Защита большого веба:

вызовы, тренды, отечественная специфика

ptsecurity.com

Исследования Positive Technologies показывают, что в 9 из 10 веб-приложений преступники могут проводить атаки на пользователей. В том числе — перенаправлять клиентов на подконтрольный им ресурс, похищать учетные данные с помощью фишинговых атак, заражать компьютер вредоносным ПО. При этом несанкционированный доступ к приложению возможен на 39% сайтов. В 2019 году полный контроль над системой был получен в 16% веб-приложений, при этом в 8% систем полный контроль над сервером веб-приложения позволял проводить атаки на локальную сеть организации. Угроза утечки важных данных присутствует в 68% веб-приложений. Среди «утекших» данных на первом месте персональные (47% утечек), а на втором — учетные (31%). Все это обуславливает актуальность вопросов кибербезопасности веб-приложений и использования для этого автоматизированных средств защиты.

В продуктовой линейке Positive Technologies с 2013 года представлен гибкий инструмент всесторонней защиты от веб-атак — PT Application Firewall (PT AF), на долю которого приходится около половины отечественного рынка WAF.

Последние пару лет компания была сфокусирована на стабильности и производительности решения, поэтому сегодня PT Application Firewall — единственный WAF, который может работать «в разрыв» в высоконагруженных публичных сервисах с SLA 99,999 и с полным сохранением своих характеристик с точки зрения защиты.

WAF и PT AF в России: детали, цифры, прогнозы

Спикер:

Максим Филиппов,
директор
по развитию
бизнеса компании
Positive Technologies
в России

Начало WAF в России

Появление PT Application Firewall стало ответом на проблему, которую red team Positive Technologies выявляла в каждом своем проекте из года в год: использование уязвимостей в веб-приложениях неизменно оставалось в топе векторов атак, позволяющих потенциальному злоумышленнику быстро проникнуть во внутреннюю сеть компании. Например, результаты пентестов в 2012 году[1] показали, что эта проблема была актуальна в каждом третьем случае. То есть проблема защищенности веба стояла достаточно остро при том, что общий подход к защите на тот момент был по своей сути реактивным: предлагалось искать уязвимости и патчить, снова искать и снова патчить.

Positive Technologies в то время предложила новый проактивный подход, основанный на анализе аномалий и позволяющий в числе прочего оперативно выявлять даже уязвимости нулевого дня. Наукоемкая разработка прошла испытания в боевом режиме на инфраструктурах ряда крупных компаний отечественного рынка, и к 2013 году PT Application Firewall появился в линейке продуктов Positive Technologies. По мере его распространения подтверждалась эффективность избранного нами подхода: продукт позволял реагировать на выявленные уязвимости прямо из коробки, не требуя каких-либо сложных изменений.

Именно в тот период на рынок WAF обратили внимание ведущие аналитики (Gartner, Forrester), которые транслировали рынку видение необходимой функциональности продуктов такого типа, формировали конкурентное поле. Positive Technologies оказалась тогда в числе немногочисленных визионеров[2], признанных международными аналитиками, что в целом и определило будущее PT AF на рынке.

Оценка рынка WAF и места PT Application Firewall

По оценкам Positive Technologies, российский рынок WAF на конец 2019 года превысил 1 млрд. рублей, при этом за последние пять лет этот рынок вырос в пять раз[3]. Это обусловлено, с одной стороны, большей цифровизацией бизнес-процессов компаний, а с другой — повышением зрелости организаций с точки зрения информационной безопасности: решения класса WAF входят в топ-3 ключевых технологий, используемых для защиты современными крупными предприятиями и компаниями среднего и малого бизнеса. На долю PT Application Firewall по итогам 2019 года приходится 50% объема рынка WAF в России. В общем финансовом результате компании PT AF занимает около 10%, при этом число продаж лицензий продукта увеличилось в два раза по сравнению с 2018 годом, а общее число клиентов, использующих PT AF, за последние два года достигло 250.

1 По данным Positive Technologies 2013 года, каждая третья атака могла быть успешно организована именно из-за использования уязвимостей веба; в 2014 уже в 60% случаев вектор потенциальной атаки основывался на уязвимостях веба; в 2015 эта цифра составила 47%, а в 2016 поднялась до 77%; в 2017 – снова оказалась на уровне примерно трети и по итогам 2018 года 75% всех потенциальных векторов проникновения были связаны именно с недостатками защиты веб-ресурсов.

2 Аналитики Gartner ранее присваивали Positive Technologies статус визионера в магическом квадранте по защите веб-приложений с 2015 по 2017 годы.

3 Собственная оценка аналитиков Positive Technologies, основанная на публичных и не публичных данных по инсталляциям продуктов класса WAF на рынке России и стран СНГ.

Кому с WAF жить хорошо

В топ отраслей, где решение наиболее востребовано, входят государственные структуры (около 50% всех внедрений PT AF), кредитно-финансовые организации (20%) и компании телекоммуникационной отрасли (15%). Это объясняется тем, что особый интерес для злоумышленников представляет большой веб — высоконагруженные проекты федерального масштаба, которые содержат персональные и платежные данные миллионов граждан. К таким проектам относятся порталы государственных услуг, банковские и финансовые сервисы, социальные сети, а также онлайн-магазины, крупные агрегаторы, онлайн-кинотеатры.

