решении задач оперативного суточного планирования поставок электроэнергии на оптовом рынке / К.Б. Остапченко, О.И. Лисовиченко // Адаптивні системи автоматичного управління. – 2014. – Вып. 1(24). – С.76-86.
13. *Щелкалин В.Н.* Гибридные модели и методы прогнозирования временных рядов на основе методов «гусеница»-SSA и Бокса-Дженкинса // Восточно-Европейский журнал передовых технологий. – 2014. – № 5/4 (71). – С.43-62.
14. *Пенко В.Г.* Прогнозирование временных рядов с помощью гибридных методов искусственного интеллекта / В.Г. Пенко // Інформатика та математичні методи в моделюванні. – 2012. – Том 2, № 2. – С.165-172.
15. *Бэнн Д.В.* Сравнительные модели прогнозирования электрической нагрузки / Д.В. Бэнн, Е.Д. Фармер. – М.: Энергоатомиздат, 1987. – 200 с.
16. *Браммер К.* Фильтр Калмана-Бьюси / К. Браммер, Г. Зиффлинг. – М.: Наука, 1982. – 200 с.
17. *Васильев В.Г.* Математическая модель краткосрочного прогнозирования электропотребления объединенной энергосистемы РУз с помощью АРМ «Оракул» / В.Г. Васильев, С.П. Васильева, А.А. Прейгель // Проблемы информатики и энергетики: Узбекский журнал. – 2000. – № 4. – С.36-41.
18. *Руссков О.В.* Планирование неравномерного потребления субъекта оптового рынка электроэнергии на основе прогноза соотношения часовых цен / О.В. Руссков, С.Э. Сараджишвили // Наука и образование. МГТУ им. Н.Э. Баумана, Электронный журнал. – 2015. – № 2. – С.115-135.
19. *Ямпольський Л.С.* Нейротехнології та нейрокомп`ютерні системи / Л.С. Ямпольський, О.І. Лісовиченко, В.В. Олійник. – К.: Дорадо-Друк, 2016. – 576 с.

http://doi.org/10.5281/zenodo.3860762

Поступила 16.09.2019р.

УДК 004.056.5

О.С. Потенко, Київ

АНАЛІЗ СИСТЕМ ЗАХИСТУ ВЕБ-ДОДАТКІВ ВІД ХАКЕРСЬКИХ АТАК

Abstract. This article analyzes and compares modern security systems for web applications and web resources.

Сучасну, навіть дуже маленьку компанію, важко уявити без власного веб-сайту, а тому захист веб ресурсу від хакерських атак являється актуальною проблемою сьогодення. Архітектури сучасних веб-сайтів та web-додатків досить складні і вимагають інтеграції багатьох гетерогенних технологій, створюючи потенціал для численних вразливостей. Дуже швидкі цикли розробки і постійні оновлення web-додатків ще більше погіршують

ситуацію. В таких умовах ризики компаній занадто великі, щоб ігнорувати дану проблему, так як уразливості в web-додатках піддають критично важливі бізнес-операції і конфіденційні дані небезпеки. Значні фінансові втрати можуть виникнути в результаті непередбачених затримок в бізнес-процесах, крадіжки інтелектуальної власності, і втрати довіри клієнтів, а також репутації бренду. У багатьох випадках, безпека web-додатків також є юридичною вимогою до компанії, яка обробляє персональні дані користувачів.

Сучасні тенденції розвитку web-сервісів вказують на відсутність єдиних стандартів безпечного програмування web-додатків, що призводить до помилок в розробці ПЗ і появи серйозних вразливостей в web-сервісах. Становище ускладнюється тим, що вразливий web-додаток може бути легко скомпрометовано без використання спеціалізованих засобів, тільки за допомогою браузера.

У цих умовах постає закономірне питання: що робити для захисту веб-додатків? Заходи для захисту можна впроваджувати на двох етапах життя вуб-додатка – на етапі розробки і етапі експлуатації. На етапі розробки – це різні інструменти тестування безпеки: статичний, динамічний, інтерактивний аналіз. Якщо говорити про безпеку вже готового додатку, то тут пропонується використовувати додаткові засоби захисту – системи запобігання вторгнень (IPS), міжмережеві екрани нового покоління (Next Generation Firewall, скорочено NGFW), а також засоби фільтрації трафіку прикладного рівня, спеціально орієнтовані на веб-додатки (Web Application Firewall, Скорочено – WAF) [1].

Найпростіше, що можна використовувати для захисту, це звичайний мережевий екран (firewall). Firewall (брандмауер, екран) – мережевий фільтр, який ставиться між довіреною внутрішньою мережею і зовнішнім Інтернетом. Цей фільтр винен блокувати підозрілі мережеві пакети на основі критеріїв низьких рівнів моделі OSI: на мережевому і канальному рівнях. Іншими словами, фільтр враховує тільки IP адреси джерела і призначення, точку фрагментації, номери портів. Міжмережеві екрани другого покоління підвищили якість і продуктивність фільтрації за рахунок контролю приналежності пакетів до активних TCP-сесій [2].

