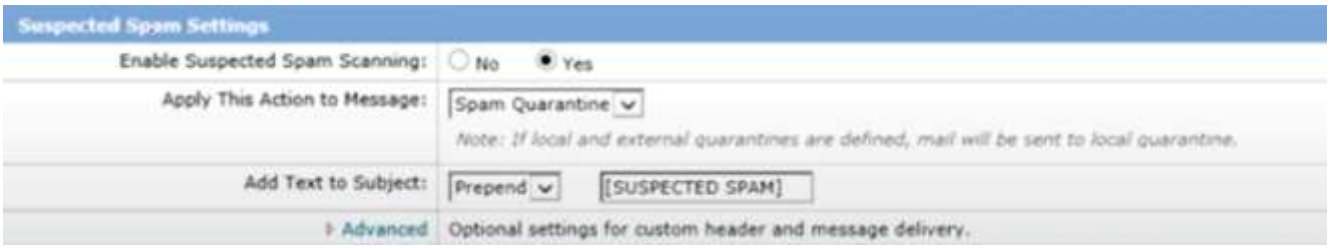
Мал.2.2.3

Вмикаємо (IronPort Anti-spam)



Мал2.2.4

Налаштовуємо дії для ідентифікованого спаму.



Мал.5

Налаштовуємо дії відносно повідомлень які підозрюються на спам.

Мал.2.2.6

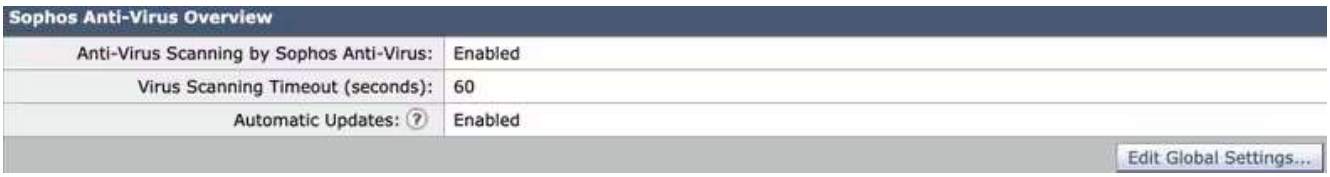
Результат налаштувань політик вхідних листів.

Антивірусний захист: ESA

Антивірусний захист є важливою складовою функціоналу Cisco Email Security Appliance (ESA), оскільки він спрямований на виявлення і блокування вірусів, троянів та інших шкідливих програм, які можуть надходити в електронних листах. Основні аспекти антивірусного захисту в ESA включають:

1. Сканування вкладень: ESA автоматично сканує вкладення в електронних листах на предмет наявності вірусів або інших шкідливих програм. Він виявляє і блокує вкладення, які містять відомі вірусні сигнатури або характеристики шкідливих файлів.
2. Хмарне антивірусне сканування: ESA може використовувати хмарні технології для перевірки вкладень на віруси з використанням централізованих антивірусних баз даних, що оновлюються в реальному часі.
3. Аналіз поведінки файлів: ESA використовує аналіз характеристик і поведінки файлів для виявлення вірусів, які можуть обхіднути стандартні сигнатурні методи виявлення.
4. Оновлення вірусних визначень: ESA регулярно оновлює свої вірусні визначення і сигнатури для забезпечення захисту від нових вірусів та інших шкідливих програм.

5. Інтеграція з іншими антивірусними рішеннями: ESA може інтегруватися з іншими системами антивірусного захисту, такими як Cisco Advanced Malware Protection (AMP), для забезпечення додаткового рівня безпеки.

