ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ В AZURE»

Виконав студент 6 курсу, групи БСДМ-63
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Макеєв К. А.
(прізвище та ініціали)
Керівник Собчук А. В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н. С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …… 10

ВСТУП ……..…… 10

1 **АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ ПРИ ЗАСТОСУВАННІ ХМАРНИХ ПЛАТФОРМ** 12

1.1 Дослідження проблеми захисту веб-додатків організації при застосуванні хмарних платформ ……. 12
1.2 Аналіз підходів до захисту веб-додатків організації при застосуванні хмарних платформ ……... 20
1.3 Аналіз існуючих рішень із захисту веб-додатків організації при застосуванні хмарних платформ ……..…..... 25

2 **АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ В AZURE** ……..…. 30

2.1 Призначення та основні функції брандмауера веб-додатків Azure 30
2.2 Призначення та основні функції брандмауера веб-додатків Azure на шлюзі додатків Azure …… 31
2.3 Призначення та застосування основних наборів правил брандмауера веб-додатків …….. 41

3 **ТЕХНОЛОГІЯ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ ПРИ ЗАСТОСУВАННІ ХМАРНИХ ПЛАТФОРМ** ……..……..……. 57

3.1 Порядок створення шлюзу додатку з брандмауером веб-додатку за допомогою порталу Azure …… 57
3.2 Технологія застосування рішення брандмауера веб-додатків на AzureFront Door …….. 63
3.3 Рекомендації щодо застосування технології захисту веб-додатків організації ……..……..…… 71

ВИСНОВКИ …….. 75

ПЕРЕЛІК ПОСИЛАНЬ 78

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 79

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

ACL – Access Control List

API – Application Programming Interface

APT – Advanced Persistent Threat

CDN – Content Delivery Network

CRS – Core Rule Sets

DDoS – Distributed Denial of Service

DNS – Domain Name System

IaaS – Infrastructure as a Service

ICMP – Internet Control Message Protocol

MFA – Multi-Factor Authentication

NTP – Network Time Protocol

OSI – Open Systems Interconnection model

OWASP – Open Web Application Security Project

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. Сьогодні сучасні організації широко використовують можливості хмарних платформ для розміщення в них своїх веб-додатків. Веб-додатки піддаються кібератакам зловмисників для досягнення ними різних злочинних цілей, що ще більш загострює проблему забезпечення безпеки інформаційних ресурсів організацій.

Використання незахищених веб-додатків в рази збільшує ризики несанкціонованого доступу до корпоративних ресурсів і порушення працездатності веб-сайтів, що веде до репутаційних, а також, фінансових втрат організацій. Застосування технології Web Application Firewall на сьогоднішній день є найбільш гнучким і точним інструментом для всебічного захисту від веб-загроз.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження технології захисту веб-додатків організації при застосуванні хмарних платформ на прикладі Azure.

Об'єкт дослідження – захист веб-додатків організації при застосуванні хмарних платформ.

Предмет дослідження – технологія захисту веб-додатків організації в Azure.

Мета роботи – розробити порядок застосування технології захисту веб-додатків організації при застосуванні хмарних платформ та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми захисту веб-додатків організації при застосуванні хмарних платформ;

проаналізувати підходи до захисту веб-додатків організації при застосуванні хмарних платформ;

проаналізувати існуючі рішення із захисту веб-додатків організації при застосуванні хмарних платформ;

проаналізувати методи та засоби захисту веб-додатків організації в Azure;

розкрити порядок реалізації технології захисту веб-додатків організації при застосуванні хмарних платформ.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології захисту веб-додатків організації при застосуванні хмарних платформ, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ ПРИ ЗАСТОСУВАННІ ХМАРНИХ ПЛАТФОРМ

1.1. Дослідження проблеми захисту веб-додатків організації при застосуванні хмарних платформ

У звіті 2022 року компанії Verizon зазначається, що базові атаки на веб-додатки зосереджуються на атаках, спрямованих безпосередньо на найбільш незахищену інфраструктуру організації, таку як веб-сервери. Ці інциденти використовують одну чи іншу з двох точок входу, використання викрадених облікових даних або використання вразливості [1].

Атаки на веб-додатки розподілені між двома областями. Першим є засоби доступу до сервера, такі як використання вкрадених облікових даних, використання вразливостей і підбір паролів. Другий представляє конкретне корисне навантаження, наприклад бекдори, які використовуються для підтримки постійності або монетизації доступу [1].

Verizon підкреслює, що переважно домінує використання викрадених облікових даних для доступу до інфраструктури організації, що виходить в Інтернет, як-от веб-серверів і серверів електронної пошти [1]. За 2022 було обліковано 4751 інцидент, у тому числі 1273 інцидент з підтвердженим розкриттям даних [1].

Типи злому веб-додатків показано на рис. 1.1. Найпопулярніші різновиди активів у базових атаках на веб-додатки показано на рис. 1.2.

Необхідно підкреслити, що підходи до забезпечення безпеки для веб-додатків докорінно змінилися. Сучасні веб-додатки важче захищати через те, як вони розроблені. Вони набагато більш відкриті та розподілені. Сучасний веб-додаток є сукупністю взаємодій між різними API, службами, кінцевими точками, пристроями тощо. Ці взаємодії охоплюють широкий діапазон кордонів як всередині організації, так і за її межами, і поверхню атаки, що постійно

розвивається, важко захистити.

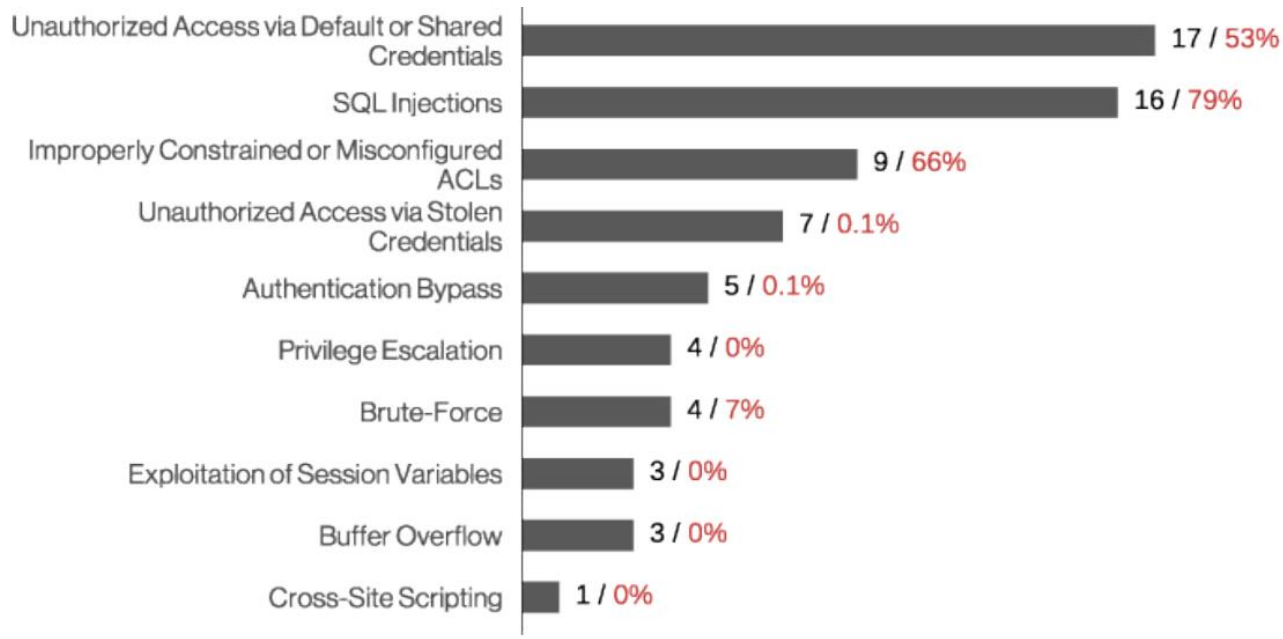

Рис. 1.1. Типи злому за кількістю порушень (чорним) і відсотком записів (червоним) (2009 DBIR) [1]

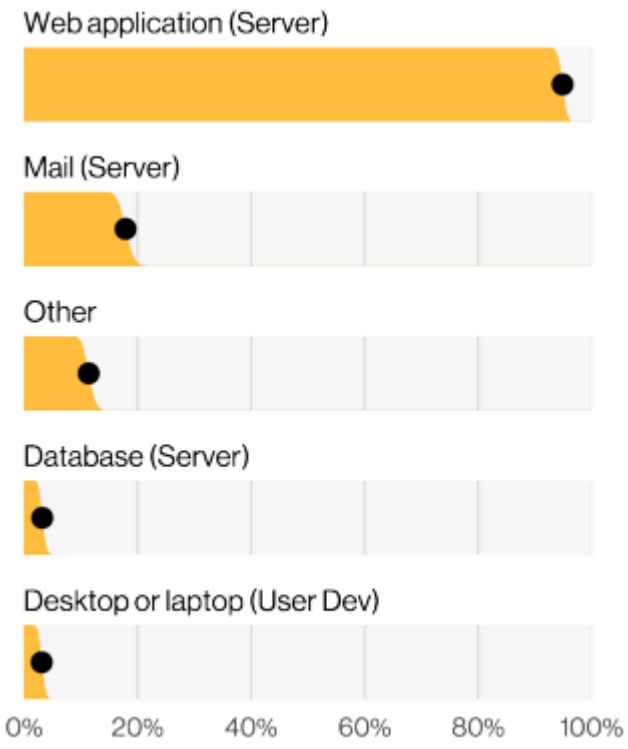

Рис. 1.2. Найпопулярніші різновиди активів у базових атаках на веб-додатки (n=1001) [1]

Занадто часто організації намагаються захиститися за допомогою неадекватних інструментів або тих, що не призначені для виконання завдання захисту, або недостатньо швидко адаптуються до нових типів атак. Результатом є занадто багато інструментів, забагато підходів і забагато думок, що призводить до обмеженої ефективності безпеки, впливає на продуктивність додатків і, у гіршому випадку, до атаки (headline-grabbing attack).

Сьогодні атаки веб-додатків є часто є повільними та методичними, досліджують всю площу великого розподіленого додатка на предмет наявності будь-якої потенційної точки входу. Як тільки вразливість знайдена, зловмисник розробляє експлойт спеціально для неї. Такі атаки розумно оптимізовані проти бізнес-моделі додатку, використовуючи автоматизовані інструменти, які постійно досліджують додаток на наявність різних слабких місць [2].

Захисні стратегії стосуються того, як розробляються та створюються сучасні додатки. Гарна безпека починається з хорошого дизайну, який враховує розподілений характер додатку [2].

В [2] підкреслюється, що безпека – це не окремий випадок, а процес, який необхідно включити в весь життєвий цикл розробки програмного забезпечення. Усі сторони, які беруть участь у розробці сучасних додатків, повинні розуміти, як безпека узгоджується з життєвим циклом розробки. Більш чітке узгодження призводить до вибору кращих інструментів і створення найкращих практик, спеціально розроблених для потреб безпеки додатків.

Оскільки одна частина стеку додатків стає все більш безпечною, хакери переходять до націлювання на нові технології. Ці нові технології часто не мають такого ж рівня вбудованого контролю безпеки, і лише шляхом проб і помилок інженери можуть розробити та впровадити належні засоби контролю безпеки [2].

Кожна нова технологія має свою унікальну поверхню атаки та вразливості. Один із способів стати відмінним хакером – це завжди бути в курсі останніх нових технологій, бо вони часто мають вразливості, які ще не опубліковані чи знайдені.

Щоб ефективно використовувати веб-додатки, потрібен широкий спектр

навичок. З одного боку, хакерові потрібні знання мережевих протоколів, методів розробки програмного забезпечення та поширених уразливостей, які можна знайти в різних типах додатків. Але з іншого боку, хакер також повинен розуміти додаток, на який він націлений. Хакер повинен розуміти мету додатку з функціональної точки зору; визначити його користувачами; як додаток приносить дохід; чому користувачі вибирають додаток перед конкурентами; хто конкуренти; яка функція міститься в програмі тощо [2].

Зрештою, розвідка веб-додатків полягає в зборі даних і побудові моделі, яка поєднує технічні та функціональні деталі веб-додатка таким чином, що дозволяє повністю зрозуміти призначення та використання веб-додатка. Без того чи іншого хакер не може належним чином націлити свою атаку.

Розвідка веб-додатків відноситься до фази дослідницького збору даних, яка зазвичай відбувається до злому веб-програми. Розвідка веб-додатків зазвичай виконується хакерами, пентестувальниками або мисливцями за помилками, але також може бути ефективним способом для інженерів безпеки знайти слабко захищені механізми у веб-додатку та виправити їх до того, як їх знайде зловмисник.

Навички розвідки самі по собі не мають значної цінності, але стають все більш цінними в поєднанні зі знаннями про напади хакерів та досвідом оборонної техніки безпеки.

Необхідно підкреслити, що більшість методів розвідки слід виконувати лише проти програм, якими ви володієте або маєте письмовий дозвіл на тестування. Розвідку можна здійснити багатьма способами. Іноді просто навігація веб-додатком і запис мережевих запитів – це все, що потрібно, щоб познайомитися з внутрішньою роботою цього додатку [2].

Однак важливо зазначити, що не всі веб-додатки будуть мати користувальницький інтерфейс, який дозволить візуально досліджувати додаток та звернути увагу на її функціональність. Більшість загальнодоступних додатків (часто додатків для бізнес-споживачів, як-от соціальні медіа) матимуть загальнодоступний користувальницький інтерфейс.

Методи розвідки є цінними для розвитку глибокого розуміння технології та структури веб-додатка та служб, які забезпечують цей веб-додаток.

Розглянемо застосування положень NIST Cybersecurity Framework [3] до забезпечення безпеки веб-додатків. NIST Cybersecurity Framework складається з трьох частин. Ядро Framework – це набір заходів з кібербезпеки, бажаних результатів і загальних посилань. У ньому представлені стандарти, керівні принципи та методи, що дає змогу повідомити про дії та результати кібербезпеки на всіх рівнях організації. Він містить чотири елементи: функції, категорії, підкатегорії та інформаційні посилання. Рівні впровадження Framework зосереджені на ризиках кібербезпеки та процесах управління цим ризиком. Профіль Framework містить повторювані результати на основі потреб бізнесу, вибраних із категорій і підкатегорій Framework.

Щоб чітко побачити, як NIST Cybersecurity Framework застосовується до веб-безпеки, краще подивитися на структуру ядра Framework. Верхній рівень ядра – це такі функції: ідентифікація, захист, виявлення, відповідь та відновлення. Кожна з функцій містить кілька категорій, наприклад, функція «Ідентифікація» (рис. 1.3) містить такі категорії, як управління активами, бізнес-середовище, управління, оцінка ризиків, стратегія управління ризиками та управління ризиками ланцюга постачання. Кожна з цих категорій має конкретні підкатегорії, які визначають бажані результати.

Жоден з елементів CSF NIST не призначений спеціально для Інтернету, але багато з них також стосуються веб-безпеки. Ось кілька яскравих прикладів:

ID.AM-2: Інвентаризація програмних платформ і додатків в організації: цей результат також стосується веб-додатків. Щоб досягти цього результату потрібно знайти спосіб створити перелік усіх веб-додатків організації.

ID.RA-2: розвідку про кіберзагрози отримують з форумів та джерел обміну інформацією: з точки зору Інтернету, це означає, що зовнішні джерела потрібні для того, щоб знати про потенційні події кібербезпеки в Інтернеті, наприклад, нові вектори атак.

PR.DS-5: реалізовано захист від витоку даних: критичні дані часто доступні

за допомогою веб-додатків. Щоб уникнути порушення даних і гарантувати безпеку даних, організації повинні впровадити відповідні засоби контролю доступу до Інтернету. Багато нещодавніх витоків були викликані незахищеними документами, доступними через Інтернет.

Рис. 1.3. NIST Cybersecurity Framework [3]

DE.CM-8: сканування вразливостей: той факт, що сканування вразливостей виділено як окрема категорія, свідчить про його важливість у процесах виявлення відповідно до NIST.

Необхідно зазначити, що ненадійне програмне забезпечення підриває безпеку критичних інфраструктур, що стосуються, наприклад, охорони здоров’я, оборони, енергетики або фінансів. Програмне забезпечення стає складнішим, пристроїв, підключених до мережі, стає більше, тому важливість забезпечення безпеки програм зростає експоненційно. Швидкий розвиток методів розробки ПЗ призводить до необхідності швидко і безпомилково виявляти, а також усувати загрози, що найчастіше виникають. Необхідно приділяти належну увагу загрозам безпеці (рис. 1.4), які представлено у списку Топ-10 OWASP [4].