Наступним поколінням захисних екранів стали системи виявлення та запобігання вторгнень (IDS / IPS). Вони здатні вивчати в TCP-пакетах поля даних і здійснювати інспекцію на рівні додатку за певними сигнатурам. Системи IDS пристосовані до того, щоб виявляти атаки не тільки зовні, але і всередині мережі за рахунок прослуховування SPAN-порту комутатора [2].

Для вдосконалення захисних механізмів в IDS / IPS стали застосовуватися декодери (розбір полів TCP-пакета) і препроцесори (розбір частин протоколу рівня додатки, наприклад, HTTP). Застосування препроцесорів в IPS Snort дозволило істотно поліпшити функціональність периметрового захисту в порівнянні з пакетним фільтром, навіть якщо останній перевіряє пакети на рівні додатків (iptables з модулем layer7).

Однак при цьому зберігся основний недолік пакетного фільтра: перевірка здійснюється попакетно, без урахування сесій, cookies та всієї іншої логіки роботи програми [3, 4].

Паралельно для боротьби з поширенням вірусів з'являються проксі-сервери, а для вирішення завдань балансування навантаження – зворотні проксі-сервери. Вони відрізняються технічно, але головне, що і ті, і інші повноцінно працюють на рівні програми: відкривається два TCP з'єднання від проксі до клієнта і від проксі до сервера, аналіз трафіку ведеться виключно на рівні додатку.

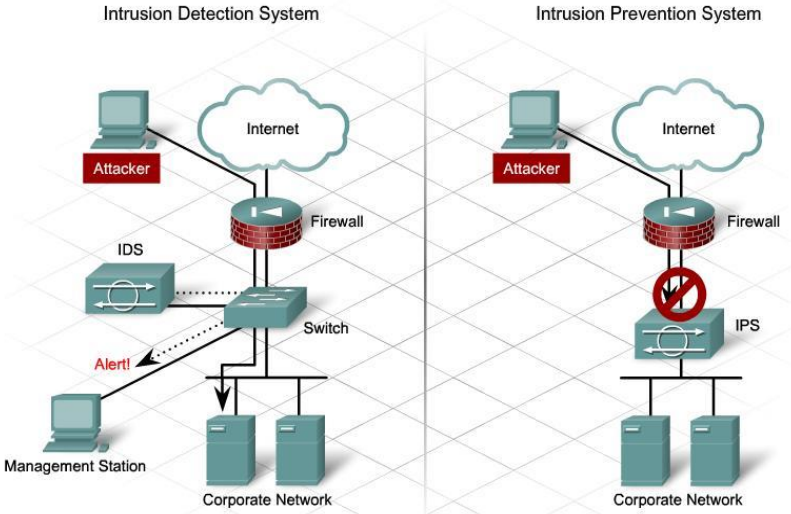

Рис. 1. Системи виявлення та запобігання вторгнень (IDS / IPS)

Наступним етапом еволюції систем виявлення вторгнень стала поява пристроїв класу UTM (Unified Threat Management, система єдиного управління погрозами) і NGFW (Next Generation Firewall, екрани нового покоління).

Системи UTM відрізняються від NGFW лише маркетингом, при цьому їх функціонал практично збігається. Обидва класи програмних продуктів з'явилися спробою об'єднати функції різних продуктів (антивірус, IDS / IPS, пакетний фільтр, VPN-шлюз, маршрутизатор, балансувальник і ін.) В одному пристрої. У той же час, виявлення атак в пристроях UTM / NGFW нерідко здійснюється на старій технологічній базі, за допомогою згаданих вище препроцесорів.

Згідно з визначенням аналітиків Gartner, міжмережеві екрани нового покоління повинні гарантовано забезпечувати наступне [5, 6]:

- захист від безперервних атак з боку інфікованих систем;
- стандартні для першого покоління фаєрволів можливості;

- сигнатури визначення типів додатків на основі движка IPS;
- повностекове інспектування трафіку, включаючи додатки, а також детальний і настроюється контроль на рівні додатків;
- можливість включати інформацію за межами брандмауера (наприклад, інтеграція з мережевими каталогами, «білими» і «чорними» списками додатків);
- постійно оновлювану базу описів додатків і загроз;
- інспекцію трафіку, що шифрується за допомогою SSL.

