МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: СИНЕРГІЯ НАУКОВИХ, ОСВІТНІХ ТА ТЕХНОЛОГІЧНИХ РІШЕНЬ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

19 травня 2023 року

У двох томах

Том 1

Видавництво
«Юридика»
2023

УДК 005.332.2(4):316.42(477)"364""20"(062.552)
Є24

Рекомендовано до друку Вченою радою
Національного університету «Одеська юридична академія»
(протокол № 3 від 16.06.2023 р.)

За загальною редакцією **С. В. Ківалова.**

Відповідальний за випуск **М. Р. Аракелян.**
Матеріали видано в авторській редакції.

Є24 **Європейські** орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавництво «Юридика», 2023. – Т. 1. – 790 с.

ISBN 978-617-8263-39-3

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень». У першому томі збірника містяться наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині в умовах повномасштабного військового вторгнення у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології. Висвітлено питання загроз національній безпеці в їхньому конституційному вимірі, у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов'язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики.

Збірник розраховано на наукових та науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)"364""20"(062.552)

ISBN 978-617-8263-37-9 (у 2 т.)
ISBN 978-617-8263-39-3 (т. 1)

СЕКЦІЯ 13
КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

КУХАРЕНКО СЕРГІЙ ВІКТОРОВИЧ

Національний університет «Одеська юридична академія», доцент кафедри кібербезпеки, кандидат технічних наук

СТАДНІК ДЕНИС АНДРІЙОВИЧ

Національний університет «Одеська юридична академія», здобувач вищої освіти

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВЕБСЕРВЕРІВ

Вебсервери є одним з найбільш цільових місць в організації. Це об'єкти, які постійно піддаються безлічі самих різних небезпек. Найсерйознішу загрозу становлять для них хакери, які можуть отримати доступ до конфіденційної інформації, розміщеної на сервері, зламати сайти і змінити їх вміст, а також вивести з ладу сервер за допомогою розподіленої атаки (DDoS-атака), тому веб-безпека залишається однією з найважливіших проблем.

Вебсервери відіграють ключову роль у роботі вебсайтів і додатків, забезпечуючи їхню доступність і функціональність.

З точки зору апаратної частини вебсервер – це комп'ютер, призначений для зберігання даних сайтів, а також він призначений для доставки файлів до веб-браузера користувачів. Веб-сервер може бути доступний через певне доменне ім'я.

З точки зору програмного забезпечення веб-сервер не може обійтися без компонентів, призначених для контролю доступу користувачів до даних, які знаходяться на сервері. В якості таких компонентів виступають HTTP-сервер (як частина програмного забезпечення) та HTTP-протоколу за допомогою якого спілкуються вебсервер та браузер.

У вебсерверів можуть бути різні вразливості, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до системи або виконання шкідливих дій. Деякі поширені вразливості вебсерверів включають [1]:

1. Вразливості вебдодатків (відсутність автентифікації або авторизації, SQL-ін'єкції тощо). Ці вразливості можуть дозволити зловмисникам виконати атаки на додаток або отримати доступ до конфіденційної інформації.

2. Уразливості операційної системи. Це може бути неправильна конфігурація операційної системи, уразливості ядра, недостатнє оновлення системи або слабкі облікові записи.

3. Уразливості вебсерверного програмного забезпечення. Програмне забезпечення може містити уразливості, такі як помилки програмування, уразливості протоколів або проблеми з конфігурацією.

4. Уразливості в мережевій інфраструктурі (атаки перехоплення даних або відмови в обслуговуванні, атаки на рівні мережі).

Оцінюванню, аналізу та заходам щодо усунення вразливостей присвячено достатньо велика кількість досліджень та рекомендацій.