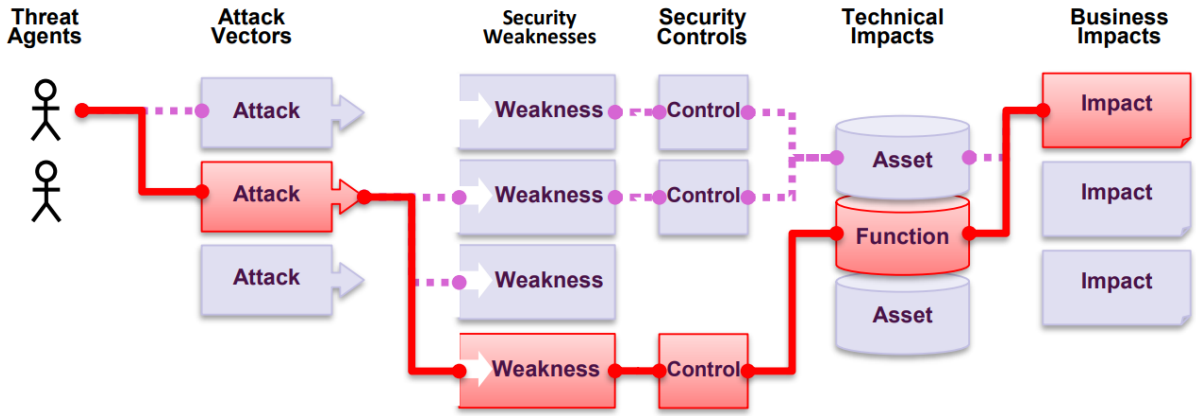

Рис. 1.4. Приклад загрози безпеці веб-додатку [4]

Іноді ці способи легко знайти та експлуатувати, іноді дуже складно. Аналогічна ситуація з можливим збитком: його може не бути зовсім, або він може відчутним для бізнесу. Щоб визначити ризики для організації, необхідно оцінювати ймовірності, пов'язані з джерелами загроз, векторами атак і недоліками безпеки, а потім поєднати їх з оцінкою технічної та репутаційної шкоди для конкретної організації. Сума цих чинників визначається сукупний ризик [4].

Десять найбільш поширених вразливостей веб-додатків за [4].

A1:2017 – Впровадження. Вразливості, пов'язані, наприклад, із використанням SQL, NoSQL, OS і LDAP, виникають, коли неперевірені дані відправляються інтерпретатору у складі команди чи запиту. Шкідливі дані можуть змусити інтерпретатор виконати непередбачені команди або звернутися до даних без відповідної авторизації [4].

A2:2017 – Недоліки автентифікації. Функції програм, пов'язані з автентифікацією та керуванням сесіями, часто некоректно реалізуються, дозволяючи зловмисникам скомпрометувати паролі, ключі або сесійні токени, а також експлуатувати інші помилки реалізації для тимчасового або постійного перехоплення облікових записів користувачів [4].

A3:2017 – Розголошення конфіденційних даних. Багато веб-додатків та API мають поганий захист критичних фінансових, медичних або персональних даних. Зловмисники можуть викрасти або змінити ці дані, а потім здійснити шахрайські

дії із кредитними картками або персональними даними. Конфіденційні дані вимагають додаткових заходів захисту, наприклад їх шифрування при зберіганні або передачі, а також спеціальних запобіжних заходів при роботі з браузером [4].

A4:2017 – Зовнішні сутності XML (XXE). Старі або погано налаштовані процесори XML обробляють посилання на зовнішні сутності всередині документів. Ці сутності можуть бути використані для доступу до внутрішніх файлів через обробники URI файлів, спільні папки, сканування портів, віддалене виконання коду та відмова в обслуговуванні [4].

A5:2017 – Недоліки контролю доступу. Дії, які дозволені автентифікованим користувачам, часто некоректно контролюються. Зловмисники можуть скористатися цими недоліками і отримати несанкціонований доступ до облікових записів інших користувачів або конфіденційної інформації, а також змінити дані користувача або права доступу [4].

A6:2017 – Некоректне налаштування параметрів безпеки. Некоректне налаштування безпеки є поширеною помилкою. Це відбувається через використання стандартних параметрів безпеки, неповного або специфічного налаштування, відкритого хмарного зберігання, некоректних HTTP-заголовків та докладних повідомлень про помилки, що містять критичні дані. Всі ОС, фреймворки, бібліотеки та додатки повинні бути не тільки налаштовані належним чином, а й своєчасно коригуватися та оновлюватись [4].

A7:2017 – Міжсайтове виконання сценаріїв (XSS). XSS має місце, коли програма додає неперевірені дані на нову веб-сторінку без їхньої відповідної перевірки чи перетворення, або коли оновлює відкриту сторінку через API браузера, використовуючи надані користувачем дані, що містять HTML- або JavaScript-код. За допомогою XSS зловмисники можуть виконувати сценарії в браузері жертви, що дозволяють їм перехоплювати сесії, підміняти сторінки сайту або перенаправляти користувачів на шкідливі сайти [4].

A8:2017 – Небезпечна десеріалізація. Небезпечна десеріалізація часто призводить до віддаленого виконання коду. Помилки десеріалізації, що не призводять до віддаленого виконання коду, можуть бути використані для атак із

повторним відтворенням, впровадженням та підвищенням привілеїв.

A9:2017 – Використання компонентів з відомими вразливістю [4]. Компоненти, такі як бібліотеки, фреймворки та програмні модулі, запускаються з привілеями програми. Експлуатація вразливого компонента може призвести до втрати даних або перехоплення контролю над сервером. Використання додатків та компонентів API з відомими вразливістю може порушити захист програми та призвести до серйозних наслідків [4].

A10:2017 – Недоліки ведення журналів та моніторингу. Недоліки ведення журналів та моніторингу, а також відсутність або неефективне використання системи реагування на інциденти, дозволяють зловмисникам розвинути атаку, приховати свою присутність та проникнути в інші системи, а також змінити, вилучити чи знищити дані. Проникнення в систему зазвичай виявляють лише через 200 днів і, як правило, сторонні дослідники, а не в рамках внутрішніх перевірок чи моніторингу [4].

1.2. Аналіз підходів до захисту веб-додатків організації при застосуванні хмарних платформ

Додатки відіграють важливу роль у підтримці ключових бізнес-процесів, тому організації намагаються забезпечити їх безпеку. Згідно з [5] 62% фахівців з кібербезпеки в кращому випадку помірно впевнені в позиції безпеки додатків своєї організації. Не дивно, що приблизно стільки ж вважають свої стратегії безпеки додатків незрілими.

За словами 41% опитаних, веб-додатки, орієнтовані на клієнтів, становлять найбільший ризик для бізнесу (рис. 1.5). Згідно з нещодавньою статтею TechRepublic, майже *кожний веб-додаток сьогодні має принаймні одну вразливість* [6]. Найбільше насторожує керівників безпеки, що час, необхідний для усунення критичних вразливостей додатків, часто вимірюється місяцями, а не днями чи навіть тижнями.

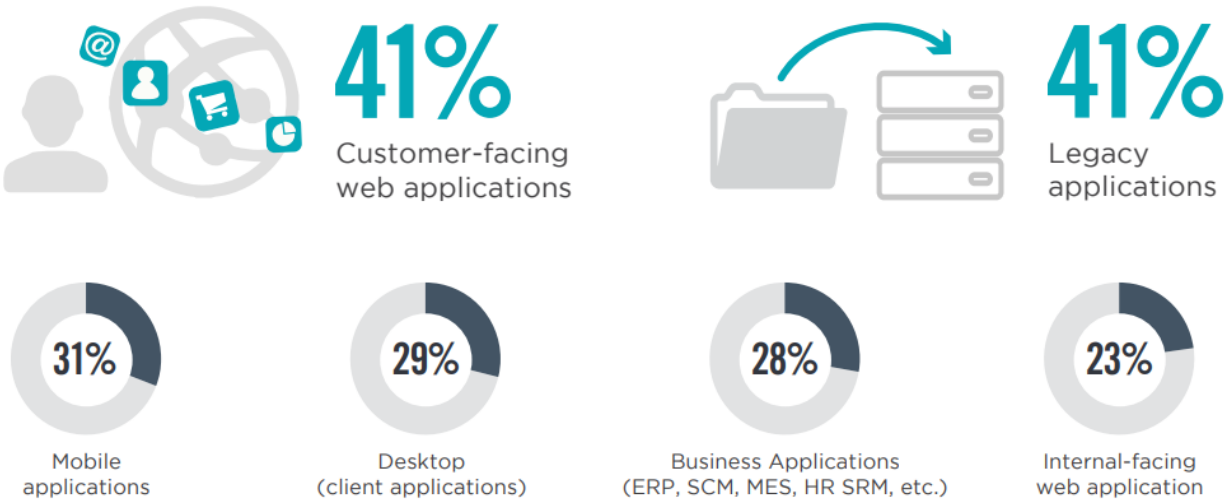

Рис. 1.5. Типи додатків та їх ризик для безпеки [5]

Відповідно до [5] 23% організацій (рис. 1.6) зазнали зламу або компромісу додатків протягом останніх 12 місяців, а 8% зазнали атаки лише протягом попереднього місяця. Більш тривожним є те, що більше третини респондентів навіть не могли повідомити, чи мали вони злами чи компроміс протягом останніх п'яти років.

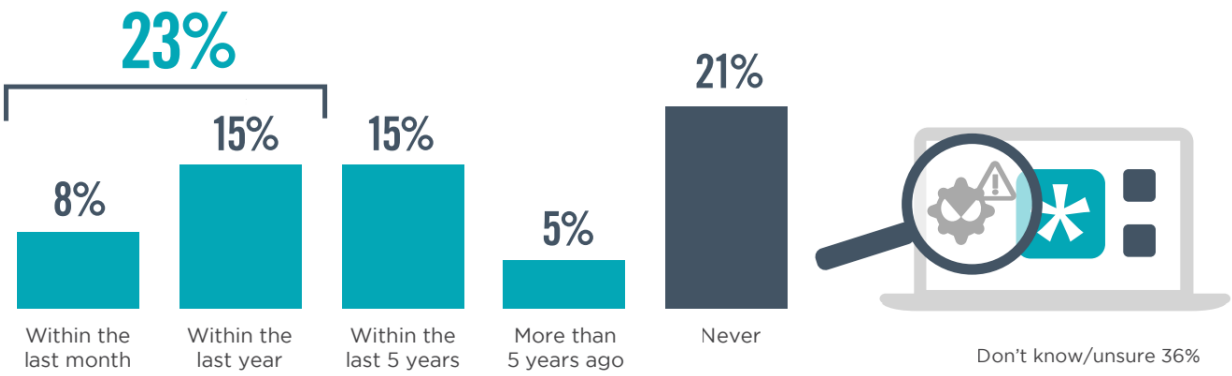

Рис. 1.6. Відповіді на питання коли в останнє було зламано бізнес-додатки [5]

Зрозуміло, що організації повинні покращити спосіб захисту бізнес-додатків, особливо з огляду на те, що все більше додатків розробляється та розміщується в Інтернеті для зовнішнього доступу.

Розглянемо рекомендації компанії Tenable щодо кращого захисту веб-додатків від останніх загроз кібербезпеці.

Через появу «тіньових IT», у яких відділи, групи та окремі користувачі

розгортають бізнес-додатки без повноважень на це або відсутність знань про централізоване управління IT, багато команд із забезпечення безпеки не бачать, які додатки використовуються в організації. Наприклад, 89% респондентів кажуть, що їхні організації не впевнені, що знають усі додатки, які використовуються. Лише 11% кажуть, що впевнені, що знають усі додатки. Крім того, 17% організацій не можуть навіть надати приблизний діапазон того, скільки додатків вони мають у своєму середовищі [5].

Погана видимість веб-додатків сьогодні є серйозною проблемою для команд безпеки. В одному нещодавньому дослідженні Symantec було визначено, що розрив між уявними та реальними хмарними додатками, що використовуються, становить понад 20 разів [5].

Найкраща практика № 1: автоматичне виявлення веб-додатків. Автоматичне виявлення додатків, розгорнутих в організації, усуває дорогі ручні здогади та небезпечні сліпі зони безпеки. Завдяки новим методам DevOps, веб-додатки створюються та розгортаються все більшою кількістю команд швидше, ніж будь-коли, і дуже важко встигати за ручними списками IP-адрес і доменних імен. Необхідно використовувати переваги рішень, які можуть ідентифікувати веб-додатки за допомогою діапазонів IP-адрес, доменних імен і сканування портів HTTP.

Керівники з кібербезпеки постійно скаржаться на брак ресурсів для захисту від останніх атак. Справді, в [5] підтверджується, що нестача кваліфікованого персоналу (37%) і брак бюджету (35%) є одними з головних перешкод, які гальмують захист від кіберзагроз.

Навички та бюджет також є двома головними проблемами, які гальмують тестування на проникнення додатків в організаціях. Щоб підкреслити дефіцит ресурсів, команди з безпеки додатків часто співвідносяться до розробників як 1:100. Через обмеження навичок, ресурсів і бюджету більшість організацій можуть оцінювати та захищати лише найбільш важливі веб-додатки – менше ніж 10% від загальної кількості веб-додатків – за допомогою ручного тестування на проникнення. Це означає, що інші 90% основних вед-додатків недостатньо

захищені та їх необхідно оцінити на предмет ризиків [5].

Найкраща практика №2: автоматизуйте сканування веб-програм. Враховуючи, що попит на навички безпеки продовжує перевищувати пропозицію, автоматизація має вирішальне значення для зниження витрат як на технології, так і на персонал.

Організаціям потрібні рішення для сканування веб-додатків, які можуть швидко, точно й автоматично оцінювати всі веб-додатки. Досліджуйте рішення, які дозволяють вам «налаштувати і забути», плануючи часті та повторювані сканування веб-додатків, щоб захистити корпоративне середовище, що постійно змінюється.

Організації мають справу зі зростаючою складністю свого IT-середовища, включаючи кількість і різноманітність бізнес-додатків, що використовуються. Також існує складність з точки зору інструментів та послуг безпеки. Не дивно, що більше половини (54%) респондентів кажуть, що простота інтеграції є найважливішим критерієм при виборі рішення безпеки програми.

Рішення з роз'єднаними точками, розроблені для конкретних типів активів, створюють відокремлену видимість і надмірні витрати на керування. Тому сканування веб-додатків має бути частиною ширшої інтегрованої платформи Cyber Exposure, щоб допомогти групам безпеки керувати та вимірювати кіберризики на всій поверхні атаки.

Найкраща практика № 3: зробіть безпеку додатків частиною вашої загальної практики Cyber Exposure. Розгорніть прості у використанні та інтуїтивно зрозумілі продукти для сканування веб-додатків, які інтегровані в більш широку платформу Cyber Exposure. Це зменшує потребу в високоспеціалізованому персоналі з безпеки додатків для налаштування, розгортання та керування цими системами.

Крім того, це дає змогу оцінити додатки на предмет кіберризиків і визначити пріоритети усунення вразливостей разом з іншими активами на поверхні атаки.

Отримайте більш широке покриття безпеки, заощаджуючи час і гроші, і

перерозподіліть персонал для інших більш цінних заходів. Оскільки з'являється так багато векторів загроз і вразливостей, важко знати, на чому зосередитися. Організаціям в середньому потрібно усувати понад 800 вразливостей на день у майже 1000 активах. Приблизно дві третини цих вразливостей мають оцінку CVSS 7,0 або вище. Це означає, що служби безпеки постійно реагують на невпинний шквал нових кіберризиків. Майже половина респондентів опитування (45%) підтверджують, що не відставання від зростаючого числа вразливостей є найбільшою проблемою безпеки додатків [5].

Проблема полягає в тому, що командам з безпеки бракує даних і розуміння, які їм потрібні, щоб визначити пріоритети виправлення, а це означає, що вони не можуть швидко вирішити найважливіші проблеми безпеки. Як наслідок, час, необхідний для усунення лише вразливостей високого та критичного ризику, часто вимірюється місяцями. Це наражає організацію на надмірний і непотрібний кіберризик.

Найкраща практика № 4: визначить пріоритети на основі ризику. Розширене визначення пріоритетів на основі фактичного кіберризику, поєднання критичності активів, серйозності вразливості та доступності експлойтів, є важливим для захисту ваших програм.

Відфільтруйте вразливі місця з меншим ризиком, щоб ви могли працювати над усуненням найбільш важливих для бізнесу проблем безпеки, і зосередьтеся на вразливостях, які активно експлуатуються суб'єктами загроз, а не на тих, які могли б бути використані лише теоретично.

Багато організацій просто занадто повільно реагують на інциденти з безпеки або недостатньо активно зупиняють атаки. Майже половина всіх опитаних організацій (48%) сканують програми щоквартально або навіть рідше. Ця нестача швидкості не забезпечить належного захисту додатків у сучасну епоху швидкої розробки програмного забезпечення [5].

Зростання DevOps означає, що випускаються нові веб-додатки, а існуючі веб-додатки оновлюються набагато швидше, ніж у минулому. Наприклад, зрілі організації DevOps випускають код кілька разів на день, і багато організацій

(59%) оновлюють існуючі веб-додатки принаймні раз на місяць. Безпека ще не адаптувалася до нової реальності DevOps [6].

Найкраща практика № 5: інтегруйте безпеку в життєвий цикл розробки програмного забезпечення. Підтримуйте високошвидкісні процеси DevOps, інтегруючи сканування веб-додатків у конвеєр DevOps перед випуском програми.

Необхідно відмітити, що, чим раніше буде усунено дефекти безпеки в життєвому циклі розробки програмного забезпечення, тим менш витратним буде їх усунення. Крім того, необхідно сканувати веб-додатки, які працюють, щонайменше раз на місяць, щоб забезпечити постійну видимість кіберризику [5].

1.3. Аналіз існуючих рішень із захисту веб-додатків організації при застосуванні хмарних платформ

Незважаючи на те, що рішення Web Application Firewall в світі вже встигли набрати достатню популярність, і такі компанії як Amazon надають захищені сервіси на базі продуктів даного класу, на ринку України для багатьох використання WAF ще в новинку. Сильними гравцями на ринку є Fortinet з рішенням FortiWeb і Imperva з SecureSphere Web Firewall Application.

FortiWeb – це WAF, який захищає розміщені веб-додатки від атак, спрямованих на відомі та невідомі експлойти [7].

