АРХІТЕКТУРНІ ОСОБЛИВОСТІ СИСТЕМ ЗАХИСТУ ВЕБ-РЕСУРСІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Бараннік В.В., Слободянюк О.В., Бараннік Н.В.
Кафедра інформатики, Кам'янець-Подільський національний університет імені Івана Огієнко, м. Кам'янець-Подільський, Україна, E-mail: slobodyanyuk.olexandr@kpnu.edu.ua

Анотація – У статті розглянуто приклад типової схеми несанкціонованого доступу до веб-ресурсів із використанням вразливостей програмного забезпечення веб-серверів та веб-сервісів. Описані методи запобіганню порушенню інформаційної безпеки он-лайн ресурсів та веб-застосунків на основі використання як комплексних систем захисту так і спеціалізованих інструментів захисту. Розглянуто архітектурні особливості, функціональні можливості та вимоги до проектування нових архітектурних рішень із використанням мережевих екранів для веб-застосунків WAF.

Ключові слова – уразливість, загроза, OWASP, WAF

I. Вступ

Аналіз статистичних даних численних звітів щодо випадків порушення інформаційної безпеки інфокомунікаційних систем засвідчують той факт, що найбільш розповсюдженим типом несанкціонованих втручань пов'язані саме із сервісами та застосунками, які працюють у середовищі Всесвітньої павутини [[2] , [3] , [5] , [4]]. Водночас питання захисту веб-ресурсів залишається найбільш проблемним, а вироблення стратегій забезпечення відповідного рівня захищеності ще перебуває на стадії проектування та відлагодження.

Високий рівень конкуренції й тотальне переведення інформаційних сервісів підприємств на он-лайн платформи стало причиною появи веб-інфраструктури, що дуже залежить від зовнішніх факторів. Крім того надзвичайно швидкий темп розвитку й запровадження нових технологічних рішень призвело до того, що архітектура веб-застосунків стала досить складною та включає у собі симбіоз різноманітних технологічних складових, які до цього були не сумісними між собою. Все це призводить до того, що ризики інформаційної безпеки подібних інфокомунікаційних систем значно зростають як кількісно так і якісно.

На відміну від ризиків, що більш характерні для вже ставших класичними, desktop-платформ ризики в он-лайн середовищі пов'язані не із виведенням із ладу окремих або усіх компонентів системи, а скоріше із несанкціонованим доступом до персональних даних користувачів та комерційної інформації підприємства. На відміну від перших, матеріальні збитки від порушення інформаційної безпеки в даному випадку оцінити набагато важче, адже вони включають у себе дуже багато факторів, у тому числі й репутаційні втрати, які взагалі неможливо точно оцінити.

II. Схема реалізації атак на веб-ресурси

Для веб-застосунків та веб-сервісів як для інших типів програмного забезпечення не існує в принципі типового алгоритму несанкціонованого проникнення зловмисниками. Кожен випадок слід розглядати індивідуально. Кожного разу для проведення атаки використовуються різні набори інструментів та методів злому систем безпеки. Однак для усіх випадків є одна спільна особливість – усі вони використовують відомості про існуючі вразливості програмних систем. Це можуть бути як давно відомі вразливості, які по недогляду обслуговуючого персоналу ресурсу не були «закриті», так і вразливості «нульового дня». Тобто ті вразливості, про які вперше стає відомо лише після їх використання при проведенні атаки на даний конкретний тип програмного комплексу.

Розглянемо простий приклад втручання у роботу інформаційного ресурсу, що працює на основі системи керування вмістом Wordpress. На рисунку 1 показана схема реалізації типової атаки на веб-ресурс за допомогою найбільш розповсюдженого типу вразливості – нестійкості до SQL ін'єкцій.

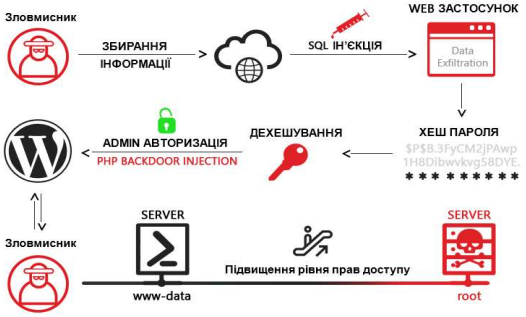

Рис. 1. Приклад схеми проведення атаки на систему керування вмістом Wordpress.

