МРНТИ 81.93.29

Л. Атымтаева[1], О. Баймуратов[2], Д.А. Хашимова[3]
[1,2,3,]Университет имени С. Демиреля, Каскелен, Казахстан

ОБЗОР УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРЕДПРИЯТИИ

Аннотация. В данной статье представлены результаты анализа по выявлению групп угроз, специфичных для инфраструктуры и систем предприятии которое является одним из основных этапов в прогнозировании. Рассмотрены состояние информационной безопасности на предприятиях, проанализированы квалификации угроз безопасности и методов классификации, основанные на методах атак и на воздействии угроз. Оценены угрозы по безопасному использованию Интернета и взламыванию сайтов, краж данных, атакам фишинга и социальной инженерии; выявление угроз безопасности облачных вычислений, которые встречаются в интернет сетях предприятии. Изучены преимущества и недостатки Файрвол веб-приложений (WAF), который применяются для защиты атак, такие как *DDoS-атаки, SQL-инъекции, межсайтовый скриптинг (XSS), и др.* Представлены работы для обеспечения защиты с применением искусственного интеллекта и машинного обучения.

Ключевые слова: информационная безопасность, файрвол веб-приложений (WAF), классификация угроз информационной безопасности.

***

Abstract. This article presents the results of an analysis to identify groups of threats specific to the infrastructure and systems of an enterprise, which is one of the main stages in forecasting. The state of information security at enterprises is considered, the qualifications of security threats and classification methods based on attack methods and the impact of threats are analyzed. Threats for the safe use of the Internet and hacking sites, data theft, phishing attacks and social engineering are assessed; Identification of cloud computing security threats that are encountered in the enterprise's Internet networks. The advantages and disadvantages of Web Application Firewall (WAF), which are used to protect attacks, such as DDoS attacks, SQL injections, cross-site scripting (XSS), and others, are studied. Works for providing protection using artificial intelligence and machine learning are presented.

Keywords: information security, Web Application Firewall (WAF), classification of information security threats.

***

Аңдатпа. Бұл мақалада болжаудың негізгі кезеңдерінің бірі болып табылатын кәсіпорынның инфрақұрылымы мен жүйелеріне тән қауіптер тобын анықтау үшін жасалған талдау нәтижелері келтірілген. Кәсіпорындардағы ақпараттық қауіпсіздіктің жай-күйі қарастырылады, қауіп-қатерлердің біліктілігі, шабуыл әдістеріне және қауіп-қатерлерге негізделген классификациялау әдістері талданады. Интернетті қауіпсіз пайдалану және сайттарды бұзу, деректерді ұрлау, фишингтік шабуылдар және әлеуметтік инженерия үшін қауіптер бағаланады. Кәсіпорынның Интернет желілерінде кездесетін бұлтты есептеу қауіпсіздігіне қауіптерді анықтау. DDoS шабуылдары, SQL инъекциялар, сайттар аралық сценарийлер (XSS) және басқалары сияқты шабуылдардан қорғау үшін қолданылатын Web Application Firewall (WAF) артықшылықтары мен кемшіліктері зерттелген. Жасанды интеллект пен машиналық оқытуды қолдана отырып қорғауды қамтамасыз ететін жұмыстар ұсынылған.

Түйін сөздер: ақпараттық қауіпсіздік, Web Application Firewall (WAF), ақпараттық қауіпсіздік қауіптерін жіктеу.

Введение

В современных условиях процесс успешного развития предприятий зависит от прогнозирования потенциальных угроз информационной безопасности. Все угрозы нуждаются в контроле и ликвидации со стороны предприятий, так как они способны нанести убытки и спровоцировать новые угрозы. Однако отечественные организации вкладывают средства только в реализацию мероприятий по устранению наступившей угрозы, а не действуют изначально на ее предупреждение.

На сегодняшний момент существуют две основные проблемы, препятствующие процессу организации деятельности по предупреждению угроз безопасности:

– несовершенство моделей оценки потенциальных угроз безопасности предприятия;

– слабая проработанность вопроса превентивных мер защиты предприятия [1].

Классификация угроз безопасности

В исследованиях [2] рассмотрен структурированный подход для выявления групп угроз, специфичных для предприятия, что является важным шагом для специалистов по планированию безопасности, которые участвуют в разработке экономически эффективных стратегий для устранения рисков информационной безопасности своих организаций. Успех программы управления рисками информационной безопасности на

предприятиях основан на точной идентификации угроз для информационных систем организации.