Використовуючи *багаторівневі та кореляційні методи* виявлення, FortiWeb захищає програми від відомих вразливостей та загроз нульового дня. Служба безпеки веб-додатків від FortiGuard Labs використовує інформацію, засновану на останніх вразливостях додатків, ботах, підозрілих URL-адресах та шаблонах даних, а також спеціалізованих евристичних механізмах виявлення для забезпечення безпеки веб додатків [7].

FortiWeb також пропонує *функцію машинного навчання*, яка дозволяє автоматично виявляти шкідливий веб-трафік. Окрім виявлення відомих атак, ця функція може виявляти потенційні невідомі атаки нульового дня для забезпечення захисту веб-серверів у режимі реального часу.

FortiWeb дозволяє налаштовувати такі функції [7]:

сканування вразливостей та виправлення;

репутація IP, сигнатури атак веб-застосунків, захист облікових даних, антивірус та FortiSandbox Cloud на базі FortiGuard;

аналіз атак та звітність у режимі реального часу за допомогою розширених інструментів візуальної аналітики;

інтеграція з FortiGate та FortiSandbox для виявлення ATP атак;

виявлення поведінкової атаки;

розширене запобігання хибно позитивним та негативним результатам виявлення.

Платформи обладнання та віртуальних машин FortiWeb доступні для середніх та великих підприємств, а також для постачальників послуг.

Перевагою FortiWeb є те, що дане рішення розроблено спеціально для захисту веб-серверів. Воно забезпечує спеціалізоване виявлення загроз на рівні додатків та захист для служб HTTP та HTTPs, у тому числі: Apache Tomcat; nginx; Microsoft IIS; JBoss; IBM Lotus Domino; Microsoft SharePoint; Microsoft Outlook Web App (OWA); RPC та ActiveSync для Microsoft Exchange Server; Joomla та WordPress

Інтегрований веб-сканер вразливостей FortiWeb значно знижує проблеми, пов’язані із захистом регульованих та конфіденційних даних, за рахунок виявлення схильності корпоративних рішень до найновіших загроз, особливо з OWASP Top 10 [7].

Брандмауер HTTP та захист від атак типу «відмова в обслуговуванні» (DoS) FortiWeb захищають корпоративні веб-додатки від атак. Використовуючи передові методи для забезпечення двоспрямованого захисту від складних загроз, таких як SQL-ін’єкції та атаки міжсайтового скріптингу (XSS), FortiWeb також допомагає захищатися від таких загроз, як крадіжка особистих даних, фінансове шахрайство та корпоративне шпигунство [7].

FortiWeb надає інструменти, необхідні для моніторингу та забезпечення дотримання державних постанов, передових галузевих практик та внутрішніх

політик безпеки, включаючи вимоги до брандмауерів та виправлень із стандарту PCI DSS (рис. 1.7) [8].

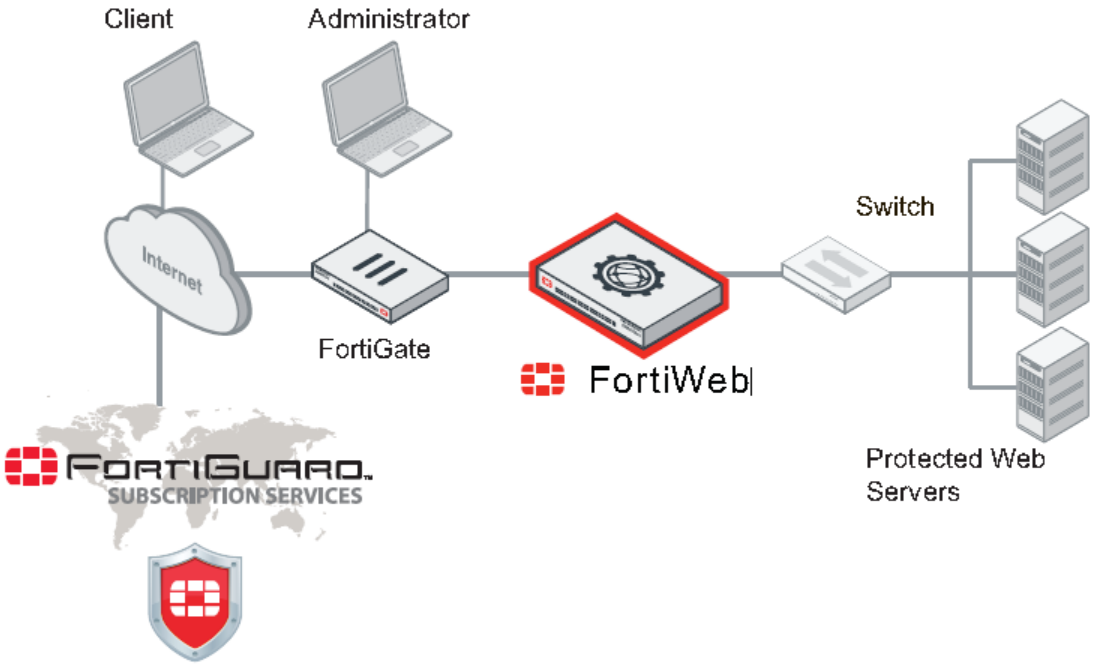

Рис. 1.7. Місце FortiWeb в архітектурі безпеки [7]

FortiWeb можна розгорнути в топології “одна рука”, але частіше він розміщується в оперативному режимі, щоб перехоплювати всі вхідні клієнтські з’єднання та перерозподіляти їх на корпоративні сервери. FortiWeb має спеціальні можливості брандмауера для TCP та HTTP. Оскільки він не призначений для безпеки веб-додатків, відмінних від HTTP/HTTPs, його слід розгортати за брандмауером, таким як FortiGate (рис. 1.7), який орієнтований на безпеку для інших протоколів, включаючи FTP та SSH. Після розгортання FortiWeb його можна налаштувати за допомогою веб-браузера або емулятора терміналу на керуючому комп’ютері [7].

Також серед переваг FortiWeb необхідно відзначити той факт, що в своїх апаратних і програмних рішеннях компанія Fortinet використовує власні технології. Так, для прискорення обробки і шифрування даних застосовуються спеціалізовані процесори FortiASIC. Крім того, розроблена своя операційна система FortiOS, оптимізована під завдання безпеки.

Fortinet якісно супроводжує свою продукцію, постійно виконуючи роботи

по виявленню нових загроз у власному центрі FortiGuard аналітичному Центр безпеки. В результаті оновлення сигнатур, чорних списків сайтів і баз репутацій відбувається кілька разів на день.

Важливо також треба відзначити тісну інтеграцію всіх пристроїв Fortinet за рахунок повної сумісності між собою, що дозволяє швидко і просто масштабувати систему. Істотною перевагою систем захисту на базі Fortinet є високий ступінь автоматизації операцій і простота їх супроводу. Це дозволяє скоротити число помилок, викликаних людським фактором і зменшити число співробітників обслуговуючого персоналу.

Imperva SecureSphere Web Firewall Application – один з лідерів в області відображення атак на веб-додатки. Рішення від Imperva забезпечують надійний захист за рахунок одночасного застосування декількох технологій в сфері ІБ: сигнатурний аналіз, перевірка протоколів на аномалії, відстеження сесій, динамічне профілювання (рис. 1.8) [8].

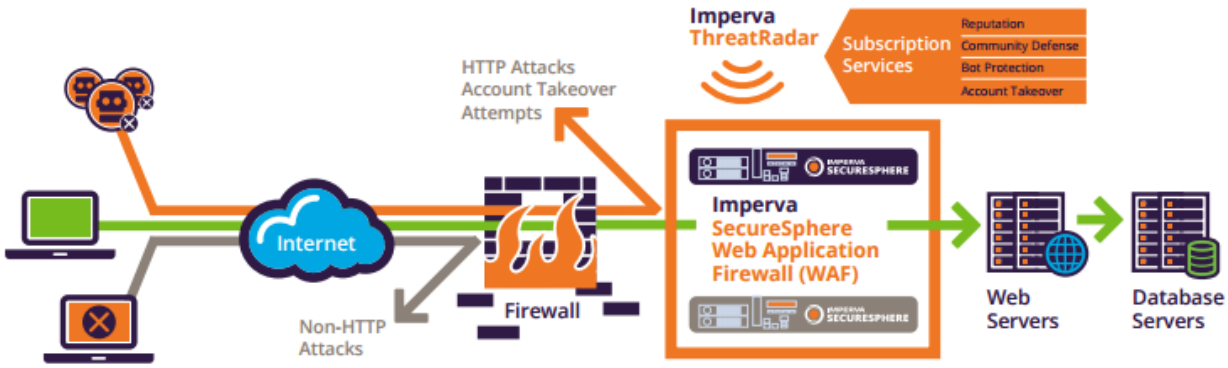

Рис. 1.8. Imperva SecureSphere Web Firewall Application [8]

Сімейство продуктів Secure-Sphere WAF успішно протидіє всім з OWASP TOP 10 атакам, так і іншим менш відомим, але більш витонченим атакам. Пристрої мають можливості по інспектування зашифрованих даних, що пересилаються по протоколу SSL (HTTPS).

Рішення складається з наступних модулів [8]:

SecureSphere Web Firewall Application – захист веб-додатків від кібератак;

ThreatRadar – репутаційна база даних.

Secure-Sphere WAF здатний глибоко аналізувати логіку роботи легального веб-додатки, виконувати інтелектуальне дослідження спроб проникнення і атак; HTTP-протидіяти атакам, включаючи атаки на переповнення буфера, дії шкідливих програм і зловмисників. Рішення має механізм захисту від черв'яків і інших шкідливих атак на веб-сервери і додатки, основу якого складають механізми на основі сигнатур популярної системи Snort і власних SQL-сигнатур, що розробляються дослідним центром ADC (Application Defense Center) компанії Imperva. Вбудований міжмережевий екран здійснює надійний захист від неавторизованих призначених для користувача запитів і атак на мережевому рівні [8].

Попередньо в системі звіти повністю задовольняють вимогам стандартів інформаційної безпеки. Можливе створення призначених для користувача звітів (в тому числі за розкладом) та експорт в різні формати. Додаткові хмарні сервіси дозволяють спростити безпеку і впорається з DDoS-атаками.

Важлива перевага пристроїв SecureSphere WAF: наявність унікального сервісу ThreatRadar, що забезпечує захист від автоматизованих атак. Завдяки швидкому отриманню достовірної інформації про джерела атак, ThreatRadar дозволяє негайно блокувати трафік, що йде від підозрілих джерел, ще до моменту здійснення будь-якого руйнівної дії. Рішення Imperva відрізняються прозорою підтримкою і простим розгортанням [8].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ В AZURE

2.1. Призначення та основні функції брандмауера веб-додатків Azure

Брандмауер веб-додатків Azure (WAF) надає централізований захист веб-додатків від поширених експлойтів і вразливостей. Веб-додатки все частіше піддаються шкідливим атакам, що використовують загальновідомі вразливості. Найбільш поширеними атаками є впровадження SQL та використання міжсайтових скриптів [9].

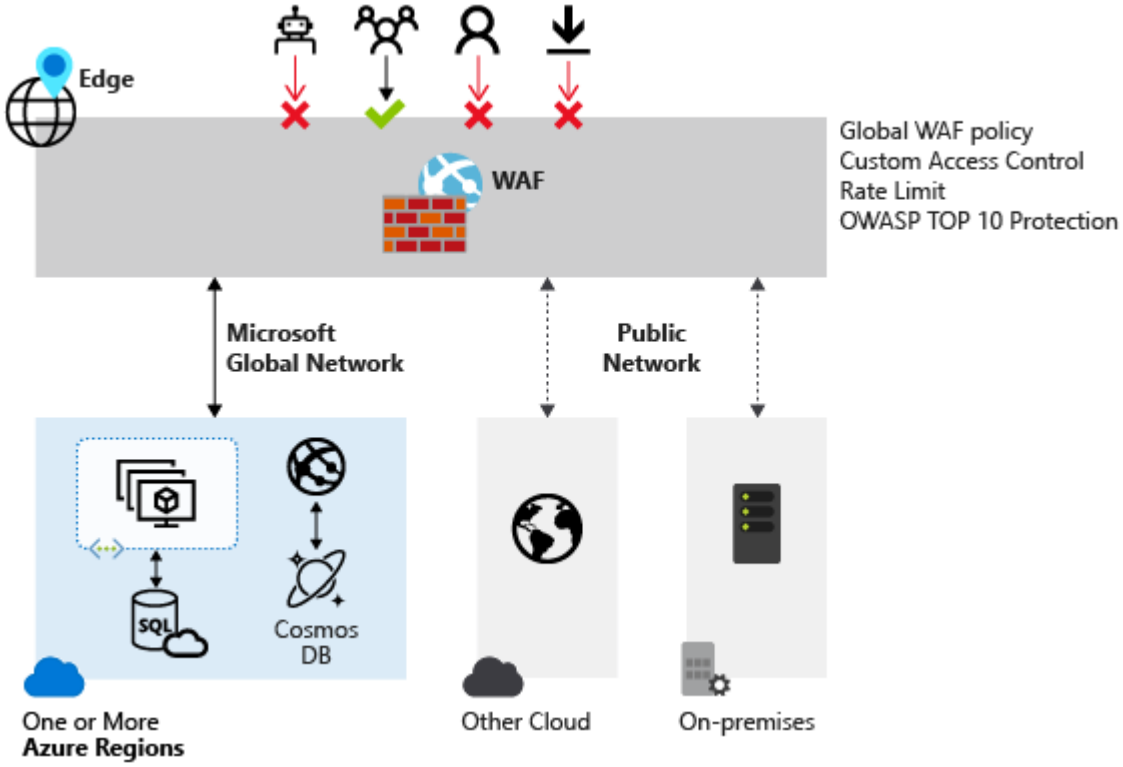

Рис. 2.1. Місце WAF в архітектурі веб-додатку [9]

Запобігти таким атакам у програмному коді складно. Це може вимагати ретельного обслуговування, виправлення та моніторингу на кількох рівнях топології додатку. Централізований брандмауер веб-додатків значно спрощує керування безпекою. WAF також надає адміністраторам додатків кращі гарантії захисту від загроз і вторгнень.

Рішення WAF може швидше реагувати на загрозу безпеці шляхом централізованого виправлення відомої вразливості, замість того, щоб захищати кожний окремий веб-додаток.

WAF можна розгорнути за допомогою Azure Application Gateway, Azure Front Door і служби Azure Content Delivery Network (CDN) від Microsoft. WAF на Azure CDN наразі знаходиться в загальнодоступній попередній версії. WAF має функції, налаштовані для кожної конкретної служби.

2.2. Призначення та основні функції брандмауера веб-додатків Azure на шлюзі додатків Azure

Брандмауер веб-додатків Azure (WAF) на шлюзі додатків Azure забезпечує централізований захист веб-додатків від поширених експлойтів і вразливостей. Веб-додатки все частіше стають мішенню зловмисних атак, які використовують загальновідомі вразливості. SQL-ін’єкція та міжсайтовий сценарій є одними з найпоширеніших атак [10].

WAF на шлюзі додатків базується на *основному наборі правил* (Core rule sets, CRS) від Open Web Application Security Project (OWASP).

Усі наведені нижче функції WAF існують у політиці WAF. Ви можете створити кілька політик, і їх можна пов’язати зі шлюзом додатків, окремими сайтами або правилами маршрутизації на основі шляху на шлюзі додатків. Таким чином, ви можете мати окремі політики для кожного сайту за вашим шлюзом додатків, якщо це необхідно.

Шлюз додатків працює як контролер доставки додатків (ADC). Він пропонує захист транспортного рівня (TLS), раніше відомий як рівень захищених сокетів (SSL), завершення, спорідненість сеансу на основі файлів cookie, циклічний розподіл навантаження, маршрутизацію на основі вмісту, можливість розміщення кількох веб-сайтів і покращення безпеки [10].

Удосконалення безпеки Application Gateway (рис. 2.2) включають керування політикою TLS і наскрізну підтримку TLS. Безпека додатків посилена інтеграцією

WAF у шлюз додатків. Ця комбінація захищає корпоративні веб-додатки від поширених уразливостей. І це забезпечує просте для налаштування центральне розташування для керування.

