ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ЗАХИСТУ WEB-РЕСУРСІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ»

на здобуття освітнього ступеня магістра

зі спеціальності _____125_Кібербезпека_____

(код, найменування спеціальності)

освітньо-професійної програми_Інформаційна та кібернетична безпека____

(назва)

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

_____ ЧЕРНЕГА Станіслав

Виконав: здобувач вищої освіти групи БСДМ-63

ЧЕРНЕГА Станіслав

(ПРІЗВИЩЕ, ім'я)

Керівник
к.т.н, доцент БОРСУКОВСЬКИЙ Юрій

(ПРІЗВИЩЕ, ім'я)

Рецензент Туровський О. Л.

(ПРІЗВИЩЕ, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки

Ступінь вищої освіти Магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____Гайдур Г.І
«___»_____2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Чернеги Станіслава Олександровича
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: «Технологія забезпечення безпеки та захисту Web-ресурсів в інформаційній системі організації»

керівник кваліфікаційної роботи БОРСУКОВСЬКИЙ Юрій, к.т.н, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи

1) Нормативно-правові акти та стандарти в сфері інформаційної безпеки;

2) Рішення Trend Micro Web App Security;

3) Наукова та технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1) Аналіз особливостей використання та регулювання Web-ресурсів;

2) Дослідження технічних та програмних рішень для посилення безпеки web-ресурсів в організації;

3) Дослідження інтеграції рішень для забезпечення безпеки Web-ресурсів.

5. Перелік ілюстративного матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Аналіз науково-технічної літератури	28.10.2023 р.	виконано
2.	Аналіз особливостей використання та регулювання Web-ресурсів	11.11.2023 р.	виконано
3.	Аналіз нормативно-правових актів та стандартів в сфері інформаційної безпеки, які здійснюють регулювання веб-ресурсів	14.11.2023 р.	виконано
4.	Дослідження категорій вразливостей веб-ресурсів	18.11.2023 р.	виконано
5.	Дослідження технічних та програмних рішень для посилення безпеки web-ресурсів в організації	20.11.2023 р.	виконано
6.	Інтеграція рішень для забезпечення безпеки Web-ресурсів	11.12.2023 р.	виконано
7.	Рекомендації до налаштувань Trend Micro	12.12.2023 р.	виконано
8.	Реферат, вступ, висновки	10.12.2023 р.	виконано
9.	Підготовка презентації	14.12.2023 р.	виконано

Здобувач вищої освіти _____ Станіслав ЧЕРНЕГА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 68 сторінок, 44 рисунків, 27 джерел.

Об'єкт дослідження – процес безпечного функціонування Web-ресурсів.

Предмет дослідження – технології та засоби забезпечення безпеки Web-ресурсів в інформаційній системі організації.

Мета роботи – підвищення рівня інформаційної безпеки в організації шляхом впровадженню технічних та програмних рішень для посилення безпеки Web-ресурсів.

Методи дослідження – теорія інформації, міжнародні та вітчизняні стандарти у сфері кібербезпеки, політики безпеки.

В роботі проаналізовано важливість захисту веб-ресурсів. Проведено аналіз нормативно-правових актів України щодо інформаційної безпеки, що регулюють використання та захист веб-ресурсів. Виокремлено необхідність комплексного підходу до захисту веб-інфраструктури.

Досліджено використання AWS для захисту веб-ресурсів. Зазначено, що AWS Security Hub є ключовим інструментом для перевірки відповідності стандартам безпеки, інтегруючи дані з різних AWS служб.

Оцінено важливість створення та налаштування груп веб-додатків у Deep Security з метою підвищення захисту веб-ресурсів через управління групами веб-додатків із різними адміністративними правами. Розроблено рекомендації щодо захисту веб-ресурсів через налаштування Trend Micro, включаючи пересилання журналів Cloud Syslog, аутентифікацію Okta та Microsoft Entra ID, віртуальні шлюзи, контроль пропускної здатності, звіти, файли PAC, і налаштування каталогових служб.

Галузь використання – кібербезпека.

WEB, РЕСУРСИ, ДОДАТКИ, ЗАХИСТ, ВРАЗЛИВІСТЬ, ЗАГРОЗА, ФАЄРВОЛ, SQL, AWS SECURITY HUB, TREND MICRO, CLOUD SYSLOG, DEEP SECURITY, БЕЗПЕКА, ОРГАНІЗАЦІЯ, OWASP TOP 10.

ABSTRACT

Qualification’s thesis: 68 pages, 44 figures, 27 sources.

The object of research – the process of safe functioning of Web resources.

The subject of research – technologies and means of ensuring the security of Web resources in an organization's information system.

The aim of research is to increase the level of information security in the organization by implementing technical and software solutions to enhance the security of Web resources.

Research methods – information theory, international and domestic standards in the field of cybersecurity, security policies.

The work analyzes the importance of protecting web resources. An analysis of Ukrainian normative legal acts regarding information security, which regulate the use and protection of web resources, has been conducted. The need for a comprehensive approach to protecting web infrastructure has been identified.

The use of AWS for the protection of web resources has been studied. It is noted that AWS Security Hub is a key tool for compliance with security standards, integrating data from various AWS services. The importance of creating and configuring web application groups in Deep Security to enhance web resource protection through the management of web application groups with different administrative rights is assessed.

Recommendations have been developed for protecting web resources through the configuration of Trend Micro, including forwarding Cloud Syslog logs, Okta and Microsoft Entra ID authentication, virtual gateways, bandwidth control, reports, PAC files, and directory services settings.

Field of use – cybersecurity.

WEB, RESOURCES, APPLICATIONS, PROTECTION, VULNERABILITY, THREAT, FIREWALL, SQL, AWS SECURITY HUB, TREND MICRO, CLOUD SYSLOG, DEEP SECURITY, SECURITY, ORGANIZATION, OWASP TOP 10.

ЗМІСТ

ВСТУП

Актуальність дослідження. З кожним роком все більше організацій використовують веб-технології для підвищення ефективності та привабливості для нових клієнтів. Це стосується як комерційних компаній, так і установ державного та місцевого управління. Хоча інтернет-сервіси пропонують чимало переваг, вони також підвищують ризики кібератак.

Веб-ресурси можуть включати веб-сайти, веб-додатки, інтернет-портали, хмарні сервіси тощо. Вони надають зручний інтерфейс для спілкування з клієнтами, обробки даних, маркетингу та інших функцій.

Згідно зі звітом Global Internet Security Threat Report, зловмисники часто експлуатують вразливості веб-додатків і операційних систем для злому веб-сайтів, використовуючи, наприклад, XSS атаки для перенаправлення користувачів на шкідливі сайти або SQL-ін'єкції для витягу конфіденційних даних. У відповідь на зростаючі виклики, було створено відкритий проєкт OWASP (Open Web Application Security Project), спрямований підвищувати безпеку як Web-технологій, так і окремих веб-ресурсів.

Однак, зловмисники та фахівці в області кібербезпеки продовжують виявляти все нові вразливості, що постійно ставлять під загрозу бізнес та безпечне функціонування організацій.

Вищенаведені аргументи актуалізують тему даної кваліфікаційної роботи, зміст якої становлять дослідження щодо технології та засоби забезпечення безпеки Web-ресурсів в інформаційній системі організації.

Об’єкт дослідження – процес безпечного функціонування Web-ресурсів.

Предмет дослідження – технології та засоби забезпечення безпеки Web-ресурсів в інформаційній системі організації.

Мета роботи – підвищення рівня інформаційної безпеки в організації шляхом впровадженню технічних та програмних рішень для посилення безпеки Web-ресурсів.

Наукові завдання:

- проаналізувати важливість захисту веб-ресурсів;
- проаналізувати нормативно-правові актів України щодо інформаційної безпеки, що регулюють використання та захист веб-ресурсів;
- дослідити категорії вразливостей та загроз веб-ресурсів;
- розробити аналіз керівних принципів безпеки веб-ресурсів;
- дослідити використання AWS для захисту веб-ресурсів;
- розробити рекомендації щодо захисту веб-ресурсів через налаштування Trend Micro.

Методи дослідження – теорія інформації, міжнародні та вітчизняні стандарти у сфері кібербезпеки, політики безпеки.

Практичне значення одержаних результатів полягає в підвищені рівня інформаційної безпеки в організації шляхом впровадженню технічних та програмних рішень для посилення безпеки Web-ресурсів.

Апробація результатів. Основні наукові результати роботи доповідалися та обговорювалися на Всеукраїнськії науково-практичній конференції «Актуальні проблеми кібербезпеки», що проходила у Навчально-науковому інституті захисту інформації 27 жовтня 2023 року. Назва тези «Ризики забезпечення безпеки Web-ресурсів в інформаційній системі».

1 ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТА РЕГУЛЮВАННЯ WEB-РЕСУРСІВ

1.1. Відмінності між веб-ресурсами та веб-додатками

В архітектурі клієнт-сервер та дворівневих додатках, таких як додатки, що використовують JDBC (Java Database Connectivity), логіка та дані специфічні для мережі, в якій вони працюють. Сервер у таких системах обмежує доступ, дозволяючи підключення тільки авторизованим клієнтам. Це створює додатковий рівень безпеки, обмежуючи можливість доступу до даних ззовні.

Для глобальної видимості та доступу до логіки та даних програм використовуються веб-додатки. Веб-додатки забезпечують доступ до ресурсів і логічних даних як для авторизованих, так і для неавторизованих користувачів, забезпечуючи цілодобовий доступ до них. Веб-додаток, розроблений або протестований в компанії, яка спеціалізується на розробці програмного забезпечення, перетворюється на веб-сайт після його розміщення в Інтернеті. Це досягається шляхом реєстрації доменного імені та забезпечення хостингу в Інтернеті. Веб-додатки являють собою комплекс веб-ресурсів, здатних генерувати веб-сторінки. Залежно від типу веб-сторінок, які вони генерують, існують два основних типи веб-додатків: статичні та динамічні. Статичні веб-додатки генерують сторінки, які не змінюються після завантаження, тоді як динамічні веб-додатки можуть змінювати зміст веб-сторінок у реальному часі відповідно до взаємодії користувача або інших факторів.

1. Програми статичних веб-ресурсів: генерує статичні веб-сторінки (приклад HTML);

2. Програми динамічних веб-ресурсів: генерує динамічні веб-сторінки (приклад програми Servlet, програми JSP, програми ASP.net тощо)

Тому, веб-сервіс — це програмна складова, яка взаємодіє з іншими системами через стандартизовані протоколи, зокрема, використовуючи XML-

документи. На відміну від традиційних Інтернет-сервісів, веб-сервіси покладаються на визначені специфікації для передачі даних і виклику методів. Веб-додаток, в свою чергу, це набір програм веб-ресурсів.

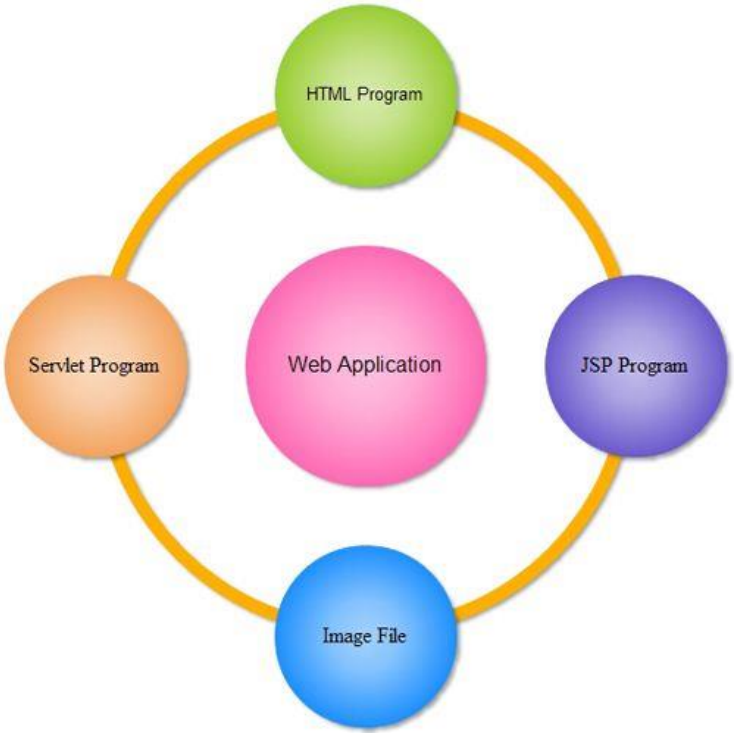


Рис.1.1. Приклад взаємозв’язку між веб-додатком та веб ресурсами

Програмне забезпечення веб-сервера відіграє ключову роль у цьому процесі. Воно не тільки обробляє запити клієнтів та виконує відповідний код веб-додатків, але й може одночасно керувати кількома веб-додатками, що дозволяє забезпечувати паралельну обробку запитів. Ця функціональність критично важлива для підтримки високої пропускної спроможності та надійності веб-сервісів, особливо в умовах великої кількості користувачів і запитів.

Веб-сервери розміщують веб-ресурси. Веб-ресурс — це джерело веб-контенту. Найпростіший вид веб-ресурсу — це статичний файл у файловій системі веб-сервера. Ці файли можуть містити будь-що: це можуть бути текстові файли, файли HTML, файли Microsoft Word, файли Adobe Acrobat, файли зображень JPEG, відеофайли AVI або будь-який інший формат. Однак, ресурси не обов'язково мають бути статичними файлами. Ресурси також можуть бути програмними додатками, які генерують контент за запитом. Ці ресурси з динамічним контентом можуть

генерувати контент, заснований на ідентичності, на тому, яку інформацію запитують, або на часі доби[1]. Вони можуть демонструвати пряму трансляцію з камери, дозволити торгувати акціями, шукати в базах даних нерухомості або купувати подарунки в онлайн-магазинах (рис.1.2).

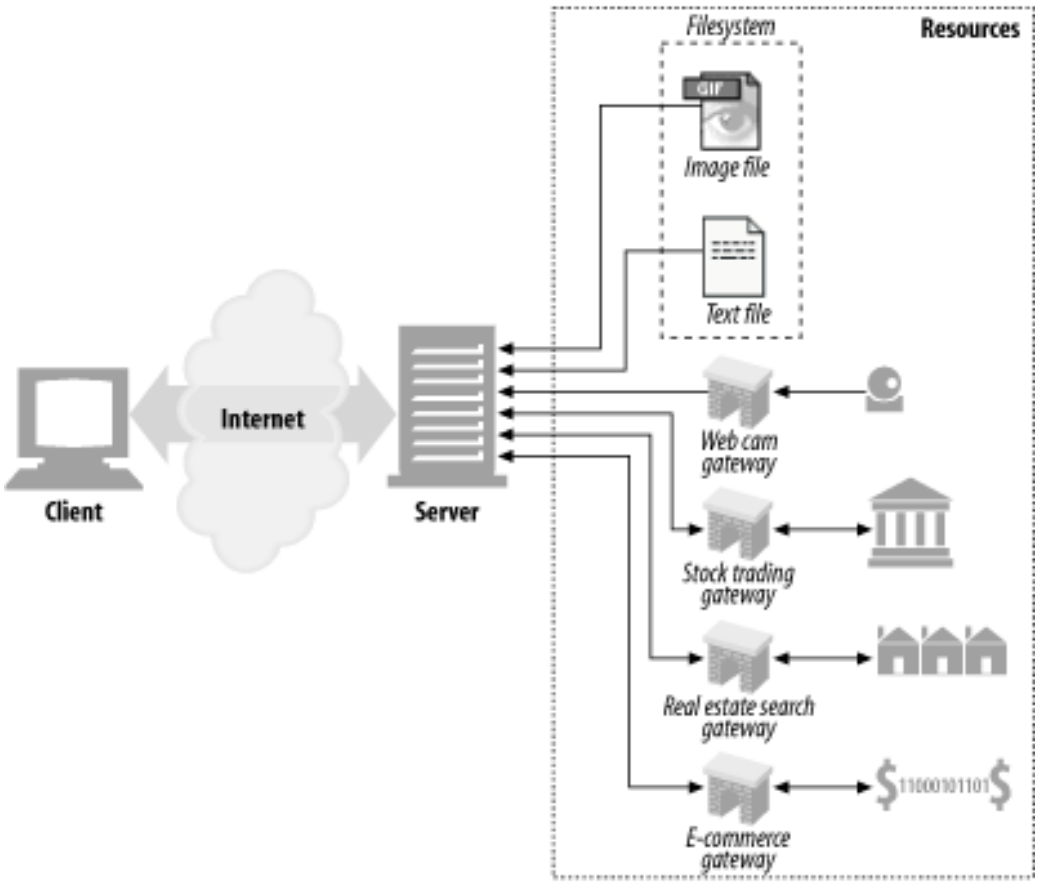


Рис.1.2. Приклад доступу до веб-ресурсу

Таким чином, ресурс – це будь-яке джерело вмісту. Файл, що містить електронну таблицю прогнозу продажів компанії, є ресурсом. Веб-шлюз для сканування даних з публічної бібліотеки є ресурсом. Інтернет-пошукова система – це ресурс.

Веб-ресурси, засновані на мові розширеної розмітки (XML), SOAP та інших відкритих стандартах, та розгорнуті у архітектурах, орієнтованих на послуги (SOA), дозволяють даним та додаткам взаємодіяти без людського втручання через динамічні та адгокові з'єднання.

Враховуючи важливість цих ресурсів, підсилення захисту веб-ресурсів стає критичним аспектом у їхньому використанні в організаціях та компаніях. Це

включає реалізацію комплексних заходів безпеки, що охоплюють як фізичний, так і цифровий аспекти. Особливу увагу слід приділити захисту від кіберзагроз, таких як шкідливе програмне забезпечення, фішинг, атаки типу «відмова в обслуговуванні» (DDoS) та інші види кібератак. Не менш важливим є забезпечення конфіденційності даних, їхньої цілісності та доступності.

Заходи безпеки повинні також включати регулярне оновлення та патчування систем, аудит безпеки та оцінку вразливостей, а також належне управління доступом і ідентифікацією користувачів. Окрім технічних аспектів, важливу роль відіграє обізнаність та навчання співробітників щодо кращих практик у сфері кібербезпеки. З огляду на те, що веб-ресурси є центральним елементом багатьох бізнес-процесів, їх захист не тільки запобігає потенційним втратам чи перервам у роботі, але й забезпечує довіру клієнтів та партнерів, що є необхідним для сталого розвитку бізнесу[2].

1.2. Аналіз звіту найпоширеніших ризиків веб безпеки «OWASP Top 10»

The Open Web Application Security Project (OWASP) є міжнародною некомерційною організацією, яка присвячена поліпшенню безпеки програмного забезпечення. Вони випускають регулярні звіти, відомі як «OWASP Top 10», які висвітлюють найбільш критичні загрози безпеці веб-ресурсів. Цей звіт є важливим ресурсом для розробників, тестувальників, архітекторів систем та будь-яких інших зацікавлених осіб у сфері безпеки веб-додатків.

Зібравши дані від понад 40 відомих компаній із захисту ресурсів, OWASP регулярно публікують звіти щодо найбільш суттєвих загроз та найнебезпечніших уразливостей.

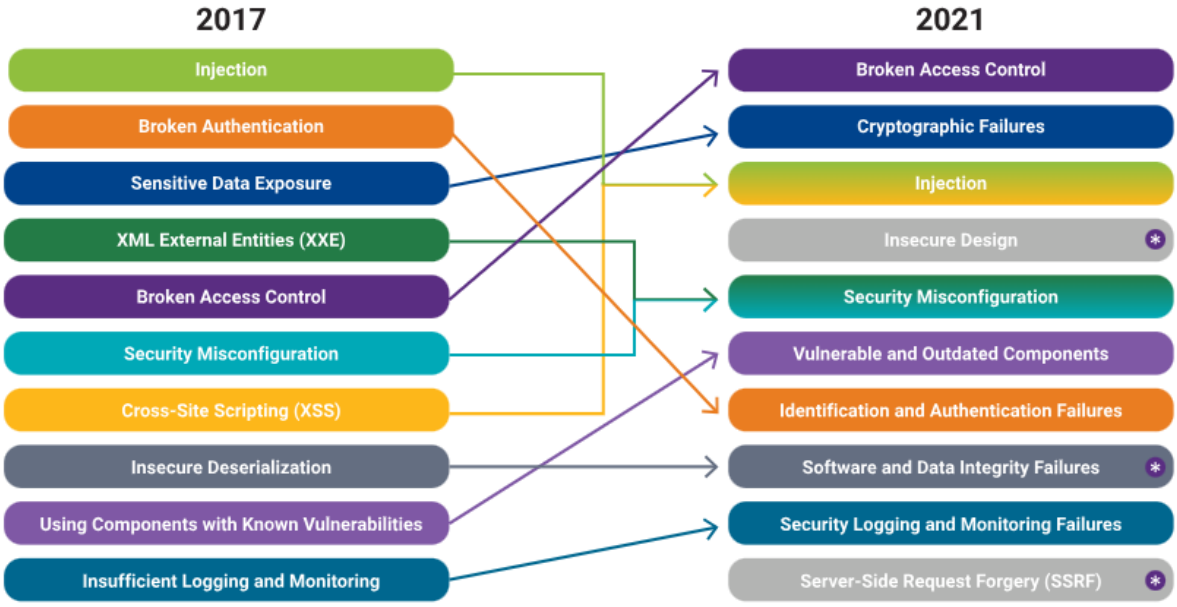


Рис.1.3. Зміни в рейтингу вразливостей «OWASP Top 10» (з 2017 по 2021рр)

Основні аспекти та теми, які зазвичай покриваються в OWASP Top 10, включають:

Ін'єкції (Injection Attacks). Ін’єкції є одним із найпоширеніших методів веб-злому (включають SQL, NoSQL, OS та інші види ін'єкцій). Ін’єкційні атаки дозволяють зловмисникам підробити дані та навіть розкрити всі дані програми, а також - вводити шкідливий код у програми для виконання неправомірних запитів. Отже, таке втручання може призвести до втрати даних або серйозних змін у структурі бази даних.

Помилки ідентифікації та автентифікації (Broken Authentication). Помилки у процесах автентифікації та управлінні сесіями, дозволяючи зловмисникам скомпрометувати паролі, ключі або токени сесії. Ці збої також пов’язані з керуванням сеансом. Наприклад, використання слабких паролів або недостатній захист ваших сеансів є ймовірністю того, що маркери можуть бути повторно використані пізніше. Отже, хакери можуть викрасти облікові дані сеансу, зламати програму або викрасти дані.

Sensitive Data Exposure. Неправильне управління конфіденційними даними, яке може призвести до їх витоку, включаючи фінансову інформацію, персональні дані тощо.

Атаки через обробку XML (XML External Entities). Атаки, пов'язані з обробкою XML, які можуть призвести до витоку даних, виконання шкідливих запитів або інших видів атак.

Порушений контроль доступу (Broken Access Control). Атаки можуть статися через недоліки в політиках та імплементації контролю доступу автентифікованого користувача, наприклад. Отже, користувач може мати більше дозволів, ніж потрібно, що дозволяють зловмисникам отримувати несанкціонований доступ до функцій та даних.

Security Misconfiguration. Неправильна конфігурація безпеки на будь-якому рівні програмного забезпечення, включаючи сервери, додатки, бази даних тощо.

Cross-Site Scripting (XSS). Атаки, при яких зловмисники вставляють шкідливі скрипти у веб-сторінки, які потім виконуються в браузерах інших користувачів.

Уразливості програми та застарілі компоненти. Атаки можуть виникнути, коли користувач не знає стан поточного програмного забезпечення. Наприклад, він може бути застарілим або бібліотеки не мають жорсткої версії. У цьому випадку потрібно перевіряти компоненти під час оновлення.

Помилки, пов'язані з десеріалізацією (Insecure Deserialization). Зазначені помилки можуть призвести до виконання шкідливого коду, витоків даних або атак DoS.

Insufficient Logging and Monitoring. Недостатнє ведення журналів та моніторинг, що може ускладнити виявлення або запобігання атакам.

Додаткові аспекти безпеки включають:

Криптографічні збої. Проблеми з шифруванням під час передачі даних, використання застарілих алгоритмів хешування. Зазвичай це проблема з шифруванням під час передавання. Наприклад, якщо використовується HTTP замість HTTPS або застарілі алгоритми хешування, такі як MD5 або SHA1. Хакери можуть легко викрасти паролі, номери кредитних карток і все, що вводить користувач на веб-сайті, без шифрування, якщо дані не зашифровані під час передачі.

Неправильна конфігурація безпеки. Стандартні паролі, шкідливі бібліотеки, наявність непотрібних компонентів у програмі.

Порушення цілісності програмного забезпечення та даних. Користувачі повинні переконатися, що на кожному кроці розробки програмного забезпечення є цілісність програми. Необхідно використовувати лише надійні репозиторії. Також переконайтеся, що код залишається інтегрованим під час потоку CI/CD (безперервна інтеграція/доставка). Конвеєр CI/CD — це абстрактна автоматизована серія кроків, які необхідно виконати для тестування, створення та доставки програми.

Збої реєстрації та моніторингу безпеки. Важливість моніторингу діяльності API, сесій та входів. Часто практикується не придивлятися до журналювання та моніторингу. Необхідно здійснювати контроль діяльності API, сесій та входи за допомогою інструментів моніторингу. Таким чином, можна побачити, коли зловмисник входив у систему та які дії він робив. Але важливо забезпечувати відсутність конфіденційних даних та облікові дані в журналах.

Підробка запитів на стороні сервера (SSRF) Атаки, що виникають через URL-адреси, які ініціюють певні дії на сервері. Можуть виникнути, коли зловмисник може надати URL-адреси, які ініціюють певну дію на сервері. Ці дії можуть бути будь-якими, від читання даних програми до метаданих сервера.