В [2] представлены набор из пяти категорий угроз высокого уровня:

· Персонал и администрация
· Сети
· Аппаратное обеспечение
· Программное обеспечение
· Экологическая и физическая безопасность

В рамках этих категорий было выявлено 21 угроз, которые использовались для взвешивания состояния безопасности информационных систем, как показано в Таблице 1 [2]. С этого момента примерно 450 рекомендуемых мер безопасности были отнесены к этим категориям угроз.

Таблица 1. Список устаревших угроз

Персональные/Административные угрозы	Террористические/Гражданские беспорядки Деятельность для личной выгоды Злоумышленные действия отдельного сотрудника Подделка или разрушение аппаратных средств и/или связанных с ними компонентов Кража оборудования и/или связанных с ними компонентов Кража ресурсов
Сетевая угроза	Необходимая линия связи/отказ оборудования Подделка Прослушивание
Аппаратное обеспечение	Существенный аппаратный сбой
Программное обеспечение	Ошибка программиста/оператора Ошибка программного обеспечения Вторжение вредоносных программ Несанкционированный доступ или привилегии исполнения
Экологическая/Физическая угрозы безопасности	Кража или фальсификация оборудования Потеря стабильной электроэнергии

	Оборудование или пожарное оборудование Стихийное бедствие Экстремальные температуры/влажность

Однако работа с пятью категориями угроз вызвала обеспокоенность. Хотя был предпринят квази-аналитический подход к определению восприятия состояния безопасности системы, анализ становился все более субъективным. При рассмотрении списка угроз было замечено несколько аномалий, которые могли поставить под сомнение достоверность общих результатов.

Таким образом, должен быть разработан полный и сбалансированный список угроз, от которых могут быть защищены информационные системы. В этой статье описывается процесс в форме шага, который используется для составления списка угроз предприятия.

На основе приведенных пяти категорий угроз субъективно определено положение безопасности и дополнительные меры безопасности для снижения риска [2].

Одним из задач в организации/предприятии является детальное и полное представление об угрозах для их информационных активов и как получить необходимые средства для борьбы с ними, что возможно скрыто продолжает создавать утечку информации. Чтобы улучшить понимание угроз безопасности, в работе [3] предлагается модель классификации угроз безопасности, которая позволяет нам изучать влияние класса угроз вместо воздействия угрозы, поскольку угроза меняется с течением времени и рассматриваются различные критерии классификации рисков безопасности информационных систем и дается обзор моделей классификации большинства угроз, также определяют гибридную модель для классификации угроз безопасности информационной системы, чтобы предложить архитектуру классификации, которая поддерживает все принципы классификации угроз и помогает организациям реализовывать свои стратегии информационной безопасности.

В исследовании [3] разделили подходы классификации угроз на два основных класса:

1. Методы классификации, основанные на методах атак

- *Трехмерная ортогональная размерная модель* - модель угроз для классификации угроз безопасности, решающая проблему путем введения трехмерной модели, которая подразделяет пространство угроз на

подпространства в соответствии с тремя ортогональными измерениями, обозначенными как мотивация, локализация и агент (рис.1):

Рисунок 1. Измерение угроз [3]

- *Гибридная модель для классификации угроз* - рассматривает три основных критерий:

- Частота угроз безопасности;
- Область действий угроз безопасности;
- Источник угрозы безопасности;

- *Модель пирамиды классификации угроз информационной безопасности* - классифицирует преднамеренные угрозы на основе трех факторов:

- Знания злоумышленников о системе;
- Критичность области;
- Потери, которые могут возникнуть в системе или в организации;

2. Методы классификации, основанные на воздействии угроз

STRIDE Model (*Spoofing* identity, *Tampering* with data, *Repudiation*, *Information* disclosure, *Denial* of service and *Elevation* of privilege) - это целенаправленный подход, при котором делается попытка проникнуть в сознание злоумышленника путем оценки угроз.

ISO model - Стандарт ISO (ISO/IEC 27001) с целью формирования комплексных требований к безопасности информации определяет три основных показателя:

- оценка рисков, с которыми сталкивается организация (определение угрозы для ресурсов, их уязвимость и вероятность возникновения угроз, а также возможный ущерб);
- соблюдение законодательных, нормативных и договорных требований, которые должны выполняться самой организацией, ее партнерами по бизнесу, подрядчиками и поставщиками услуг;
- формирование комплекса принципов, целей и требований к обработке информации, разработанных организацией для поддержки своей деятельности [4].