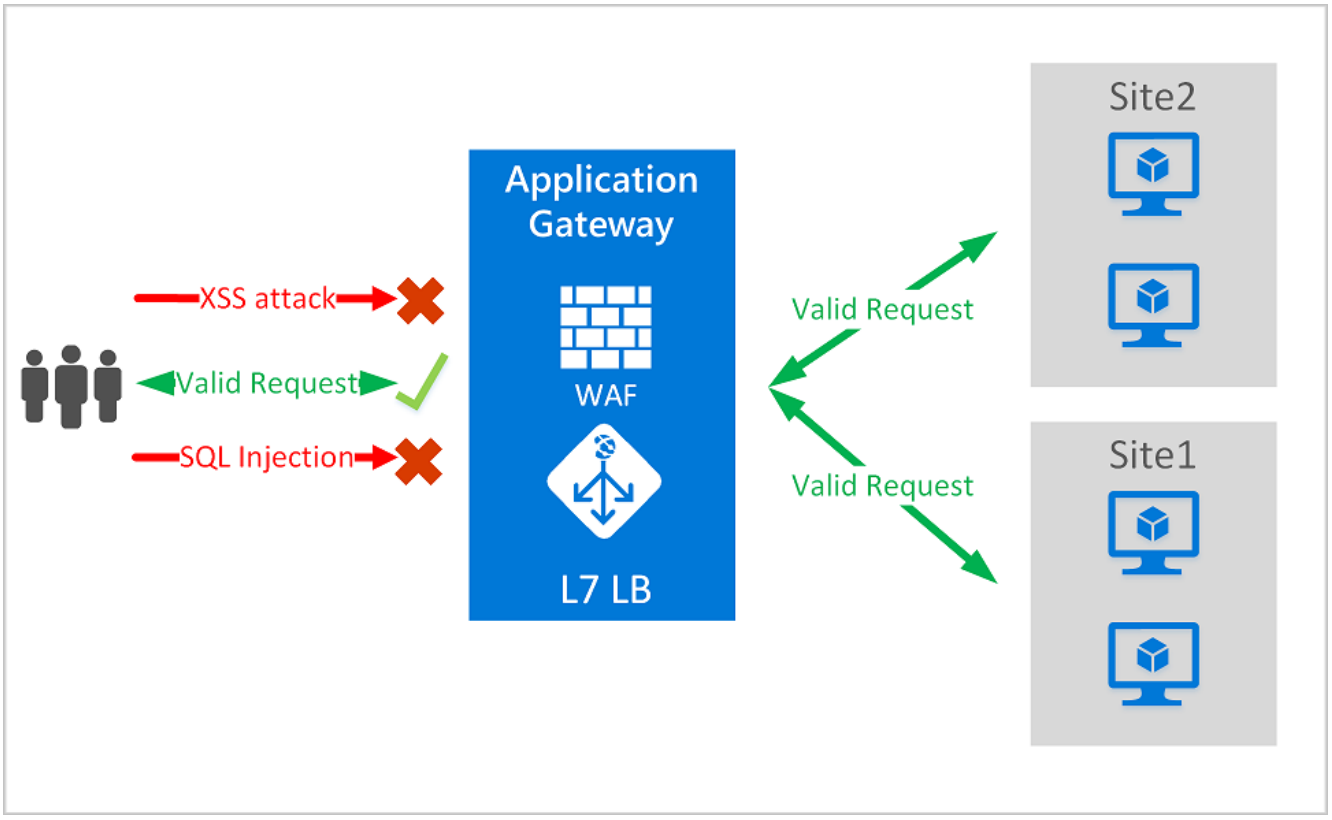

Рис. 2.2. Принцип роботи WAF на шлюзі додатків Azure [10]

Розглянемо основні переваги WAF на шлюзі додатків [10]:

захист веб-додатків від веб-вразливостей і атак без змін у базовому коді. Захист кількох веб-додатків одночасно. Примірник Application Gateway може розмістити до 40 веб-сайтів, захищених брандмауером веб-додатків;

можливість створення власних політик WAF для різних сайтів за одним WAF;

захист своїх веб-додатків від шкідливих ботів за допомогою набору правил репутації IP;

моніторинг атак на ваші веб-додатки за допомогою журналу WAF у реальному часі. Журнал інтегровано з Azure Monitor для відстеження сповіщень WAF і легкого моніторингу тенденцій. Application Gateway WAF інтегровано з

Microsoft Defender for Cloud. Defender for Cloud забезпечує централізований перегляд стану безпеки всіх ваших ресурсів Azure, гібридних і мультихмарних ресурсів;

можливість налаштування правил та груп правил WAF відповідно до вимог додатків та усунення помилкових спрацьовувань. Зв’язок політик WAF для кожного сайту за вашим WAF, щоб забезпечити конфігурацію для конкретного сайту;

можливість створення власних правил відповідно до потреб веб додатків.

Розглянемо основні особливості WAF на шлюзі додатків [10]:

захист від SQL ін'єкції;

захист міжсайтових сценаріїв;

захист від інших поширених веб-атак, таких як впровадження команд, контрабанда HTTP-запитів, розділення відповідей HTTP та віддалене включення файлів;

захист від порушень протоколу HTTP;

захист від аномалій протоколу HTTP, таких як відсутність агента користувача та приймання заголовків;

захист від сканерів;

виявлення типових неправильних конфігурацій додатків (наприклад, Apache та IIS);

настроювані обмеження розміру запиту з нижньою та верхньою межами;

списки виключень дозволяють виключити певні атрибути запиту з оцінки WAF. Типовим прикладом є маркери, вставлені в Active Directory, які використовуються для автентифікації або полів пароля;

створення власних правил відповідно до конкретних потреб ваших додатків;

географічний фільтр трафіку, щоб дозволити або заблокувати певним країнам/регіонам доступ до ваших додатків;

захист свої додатків від ботів за допомогою набору правил пом’якшення ботів;

перевірка JSON і XML у тілі запиту.

Розглянемо політики та правила WAF.

Щоб увімкнути брандмауер веб-додатків на шлюзі додатків, необхідно створити політику WAF. У цій політиці існують усі керовані правила, користувацькі правила, виключення та інші налаштування, наприклад обмеження на завантаження файлів [10].

Ви можете налаштувати політику WAF і пов’язати цю політику з одним або кількома шлюзами додатків для захисту. Політика WAF складається з двох типів правил безпеки:

спеціальні правила, які ви створюєте;

керовані набори правил, які є набором попередньо налаштованих правил, керованих Azure.

Якщо обидва типи правил наявні, настроювані правила обробляються перед обробкою правил у керованому наборі правил. Правило складається з умови відповідності, пріоритету та дії. Підтримуються такі типи дій: ДОЗВОЛИТИ, БЛОКУВАТИ та ЗАХОДИТИ. Ви можете створити повністю налаштовану політику, яка відповідає вимогам захисту ваших конкретних додатків, поєднавши керовані та спеціальні правила.

Правила в межах політики обробляються в пріоритетному порядку. Пріоритет – це унікальне ціле число, яке визначає порядок правил для обробки. Менше ціле значення означає вищий пріоритет, і ці правила оцінюються перед правилами з вищим цілим значенням. Коли правило збігається, до запиту застосовується відповідна дія, визначена в правилі. Після обробки відповідності правила з нижчим пріоритетом більше не обробляються [10].

Веб-додаток, наданий шлюзом додатків, може мати політику WAF, пов’язану з нею на глобальному рівні, на рівні сайту або на рівні URI.

Основні набори правил. Шлюз додатків підтримує кілька наборів правил, включаючи CRS 3.2, CRS 3.1 і CRS 3.0. Ці правила захищають ваші веб-додатки від зловмисної діяльності.

Спеціальні правила. Шлюз додатків також підтримує спеціальні правила. За допомогою спеціальних правил ви можете створювати власні правила, які

оцінюються для кожного запиту, що проходить через WAF. Ці правила мають вищий пріоритет, ніж інші правила в керованих наборах правил. Якщо виконується набір умов, виконується дія для дозволу або блокування.

Пом'якшення ботів. Набір керованих правил захисту від ботів можна ввімкнути для вашого WAF, щоб блокувати або реєструвати запити від відомих шкідливих IP-адрес, поряд із керованим набором правил. IP-адреси отримані з каналу Microsoft Threat Intelligence. Intelligent Security Graph забезпечує розвідку загроз Microsoft і використовується багатьма службами, включаючи Microsoft Defender for Cloud.

Якщо захист від ботів увімкнено, вхідні запити, які збігаються з IP-адресами клієнта зловмисного бота, реєструються в журналі брандмауера.

Режими WAF. Application Gateway WAF можна налаштувати для роботи в таких двох режимах:

режим виявлення: відстежує та реєструє всі сповіщення про загрози. Ви вмикаєте діагностику журналювання для шлюзу додатків у розділі *Діагностика*. Ви також повинні переконатися, що журнал WAF вибрано та ввімкнено. Брандмауер веб-додатків не блокує вхідні запити, коли він працює в режимі виявлення;

режим запобігання: блокує вторгнення та атаки, які виявляють правила. Зловмисник отримує виняток «403 несанкціонований доступ», і з’єднання закривається. Режим запобігання фіксує такі атаки в журналах WAF.

Рекомендується запустити нещодавно розгорнутий WAF у режимі виявлення протягом короткого періоду часу у робочому середовищі. Це надає можливість отримати журнали брандмауера та оновити будь-які винятки або спеціальні правила до переходу в режим запобігання. Це може допомогти зменшити випадки неочікуваного блокування трафіку.

Механізм брандмауера веб-додатків Azure (WAF) – це компонент, який перевіряє трафік і визначає, чи містить запит підпис, який представляє потенційну атаку. Коли ви використовуєте CRS 3.2 або новішої версії, ваш WAF працює на новому механізмі WAF, який забезпечує вищу продуктивність і покращений набір

функцій. Коли ви використовуєте попередні версії CRS, ваш WAF працює на старішій системі. Нові функції будуть доступні лише на новому механізмі Azure WAF.

Клієнти WAF можуть вибрати, яку дію виконувати, коли запит відповідає умовам правил. Нижче наведено список підтримуваних дій.

Дозволити: запит проходить через WAF і пересилається на серверну частину. Жодні інші правила нижчого пріоритету не можуть заблокувати цей запит. Дії дозволу застосовуються лише до набору правил Bot Manager і не застосовуються до основного набору правил.

Заблокувати: запит блокується, і WAF надсилає відповідь клієнту, не пересилаючи запит до серверної частини.

Журнал: запит реєструється в журналах WAF, і WAF продовжує оцінювати правила нижчого пріоритету.

Оцінка аномалії: це дія за замовчуванням для набору правил CRS, де загальна оцінка аномалії збільшується, коли збігається правило з цією дією. Оцінка аномалій не застосовується до набору правил Bot Manager.

Режим оцінки аномалій: OWASP має два режими для прийняття рішення щодо блокування трафіку: традиційний режим і режим підрахунку аномалій.

У традиційному режимі трафік, який відповідає будь-якому правилу, розглядається незалежно від будь-яких інших збігів правил. Цей режим простий для розуміння. Але відсутність інформації про те, скільки правил відповідає конкретному запиту, є обмеженням. Отже, був представлений режим підрахунку аномалій. Це типове значення для OWASP 3.x .

У режимі підрахунку аномалій трафік, який відповідає будь-якому правилу, не блокується одразу, коли брандмауер перебуває в режимі запобігання. Правила мають певний ступінь серйозності: Критичний, Помилка, Попередження або Повідомлення. Цей рівень серйозності впливає на числове значення для запиту, яке називається показником аномалії. Наприклад, один матч за правилом попередження дає 3 бали в рахунок. Один збіг критичного правила дає 5.

Існує порогове значення 5 для показника аномалії, щоб блокувати трафік. Таким чином, достатньо одного критичного збігу правила, щоб WAF шлюзу додатків заблокував запит, навіть у режимі запобігання. Але один збіг правила попередження лише збільшує показник аномалії на 3, що само по собі недостатньо для блокування трафіку.

Повідомлення, яке реєструється, коли правило WAF відповідає трафіку, містить значення дії «Заблоковано». Але фактично трафік блокується лише за показник аномалії 5 або вище.

Конфігурація: ви можете налаштувати та розгорнути всі політики WAF за допомогою порталу Azure, REST API, шаблонів Azure Resource Manager і Azure PowerShell. Ви також можете масштабно налаштовувати політики Azure WAF і керувати ними за допомогою інтеграції Firewall Manager (попередня версія).

Моніторинг WAF: важливо стежити за справністю шлюзу додатків. Відстеження справності вашого WAF і додатків, які він захищає, підтримується інтеграцією з Microsoft Defender for Cloud, Azure Monitor і журналами Azure Monitor.

Журнали Application Gateway інтегровані з Azure Monitor (рис. 2.3). Це дозволяє відстежувати діагностичну інформацію, включно зі сповіщеннями та журналами WAF. Ви можете отримати доступ до цієї можливості на вкладці *Діагностика* ресурсу Application Gateway на порталі або безпосередньо через Azure Monitor. Microsoft Defender для хмари

Defender for Cloud допомагає запобігати загрозам, виявляти їх і реагувати на них. Він забезпечує покращену видимість і контроль безпеки ваших ресурсів Azure. Application Gateway (рис. 2.5) інтегровано з Defender for Cloud. Defender for Cloud сканує ваше середовище, щоб виявити незахищені веб-додатки. Він може рекомендувати Application Gateway WAF для захисту цих вразливих ресурсів. Ви створюєте брандмауери безпосередньо в Defender for Cloud. Ці екземпляри WAF інтегровані з Defender for Cloud. Вони надсилають сповіщення та інформацію про здоров’я в Defender for Cloud для звітування.

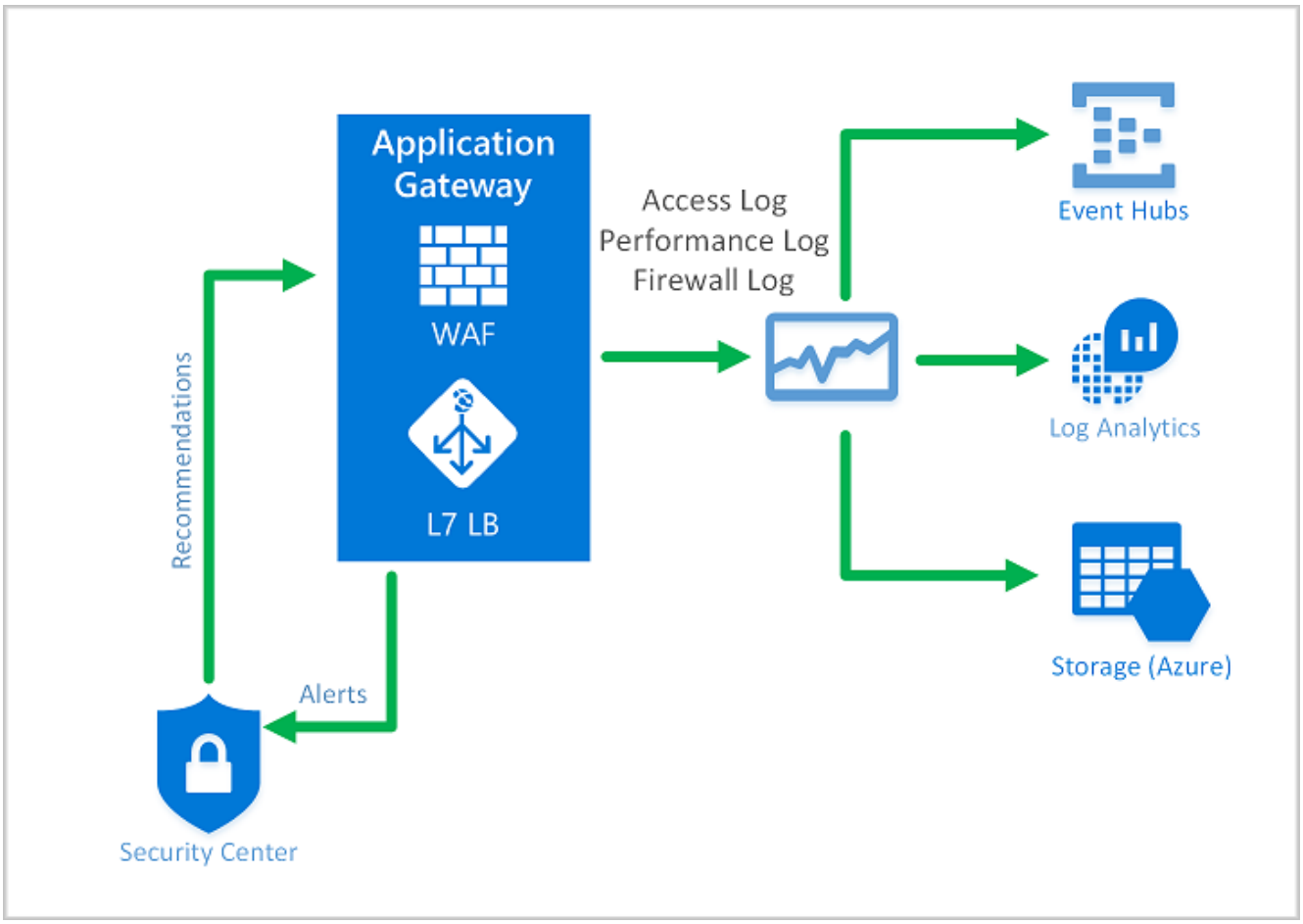

Рис. 2.3. Процеси Azure Monitor [10]

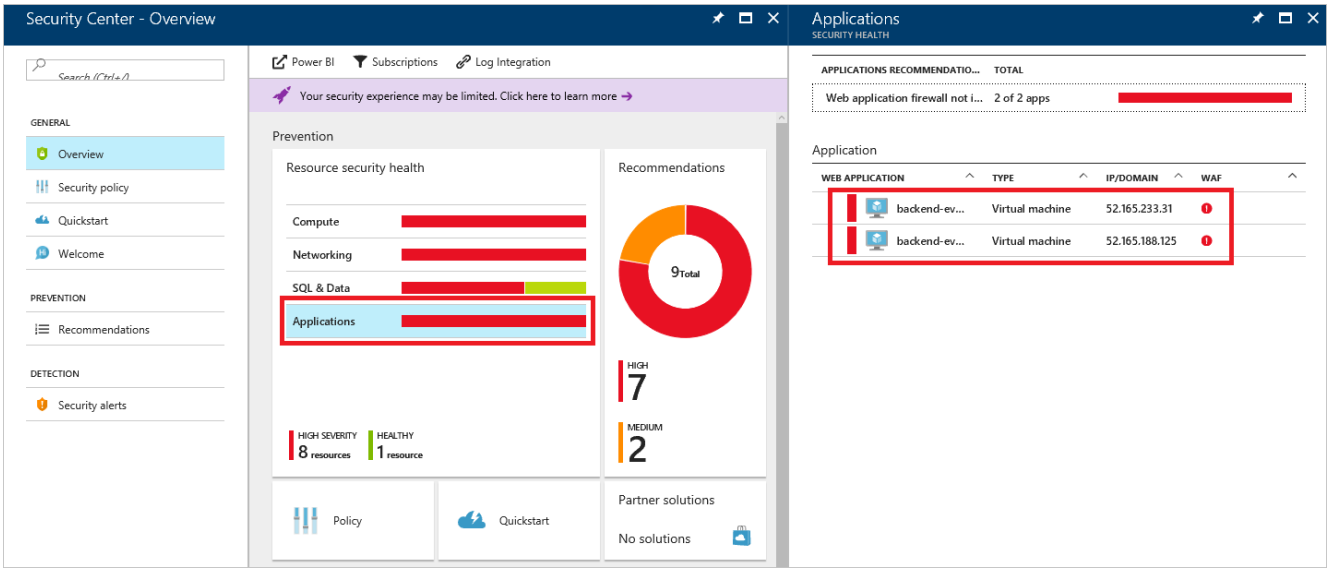

Рис. 2.4. Інтерфейс Security Center [10]