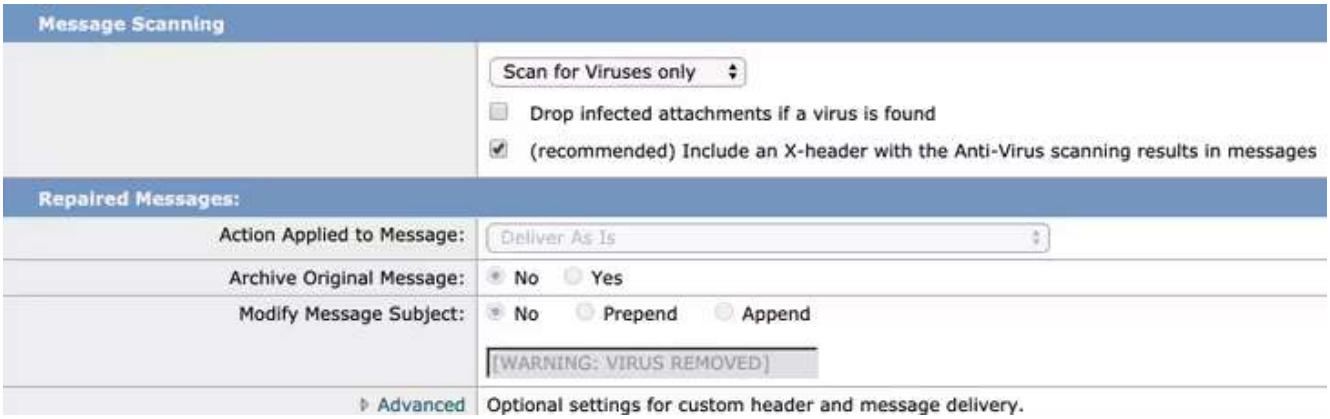


Мал 2.2.7

Перейдимо до Служби безпеки> Антивірус - Sophos

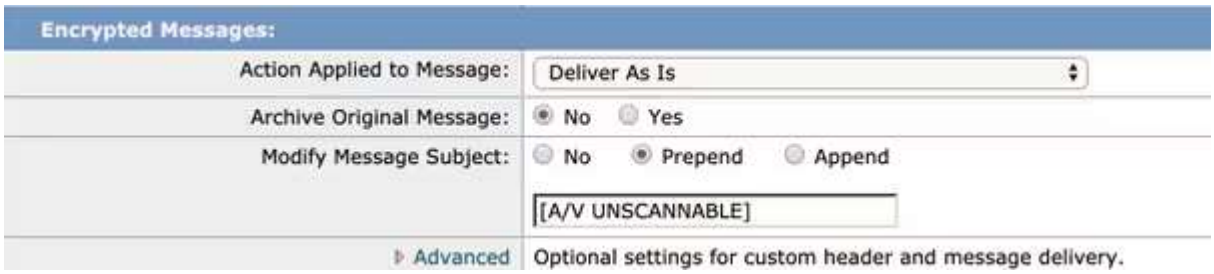
Мал. 2.2.8

Вмикаємо антивірусне сканування для цих політик.



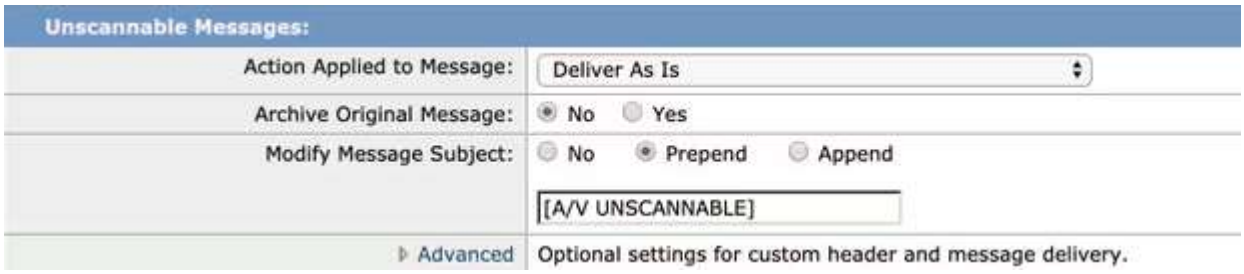
Мал. 2.2.9

Ми не намагаємося виправити файл, тому сканування повідомлень залишається лише скануванням на наявність вірусів.



Мал. 2.2.10

Рекомендована дія як для зашифрованих, так і для повідомлень, які не підлягають скануванню, полягає в доставці як є зі зміненою темою для їхньої уваги.



Мал. 2.2.11

Рекомендованою політикою для антивірусу є видалення всіх заражених вірусами повідомлень, як показано на зображенні нижче.

Мал. 2.2.12

Далі зберігаємо зміни внесені в політики антивірусного сканування.

Захист від витоку інформації: ESA

Захист від витоку інформації є важливою складовою функціоналу Cisco Email Security Appliance (ESA). Ця функція спрямована на запобігання ненавмисногої передачі конфіденційної інформації через електронну пошту. Основні аспекти захисту від витоку інформації в ESA включають:

1. Класифікація даних: ESA може аналізувати вміст електронних повідомлень для ідентифікації чутливої інформації, такої як фінансові дані, медична інформація, особиста інформація тощо.
2. Політики захисту даних: Адміністратори можуть налаштовувати політики

захисту даних, які визначають, як обробляти повідомлення, що містять чутливу інформацію. Ці політики можуть включати блокування, шифрування або маскування інформації перед її відправленням.

3. Запобігання витоку даних через електронну пошту: ESA може блокувати відправку електронних листів, які містять чутливу інформацію, на зовнішні адреси або недозволені канали комунікації, щоб запобігти витоку даних.

4. Аудит і звітність: ESA може вести журнали подій та забезпечувати звіти про використання електронної пошти для передачі чутливої інформації, що допомагає виявляти можливі витоки даних і вживати відповідних заходів для їх запобігання.

5. Інтеграція з системами захисту даних: ESA може інтегруватися з іншими системами захисту даних, такими як системи захисту від витоку даних (DLP), для забезпечення комплексного захисту інформації в організації.

Захист від витоку інформації (Data Loss Prevention, DLP) є важливою складовою функціоналу Cisco Email Security Appliance (ESA). Ця функція спрямована на запобігання ненавмисного витоку конфіденційної інформації через електронну пошту. Основні аспекти захисту від витоку інформації в ESA включають:

1. Ідентифікація конфіденційної інформації: ESA може аналізувати вміст електронних повідомлень для ідентифікації чутливої інформації, такої як фінансові дані, особиста інформація, медична інформація тощо.

2. Використання політик безпеки: Адміністратори можуть налаштовувати політики безпеки, що визначають дії з повідомленнями, які містять чутливу інформацію. Ці політики можуть включати блокування, шифрування або маскування інформації перед відправленням.

3. Блокування небажаних витоків даних: ESA може блокувати відправку електронних листів, які містять чутливу інформацію, на зовнішні адреси або недозволені канали комунікації, щоб запобігти витоку даних.