Большинство классификаций угроз безопасности обычно ограничиваются использованием одного или двух критериев для классификации угроз (не все угрозы включены в классификацию), и их категории не взаимоисключающие. Этого может быть достаточно для стабильной среды (небольшой организации), где угрозы безопасности относительно стабильны, но в постоянно меняющихся средах организации не могут защитить от внутренних угроз [5].

На самом деле, организации подвержены нескольким видам угроз, которые влияют на их репутацию, и важно, чтобы они идентифицировали все характеристики угроз, чтобы снизить их риски.

Классификация позволяет организации знать угрозы, которые влияют на их активы и области, на которые может повлиять каждая угроза, и следовательно, заранее защищать свои активы. Кроме того, помогает менеджерам создавать информационные системы своих организаций с меньшей степенью уязвимости [5]. Основные проблемы могут быть выявлены в работе существующих угроз. Фактически, существующие классификации не поддерживают принципы классификации [6], [7], [8]. На этом этапе обычным решением является объединение различных классификаций и создание гибридной.

Из-за приведенных выше результатов, [3] предлагают гибридную модель для классификации угроз безопасности информационной системы, которую назвали многомерной моделью для классификации угроз с целью соблюдения всех принципов классификации угроз.

В следующей работе [9] были оценены «угрозы по безопасному использованию Интернета», опросив избирателей, задавая следующие вопросы: «Какая угроза поразила вас больше всего?», «Как вы думаете,

какая угроза имеет значительное влияние на общество?» и т.д., разделив респондентов на три группы: «организации», «пользователи» и «системные администраторы/разработчики», и выявили 10 основных угроз безопасности. Соответствующие угрозы были назначены каждой группе, а затем собраны сведения, включая краткое изложение инцидента, как он произошел, степень ущерба и как он был нанесен, и какие меры были приняты. Следующим образом были представлены угрозы трех групп:

- *Угрозы для организаций:*
  - угроза отравления DNS-кешем;
  - сложные целевые атаки;
  - утечка информации, происходящая ежедневно;
- *Угрозы для пользователей:*
  - разнообразные пути заражения компьютерных вирусов и ботов;
  - угрозы, возникающие из-за уязвимости шифрования беспроводной локальной сети;
  - никогда не уменьшать спам;
  - угрозы, возникающие при использовании одного и того же идентификатора пользователя и пароля;
- *Угрозы системным администраторам/разработчикам:*
  - Угрозы атак через законный сайт;
  - Актуальные пассивные атаки;
  - Потенциальная уязвимость встраиваемых систем/устройств;

Далее рассмотрим облачные вычисления в корпоративной инфраструктуре, приведенные в [10], где обсуждены риски и проблемы безопасности в облачных вычислениях и просвещенные шаги, которые предприятие может предпринять, чтобы снизить риски безопасности и защитить свои ресурсы.

Облачные вычисления - модель обеспечения удобного сетевого *доступа по требованию* к некоторому общему фонду конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам — как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру [11].

Предприятия начинают рассматривать технологию облачных вычислений как способ сокращения затрат и повышения прибыльности, потому что во всех отраслях ИТ-директорам постоянно приходится сокращать капитальные активы, количество сотрудников и расходы на

поддержку, а облачные системы дают им возможность достичь этих целей. На рисунке 2 показано доступные ресурсы для предприятий в облаке (Брендл, 2010) [10].

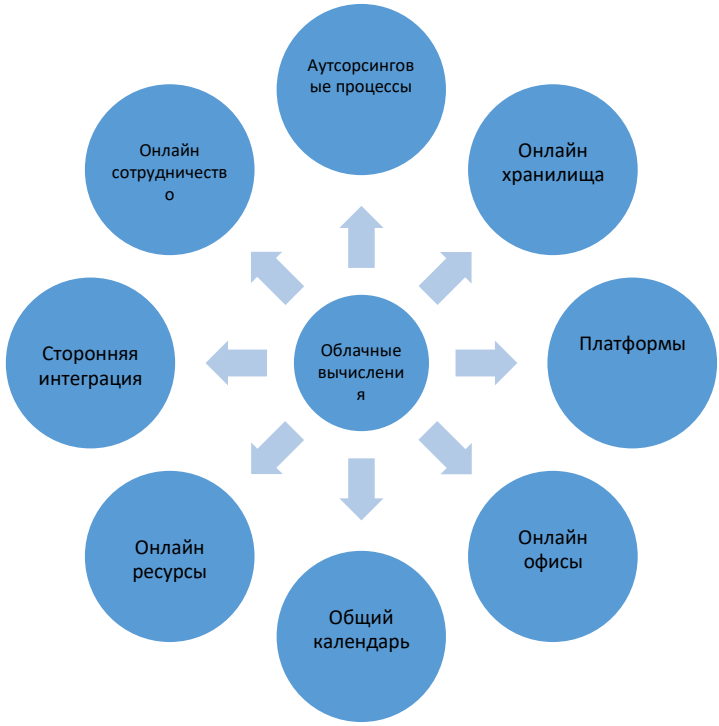

Рисунок 2. Ресурсы облачных вычислений (CloudTweaks, 2010) [10]