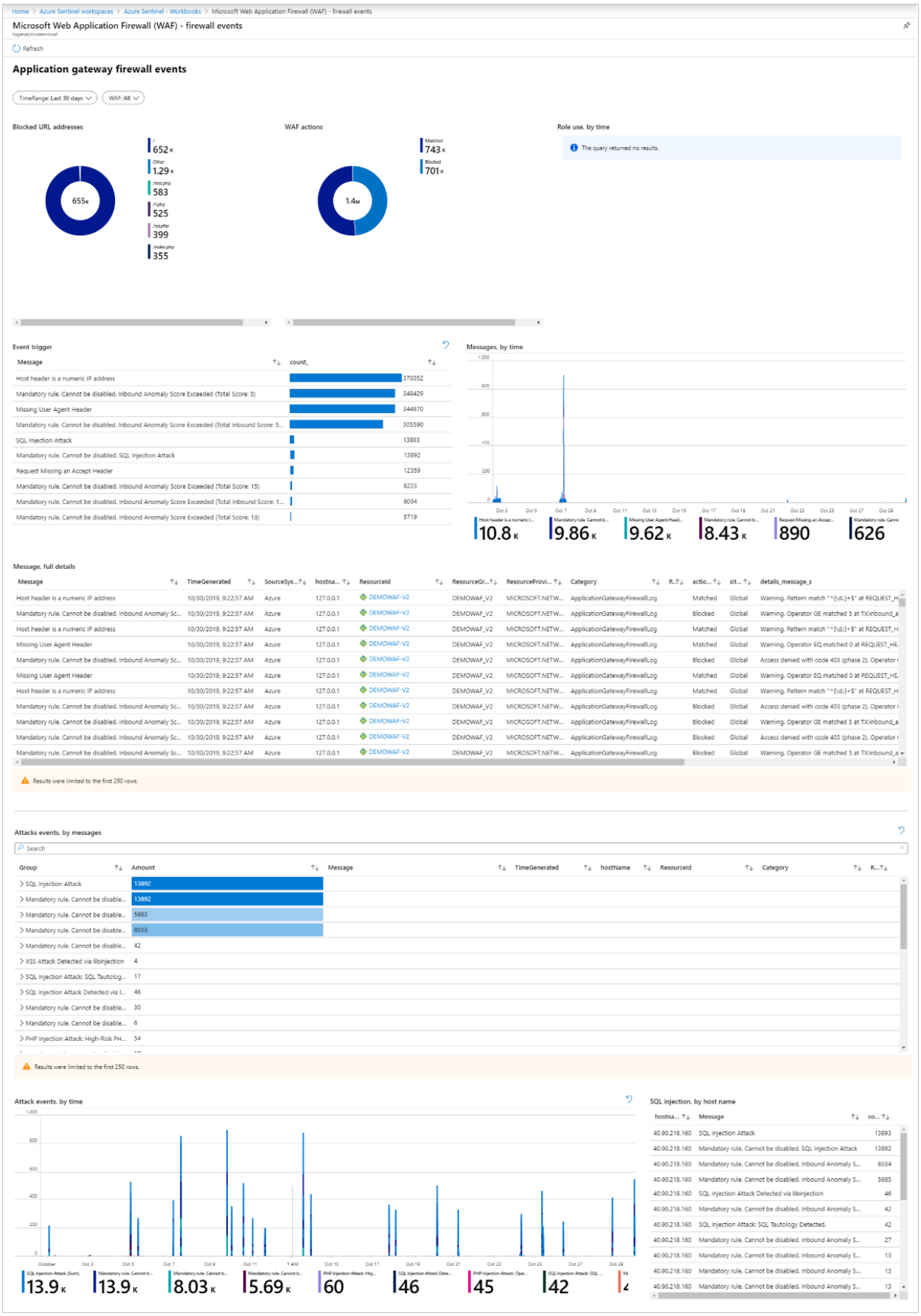

Рис 2.5. Application Gateway WAF

Microsoft Sentinel – це масштабоване хмарне рішення для керування подіями безпеки (SIEM) і автоматизованого реагування на оркестрування безпеки (SOAR). Microsoft Sentinel забезпечує інтелектуальну аналітику безпеки та розвідку про загрози для всього підприємства, надаючи єдине рішення для виявлення попереджень, видимості загроз, проактивного пошуку та реагування на загрози.

За допомогою вбудованої робочої книги подій брандмауера Azure WAF ви можете отримати огляд подій безпеки на своєму WAF (рис. 2.5). Це включає події, відповідні та заблоковані правила та все інше, що реєструється в журналах брандмауера.

Робоча книга Azure Monitor для WAF дозволяє користувацьку візуалізацію подій WAF, пов’язаних із безпекою, на кількох панелях, які можна фільтрувати. Він працює з усіма типами WAF, включаючи Application Gateway, Front Door і CDN, і може бути відфільтрований на основі типу WAF або конкретного екземпляра WAF. Імпорт через шаблон ARM або шаблон галереї.

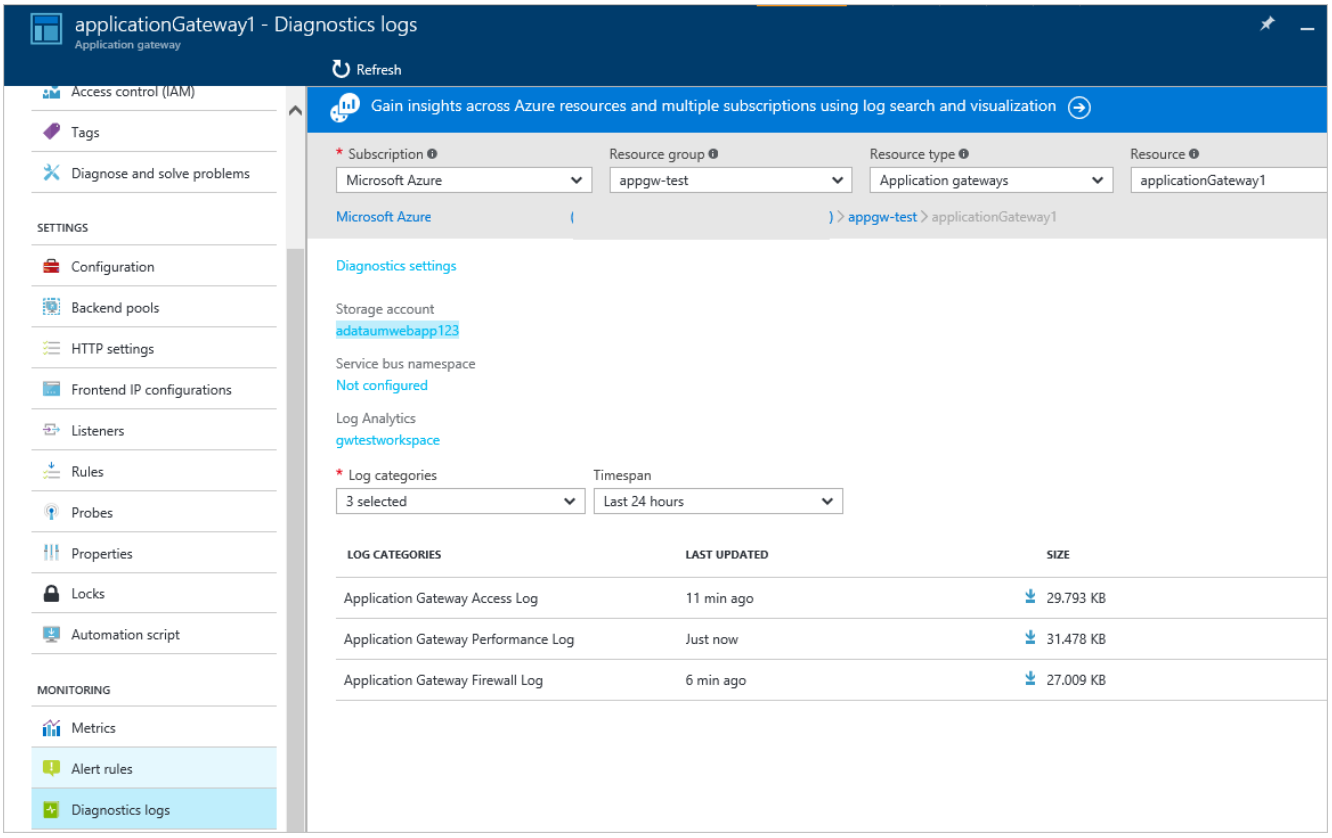

Рис. 2.6. Журнали Application Gateway WAF

Application Gateway WAF надає докладний звіт про кожну виявлену загрозу (рис. 2.6). Ведення журналів інтегровано з журналами Azure Diagnostics. Сповіщення записуються у форматі .json. Ці журнали можна інтегрувати з журналами Azure Monitor.

2.3. Призначення та застосування основних наборів правил брандмауера веб-додатків

Брандмауер веб-додатків (WAF) Application Gateway захищає веб-додатки від поширених уразливостей і експлойтів. Це робиться за допомогою правил, визначених на основі основних наборів правил OWASP 3.2, 3.1, 3.0 або 2.2.9. Для кожної системи правил можна вимикати окреме правило або можна встановити певні дії за окремим правилом [12].

Розглянемо що із себе представляють *основні набори правил (Core rule sets, CRS).*

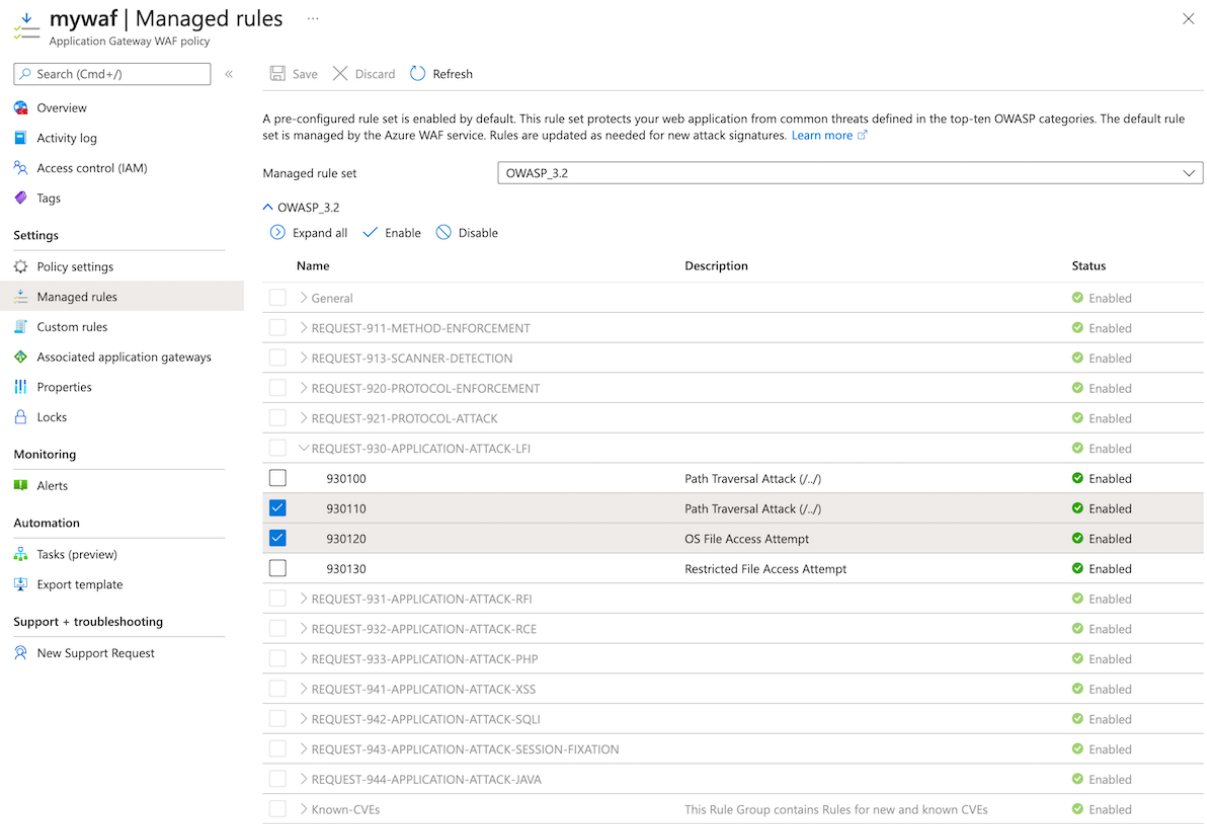

Рис. 2.7. Інтерфейс керування CRS [12]

Шлюз додатків WAF за замовчуванням попередньо налаштований із CRS 3.2, але можна вибрати будь-яку іншу підтримувану версію CRS.

CRS 3.2 пропонує новий механізм і нові набори правил для захисту від інфекцій Java, початковий набір перевірок завантаження файлів і менше помилкових спрацьовувань порівняно з попередніми версіями CRS. Адміністратор може налаштувати правила відповідно до своїх потреб. Інтерфейс керування правилами показано на рис. 2.7.

WAF захищає від таких веб-уразливостей:

атаки SQL-ін'єкції;

міжсайтові скриптові атаки;

інші поширені атаки, такі як ін’єкція команди, контрабанда запитів HTTP, розбиття відповіді HTTP та віддалене включення файлів;

порушення протоколу HTTP;

аномалії протоколу HTTP, такі як відсутність агента користувача та приймання заголовків;

боти, сканери та сканери;

поширені неправильні налаштування додатків (наприклад, Apache та IIS).

CRS увімкнено за умовчанням у режимі виявлення у політиках WAF. Ви можете вимкнути або ввімкнути окремі правила в основному наборі правил відповідно до вимог ваших додатків. Ви також можете встановити конкретні дії для кожного правила. CRS підтримує блокування, журнал і оцінку аномалій. Набір правил Bot Manager підтримує дії дозволу, блокування та журналу [12].

Іноді вам може знадобитися пропустити певні атрибути запиту з оцінки WAF. Типовим прикладом є маркери, вставлені в Active Directory, які використовуються для автентифікації. Ви можете налаштувати виключення для застосування під час оцінки певних правил WAF або глобального застосування до оцінки всіх правил WAF. Правила виключення застосовуються до всіх веб-додатків.

За замовчуванням CRS версії 3.2 і вище використовуватиме підрахунок аномалій, коли запит збігається з правилом, CRS 3.1 і нижче блокуватимуть

відповідні запити за замовчуванням. Крім того, у тій самій політиці WAF можна налаштувати власні правила, якщо ви бажаєте обійти будь-які попередньо налаштовані правила в основному наборі правил [12].

Користувацькі правила завжди застосовуються до того, як оцінюються правила в основному наборі правил. Якщо запит відповідає спеціальному правилу, застосовується відповідна дія правила. Запит або блокується, або передається до серверної частини. Жодні інші спеціальні правила або правила в основному наборі правил не обробляються.

Підрахунок аномалій. Коли ви використовуєте CRS, ваш WAF налаштований на використання оцінки аномалій за замовчуванням. Трафік, який відповідає будь-якому правилу, не блокується негайно, навіть коли ваш WAF перебуває в режимі запобігання. Натомість набори правил OWASP визначають рівень серйозності для кожного правила: критичне, помилка, попередження або сповіщення. Серйозність впливає на числове значення для запиту, яке називається оцінкою аномалії:

Якщо оцінка аномалії становить 5 або більше, WAF блокує запит. Наприклад, одного збігу критичного правила достатньо, щоб WAF заблокував запит, оскільки загальна оцінка аномалії становить 5. Однак одна відповідність правила Попередження збільшує оцінку аномалії лише на 3, що само по собі недостатньо для блокування трафік.

OWASP CRS 3.2 – CRS 3.2 містить 14 груп правил, як показано в наступній таблиці 2.1. Кожна група містить кілька правил, які можна вимкнути. Набір правил базується на версії OWASP CRS 3.2.0.

Механізм брандмауера веб-застосунків Azure (WAF) – це компонент, який перевіряє трафік і визначає, чи містить запит підпис, який представляє потенційну атаку, і вживає відповідних дій залежно від конфігурації.

Новий механізм WAF є високопродуктивним, масштабованим, запатентованим механізмом Microsoft і має значні покращення порівняно з попереднім механізмом WAF.