В 20% всех зафиксированных нами случаев в 2019 году злоумышленники атаковали веб-ресурсы организаций, при этом в основном они преследовали две цели — получение данных и финансовую выгоду (до 90% всех атак в 2019 году).

SME тоже использует WAF

PT Application Firewall — одна из наиболее востребованных технологий Positive Technologies в сегменте SME[4]: на долю PT AF приходится до 21% всех конечных продаж продуктов Positive Technologies в компаниях среднего и малого бизнеса в России и странах СНГ. Для этого типа организаций использование веб-технологий и их защита весьма актуальны. PT AF является в линейке Positive Technologies одним из наиболее подготовленных для использования SME как с точки зрения ценообразования, так и с точки зрения удобства и простоты его внедрения и использования.

Результаты опроса[5], проведенного Positive Technologies в конце 2019 года, показывают, что 37% респондентов из SME-компаний упоминают средства защиты класса web application firewall в числе обязательно используемых.

Что изменится на рынке WAF и почему

Общие показатели рынка WAF ближайшие год-два останутся на прежнем уровне. Однако тренды в ИТ и ИБ повлияют на его развитие: появляются новые требования по повышению защищенности онлайн-сервисов, необходимых для ведения бизнеса в распределенном и удаленном режиме.

Отдельного внимания заслуживает необходимость динамичного изменения самих веб-приложений, нуждающихся в защите: высокотехнологичные компании, оказывающие львиную долю своих сервисов через веб-приложения, ускоряют запуски обновлений до нескольких раз в сутки, максимально сокращая time-to-market и предъявляя соответствующие требования по высокой адаптивности к их защите. Все это может простимулировать рынок WAF. Поэтому среди прочих технологий в сфере кибербезопасности именно рынок WAF сегодня имеет больше возможностей для роста.

На горизонте одного-двух лет Positive Technologies прогнозирует занять 60—70% рынка WAF в регионе. В том числе за счет наращивания числа крупных инсталляций: сейчас на долю внедрений в области большого веба (высоконагруженных проектов, в том числе федерального масштаба) приходится 6% внедрений продукта ежегодно. В денежном эквиваленте это почти 40% от общего оборота по продукту в год. Возможности обновленной версии продукта позволяют ожидать прироста в этом секторе (даже в тех проектах, где по требованиям ранее подходили только зарубежные аналоги WAF).

4 Компании, численностью до 500 сотрудников (SME, small and medium-sized enterprises).

5 Опрос проводился среди посетителей сайта компании Positive Technologies, аудитории интернет-портала SecurityLab.ru и участников ряда отраслевых сообществ, совокупная аудитория которых более 16 000 ИТ- и ИБ-экспертов из различных сфер отечественного бизнеса.

Атаки на веб: топ наиболее атакуемых отраслей и типовой портрет атакующего

Спикер:
Алексей Новиков,
директор экспертного центра безопасности Positive Technologies (PT Expert Security Center)

Веб-ресурсы как объект атаки

Динамика атак на веб-ресурсы за последние три года демонстрирует завидную стабильность: атаки на веб три года подряд входят в топ-2 наиболее атакуемых объекта (в 2019 на их долю пришлось 20% всех зафиксированных атак, в 2018 и 2017 — по 26% соответственно). При этом топ-5 отраслей, веб-приложения которых атакуются злоумышленниками наиболее активно в последние три года, входят:

- государственные учреждения (первое место по частоте атак);
- компании кредитно-финансовой отрасли, ритейла, сферы образования и науки, ИТ и медицинские организации — за последние три года показывали различные позиции, но за границы топ-5 не выходили;
- отдельное место занимают атаки на онлайн-сервисы вне привязки к отрасли.

Таким образом злоумышленники демонстрируют вполне устойчивый интерес к атакам именно на веб-приложения. Это не удивительно, так как исследования в области защищенности веб-приложений также демонстрируют далеко не утешительные результаты. За последние пять лет результаты работ по тестированию на проникновение в организациях России и стран СНГ показывают, что векторы атак, основанные на реализации уязвимостей веб-приложений, входят в топ наиболее реализуемых и составляют от 28% до 75% успешных случаев[6].

Анализируя данные за последние пять лет, мы видим снижение доли сайтов, содержащих критически опасные веб-уязвимости, однако речь не идет о снижении числа уязвимостей до нуля: среднее число критически опасных уязвимостей на одно приложение — 4,1, среднего уровня риска — 12,3, а низкого уровня — 5,7[7]. При этом для атаки злоумышленнику часто достаточно воспользоваться одной такой уязвимостью.

Типовой портрет злоумышленника, атакующего через веб

По итогам 2019 года в целом в пятой части атак на юридические лица злоумышленники в качестве объекта атаки избирали именно веб-ресурсы. Кто такой злоумышленник, атакующий веб, и какова его мотивация?