Рентабельность облачных вычислений может быть объяснена в формулах «ассоциативность затрат», показанных в формуле (1). Левая часть умножает чистый доход на пользовательский час на количество часов пользователя, давая ожидаемую прибыль от использования облачных вычислений, в то время как правая сторона выполняет те же вычисления для центра обработки данных с фиксированной емкостью, учитывая среднюю загрузку, включая непиковые рабочие нагрузки центра обработки данных; какая сторона больше, тем больше возможностей для получения прибыли (Armbrust et al., 2009) [12].

В работе [12] (Armbrust et al., 2009, стр. 10-11) привели пример эластичности с расчетами потенциалов экономии облачных вычислений и снижения затрат:

$$\text{Пользовательские часы}_{\text{облочный сегмент}} \times (\text{Доход} - \text{Стоимость}_{\text{облочный сегмент}}) \geq$$

$$\geq \text{Пользовательские часы}_{\text{Центр обработки данных}} \times (\text{Доход} - \frac{\text{Стоимость}_{\text{облочный сегмент}}}{\text{Использование}}) \quad (1)$$

Существует несколько крупных поставщиков облачных вычислений, в том числе Amazon [21], Google [22], Salesforce [23], Yahoo [24], Microsoft [25], Alibaba [26], IBM [27] и другие, которые предоставляют услуги облачных вычислений, предоставляя клиентам разнообразные услуги, такие как Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Storage-as-a-Service и Infastructure-as-a-Service (IaaS) в число которых входят электронная почта, хранилище, программное обеспечение и инфраструктура в качестве услуг.

Облачные вычисления сталкиваются с таким же количеством угроз безопасности, которые в настоящее время встречаются в существующих вычислительных платформах, интернет сетях предприятии. Эти угрозы, уязвимости риска бывают разных форм. Cloud Security Alliance [13] провел исследование угроз, стоящих перед облачными вычислениями, и выявил семь основных угроз:

- злоупотребления и злонамеренное использование облачных вычислений;
- небезопасные интерфейсы прикладного программирования;
- злобные инсайдеры;
- уязвимости общих технологий;
- потеря данных/утечка;
- учетная запись, обслуживание и угон трафика;
- неизвестный профиль риска;

Перенос ваших данных в облачный сервис - это все равно, что «положить все яйца в одну корзину» согласно [14]. Исследования показали, что злоумышленники могут точно определить, где находятся данные в «облаке», и использовать различные приемы для сбора информации. Для успешной реализации облачных вычислений на предприятии требует правильного планирования и понимания возникающих рисков, угроз, уязвимостей и возможных контрмер. В [10] полагают, что предприятие должно проанализировать риски безопасности, угрозы и имеющиеся меры противодействия компании/организации, прежде чем применять эту технологию.

Структура веб-приложений и типы атак

С развитием технологий каждое предприятие имеет свой веб-сайт. А веб-сайт, в свою очередь, это система электронных документов (файлов данных и кода), принадлежащий частному лицу или организации, и может быть доступным в компьютерной сети под общим доменным именем и IP-адресом или локально на одном компьютере. Как правило, веб-интерфейс, обращенный к общедоступному Интернету, считается наиболее уязвимым и «рискованным», когда речь идет об уязвимостях, поэтому веб-сайты являются одной из основных целей для хакеров. Как только злоумышленник достигнет веб-приложения, это может привести к тому, что он достигнет компьютерной системы или базы данных, сервера или конфигураций реализации или операционной системы.

Приведем некоторые анализы по взламыванию сайтов на предприятиях.

В среднем от 30 000 до 50 000 сайтов каждый день взламывается, и на самом деле большинство из этих 30 000 сайтов являются законными малыми предприятиями, которые невольно распространяют вредоносный код для киберпреступников.

64% компаний сталкивались с веб-атаками на основе доступной в настоящее время статистики. 62% подвергались атакам фишинга и социальной инженерии, а 59% компаний сталкивались с вредоносным кодом и ботнетами [15].