Таблиця 2.1

Групи правил CRS 3.2

Група правил	опис
Загальний	Загальна група
ВІДОМО-CVES	Допоможіть виявити нові та відомі CVE
ЗАПИТ-911-МЕТОД-ВИКОНАННЯ	Методи блокування (PUT, PATCH)
ЗАПИТ-913-СКАНЕР-ВИЯВЛЕННЯ	Захист від сканерів портів і середовища
ЗАПИТ-920-ПРОТОКОЛ-ВИКОНАННЯ	Захист від проблем з протоколом і кодуванням
ЗАПИТ-921-ПРОТОКОЛ-АТАКА	Захист від введення заголовка, контрабанди запитів і розділення відповідей
REQUEST-930-APPLICATION-ATTACK-LFI	Захист від атак на файли та шляхи
REQUEST-931-APPLICATION-ATTACK-RFI	Захист від атак віддаленого включення файлів (RFI).
REQUEST-932-APPLICATION-ATTACK-RCE	Знову захистити від атак віддаленого виконання коду
REQUEST-933-APPLICATION-ATTACK-PHP	Захист від PHP-ін'єкційних атак
REQUEST-941-APPLICATION-ATTACK-XSS	Захист від атак міжсайтових сценаріїв
REQUEST-942-APPLICATION-ATTACK-SQLI	Захист від атак SQL-ін'єкцій
ЗАПИТ-943-ЗАЯВКА-АТАКА-СЕСІЯ-ФІКСАЦІЯ	Захист від атак із фіксацією сесії
REQUEST-944-APPLICATION-ATTACK-JAVA	Захист від атак JAVA

Новий двигун, випущений разом із CRS 3.2, забезпечує такі переваги:

Покращена продуктивність: значне покращення затримки WAF, включаючи затримки P99 POST і GET. Ми спостерігали значне зменшення хвостових затримок P99 із приблизно 8-кратним скороченням обробки запитів POST і приблизно 4-кратним скороченням обробки запитів GET.

Збільшений масштаб: більша кількість запитів за секунду (RPS), використовуючи ту саму обчислювальну потужність і з можливістю обробки запитів більшого розміру. Наш двигун наступного покоління може масштабувати до 8 разів більше RPS, використовуючи ту саму обчислювальну потужність, і має здатність обробляти в 16 разів більші розміри запитів (розміри запитів до 2 МБ), що було неможливо з попереднім механізмом.

Кращий захист: новий оновлений механізм із ефективною обробкою регулярних виразів забезпечує кращий захист від атак на відмову в обслуговуванні (DOS) RegEx, зберігаючи стабільну затримку.

Багатший набір функцій: нові функції та майбутні вдосконалення доступні лише через новий механізм.

Підтримка нових функцій. Є багато нових функцій, які підтримуються лише механізмом Azure WAF. Функції включають:

CRS 3.2;

обмеження розміру тіла запиту збільшено до 2 МБ;

обмеження завантаження файлів збільшено до 4 ГБ;

показники WAF v2;

виключення за правилом і підтримка атрибутів виключення за назвою;

нові функції WAF будуть випущені лише з пізнішими версіями CRS на новому механізмі WAF.

Існує різниця між запитами журналу попереднього механізму та нового механізму WAF, коли спеціальне правило визначає тип дії як Log.

Коли ваш WAF працює в режимі запобігання, попередній механізм реєструє тип дії запиту як заблокований, навіть якщо запит дозволено настроюваним правилом. У режимі виявлення попередній механізм реєструє той самий тип дії запиту, що й Detected. Навпаки, нова система WAF реєструє тип дії запиту як Log, незалежно від того, чи працює WAF у режимі запобігання чи виявлення.

3 ТЕХНОЛОГІЯ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ ПРИ ЗАСТОСУВАННІ ХМАРНИХ ПЛАТФОРМ

3.1. Порядок створення шлюзу додатку з брандмауером веб-додатку за допомогою порталу Azure

Розглянемо, як використовувати портал Azure для створення шлюзу додатків із брандмауером веб-додатків (WAF). WAF використовує правила OWASP для захисту веб додатків. Ці правила включають захист від таких атак, як впровадження SQL, атаки міжсайтових сценаріїв і викрадення сеансу [13].

Після створення шлюзу додатків ви перевіряєте його, щоб переконатися, що він працює правильно. За допомогою Azure Application Gateway ви спрямовуєте веб-трафік свого додатку на певні ресурси, призначаючи слухачів для портів, створюючи правила та додаючи ресурси до фонового пулу [13].

Ми розглянемо налаштування із загальнодоступною IP-адресою переднього плану, базовим слухачем для розміщення одного сайту на цьому шлюзі додатку, двома віртуальними машинами, які використовуються для фонового пулу, і базовим правилом маршрутизації запитів.

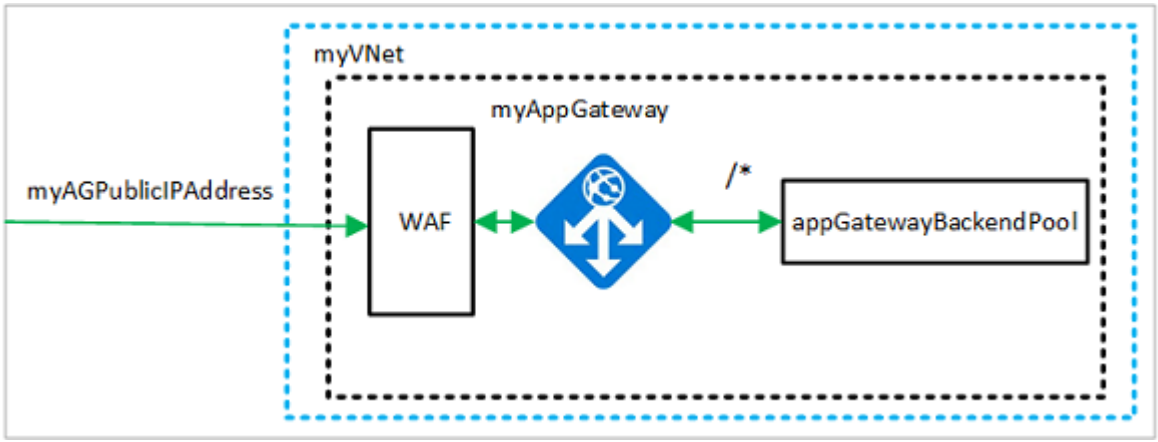

Рис. 3.1. Схема налаштувань WAF [13]

Розглянемо порядок створення шлюзу додатку з увімкненим WAF [13]:

1. Виберіть *Створити ресурс* у лівому меню порталу Azure. З'явиться нове вікно.

2. Виберіть *Мережа*, а потім виберіть *Шлюз додатків* у списку *Рекомендовані*.

Вкладка *Basics* (рис. 3.2).

1. На вкладці *Basics* введіть ці значення для таких налаштувань шлюзу додатків:

- Група ресурсів: виберіть *myResourceGroupAG* для групи ресурсів. Якщо він не існує, виберіть *Створити новий*, щоб створити його.

- Назва шлюзу додатків: введіть *myAppGateway* як назву шлюзу додатків.

- Рівень: виберіть *WAF V2*.

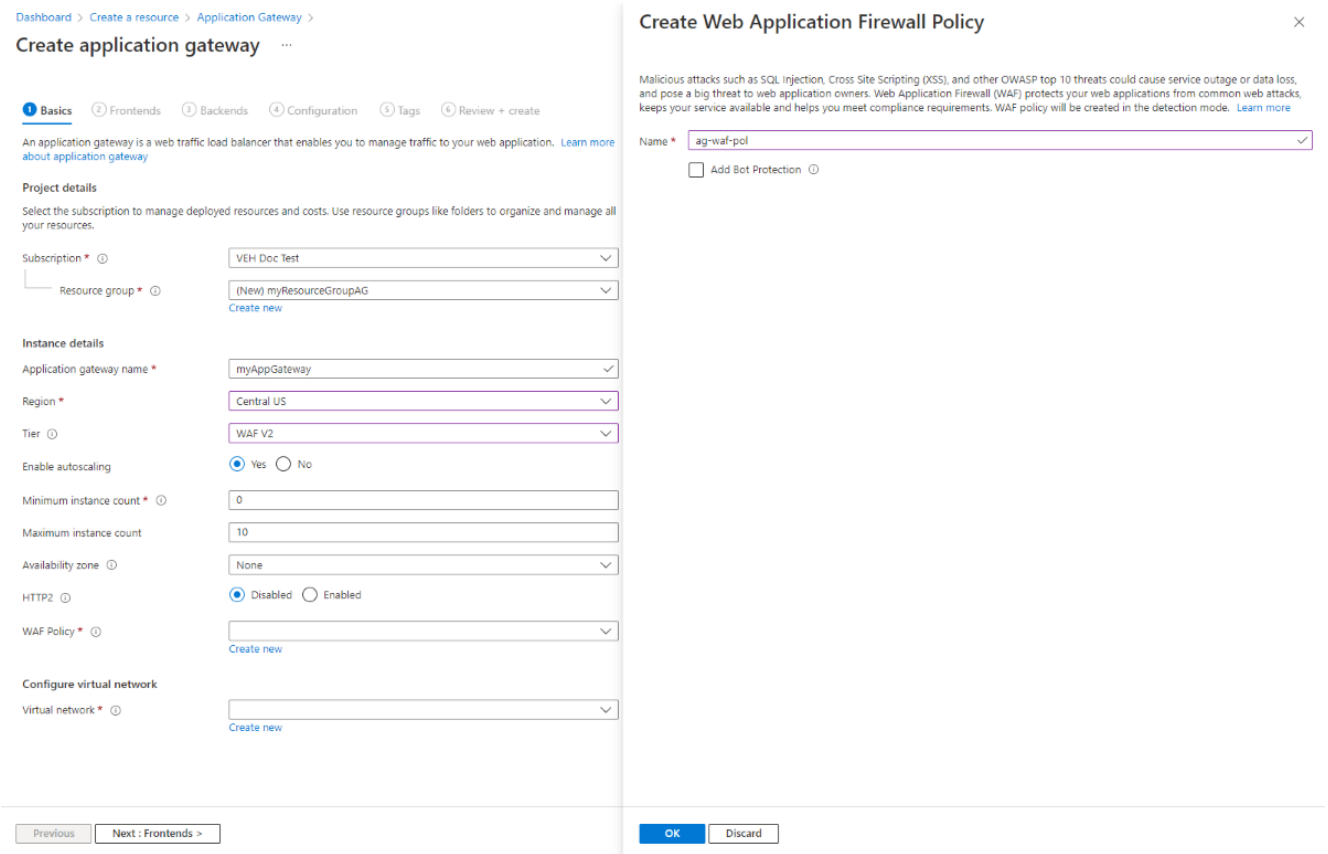

Рис. 3.2. Вкладка Basics

- Політика WAF: виберіть *Створити нову*, введіть ім’я для нової політики, а потім виберіть *ОК*. Це створює базову політику WAF із керованим набором

основних правил (CRS).

Щоб Azure міг обмінюватися даними між ресурсами, які ви створюєте, йому потрібна віртуальна мережа. Ви можете створити нову віртуальну мережу або використати існуючу. У цьому прикладі ви створюєте нову віртуальну мережу одночасно зі створенням шлюзу додатків. Екземпляри Application Gateway створюються в окремих підмережах. У цьому прикладі ви створюєте дві підмережі: одну для шлюзу додатків, а іншу – для внутрішніх серверів [13].

У вкладці *Налаштувати віртуальну мережу* (рис. 3.3) виберіть *Створити нову*, щоб створити нову віртуальну мережу. У вікні *Створити віртуальну мережу*, що відкриється, введіть такі значення, щоб створити віртуальну мережу та дві підмережі:

- Ім’я: введіть *myVNet* як назву віртуальної мережі.
- Ім’я підмережі (підмережа шлюзу додатків): у сітці підмереж відображатиметься підмережа під назвою *За замовчуванням*. Змініть назву цієї підмережі на *myAGSubnet*.
- Підмережа шлюзу додатків може містити лише шлюзи додатків. Інші ресурси заборонені.
- Ім’я підмережі (підмережа внутрішнього сервера): у другому рядку сітки підмереж введіть *myBackendSubnet* у стовпці *Ім’я підмережі*.

Діапазон адрес (підмережа внутрішнього сервера): у другому рядку таблиці підмереж введіть діапазон адрес, який не збігається з діапазоном адрес *myAGSubnet*. Наприклад, якщо діапазон адрес *myAGSubnet* становить 10.21.0.0/24, введіть 10.21.1.0/24 для діапазону адрес *myBackendSubnet*.

Виберіть *OK*, щоб закрити вікно створення віртуальної мережі та зберегти налаштування віртуальної мережі.

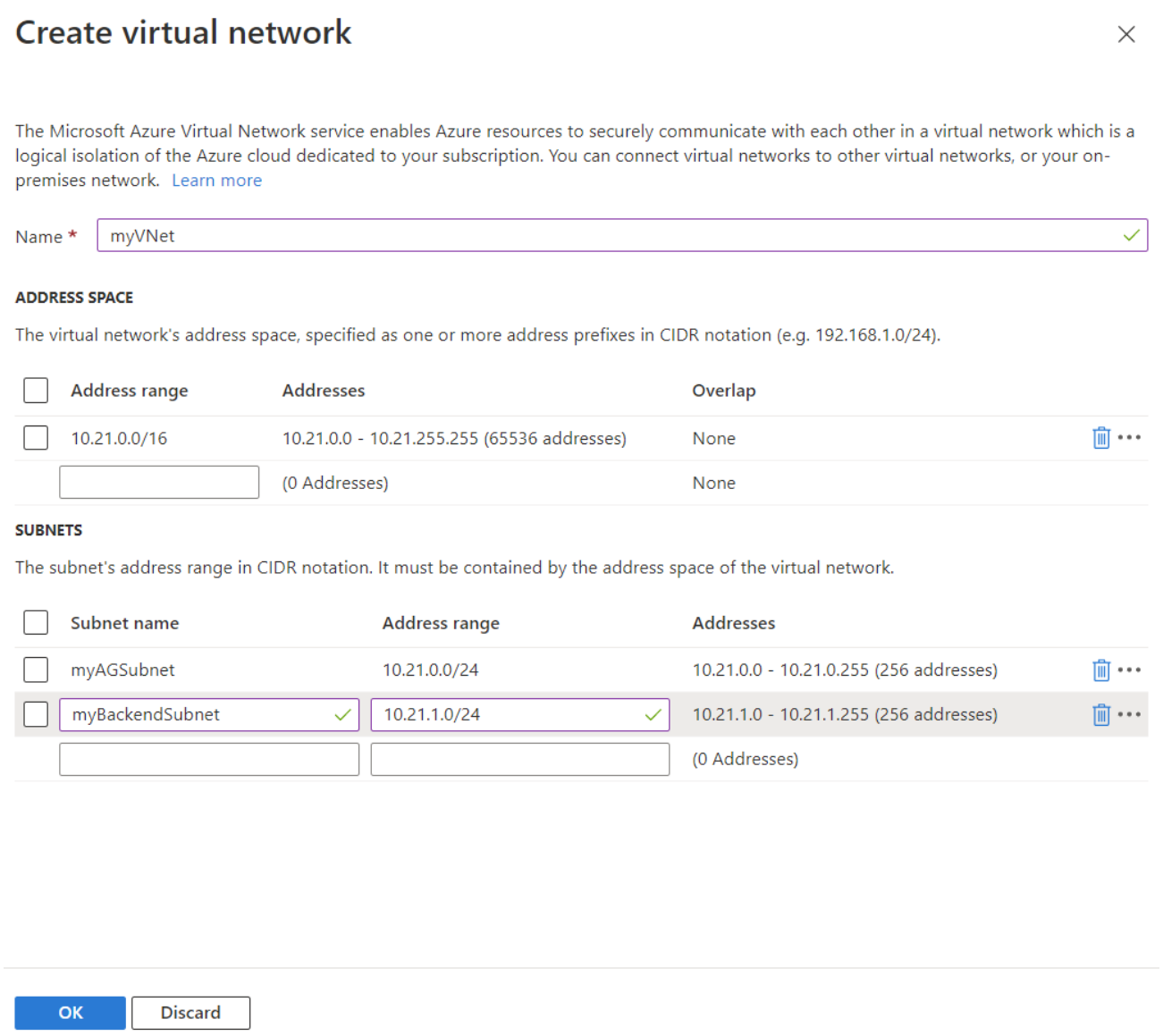

Рис. 3.3. Вкладка Налаштувати віртуальну мережу

На вкладці *Basics* прийміть значення за замовчуванням для інших налаштувань, а потім виберіть *Далі: Інтерфейси*.

Вкладка *Frontends* (рис. 3.4).

1. Переконайтеся, що на вкладці *Frontend* для типу IP-адреси *Frontend* встановлено значення *Public*.

Ви можете налаштувати IP-адресу зовнішнього інтерфейсу як загальнодоступну або обидва відповідно до свого сценарію використання. У цьому прикладі ви виберете публічну IP-адресу зовнішнього інтерфейсу.

2. Виберіть *Додати нову* для загальнодоступної IP-адреси та введіть *myAGPublicIPAddress* для загальнодоступної IP-адреси, а потім виберіть *ОК*.