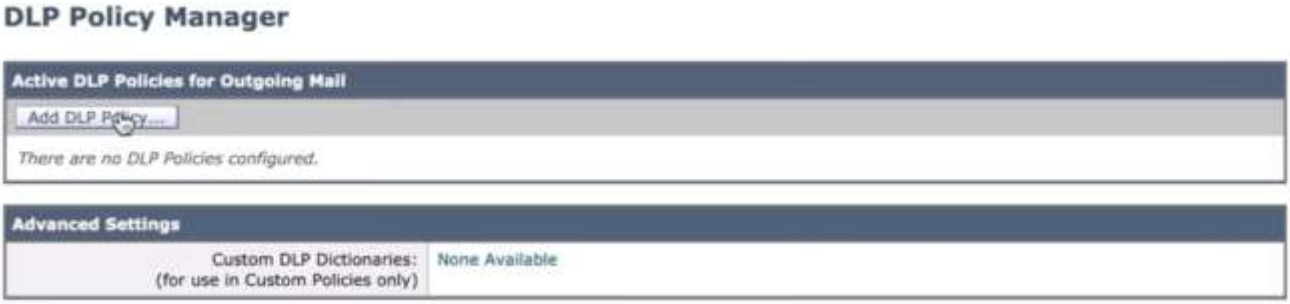
4. Аудит і звітність: ESA веде журнали подій та надає звіти про використання електронної пошти для передачі чутливої інформації. Це допомагає виявляти можливі витоки даних і вживати відповідних заходів для їх запобігання.

5. Інтеграція з іншими системами DLP: ESA може інтегруватися з іншими

системами захисту від витоку даних для забезпечення комплексного захисту інформації в організації.

Мал. 2.2.13

Переходимо до розділу (DLP Policy Manager)

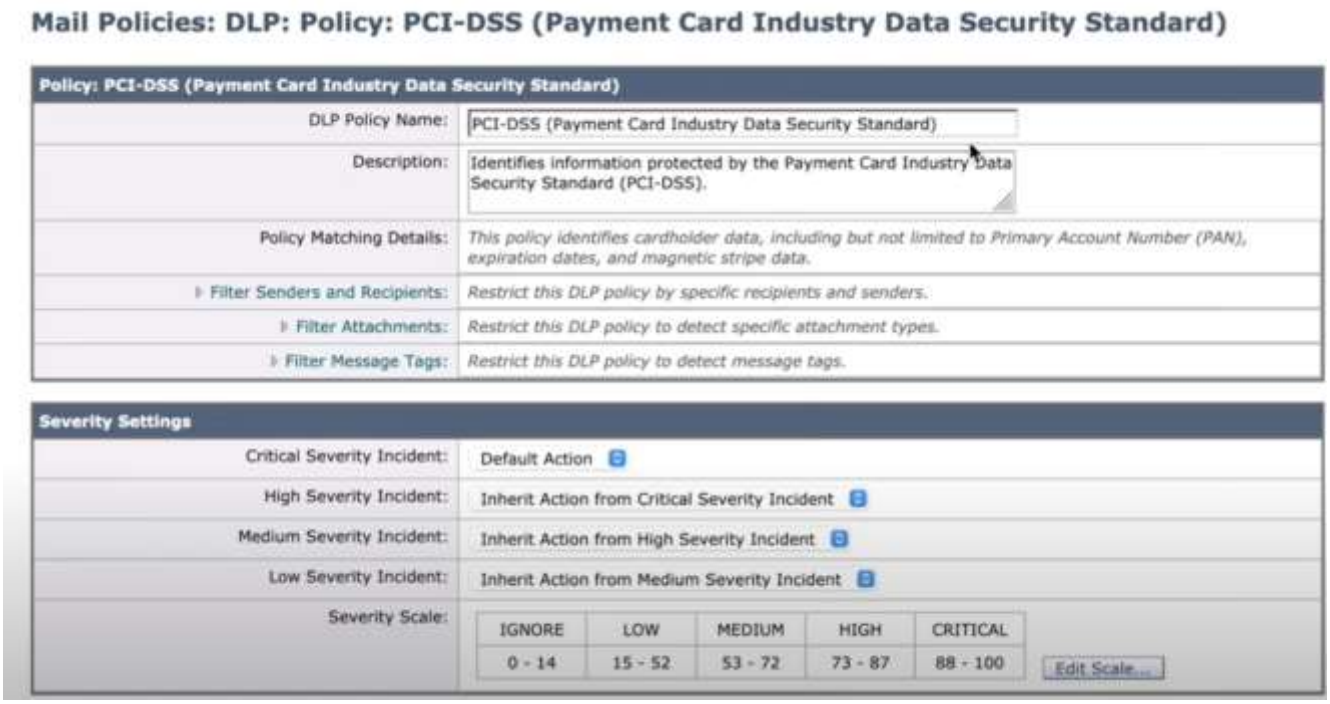


Мал. 2.2.14

Створюємо нові політики для витоку інформації.

Мал. 2.2.15

Обираємо потрібні нам політики та переходимо до їх налаштувань.



Мал. 2.2.16

Налаштовуємо обрані нам політики відподно до наших вимог.

Мал. 2.2.17

Створені політики витоку інформації.

Мал. 2.2.18

Переходимо до налаштуванб політик пошти та вмикаємо потрібні нам політики витоку інформації.