По приведенным выше данных видим значимость необходимости обеспечения информационной безопасности веб-приложений предприятий, каждодневно использующие интернет ресурсы.

В связи с этим рассмотрим структуру веб-приложений и приведем типы атак для исследования дальнейшей работы.

Чтобы понять слабость веб-среды, мы также должны знать компоненты веб-приложения. Веб-приложения состоят из трех основных частей, как показано на *рисунке 3.* Язык программирования используется для разработки клиентской части и для создания запросов к базе данных. Протокол передачи гипертекста (http), который используется для связи стороны клиента со стороной сервера. В добавок бизнес-процесс, который является отличительной частью любого веб-приложения.

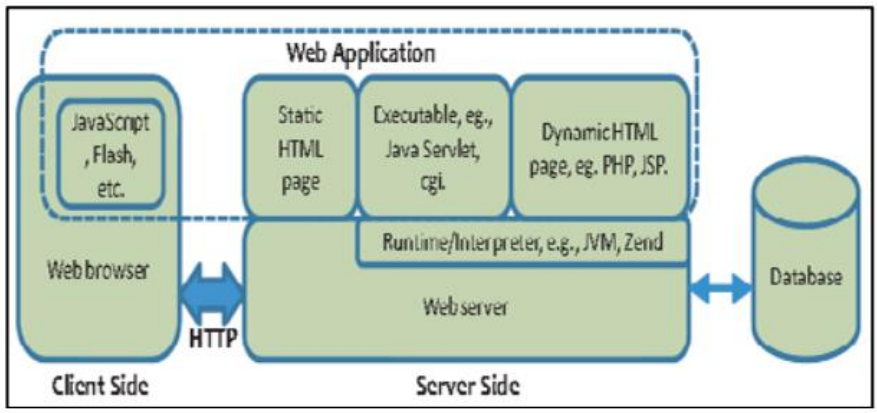

Рисунок 3. Компоненты веб-приложения [16]

Еще одна главная угроза в интернет-безопасности и веб-приложениях, которую пользователи просматривают через порт по умолчанию номер 80 с использованием протокола http и номер порта 443 с использованием протокола безопасного уровня https. Злоумышленник начинает использовать Интернет как обычный клиент или пользователь веб-сайта, затем эти порты используются для атаки на сайт и доступ к данным и файлам клиентов. Размер атаки зависит от важности данных и бизнеса компаний, которые владеют этими сайтами [16].

Далее приведем самые распространенные виды атак в веб-приложениях:

1. *DDoS-атаки:* DDoS-атаки направлены на подавление целевого веб-приложения/ веб-сайта/сервера ложным трафиком, снижая пропускную способность сети и делая ее недоступной для законных пользователей. Некоторые распространенные, но опасные типы DDoS-атак включают усиление DNS, Ping of death, Smurf-атаки, HTTP-флуд, SYN-флуд и т. д. [17].
2. *Атаки SQL-инъекций.* В этих атаках злоумышленник внедряет вредоносный код SQL в виде запросов или запросов в поля ввода пользователя в веб-приложениях, таких как формы отправки, контактные формы и т. д. Таким образом, они получают доступ к внутренней базе данных приложения, куда они проникают извлекать конфиденциальную информацию о клиентах или самой компании, получать несанкционированный административный доступ, изменять или удалять данные и т.д. или даже получать полный контроль над веб-приложением [17].
3. *Атаки межсайтового скриптинга (XSS).* Атаки XSS направлены на пользователей уязвимых веб-приложений/веб-сайтов, чтобы

получить доступ к браузерам и управлять ими. Здесь злоумышленники используют уязвимости и пробелы в приложении для внедрения вредоносных скриптов/кодов, которые выполняются, когда ничего не подозревающий пользователь загружает приложени/веб-сайт. Атаки XSS ставят под угрозу личную и конфиденциальную информацию пользователя и часто приводят к краже личных данных, перехвату сеансов и т.д. [17].

4. *Атаки нулевого дня (Zero-day Attacks).* Атаки нулевого дня - это те, в которых организация знает о существовании уязвимостей в аппаратном/программном обеспечении только тогда, когда атака происходит. Это неожиданно и, следовательно, очень вредно для бизнеса, поскольку у них нет быстрых исправлений или исправлений для защиты своего приложения [17].