«OWASP Top 10» забезпечує керівництво та рекомендації щодо запобігання зазначеним загрозам, включаючи найкращі практики кодування, конфігурації та інші заходи безпеки. Цей звіт регулярно оновлюється для відображення нових тенденцій та вразливостей у світі кібербезпеки [3].

1.3. Аналіз нормативно-правових актів та стандартів в сфері інформаційної безпеки, які здійснюють регулювання веб-ресурсів

Функціонування веб-ресурсів в організаціях в Україні регулюється низкою законодавчих актів та нормативів, які визначають вимоги до безпеки,

конфіденційності, зберігання та обробки даних, а також відповідальності за порушення.

Закон України «Про захист персональних даних». Зазначений закон встановлює правила для збору, обробки та зберігання персональних даних. Організації, які володіють веб-ресурсами, повинні забезпечувати конфіденційність даних користувачів і дотримуватися законних процедур їх обробки. Закон є фундаментальним нормативно-правовим актом, який регулює обробку персональних даних в Україні, в тому числі й на веб-ресурсах організацій[4].

До основних положень можна віднести:

- Закон визначає персональні дані як будь-яку інформацію про ідентифіковану або ідентифіковану фізичну особу. Це означає, що будь-яка інформація, яка дозволяє ідентифікувати особу (наприклад, ім'я, адреса, email, IP-адреса), підлягає захисту за цим законом;
- Закон вимагає, щоб згода на обробку персональних даних була свідомою та вольовою. Тому веб-ресурси організацій мають отримати чітку згоду від користувачів перед збором та обробкою їхніх даних;
- Дані можуть збиратися тільки для конкретних, ясно визначених та законних цілей. Організації повинні чітко інформувати користувачів про цілі збору та обробки їхніх даних;
- Закон встановлює, що персональні дані мають зберігатися не довше, ніж це необхідно для цілей, для яких вони були зібрані. Після цього дані повинні бути знищені або анонімізовані;
- Організації мають вжити належних заходів для захисту персональних даних від незаконного доступу, зміни, розкриття, знищення чи втрати (включаючи фізичні, технічні та адміністративні заходи безпеки);
- Закон передбачає відповідальність за порушення правил обробки персональних даних (включаючи адміністративні штрафи, цивільну та кримінальну відповідальність);
- Передача персональних даних за кордон можлива тільки за умови, що

країна-отримувач забезпечує адекватний захист цих даних.

Для організацій, які володіють або управляють веб-ресурсами, важливо дотримуватися цих положень, щоб забезпечити законність обробки персональних даних та уникнути юридичних наслідків. Також вони мають вжити відповідних заходів для забезпечення безпеки даних та інформувати користувачів про свої політики щодо конфіденційності та обробки даних[5].

Закон України «Про інформаційну безпеку України». Зазначений закон містить положення, які стосуються захисту інформації та інформаційних систем. Веб-ресурси організацій повинні бути захищені від несанкціонованого доступу, втрати даних та інших кіберзагроз[6].

Особливості:

- Закон визначає інформаційну безпеку як стан захищеності національних інтересів у сфері інформації. Це означає, що організації, що володіють/управляють веб-ресурсами, мають забезпечувати захист інформації від несанкціонованого доступу, зміни, блокування, копіювання, надання та поширення;
- Закон наголошує на необхідності захисту інформаційних систем від кіберзагроз. Тому організації повинні вживати заходів для захисту своїх веб-ресурсів від кібератак, таких як віруси, хакерські атаки, фішинг та інші форми кіберзлочинності;
- Веб-ресурси організацій повинні забезпечувати безпечне зберігання та обробку інформації, зокрема персональних даних користувачів (включаючи використання захищених протоколів зв'язку, шифрування даних та інші заходи безпеки);
- Організації повинні контролювати зміст інформації, яка публікується на їхніх веб-ресурсах, для запобігання поширенню дезінформації, екстремістського контенту та іншої інформації, що може загрожувати національній безпеці або порушувати закон;
- Закон передбачає відповідальність за порушення норм інформаційної

безпеки;

- У контексті глобалізації та міжнародного характеру інтернету, закон також може враховувати міжнародні стандарти та практики у сфері інформаційної безпеки.

Закон «Про інформаційну безпеку України» вимагає від організацій, що володіють веб-ресурсами, вживати комплексних заходів для забезпечення безпеки інформації. Це включає технічні, організаційні та юридичні аспекти, враховуючи сучасні кіберзагрози та швидко змінюваний характер інформаційного середовища[7].

Закон України «Про рекламу». Різні законодавчі акти, включаючи Закон України «Про рекламу», встановлюють правила щодо змісту, який розміщується на веб-сайтах, особливо у випадках, коли це стосується рекламних матеріалів. Зазначений закон встановлює основні принципи та правила щодо розповсюдження та показу реклами, включаючи ту, яка розміщується на веб-ресурсах організацій. Цей закон має важливе значення для веб-ресурсів, оскільки регулює як зміст, так і форму рекламних повідомлень. Законодавство України передбачає відповідальність за розміщення незаконного контенту на веб-ресурсах, включаючи авторські права, наклеп, розповсюдження дезінформації тощо[8].

Закон України «Про основні засади забезпечення кібербезпеки України». Зазначений закон встановлює фундаментальні принципи та вимоги, спрямовані на забезпечення кібербезпеки в країні, в тому числі захист веб-ресурсів організацій від кібератак та кіберзлочинів. Серед положень та заходів можна виокремити наступні:

- Організації повинні ідентифікувати потенційні кіберзагрози для своїх веб-ресурсів та розробити стратегії управління цими ризиками (включаючи регулярну оцінку вразливостей та потенційних векторів атак);
- Організації повинні впровадити відповідні заходи, для забезпечення безпеки інформаційних систем, які підтримують веб-ресурси, включаючи шифрування, захист від вірусів, файрволи, системи виявлення та запобігання вторгненням.

- Організації мають забезпечити постійний моніторинг своїх веб-ресурсів для виявлення та реагування на кіберзагрози або інциденти;
- Контроль доступу до веб-ресурсів та їхніх адміністративних панелей є ключовим;
- Регулярне навчання персоналу щодо кібербезпеки та найкращих практик може значно знизити ризики від людських помилок та соціальної інженерії;
- Регулярне резервне копіювання критично важливих даних та забезпечення можливості їх відновлення у разі кібератаки є важливими компонентами стратегії кібербезпеки.
- Організації можуть бути зобов'язані співпрацювати з державними органами у сфері кібербезпеки для обміну інформацією про загрози та інциденти.
- Дотримання законодавчих вимог та міжнародних стандартів, таких як ISO/IEC 27001, є важливим для забезпечення комплексної кібербезпеки.

Впровадження цих заходів вимагає не тільки технічної компетентності, але й організаційного підходу до управління кібербезпекою на всіх рівнях організації. Успішне виконання цих вимог не тільки захищає організацію та її веб-ресурси, але й сприяє довірі клієнтів та партнерів[9].

ISO/IEC 27001 (Міжнародний стандарт з систем управління інформаційною безпекою). ISO/IEC 27001 - це міжнародний стандарт, який встановлює вимоги до систем управління інформаційною безпекою (ІБ) в організаціях. Він допомагає організаціям забезпечити захист інформації від загроз, зберегти конфіденційність, цілісність та доступність інформації, а також відновити інформаційні процеси у разі виникнення інцидентів[10].

- Основні елементи стандарту ISO/IEC 27001 з точки зору безпеки веб-ресурсів організації включають наступне:
- Організація повинна провести аналіз ризиків для ідентифікації потенційних загроз безпеці веб-ресурсів. Ця оцінка допомагає визначити, які заходи і контролі необхідно впровадити для забезпечення безпеки.

- Організація повинна визначити всі активи, пов'язані з веб-ресурсами (сервери, бази даних, додатки тощо) і розробити стратегії їх захисту.
- Організація має розробити політику і процедури безпеки, які визначають правила та вимоги щодо використання веб-ресурсів і забезпечують відповідність стандарту ISO/IEC 27001.
- Налаштування прав доступу, аутентифікація та авторизація користувачів до веб-ресурсів для запобігання несанкціонованому доступу.
- Організація повинна вести моніторинг безпеки веб-ресурсів і реагувати на інциденти, проводячи аналіз і вдосконалюючи заходи безпеки.

За допомогою впровадження стандарту ISO/IEC 27001 для безпеки веб-ресурсів організація може досягти кращого захисту від кіберзагроз, зменшити ризик порушення безпеки даних і підвищити довіру клієнтів та партнерів[11].

GDPR (General Data Protection Regulation - Загальний регламент захисту даних ЄС). Європейський регуляторний стандарт, який набрав чинності в травні 2018 року і стосується захисту особистих даних громадян Європейського Союзу. GDPR має величезне значення для організацій, які збирають, обробляють та зберігають особисті дані на веб-ресурсах. Основна мета GDPR - забезпечити більшу прозорість, конфіденційність та безпеку особистих даних громадян.

Основні аспекти безпеки веб-ресурсів організації згідно з GDPR включають наступне:

- GDPR вимагає від організацій вживати необхідних заходів для захисту особистих даних, які вони обробляють (включаючи шифрування даних, контроль доступу, встановлення паролів та ін);
- Організації повинні встановити легальні підстави для збирання та обробки особистих даних. Вони також повинні повідомляти осіб, чиї дані збираються, про цілі обробки та їх права;
- Важливо розробити та впровадити політику безпеки даних, яка визначає правила та процедури для забезпечення безпеки особистих даних. Ця політика має бути документованою і підтримуватися актуальною;

- GDPR вимагає від організацій документувати всі інциденти безпеки даних і повідомляти про них відповідні органи і осіб, чиї дані стосуються, якщо це необхідно;
- Важливо постійно моніторити безпеку веб-ресурсів та процесів обробки даних і проводити регулярні перевірки на вразливості[12].

HATO Cyber Defence Pledge. Ініціатива, яку запровадила Північноатлантична організація НАТО для зміцнення кібербезпеки серед своїх членів, має на меті підвищити готовність та спроможність країн-членів НАТО у сфері кіберзахисту, включаючи захист веб-ресурсів та інфраструктури в мережі Інтернет.

Основні особливості:

- Захист веб-ресурсів представлено як один із ключових аспектів. Зобов'язання щодо кіберзахисту НАТО - це захист веб-ресурсів організацій-членів від кібератак. Включає в себе захист веб-сайтів, веб-додатків, серверів та іншої інфраструктури в інтернеті від кіберзагроз, таких як хакерські атаки, DDoS-атаки і інші;
- Зобов'язання НАТО спрямоване на підвищення готовності організацій-членів до дій в кіберпросторі, включає розвиток кадрового потенціалу та навичок для виявлення, реагування і відновлення після кіберінцидентів, які можуть вплинути на безпеку веб-ресурсів;
- НАТО закликає своїх членів до активного співробітництва та обміну інформацією стосовно кіберзагроз і інцидентів, що допомагає забезпечити об'єднану підтримку у вирішенні проблем кібербезпеки;
- НАТО також надає рекомендації щодо технічних заходів для забезпечення безпеки веб-ресурсів, таких як використання систем виявлення вторгнень, антивірусного програмного забезпечення тощо;
- НАТО сприяє створенню інфраструктури для забезпечення безпеки веб-ресурсів, включаючи центри обробки кіберзагроз та інші ресурси для реагування на кібератаки.

Зазначені закони та стандарти формують основу для регулювання веб-ресурсів, забезпечуючи захист інформації, персональних даних, а також загальну кібербезпеку. Важливо враховувати, що інформаційна безпека є швидко змінною сферою, тому потрібно постійно слідкувати за оновленнями законодавства та стандартів[13].

1.4. Виокремлення необхідності комплексного підходу щодо захисту веб-ресурсів організації в сучасних IT-системах

Веб-ресурси все більше стають невід'ємною частиною інформаційно-технологічних інфраструктур організацій, незважаючи на існуючі невирішені проблеми безпеки. Відповідно, розробка та впровадження безпечних веб-ресурсів є важливою для багатьох IT-інфраструктур організацій.

Однак стандарти безпеки веб-ресурсів не забезпечують усіх необхідних властивостей для розробки надійних, безпечних та стабільних веб-складових. Для адекватної підтримки потреб додатків, заснованих на веб-складових, важливе ефективне управління ризиками та відповідне впровадження альтернативних контрзаходів (рис.1.4).

Оборона на глибину через інженерію безпеки, безпечну розробку програмного забезпечення та управління ризиками може забезпечити значну частину потрібної надійності та стабільності цих додатків.

Рис.1.4. Комплексний підхід до захисту веб-ресурсів

Часто причиною таких проблем є помилки у програмному коді, написаному розробниками, або недооцінка важливості безпечного програмування. Захист веб-інфраструктури є життєво важливим для будь-якої компанії. Із різноманітних захисних рішень, таких як firewall, IPS/IDS, NGFW (Next Generation Firewall) та WAF (Web-Application Firewall), саме Web Application Firewall забезпечує комплексний захист веб-додатків від різноманітних загроз та відповідає регуляторним вимогам, таким як PCI DSS. Інші рішення, як традиційні firewall або IPS/IDS, не можуть надати достатнього рівня безпеки для веб-додатків, оскільки вони не враховують специфіку веб-складових, таку як SQL-ін'єкції, крос-сайт скриптові атаки та інші веб-специфічні вразливості.

Крім того, існують загрози з боку зловмисників, які намагаються отримати несанкціонований доступ до веб-ресурсів шляхом використання вразливостей. Це може включати атаки за типом «людина посередині» (Man-in-the-middle attacks), DDoS атаки, а також інші методи, що використовують слабкості в шифруванні та аутентифікації. Особливу увагу потрібно приділити захисту даних, які передаються та зберігаються на веб-серверах, включаючи конфіденційну інформацію користувачів та комерційні таємниці.

На сучасному етапі розвитку IT-індустрії, важливо також враховувати потенційні ризики, пов'язані з хмарними технологіями та іншими новітніми розробками у сфері інформаційних технологій. Хмарні сервіси та контейнеризація пропонують нові можливості для масштабування та ефективності, але також створюють нові виклики у сфері безпеки. Наприклад, неправильне управління доступом у хмарному середовищі може призвести до витоку даних, а недостатня ізоляція контейнерів може сприяти поширенню шкідливого коду.

Тому важливо розробляти комплексні стратегії безпеки, які б враховували всі аспекти IT-інфраструктури - від фізичного обладнання та мережевої інфраструктури до програмного забезпечення та додатків. Такий підхід повинен включати регулярні аудити безпеки, використання сучасних технологій шифрування, розробку та впровадження політик безпеки, освіту персоналу щодо найкращих практик у сфері кібербезпеки, а також оперативне реагування на

інциденти безпеки. Також дозволяє не тільки запобігти потенційним атакам, але й швидко реагувати на них у випадку їх виникнення, мінімізуючи можливі збитки[14].

Висновки до 1 розділу

Досліджено важливість захисту веб-ресурсів. Проаналізовано різницю між веб-ресурсами та веб-додатками. Веб-ресурси забезпечують доступ до контенту та логічних даних, тоді як веб-додатки дозволяють генерацію веб-сторінок, які можуть бути статичними або динамічними. Виокремлено роль веб-сервера у веб-архітектурі:

Проаналізовано «OWASP Top 10» як ключовий інструмент у веб-безпеці. Описано основні загрози веб-безпеки та рекомендації щодо їх запобігання, що регулярно надаються міжнародною організацією OWASP.

Проведено аналіз нормативно-правових актів України щодо інформаційної безпеки, що регулюють використання та захист веб-ресурсів, включно із законами «Про захист персональних даних», «Про інформаційну безпеку України», «Про рекламу», та «Про основні засади забезпечення кібербезпеки України».

Виокремлено необхідність інтегрованого підходу до захисту веб-інфраструктури, який повинен включати безпечну розробку, управління ризиками та впровадження комплексних захисних механізмів, таких як Web Application Firewalls, наприклад, та інші технічні заходи.

2 ДОСЛІДЖЕННЯ ЗАГРОЗ БЕЗПЕЦІ ТА МЕТОДИ ЇХ ПОМ'ЯКШЕННЯ У КОНТЕКСТІ ВЕБ-РЕСУРСІВ ОРГАНІЗАЦІЇ

2.1. Особливості корпоративних веб-ресурсів

Корпоративні веб-ресурси мають певні властивості, які призводять до специфічних проблем безпеки.

Особливості корпоративних веб-ресурсів включають:

- Використання розподіленої n-рівневої архітектури, яка сприяє розподілу функцій між різними рівнями, що може ускладнити контроль безпеки;
- Необхідність впровадження прозорості та сумісності для забезпечення безперервної роботи та взаємодії між різними компонентами та системами;
- Використання різноманітних технологій та платформ може створювати додаткові виклики у забезпеченні безпеки;
- Забезпечення доступності та розширення можливостей без компромісу з безпекою;
- Важливість високої наявності та ефективного управління ресурсами.
- Віддалений доступ та робота в реальному часі: необхідність забезпечення безпечного та ефективного доступу до ресурсів;
- Підвищений ризик з огляду на глобальний доступ мережі Інтернет та різноманітність користувачів та їх пристроїв;
- Потреба в ретельній перевірці вхідних даних для запобігання зловмисним атакам.

Зазначені характеристики мають безпосередній вплив на основні служби безпеки в організації, а саме: конфіденційність, цілісність, доступність, автентичність та авторизацію. Адже, конфіденційність є критичною при передачі даних через мережу Інтернет, а автентичність та авторизація набувають особливої важливості через віддалений доступ та потенційні вразливості у вхідних даних.

Корпоративні веб-ресурси часто включають численні компоненти від різних IT постачальників, що створює додаткові ризики для безпеки в організації. Веб-ресурси також розповсюджуються на різних апаратних та програмних платформах, що додає додаткових викликів у забезпеченні безпеки. Існує принцип «найслабшої ланки» згідно з яким система є настільки безпечною, наскільки безпечна її найслабша частина. У корпоративних веб-ресурсах можливості для «слабких ланок» численні, що підкреслює необхідність постійного вдосконалення та оновлення безпеки на всіх рівнях[15].

2.2. Архітектура веб-ресурсів

N-рівнева архітектура. Архітектура є ключовою концепцією, яка часто використовується для забезпечення масштабованості, гнучкості та безпеки. Типова n-рівнева архітектура містить такі основні компоненти:

- Рівень веб-сервера – відповідає за обробку HTTP запитів, управління сесіями, маршрутизацію запитів та доставку веб-вмісту;
- Рівень сервера додатків – забезпечує бізнес-логіку та обробку даних, включаючи транзакції, координацію процесів та інтеграцію з іншими сервісами;
- Рівень збереження (бази даних) – відповідає за зберігання, управління та доступом до даних, забезпечуючи цілісність та безпеку інформації.

Кожен з цих рівнів має свої специфічні загрози безпеки, що вимагають індивідуального підходу до пом'якшення. Захист веб-ресурсів має включати комплексний аналіз та заходи безпеки на кожному рівні архітектури, використовуючи принцип «глибокої оборони».

Розробка безпеки на рівні програмного забезпечення є важливою. Розробники, архітектори та дизайнери повинні інтегрувати заходи безпеки на кожному етапі створення веб-ресурсів, роблячи безпеку інтегральною частиною архітектури, а не додатковою функцією.

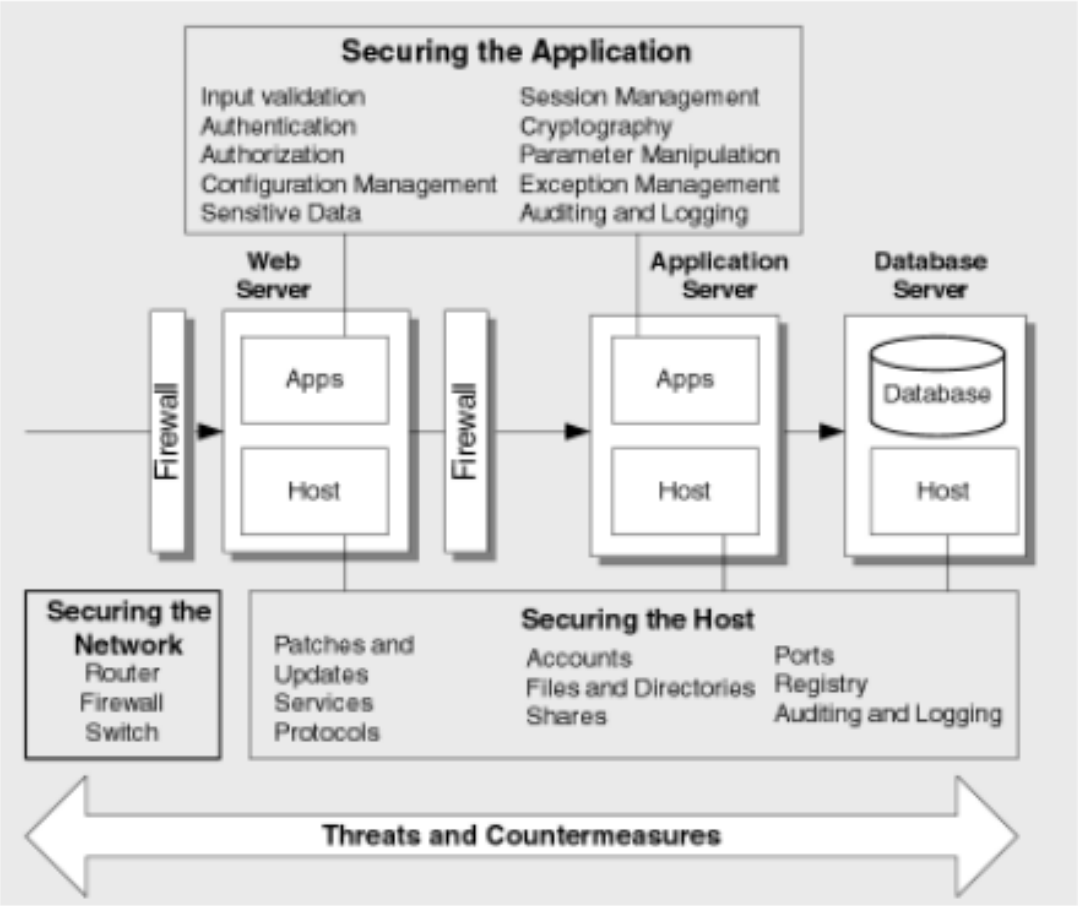


Рис.2.1. Приклад організації захисту 3-рівневої архітектури корпоративних веб-ресурсів

Контрольні елементи безпеки можуть бути вбудовані в базові технології, але додаткові заходи безпеки мають бути реалізовані розробниками. Вони можуть включати валідацію вхідних даних, аутентифікацію, авторизацію, обробку помилок та аудит. Налаштування безпеки повинно бути розроблено так, щоб забезпечувати захист на різних рівнях - мережі, додатків або хостів. Надмірність заходів безпеки є ключовою для забезпечення безпеки веб-ресурсів, оскільки деякі загрози можуть бути пом'якшені на декількох рівнях, тоді як інші - лише на певних.

Такий інтегрований підхід до безпеки дозволяє виявити та ефективно реагувати на різноманітні вразливості та загрози, забезпечуючи всебічний захист корпоративних веб-ресурсів. Тому, захист 3-рівневої архітектури корпоративних веб-ресурсів базується на наступних складових:

Рівень веб-сервера (рівень презентації). Зловмисники, які отримують віддалений доступ до веб-сервера, можуть зробити його вразливим для атак, оскільки він часто є фронтендом веб-ресурсу. На рівні веб-сервера існують загрози, такі як профілювання, заперечення обслуговування, несанкціонований доступ, виконання довільного коду, підвищення привілеїв, а також загрози від вірусів, хробаків та троянських коней. Важливо передбачати ці загрози та розробляти відповідні протизаходи.

Рівень сервера додатків. Рівень зазвичай містить бізнес-логіку веб-ресурсу і може бути вразливим до прослуховування мережі, несанкціонованого доступу, а також до вірусів, троянів та хробаків. Проблеми безпеки на цьому рівні можуть включати переповнення буфера, проблеми з ін'єкцією команд, SQL-ін'єкції тощо.

Рівень сервера баз даних. На цьому рівні знаходяться бази даних, які зберігають дані веб-ресурсу. Основні загрози включають SQL-ін'єкції, підслуховування мережі, несанкціонований доступ та злом паролів. Більшість проблем з SQL-ін'єкціями виникає через недостатню перевірку вхідних даних. Незахищене зберігання даних, коли дані зберігаються у незашифрованому вигляді, також є важливою проблемою.

Рівень веб-ресурсу. До ключових проблемних областей на рівні належать перевірка введення, автентифікація, авторизація, керування конфігурацією, захист конфіденційних даних, управління сесіями, криптографія, маніпулювання параметрами, управління винятками та аудит/реєстрація. Кожен з зазначених аспектів вимагає уваги та ретельної реалізації з метою запобігання потенційним загрозам і забезпечення високого рівня безпеки корпоративних веб-ресурсів.

2.3. Дослідження категорій вразливостей веб-ресурсів

Необхідно розглянути деякі з найпоширеніших вразливостей на прикладному рівні, які становлять загрозу для корпоративних веб-ресурсів.

Неперевірене введення. Неперевірене введення – це широка категорія вразливості, що має серйозні наслідки. Всі веб-ресурси обробляють вхідні дані з

різних ненадійних джерел, включаючи користувачів ресурсу. Неперевірене введення може дозволити зловмисникам атакувати серверні компоненти ресурсу. Перевірка даних має відбуватися кожного разу, коли дані перетинають межу довіри. Перевірка має також відбуватися на рівнях сервера додатків та баз даних. Різноманітність атак на прикладному рівні може бути уникнута, якщо перевірка вхідних даних виконується належним чином, уникнення атак таких як SQL-ін'єкції, міжсайтовий сценарій (XSS), переповнення буфера, введення команд тощо.

Порушений контролю доступу. Проблеми з контролем доступу (авторизацією) виникають, коли обмеження для автентифікованих користувачів не застосовуються належним чином (рис.2.2).