Так бачимо, що будь-яке несанкціоноване втручання обов'язково розпочинається з етапу збирання максимально можливої інформації про ресурс, особливості його побудови, наявності відкритих незахищених даних тощо. Після цього зловмисник проводить пошук вразливості та підбір відповідного метода атаки. Це робиться як на основі відомостей про тип встановленого програмного забезпечення на веб-сервері так і на основі простого перебору найбільш популярних способів несанкціонованого проникнення.

Наступним етапом є отримання внаслідок успішно проведеної атаки пароля користувача «нульового» рівня. Тобто адміністратора системи. Як правило усі паролі зберігаються у веб-системах у хешованому вигляді. Наприклад із використанням 128-бітного алгоритму кодування md5. Раніше даний алгоритм вважався досить надійним методом отримання хешу послідовності, однак спочатку у 2004 році в ньому було знайдено критичну вразливість, яка дозволяла проводити дехешування менш ніж за годину на кластерній системі, а вже за два роки час дехешування знизився до декількох хвилин на звичайному персональному комп'ютері. Незважаючи на це, даний алгоритм до цих пір є одним із найбільш популярних серед розробників веб-застосунків.

Останнім кроком зловмисника є проходження авторизації в системі з отриманням прав доступу адміністратора системи з можливістю доступу як до даних он-лайн контенту ресурсу так і масиву персональних даних його користувачів.

III. Використання інструментів захисту веб-ресурсів

Питанням захисту веб-ресурсів почали перейматися відносно нещодавно. І ще дуже часто інструменти захисту веб-застосунків та веб-сайтів плутають з інструментами захисту від мережевих атак, які вже стали класичними – брандмауерами або файєрволами. По суті класичний брандмауер представляє собою міжмережевий фільтр, який працює на мережевому та канальному рівнях моделі OSI. Дещо пізніше з'явилися шлюзи сеансового рівня або брандмауери другого покоління. Однак ні перші ні другі не здатні справитися із сучасними кібер-загрозами, оскільки понад 90% успішних атак проводяться саме на рівні програмного за-

безпечення, а не на рівні мережевої інфраструктури.

Наступним кроком розвитку інструментів захисту від кібер-загроз для веб-ресурсів стала поява комплексних систем виявлення та запобігання вторгнень (IDS/IPS). Дані системи були адаптовані для того щоб виявляти атаки не лише зовні але й всередині мережі за рахунок прослуховування SPAN-портів комутаторів та використання розбору полів TCP-пакетів та частин протоколу рівня представлення моделі OSI. Головним недоліком даних систем є те, що аналіз проводиться попакетно, без урахування даних сесій, cookies та елементів сховищ даних браузера. Однак, вони дозволили значно знизити ризики розповсюдження вірусів через веб-сайти, а також значно збалансували навантаження на проксі-сервери.

Наступними на ринку інструментів захисту веб-ресурсів від кібер-загроз стали системи виявлення вторгнень на основі UTM-пристроїв (unified threat management, система єдиного управління) та NGFW-брандмауери (next generation firewall). Системи на базі UTM практично не відрізняються від NGFW. Обидва класи програмних продуктів з'явилися з метою об'єднати функції різних продуктів в одному єдиному апаратному пристрої: антивірус, IDS/IPS, пакетний файєрвол, VPN-шлюз, маршрутизатор тощо.

Специфіка веб-застосунків передбачає, що за один сеанс роботи користувача з веб-сервером може здійснюватися велика кількість різних TCP-з'єднань, які відкриваються з різних адрес, але мають один (можливо динамічний) ідентифікатор сесії. Атаки на веб-ресурси, які маніпулюють програмним забезпеченням для досягнення шкідливих цілей, як правило, проходять одночасно з сесіями легітимних користувачів і, переважно, використовують стандартні HTTP-порти. Блокування всього трафіку на рівні цих портів не є доцільним, оскільки доступ до веб-ресурсів буде повністю закритий ззовні або зсередини. Саме така дилема мережевої безпеки є відмінною можливістю для пошуку хакерами вразливостей на рівні веб-застоунків. Виходом із даної ситуації є використання брандмауерів веб-застосунків WAF (Web Application Firewall).

Ринок WAF-брандмауерів є досить молодим, однак готові рішення вже пропонуються такими великими гравцями як Amazon (AWS WAF), Citrix (NetScaler Web App Security service), Cloudflare (Cloudflare WAF service), Oracle (Oracle WAF) та Microsoft (Microsoft Azure WAF). Однак згідно з дослідженнями компанії Gartner лідерами у даному сегменті є рішення від компаній Akamai та Imperva.