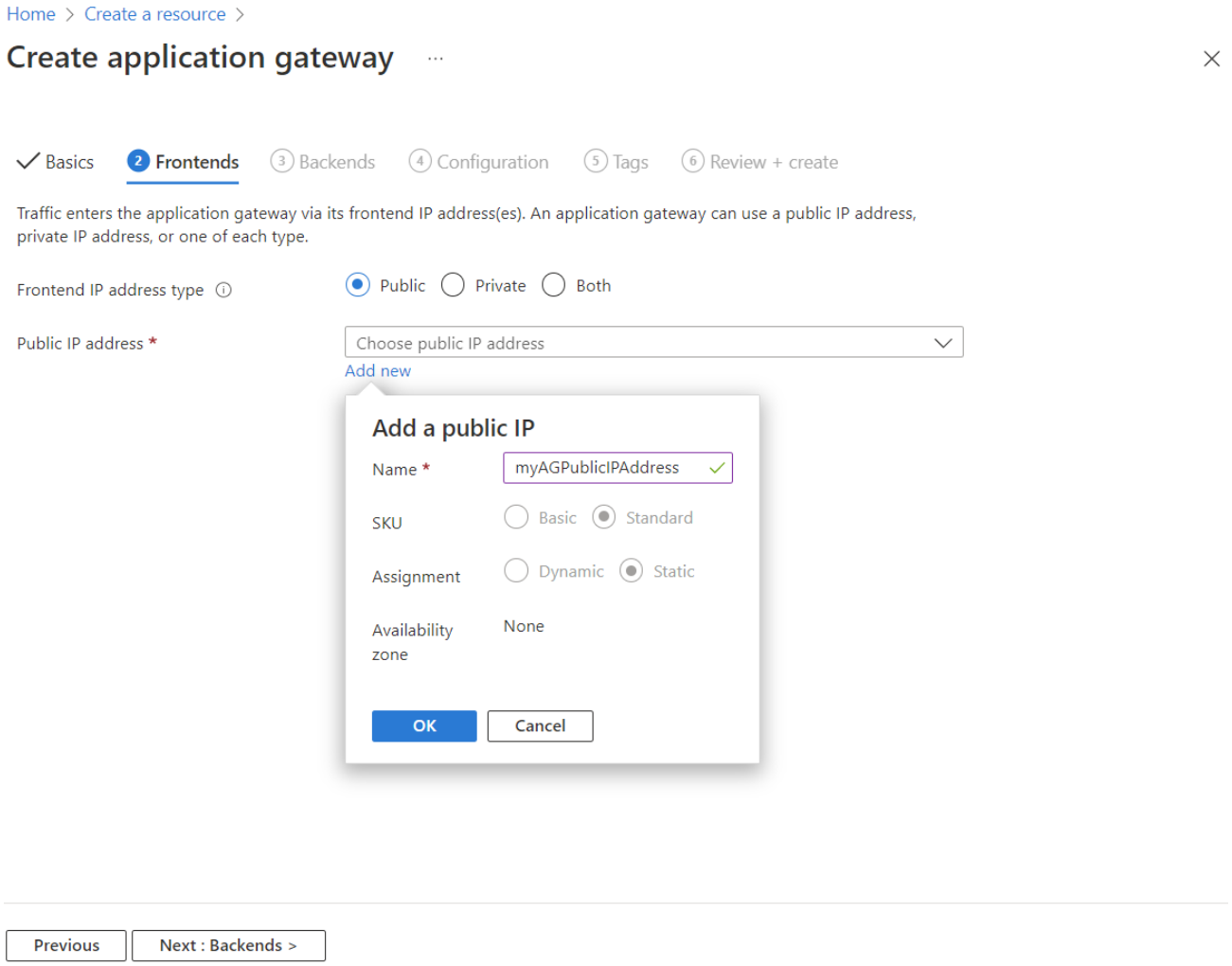

Рис. 3.4. Вкладка Frontends

Вкладка *Backends* (рис. 3.5).

1. Базовий пул використовується для маршрутизації запитів на внутрішні сервери, які обслуговують запит. Бекенд-пули можуть складатися з мережевих карток, масштабованих наборів віртуальних машин, загальнодоступних IP-адрес, внутрішніх IP-адрес, повних доменних імен (FQDN) і мультитенантних серверних інтерфейсів, як-от Azure App Service. У цьому прикладі створюється порожній серверний пул зі шлюзом додатків, а потім додається до нього серверні дані.

2. На вкладці *Сервери* виберіть *Додати пул серверів*.

У вікні *Додати внутрішній пул*, що відкриється, введіть такі значення, щоб створити порожній внутрішній пул:

Ім’я: введіть *myBackendPool* як назву внутрішнього пулу.

3. Додати внутрішній пул без цілей: виберіть *Так*, щоб створити внутрішній

пул без цілей. Ви додасте серверні цілі після створення шлюзу додатків.

У вікні *Add a backend pool* виберіть *Додати*, щоб зберегти конфігурацію серверного пулу та повернутися до вкладки Backends.

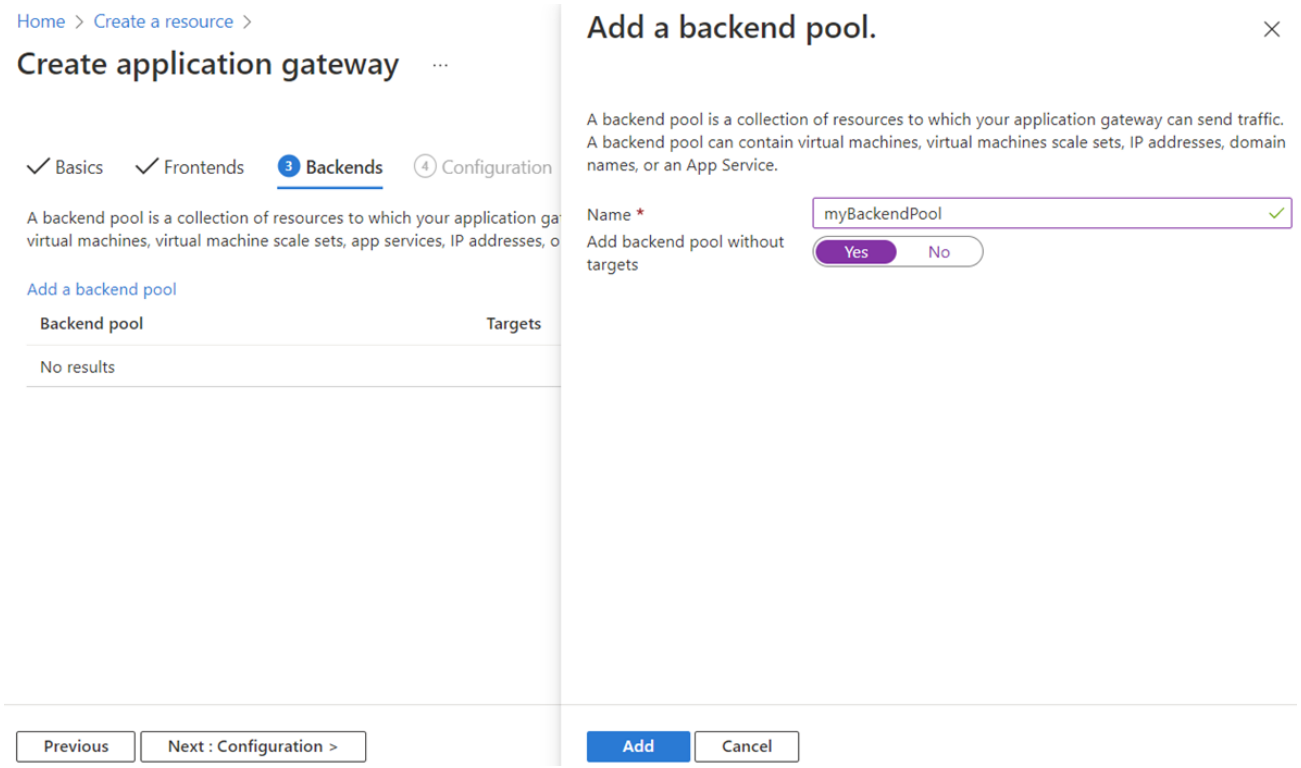

Рис. 3.5. Вкладка Backends

На вкладці *Сервери* виберіть *Далі: Конфігурація*.

Вкладка *Конфігурації* (рис. 3.6).

1. На вкладці *Конфігурація* ви з'єднаєте зовнішній і внутрішній пул, створений за допомогою правила маршрутизації.

2. Виберіть *Додати правило маршрутизації* в стовпці *Правила маршрутизації*.

3. У вікні *Додати правило маршрутизації*, що відкриється, введіть *myRoutingRule* для імені правила.

4. У полі *Пріоритет* введіть номер пріоритету.

Для правила маршрутизації потрібен слухач. На вкладці *Прослуховувач* у вікні *Додати правило маршрутизації* введіть такі значення для приймача:

- Ім’я слухача: введіть *myListener* для імені слухача.
- IP-адреса зовнішнього інтерфейсу: виберіть *Загальнодоступний*, щоб вибрати загальнодоступну IP-адресу, яку ви створили для інтерфейсу.

Прийміть значення за замовчуванням для інших параметрів на вкладці *Listener*, а потім виберіть вкладку *Backend targets*, щоб налаштувати решту правила маршрутизації.

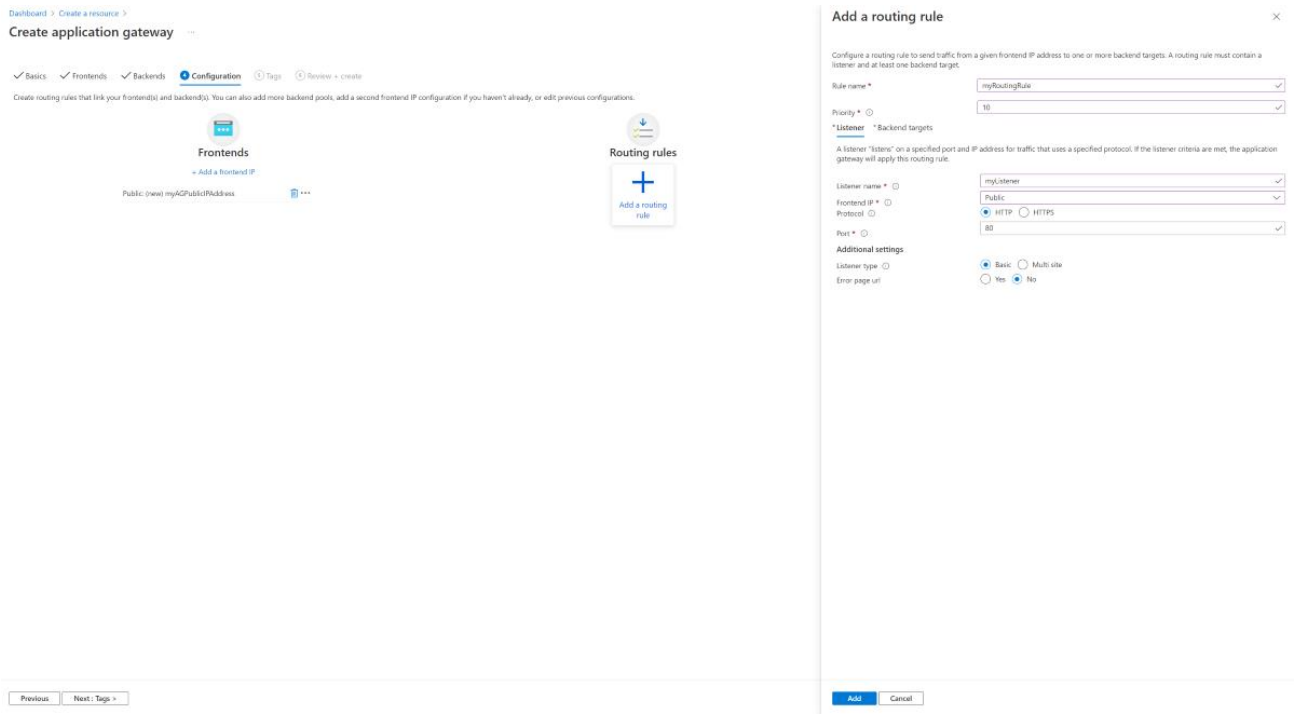

Рис. 3.6. Вкладка Конфігурації

5. На вкладці *Backend targets* (рис. 3.7) виберіть *myBackendPool* для *Backend target.*

6. Щоб створити нове налаштування серверної частини, виберіть *Додати новий*. Цей параметр визначає поведінку правила маршрутизації. У вікні *Add Backend setting*, що відкриється, введіть *myBackendSetting* для назви налаштувань *Backend*. Прийміть значення за замовчуванням для інших параметрів у вікні, а потім виберіть *Додати*, щоб повернутися до вікна *Додати правило маршрутизації.*

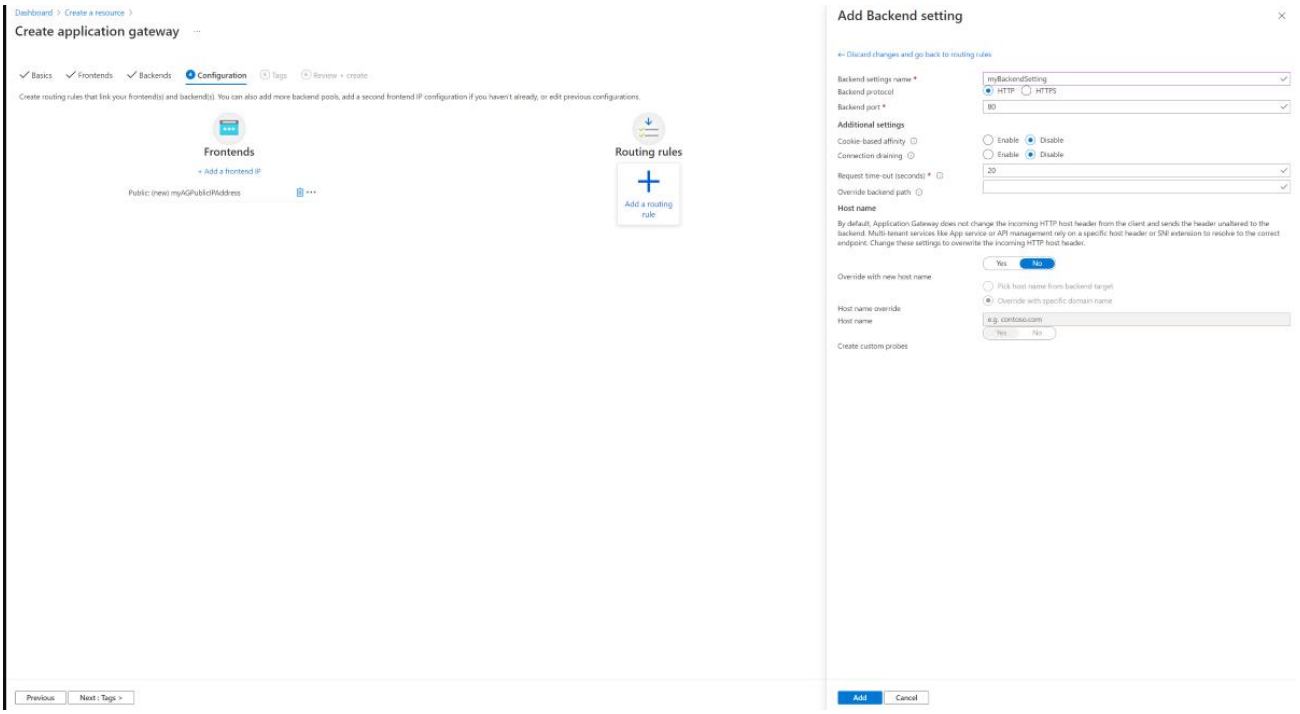

Рис. 3.7. Вкладка Backend targets

7. У вікні *Додати правило маршрутизації* виберіть *Додати*, щоб зберегти правило маршрутизації та повернутися на вкладку *Конфігурація*.

8. Виберіть *Далі: теги*, а потім *Далі: перегляд + створення*.

Перегляд + створення вкладки.

Перегляньте налаштування на вкладці *Перегляд + створення*, а потім виберіть *Створити*, щоб створити віртуальну мережу, загальнодоступну IP-адресу та шлюз додатків. Створення шлюзу додатків в Azure може зайняти кілька хвилин.

Зачекайте, поки розгортання завершиться успішно, перш ніж переходити до наступного розділу.

Додайте серверні цілі.

У цьому прикладі ви використовуватимете віртуальні машини як цільовий сервер. Ви можете використовувати існуючі віртуальні машини або створювати нові. Ви створите дві віртуальні машини, які Azure використовуватиме як внутрішні сервери для шлюзу додатків.

Для цього ви:

1. Створіть дві нові віртуальні машини Linux, *myVM* і *myVM2*, які

використовуватимуться як внутрішні сервери.

2. Встановіть NGINX на віртуальних машинах, щоб переконатися, що шлюз додатків створено успішно.

3. Додайте внутрішні сервери до внутрішнього пулу.

Створіть віртуальну машину.

1. На порталі Azure виберіть *Створити ресурс*. З'явиться вікно *Створити ресурс*.

2. У розділі *Віртуальна машина* виберіть *Створити.*

3. Введіть ці значення на вкладці *Basics* для таких параметрів віртуальної машини:

- Група ресурсів: виберіть *myResourceGroupAG* для імені групи ресурсів.

- Ім'я віртуальної машини: введіть *myVM* для імені віртуальної машини.

- Зображення: *Ubuntu Server 20.04 LTS - Gen2.*

- Тип автентифікації: *Пароль*.

- Ім'я користувача: введіть ім'я користувача адміністратора.

- Пароль: введіть пароль для пароля адміністратора.

- Публічні вхідні порти: виберіть *Немає.*

4. Прийміть інші параметри за замовчуванням і виберіть *Далі: Диски*.

5. Прийміть стандартні налаштування вкладки *Диски*, а потім виберіть *Далі: Мережа*.

6. На вкладці *Мережа* переконайтеся, що для віртуальної мережі вибрано *myVNet*, а для підмережі встановлено значення *myBackendSubnet.*

7. Для *Public IP* виберіть *None*.

8. Прийміть інші параметри за замовчуванням і виберіть *Далі: Керування*.

9. Виберіть *Далі: Моніторинг*, встановіть *Діагностика завантаження* на *Вимкнути*. Прийміть інші параметри за замовчуванням і виберіть *Переглянути + створити*.