Захист від фішингу

Cisco Email Security Appliance (ESA) надає широкий спектр заходів для захисту від фішингу, який є однією з найпоширеніших загроз через електронну пошту. Ось деякі засоби та функції, які ESA використовує для боротьби з фішингом:

1. Аналіз вмісту повідомлень: ESA аналізує вміст електронних повідомлень, виявляючи характеристики, які можуть свідчити про фішингову спробу. Це може включати перевірку наявності підроблених або підозрілих веб-адрес, запитів конфіденційної інформації тощо.
2. Перевірка доменних імен: ESA використовує механізми перевірки доменних імен для виявлення фішингових доменів або доменів, що намагаються імітувати

легітимні веб-сайти.

3. Використання спеціалізованих баз даних: ESA використовує бази даних відомих фішингових сайтів та доменів для виявлення та блокування фішингових атак.

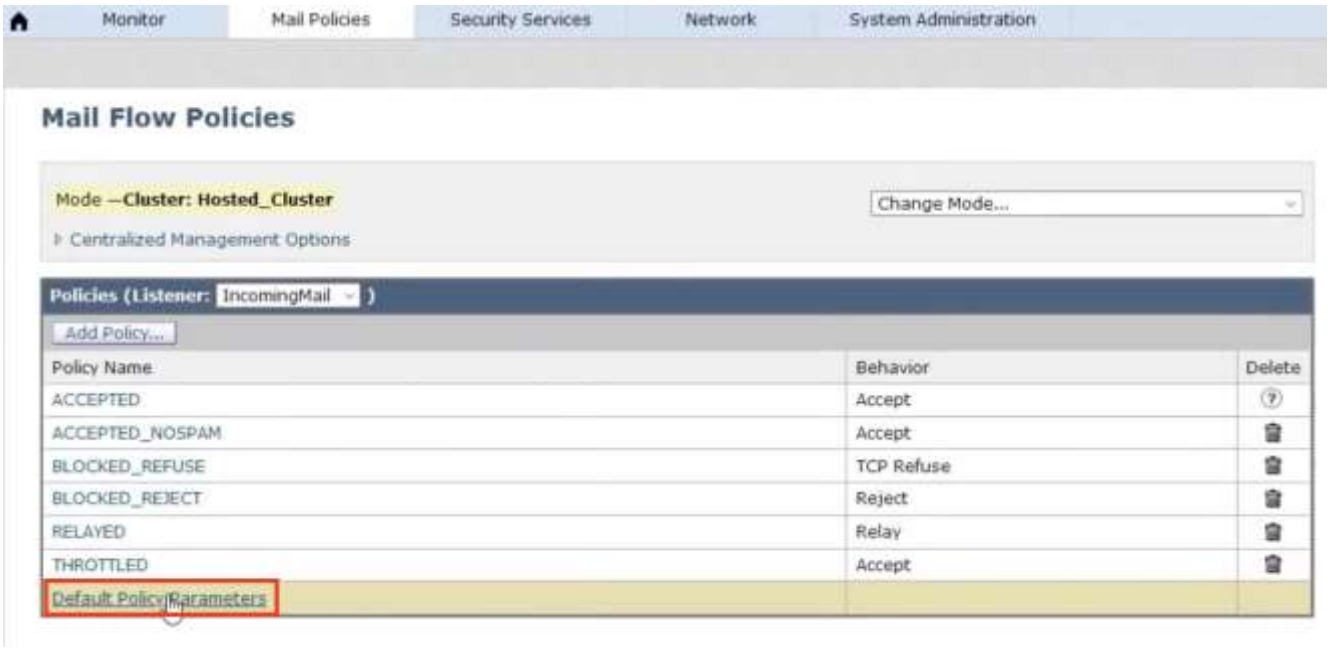
4. Механізми машинного навчання та аналізу поведінки: ESA може використовувати розумові алгоритми для виявлення непередбачуваних патернів у фішингових атаках, що дозволяє вчасно реагувати на нові загрози.

5. Шифрування та аутентифікація: ESA може застосовувати методи шифрування та аутентифікації, щоб запобігти витоку конфіденційної інформації та захистити користувачів від фішингових атак.