Наприклад для усунення вразливостей вебсервера можна застосовувати такі заходи безпеки [2]:

1. Регулярне оновлення операційної системи.
2. Застосування патчів.
3. Жорстка конфігурація безпеки.
4. Використання файрволу та мережевих налаштувань.
5. Використання шифрування для захисту передачі даних між клієнтами та сервером та сертифікатів для забезпечення довіри та захисту від атак типу «перехоплення і розшифрування».
6. Автентифікація та авторизація.
7. Моніторинг і реагування на інциденти.
8. Тестування на проникнення.

Згідно провідних міжнародних практик оцінка заходів щодо усунення вразливостей – це процес визначення, ідентифікації, класифікації та приоритизації вразливостей мережевій інфраструктурі, який проводиться в декілька етапів [3]:

1. Ідентифікація вразливостей: Необхідно провести аналіз вразливостей веб-сервера за допомогою спеціалізованих інструментів, таких як сканери вразливостей. Це дає змогу виявити вразливості, які можуть стати об'єктом атаки зловмисників.

2. Оцінювання ризиків: Оцінювання ризиків дає змогу визначити ступінь загрози та потенційний збиток, який може бути завдано в разі експлуатації вразливості. Це допомагає визначити пріоритети в усуненні вразливостей і вибрати найефективніші заходи щодо їх усунення.

3. Вибір заходів для усунення вразливостей: Визначення заходів для усунення вразливостей має ґрунтуватися на результаті оцінювання ризиків і засобах, доступних для реалізації заходів. Необхідно вибрати заходи, які максимально ефективно усунуть уразливості та знизять ризик найімовірніших атак.

4. Реалізація заходів щодо усунення вразливостей: Реалізація заходів щодо усунення вразливостей повинна здійснюватися відповідно до обраних заходів і рекомендацій безпеки. Важливо переконатися в правильному налаштуванні та роботі всіх засобів, що використовуються для усунення вразливостей.

5. Перевірка ефективності заходів: Перевірка ефективності заходів щодо усунення вразливостей дає змогу визначити, наскільки добре вони працюють у реальних умовах. Перевірка може включати проведення тестів на проникнення, моніторинг системи та аналіз логів. Це дає змогу переконатися в тому, що заходи з усунення вразливостей працюють належним чином і не створюють нових проблем безпеки.

Загалом, оцінювання заходів з усунення вразливостей веб-сервера є безперервним процесом, який вимагає постійного моніторингу та оновлення заходів безпеки відповідно до появи нових вразливостей і атак.

Оцінювання заходів з усунення безпеки може здійснюватися за різними критеріями. Ось деякі з них:

1. Ефективність: Оцінка заходів з усунення безпеки має визначити, наскільки успішно вони запобігають або знижують ризик

уразливості. Ефективність може бути оцінена на основі історичних даних, результатів тестування на проникнення або статистичної інформації.

2. Ресурсоємність: Оцінка заходів з усунення безпеки має враховувати витрати на їхню реалізацію та підтримку. Це може включати фінансові витрати, необхідність навчання персоналу, використання обчислювальних ресурсів і часові витрати. Оцінка ресурсоємності допомагає визначити, наскільки ефективно використовуються ресурси під час реалізації заходів безпеки.

3. Відповідність стандартам і регулятивним вимогам: Оцінка заходів з усунення безпеки може визначати, наскільки вони відповідають встановленим стандартам безпеки та вимогам регуляторів. Це може включати дотримання нормативних документів, таких як стандарти PCI DSS, HIPAA, GDPR та інші.

4. Практичність: Оцінка заходів щодо усунення безпеки має враховувати їхню практичну застосовність і зручність використання. Це охоплює зручність управління та налаштування, інтеграцію з іншими системами, мінімізацію негативного впливу на продуктивність або користувацький досвід.

5. Адаптивність: Оцінка заходів щодо усунення безпеки повинна враховувати їхню здатність адаптуватися до мінливого загрозливого середовища. Заходи безпеки мають бути гнучкими і здатними адаптуватися до нових видів вразливостей і атак.

