Алгоритм защиты веб-приложений
по модели MSS

Михаил ГОРШИЛИН,
руководитель направления управляемых сервисов кибербезопасности компании RED Security

Ежедневно увеличивается количество атак на веб-приложения. Принятие взвешенного решения о том, какую схему защиты выбрать, имеет ключевое значение для безопасности компании. Рассмотрим, как услуга Web Application Firewall (WAF) в модели MSS (Managed Security Services – «управляемые сервисы безопасности») помогает организациям эффективно защищать веб-приложения, и чем такой вариант поставки отличается от классической модели On-Premise – метода развертывания ПО на собственных серверах и инфраструктуре.

В 2023 г. на атаки через веб-ресурсы пришлось более 46% общего числа всех атак на компании, а 58% инцидентов приводили к прерыванию важных бизнес-процессов. В связи с увеличением количества атак аналитики RED Security прогнозируют стремительный рост рынка решений для защиты веб-приложений в ближайшие годы. К 2026 г. объем рынка может превысить 7 млрд руб.

Системы WAF защищают веб-приложения компаний от различных типов целевых и массовых атак из списка OWASP TOP-10 (актуальный рейтинг основных угроз безопасности веб-приложений), направленных на проникновение в веб-приложения с целью кражи или подмены конфиденциальных данных, а также от атак на API, 0-day и 1-day угроз.

Межсетевые экраны уровня приложений обеспечивают сканирование ресурсов на наличие уязвимостей и их виртуальный патчинг, реализуют защиту на основании уникальной бизнес-логики веб-приложений компаний. Защита веб-ресурсов с помощью WAF актуальна для всех организаций, чей бизнес напрямую связан с интернет-операциями. Например, для крупных маркетплейсов или компаний, работа которых может полностью остановиться из-за блокировки или дефейса сайта (от англ. deface – «искажать») – метода взлома, при котором изменяется внешний вид страницы с целью размещения на ней противоправного контента.

Организации разного размера в любой сфере деятельности, публикующие веб-сайт или приложение в сети Интернет, рискуют пострадать от утечек данных клиентов и сотрудников или иной конфиденциальной коммерческой информации. Злоумышленники предпочитают начинать атаки со взлома сайтов, потому что они находятся в открытом доступе, в отличие от защищенной внутренней инфраструктуры компании. Иными словами, любой желающий может «потренироваться» на сайте или веб-приложении и осуществить попытку взлома из любой точки мира.

Чем больше у компании цифровых услуг и сервисов, тем выше шанс рано или поздно столкнуться с кибератакой. Однако не всегда у организаций есть возможность и достаточная экспертиза для самостоятельного администрирования всех используемых решений. Кроме того, новое оборудование и внедрение сервисов требуют больших разовых инвестиций и долго окупаются, а на развертывание ИБ-решений во внутренней инфраструктуре уходят месяцы работы. Сложность процесса усугубляется явным дефицитом ИБ-специалистов на рынке труда.

WAF в модели поставки MSS

Использование MSS-модели подразумевает аутсорсинг управления системами безопасности заказчика. Когда критически важные системы находятся в руках внешней организации, у ИТ-команд клиента появляется больше времени для участия в важных проектах и выполнения профильных задач бизнеса. Задача провайдера