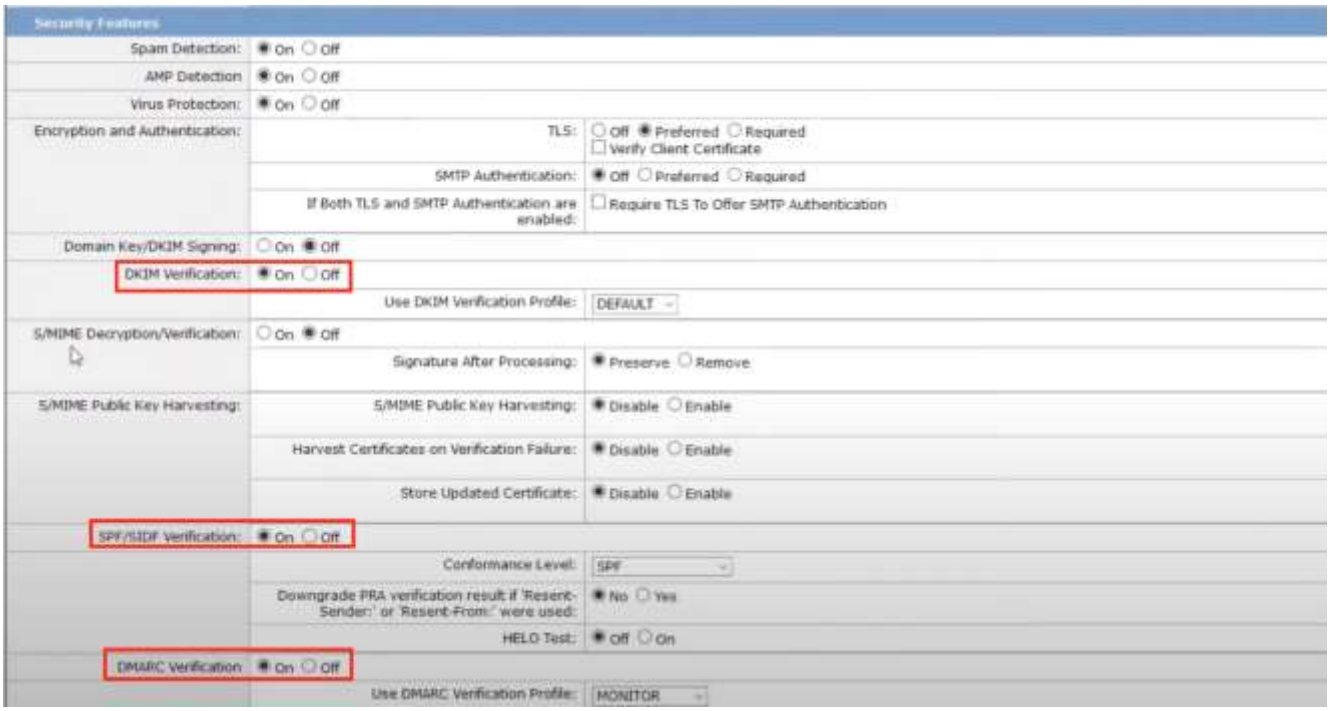
6. Оновлення та інтелектуальні оновлення: Cisco постійно оновлює бази даних та алгоритми захисту, щоб ESA був ефективним проти нових типів фішингових загроз.

Мал. 2.2.19

Для ефективного викростання захисту від вішингу на базі ESA спочатку налаштуємо політики фільтрації пошти.