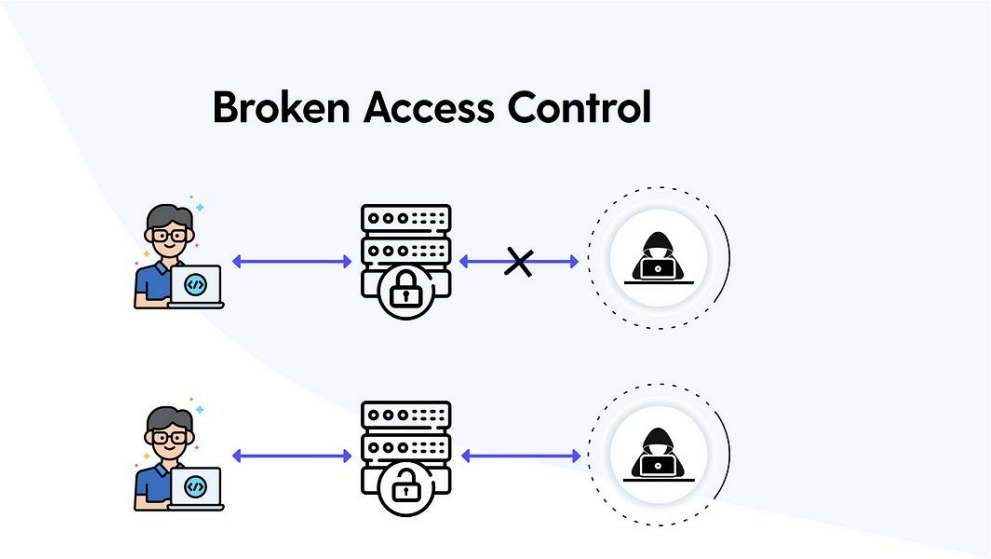


Рис.2.2. Приклад порушення контролю доступу

Уразливості, що відносяться до цієї категорії, можуть дозволити зловмисникам отримувати доступ до облікових записів інших користувачів, переглядати конфіденційну інформацію, або використовувати несанкціоновані функції. Важливі проблеми контролю доступу включають незахищені ідентифікатори, обхід шляху, неналежне управління файлами та кешуванням на стороні клієнта.

Порушена автентифікація та керування сеансами у веб-ресурсах. Належні заходи повинні бути вжиті для захисту маркерів сеансу та облікових даних, таких як паролі, ключі, та файли cookie сеансу в веб-ресурсах. Якщо ці

механізми автентифікації не захищені належним чином, зловмисники можуть використовувати їх для порушення автентифікації та припущення ідентичності інших користувачів (рис.2.3).

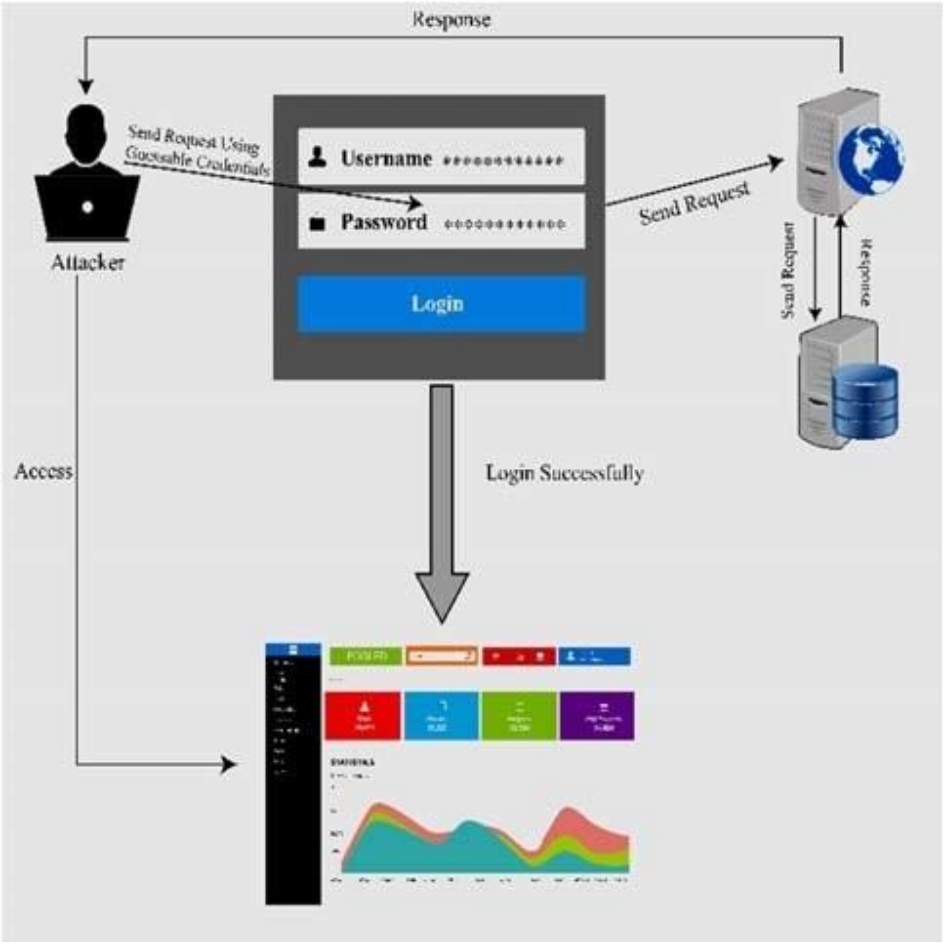


Рис.2.3. Порушена автентифікація та керування сеансами у веб-ресурсах

Функції керування обліковими даними, такі як зміна пароля, відновлення забутого пароля, оновлення облікового запису та інші, повинні бути ретельно захищені в контексті веб-ресурсів. Маркери сеансу, створені після аутентифікації, повинні бути надійно захищені від викрадення. Технологія secure sockets layer (SSL) може внести значний вклад у безпеку сеансу, проте часто вона не реалізована належним чином у веб-ресурсах. Атаки, як міжсайтовий сценарій (XSS), можуть дозволити зловмисникам отримувати маркери сеансу навіть у випадках використання SSL.

Міжсайтовий сценарій (XSS) у веб-ресурсах. Атаки міжсайтового сценарію (XSS) використовують уразливості, пов'язані з недостатньою перевіркою введення.

Зловмисники можуть вставляти виконувані сценарії в веб-ресурси, які потім виконуються в браузерах інших користувачів. Ці атаки можуть призвести до розкриття маркерів сесії користувача, компрометації машини кінцевого користувача або підробки вмісту, щоб обдурити користувача. XSS-атаки можуть відбуватися на рівнях веб-ресурсів або додатків, і необхідна агресивна перевірка білого списку вводу для запобігання цим нападам.

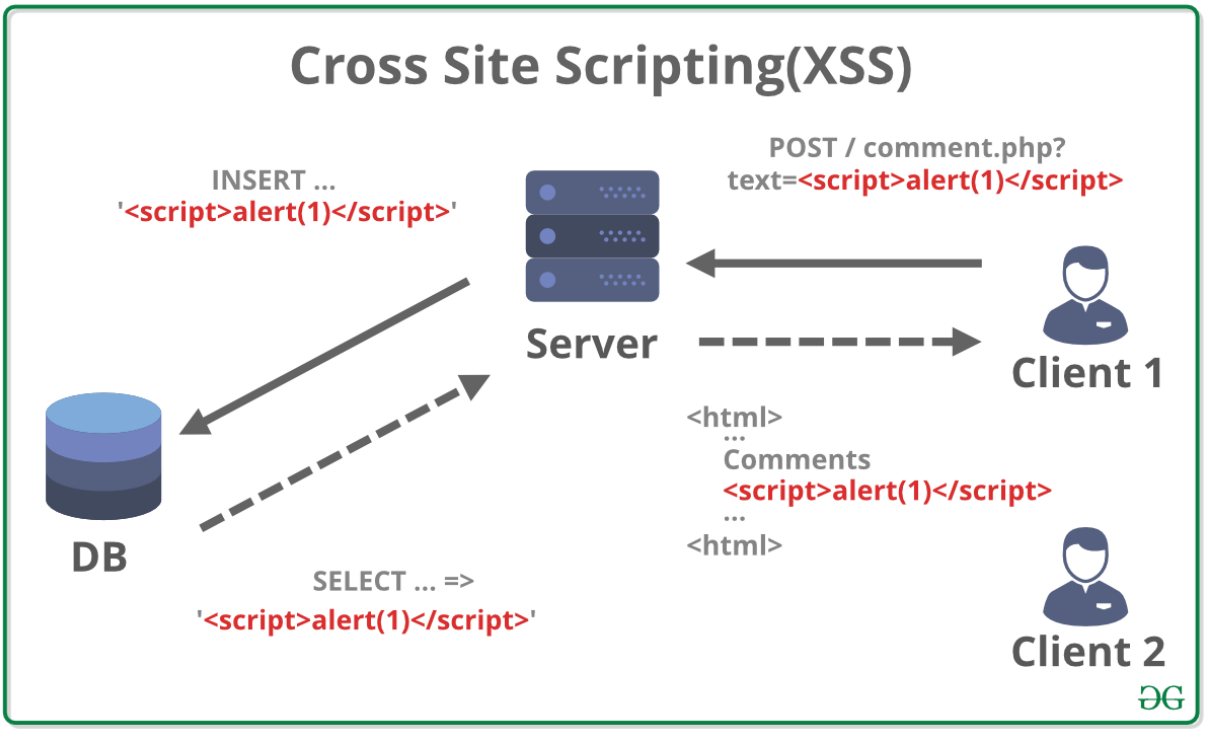


Рис.2.4. XSS-атака

Існують два типи XSS-атак: збережені та відображені. У збережених атаках шкідливий сценарій зберігається в веб-ресурсі для подальшого отримання користувачем, а в відображених атаках шкідливий сценарій передається на сервер і повторюється назад до користувача.

Переповнення буфера у веб-ресурсах. Атаки переповнення буфера відбуваються, коли вхідні дані користувача не обмежені належним чином у веб-ресурсах, що дозволяє зловмисникам переписати вказівник повернення та лічильник програми для виконання шкідливого коду.

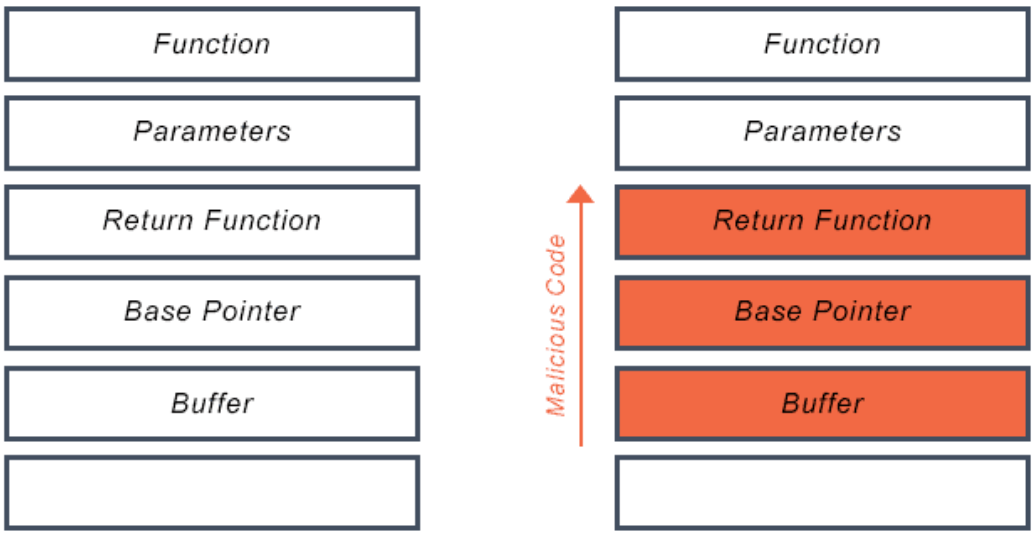


Рис.2.5. Атака переповнення буфера у веб-ресурсах

Це може призвести до серйозного порушення авторизації веб-ресурсу, включаючи виконання довільного коду з тими ж привілеями, що й веб-ресурс. Атаки переповнення буфера часто спричиняють збої системи, впливаючи на доступність системи. Вони можуть бути уникнуті за допомогою належної перевірки вхідних даних та безпечного використання функцій обробки рядків і пам'яті.

Введення команд у веб-ресурсах. У корпоративних веб-ресурсах, які передають параметри при зверненні до зовнішніх систем, додатків або використанні локальних ресурсів ОС, існує ризик ін'єкції команд. Ці параметри не повинні надходити безпосередньо від користувача та повинні бути суворо перевірені перед використанням. Якщо зловмисник може вставити шкідливі команди в ці параметри, вони можуть виконуватися хост-системою, спричиняючи серйозні порушення безпеки. SQL-ін'єкція є поширеним видом ін'єкції команд, що може призвести до витоку або пошкодження даних. Захист від ін'єкції команд у веб-ресурсах вимагає ретельної перевірки введення та використання безпечних методів обробки даних.

Неналежна обробка помилок (керування винятками) у веб-ресурсах. Неналежна обробка помилок та винятків у корпоративних веб-ресурсах може призвести до розголошення інформації та інших проблем безпеки. Помилки, що

відображаються користувачам без обробки, можуть надавати зловмисникам інформацію про систему та її компоненти[16].

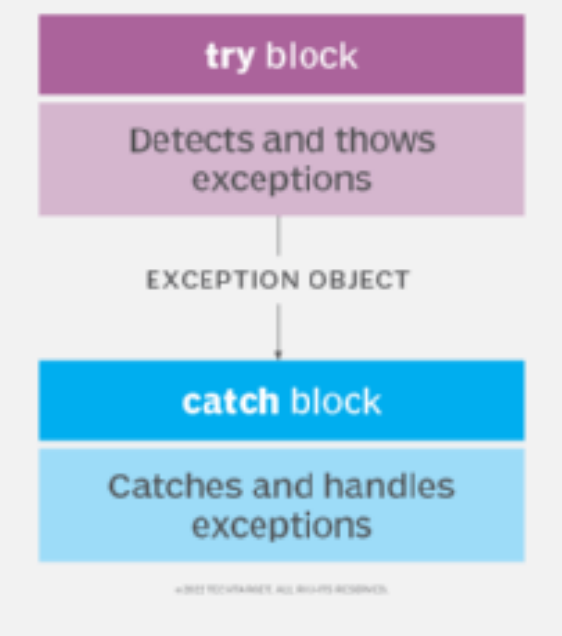


Рис.2.6. Неналежна обробка помилок та винятків у корпоративних веб-ресурсах

Неправильне управління винятками може також вплинути на доступність та безпеку системи.

Незахищене зберігання у веб-ресурсах. Зберігання даних у безпечному вигляді є критично важливим для корпоративних веб-ресурсів. Шифрування даних сприяє конфіденційності та захисту даних, таких як програмні дані, паролі, ключі тощо. Проте, часто шифрування не використовується належним чином. Загрози безпеки можуть включати слабке шифрування критичних даних, незахищене зберігання ключів, вибір ненадійних алгоритмів шифрування тощо. Хешування може бути використане для забезпечення цілісності даних. Мінімізація збереження чутливої інформації є ключовим елементом захисту даних у веб-ресурсах, наприклад, можна не зберігати номери кредитних карток, а замість цього вимагати їх повторного введення при кожній транзакції.

Відмова в обслуговуванні (DoS) у веб-ресурсах. Зловмисники можуть використовувати атаки відмови в обслуговуванні (DoS) для вичерпання ресурсів веб-ресурсу, роблячи його недоступним для інших користувачів(рис.2.7). Такі атаки можуть включати блокування облікових записів законних користувачів або

виклик збоїв у компонентах веб-ресурсу. Різноманітні проблеми кодування, такі як використання неініціалізованих змінних, нульове розіменування покажчика, погане управління паралелізмом, можуть спричинити DoS-атаки.

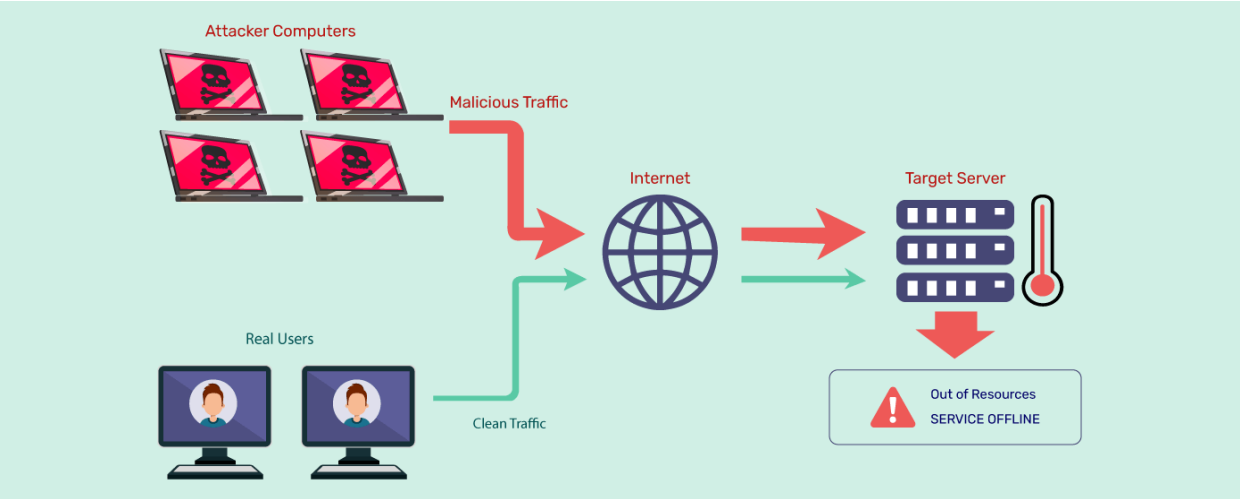


Рис.2.7. DoS у веб-ресурсах

Методи балансування навантаження можуть допомогти зменшити вплив цих атак на доступність веб-ресурсу. Неправильна обробка помилок також може призвести до збоїв, що сприяють DoS-атакам.

Керування незахищеною конфігурацією. Забезпечення захищеної конфігурації на рівнях веб-ресурсу, мережі та хоста є критично важливим для загальної безпеки. Більшість конфігурацій за замовчуванням не забезпечують адекватного рівня безпеки і потребують модифікації. Згідно з принципом найменших привілеїв, конфігурація повинна надавати мінімально необхідний доступ. Необхідно забезпечити безпечну конфігурацію веб-серверів, серверів додатків та баз даних, які є частиною веб-ресурсу. Неправильна конфігурація може бути пов'язана з невиправленими недоліками безпеки в серверному програмному забезпеченні, неправильними дозволами на файли та каталоги, надмірно інформативними повідомленнями про помилки, неправильною конфігурацією SSL та параметрами шифрування, використанням стандартних сертифікатів, неправильними налаштуваннями сервера, що дозволяють атаки на перелік каталогів та обхід каталогів у контексті веб-ресурсу[17].

2.4. Аналіз керівних принципів безпеки веб-ресурсів

Деякі з керівних принципів безпеки відіграють важливу роль у реалізації безпеки на всіх етапах розробки веб-ресурсів і є фундаментальними в інших сферах безпеки, таких як мережевий та хост-захист.

Захист «найслабшої» ланки. Цей принцип стверджує, що безпека системи настільки міцна, наскільки міцна її найслабша ланка. У контексті веб-ресурсів, важливо вбудовувати всебічну безпеку і переконатися, що не залишається дір у безпеці. Наприклад, слабкі місця можуть бути у зберіганні даних або у захисті від зовнішніх атак. Розуміння та захист цих слабких ланок є ключовим для забезпечення загальної безпеки веб-ресурсу.

Створення глибокого захисту. Цей принцип акцентує на необхідності створення різноманітних, перекриваючих захисних стратегій, щоб у разі скомпрометування одного рівня захисту, інший рівень був здатний зірвати атаку та запобігти повному прориву.

У контексті веб-ресурсів, це може означати використання зашифрованого зв'язку, захищених серверів, надійних методів автентифікації та захисту від програмних атак. Множинні рівні захисту значно ускладнюють задачу зловмисника щодо повного порушення системи та забезпечують кращий захист найслабших ланок. Ці принципи, застосовані до веб-ресурсів, вимагають ретельного планування та виконання на всіх рівнях організації, від розробки до впровадження та підтримки.

«Безпечний» збій у веб-ресурсах. Здатність програмної системи адекватно впоратися із збоями є критично важливою для забезпечення безпеки веб-ресурсів. Хоча повністю уникнути збоїв не завжди можливо, безпечне їх оброблення дозволяє запобігти багатьом атакам, зокрема пов'язаним з відмовою в обслуговуванні (DoS) та розкриттям інформації.

Цей принцип передбачає, що системні збої у веб-ресурсах не повинні відображатися користувачам без належної фільтрації, оскільки це може надати зловмисникам цінну інформацію для подальших атак. Всі помилки слід виявляти

та обробляти належним чином, щоб запобігти використанню збоїв у атаках DoS, які виникають через неправильно оброблені помилки.

Зловмисникам часто необхідно спричинити помилку або дочекатися її виникнення для компрометації системи. У контексті веб-ресурсів, безпечний збій означає ретельне планування та обробку потенційних збоїв, щоб знизити ризик виникнення безпекових проблем, пов'язаних із неправильно обробленими помилками та винятками. Це включає реалізацію механізмів виявлення помилок, адекватну обробку винятків, фільтрацію даних перед відображенням користувачам та інші заходи, які запобігають компрометації системи у разі виникнення помилок чи збоїв.

Найменший привілей у веб-ресурсах. Принцип «найменшого привілею» полягає в наданні користувачам або процесам мінімуму привілеїв, необхідних для виконання їх завдань, і обмеженні часу, протягом якого ці привілеї є доступними у веб-ресурсах. Це означає, що права доступу повинні бути налаштовані мінімалістично.

У випадку компрометації облікових даних користувача або захоплення процесу зловмисником, збиток буде обмежений правами, якими користувач або процес володів. Таким чином, не рекомендується входити в систему з адміністративними привілеями або надавати процесам більше прав, ніж це абсолютно необхідно у контексті веб-ресурсу.

Наприклад, у випадку переповнення буфера в додатку, можливість виконання довільного коду буде обмежена правами скомпрометованого процесу. Якщо дозволи були консервативними, обсяг можливої шкоди буде мінімізовано. Обмеження часу, протягом якого доступ дозволений, також зменшує вікно можливостей для зловмисників. Управління привілеями знижує ризик безпеки і є ключовим елементом в захисті корпоративних веб-ресурсів.

«Розділення на складові» у веб-ресурсах. Принцип «розділення на складові» в контексті контролю доступу до веб-ресурсів полягає в тому, що доступ до різних частин системи має бути обмеженим і специфічним, а не універсальним. Це допомагає дотримуватися принципу найменшого привілею, забезпечуючи, що

у разі компрометації одного відсіку системи, зловмисник не отримає доступу до інших частин системи. Проте, реалізація компартменталізації в контексті веб-ресурсів може бути складною та вимагати деталізованої структури контролю доступу.

Важливо визначати ролі безпеки, які сприяють компартменталізації, наприклад, розподіл критично важливих серверних модулів веб-ресурсів на різні машини, щоб у випадку компрометації одного з них інші залишалися недоторканими. Цей принцип допомагає мінімізувати ризики, пов'язані з компрометацією системи, та забезпечує, що збиток від можливих атак обмежений лише окремими частинами системи, а не впливає на всю систему в цілому. Реалізація цього принципу в контексті веб-ресурсів вимагає ретельного планування та управління, але є важливою складовою комплексної стратегії безпеки веб-ресурсів організації.

Простота дизайну у веб-ресурсах. Принцип простоти дизайну в безпеці веб-ресурсів наголошує на тому, що надмірно складні дизайни та реалізації можуть призвести до серйозних проблем з безпекою. Кращою інженерною практикою є створення систем, які виконують свої функції найпростішим можливим способом. Складність збільшує ризик помилок, ускладнює оцінку стану безпеки веб-ресурсу та підвищує ймовірність непередбачених наслідків.

Простий та чистий код веб-ресурсу є безпечнішим, оскільки його легше написати та перевірити на безпечність. Повторне використання перевірених компонентів також є розумною практикою з точки зору безпеки. Використання існуючих, добре випробуваних компонентів зменшує ймовірність внесення нових проблем, особливо у випадку криптографічних алгоритмів.

Конфіденційність інформації в веб-ресурсах. Веб-ресурси повинні бути розроблені з мінімізацією зберігання конфіденційної інформації. Наприклад, не завжди є необхідність у зберіганні номерів кредитних карток, оскільки користувачі можуть повторно вводити їх при кожній транзакції. Це зменшує кількість конфіденційних даних, які потребують захисту.

Розробники веб-ресурсів повинні бути обережними, щоб уникнути ненавмисного розкриття інформації, яка може допомогти зловмисникам у плануванні атак. Наприклад, інформація про використовувану операційну систему або версію бази даних може бути цінною для зловмисників. Забезпечення конфіденційності даних не обмежується лише технічними заходами, але також включає в себе процедури та практики, які забезпечують, що конфіденційна інформація зберігається безпечно та використовується тільки за призначенням у веб-ресурсах.

Розумне приховування секретів у веб-ресурсах. Приховування секретів, таких як ключі шифрування, у веб-ресурсах вимагає особливої обережності та правильного підходу. Жорстке кодування ключів шифрування безпосередньо у вихідному коді може бути ризикованим, оскільки зловмисники можуть отримати доступ до вихідного коду або декомпілювати двійковий файл. Безпечнішим підходом є зберігання всіх секретів, включаючи ключі шифрування, у базі даних на окремій системі, забезпечуючи їх надійність та доступність лише для авторизованих процесів.