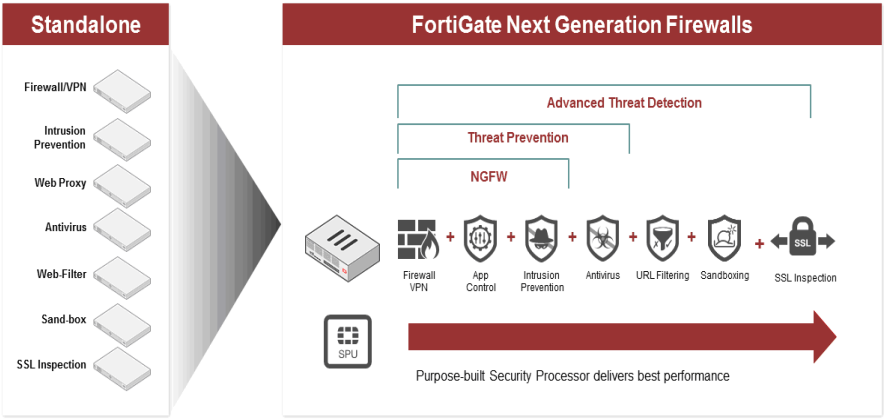

Рис. 2. Next generation firewall

Web Application Firewall – засоби фільтрації трафіку прикладного рівня, спеціально орієнтовані на веб-додатки. Застосування Web Application Firewall традиційно вважається найбільш ефективним підходом до захисту веб-ресурсів. WAF може бути реалізований як хмарний сервіс, додаток на веб-сервері або спеціалізоване залізний або віртуальний пристрій.

WAF здатний виявляти і блокувати такі сучасні атак на веб-додатки, в тому числі і з використанням вразливостей нульового дня [5]:

- SQL Injection – sql ін'єкції;
- Remote Code Execution (RCE) – віддалене виконання коду;
- Cross Site Scripting (XSS) – міжсайтовий скриптинг;
- Cross Site Request Forgery (CSRF) – міжстайтова підробка запитів;
- Remote File Inclusion (RFI) – віддалений інклуд;
- Local File Inclusion (LFI) – локальний інклуд;
- Auth Bypass – обхід авторизації;
- Insecure Direct Object Reference – небезпечні прямі посилання на об'єкти;

- Bruteforce – підбір паролів.

Загальні вимоги до сучасного Web Application Firewall [5]:

- системні компоненти WAF повинні відповідати вимогам PCI DSS;
- можливість реагування на загрози, описані в OWASP Top Ten;
- інспектування запитів і відповідей відповідно до політики безпеки, журнал роботи подій; запобігання витоку даних – інспекція відповідей сервера на наявність критичних даних;
- застосування як позитивної, так і негативної моделі безпеки; інспектування всього вмісту веб-сторінок, включаючи HTML, DHTML і CSS, а також нижчих протоколів доставки вмісту (HTTP / HTTPS);
- інспектування повідомлень веб-сервісу, якщо веб-сервіс підключений до інтернету (SOAP, XML);
- інспектування будь-якого протоколу або конструкції даних, що використовуються для передачі даних веб-додатки незалежно від того, чи є він пропрієтарним або стандартизованим (як для вхідних, так і вихідних потоків даних);
- захист від загроз, спрямованих безпосередньо на WAF;
- підтримка SSL \ TLS-термінації з'єднання;
- запобігання або виявлення підробки ідентифікатора сесії;
- автоматичне скачування оновлень сигнатур атак і застосування їх;
- можливість установки режиму fail-open і fail-close;
- підтримка пристроєм клієнтських SSL-сертифікатів;
- підтримка апаратного зберігання ключів (FIPS).

Web Application Firewall підтримує два основні режими роботи:

- Gateway
- Monitor

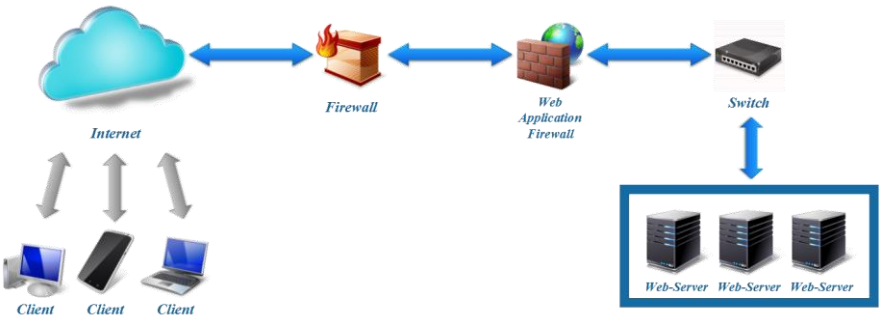

Рис. 3. Режим роботи Gataway

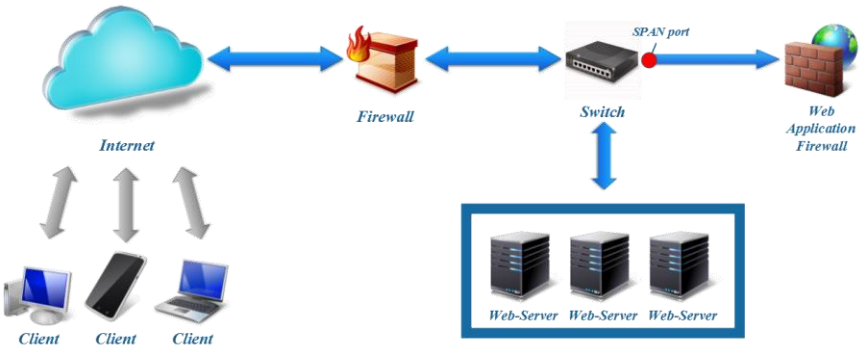

Рис. 4. Режим роботи Monitor

Таблиця 1

Основні відмінності WAF, IDS/IPS та NGFW

	WAF	IDS/IPS	NGFW
Multiprotocol Security	-	+	+
IP Reputation	-/+	-/+	-/+
Web Attack Signatures	+	-/+	-
Web Vulnerabilities Signatures	+	-/+	-/+
Automatic Policy Learning	+	-	-
URL, Parameter Cookie, and Form Protection	+	-	-
Laverage Vulnerability Scan Results	+	-/+	-

Висновки

Захист вразливих web-додатків може здійснюватися або шляхом усунення вразливостей в web-додатку або за допомогою спеціалізованих засобів захисту web-додатків – Web Application Firewall (WAF). Сьогодні розміщення традиційних брендмауерів, Next Generation Firewalls (NGFW) або Intrusion Prevention Systems (IPS) по периметру мережі або в якості шлюзів для довірених сегментів мережі, є недостатнім фактором для забезпечення повноцінного захисту мережевої інфраструктури. Атаки на web-ресурси, які використовують програмне забезпечення для досягнення шкідливих цілей, як правило, проходять одночасно з сесіями легітимних користувачів і майже завжди використовують стандартні HTTP (80) і HTTPS (443) порти. Блокування всього трафіку на рівні порту не є варіантом виходу з цього становища, так як доступ до web-додатків буде повністю закритий ззовні або зсередини. Саме така проблема мережевої безпеки призводить для пошуку хакерами вразливостей на рівні web-додатків.

1. Intro to Next Generation Firewalls [Електронний ресурс] – https://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html.
2. Чим захищають сайти, або Навіщо потрібен WAF? [Електронний ресурс] – https://habr.com/ru/company/pt/blog/269165.
3. Ефективність Web Application Firewall [Електронний ресурс] – https://xakep.ru/2011/11/21/57840.
4. Применение IDS / IPS [Електронний ресурс] – https://xakep.ru/2012/10/29/ids-ips/
5. Web Application Firewall – захист сайту від хакерських атак [Електронний ресурс] – https://habr.com/ru/post/60590.
6. Сетевая безопасность, Часть 2. Next-Generation Firewall [Електронний ресурс] – https://habr.com/ru/company/hpe/blog/262123.

http://doi.org/10.5281/zenodo.3860764

Поступила 9.09.2019р.

УДК 621.3;543.7.4;543.8

О.О. Огір, Київ
О.Р. Ярема, Львів

ДОСЛІДЖЕННЯ МАТЕМАТИЧНИХ МОДЕЛЕЙ УЛЬТРАЗВУКОВИХ СИГНАЛІВ ДЛЯ СИСТЕМ ДЕФЕКТОСКОПІЇ

Abstract. The investigation of mathematical models of ultrasonic signals used in acoustic imaging systems forming the internal structure of controlled materials and media objects energy industry. Such models make it possible to take into account all effects in wave processes: radiation and reflection of waves, phenomena of interference and diffraction of waves, wave type transformations during reflection and the appearance of damped waves at the interfaces of opaque media.

Вступ

Відомо, що хвильове рівняння в твердому тілі з граничними умовами (поверхні дефектів, границі об'єктів) дає множину рішень для хвиль, що розповсюджуються в об'єкті контролю (ОК), по границях, відбитих повторно хвиль. Крім цього, з'являться рішення для хвиль з наростаючою та спадаючою амплітудою. Рішення задачі в аналітичному вигляді передбачає вибір фізичних хвильових процесів, деякий "штучний відбір" [1]. Часто при завданні множинних граничних умов, хвильова задача виявляється настільки складною, що аналітичне рішення не може бути одержане. Накопичений досвід в точному вирішенні хвильових акустичних задач практично неможливо використати для наших цілей, оскільки в самому загальному випадку не доведено існування і єдність рішення оберненої задачі.