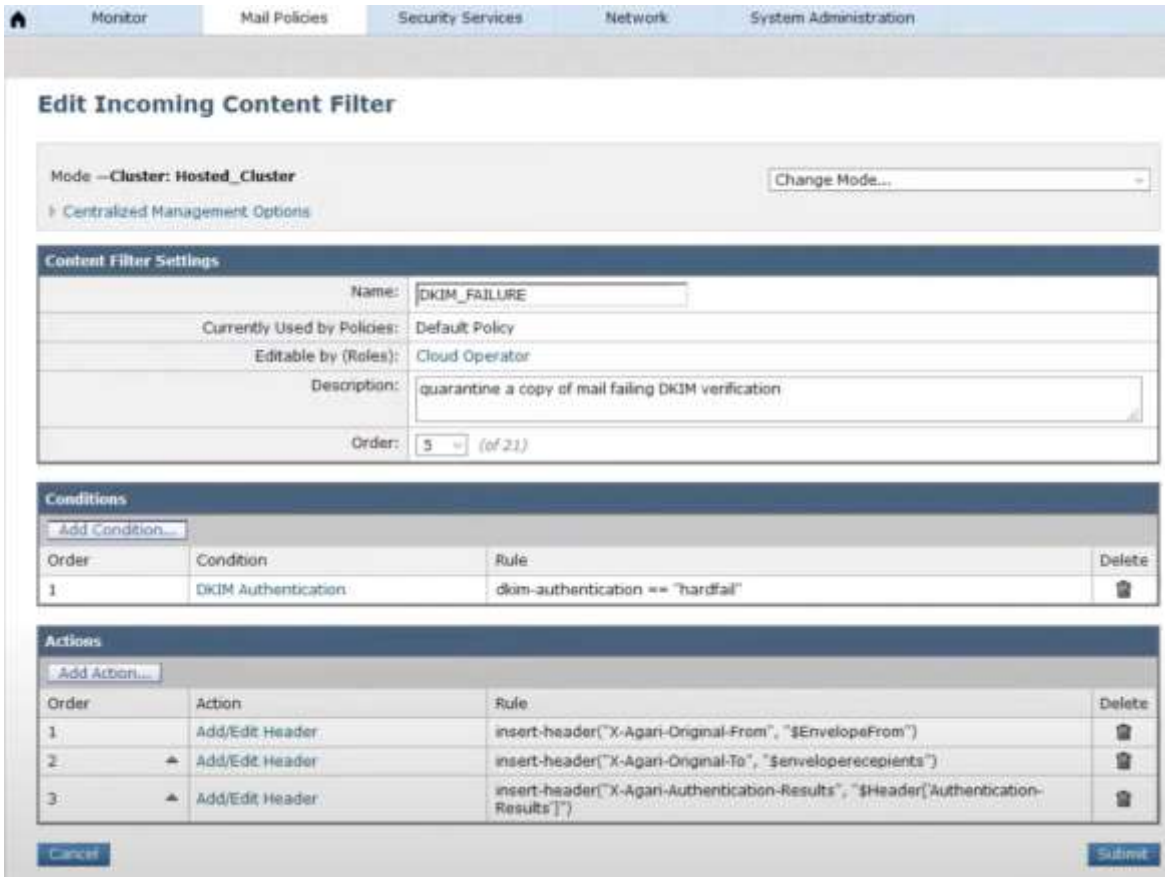


Мал. 2.2.20



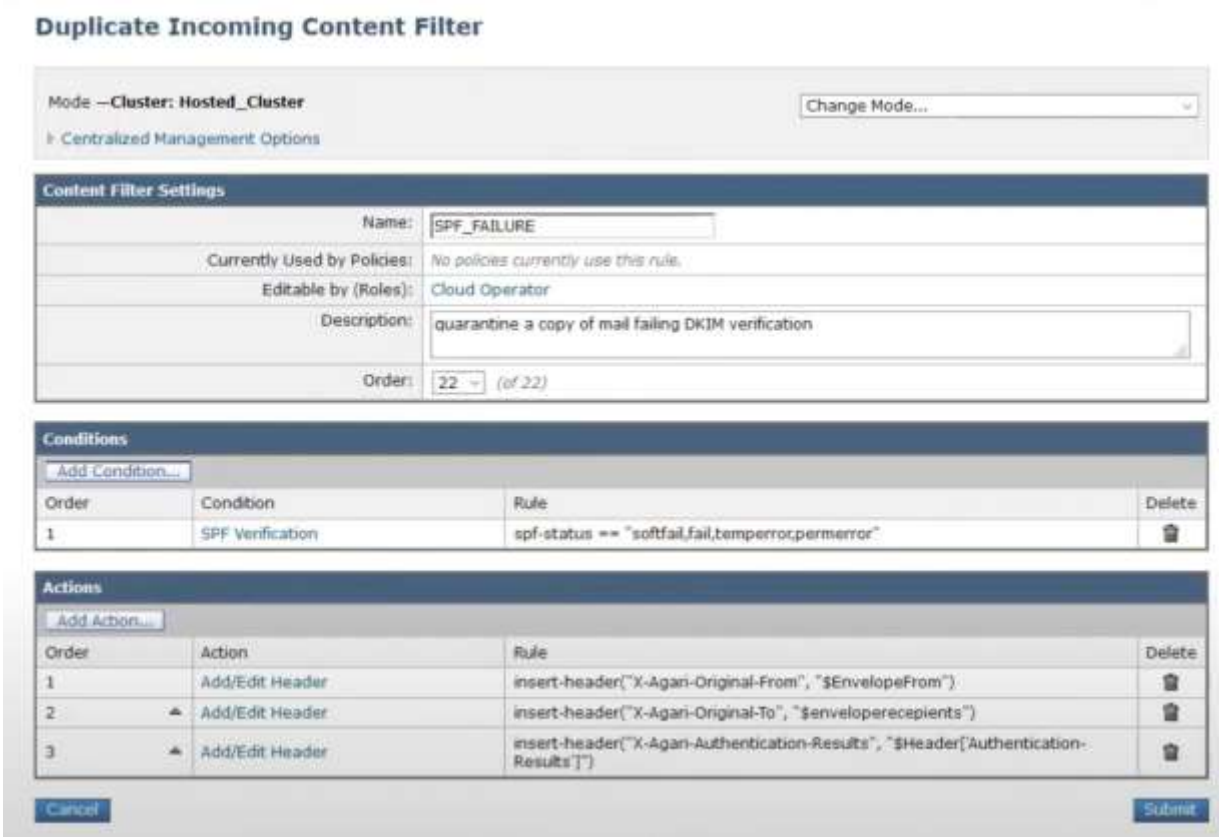
Мал. 2.2.21

В розділі функій безпеки вмакаємо (DKIM Verification) , (SPF/SIDF Verification) та (DMARC Verification)



Мал. 2.2.21

Далі налаштовуємо потрібні нам фільтри відповідно до наших вимог.



Мал. 2.2.22

Мал. 2.2.23

Далі в розділі засобів безпеки переходимо до налаштувань (Advanced Phishing Protection)

Мал. 2.2.24

Вмикаємо фунцію Advanced Phishing Protection

Мал. 2.2.25

Після ввімкення функції просунутого захисту від фішингу переходимо до його детального налаштування відпоавідно на наших вимог.

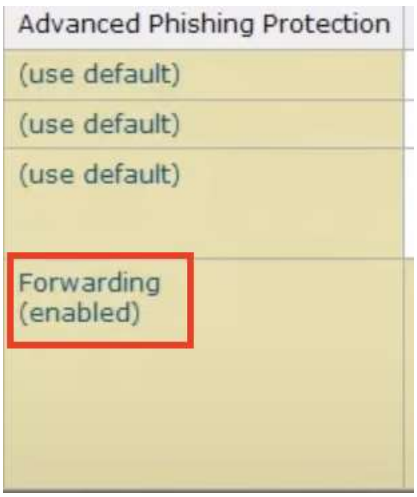
Мал. 2.2.26

Потім переходимо до налаштуваннь політик пошти та вмикаємо функцію захисту від фішингових атак.

Мал. 2.2.27

Обираємо потрібні нам налаштування та підтвержуємо їх.

Мал. 2.2.28



2.2.29

Уввімкнена функція просунутого захисту від фішингових атак в політиках пошти.