Скептицизм щодо довіри у веб-ресурсах. Необхідно підходити зі скептицизмом до будь-якої довіри в контексті веб-ресурсів, розширюючи її лише після достатньої автентифікації. Важливо ставитися до всього мобільного коду як до підозрілого, перш ніж його безпека буде підтверджена. У контексті веб-ресурсів, сервери не повинні безумовно довіряти клієнтам, а повинні здійснювати належну перевірку та автентифікацію.

Використання перевірених технологій у веб-ресурсах. Вибір перевірених та відомих технологій є кращим вибором для використання у веб-ресурсах. Використання загальновідомих компонентів, які пройшли ретельне тестування та аналіз проблем безпеки, зменшує ризик нерозкритих вразливостей. Це стосується як криптографічних рішень, так і бібліотек безпеки, які мають підтримку спільнот, зосереджених на безпеці. Використання перевірених технологій дозволяє використовувати перевагу «багатьох очей», забезпечуючи, що більша кількість людей переглядає код, знижуючи ймовірність проблем, які не були виявлені.

2.5. Особливості використання фреймворку WS-Security

Досягнення правильного поєднання різних технологій та рівнів захисту важливо для мінімізації ризиків від несанкціонованого доступу, перехоплення повідомлень та зловживань, які стали занадто звичними в Інтернеті.

Фреймворк WS-Security інтегрує різні технології безпеки в контексті заголовків SOAP, надаючи можливості для використання імен користувачів/паролів, квитків Kerberos, сертифікатів X.509 та інших стандартів. Це допомагає забезпечити консистентність та стандартизацію в захисті веб-ресурсів, включаючи специфікації, такі як WS-Trust, WS-SecureConversation та WS-Federation, які визначають протоколи для угод між запитувачами та постачальниками щодо захисту, а також WS-SecurityPolicy для оголошення вимог постачальника до підтримки безпеки.

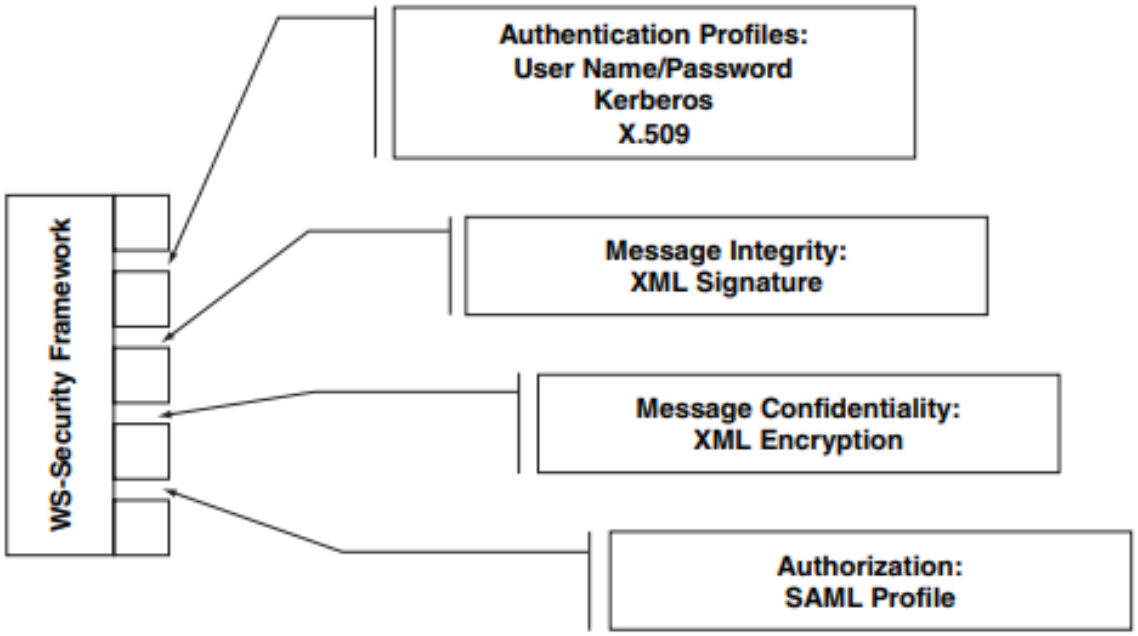


Рис.2.8. Складові фреймворку WS-Security

Безпека є критичною проблемою для веб-ресурсів, оскільки все, що залучено до їх середовища, потребує певного рівня захисту від численних загроз та викликів. Наприклад, повідомлення SOAP у веб-ресурсах повинні бути захищені, файли WSDL можуть вимагати захисту від несанкціонованого доступу, а порти

брандмауера можуть потребувати додаткових механізмів для захисту. Важливою частиною технологій безпеки для веб-ресурсів є забезпечення можливості продовжувати працювати технологіям середовища виконання, додаючи до них механізми безпеки.

На базовому рівні, захист мережі забезпечується за допомогою IPsec (Internet Protocol Security), SSL (Secure Sockets Layer) та базових служб аутентифікації, які надають базовий рівень захисту.

На наступному рівні, фреймворк WS-Security надає можливості для захисту повідомлень за допомогою різних технологій безпеки. WS-Security визначає, як використовувати ці технології в середовищі веб-ресурсів. Основні механізми для захисту включають підписання та шифрування повідомлень для забезпечення цілісності та конфіденційності даних, а також перевірка супутньої інформації про квитки та токени для аутентифікації та авторизації. Ці механізми часто використовуються разом, оскільки потрібно враховувати широкий спектр ризиків.

В рамках WS-Security, до повідомлень SOAP можна додавати заголовки перед їх відправленням, включаючи дані аутентифікації, авторизації, шифрування та підпису. Це дозволяє постачальнику послуг перевірити облікові дані запитувача перед виконанням послуги.

```
<wsse:Security
 xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/12/secext">
 <wsse:UsernameToken>
  <wsse:Username>Ericn</wsse:Username>
  <wsse:Password>8Bcnu6</wsse:Password>
 </wsse:UsernameToken>
</wsse:Security>
```

Рис.2.9. Приклад коду заголовку безпеки у повідомленнях SOAP для веб-ресурсів

Запитувачі зазвичай включають інформацію про аутентифікацію та авторизацію у формі токенів, що вимагає координації інформації про безпеку між запитувачем та постачальником або в ланцюгу запитувачів, постачальників і проміжних серверів SOAP.

Фреймворк WS-Security визначає кілька розширень заголовків SOAP, які використовуються для успішного керування шифруванням та аутентифікацією для обміну повідомленнями від кінця до кінця. Це забезпечує інтегрований та стандартизований підхід до захисту веб-ресурсів, зменшуючи ризики та забезпечуючи конфіденційність та цілісність даних у мережі.

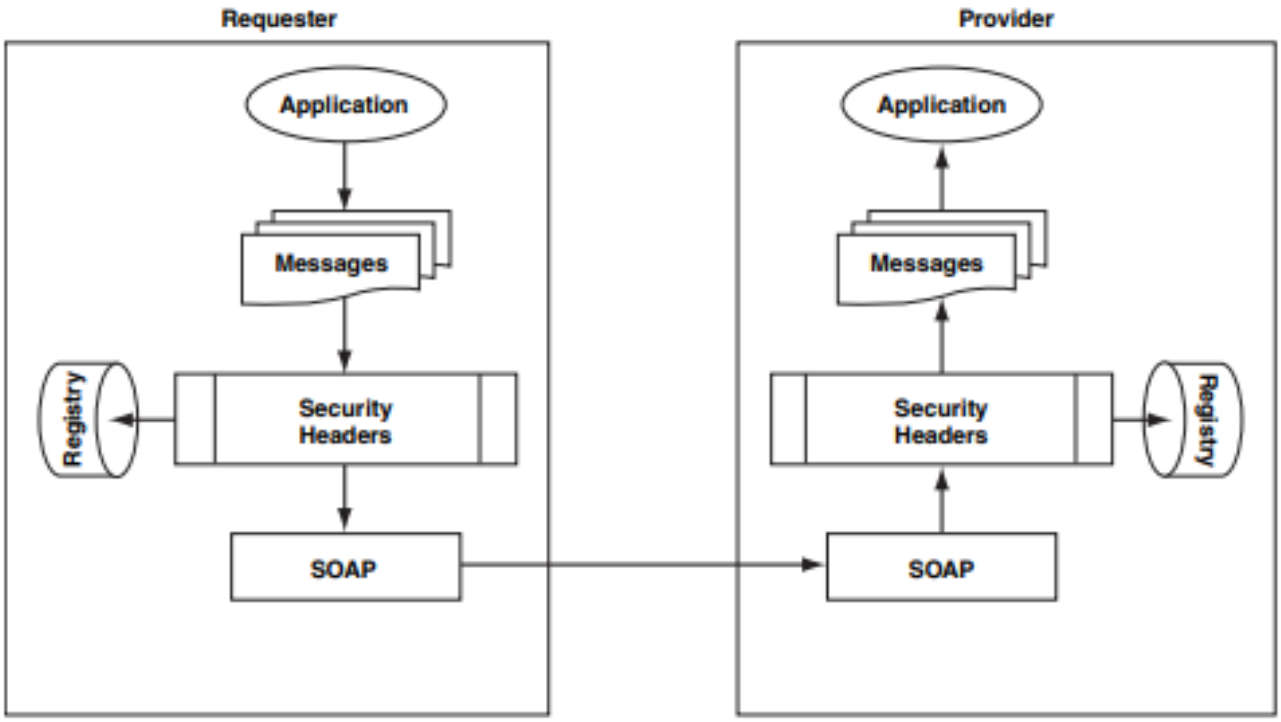


Рис.2.10. Пересилання повідомлень SOAP

У рамках простору імен WS-Security можлива аутентифікація користувача за допомогою чіткого тексту пароля. Включення заголовків WS-Security в повідомлення SOAP забезпечує доступність облікових даних користувача/пароля для обробки як посередниками, так і на кінцевому пункті призначення повідомлення(рис.2.11). Це важливо для веб-ресурсів, оскільки забезпечує необхідну аутентифікацію та безпеку даних у процесі передачі.

Наприклад, якщо постачальник веб-ресурсу потребує використання токена Kerberos, оголошення WS-SecurityPolicy, пов'язане з WSDL постачальника, може вказувати на необхідність використання цієї технології. Це дозволяє забезпечити більш надійний рівень безпеки для взаємодії між клієнтами та постачальниками

веб-ресурсів, гарантуючи відповідність вимогам безпеки та аутентифікації (рис.2.11).

```
<SecurityToken wsp:Requirement=Kerberos
  <TokenType>... </TokenType>
  <TokenIssuer> ... </TokenIssuer>
</SecurityToken>
```

Рис.2.11. Приклад токену Kerberos

Як показано на рис.2.12. в контексті веб-ресурсів можна використовувати пару ключів (або інший механізм шифрування) для шифрування повідомлення перед його передачею і розшифрування після отримання, але перед обробкою веб-ресурсом. Шифрування передає інформацію у кодованому вигляді, подібно до методів, які використовуються військовими для захисту конфіденційної інформації. Для перехоплення та розшифрування зашифрованої передачі, зловмисникам потрібно мати відповідні ключі або знання для розкодування.

Шифрування є важливим інструментом у захисті даних, зокрема аутентифікаційних та авторизаційних даних (таких як паролі), що забезпечує безпеку цих даних під час передачі, навіть якщо інші дані в тілі повідомлення SOAP не шифруються. Це дозволяє забезпечити конфіденційність та цілісність інформації, яка передається між клієнтами та серверами веб-ресурсів, та є ключовим елементом у загальній стратегії безпеки веб-ресурсів.

Шифрування відіграє ключову роль у захисті повідомлень від перехоплення у веб-ресурсах. Використання пари ключів, або іншого механізму шифрування, дозволяє шифрувати повідомлення перед передачею і розшифровувати його після отримання, але перед обробкою веб-ресурсом. Шифрування особливо важливе для захисту даних аутентифікації та авторизації, наприклад паролів, навіть якщо інші дані в тілі SOAP не шифруються.

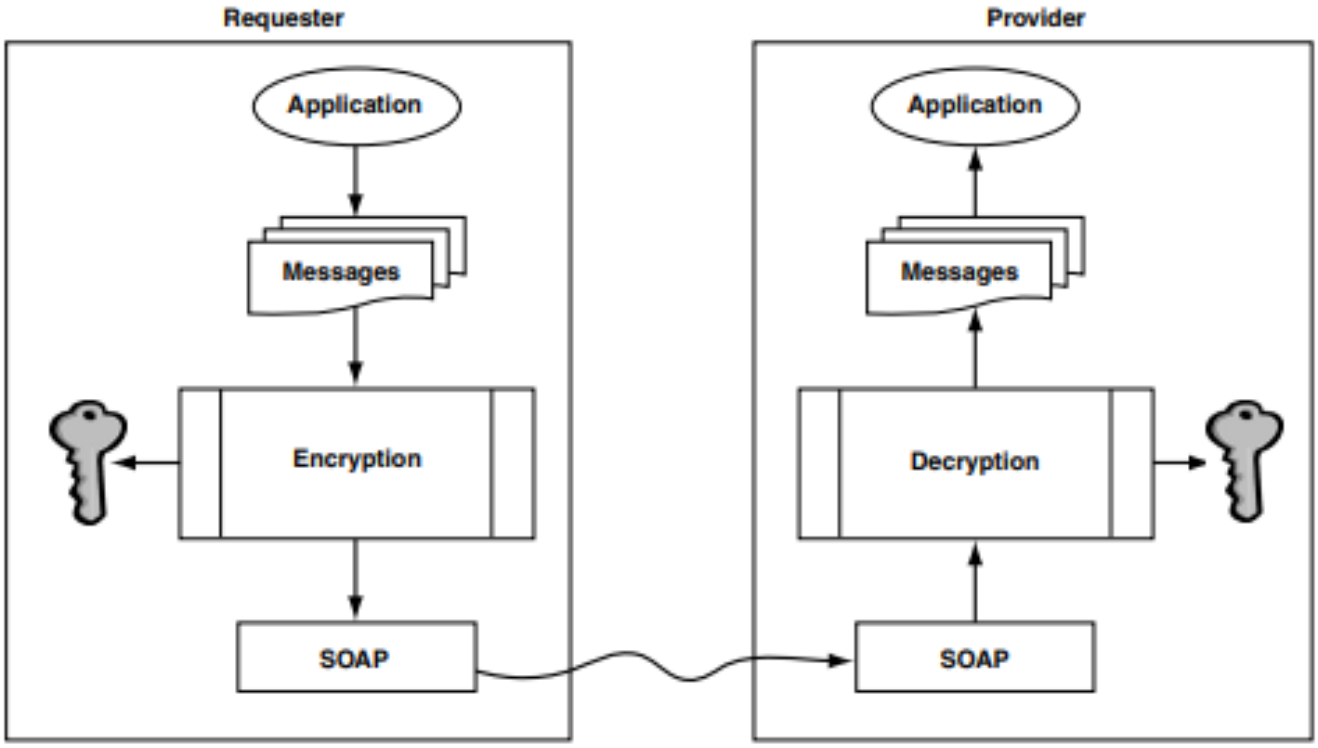


Рис.2.12. Шифрування у захисті повідомлень веб-ресурсів

Інформація про шифрування може бути включена в заголовок WS-Security, щоб постачальник міг знати, який алгоритм шифрування був використаний для шифрування повідомлення. Існують різні стандарти для шифрування, включаючи Secure Shell (SSH) і RSA. Приватний ключ використовується для шифрування, а публічний - для розшифрування повідомлення. У контексті веб-ресурсів, XML специфікація управління ключами (XKMS) може бути використана для управління розповсюдженням публічних та приватних ключів, забезпечуючи безпечний зв'язок.

Також технології обробки транзакцій важливі для координації транзакційних протоколів і вимагають безпеки для запобігання їх порушенню. Управління веб-ресурсами також включає захист інфраструктури управління від несанкціонованого використання та забезпечення можливості відстежувати та управляти інфраструктурою безпеки[18].

2.6. Використання інструментів управління веб-ресурсами

Інструменти управління веб-ресурсами зазвичай реалізують певний рівень функціональності забезпечення безпеки за допомогою проміжних серверів SOAP або перехоплювачів SOAP. Це дозволяє контролювати та захищати взаємодію з веб-ресурсами, забезпечуючи відповідний рівень безпеки та аутентифікації.

Управління ідентичністю для веб-ресурсів. Управління ідентичністю у веб-ресурсах подібне до управління ідентичністю у будь-якій IT-системі. Суб'єкт (людина, машина, програма або абстракція, як потік процесів) отримує унікальне або однозначне ім'я в межах безпекової ділянки, чию дійсність можна перевірити. Ідентичність запитувача веб-ресурсу може бути критичною для постачальника для встановлення довіри, оскільки доступ до послуги чи ресурсу постачальника залежить від ідентичності запитувача.

Управління ідентичністю у веб-ресурсах може бути складним, особливо коли вони охоплюють різні відділи та підприємства. Традиційно управління ідентичністю виконується на рівні місця, відділу або в межах підприємства, забезпечуючи унікальність імені кожного працівника в мережі. Проте, коли ідентичність потрібно унікально керувати через Інтернет і між підприємствами, адміністрування стає складнішим, і виникає збільшена потреба в довірі.

Різні ініціативи, наприклад ті, що фінансуються Liberty Alliance, спрямовані на розробку механізмів для управління ідентичністю в Інтернеті, що включає веб-ресурси. Ці ініціативи важливі для забезпечення надійної ідентифікації та аутентифікації користувачів у глобальному масштабі, особливо в контексті взаємодії між різними організаціями та платформами.

Аутентифікація у веб-ресурсах. Аутентифікація є процесом, в якому авторитет підтверджує ідентичність суб'єкта (як правило, особи, програми, або машини) на основі певного набору доказів, таких як пароль або персональний ідентифікаційний номер (PIN). Процес аутентифікації створює принципала, який представляє аутентифікованого суб'єкта, такого як обліковий запис користувача або токен.

Веб-ресурси часто використовують форму механізму імені користувача/пароля для базової аутентифікації, але також можуть застосовувати більш складні форми, як-от цифрові підписи. Аутентифікація визначається як процес підтвердження того, що суб'єкт є тим, ким він видає себе. Наприклад, у веб-інтерфейсах це може виглядати як спливаюче вікно з ім'ям користувача/паролем, яке використовує cookie для підтримки сеансу користувача.

Запитувачі веб-ресурсів можуть включати інформацію про аутентифікацію, використовуючи ім'я користувача/пароль у заголовках SOAP, які постачальник послуг може перевірити. Ідентифікатор користувача та пароль також можуть передаватися через HTTP. Постачальник веб-ресурсу часто здійснює подальші налаштування цієї моделі для специфічних перевірок авторизації, дозволяючи доступ до певних послуг або ресурсів даних. Іноді запитувачам надаються певні ролі, які можуть бути використані для визначення доступу до авторизаційних даних.

Аутентифікація є життєво необхідною для веб-ресурсів, оскільки вона дозволяє перевірити ідентичність як постачальника, так і запитувача послуги. У деяких випадках може бути потрібна взаємна аутентифікація, де постачальник і запитувач взаємно підтверджують ідентичність один одного[19].

Цифровий підпис у веб-ресурсах. Цифровий підпис використовує пару ключів «публічний/приватний» для підписання дайджесту повідомлення. Алгоритм хешування створює дайджест повідомлення, після чого алгоритм шифрування використовує приватний ключ для підпису дайджесту. Одержувач використовує публічний ключ для розшифровки підпису, повторно обчислює дайджест повідомлення і порівнює їх. Якщо повідомлення було змінено, результати не співпадають, сигналізуючи про можливе втручання в повідомлення. Зазвичай для підписування використовуються асиметричні алгоритми ключів.

Для ефективного забезпечення безпеки важливо розглядати виклики та загрози, з якими можуть зіткнутися веб-ресурси, в контексті їх загальної архітектури. Рішення з безпеки слід визначати, виходячи з конкретних загроз, які потребують захисту, і загального контексту безпеки, в який планується інтегрувати

рішення. Наприклад, використання SSL може бути достатнім у деяких сценаріях, але в інших випадках може вимагатися більш комплексний підхід.

Висновки до 2 розділу

Проаналізовано особливості корпоративних веб-ресурсів. Корпоративні веб-ресурси характеризуються використанням розподіленої n-рівневої архітектури, необхідністю прозорості та сумісності, використанням різних технологій та платформ, а також забезпеченням доступності та розширення можливостей без компромісу з безпекою.

Досліджено концепцію «найслабшої ланки» у контексті безпеки веб-ресурсів. Важливо постійно вдосконалювати та оновлювати безпеку на всіх рівнях, оскільки система є настільки безпечною, наскільки безпечна її найслабша частина.

Виокремлено різні категорії вразливостей та загроз веб-ресурсів. Досліджено категорії включають неперевірене введення, порушення контролю доступу, проблеми з автентифікацією та керуванням сеансами, міжсайтовий сценарій (XSS), переповнення буфера, введення команд, неналежна обробка помилок, незахищене зберігання даних, а також відмова в обслуговуванні.

Розроблено аналіз керівних принципів безпеки веб-ресурсів. Важливість керівних принципів безпеки, таких як захист «найслабшої» ланки, створення глибокого захисту, «безпечний» збій, найменший привілей та розділення на складові для ефективної реалізації безпеки веб-ресурсів.

Виокремлено значення фреймворку WS-Security для захисту веб-ресурсів. Фреймворк WS-Security інтегрує різні технології безпеки, що допомагає забезпечити консистентність та стандартизацію в захисті веб-ресурсів.

3 ВИКОРИСТАННЯ ТЕХНІЧНИХ ТА ПРОГРАМНИХ РІШЕНЬ ДЛЯ ПОСИЛЕННЯ БЕЗПЕКИ WEB-РЕСУРСІВ В ОРГАНІЗАЦІЇ

Забезпечення безпеки веб-додатків від кіберзлочинців, хакерів і зловмисних атак - це безперервна робота. Зі зростанням кількості веб-додатків, ландшафт загроз стрімко розширюється, і виклики в галузі безпеки стають все більш складними.

Ніколи раніше організації не були настільки вразливі перед загрозами, які важко виявити і захиститися від них, і традиційні підходи до сканування на вразливості і безпеці додатків більше не розв’язкують ці проблеми.

3.1. Особливості рішення AWS для захисту веб-ресурсів

AWS пропонує набір послуг, спрямованих на захист веб-ресурсів, включаючи практики безпеки архітектури, забезпечення безпеки інфраструктури та мережі.

Amazon VPC. Одним із важливих інструментів є Amazon VPC (Virtual Private Cloud), що дозволяє запускати ресурси AWS у логічно ізольованій віртуальній мережі. Однак, необхідно налаштувати інфраструктуру для розташування у приватній підмережі з NAT, використовувати ACL для VPC, налаштувати групи безпеки VPC та налаштувати журнали потоків для VPC. Також важливо зробити базу даних недоступною через Інтернет та зашифрувати її за допомогою ключів AWS KMS (рис.3.1).

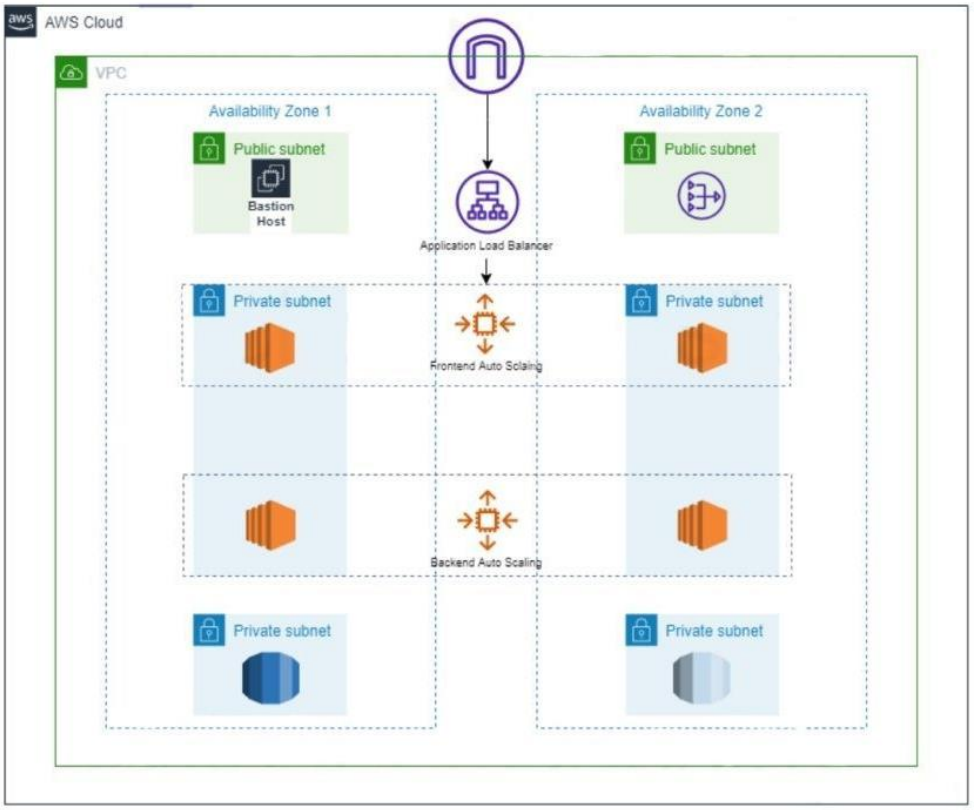


Рис.3.1.Складові AWS

Налаштування Amazon VPC включає наступні кроки:

Крок 1. Розташування в приватній підмережі з NAT:

- Необхідно створити новий VPC у консолі AWS;
- В рамках VPC, необхідно створити одну або кілька приватних підмереж;
- Необхідно налаштувати NAT gateway у публічній підмережі, щоб дозволити приватним підмережам доступ до інтернету, зберігаючи їх ізольованість[20].