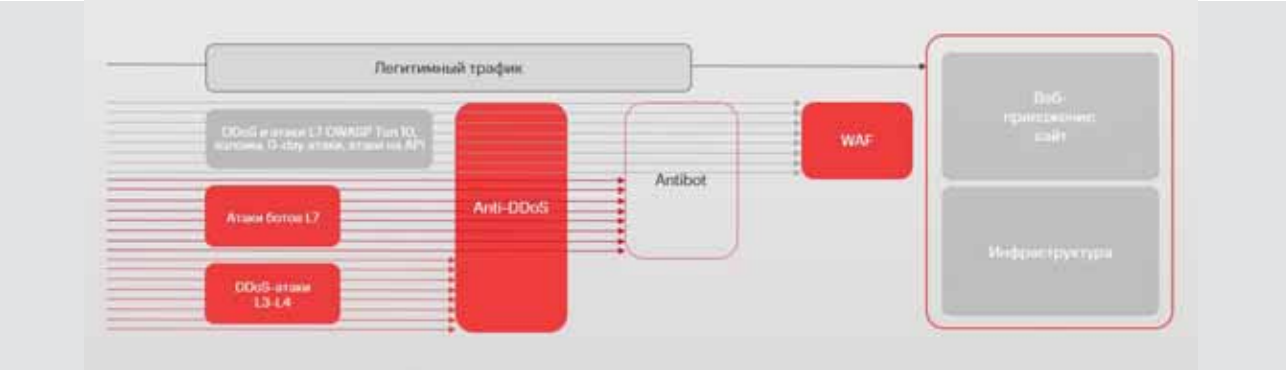

Рис. 1. *Схема реализации многоуровневой защиты веб-приложений*

MSS – облегчить нагрузку на ИТ-отделы заказчика, предоставив собственную экспертизу и человеческий ресурс. Главное для компании – правильно выбрать партнера, которому можно доверить критически важные функции для обеспечения информационной безопасности.

Выбор сервиса и провайдера, как правило, проводится посредством пилотного тестирования.

Один из важных аспектов при выборе решений класса WAF – возможность оперативного масштабирования системы. Сезонные акции, «черные пятницы», распродажи и другие факторы, подогревающие интерес пользователей, стимулирующие рост количества запросов к веб-приложению, требуют наращивания производительности инфраструктуры, на которой развернут WAF, а также пропускной способности канала доступа в интернет.

В случае бездействия система может перегрузиться и заблокировать слишком много легитимных запросов. Всем знакома ситуация, когда в периоды повышенного спроса сайты не справляются и выдают ошибку – для бизнеса это означает не только потерю клиента и прибыли, но и репутации. Если речь идет о поставке по модели MSS, то провайдер предусматривает возможность увеличить производительность инфраструктуры и пропускную способность канала связи в рамках используемого тарифа.

В модели поставки MSS администрирование выполняется высококвалифицированными аналитиками, которые каждый день настраивают и корректируют правила защиты для веб-приложений разных заказчиков, тем самым расширяя свою экспертизу.

Важный аспект при выборе провайдера – возможность многоуровневой защиты веб-приложений для блокировки разных типов атак, особенно если заказчик работает с большим объемом трафика. Одного решения для обеспечения безопасности может быть недостаточно – WAF не станет полноценной заменой решений Anti-DDoS для защиты от атак на сетевом и транспортном уровнях (L3–L4). Наибольший эффект достигается при эшелонированном подходе, когда запросы к веб-ресурсам сначала проходят проверку системой Anti-DDoS, затем системой Anti-Bot определяется наличие вредоносных ботов, и уже WAF защищает веб-приложения от взлома злоумышленниками.

WAF в инфраструктуре заказчика

В модели поставки On-Premise администрирование WAF происходит на стороне заказчика, и качество защиты в высокой степени зависит от экспертизы его собственных сотрудников. В такой модели может быть ограничена возможность оперативного масштабирования инфраструктуры: как правило, лицензии предоставляются на определенное количество RPS (количество запросов в одну секунду). В моменты резкого увеличения количества запросов заказчик может быть вынужден переключаться на более производительную лицензию либо в срочном порядке масштабироваться.

Если интегратор внедряет WAF с базовым уровнем технической поддержки, команда заказчика может испытывать трудности в настройке правил

В модели поставки MSS администрирование выполняется высококвалифицированными аналитиками, которые каждый день настраивают и корректируют правила защиты для веб-приложений разных заказчиков, тем самым расширяя свою экспертизу.

фильтрации и общего функционирования системы. Некорректно настроенные правила в WAF могут осложнить работу всего веб-приложения и блокировать легитимный трафик. В таком случае, если у команды нет опыта настройки WAF, от системы будет больше вреда, чем пользы.

Схема взаимодействия заказчика и провайдера

В рамках модели поставки MSS все действия по модификации и анализу трафика происходят на мощностях провайдера. Для корректного подключения к сервису клиент должен предоставить следующие данные:

- DNS-запись;
- IP-адрес бэкенда;
- SSL-сертификат;
- сетевые доступы и данные о самом сервисе.

> В модели поставки On-Premise администрирование WAF происходит на стороне заказчика, и качество защиты в высокой степени зависит от экспертизы его собственных сотрудников.

Для настройки сервиса заказчики часто нанимают дополнительного подрядчика, что в итоге сопоставимо по стоимости с моделью MSS, но все еще без возможности оперативного масштабирования.

