White Paper

Web Application Firewall
Подробный анализ

Содержание

Введение

Несмотря на то, что Файрвол веб-приложений (Web Application Firewall, WAF) повсеместно используется и активно совершенствуется, вопрос о его необходимости и даже обязательности, требует подробного рассмотрения.

Из данного материала вы также узнаете об алгоритмах работы WAF, особенностях его выбора и подключения. Кроме того, вашему вниманию предлагается прогноз того, как будет развиваться рынок обеспечения безопасности веб-ресурсов.

Для чего нужен WAF?

Некоторые полагают, что любой файрвол не является необходимым элементом в системе обеспечения безопасности, что можно ограничиться поддержанием программного обеспечения в актуальном состоянии и своевременным «пропатчиванием». Однако Файрвол веб-приложений принципиально отличается от остальных файрволов, в т. ч. и файрволов следующего поколения (NGFW, Next Generation Firewall).

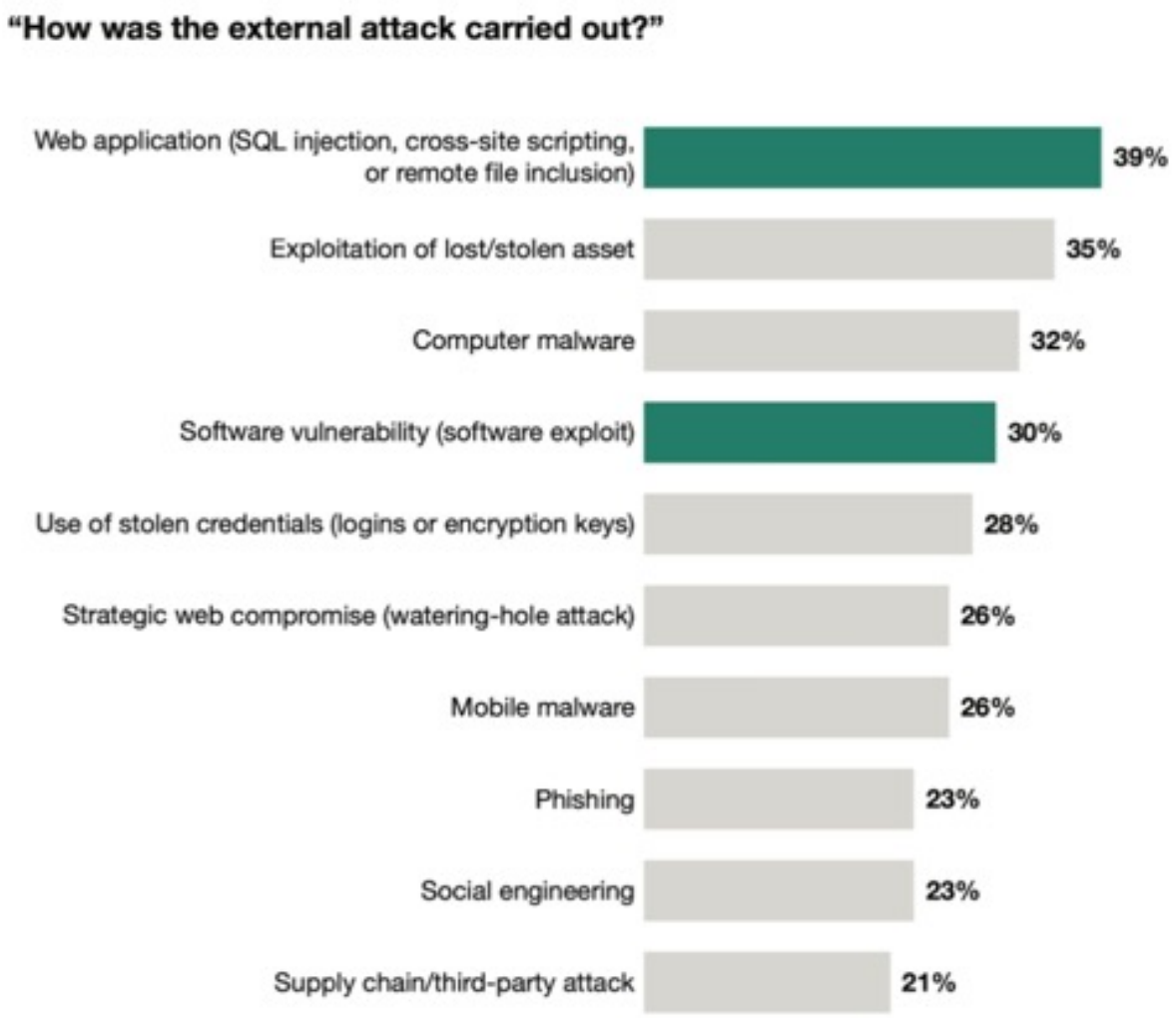
WAF используется для защиты веб-приложений от внешнего трафика (внешних пользователей, клиентов). Зачастую этот трафик включает хакеров (и ботов), которые пытаются украсть данные клиентов, вызвать отказ в обслуживании и даже проникнуть во внутренние базы данных.