5. *Атаки бизнес-логики (Business Logic Attacks).* Бизнес-логика является критическим элементом, соединяющим и передающим информацию между пользовательским интерфейсом и базами данных и системами программного обеспечения, позволяя пользователям эффективно использовать веб-приложение/веб-сайт. Когда в бизнес-логике есть пробелы, ошибки или совпадения, это создает уязвимости, которые часто используются кибер-атакующими для получения денежных и других преимуществ. Злоумышленники не используют искаженные запросы и вредоносную нагрузку для организации атак бизнес-логики. Они используют законные ценности и правовые запросы для использования косвенных уязвимостей в приложении [17].

6. *Атаки «человек посередине» (Man-in-the-middle attacks).* Эти атаки происходят, когда злоумышленники позиционируют себя между приложением и законными пользователями для извлечения конфиденциальной информации, такой как пароли, учетные данные для входа, данные кредитной карты и т. Д., Выдавая себя за одну из двух сторон. Атака может быть организована с помощью простых средств, таких как предоставление бесплатных, вредоносных точек доступа в общественных местах, которые не защищены паролем. Когда жертвы подключаются к этим точкам доступа, они предоставляют злоумышленнику полную прозрачность обмена данными в Интернете [17].

7. Вредоносные программы (Malware). Атаки вредоносных программ организуются путем использования уязвимостей приложений или с помощью методов социальной инженерии, таких

как фишинг, для внедрения вредоносных программ, таких как трояны, вымогатели, шпионское ПО, руткиты и т.д., на веб-сайт/веб-приложение/сервер. Тем самым злоумышленник получает доступ к конфиденциальной информации, конфиденциальным частям приложения, изменениям конфигурации системы [17].

8. Пороки (Defacements). При атаках с использованием фальсификации, самой простой из всех кибератак, злоумышленники изменяют контент веб-сайта и заменяют его своим собственным контентом, чтобы отразить политическую идеологию/повестку дня, шокировать пользователей спорными сообщениями или образами. До устранения порчи веб-приложение может стать недоступным для пользователей [17].

Исследуя вышеуказанные работы выявили какие есть угрозы безопасности в организациях, и рассмотрели структуры веб-приложений с распространенными видами атак.

Традиционные решения безопасности, такие как сетевые брандмауэры, системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS), хороши для предотвращения незаконного трафика и обеспечения безопасности на уровне сети. Но у них нет возможности обнаруживать и останавливать внедрение SQL, перехват сеансов, межсайтовый скриптинг (XSS) и другие атаки, возникающие в результате уязвимостей, присущих веб-приложениям, одним из решений является конфигурация WAF (Web application firewall).

Обоснования WAF (Web application firewall) и его преимущества

Файрвол веб-приложений предоставляют эффективное решение для обнаружения угроз путем проверки входящих HTTP-запросов еще до того, как они достигнут сервера. WAF (Web application firewall) обнаруживает и блокирует злонамеренные атаки, связанные с безопасным трафиком веб-сайта, который мог просочиться через традиционные решения безопасности. WAF также используются, чтобы помочь организациям соблюдать требования HIPAA и PCI-DSS [20].

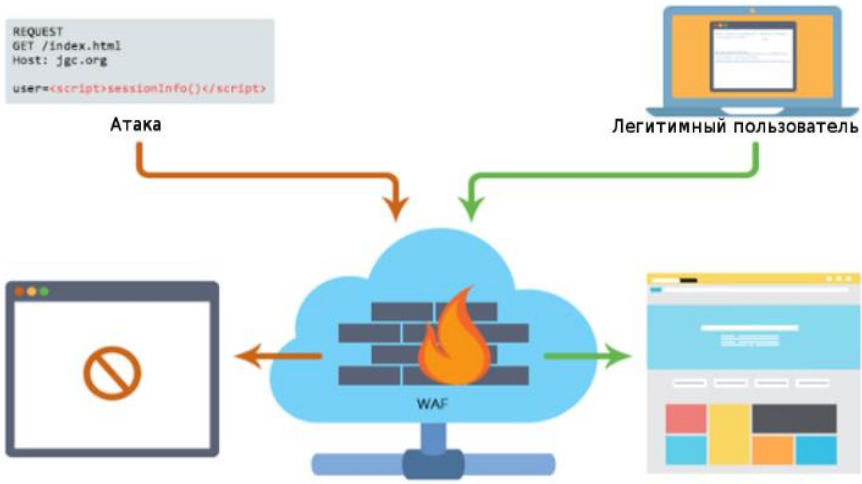

Рисунок 4. Структура защиты WAF

Работа WAF обычно основана на одной из трех моделей безопасности:

1. Черный список или модель с отрицательной защитой - при этом используются общие подписи для защиты сайта от известных атак и специальные подписи для предотвращения атак, которые могут использовать уязвимости в веб-приложении;

2. Белый список или модель позитивной безопасности - при этом используются сигнатуры, а иногда и дополнительная логика, чтобы разрешить только трафик, соответствующий определенным критериям. Примером является разрешение только HTTP-запросов GET с определенного URL-адреса и блокирование всего остального;

3. Гибридная модель безопасности - это касается как негативных, так и позитивных моделей. Некоторые из настраиваемых параметров включают блокировку запроса, блокировку сеанса, блокировку IP-адреса, блокировку пользователя или выход пользователя из системы [20].

Веб-приложения и SQL-инъекция

Связь между базой данных и веб-приложениями очень прочна, поскольку большинство веб-приложений предназначены для извлечения и хранения данных клиентов в базах данных. Поэтому SQL-инъекция становится серьезной атакой на веб-приложение для извлечения или хранения данных без авторизации или разрешения доступа. SQL-инъекция

- это метод внедрения веб-приложения с параметром ошибки через SQL-сообщения для получения несанкционированного доступа [16].

У WAF есть некоторые недостатки из-за отсутствия автоматизации, масштабируемости и охвата возникающих угроз, поскольку современные бот-сети становятся все более и более эффективными и агрессивными. Эти ботнеты теперь создаются с помощью функции искусственного интеллекта (ИИ) поверх «старых» ботнетов Интернет вещей (IoT), которые становятся все более универсальными в своей способности атаковать с различными векторами. Функциональность, которую предлагает классический WAF, стала предметом недовольства, в то время как WAF следующего поколения, которые были рождены как системы искусственного интеллекта, которые могут справиться с такой многомерной сложностью угроз, встречаются довольно редко.

В сегменте киберзащиты сети и защиты приложений не так много решений по искусственному интеллекту/машинному обучению (AI/ML). Однако все больше и больше решений AI и ML начинают проявляться в качестве основного успеха против атак распределенного отказа в обслуживании (DDoS) и, более конкретно, против мира приложений DDoS **(**Distributed Denial of Service***)***, что было продемонстрировано L7 Defense с его неконтролируемым подходом к обучению. Такая технология также может играть решающую роль в решениях WAF, таких как защита от тех же многоцелевых ботнетов [18].

Заключение

Что касается защиты, традиционные методы используют некоторый словарь или базу данных известных уязвимостей.

WAF должен быть в состоянии бороться с множеством многовекторных атак, таких как внедрение SQL, удаленное выполнение команд, включение удаленных файлов, включение локальных файлов, внедрение PHP, внедрение LDAP, внедрение Memcache и межсайтовый скриптинг (XSS); все вместе. Нам нужен опыт, чтобы идентифицировать эти типы атак и классифицировать их с максимальной точностью с первого запроса. Объективно, это критически важная часть для определения по «самому первому запросу» [18].

Ложные срабатывания и ложные отрицания должны быть ограничены, что было бы близко к нулю на уровне веб-страницы.

Нам нужно найти решение, которое использует те же концепции AI из Applicative DDoS и необходимо добавить конкретные классификации в дополнение к возможности алгоритмически динамически идентифицировать все типы атак на лету. WAF должна быть предоставлена дополнительная возможность, чтобы он мог точно

определить, есть ли какая-то агрегация трафика в вашем веб-интерфейсе, идущем к вам, используя машинное обучение, которое будет нашей дальнейшей работой [18].

Для качественной организации деятельности по предупреждению угроз информационной безопасности предприятию необходимо:

– качественное прогнозирование угроз;

– разработка превентивных мер защиты предприятия.

В организации деятельности по предупреждению угроз информационной безопасности основной задачей является прогнозирование и оценка возможных угроз предприятии.

Таким образом, очень важно, чтобы предприятие приняло структурированную методологию для определения соответствующих угроз, переоценки остаточных уязвимостей и выявления новых угроз.