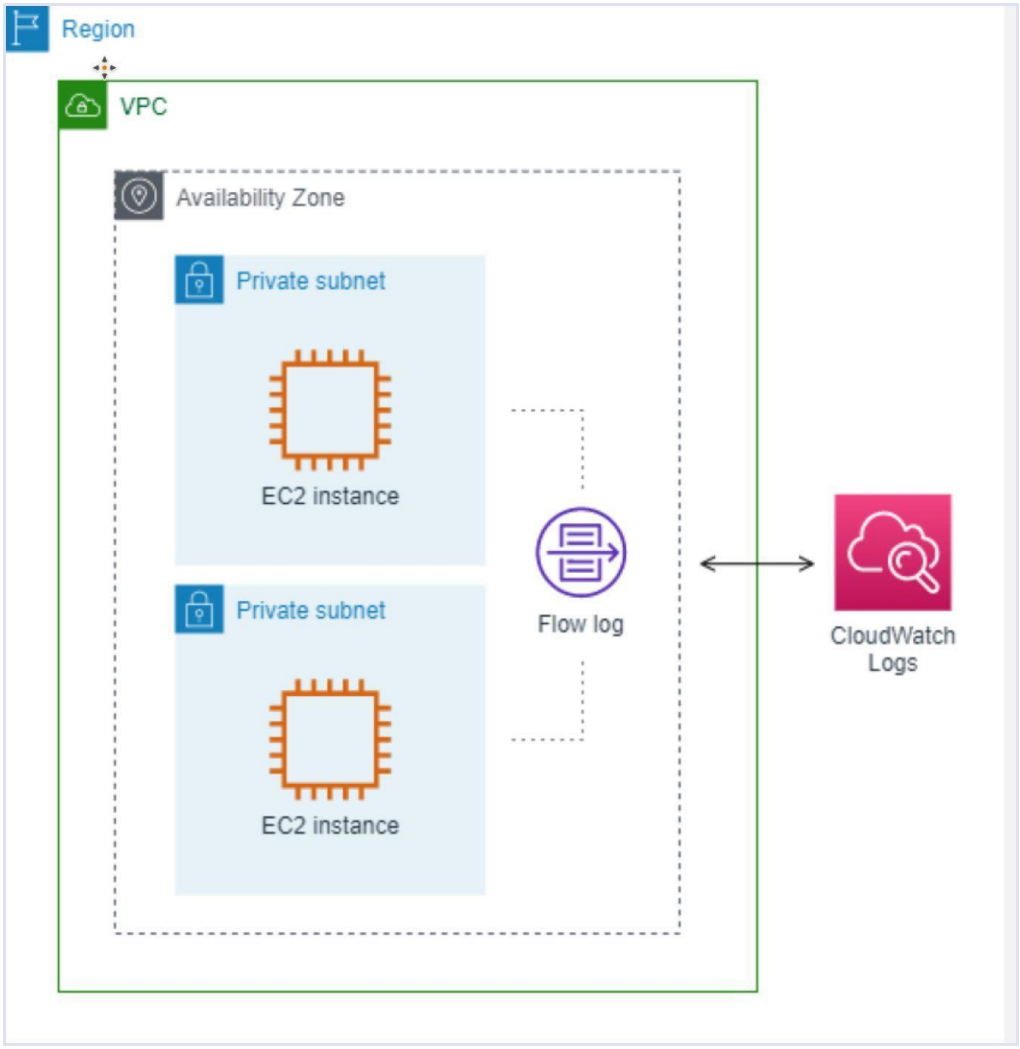


Рис.3.2. Налаштування VPC

Крок 2. Використання ACL для VPC:

- Необхідно створити новий ACL для VPC;
- Необхідно додати правила для визначення дозволених або заборонених вхідних та вихідних з'єднань.

Крок 3. Налаштування груп безпеки VPC:

- Необхідно створити нову групу безпеки в рамках VPC.
- Необхідно налаштувати правила для контролю доступу до ресурсів у VPC, включаючи налаштування IP-адрес та портів.

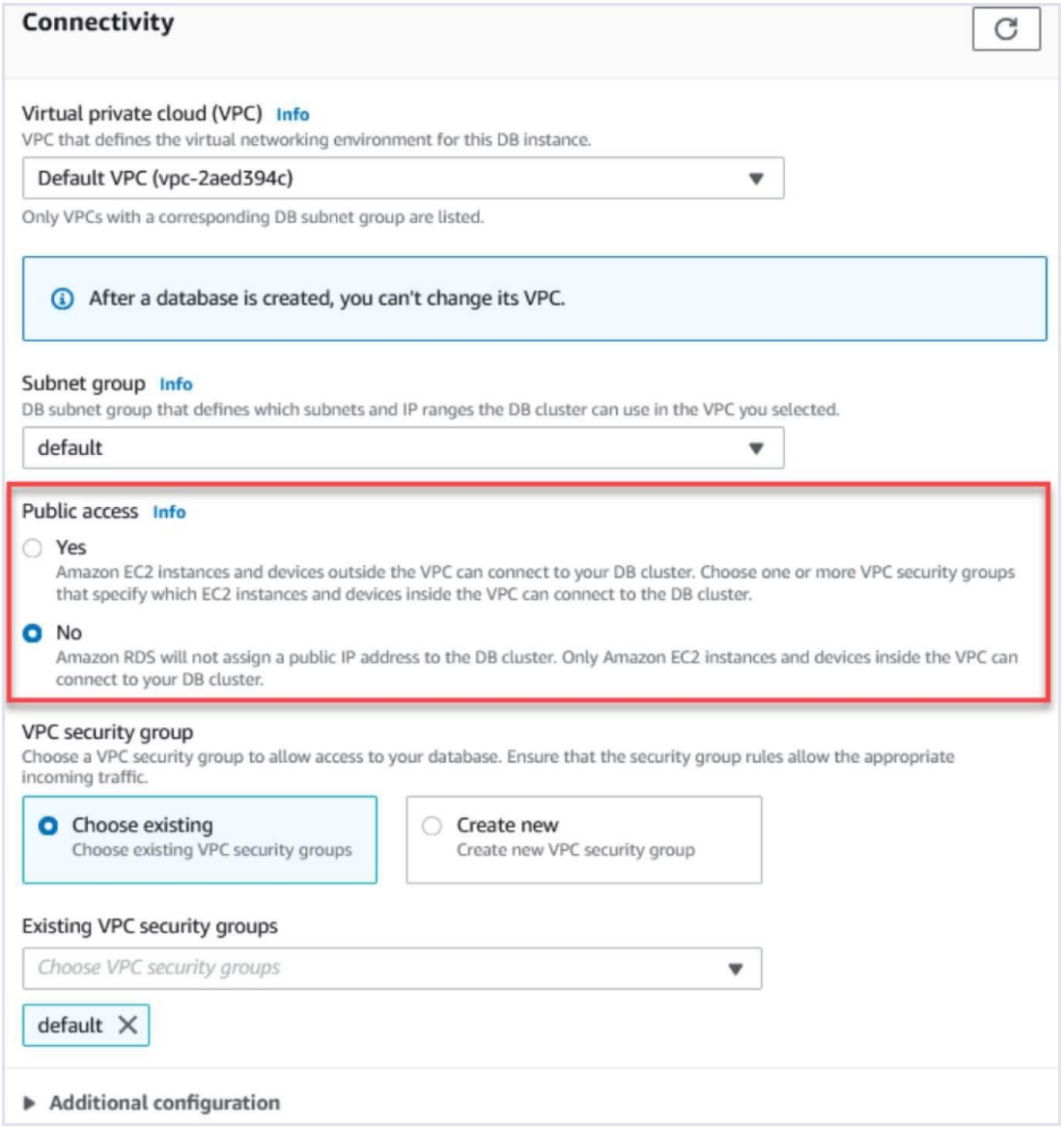


Рис.3.3. Налаштування груп безпеки VPC

Крок 4. Журнали потоків для VPC:

- Необхідно увімкнути журнали потоків для VPC або окремих підмереж;
- Необхідно використовувати зібрані дані для моніторингу трафіку та аналізу безпеки.

Крок 5. Безпека баз даних:

- Необхідно розмістити бази даних у приватних підмережах;
- Необхідно використовуйте AWS key management service (KMS) для шифрування даних баз даних[21].

AWS Security Hub. AWS Security Hub є ще одним важливим інструментом, який збирає дані з різних служб AWS для перевірки відповідності стандартам безпеки, як-от PCI DSS та AWS Foundational Security Best Practices[22].

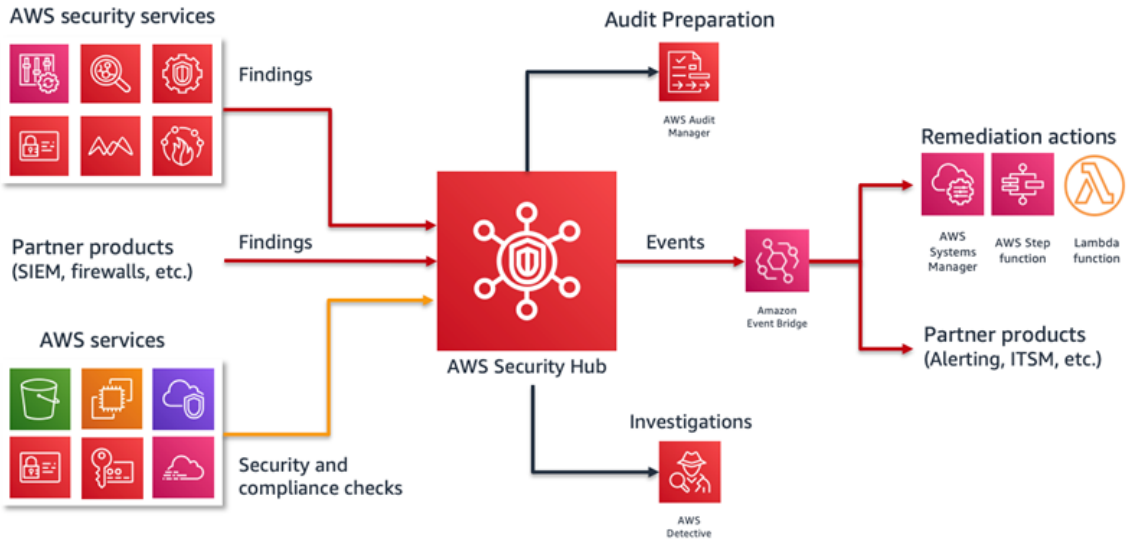


Рис.3.4. AWS Security Hub

Налаштування AWS Security Hub включає наступні кроки:

Крок 1. Активація Security Hub:

- Увімкнення служби. Для цього необхідно активувати AWS Security Hub у консолі AWS;
- Інтеграція з іншими службами AWS. Необхідно налаштувати інтеграцію з іншими службами AWS, які використовуються (наприклад, AWS IAM, Amazon VPC).

Крок 2. Перевірка відповідності:

- Контроль стандартів. Можливо використовувати Security Hub для контролю відповідності популярним стандартам безпеки, таким як PCI DSS;
- Відстеження рекомендацій. Необхідно аналізувати та відстежувати рекомендації безпеки, надані Security Hub[23].

AWS Identity and Access Management. AWS IAM (Identity and Access Management) допомагає безпечно контролювати доступ до ресурсів Amazon. Необхідно забезпечити використання багатофакторної аутентифікації (MFA), налаштувати політики паролів облікових записів та забезпечити зміну паролів.

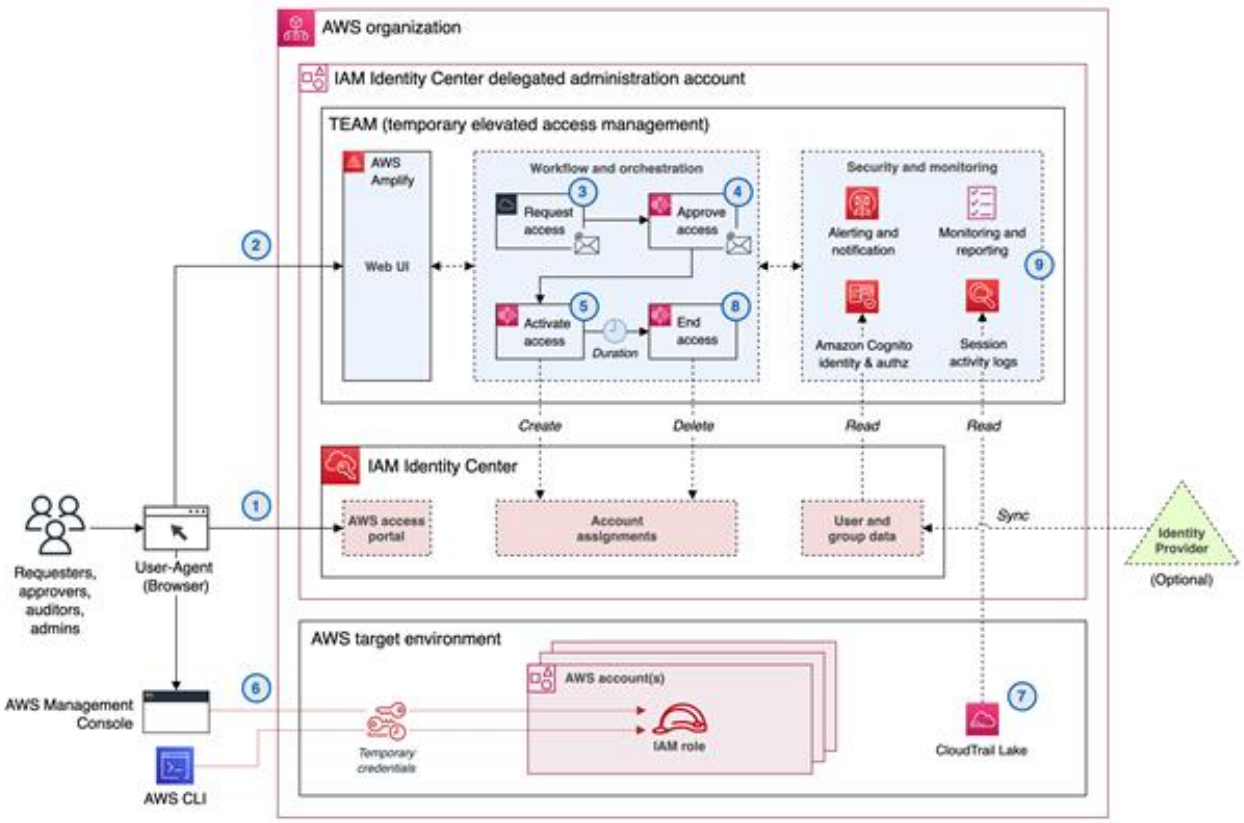


Рис.3.5. Архітектура AWS IAM

Використання принципу найменшого наданого повноваження та ролей IAM для ідентифікації також є ключовими аспектами безпеки.

Налаштування AWS IAM включає наступні кроки:

Крок 1. Багатофакторна аутентифікація (MFA):

- Активація MFA. Необхідно налаштувати використання MFA для всіх користувачів AWS IAM;
- Застосування MFA для критичних операцій. Необхідно забезпечити використання MFA при зміні паролів або виконанні важливих операцій.

Крок 2. Політики паролів:

- Налаштування сильних політик паролів. Необхідно встановити вимоги до складності та тривалості паролів;
- Регулярна зміна паролів. Необхідно забезпечити регулярну зміну паролів, наприклад, кожні три місяці.

Крок 3. Принцип найменших повноважень:

- Обмеження доступу. Необхідно надати користувачам лише ті доступи,

які необхідні для виконання їх завдань;

- Використання ролей IAM. Можливо використовувати ролі IAM для надання тимчасового доступу до ресурсів AWS без необхідності постійних облікових даних.

AWS Route 53. AWS Route 53 — це високодоступний та масштабований DNS-сервіс. Він керує DNS-записами, перетворюючи доменні імена в IP-адреси, що дозволяє веб-ресурсам завантажуватися в браузерах(рис.3.6).

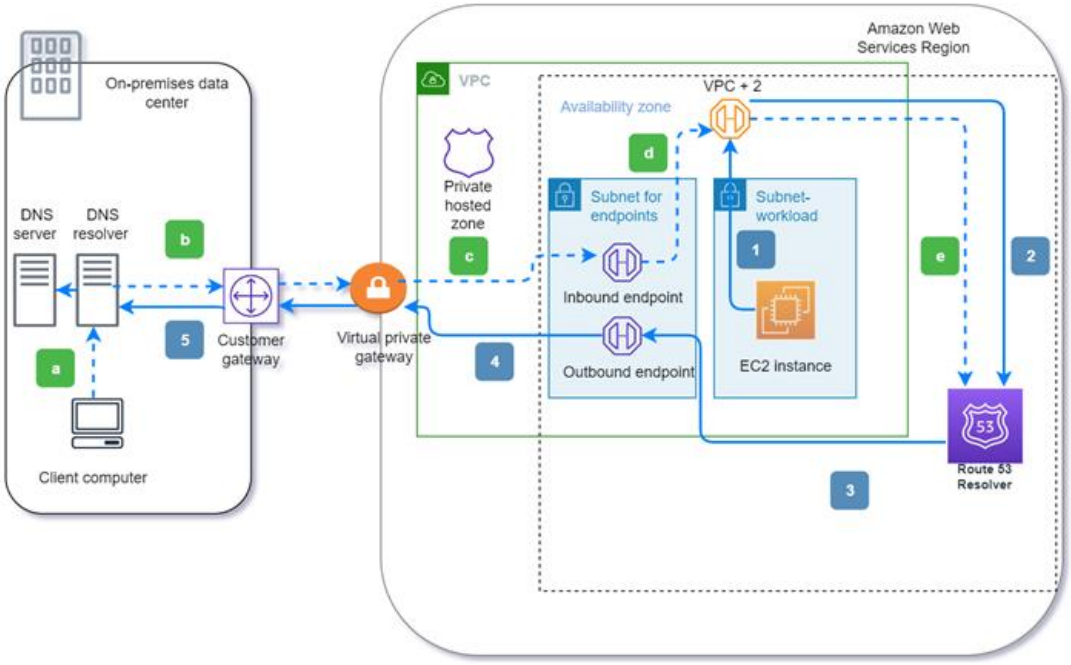


Рис.3.6. AWS Route 53

Route 53 включає DNSSEC, який захищає веб-ресурси від отруєння кешу DNS.

Налаштування включає наступні кроки:

- Необхідно налаштувати DNS-записи для доменів;
- Активувати DNSSEC для додаткового захисту від атак, що маніпулюють DNS.

Служба AWS Route 53 дозволяє керувати DNS-записами і має вбудовану функцію DNSSEC (Domain Name System Security Extensions). Ця функція захистить веб-додатки від отруєння кешу DNS. Це відбувається, коли зловмисник змінює

джерело домену і може перенаправити його на зловмисну веб-сторінку. DNSSEC допоможе запобігти цим атакам.

AWS Web Application Firewall (WAF). AWS WAF захищає веб-ресурси від різноманітних загроз, включно з OWASP top 10. Він дозволяє керувати правилами безпеки, що блокують шкідливий трафік(рис.3.7).

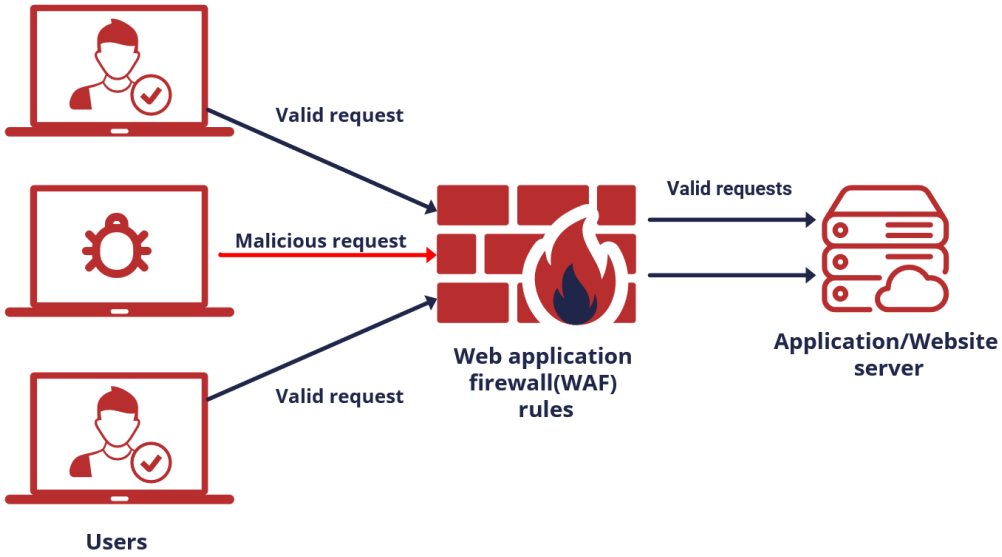


Рис.3.7. AWS Web Application Firewall (WAF)

Налаштування включає наступні кроки:

- Необхідно налаштувати правила WAF, які включають стандартні шаблони (наприклад, OWASP top 10) та власні правила;
- Інтеграція з CloudFront, Application Load Balancer і API Gateway для забезпечення всебічного захисту.

AWS Shield. AWS Shield надає захист від DDoS-атак. Існують два варіанти: Default і Advanced, з яких Advanced надає розширені можливості.

Налаштування включає наступні кроки:

- Необхідно активувати Shield Default для базового захисту;
- За необхідності активувати Shield Advanced для покращеного захисту, підтримки та відшкодування витрат при атаках.

AWS CloudFront. AWS CloudFront — це CDN-рішення, яке покращує швидкість завантаження веб-ресурсів і забезпечує захист від DoS/DDoS-атак.

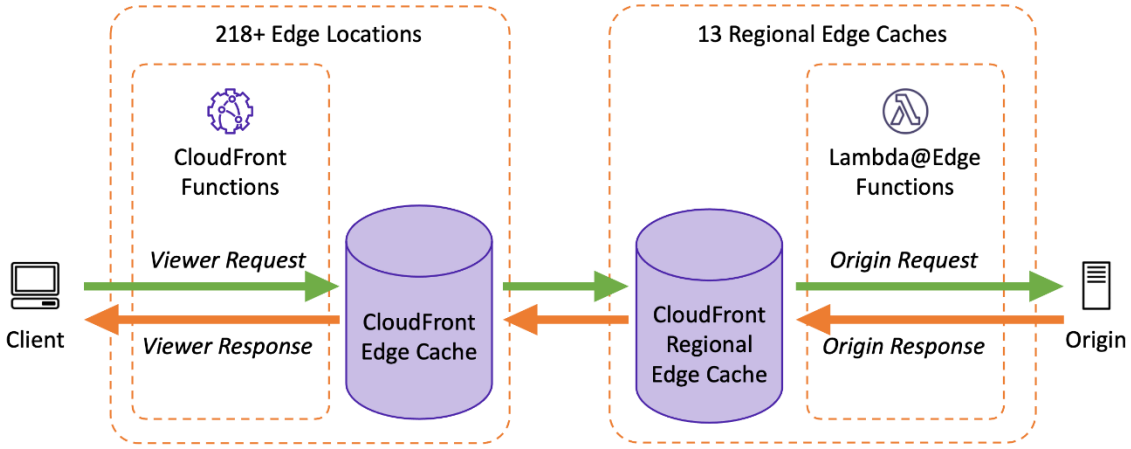


Рис.3.8. Приклад використання AWS CloudFront

Налаштування включає наступні кроки:

- Необхідно налаштувати CDN для розподілу контенту веб-ресурсу через мережу крайових точок;
- Використання кешування та гео-обмежень для оптимізації доступу до веб-ресурсу.

Також варто зазначити, що для налаштування захисту веб-ресурсів, використання комбінації різних інструментів AWS є ефективним підходом. Кожен інструмент пропонує унікальні функції, що разом забезпечують всеосяжний захист.

Комбінування AWS Route 53 та AWS WAF. AWS Route 53 забезпечує надійне управління DNS, що допомагає в оптимізації доступу до веб-ресурсів і захисту від атак на DNS-рівні. AWS WAF працює на рівні веб-додатків для фільтрації та блокування шкідливих запитів. Необхідно налаштувати обидва інструменти для забезпечення захисту від широкого спектру атак, включаючи DNS-спуфінг та веб-загрози.

Використання AWS Shield разом з AWS CloudFront. AWS Shield, особливо у варіанті Advanced, ефективно протидіє DDoS-атакам. AWS CloudFront покращує швидкість завантаження веб-ресурсів і додатково забезпечує захист від атак типу DoS/DDoS завдяки глобальній CDN-мережі. Необхідно налаштувати ці служби для забезпечення не тільки швидкого доступу до веб-ресурсів, але й їх захисту від

масштабних DDoS-атак. Налаштування захисту веб-ресурсів включає використання різних інструментів AWS, кожен з яких виконує специфічні функції для забезпечення безпеки та ефективності.

3.2. Налаштування Trend Micro Web App Security

Trend Micro Web App Security as a Service та Imperva SecureSphere об'єднали зусилля для надання інтегрованого рішення для вирішення веб проблем та полегшення максимального підвищення безпеки веб-додатків для клієнтів.

Trend Micro Web App Security ідентифікує вразливості в веб-додатках і платформах, на яких вони розгорнуті, і разом з Imperva SecureSphere Web Application Firewall, захищає вразливості, перш ніж їх можна використовувати для атак. Це інтегроване рішення допомагає скоротити вікно вразливості і уникнути перерви в циклах екстреної виправки та тестування. Організації можуть використовувати цю спільну пропозицію для відстеження зловживання додатками, зупинки атак на додатки та виконання вимог PCI DSS 6.6, спрощуючи аудити безпеки.