1. Отказ от использования Файрвола веб-приложений имеет смысл только в том случае, если у предприятия вообще отсутствуют веб-ресурсы или они есть, но не играют критически важной роли. Смысл в том, что WAF направлен на защиту важнейших веб-ресурсов предприятий, в которых содержатся персональные данные, платежная информация и др.

В зависимости от размера и типа организации атака может варьироваться от мелкой неприятности до нанесения ей непоправимого ущерба. Клиенты веб-сайтов этих компаний также могут подвергаться опасности, поскольку атаки могут привести к заражению компьютеров пользователей вредоносными программами и краже учетных данных.

Мишенями оказались государственные организации и компании электронной торговли. Два этих сектора подвергаются наивысшему уровню попыток взлома. Электронная коммерция подвергается атакам, направленных на то, чтобы вызвать простои и получить доступ к внутренним файлам. Напротив, 65% всех атак в финансовом секторе направлены на кражу регистрационной информации посетителей веб-сайта.

Такие кибератаки на веб-приложения являются движущей силой рынка. Банковские, финансовые услуги и страхование занимают наибольшую долю рынка. Специалисты в области информационной безопасности признают, что незащищенные веб-приложения стали целями для доступных хакерам точек входа в их сети. Это главный аргумент для фирм, предоставляющих финансовые услуги, которые считают, что их защита периметра полностью защищает их. Защита персональных данных пользователей обычно является слабым звеном для многих компаний, поскольку внутренние группы разработчиков приложений не могут быть в курсе всех новых типов атак.



2. WAF эффективно защищает кастомные разработки, которые часто используют успешные компании. А в кастомных разработках по умолчанию больше уязвимостей и угроз безопасности, чем в стандартных решениях.

3. Согласно Сетевой модели OSI (Open Systems Interconnection), Файрвол веб-приложений работает на уровне 7 (прикладном), где пользовательские приложения обращаются к сети.

Тем самым WAF имеет дело с запросами, которые находятся вне контроля стандартных файрволов. Также Файрвол веб-приложений предоставляет защиту от DDoS-атак, осуществляет контроль интеграций с внешними сервисами, защиту сайта и веб-сервера приложений.

4. От межсетевых экранов Файрвол веб-приложений отличается:

• Архитектурно: метод подключения и установки в сеть (WAF изначально функционирует по принципу реверс-прокси).

• Функционально: в отличие от файрволов следующего поколения, WAF «понимает»m специальные форматы внутри протокола HTTP (к примеру, JSON).

Еще раз: WAF занимается протоколами веб-приложений, использующими HTTP в качестве транспорта, тогда как стандартные файрволы, файрволы следующего поколения и IPS (Intrusion Prevention System, Система предотвращения вторжений) являются многопротокольными.

Файрвол веб-приложений считается высокоэффективным решением, поскольку глубоко анализирует специализированные протоколы, определяет подходящие политики безопасности в зависимости от объекта, на который поступает трафик.

Само собой, при внедрении Файрвола веб-приложений можно использовать открытое программное обеспечение (open-source software), однако это решение имеет немало минусов, основной из которых – полная ответственность предприятия за функционирование, доработку, исправление ошибок и поддержание в актуальном состоянии.

Также существует выбор места размещения WAF – локальная или облачная среда. Большинство экспертов рекомендуют использование облака, что подтверждается соответствующей тенденцией в сфере безопасности веб-приложений. Хотя решение остается за компанией и зависит в немалой степени от уровня доверия к провайдеру облачных сервисов.

Файрвол веб-приложений может быть реализован исключительно программно или в виде программно-аппаратного комплекса. Что выбрать? На ответ влияют потребности предприятия, сроки внедрения и бюджет. Считается, что специфические программно-аппаратные комплексы более эффективны, но для многих предприятий гораздо проще сохранить свою структуру аппаратных платформ, воспользовавшись универсальными решениями.

Как работает файрвол веб-приложений?

Поток данных проходит через ряд модулей защиты Файрвола веб-приложений, включая блоки защиты от DDoS-атак, а также сигнатурного анализа, образно говоря, через базовые уровни. На следующих уровнях могут находиться подсистема матобучения и специально разработанные политики безопасности, блок интеграции с внешними системами.

Файрволы веб-приложений «комплектуются» пассивным/активным сканером для выявления уязвимостей, анализа ответов сервера, опроса конечных точек. Опционально WAF доступно определение неправомерной активности в браузере. При определении атак WAF выполняет функцию валидации (проверяется информация в конкретных запросах), исследование поведения, в каждом из которых имеются собственные специальные алгоритмы. Говоря об этапах обработки запросов, специалисты вспоминают о блоке парсеров, модулях декодирования, наборе правил блокировки, которые отвечают за окончательное решение. Дополнительно существует уровень политики безопасности, разрабатываемых человеком или с помощью машинного обучения.

В вопросе контейнеров Web Application Firewall различаются способы развертывания при сохранении принципов функционирования. Так, Файрвол веб-приложений может работать в форме контейнера, интегрируясь с шиной передачи данных, а может быть внедрен и другими методами, к примеру, в формате фильтра запросов на вход в среду виртуализации, то есть в роли IP-шлюза.