За типом розгортання WAF бувають мережевими, автономними та хмарними. Перші як правило виконані у вигляді апаратних пристроїв і суміщають у собі функції як класичних мережевих фільтрів так і файєрволів веб-застосунків. Автономні зазвичай представляють собою прості програмні комплекси, які встановлюються у вигляді настільних застосунків відповідної операційної системи комп'ютера-хоста. Хмарні WAF виконані як правило у вигляді мережевого сервісу і надаються користувачам у вигляді послуг типу SaaS (software as a service).

Основними функціями WAF є:

1) Фільтрація мережевих протоколів.

2) Фільтрація протоколів HTTP.

3) Моніторинг стану з'єднання.

4) Підтримка високої доступності.

5) Контроль управління сеансами: оцінки потоків трафіку, використання тайм-аутів, моніторинг перехоплень сеансів.

6) Моніторинг/захист файлів cookie.

7) Контроль за значеннями прихованих полів.

8) Моніторинг наявності перебору значень (застосування методу Brute-force).

Типова структура файєрволу веб-застосунків виглядає наступним чином (рис. 2).

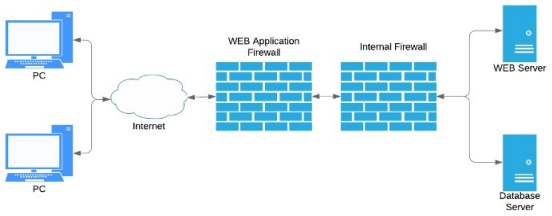

Рис. 2. Приклад типової WAF архітектури.

При проектуванні архітектури нового WAF-рішення необхідно дотримуватись виконання наступних вимог:

1) Підтримка виконання вимог стандартів PCI DSS та DA DSS, які визначають умови безпечної обробки даних платіжних карток.

2) Оперативна реакція (визначається активною політикою та набором правил) на проведення атак із використанням популярних типів вразливостей (TOP 10 OWASP/WASC) [5] .

3) Перевірка вхідного HTTP/HTTPS трафіку і запитів до веб-застосунків та прийняття превентивних заходів на основі активних політик й правил.

4) Підтримка і дотримання коректного функціонування позитивної та негативної моделі безпеки.

5) Аналіз веб-контенту (HTML, DHTML, CSS).

6) Запобігання витоку даних.

7) Аналіз повідомлень веб-сервісів, особливо публічних. Як правило, включає в себе перевірку Simple Object Access Protocol (SOAP) та eXtensible Markup Language (XML), а також Remote Procedure Call (RPC) орієнтованих моделей взаємодії з веб-сервісами, засновані на базі HTTP.

8) Захист від загроз, спрямованих безпосередньо на WAF.

9) Термінація SSL та TLS (розшифровка й перевірка трафіку перед відправкою веб-застосунку).

IV. Висновки

За інформацією компанії Gartner у 2020 році розгортання нових апаратних брандмауерів, що будуть містити підтримку режиму WAF буде складати близько 20%. Зараз цей показник складає 35%. Однак до 2023 року лише 30% публічних веб-застосунків буде захищено службами захисту веб-застосунків та API (WAAP), які поєднують захист DDoS, захист від ботів, захист API та WAF. Зараз цей показник складає лише 10% [4] . Ці прогнози можуть свідчити лише про те, що задача захисту веб-ресурсів не є аж такою тривіальною як може здатися спочатку. Тому безпековий аудит та виявлення й ліквідація вразливостей у існуючих програмних системах залишатиметься актуальним інструментом захистом ще досить тривалий час.

V. Список літератури

[1] Безпека додатків [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://bit.ly/2LL77JC.

[2] Годовой отчет Cisco по информационной безопасности [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://bit.ly/2XTjRTQ.

[3] Уязвимости веб приложений [Електронний ресурс] // Positive Technologies. – 2018. – Режим доступу до ресурсу: http://bit.ly/2V92q4P.

[4] D'Hoinne J. Magic Quadrant for Web Application Firewalls. [Електронний ресурс] / Jeremy D'Hoinne, Adam Hils, Ayal Tirosh, Claudio Neiva. – 2018. – Режим доступу до ресурсу: https://gtnr.it/2IVLx72

[5] OWASP Top 10 – 2017. The Ten Most Critical Web Application Security Risks. [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://bit.ly/2IS60tz.

[6] Yaworski P. Web Hacking 101. How to Make Money Hacking Ethically [Електронний ресурс] / Peter Yaworski // Lean Publishing. – 2017. – Режим доступу до ресурсу: http://leanpub.com/web-hacking-101.