Для захисту клієнтів в складному загрозовому середовищі сьогодення, Trend Micro розробила перший комплексний набір засобів безпеки, спеціально розроблений для виявлення вразливостей та захисту веб-додатків в єдиному інтегрованому пропозиції. Trend Micro Web App Security as a Service надає виявлення загроз та захист від загроз веб-додатків з такими можливостями:

• Повне «розумне» тестування додатків для сучасного складного середовища загрози. З використанням як автоматичного сканування, так і експертного тестування, веб-додатки можуть бути постійно захищені від найскладніших атак, уникнувши при цьому помилкових позитивів, які часто сповільнюють роботу команди з безпеки;

• Інтегроване виявлення та захист для мінімізації часу реакції на загрози безпеки з можливістю швидко блокувати нові атаки без затримок у внесенні патчів у поточну інфраструктуру або оновленні додатка;

• Включено необмежене число SSL-сертифікатів для захисту та безпечного забезпечення всіх веб-додатків і підвищення довіри клієнтів без додаткових витрат.

З патентованою технологією Dynamic Profiling, SecureSphere автоматично створює модель законної поведінки та адаптується до змін додатка з плином часу, оновлюючи свої захисти без ручної конфігурації. Imperva SecureSphere надає практичний і високо безпечний рішення для забезпечення безпеки веб-додатків та даних.

• Автоматично вивчає структуру веб-додатків та поведінку користувачів;

• Оновлює веб-захисти інтелектуальною інформацією щодо поточних загроз;

• Визначає трафік, який виходить зі зловмисних та шахраївських джерел за допомогою ThreatRadar;

• Практично виправляє додатки за допомогою інтеграції із сканером на вразливості;

• Забезпечує високу продуктивність, розгортання та чіткі, бізнес-зв'язані звіти та сповіщення;

• Повністю відповідає вимогам PCI DSS 6.6.

Trend Micro Web App Security поєднує зручність облачного сканування вразливостей платформи та компонентів додатків з ретельним тестуванням бізнес-логіки експертів з безпеки та видаленням помилкових позитивів. Trend Micro Web App Security виявляє вразливості додатків і створює вихідний файл у форматі, який можна обробити брандмауером веб-додатків Imperva SecureSphere, який автоматично перетворює інформацію про вразливість на правила захисту в Imperva SecureSphere. Ці правила потім можна застосовувати для захисту від використання вразливостей додатків до виправлень коду та конфігурації. Це дозволяє значно зменшити витрати та розлад від екстрених циклів виправлень.

Виправлення, надане SecureSphere, миттєво усуває вразливості, дозволяючи організаціям розробляти та впроваджувати виправлення коду за своїм розкладом та уникати процесів екстрених виправлень та тестування. Крім того, моніторинг веб-атак та помилок додатків дозволяє розробникам додатків визначати пріоритети заходів щодо усунення[24].

3.3. Створення та налаштування різних груп веб-додатків в Deep Security

Для підвищення захисту веб-ресурсів, важливо створювати та налаштовувати веб групи у системі Deep Security для веб-додатків. А саме:

1. Об'єднання веб-додатків у групи за географічними або функціональними особливостями. Цей крок дозволить ефективно управляти безпекою веб-додатків, які обслуговують різні регіони або виконують різні функції. Наприклад, групування веб-додатків для окремих географічних областей дозволяє спрямовувати захисні заходи з урахуванням локальних особливостей та вимог;

2. Створення спеціальних груп для високоризикових та критично важливих додатків. Цей крок дозволяє зосередити увагу на захисті тих веб-додатків, які мають найбільшу важливість або найвищий рівень ризику. Використання окремих груп для цих додатків спрощує моніторинг та управління безпекою.

3. Моніторинг та відображення результатів сканування для кожної групи. Цей крок забезпечує зручність у відстеженні потенційних вразливостей та загроз у кожній групі веб-додатків. Сторінки «Сканування платформи», «Сканування додатків» та «Виявлення шкідливих програм» у консолі дозволяють легко виявляти та реагувати на можливі проблеми безпеки;

4. Налаштування адміністративних прав для кожної групи. Цей крок забезпечує можливість тільки авторизованим особам мати доступ до управління та моніторингу безпеки певних груп веб-додатків. Наявність різних адміністраторів для різних груп дозволяє ефективно розподіляти відповідальність та забезпечувати відповідний рівень безпеки;

5. Легкість управління через користувальницький інтерфейс. Процес додавання нових груп є інтуїтивно зрозумілим і включає кроки, такі як введення назви та опису групи на вкладці «Загальні налаштування». Цей крок дозволяє легко створювати та налаштовувати групи залежно від потреб організації.

Зазначені кроки сприяють покращенню захисту веб-ресурсів, дозволяючи більш ефективно управляти безпекою веб-додатків та забезпечувати відповідний рівень захисту для різних категорій додатків.

Створення та налаштування груп веб-додатків. Потрібно перейти за посиланням на вкладку «Веб-додатки в групі». У стовпці «Веб-додатки, не включені в групу» відображаються всі веб-додатки, доступні для адміністрування. Для переміщення відповідних веб-додатків в стовпець «Веб-додатки, включені в групу», потрібно використовувати кнопки зі стрілками. Однострілкові кнопки переміщують вибраний веб-додаток, тоді як двострілкові кнопки переміщають всі веб-додатки з одного стовпця в інший (рис.3.9).

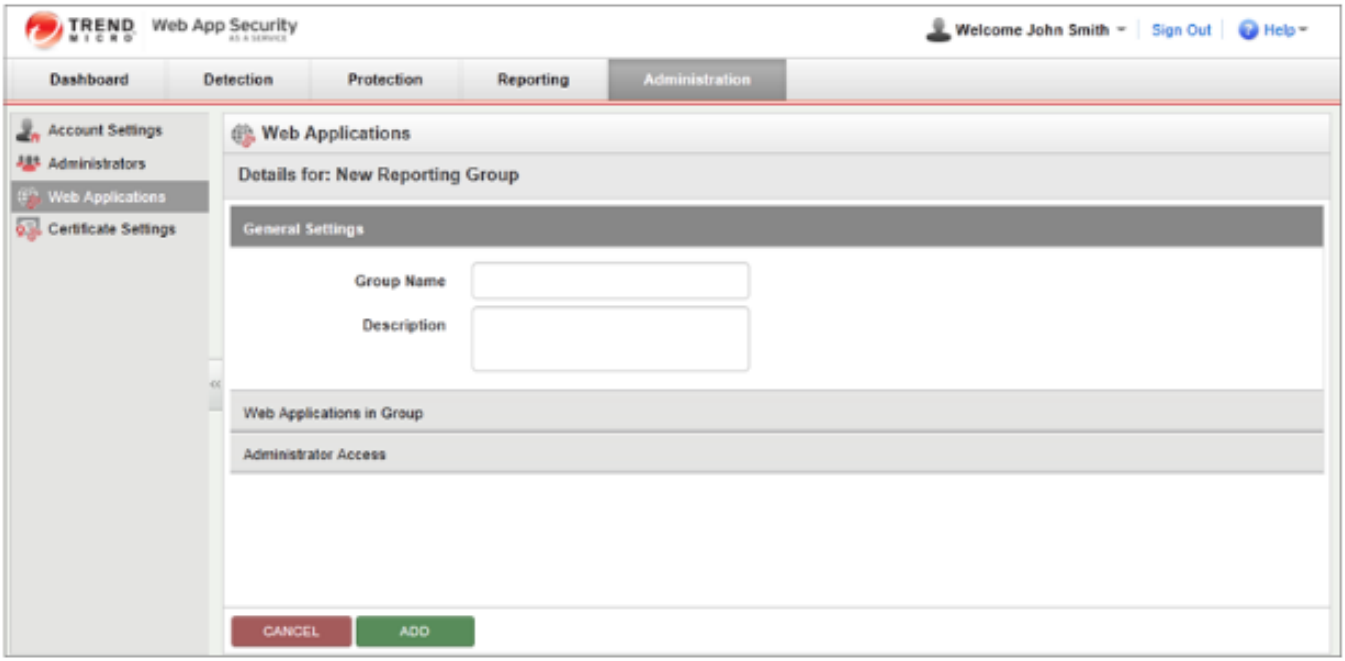


Рис.3.9. Налаштування Deep Security для веб-додатків

Додавання нових веб-додатків до групи. Якщо необхідно додати веб-додатки, які відсутні у списку, спочатку потрібно додати їх до облікового запису. Після цього можна продовжити процедуру та редагувати веб-додаток для додавання адміністраторів.

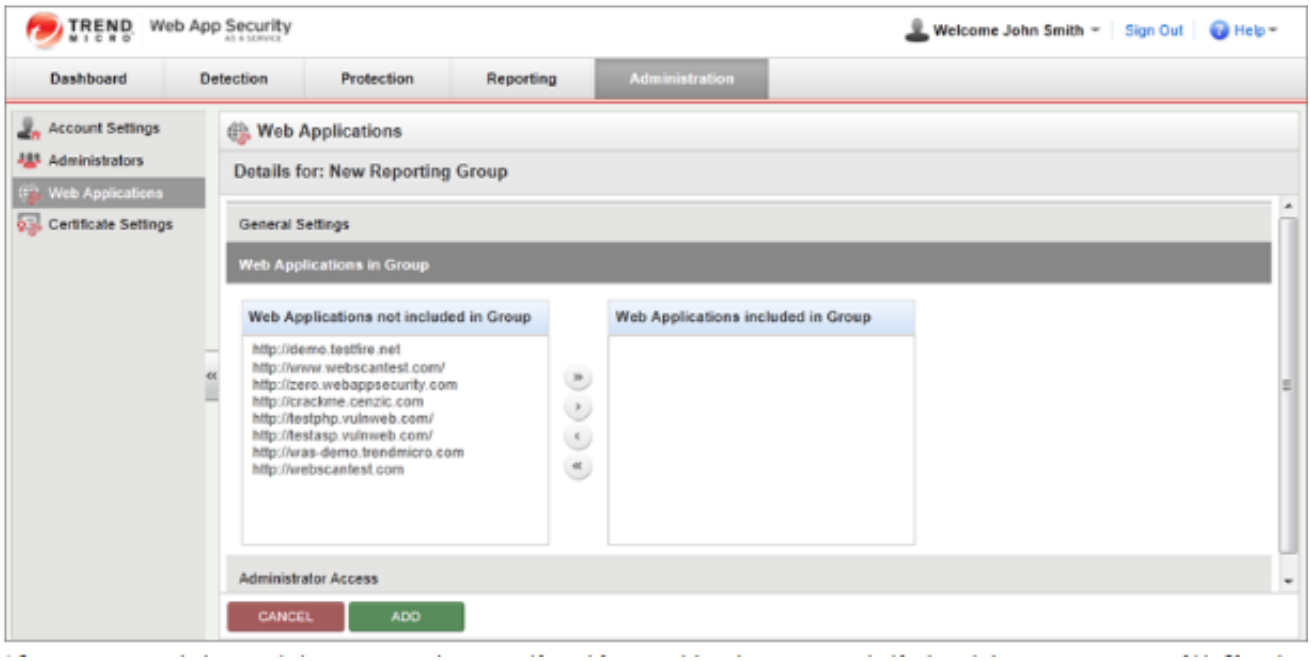


Рис.3.10. Приклад **додавання нових веб-додатків до групи**

Управління доступом адміністраторів до групи веб-додатків. Потрібно клацнути на «Доступ адміністратора». У стовпці «Адміністратори без доступу до профілю» відображаються всі адміністратори, пов'язані з обліковим записом. Особи, що перелічені в стовпці «Адміністратори з доступом до профілю», матимуть можливість вносити зміни до налаштувань цієї групи додатків.

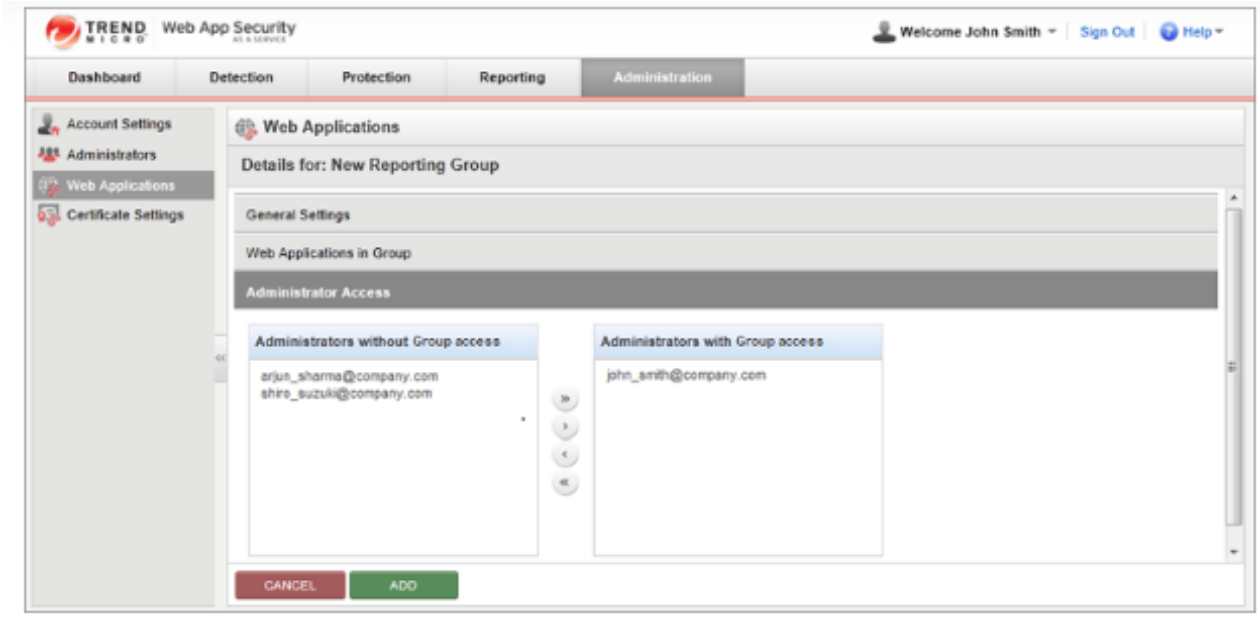


Рис.3.11. Управління доступом адміністраторів до групи веб-додатків

Для переміщення адміністраторів між стовпцями також потрібно використовувати кнопки зі стрілками. Однострілкові кнопки служать для переміщення окремого адміністратора, тоді як двострілкові кнопки переміщають всіх адміністраторів.

Додавання нових адміністраторів до групи. Якщо потрібно додати адміністраторів, які відсутні у списку, спочатку необхідно додати їх до облікового запису. Потім можна продовжити процедуру та редагувати групу для додавання відсутніх адміністраторів.

Підтвердження внесених змін. Після завершення налаштувань потрібно клацнути «Додати». У вікні підтвердження, яке з'явиться, потрібно клацнути «ОК» для фіналізації процесу[25].

3.4. Рекомендації до налаштувань Trend Micro

Для забезпечення ефективного захисту веб-ресурсів важливо налаштувати та використовувати належні інструменти та процедури, особливо в контексті систем безпеки, таких як Trend Micro.

Пересилання журналів Cloud Syslog. Для вимкнення пересилання журналів Cloud Syslog потрібно видалити «Адресу сервера» у налаштуваннях. Це призведе до того, що дані не будуть відправлятися до Trend Micro.

Налаштування розташовані в розділі консолі під назвою «Журнали та звіти» - «Cloud Syslog Forwarding». Потрібно вибрати опцію «Увімкнути» та внести зміни в «Адресу сервера».

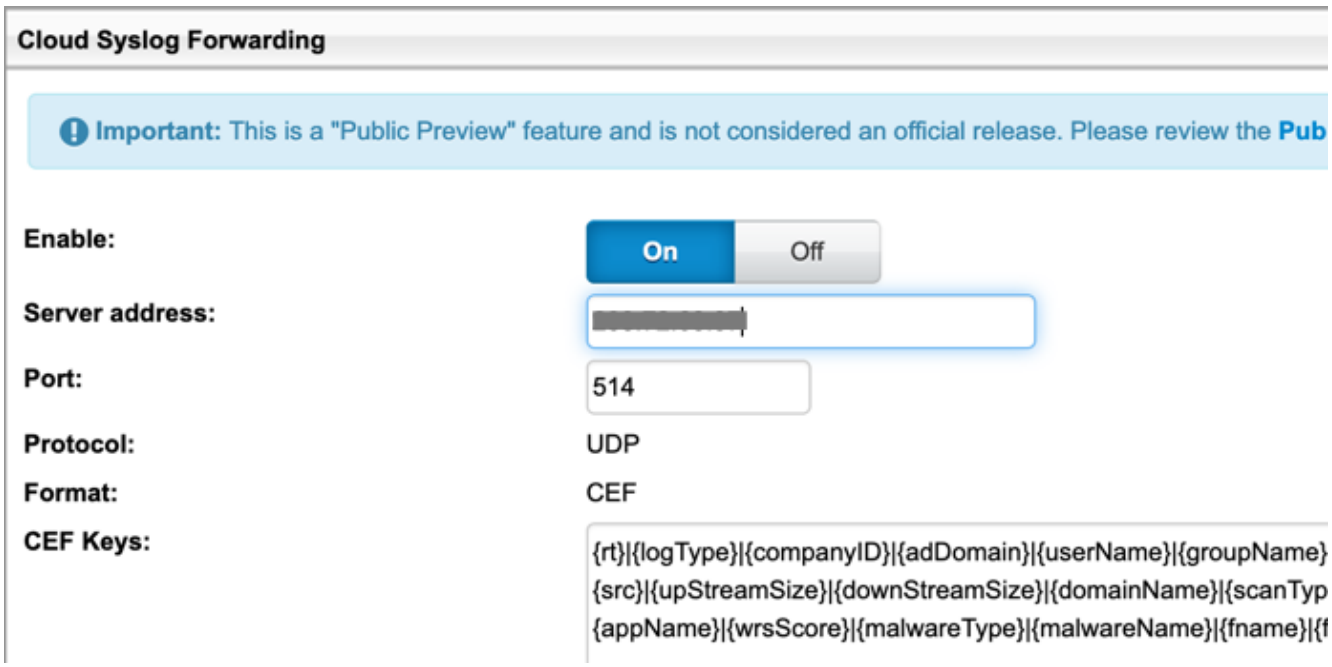


Рис.3.12. Налаштування Cloud Syslog

Аутентифікація через Okta. Для запобігання неналежному відправленню даних до Trend Micro, потрібно уникати завантаження фальшивого сертифіката та очищати вміст текстового поля при виборі методу аутентифікації.

Розташування налаштувань для аутентифікації Okta знаходиться в «Адміністрування» - «Служби каталогів». Потрібно перейти за посиланням «Натиснути тут» і вибрати метод автентифікації «Okta», де налаштовуються «URL-адреса сервера» та «Публічний сертифікат SSL».

Аутентифікація через Microsoft Entra ID. Подібно до Okta, для аутентифікації через Microsoft Entra ID, потрібно уникати завантаження фальшивих сертифікатів і очищати вміст текстового поля для забезпечення коректної передачі даних до Trend Micro.

Налаштування для аутентифікації через Microsoft Entra ID розташовані в «Адміністрування» - «Служби каталогів». Потрібно перейти за посиланням «Натиснути тут» та вибрати метод автентифікації «Microsoft Entra ID», де потрібно налаштувати «URL-адресу сервера» та «Публічний сертифікат SSL» (рис.3.13).

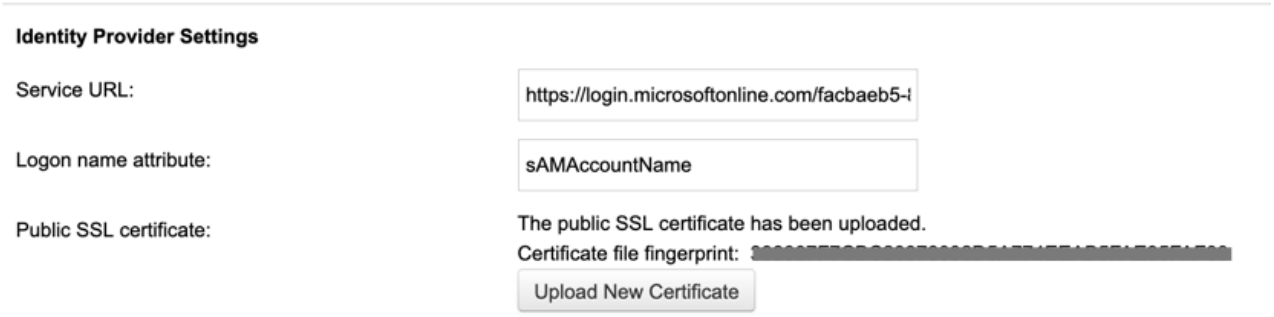


Рис.3.13. Налаштування публічного сертифікату SSL

Віртуальний шлюз (Virtual Gateway). Віртуальні шлюзи веб-безпеки Trend Micro перевіряють та фільтрують мережевий трафік користувачів на основі налаштованих політик (рис.3.14). Це захищає організацію від мережевих загроз. Для вимкнення віртуальних шлюзів потрібно перейти за посиланням «Шлюзи» - «Додати/змінити віртуальний шлюз» - «Основна інформація».

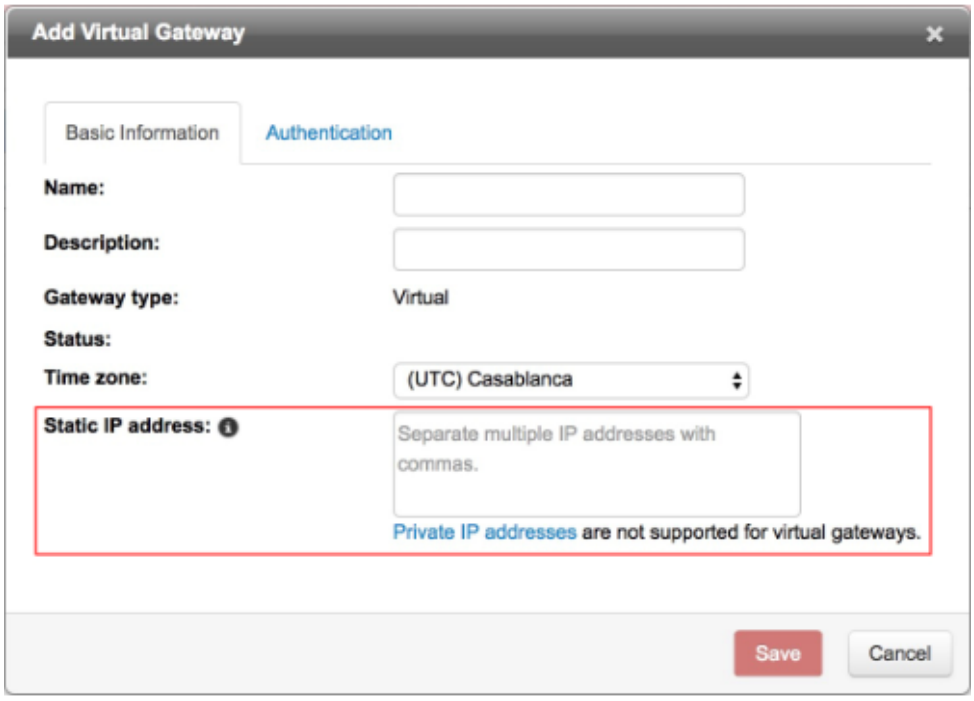


Рис.3.14. Налаштування віртуального шлюзу

Вимкнення віртуальних шлюзів може блокувати відсилання даних до Trend Micro, але перед доступом до Інтернет-сервісів потрібно буде аутентифікуватись за допомогою імені користувача та паролю[26].

Шлюз (On-Premises Gateway). Шлюзи від Trend Micro Web Security здійснюють інспекцію та фільтрацію мережевого трафіку на основі налаштованих політик. При вимкненні шлюзів, трафік користувачів потрібно передавати у хмару Trend Micro Web Security. Це допомагає уникнути відсилання зазначених даних до Trend Micro, забезпечуючи при цьому адекватний рівень безпеки.

Віртуальний аналізатор (Virtual Analyzer). Віртуальний аналізатор є хмарною пісочницею, призначеною для аналізу підозрілих об'єктів. Він дозволяє спостерігати за поведінкою файлів у середовищі, що моделює кінцеві точки мережі без ризику компрометації (рис.3.15).

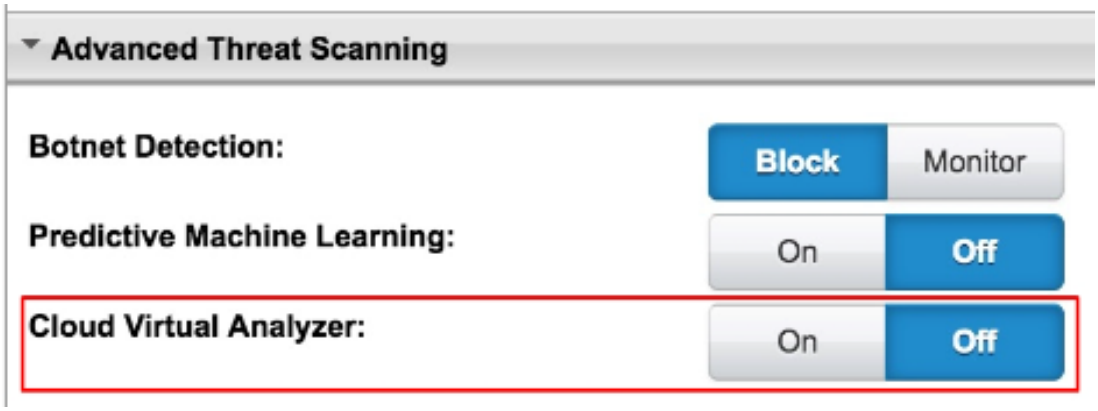


Рис.3.15. Активація віртуального аналізатора

Вимкнення віртуального аналізатора впливає на можливість Trend Micro Web Security виявляти видачу вірусів, тому це може серйозно знизити рівень захисту від кіберзагроз.