Помимо прочего, WAF может предоставляться в формате «программного обеспечения как сервиса» (software as a service, SaaS), когда дается полный доступ к приложению и администрированию приложения в облаке. По мнению экспертов, особых достоинств этот формат не имеет, но в то же время это первый этап в переносе инфраструктуры в облачную среду. В случае делегирования провайдеру технической поддержки системы имеет смысл говорить о модели MSSP (managed security service provider). Что касается эффективности работы Файрвола веб-приложений и методов ее оценки, то здесь применяется упомянутый ранее Penetration test, проводимый заказчиком на этапе пилотирования проекта. И, конечно же, аналитическую информацию о трафике в виде периодических отчетов заказчику должны предоставлять продавцы услуги и ее интеграторы.

Подключение Web Application Firewall

Внедряется Файрвол веб-приложений по следующему сценарию:

1) Проводится пилотирование проекта.
2) Выбирается провайдер.
3) Определяется архитектура.
4) Определяется технология резервирования.
5) Развертывание программного или программно-аппаратного комплекса.
6) Обучение сотрудников.

На внедрение Файрвола веб-приложений влияет метод развертывания, выбранное приложение, подлежащий контролю трафик. Этому процессу следует уделить пристальное внимание во избежание ложных срабатываний файрвола в будущем, а именно: осуществить тестирование в два этапа, до запуска системы и, соответственно, после него. В процессе тестирования обязательно должен участвовать грамотный специалист, который проанализирует принимаемые Файрволом решения, «откалибрует» его. Для борьбы с ложными срабатываниями необходимо по итогам 1-го месяца проанализировать статистическую информацию WAF, чтоб предотвратить блокировку «хорошего» трафика.

Фильтры помогают предотвратить атаки, такие как XSS и SQL-инъекция, от попадания в уязвимое приложение. Фильтры являются либо положительными фильтрами, которые позволяют только «заведомо хорошим» входам достигать приложения, либо отрицательными фильтрами, которые блокируют «заведомо плохие» входы. Положительные фильтры очень эффективны при блокировании атак, но требуют постоянной настройки. Команды должны проверять и, возможно, корректировать эту настройку каждый раз, когда приложение изменяется.

Среди направлений интеграции Файрвола веб-приложений с иными средствами безопасности специалисты называют DLP-системы (Data Loss Prevention, предотвращение утечки данных), NGFW, SIEM-системы (Security information and event management), песочницы, сканеры уязвимостей, антивирусные ядра, а также средства безопасности внутри платформы Kubernetes.

Поскольку проверка запросов и ответов требует больших вычислительных ресурсов, WAF может производить задержку трафика. Степень этой задержки и то, будет ли она терпима для конечного пользователя, зависит от производительности WAF, сложности политики и используемого приложения.
В ходе проведенного опроса выяснилось, что только 20 % респондентов, использующих Файрвол веб-приложений, не видят сложностей в его внедрении. 32 % участников опроса считают недостатком данного решения ложные срабатывания. По мнению 21 % опрошенных, Файрвол веб-приложений тяжело администрировать. 18 % респондентов обратили внимание на дороговизну продукта. В свою очередь, 5 % и 4 % заявили о пониженной производительности сайтов и недостаточной масштабируемости соответственно.

Как будет развиваться рынок WAF?

Эксперты положительно оценивают тенденции на рынке и продолжение распространения открытых WebAPI, которые в исследовательской компании Gartner называют термином WAAP (Web Application & API Protection). Распространение пандемии и карантин способствуют повышенному спросу на онлайн, который безусловно влияет на значение WAF как основы безопасности веб-сайта.

Прогнозируется постепенное сближение и встраивание WAF в процесс разработки приложений.

Можно с уверенностью предположить, что в Файрвол веб-приложений будут встраиваться системы ИИ, а также многоуровневое машинное обучение, будут разрабатываться новые подходы выявления неизвестных угроз, а поведенческие факторы начнут активнее использоваться в механизмах фильтрации.

И, наконец, продолжится тенденция переноса Web Application Firewall в облачную среду, интеграция с соответствующими облачными сервисами, а возможно и повышение открытости WAF.

Чем мы можем Вам помочь?

ООО «НТЦ ЕВРААС», являясь многопрофильной коммерческой структурой, имеет все необходимые лицензии регуляторов рынка информационной безопасности, в том числе лицензии на осуществление работ с использованием сведений, составляющих государственную тайну.

Обладая фундаментальными знаниями и опытом в области защиты информации, эксперты НТЦ «ЕВРААС» предлагают новейшие комплексные разработки в сфере обеспечения безопасности компаний розничной торговли.

Мы проектируем системы под конкретные нужды и специфику организаций, тем самым гарантируя, что система информационной безопасности комплексно решает все задачи и обеспечивает надежную круглосуточную защиту ваших корпоративных ресурсов и данных.

Контакты:

г. Москва, ул. Автозаводская 13/1

8 (495) 748-09-44

evraas@evraas.ru