10. На вкладці *Перегляд + створення* перегляньте налаштування, виправте всі помилки перевірки, а потім виберіть *Створити.*

11. Перш ніж продовжити, дочекайтеся завершення створення віртуальної

машини.

3.2. Технологія застосування рішення брандмауера веб-додатків на AzureFront Door

Загальні практичні поради по застосуванню WAF [14]:

увімкніть WAF;

налаштуйте свій WAF;

використовуйте режим запобігання;

визначте конфігурацію WAF як код Рекомендації щодо керованого набору правил;

увімкніть набори правил за замовчуванням;

увімкніть правила керування ботом.

Розглянемо найкращі методи використання брандмауера веб-додатків на AzureFront Door. Для додатків, що мають доступ до Інтернету, рекомендуємо ввімкнути брандмауер веб-додатків і налаштувати його на використання керованих правил.

Якщо ви використовуєте WAF і правила, керовані Microsoft, ваш веб-додаток буде захищеним від ряду атак. Правила у вашому WAF слід налаштувати відповідно до вашого робочого навантаження. Якщо ви не налаштуєте свій WAF, він може випадково заблокувати запити, які повинні бути дозволені [14].

Налаштування може передбачати створення виключень правил для зменшення помилкових позитивних виявлень. Поки ви налаштовуєте свій WAF, подумайте про використання режиму виявлення, який реєструє запити та дії, які зазвичай виконує WAF, але фактично не блокує трафік.

Після того, як ви налаштували свій WAF, ви повинні налаштувати його для роботи в режимі запобігання. Працюючи в режимі запобігання, ви гарантуєте, що WAF фактично блокує запити, які він визначає як шкідливі. Запуск у режимі виявлення корисний під час налаштування та конфігурації WAF, але не забезпечує захисту.

Коли ви налаштовуєте свій WAF для робочого навантаження додатку, ви зазвичай створюєте набір виключень правил, щоб зменшити помилкові позитивні виявлення. Якщо ви вручну налаштуєте ці винятки за допомогою порталу Azure, то під час оновлення WAF для використання новішої версії правил вам потрібно буде повторно налаштувати ті самі винятки для нової версії правил.

Цей процес може зайняти багато часу та спричинити помилки. Натомість подумайте про те, щоб визначити свої виключення правил WAF та іншу конфігурацію як код, наприклад, за допомогою Azure CLI, Azure PowerShell, Bicep або Terraform. Тоді, коли вам знадобиться оновити свою версію набору правил WAF, ви зможете легко повторно використати ті самі виключення.

Стандартні набори правил Microsoft розроблено для захисту веб-додатку шляхом виявлення та блокування типових атак. Правила базуються на різних джерелах, включаючи 10 найпопулярніших типів атак OWASP та інформацію від MicrosoftThreat Intelligence.

Боти відповідають за значну частку трафіку до веб-додатків. Набір правил захисту від ботів WAF класифікує ботів на основі того, чи вони хороші, погані чи невідомі. Поганих ботів можна заблокувати, тоді як хорошим роботам, як-от ботам пошукових систем, дозволено до вашого веб додатку.

Корпорація Майкрософт регулярно оновлює керовані правила, щоб врахувати поточний ландшафт загроз. Переконайтеся, що ви регулярно перевіряєте наявність оновлень для наборів правил, якими керує Azure.

WAF Front Door дозволяє контролювати кількість дозволених запитів з IP-адреси кожного клієнта протягом певного періоду часу. Рекомендується додати обмеження швидкості, щоб зменшити вплив клієнтів, які випадково або навмисно надсилають великі обсяги трафіку до вашої служби, наприклад, під час шторму повторних спроб.

Налаштуйте правило обмеження швидкості брандмауера веб-додатків за допомогою Azure PowerShell. Чому додаткові запити, що перевищують порогове значення, налаштоване для мого правила обмеження швидкості, передаються на мій внутрішній сервер? Зазвичай доцільно встановити досить високий поріг

обмеження швидкості. Наприклад, якщо ви знаєте, що IP-адреса одного клієнта може надсилати близько 10 запитів на ваш сервер щохвилини, подумайте про встановлення порогу в 20 запитів на хвилину.

Високі порогові значення швидкості дозволяють уникнути блокування законного трафіку, водночас забезпечуючи захист від надзвичайно великої кількості запитів, які можуть перевантажити вашу інфраструктуру. Багато веб-додатків розроблено для користувачів у певному географічному регіоні. Якщо ця ситуація стосується вашого додатку, подумайте про впровадження геофільтрації, щоб блокувати запити, які надходять із-за меж країн, з яких ви очікуєте отримати трафік.

Деякі IP-адреси не зіставляються з місцями в нашому наборі даних. Якщо IP-адресу не можна зіставити з місцем, WAF призначає трафік невідомій (ZZ) країні. Щоб уникнути блокування дійсних запитів із цих IP-адрес, подумайте про дозвіл невідомого (ZZ) через ваш геофільтр.

WAF Front Door інтегрується з Azure Monitor. Важливо зберігати журнали WAF у цільовому місці, наприклад у Log Analytics. Ви повинні регулярно переглядати журнали WAF. Перегляд журналів допомагає вам налаштувати політику WAF, щоб зменшити кількість хибно-позитивних виявлень і зрозуміти, чи був ваш додаток об’єктом атак.

Надсилання журналів до Microsoft Sentinel.

MicrosoftSentinel – це система керування інформацією про безпеку та подіями (SIEM), яка імпортує журнали та дані з багатьох джерел, щоб зрозуміти ландшафт загроз для вашого веб-додатку та загального середовища Azure. Журнали WAF Front Door слід імпортувати в MicrosoftSentinel або інший SIEM щоб ваші властивості, що виходять в Інтернет, були включені в його аналіз. Для MicrosoftSentinel використовуйте з’єднувач Azure WAF, щоб легко імпортувати свої журнали WAF.

3.3. Рекомендації щодо застосування технології захисту веб-додатків організації

Як рекомендують в OWASP [3] необхідно розробити та втілити програму забезпечення безпеки додатків.

Безпека додатків є необхідною умовою бізнесу. Під тиском регуляторів та зростаючої кількості атак організації повинні розробляти ефективні процеси та засоби забезпечення безпеки своїх додатків та API. Багато організацій намагаються впоратися з величезною кількістю вразливостей у неймовірному обсязі коду вже випущених програм та API.

OWASP [3] рекомендує розробити програму забезпечення безпеки, щоб проаналізувати та покращити безпеку додатків та API. Забезпечення безпеки потребує ефективної взаємодії різних підрозділів організації, включаючи аудиторів, розробників, керівників та адміністраторів. Безпека повинна бути наочною та вимірюваною, щоб можна було побачити та зрозуміти стан безпеки додатків. Зробіть акцент на роботах та результатах, які реально покращать безпеку та усунуть чи зменшать ризики.

На початку роботи необхідно:

задокументувати всі веб-додатки та пов’язані з ними дані. Великим організаціям рекомендується використовувати з цією метою базу даних управління конфігурацією;

розробити програму забезпечення безпеки додатків та почати її реалізацію;

проведіть аналіз можливостей, порівнявши свою організацію з іншими компаніями, щоб визначити ключові області поліпшення та план дій;

отримати схвалення посібника з цих питань та розробити план підвищення поінформованості про безпеку додатків для всієї організації.

Щоб реалізувати загальний підхід на основі ризиків необхідно:

визначити необхідний рівень захисту веб-додатків з погляду бізнесу. При цьому необхідно керуватися законами про конфіденційність та іншими нормативними документами, що стосуються захищених даних;

розробити модель оцінки найбільш поширених загроз із зазначенням факторів ймовірності та ризику, що відображають стійкість вашої організації до атак;

оцінити та пріоритезувати веб-додатки та API. Занести результати до БД керування конфігурацією.

розробити посібник із коректного визначення необхідного рівня покриття та точності.

Під час підготовки надійної бази необхідно:

розробити спеціальні політики та стандарти, які будуть використовуватися всіма розробниками як основи безпеки додатків;

визначити набір стандартних засобів безпеки, які доповнюватимуть ці політики та стандарти, а також які міститиме посібник з їх використання при проектуванні та розробці;

розробити курси з безпеки додатків, присвячені різним темам і цілям розробки.

Необхідно інтегрувати заходи та засоби безпеки в існуючі процеси. Для цього необхідно:

визначити та впровадити в існуючі процеси розробки та експлуатації заходи щодо безпечної реалізації та контролю. Це включає такі заходи: моделювання загроз, безпечне проектування та аналіз проектів, написання безпечного коду та його аналіз, проведення пентесту та усунення недоліків за результатами;

залучати експертів у предметній галузі та служб підтримки для розробників та проектної команди.

Необхідно забезпечити візуальний контроль процесів. Для цього необхідно:

використовувати різні метрики. Приймати рішення про поліпшення та фінансування необхідно на основі метрик та даних аналітики. Метрики повинні відображати засоби та методи забезпечення безпеки, виявлені та усунені вразливості, покриття додатків, опис помилок за типом та кількістю тощо;

проводити аналіз даних щодо реалізації та контролю для пошуку основних причин та шаблонів вразливостей при проведенні стратегічних та системних

покращень у компанії. Враховуйте помилки та пропонуйте заохочення для просування покращень.

Для правильного управління життєвим циклом веб-додатків пропонуються такі заходи відповідно до [3].

Необхідно зазначити, що веб-додатки відносяться до найбільш складних систем, які люди постійно створюють та обслуговують. Адміністрування додатків необхідно доручати IT-фахівцям, які відповідатимуть за весь їхній життєвий цикл. Необхідно призначати адміністраторів додатків, які відповідатимуть за технічні аспекти додатків протягом їх життєвого циклу, починаючи зі збору вимог і закінчуючи виведенням систем з експлуатації, про що часто забувають.

Для організації управління ресурсами необхідно:

зібрати та обговорити із замовником бізнес-вимоги до веб-додатків, включаючи забезпечення конфіденційності, справжності, цілісності та доступності всіх інформаційних активів, а також очікувану бізнес-логіку;

скласти перелік технічних вимог, включаючи функціональні та нефункціональні вимоги щодо безпеки;

спланувати та обговорити бюджет, що охоплює всі аспекти проектування, створення, тестування та експлуатації, а також роботи із забезпечення безпеки.

На етапі запиту пропозицій та укладання контракту необхідно:

обговорити вимоги з внутрішніми та зовнішніми розробниками, включаючи нормативи та вимоги програми безпеки, наприклад, рекомендації щодо життєвого циклу розробки програмного забезпечення;

оцінити виконання всіх технічних вимог, включаючи етап планування та проектування;

обговорити всі технічні вимоги, включаючи проектування, безпеку та гарантійні зобов’язання;

використовувати шаблони та контрольні списки, а також проконсультуватися з юристом перед його використанням.

На етапі планування та проектування веб-додатків необхідно:

обговорити плани та проекти з розробниками та внутрішніми партнерами,

наприклад, фахівцями з безпеки;

визначити архітектуру та засоби керування безпекою, а також контрзаходи, які відповідають вимогам захисту та очікуваним рівням небезпеки. Все це має забезпечуватись фахівцями з безпеки;

переконатися, що власник додатку приймає інші ризики або надає додаткові ресурси.

забезпечити створення записів з безпеки із зазначенням обмежень, доданих для нефункціональних вимог.

На етапі розгортання, тестування та впровадження веб-додатків необхідно:

автоматизувати безпечне розгортання додатку, інтерфейсів та компонентів, а також отримання необхідних дозволів;

протестувати технічні можливості та інтеграцію з IT-архітектурою, а також організувати бізнес-тестування;

протестуйте штатне та нештатне використання технічних та продуктивних можливостей;

організувати тестування безпеки відповідно до внутрішніх процесів, вимог захисту та передбачуваного рівня небезпеки для кожного веб-додатку;

ввести веб-додаток в експлуатацію та заборонити використовувати старі програми без потреби;

погодити всю документацію, базу даних контролю змін та архітектуру безпеки.

На етапі проведення роботи та контролю змін необхідно:

роботи повинні включати управління безпекою веб-додатку (наприклад, управління оновленнями);

постійно звертати увагу користувачів на безпеку та знайти компроміс між практичністю та безпекою;

спланувати та проводити модифікації, наприклад, перехід на нову версію програми або використання інших компонентів (ОС, програмне забезпечення або бібліотек);

оновлювати документацію, включаючи документацію з контролю змін,

архітектуру безпеки, елементи керування та заходи протидії, а також документацію з поточних завдань або проектів.

На етапі виведення з експлуатації додатку необхідно:

усі важливі дані необхідно заархівувати, а решту безпечно видалити;

здійснити безпечне виведення додатку з експлуатації, включаючи видалення облікових записів, що не використовуються, а також ролей і дозволів;

встановити статус додатку “виведено з експлуатації” у БД контролю змін.

Необхідно підкреслити важливість такого організаційного моменту при побудові системи захисту веб-додатків як тест на проникнення. Саме він стане оптимальним способом перевірки захищеності інформаційної системи за допомогою імітації спрямованих атак. Тест на проникнення дає можливість оцінити захищеність інформаційної системи від несанкціонованого впливу, використовуючи різні моделі вторгнень.

Тест на проникнення для веб-додатків фокусує свою увагу виключно на оцінці рівня захисту веб-додатків. Процес складається з активного аналізу додатків і пошуку в них вразливостей, технічних помилок або інших проблем. Інформацію про всі слабкі місця відображається в підсумковому звіті.

ВИСНОВКИ

В роботі проведено дослідження проблеми захисту веб-додатків організації при застосуванні хмарних платформ як складової частини забезпечення кібербезпеки її інформаційних ресурсів.

Microsoft Azure – це платформа хмарних обчислень, яка допомагає розробляти, зберігати дані, розміщувати та керувати послугами. Інструмент Azure розміщує веб-додатки через Інтернет за допомогою центрів обробки даних Microsoft. Тому, Microsoft Azure широко застосовується у сучасних організаціях.

Проаналізовано існуючі технології захисту веб-додатків організації при застосуванні хмарних платформ. Рішення брандмауера веб-додатків (Web Application Firewall) в світі вже встигли набрати достатню популярність, і такі компанії як Amazon та Microsoft надають захищені сервіси на базі продуктів даного класу. WAF захищає розміщені веб-додатки від атак, спрямованих на відомі та невідомі експлойти.

Досліджено методи та засоби захисту веб-додатків організації в Azure. Розглянуто призначення та основні функції брандмауера веб-додатків Azure. Він надає централізований захист веб-додатків від поширених експлойтів і вразливостей.

Розглянуто призначення та основні функції брандмауера веб-додатків Azure на шлюзі додатків Azure. WAF на шлюзі додатків базується на основному наборі правил (Core rule sets, CRS) від Open Web Application Security Project (OWASP).

Досліджено призначення та застосування основних наборів правил брандмауера веб-додатків. Захист веб-додатків відбувається за допомогою правил, визначених на основі основних наборів правил OWASP 3.2, 3.1, 3.0 або 2.2.9. Для кожної системи правил можна вимикати окреме правило або можна встановити певні дії за окремим правилом.

У роботі розглянуто порядок створення шлюзу додатку з брандмауером веб-додатку за допомогою порталу Azure та технологію застосування рішення

брандмауера веб-додатків на AzureFront Door.

Розроблено рекомендації фахівцям з кібербезпеки щодо застосування технології захисту веб-додатків організації при застосуванні хмарних платформ.

Таким чином, правильна реалізація технології захисту веб-додатків організації при застосуванні хмарних платформ має забезпечити ефективний захист корпоративних даних та кібербезпеку інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Data Breach Investigations Report. Verizon. 2022. [Електронний ресурс] – Режим доступу: https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf

2. Andrew Hoffman. Web Application Security Exploitation and Countermeasures for Modern Web Applications. O'Reilly Media. 2020. 331 p. [Електронний ресурс] – Режим доступу: https://www.nginx.com/resources/library/web-application-security.

3. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. National Institute of Standards and Technology. April 16, 2018. [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

4. OWASP Top 10 – 2017. The Ten Most Critical Web Application Security Risks. [Електронний ресурс] – Режим доступу: https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf.

6. 5 Best Practices for Application Security. A How-To Guide. Tenable. [Електронний ресурс] – Режим доступу: https://static.tenable.com/marketing/whitepapers/Whitepaper-5_Best_Practices_for_Application_Security.pdf.

7. FortiWeb 6.4.1. Administration Guide. Fortinet Document Library. . [Електронний ресурс] – Режим доступу: https://docs.fortinet.com/document/fortiweb/6.4.1/administration-guide/60895/introduction.

8. Захист веб-додатків: чому це важливо? ITBIZ. [Електронний ресурс] – Режим доступу: https://itbiz.ua/statti-ta-obzori/zaxist-veb-dodatkiv-chomu-ce-vazhlivo/#.

9. Web Application Firewall documentation [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/azure/web-application-firewall/.

10. What is Azure Web Application Firewall on Azure Application Gateway? [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview.

11. Azure Web Application Firewall on Azure Front Door [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview.

12. Web Application Firewall CRS rule groups and rules. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/application-gateway-crs-rulegroups-rules?tabs=owasp32.

13. Tutorial: Create an application gateway with a Web Application Firewall using the Azure portal. 11/10/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/application-gateway-web-application-firewall-portal?source=recommendations.

14. Best practices for Web Application Firewall (WAF) on Azure Front Door. 09/08/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-best-practices.

15. Макеєв Костянтин Андрійович. Технологія захисту веб-додатків організації в Azure. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний Університет Телекомунікацій. 27 жовтня 2022. Тези доповідей. С. 18-20. [Електронний ресурс] – Режим доступу: https://dut.edu.ua/uploads/p_2121_20358827.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)