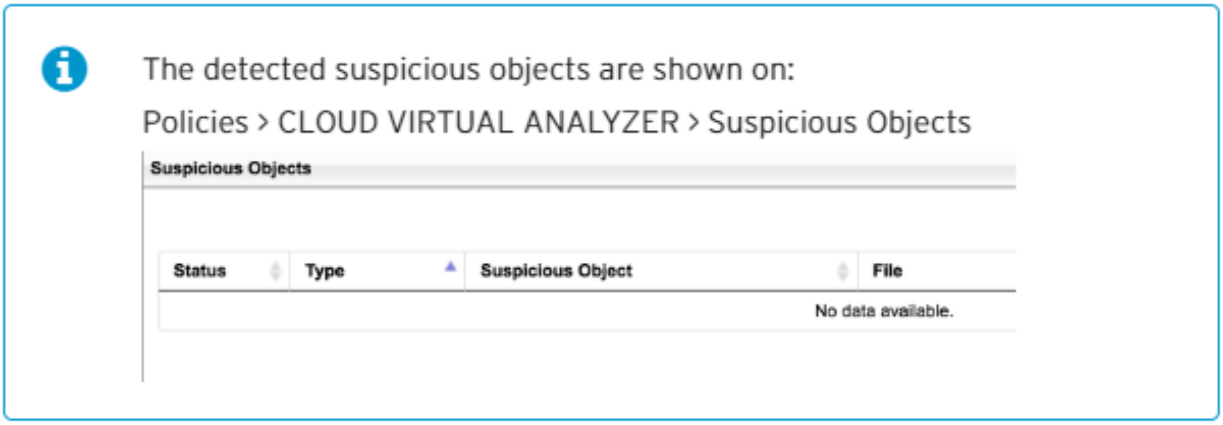


Рис.3.16. Налаштування віртуального аналізатора

Збір даних для захисту від загроз. Зібрані дані включають IP-адреси, URL-адреси, імена хостів та імена файлів/шляхи. Налаштування для захисту від загроз можна знайти за допомогою переходу в «Політики розташування консолі» - «Захист від загроз» - «Додати/Редагувати» - «Розширене сканування загроз».

Веб-репутація. Trend Micro Web Security використовує служби Web Reputation Services для сканування URL-адрес. Вимкнення Web Reputation може вплинути на здатність системи виявляти шкідливі URL-адреси.

Налаштування веб-репутації знаходяться в «Політики розташування консолі» - «Захист від загроз» - «Додати/Редагувати» - «Веб-репутація».

Прогнозне машинне навчання. Використовує передові технології машинного навчання для аналізу загроз. Вимкнення цієї функції може зменшити здатність системи виявляти нові або невідомі загрози.

Налаштування прогнозного машинного навчання доступні в «Політики розташування консолі» - «Захист від загроз» - «Додати/Редагувати» - «Розширене сканування загроз».

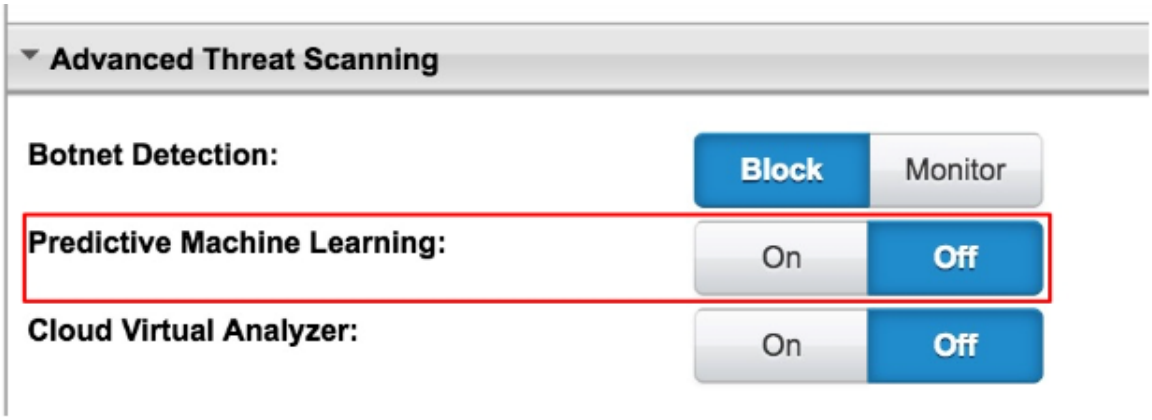


Рис.3.17. Налаштування машинного навчання

Перевірка HTTPS. Дозволяє адміністраторам встановлювати довірчі зв'язки між сертифікатами. Вимкнення перехресного підпису сертифіката або керування сертифікатами може призвести до відображення попереджень про сертифікат в клієнтських браузерах. Налаштування перевірки HTTPS розташовані в «Політики розташування консолі» - «Глобальні налаштування» - «Перевірка HTTPS».

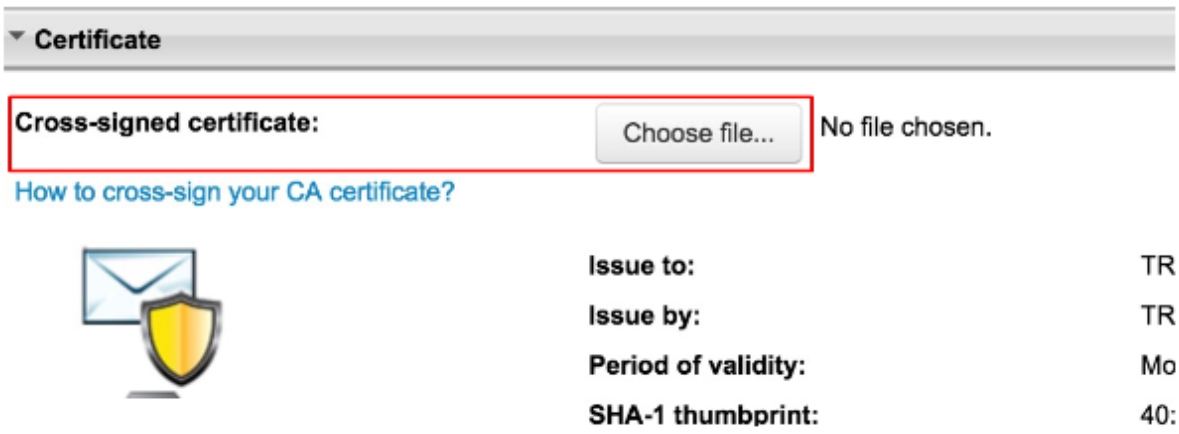


Рис.3.18. Налаштування сертифікації

Тунелювання HTTPS. Дозволяє управляти довіреними доменами, які не підпадають під дію політик Trend Micro Web Security. Вимкнення тунелювання HTTPS може призвести до відображення сторінок помилок при невдалому дешифруванні HTTPS. Налаштування тунелювання HTTPS знаходяться в «Політики розташування консолі» - «Глобальні налаштування» - «Перевірка HTTPS».

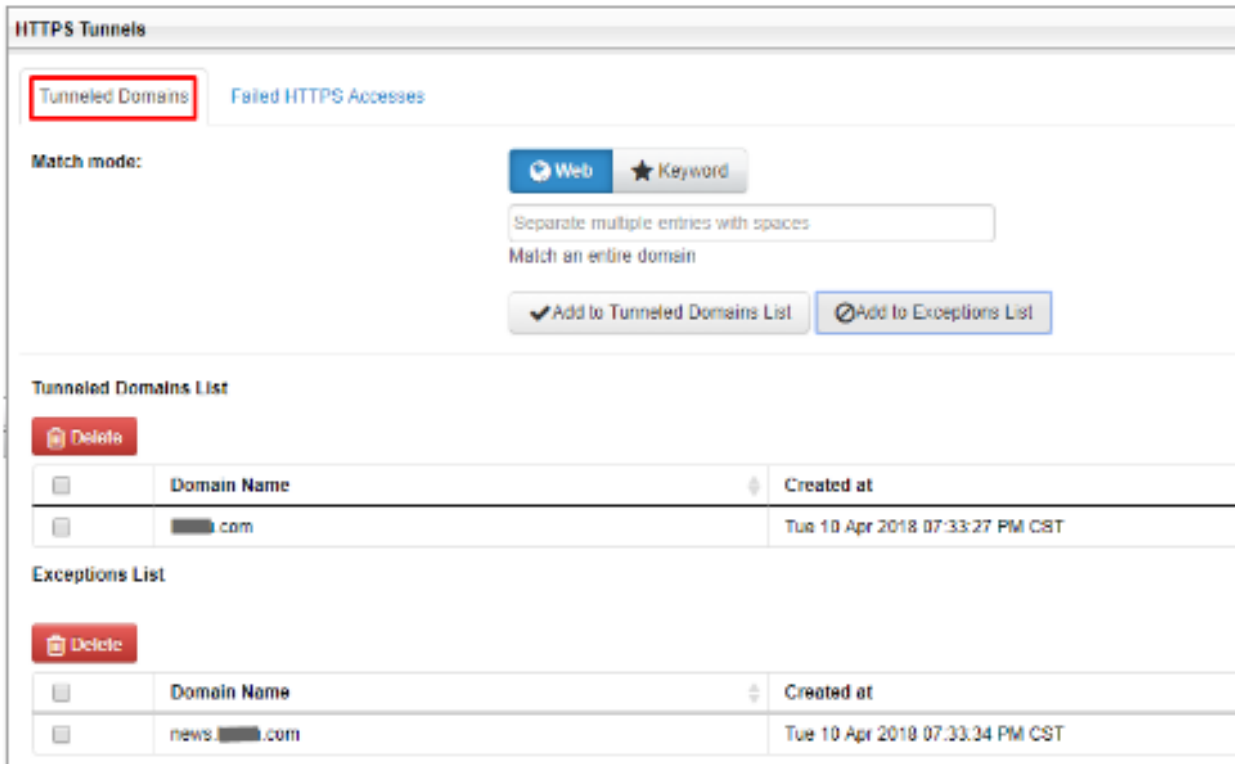


Рис.3.19. Налаштування тунелювання HTTPS

Зазначені інструменти та налаштування є важливими для захисту веб-ресурсів, оскільки вони дозволяють ефективно фільтрувати та аналізувати мережевий трафік, виявляти шкідливі URL-адреси та невідомі загрози, а також забезпечувати безпеку з'єднань HTTPS.

Налаштування категорії URL. Адміністраторам дозволяється додавати спеціальні категорії URL-адрес. Вимкнення налаштованих категорій URL-адрес може призвести до неможливості застосування налаштованих політик Trend Micro до URL-адрес, які не входять до попередньо визначених категорій.

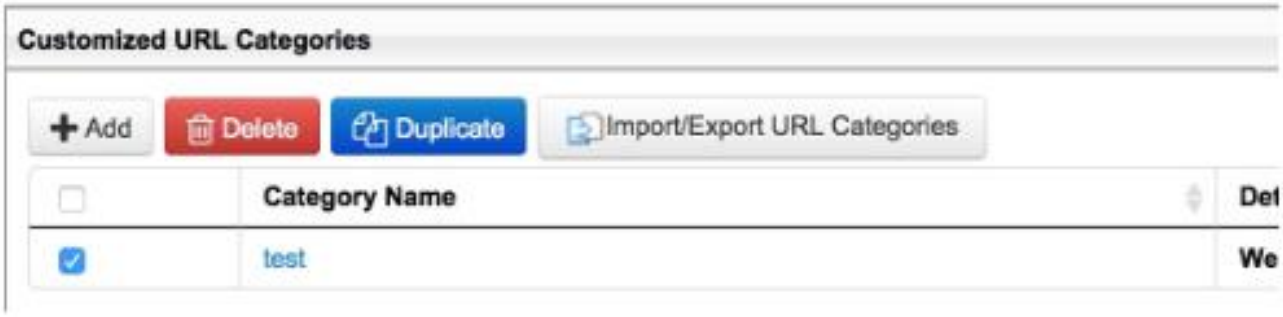


Рис.3.20. Налаштування категорії URL

Групи IP-адрес. Адміністраторам дозволяється додавати групи IP-адрес. Вимкнення груп IP-адрес може призвести до незастосування налаштованих політик чи параметрів на основі цих IP-адрес. Для налаштування доступні за посиланням «Політики розташування консолі» - «Об’єкти» - «Налаштування категорії URL-адрес».

Аналіз журналу. Журнали зберігаються протягом 181 дня. Журнали включають такі дані, як час збору даних, імена користувачів, кафедри, домени, URL-адреси та IP-адреси. Налаштування для аналізу журналів доступні в «Журнали та звіти» - «Аналіз журналів».

Вибрані журнали (Lod Favorites). Дозволяє адміністраторам зберігати умови запиту для швидкого доступу до журналів. Вимкнення вибраних журналів може потребувати встановлення умов запиту щоразу при пошуку в журналах. Налаштування доступні в «Журнали та звіти» - «Вибраний журнал».

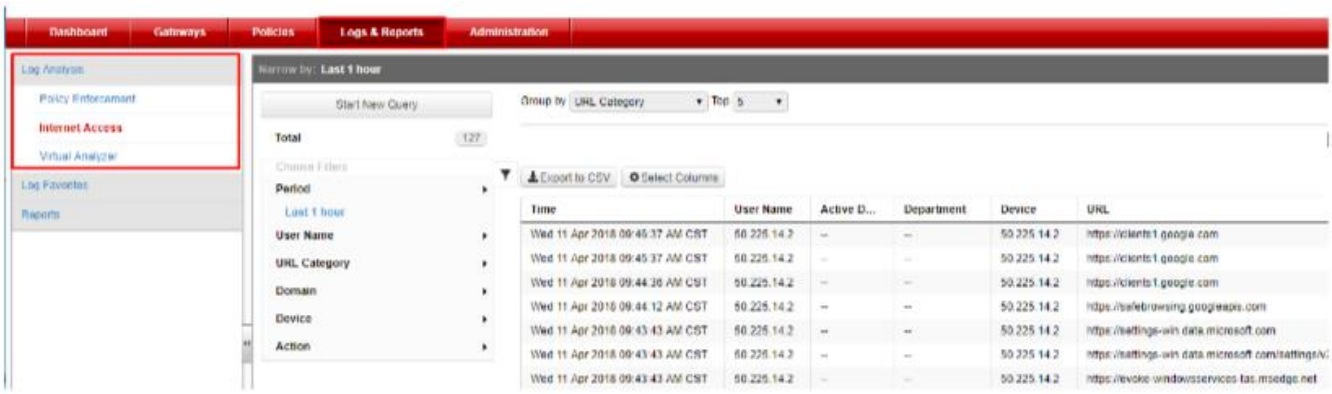


Рис.3.21. Налаштування вибраних журналів

Звіти. Вимкнення звітів може перешкоджати аналізу загроз та пов'язаних із безпекою подій. Розташування для управління звітами знаходиться в «Журнали та звіти» - «Звіти» на консолі. Параметри консолі дозволяють додавати, дублювати або редагувати звіти.

Файли PAC. Використовуються для пересилання веб-трафіку до Trend Micro Web Security. Вимкнення файлів PAC може призвести до того, що деякі веб-сайти не відкриватимуться. Налаштування знаходяться в «Адміністрування» - «Розгортання сервісу» - «Файли PAC», де можна додавати, створювати копії або редагувати файли PAC.

Рис.3.22. Налаштування файлів PAC

Enforcement Agent. Використовується для збору даних, таких як IP-адреси клієнтів, назви програм, імена користувачів та ідентифікатори. Налаштування знаходяться в «Адміністрування» - «Розгортання служби» - «Enforcement Agent».

Зібрані дані можуть включати журнали налагодження поведінки агента, основну інформацію про мобільний телефон (модель пристрою, версія ОС Android, мова, версія агента TMWS).

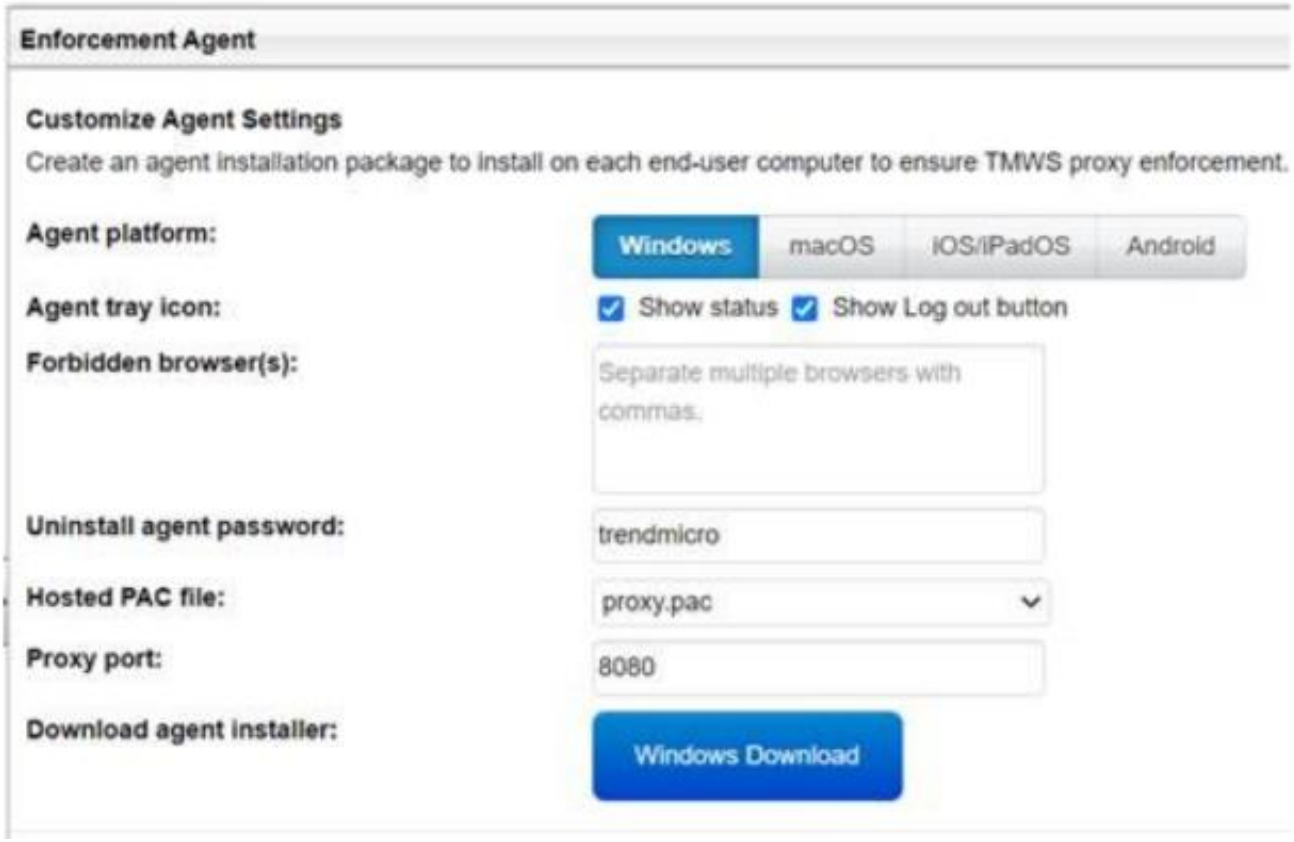


Рис.3.23. Налаштування Enforcement Agent

Збір даних через Trend Micro Web Security Agent. Дані, які збираються, можуть включати дані трафіку HTTP в браузері, токени, а також основну інформацію про мобільні пристрої. Збір даних може бути вимкнений або включений залежно від налаштувань розгортання через Microsoft Intune та інші параметри. Налаштування знаходяться в «Адміністрування» - «Розгортання сервісу» - «Enforcement Agent».

Каталогові служби. Trend Micro Web Security інтегрує домени Active Directory (AD) для автентифікації користувачів AD. Вимкнення служб каталогів

може призвести до того, що Trend Micro Web Security не буде автентифікувати користувачів AD та застосовувати до них політики. Для налаштування потрібно перейти за посиланням «Адміністрування» - «Користувачі та автентифікація» - «Служби каталогів».

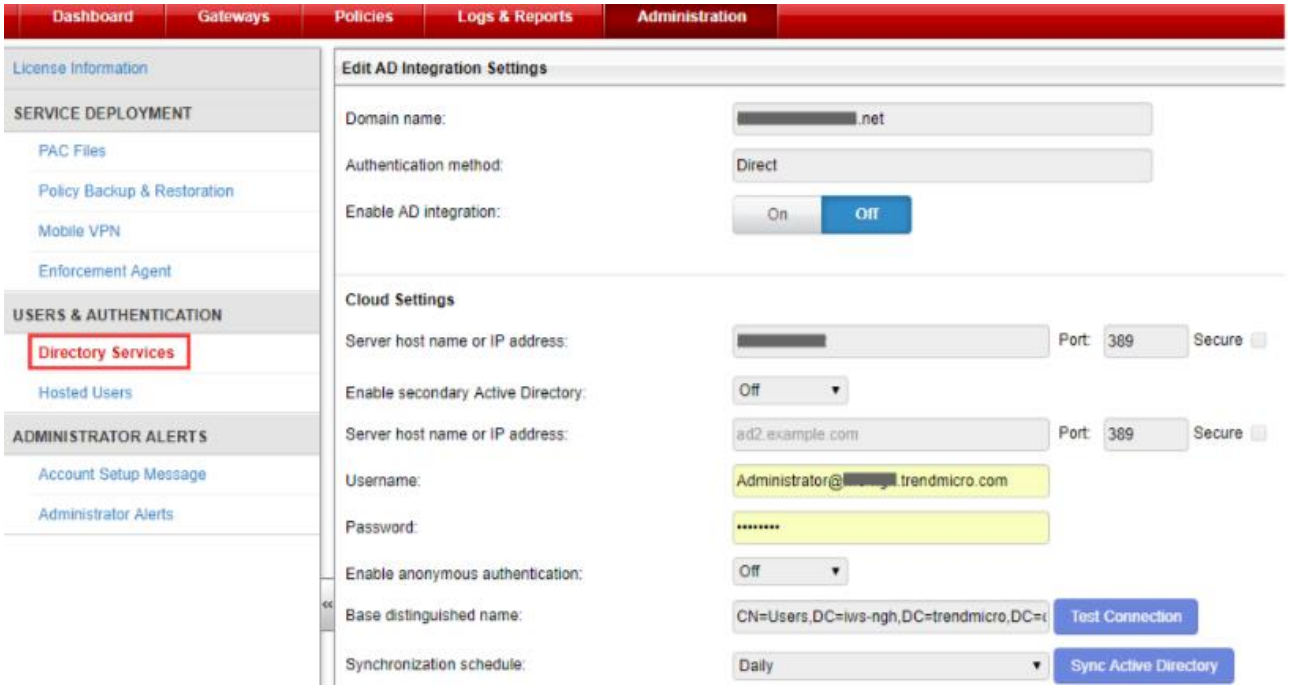


Рис.3.24. Налаштування каталогових служб

Автентифікація SAML. Використовується для інтеграції AD та автентифікації користувачів AD. Вимкнення автентифікації SAML може вплинути на автентифікацію ADFS користувачів AD.

Налаштування знаходяться в «Адміністрування» - «Користувачі та автентифікація» - «Служби каталогів» - «Клацнути тут» - «SAML».

Автентифікація агента. Використовується для інтеграції AD і автентифікації користувачів AD. Вимкнення автентифікації агента може призвести до того, що Trend Micro Web Security не підтримуватиме автентифікацію агента для користувачів AD. Налаштування знаходяться в «Адміністрування» - «Користувачі та автентифікація» - «Служби каталогів» - «Клацнути тут» - «Агент».

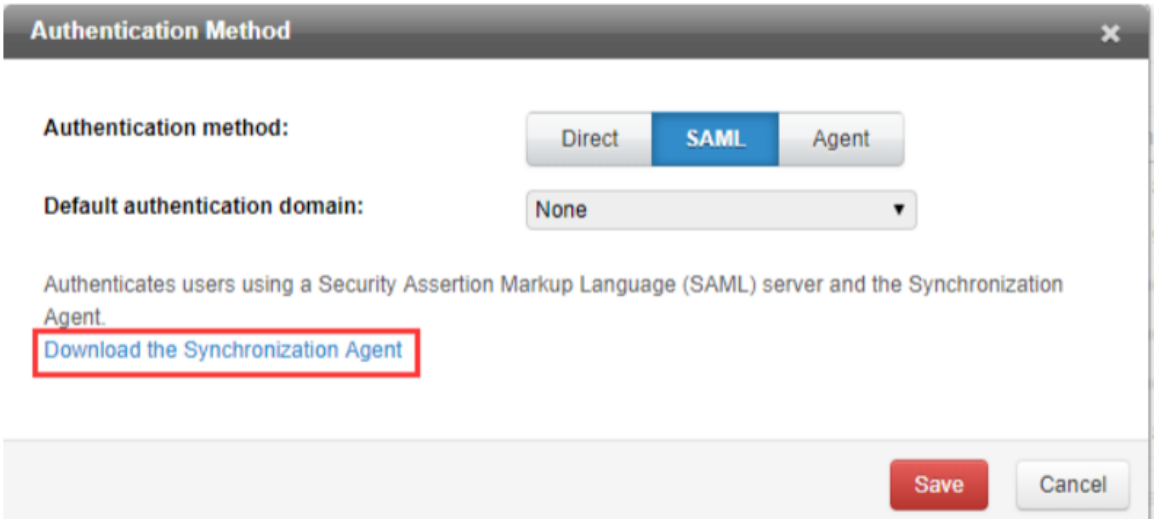


Рис.3.25. Налаштування агента автентифікації

Агент синхронізації. Використовується для синхронізації інформації про користувачів AD. Вимкнення агента синхронізації може призвести до неможливості синхронізації користувачів AD для автентифікації за допомогою SAML або агента. Налаштування знаходяться в «Адміністрування» - «Користувачі та автентифікація» - «Служби каталогів» - «Клацнути тут» - «SAML/Агент».