Список использованной литературы:

1 Сергеева И.А., Володин В.М. Прогнозирование потенциальных угроз - основа превентивных мер финансовой безопасности организации // Общественные науки. Экономика. – 2017. – № 1 (41). – С. 140-148.
2 Stacey, T.R., Helsle, R.E., Baston, J.V. Identifying Information Security Threats. – pp. 1-13.
3 Jouinia, M., Rabaia, L.B.A., Aissab, A.B. Classification of security threats in information systems. Procedia Computer Science, 32 (2014): pp. 489 – 496.
4 ISO/IEC 27001 (ГОСТ Р ИСО/МЭК 27001). URL: https://rusregister.ru/standards/iso-27001/
5 Geric, S., Hutinski. Z. Information system security threats classifications. Journal of Information and Organizational Sciences, 31 (1), (2007): pp. 51-61.
6 Lindqvist, U., Jonsson, E. How to systematically classify computer security intrusions. IEEE Symposium on Security and Privacy, (1997): pp.154-163.
7 Tang, J., Wang, D., Ming, L., Li, X. A Scalable Architecture for Classifying Network Security Threats. Science and Technology on Information System Security Laboratory; 2012.
8 Howard J.D. An Analysis Of Security Incidents On The Internet 1989 – 1995. Doctoral Dissertation, Carnegie Mellon University Pittsburgh, PA, USA; 1998

9 10 M a j o r Security Threats Attacking Techniques Become More and More Sophisticated. Information Security White Paper, Japan, June 2009 – P. 1-25.
10 Bisong, A., Rahman, S.M. An overview of the security concerns in enterprise cloud computing. International Journal of Network Security & Its Applications (IJNSA), 3 (1), (2011): pp. 30-44.
11 Облачные вычисления. URL: https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D0%BB%D0%B0%D1%87%D0%BD%D1%8B%D0%B5_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F
12 Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M. Above the Clouds: A Berkeley View of Cloud Computing. – pp. 10-11 URL: http://d1smfj0g31qzek.cloudfront.net/abovetheclouds.pdf
13 Cloud Security Alliance (2010). Top Threats to Cloud Computing. Cloud Security Alliance. URL: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
14 Perez, S. (2009). The Cloud Isn't Safe?! (Or Did Black Hat Just Scare Us?). August 5, 2009. ReadWriteWeb. URL: http://www.readwriteweb.com/archives/the_cloud_isnt_safe_or_did_blackhat_just_scare_us.php
15 What is Web Application Firewall (WAF)? Updated: July 19, 2019 by Agnes Talalaev. URL: https://www.webarxsecurity.com/web-application-firewall/
16 Abusaimeh, H., Shkoukani, M. Survey of Web Application and Internet Security Threats. IJCSNS International Journal of Computer Science and Network Security, 12 (12), (2012): pp. 67-76.
17 8 Types of Cyberattacks a WAF is Designed to Stop. April 17, by Venkatesh Sundar URL: https://www.indusface.com/blog/8-types-of-cyberattacks-a-waf-designed-to-stop/
18 The WAF backed by artificial intelligence (AI). By Matt Conran, Oct 2, 2018. URL: https://www.networkworld.com/article/3310359/the-waf-backed-by-artificial-intelligence-ai.html.
19 Web Application Firewall — защита сайта от хакерских атак. Luka Safonov, 27 мая 2009 в 14:08. URL: https://habr.com/ru/post/60590/
20 What is a Web Application Firewall? URL: https://chesstrending.com/crm/knowledge-base/web-application-firewall-waf.

21 Что такое облочные вычисления. URL: https://aws.amazon.com/ru/what-is-cloud-computing/.

22 Google Cloud Platform Overview. URL: https://cloud.google.com/docs/overview.

23 Cloud computing – apps on tap. URL: https://www.salesforce.com/ap/cloudcomputing/.

24 Cloud Computing Today. URL: https://cloud-computing-today.com/category/yahoo/.

25 Microsoft Azure. URL: https://en.wikipedia.org/wiki/Microsoft_Azure.

26 Alibaba Cloud. URL: https://en.wikipedia.org/wiki/Alibaba_Cloud.

27 Cloud computing: A complete guide. URL: https://www.ibm.com/cloud/learn/cloud-computing.

Форматы 70×100 1/16. 12 б.т.
Таралымы 300 дана

С. Демирел атындағы университеттің хабаршысы
Абылай хан көшесі, 1/1
Алматы облысы, Қаскелең қаласы
040900, Қазақстан
Тел.: +7 727 307 95 60 (іш. 236)
Факс: +7 727 307 95 58
e-mail: info@sdu.edu.kz

Format 70×100 1/16. 12 p's sh.
Edition 300 copies

The editorial office of the scientific journal
Suleyman Demirel University
1/1 Abylai Khan Street, Kaskelen
Kazakhstan, 040900
Tel: +7 727 307 95 60 (ext. 236)
Fax: +7 727 307 95 58
info@sdu.edu.kz