3.1 Варіант розгортання системи захисту внутрішніх листуваннь на базі Cisco email security

Розгортання системи захисту внутрішніх листувань на базі Cisco Email Security Appliance може бути досить ефективним для захисту внутрішніх корпоративних комунікацій від різних загроз. Ось кілька кроків та варіантів розгортання для цієї системи:

1. Аналіз внутрішніх листів: Cisco Email Security Appliance може бути налаштований для моніторингу та аналізу внутрішніх електронних повідомлень. Це включає в себе виявлення спаму, вірусів, фішингових атак та інших загроз, які можуть надходити між користувачами внутрішньої мережі.
2. Контроль за вкладеннями та URL-адресами: Cisco ESA може сканувати вкладення та URL-адреси відправлених листів для виявлення шкідливого вмісту або посилань на фішингові веб-сайти.
3. Шифрування внутрішніх листів: Для захисту конфіденційної інформації, внутрішні листи можуть бути шифровані за допомогою Cisco ESA, щоб запобігти доступу до них з боку неповинних осіб.
4. Управління політиками безпеки: Адміністратори можуть налаштовувати різні політики безпеки для внутрішніх листів, включаючи фільтрацію спаму, блокування певних типів вкладень, встановлення правил пересилання тощо.
5. Моніторинг та звітність: Cisco ESA надає можливості моніторингу та звітності про внутрішні листи, що дозволяє адміністраторам відстежувати потенційні загрози та виявляти ненормативну поведінку користувачів.
6. Інтеграція з іншими системами безпеки: Cisco ESA може бути інтегрований з іншими системами безпеки для створення цілісної захисної архітектури в організації.

Аналіз внутрішніх листів

Аналіз внутрішніх листів може бути важливим етапом у забезпеченні безпеки корпоративної мережі та захисті від внутрішніх загроз. Ось деякі аспекти аналізу внутрішніх листів:

1. Виявлення шкідливих вкладень: Аналізатор електронних повідомлень може

сканувати вкладення в листах, щоб виявити наявність шкідливих програм або файлів. Це може включати в себе аналіз файлових типів, сигнатурний аналіз та аналіз вмісту для виявлення потенційно небезпечних вкладень.

2. Перевірка URL-адрес: Аналізатор може також сканувати URL-адреси, включені в текст листів, для виявлення посилань на шкідливі або фішингові веб-сайти. Це може допомогти запобігти користувачам переходити на шкідливі сторінки та стати жертвами атак.

3. Фільтрація конфіденційної інформації: Аналіз внутрішніх листів може включати також фільтрацію конфіденційної інформації, такої як особисті дані клієнтів, фінансова інформація тощо. Це допомагає захистити конфіденційні дані від витоку через електронну пошту.

4. Виявлення аномальної поведінки: Аналізатор може моніторити поведінку користувачів та виявляти аномальні або ненормативні активності, які можуть свідчити про потенційні загрози або вразливості.

5. Захист від витоку інформації: Аналіз внутрішніх листів може також включати заходи для захисту від витоку конфіденційної інформації. Це може бути реалізовано через шифрування електронної пошти, фільтрацію аташированих документів тощо.

6. Аудит та звітність: Аналіз внутрішніх листів також може включати створення аудиторських журналів та звітів про активність користувачів та виявлені загрози. Це допомагає адміністраторам відстежувати події та приймати відповідні заходи.

Управління політиками безпеки

Управління політиками безпеки включає в себе визначення, налаштування та контроль за правилами та процедурами, які визначають рівень безпеки в організації. Для ефективного управління політиками безпеки, включаючи захист

електронної пошти, використовуються різні інструменти та підходи. Ось деякі ключові аспекти управління політиками безпеки:

1. Визначення вимог безпеки: Перший крок - визначення конкретних вимог та потреб безпеки для вашої організації. Це може включати в себе визначення дозволених та заборонених дій, встановлення рівня доступу до ресурсів, захист конфіденційної інформації тощо.
2. Розробка політик безпеки: На основі визначених вимог розробляються конкретні політики безпеки, які визначають стандарти та процедури для досягнення цих вимог. Це може включати в себе політики в області електронної пошти, доступу до мережі, аутентифікації користувачів, зберігання даних тощо.
3. Налаштування та впровадження: Після розробки політик вони налаштовуються та впроваджуються в системах безпеки. Це може включати в себе конфігурацію мережевих пристроїв, застосунків безпеки, систем реєстрації та моніторингу тощо.
4. Моніторинг та аналіз виконання: Після впровадження політик важливо постійно моніторити їхнє виконання та ефективність. Це включає в себе аналіз журналів подій, збирання статистики та звітності про відповідність політикам безпеки.
5. Оновлення та оптимізація: Політики безпеки повинні бути регулярно оновлювані та оптимізовані для врахування змін у загрозах, технологіях та вимогах організації. Це може включати в себе внесення змін до політик, удосконалення процесів та впровадження нових заходів безпеки.

Інтеграція з іншими системами безпеки

Інтеграція з іншими системами безпеки є важливим аспектом створення комплексного захисту інформації та мережі в організації. Для інтеграції Cisco Email Security Appliance з іншими системами безпеки можна використовувати різні методи та протоколи, залежно від конкретних потреб та можливостей системи. Ось кілька способів, які можна використовувати для інтеграції:

1. API і веб-служби: Багато систем безпеки, включаючи Cisco Email Security Appliance, надають API або веб-служби для взаємодії з іншими системами. Це

дозволяє автоматизувати інтеграцію та обмін даними між системами безпеки, такими як моніторинг, реагування на події та взаємодія з іншими захисними рішеннями.