Розміщені користувачі. Підтримка розміщених облікових записів дозволяє користувачам пересилати веб-трафік через Trend Micro Web Security. Вимкнення розміщених користувачів призведе до неможливості перенаправлення їхнього мережевого трафіку через Trend Micro Web Security для застосування політики. Для налаштування потрібно перейти за посиланням «Адміністрування» - «Користувачі та автентифікація» - «Розміщені користувачі».

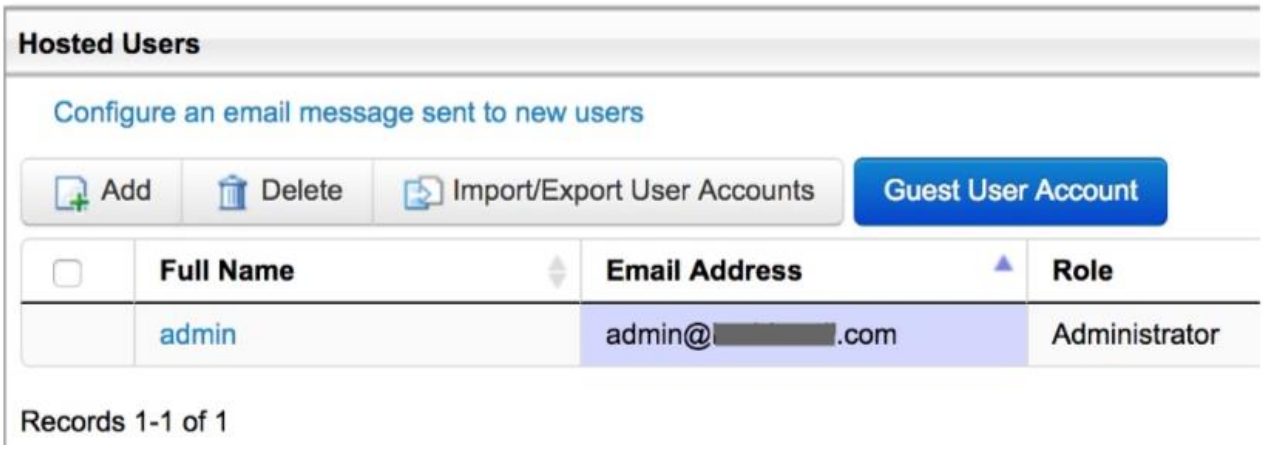


Рис.3.26. Налаштування розміщених користувачів

Сповіщення адміністратора. Використовуються для сповіщення адміністраторів про певні події. Вимкнення сповіщень може призвести до того, що адміністратори не отримуватимуть інформацію про важливі події для моніторингу активності користувачів. Налаштування розташовані в «Адміністрування» - «Сповіщення адміністратора» - «Сповіщення адміністратора».

Контроль пропускної здатності. Забезпечує справедливий доступ до мережевих ресурсів для всіх користувачів.

Вимкнення контролю пропускної здатності призведе до неможливості контролю мережевого трафіку користувачів.

Налаштування знаходяться в «Шлюзи» - «Редагувати локальний шлюз» - «Контроль пропускної здатності».

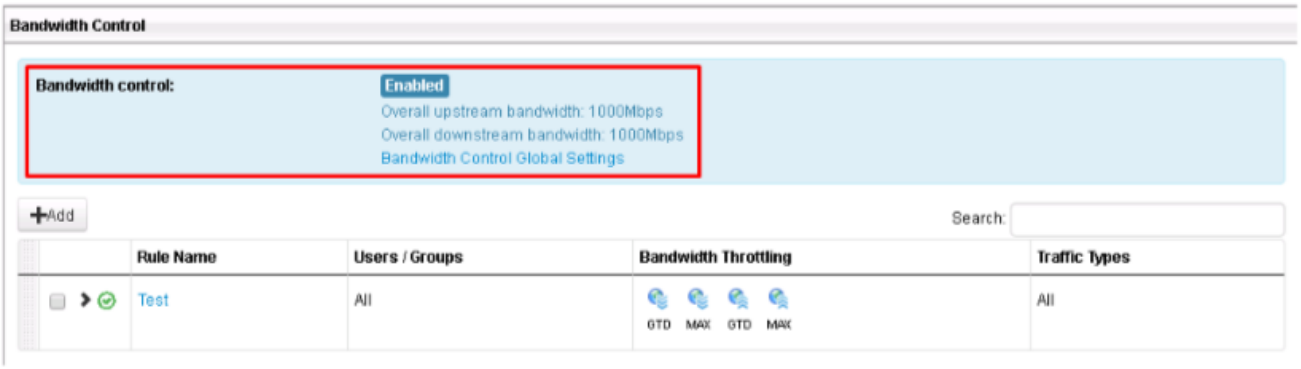


Рис.3.27. Налаштування пропускної спроможності

Схвалені/заблоковані URL-адреси. Дозволяє адміністраторам визначати довірені та заборонені веб-сайти. Вимкнення цієї функції перешкоджає встановленню постійного доступу або блокуванню певних веб-сайтів. Налаштування доступні в «Політика розташування консолі» - «Схвалені/заблоковані URL-адреси».

Цифрові сертифікати. Важливі для встановлення довірчих зв'язків і безпеки HTTPS-з'єднань.

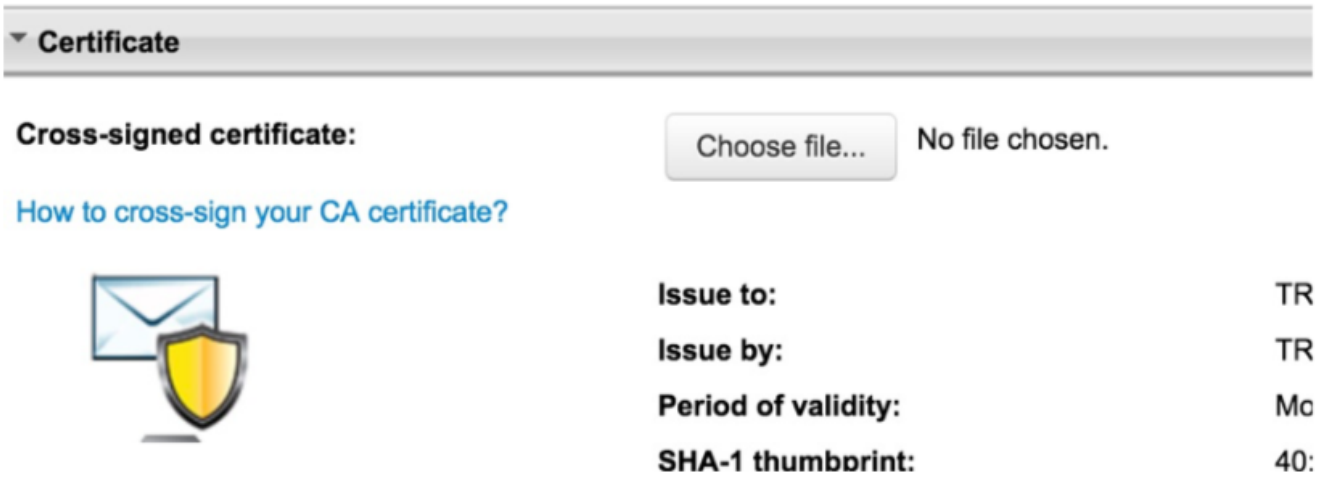


Рис.3.28. Налаштування цифрових сертифікатів

Вимкнення перехресного підпису сертифікатів може призвести до попереджень у браузерах клієнтів. Налаштування розташовані в «Політики» - «Глобальні налаштування» - «Перевірки HTTPS» - «Розширені налаштування».

Sync Agent. Використовується для синхронізації інформації користувачів AD. Налаштування розташовані в «Адміністрування» - «Користувачі та автентифікація» - «Служба каталогів» - «Натиснути тут» - «AD FS/Агент»[27].

Висновки до 3 розділу

Досліджено використання AWS для захисту веб-ресурсів, включаючи важливість Amazon VPC, яка дозволяє ізолювати ресурси у приватній мережі, використовуючи NAT, ACL для VPC, налаштування груп безпеки VPC та налаштування журналів потоків для VPC.

Виявлено, що AWS Security Hub є ключовим інструментом для перевірки відповідності стандартам безпеки, інтегруючи дані з різних AWS служб.

Виокремлено значення AWS Identity and Access Management (IAM) у забезпеченні безпечного доступу до ресурсів Amazon, включаючи використання багатофакторної аутентифікації та політик паролів.

Зазначено, що AWS Route 53 включає DNSSEC для захисту веб-ресурсів від атак, пов’язаних з DNS.

Розроблено стратегію інтеграції AWS WAF для захисту веб-ресурсів від різноманітних загроз, включаючи OWASP top 10.

Описано роль AWS Shield у захисті від DDoS-атак та AWS CloudFront як CDN-рішення для покращення швидкості завантаження веб-ресурсів і захисту від DoS/DDoS-атак.

Виявлено, що Trend Micro Web App Security та Imperva SecureSphere пропонують інтегроване рішення для виявлення вразливостей та захисту веб-додатків, у тому числі відповідність PCI DSS 6.6.

Оцінено важливість створення та налаштування груп веб-додатків у Deep Security для веб-додатків, з метою підвищення захисту веб-ресурсів через управління групами веб-додатків із різними адміністративними правами.

Визначено важливість захисту веб-ресурсів через налаштування Trend Micro, включаючи пересилання журналів Cloud Syslog, аутентифікацію Okta та Microsoft Entra ID, віртуальні шлюзи, контроль пропускної здатності, звіти, файли PAC, і налаштування каталогових служб.

ВИСНОВКИ

В кваліфікаційній роботі отримано наступні наукові та науково-практичні результати:

1) Досліджено важливість захисту веб-ресурсів та проаналізовано різницю між веб-ресурсами та веб-додатками;

2) Проведено аналіз нормативно-правових актів України щодо інформаційної безпеки, що регулюють використання та захист веб-ресурсів;

3) Виокремлено різні категорії вразливостей та загроз веб-ресурсів. Досліджено категорії включають неперевірене введення, порушення контролю доступу, проблеми з автентифікацією та керуванням сеансами, міжсайтовий сценарій (XSS), переповнення буфера, введення команд, неналежна обробка помилок, незахищене зберігання даних, а також відмова в обслуговуванні;

4) Виокремлено значення фреймворку WS-Security для захисту веб-ресурсів. Фреймворк WS-Security інтегрує різні технології безпеки, що допомагає забезпечити консистентність та стандартизацію в захисті веб-ресурсів;

5) Досліджено використання AWS для захисту веб-ресурсів. Виокремлено значення AWS Identity and Access Management (IAM) у забезпеченні безпечного доступу до ресурсів Amazon, включаючи використання багатофакторної аутентифікації та політик паролів.Розроблено стратегію інтеграції AWS WAF для захисту веб-ресурсів від різноманітних загроз, включаючи OWASP top 10;

6) Оцінено важливість створення та налаштування груп веб-додатків у Deep Security для веб-додатків, з метою підвищення захисту веб-ресурсів через управління групами веб-додатків із різними адміністративними правами;

7) Розроблено рекомендації щодо захисту веб-ресурсів через налаштування Trend Micro, включаючи пересилання журналів Cloud Syslog, аутентифікацію Okta та Microsoft Entra ID, віртуальні шлюзи, контроль пропускної здатності, звіти, файли PAC, і налаштування каталогових служб.

ПЕРЕЛІК ПОСИЛАНЬ

1. Introduction To Web Resource. [Електронний ресурс] - Режим доступу: https://ecomputernotes.com/servlet/intro/introductiontowebresource
2. Website Security Statistics Report. [Електронний ресурс] - Режим доступу: https://info.whitehatsec.com/Website-StatsReport-2015.html
3. OWASP. Types of Cross-Site Scripting. [Електронний ресурс] - Режим доступу: https://www.owasp.org/index.php/Types_of_Cross-Site_Scripting
4. Закон України «Про захист персональних даних». [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text
5. Закон України «Про захист персональних даних». [Електронний ресурс] - Режим доступу: https://ips.ligazakon.net/document/T102297
6. Закон України «Про інформаційну безпеку України». [Електронний ресурс] - Режим доступу: https://ips.ligazakon.net/document/JG3TH00A
7. Закон України «Про інформаційну безпеку України». [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/685/2021#Text
8. Закон України «Про рекламу». [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80#Text
9. Закон України «Про основні засади забезпечення кібербезпеки України». [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text
10. ISO/IEC 27001. [Електронний ресурс] - Режим доступу: https://www.iso.org/standard/27001
11. ISO/IEC 27001:2013. [Електронний ресурс] - Режим доступу: http://www.itgivernance.co.uk/standards.arx
12. General Data Protection Regulation. [Електронний ресурс] - Режим доступу: http://surl.li/oelsi
13. НАТО Cyber Defence Pledge. [Електронний ресурс] - Режим доступу:

https://www.nato.int/cps/uk/natohq/photos_208931.htm

14. Defining Incident Management Processes for CSIRTs: A Work in Progress. CMU/SEI-2004-TR-015: ESC-TR-2004-015 Chris Alberts, Audrey

15. Web Services Security [Електронний ресурс] - Режим доступу: https://cdn.ttgtmedia.com/searchWebServices/downloads/Newcomer_08.pdf

16. OWASP. Cross-site Scripting (XSS). [Електронний ресурс] - Режим доступу: https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

17. OWASP. [Електронний ресурс] - Режим доступу: https://www.owasp.org/index.php/Main_Page

18. W3C. Same Origin Policy. [Електронний ресурс] - Режим доступу: https://www.w3.org/Security/wiki/Same_Origin_Policy

19. HTTP: The Definitive Guide by David Gourley, Brian Totty, Marjorie Sayer, Anshu Aggarwal, Sailu Reddy. [Електронний ресурс] - Режим доступу: https://www.oreilly.com/library/view/http-the-definitive/1565925092/ch01s03.html

20. Amazon Virtual Private Cloud (VPC). [Електронний ресурс] - Режим доступу: https://docs.aws.amazon.com/toolkit-for-visual-studio/latest/user-guide/vpc-tkv.html

21. Service networks in VPC. [Електронний ресурс] - Режим доступу: https://docs.aws.amazon.com/vpc-lattice/latest/ug/service-networks.html

22. AWS Security Hub. [Електронний ресурс] - Режим доступу: https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html

23. AWS Security Hub features. [Електронний ресурс] - Режим доступу: https://aws.amazon.com/ru/security-hub/features/

24. Protection your web applications. [Електронний ресурс] - Режим доступу: https://www.imperva.com/docs/SB_Imperva_Trend_Micro.pdf

25. SecureSphere. . [Електронний ресурс] - Режим доступу: https://www.imperva.com/resources/datasheets/DS_SecureSphere_Management_Solutions.pdf

26. Deep Security. [Електронний ресурс] - Режим доступу: https://success.trendmicro.com/dcx/s/solution/1097574-adding-groups-in-deep-security-

for-web-apps-2-0?language=en_US&sfdcIFrameOrigin=null

27. Trend Micro Web Security Data Collection Notice. [Електронний ресурс] - Режим доступу: https://success.trendmicro.com/dcx/s/solution/1119974-trend-micro-web-security-data-collection-notice?language=en_US&sfdcIFrameOrigin=null

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА
НА ТЕМУ:

«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ЗАХИСТУ WEB-РЕСУРСІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ»

Виконав:
здобувач вищої освіти
групи БСДМ-63
ЧЕРНЕГА Станіслав

Керівник:
к.т.н, доцент кафедри
БОРСУКОВСЬКИЙ Юрій

Київ 2024

- *Об'єкт дослідження* – процес безпечного функціонування Web-ресурсів.
- *Предмет дослідження* – технології та засоби забезпечення безпеки Web-ресурсів в інформаційній системі організації.
- *Мета роботи* – підвищення рівня інформаційної безпеки в організації шляхом впровадженню технічних та програмних рішень для посилення безпеки Web-ресурсів.

Наукові завдання:
- проаналізувати важливість захисту веб-ресурсів;
- проаналізувати нормативно-правові актів України щодо інформаційної безпеки, що регулюють використання та захист веб-ресурсів;
- дослідити категорії вразливостей та загроз веб-ресурсів;
- розробити аналіз керівних принципів безпеки веб-ресурсів;
- дослідити використання AWS для захисту веб-ресурсів;
- розробити рекомендації щодо захисту веб-ресурсів через налаштування Trend Micro.

2

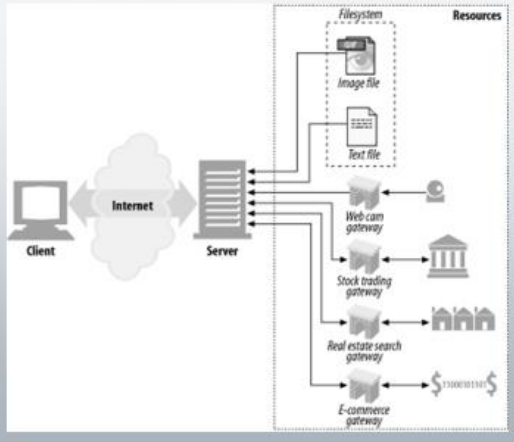


Рис.1.Приклад доступу до веб-ресурсу

3

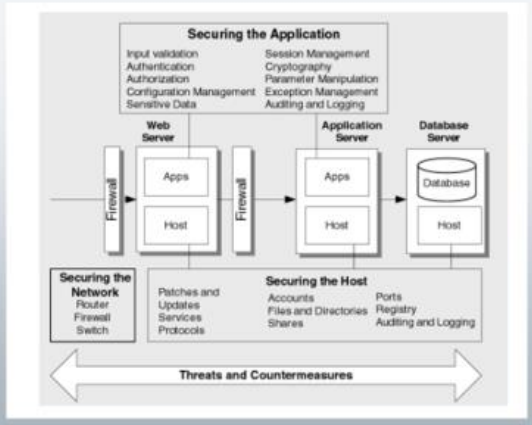


Рис.2. Приклад організації захисту 3-рівневої архітектури корпоративних веб-ресурсів

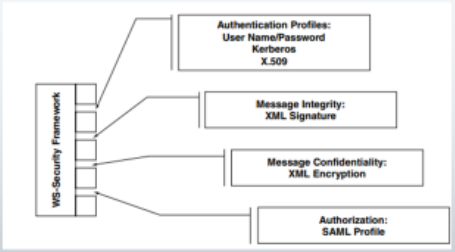
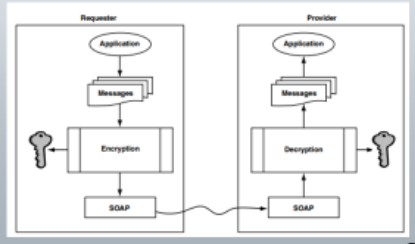


Рис.3. Складові фреймворку WS-Security

Рис.4. Шифрування у захисті повідомлень веб-ресурсів



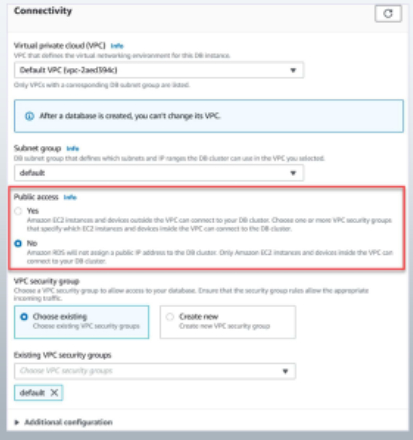


Рис.5. Налаштування груп безпеки VPC

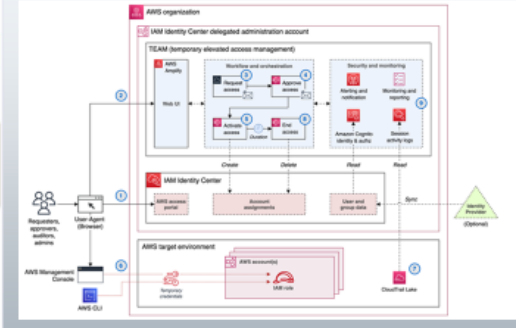


Рис.6. Архітектура AWS IAM

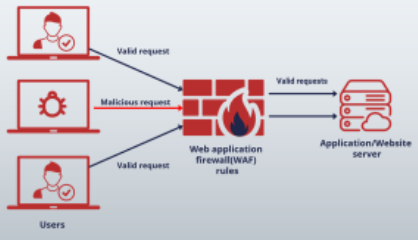


Рис.7. AWS Web Application Firewall (WAF)

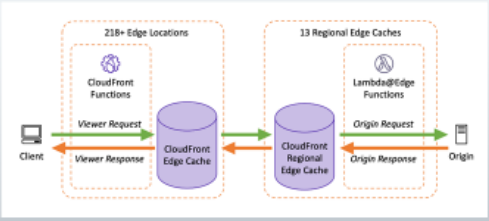


Рис.8. Приклад використання AWS CloudFront

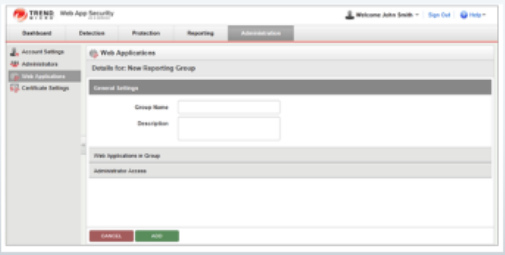
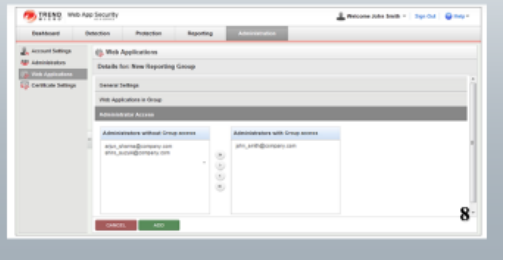


Рис.9. Налаштування Deep Security для веб-додатків

Рис.10. Управління доступом адміністраторів до групи веб-додатків



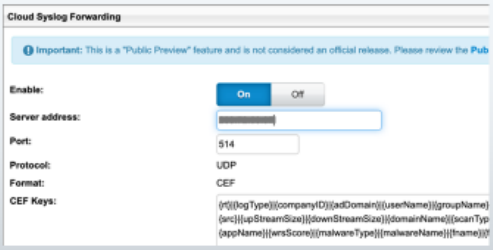


Рис.11. Налаштування Cloud Syslog

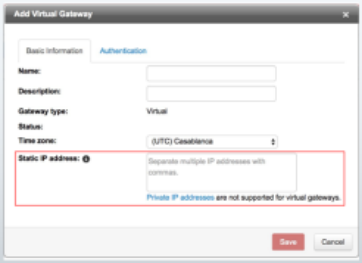


Рис.13. Налаштування віртуального шлюзу

Рис.12. Налаштування публічного сертифікату SSL

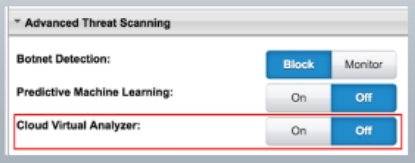


Рис.14. Активація віртуального аналізатора

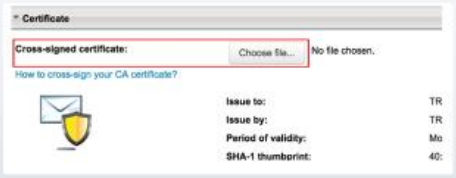


Рис.15. Налаштування сертифікації

Рис.16. Налаштування тунелювання HTTPS

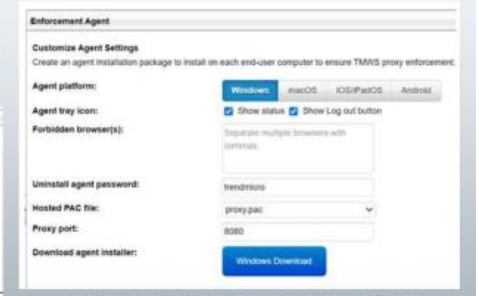


Рис.17. Налаштування Enforcement Agent

Висновки:

1. Досліджено важливість захисту веб-ресурсів та проаналізовано різницю між веб-ресурсами та веб-додатками;
2. Проведено аналіз нормативно-правових актів України щодо інформаційної безпеки, що регулюють використання та захист веб-ресурсів;
3. Виокремлено різні категорії вразливостей та загроз веб-ресурсів. Досліджено категорії включають неперевірене введення, порушення контролю доступу, проблеми з автентифікацією та керуванням сеансами, міжсайтовий сценарій (XSS), переповнення буфера, введення команд, неналежна обробка помилок, незахищене зберігання даних, а також відмова в обслуговуванні;
4. Виокремлено значення фреймворку WS-Security для захисту веб-ресурсів. Фреймворк WS-Security інтегрує різні технології безпеки, що допомагає забезпечити консистентність та стандартизацію в захисті веб-ресурсів;
5. Досліджено використання AWS для захисту веб-ресурсів. Виокремлено значення AWS Identity and Access Management (IAM) у забезпеченні безпечного доступу до ресурсів Amazon, включаючи використання багатофакторної аутентифікації та політик паролів.Розроблено стратегію інтеграції AWS WAF для захисту веб-ресурсів від різноманітних загроз, включаючи OWASP top 10;
6. Оцінено важливість створення та налаштування груп веб-додатків у Deep Security для веб-додатків, з метою підвищення захисту веб-ресурсів через управління групами веб-додатків із різними адміністративними правами;
7. Розроблено рекомендації щодо захисту веб-ресурсів через налаштування Trend Micro, включаючи пересилання журналів Cloud Syslog, аутентифікацію Okta та Microsoft Entra ID, віртуальні шлюзи, контроль пропускної здатності, звіти, файли PAC, і налаштування каталогових служб.