6. Постійне поліпшення: Оцінка заходів щодо усунення безпеки може також включати аналіз можливостей постійного поліпшення і вдосконалення. Це може включати зворотний зв'язок від користувачів та експертів, проведення аудитів безпеки та постійне оновлення заходів безпеки відповідно до нових загроз і технологій.

Аналізуючи вище викладене можливо дійти висновку, що серед основних заходів, щодо забезпечення безпеки вебсерверів можливо виділити наступні: видалення непотрібних сервісів, управління дозволами та привілеями, видалення непотрібних модулів та розширення програм, моніторинг та аудит вебсервера.

Отже, забезпечення безпеки вебсервера вимагає комплексного підходу і постійного моніторингу. Застосування відповідних заходів безпеки та регулярне оновлення системи допоможуть знизити ризик вразливостей і підвищити безпеку вебсерверів. Оцінка заходів щодо усунення вразливостей допомагає визначити і поліпшити ефективність системи захисту і підтримувати її на актуальному рівні для захисту від загроз, що постійно розвиваються.

Список використаних джерел:

1. Top 10 Web Application Security Risks [Електронний ресурс]. – Режим доступу до ресурсу: https://owasp.org/www-project-top-ten/
2. Ultimate Guide to Server Security Vulnerabilities [Електронний ресурс]. – Режим доступу до ресурсу: https://www.eurovps.com/blog/server-security-vulnerabilities/

3. How To Perform A Vulnerability Assessment [Електронний ресурс]. – Режим доступу до ресурсу: https://www.intruder.io/guides/vulnerability-assessment-made-simple-a- step-by-step-guide

Ключові слова: Веб-сервер, безпека, заходи, вразливості, оцінка.
Key words: Web server, security, measures, vulnerabilities, assessment.

ЧЕПУРНА ОЛЕНА ЄВГЕНІВНА

Національний університет «Одеська юридична академія», доцент кафедри кібербезпеки, кандидат фізико-математичних наук, доцент

КУЛЕШОВА ЄВГЕНІЯ РОМАНІВНА

Національний університет «Одеська юридична академія», аспірант кафедри кібербезпеки

СУЧАСНІ МАТЕМАТИЧНІ МЕТОДИ ОПТИМІЗАЦІЇ ЗАХОДІВ КІБЕРБЕЗПЕКИ

Сучасний світ можна назвати світом інформаційно-комунікаційних технологій. Кожну долю секунди народжується інформаційна одиниця, здійснюється інформаційний обмін. Глобалізація сучасного світу, розвиток новітніх технологій передачі інформації породжує нові загрози її викрадення, маніпуляцій та порушень. Впровадження ефективних заходів кібербезпеки є серйозним викликом для фахівців, зважаючи на те, що кількість і технічний рівень приладів зростає, а рівень кіберзлочинів і кіберзлочинців росте з їх розвитком [1].

Згідно з «Глобальним дослідженням інформаційної безпеки», що його провела компанія EY, 55 % організацій не розглядають захист інформації як частину загальної бізнес-стратегії. Водночас 87 % організацій мають обмежений бюджет на забезпечення необхідного рівня кібербезпеки. Однак бюджети на кібербезпеку зростають – великі компанії витрачають на кібербезпеку більше вже в цьому (63 %) і наступних роках (67 %), менші компанії – 50 % і 66 % відповідно [2]. З огляду на нагальні потреби в розвитку ефективних систем захисту інформації як особистої, так і організацій різних форм власності, постає задача застосування осучаснених методів і систем кіберзахисту, та оптимізація вже існуючих.

Підвищення ефективності захисту інформації можливе за наступними напрямками :

– заміна обладнання на більш сучасне;
– оптимізація програмного забезпечення вже існуючого обладнання;
– застосування хмарних технології в обробці і зберіганні інформації;
– застосування математичних методів в різних сферах організації кіберзахисту.