2. Централізована система керування: Деякі організації використовують централізовані системи керування для управління різними захисними рішеннями, включаючи Cisco Email Security Appliance. Це дозволяє забезпечити єдиний пункт управління та моніторингу безпекою всієї мережі.

3. Інтеграція журналів подій: Інтеграція журналів подій дозволяє аналізувати дані з Cisco ESA разом з даними з інших систем безпеки для виявлення та реагування на загрози.

4. Інтеграція з системами аналізу вразливостей: Інтеграція Cisco ESA з системами аналізу вразливостей дозволяє автоматично виявляти та реагувати на потенційні вразливості, що можуть використовуватися для атак через електронну пошту.

5. Інтеграція з системами управління ідентифікацією та доступом: Інтеграція з системами управління ідентифікацією та доступом дозволяє забезпечити контроль доступу до електронної пошти та ідентифікацію користувачів для підвищення безпеки.

Це лише загальні кроки та варіанти розгортання системи захисту внутрішніх листувань на базі Cisco Email Security Appliance. Реальні налаштування будуть залежати від конкретних потреб та вимог організації.

3.2 Рекомендації щодо застосування методів та засобів захисту від атак з використанням соціальної інженерії

Захист від атак з використанням соціальної інженерії важливий для забезпечення безпеки організації, оскільки ці атаки часто використовуються для обману користувачів та отримання несанкціонованого доступу до конфіденційної інформації. Ось деякі рекомендації щодо застосування методів та засобів захисту від атак з використанням соціальної інженерії:

1. Навчання персоналу: Однією з ключових стратегій захисту є навчання персоналу. Важливо навчити співробітників розпізнавати ознаки соціально-інженерної атаки, такі як надмірний тиск на швидке прийняття рішення, прохання про конфіденційну інформацію через електронну пошту тощо.

2. Використання антивірусного та антифішингового програмного забезпечення: Застосування антивірусного та антифішингового програмного забезпечення може допомогти виявити та блокувати спроби соціально-інженерних атак через електронну пошту або веб-сайти.

3. Моніторинг активності користувачів: Важливо встановити системи моніторингу активності користувачів, щоб виявляти ненормативну або підозрілу поведінку, яка може свідчити про соціально-інженерні атаки.

4. Створення сильних паролів та багатофакторної аутентифікації: Використання сильних паролів та багатофакторної аутентифікації допоможе запобігти незаконному доступу до облікових записів користувачів, який може бути отриманий шляхом соціально-інженерних методів.

5. Актуалізація політик безпеки: Важливо постійно оновлювати політики безпеки організації з урахуванням нових загроз та методів соціальної інженерії.

6. Шифрування даних та комунікацій: Використання шифрування даних та комунікацій може допомогти захистити конфіденційну інформацію від перехоплення соціальними інженерами.

7. Перевірка безпеки інфраструктури: Регулярна перевірка безпеки інфраструктури на наявність вразливостей та підозрілі активності може допомогти вчасно виявити та запобігти соціально-інженерним атакам.

Ці рекомендації можуть допомогти організаціям ефективно захиститися від атак з використанням соціальної інженерії, зменшуючи ризики для безпеки та конфіденційності даних.

Висновки

В даній роботі було досліджено проблему атак з викростанням соціальної інженерії.Розкрито проблему захисту внутрішніх листуваннь та електронних зв’язків.Розроблено та продемнстровано приклад налаштування системи захисту внутрішніх листувань на базі Cisco email security (ESA).Також були показані методи та заходи створення політик так їх налаштування відповідно до поставлених задач по захисту корпоративних листувань.Проблема атак з використанням соціальної інженерії залишається актуальною та продовжує розвиватись тому компонування та інтеграція інших програмних заходів може підвищи якість захисту систем та підвищить загальний рівень безпеки компанії.

Список використаних джерел

1. https://nadiyno.org/shho-take-soczialna-inzheneriya/
2. 2. https://www.eset.com/ua/support/information/entsiklopediya-ugroz/sotsialnaya-inzheneriya/
3. https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing
4. https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/
5. https://cert.gov.ua/articles/2
6. https://am-bits.com/en/2019/04/22/cisco-email-security-appliance-esa-4
7. https://www.smart-planet.com.ua/protect-from-phishing-attacks/
8. https://support.microsoft.com/uk-ua/windows/%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82-%D0%B2%D1%96%D0%B4-%D1%84%D1%96%D1%88%D0%B8%D0%BD%D0%B3%D1%83-0c7ea947-ba98-3bd9-7184-430e1f860a44
9. https://www.eset.com/ua/support/information/entsiklopediya-ugroz/antifishing/
10. https://hackyourmom.com/kibervijna/shho-take-soczialna-inzheneriya-napady-metody-ta-zapobigannya/
11. https://hackyourmom.com/kibervijna/instrumenty-yaki-vykorystovuyutsya-dlya-fishyngovyh-atak/
12. https://hackyourmom.com/kibervijna/golosovyj-fishyng/
13. https://hackyourmom.com/kibervijna/shho-take-spear-phishing-ta-yak-vid-nogo-zahystytysya/
14. https://hackyourmom.com/kibervijna/%e2%84%968-haking-u-praktychnomu-zastosuvanni-ta-soczialna-inzheneriya-zahyst-vid-soczialnoyi-inzheneriyi/
15. https://hackyourmom.com/servisy/%e2%84%966-ethical-hacking-labs-soczialna-inzheneriya/