Темная сторона API First

Тенденции таковы, что WAF будет значимой частью экосистемы безопасности банка, став полностью интегрированной его компонентой. А концепция API First добавит в WAF функционал веб API-Security и API-Protection



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

Рынок средств веб-Security представляет собой динамично развивающийся сегмент ИБ-индустрии. Эти инструменты позволяют разработчикам и администраторам приложений защитить веб-сервисы и их API от атак и утечек данных. Средства веб API-Security и API-Protection включают в себя широкий спектр технологий и методов, таких как шифрование данных, аутентификация, авторизация, контроль доступа, анализ трафика и многое другое.

От WAF к WAAP

Для чего нужны веб-API (application programming interface)? Они представляют собой набор правил и протоколов, используемых ПО для взаимодействия друг с другом в целях обмена данными, что повышает функциональность решения в целом. Обратной стороной повышенной популярности является пристальное внимание к веб со стороны злоумышленников. Поэтому для защиты веб-приложений на рынке появился специализированный класс решений — WAF (Web Application Firewall), который позволяет предотвратить атаки на прикладном уровне (L7).

Файрвол выступает своего рода посредником между пользователем и приложением, проверяя входящий и исходящий трафики на наличие источников потенциальных рисков. В случае обнаружения опасности WAF может попытаться детектировать вредоносный код или полностью заблокировать запрос. Но время не стоит на месте. На ведущие позиции постепенно выходит возможность интеграции приложения с другими сервисами посредством API. Аналитики Gartner в этой связи даже предложили новый термин — WAAP (Web Application and API Protection), обозначающий брандмауэр веб-приложений следующего поколения, где на первый план выходит концепция API First.

Одним из ключевых трендов на рынке WAF является увеличение спроса на решения, способные обеспечить безопасность в реальном времени. С учетом того, что киберугрозы постоянно эволюционируют и становятся все более изощренными, финансовые организации должны иметь возможность мгновенной реакции на них.

Другое значимое направление развития рынка средств веб API-Security и API-Protection (в терминах WAAP) — увеличение уровня интеграции с облачными платформами и сервисами. Этот подход позволяет обеспечить более широкую защиту веб-приложений и их API, а также повысить удобство пользования средствами безопасности, а также управления ими.

К самым свежим направлениям развития WAF можно отнести развитие функции сравнения OAS (Open API Specification), активно продвигаемой на отечественном рынке компанией «Вебмонитрэкс». OAS, в частности, помогает специалистам сравнивать спецификацию, генерируемую на этапе разработки API, с тем, что наблюдается средствами защиты в реальном трафике. Эта аналитика позволяет привести ИБ-инфраструктуру в соответствие со спецификацией.

Кроме того, бездумное следование некоторыми финтехами концепции API First зачастую приводит к появлению зоопарка нетипичных источников рисков: теневых (shadow), неиспользуемых (orphan) и призрачных (zombie) API. Понятно, что подобные угрозы, появляющиеся и исчезающие практически случайным образом, требуют механизмов защиты API, построенных на основе поведенческого ИИ.

Вырастем на 22%

Одним из примеров успешного использования веб-API в банковской сфере является возможность интеграции финансовых услуг с различными приложениями и сервисами. Например, банки начали предоставлять API для сторонних разработчиков, чтобы те могли создавать собственные приложения для управления финансами, совершения платежей и проверки баланса.

Однако любой комфорт имеет свою цену. По данным компании «Гарда», ссылающейся на заявление помощника секретаря Совета Безопасности РФ **Дмитрия Грибкова,** за 2023 год было совершено около 200 тыс. серьезных опасных киберпреступлений против отечественных веб-ресурсов. Это стало причиной того, что решения класса межсетевых экранов для защиты веб-приложений вошли в топ-3 наиболее востребованных информационных технологий для защиты информации.

По данным компании MTC RED, в 2023 году свыше 46% атак на бизнес-структуры были проведены через веб-ресурсы — это на 14% больше, чем в 2022 году. Основными мишенями при этом были сфера финансов и ретейл. По итогам 2023 года объем этого сегмента рынка должен составить примерно 4,6 млрд рублей, а в 2026-м он достигнет 7,2 млрд рублей. В MTC считают, что в ближайшие годы сегмент WAF будет продолжать расти почти так же стремительно, как и весь рынок ИБ (на 22 и 24,6% в год соответственно). Его развитию в значительной мере способствуют рост объемов создаваемых веб-приложений и числа, частоты и сложности использующих этот вектор атак.

Со стороны финансового сообщества к современным WAF предъявляется ряд отраслевых требований, описанных, например, в Стандарте безопасности индустрии платежных карт PCI DSS, а также в документах Банка России. Также службы ИБ банков инспектируют запросы и ответы HTTP/HTTPS-протокола передачи данных в соответствии со своей политикой безопасности. Главное, чего от них ждут в будущем, — проводить всесторонний анализ веб-трафика, формируя индивидуальный профиль защищаемых ресурсов с возможностью мгновенной блокировки вредоносных запросов.

Хоть финансисты предпочитают не афишировать те или иные факты ИБ-внедрений, открываются некоторые данные за 2022 год, позволяющие предметно исследовать кейсы.

Например, в компании «ВебЗайм» — онлайн-сервисе, предоставляющем услуги кредитования для граждан России из рейтинга 10 крупнейших МФО по итогам 2022 года, — утверждают: «Риски, связанные с непрерывностью, являются для нас критичными. Сбой в работе сервиса ведет к остановке всех бизнес-процессов, рискам утечек персональных данных клиентов и соответственно регуляторным рискам». Выбор пал на облачный WAF от IT-провайдера CORTEL, что обеспечило быстрые сроки выполнения проекта. Помимо веб-угроз CORTEL защищает «ВебЗайм» и от другой извечной сетевой проблемы — DDoS-атак.

Еще один кейс: компания «РТК-Солар» обеспечила защиту онлайн-ресурсов банка «Приморье» с помощью облачного сервиса Web Application Firewall экосистемы Solar MSS. Сервис обеспечивает защиту сайта и веб-приложений банка, включая личный кабинет клиента, от атак уровня L7 (DDoS-атак и атак из списка OWASP Top 10). При этом WAF уже доказал свою эффективность: за третий квартал 2022 года сервис зафиксировал более 1,7 млн событий ИБ, идентифицированных как атаки. Все они были успешно отражены и никак не повлияли на работоспособность онлайн-ресурсов. Сервис WAF реализован в виде отказоустойчивого кластера, размещенного в облачной платформе компании «Ростелеком».

Советы бывалых

Как выбрать WAF? По итогам прошедшего года на этот непростой вопрос на основе богатой, но большей частью закрытой статистики отечественные вендоры в рамках эфира AM Live «Как выбрать Web Application Firewall в 2023 году?» дали несколько полезных советов.

Во-первых, по мнению **Владимира Зайцева,** директора по клиентскому сервису компании NGENIX, не надо путать WAF с другими типами файрволов: «WAF настраивается для работы с конкретным приложением, в то время как NGFW смотрит на сеть несколько шире и не может защитить от всех угроз на седьмом уровне по классификации OSI. Большая часть трафика, с которым мы сейчас работаем, — это HTTP, и WAF учитывает особенности приложения, анализируя его».

Во-вторых, **Анастасия Афонина,** операционный директор компании «Вебмониторэкс», предостерегает от самонадеянности: «Если заказчик считает, что его ранее не взламывали, то, возможно, он просто не знает об этом. В нашей практике после начала использования WAF, в том числе со сканированием, с уязвимостями, с обнаружениями, многие понимали, что в прошлом их уже взламывали». Б.О