Для корректного перенаправления трафика клиент должен изменить IP-адрес в DNS-записи на защищенный IP-адрес, предоставленный провайдером MSS. Заказчик прописывает его в DNS-записи, и трафик автоматически поступает на дальнейшую обработку. Когда пользователь заходит на сайт и вводит запрос в браузер, DNS-запись URL сопоставляется с IP-адресом WAF. Трафик поступает на сервис защиты веб-приложений, анализируется, а затем расшифровывается с помощью сертификата, который ему предоставил клиент. Потом запрос отправляется на серверную часть веб-приложения (бэкенд), после чего WAF зашифровывает и отправляет его обратно пользователю.

Большинство провайдеров MSS работают именно по такой схеме, однако есть и исключения – еще один способ анализа трафика для государственных компаний, которым запрещено передавать свой SSL-сертификат третьим лицам. В таком формате работы заказчик в режиме дублирования отправляет в сторону

Рис. 2. *Схема взаимодействия MSS-провайдера и заказчиков из государственных или финансовых секторов*

провайдера access-лог веб-сервера. Аналитики на стороне провайдера обрабатывают логи и прописывают правила, которые блокируют или разрешают проход трафика без шифрования, потому что сертификат в этом процессе не используется – он остается у клиента. Это частный случай, который подходит в основном государственным компаниям и финансовым организациям, потому что они зависят от стандартов PCI DSS и других нормативных актов.

Многих заказчиков волнует безопасность данных при обработке трафика провайдером MSS. Если компания работает с персональными данными пользователей (ПДн), клиент может обязать провайдера применять маскирование данных. При правильной конфигурации даже администратор WAF не будет видеть учетные данные пользователей, пароли и другую конфиденциальную информацию. Большинство заказчиков заключают NDA с поставщиком и фиксируют требования, которые обязывают эти данные защищать. Такие условия актуальны для всех компаний, работающих с ПДн, учитывая новый пакет законопроектов, который ужесточает административную и вводит уголовную ответственность за утечку персональных данных.

Параметры производительности и надежности

WAF в модели поставки MSS позволяет защищать высоконагруженные веб-приложения с десятками тысяч запросов в секунду и реализовывать геораспределенную резервируемую инфраструктуру. При этом в договоре могут быть предусмотрены показатели качества и работы сервиса, в соответствии с которыми максимально возможное время остановки работы будет составлять всего несколько минут в месяц. Отличительная особенность провайдеров MSS – декларация доступности сервиса, близкой к 99,99%.

> Отличительная особенность провайдеров MSS – декларация доступности сервиса, близкой к 99,99%.

Основными параметрами производительности WAF считаются показатели RPS и полоса пропускания трафика – пропускная способность системы напрямую зависит от размера запроса. Сервисы с малым показателем RPS могут отправлять редкие, но большие запросы, нагружая при этом всю систему защиты веб-приложений. Исходя из этих показателей, заказчик может выбрать наиболее подходящий тариф для актуальных задач, а компания-поставщик WAF обязуется выполнять все технические требования, зафиксированные в SLA (Service Level Agreement).

> Работа WAF подразумевает минимальный временной лаг на обработку, шифрование и отправку трафика.

Многих клиентов также волнует задержка при передаче трафика. Работа WAF подразумевает минимальный временной лаг на обработку, шифрование и отправку трафика. В большинстве случаев это решается путем размещения узла WAF территориально близко по отношению к инфраструктуре клиента. Задержка будет минимальная, если заказчик и провайдер взаимодействуют в рамках одного города.

Заключение

Наиболее частый аргумент в пользу размещения WAF в своем контуре – его полный контроль, однако создание собственной команды квалифицированных специалистов, способных качественно работать с системой, подразумевает значительные финансовые затраты.

WAF в сервисной модели подходит клиентам, у которых высокие требования к отказоустойчивости собственных веб-приложений, но при этом нет возможности или желания самостоятельно администрировать сервис. Аутсорсинг управления системами безопасности дает компаниям разного уровня возможность эффективно защищать свою инфраструктуру без потери качества предоставляемых услуг и в рамках принятых стандартов ИБ-индустрии.

Представители малого и среднего бизнесов могут значительно сократить затраты на обеспечение информационной безопасности, в то время как крупные компании – оптимизировать процессы ИБ и эффективно решить актуальные ИБ-задачи с помощью экспертизы специалистов провайдера. Стоит отметить, что затраты на сервис не будут превышать стоимость покупки лицензии на его использование и содержания целой команды. Однако все зависит от сложности веб-приложений и мер защиты, которые заказчик намерен применять. ■