- **Различные автоматизированные бот-сети.** Их операторы в первую очередь нацелены на получение контроля над максимальным числом зараженных узлов. Поэтому для них играет роль максимальная автоматизация всех этапов атаки — от получения первоначального доступа до загрузки полезной нагрузки и дальнейшей эксплуатации зараженных узлов. Характерным примером может быть в данном случае история Neutrino. После получения доступа к большому количеству узлов операторы этой бот-сети монетизируют их по-разному: майнинг криптовалюты, продажа взломанных узлов, организация DDoS-атак, заражение пользователей (посетителей сайтов) и перенаправление трафика.

6 Результаты пентестов за 2014, 2015, 2016, 2017 и 2018 годы показали, что векторы атаки, основанные на эксплуатации уязвимостей веб-приложений, актуальны для 60%, 47%, 77%, 28% и 75% случаев соответственно.

7 Результаты оценки уязвимости и угроз веб-приложений в 2019 году, Positive Technologies.

В число наиболее вероятных жертв таких атак входят те, кто использует распространенные CMS, в которых периодически находят уязвимости (в том числе пользователи Joomla, WordPress и плагинов и расширений для них). Наша статистика показывает, что в среднем уже через два дня злоумышленники активно начинают эксплуатировать уязвимости после их публичного анонса. Владельцам уязвимых сервисов при этом в подавляющем большинстве случаев двух дней для тестирования и установки обновлений не хватает. Решить проблему можно с помощью систем защиты (в частности, WAF) обладающих функциями выявления известных уязвимостей в распространенных сервисах и системах.

- **Финансово ориентированные злоумышленники.** Развитие e-commerce идет семимильными шагами, а нынешняя ситуация, заставившая многих перевести свой бизнес в онлайн, не может остаться незамеченной злоумышленниками.

  На долю финансово мотивированных атак приходится не менее трети их общего числа ежеквартально. А в общей массе атак, нацеленных на получение каких-либо данных, не менее 34% приходится на персональные данные, 19% — на данные платежных карт, и еще 15% атак совершаются ради доступа к учетным данным.

  Это говорит о том, что возможными становятся последующий доступ к платежным сервисам пользователей, атаки на различные системы лояльности. И в данном случае необходимы функции средства защиты, связанные с анализом действий пользователя и выявлением поведенческих аномалий или признаков бота (в том числе с использованием технологий машинного обучения).

- **Атаки APT-группировок на веб-приложения.** Атака на веб-ресурс может быть использована при организации таргетированной атаки на четко определенную группу пользователей. Речь идет о классических атаках типа watering hole, основанных на том, что злоумышленники изучают интересы атакуемой группы: например, то, какие сайты эта группа посещает чаще всего, и заражают один или несколько из них вредоносным ПО. Такой подход является успешным, так как обеспечивает широкий охват нужной аудитории при ограниченном числе точек заражения.

  Так, в 2019 году группировка Turla компрометировала ряд сайтов государственных организаций Республики Армения. Иногда компрометируют сайты СМИ и даже сайты популярных сервисов, которые могут быть востребованы в той или иной среде пользователей.

  Атаки такого типа используются и финансово ориентированными группировками. Такая атака может послужить одним из первых звеньев многоступенчатой целевой атаки на конкретную организацию. К примеру, в марте этого года был опубликован отчет об атаках группировки APT41, которая в рамках вредоносной кампании использовала три разные уязвимости в веб-приложениях различных устройств, в том числе уязвимость в Citrix. Следует учитывать, что атакованы могут быть не только веб-приложения и сайты организации, но и веб-интерфейсы панелей администрирования различных устройств. А это означает, что они также требуют защиты специализированных решений класса WAF.

PT Application Firewall 4.0: работа «в разрыв», deep machine learning и пять девяток

Спикер:
Виктор Рыжков
менеджер по продуктовому маркетингу направления Application Security, Positive Technologies

PT Application Firewall появился в линейке Positive Technologies в 2013 году и сразу же был успешно использован во время XXVII Всемирной летней универсиады в Казани. Сегодня 250 наших клиентов из разных отраслей используют PT AF: порядка 50% из них — это компании государственного сектора, 20% — кредитно-финансовые организации, 15% — компании телекоммуникационной отрасли.

Доступность, время отклика, защищенность

Высоконагруженные приложения федерального масштаба обрабатывают десятки, сотни тысяч запросов в секунду. Они взаимодействуют не только с пользователями, но и другими приложениями посредством API, а также работают с трафиком автоматизированных ботов. Если исходное приложение не обеспечивает должное время отклика или вовсе не обеспечивает доступность, то страдают от этого как пользователи, так и сотни других приложений. Поэтому требования к доступности веб-приложения высоки: до пяти девяток — то есть 99,999% времени. Это не более 5,5 минут простоя в год.

Чтобы обеспечить такие высокие показатели, необходимо не только правильно написать веб-приложение, но и защитить его от атак, и здесь никак не обойтись без WAF, причем именно в активном режиме — «в разрыв». При этом включая WAF в активном режиме, нужно понимать, что на него переносятся те же требования доступности (те же пять девяток) и времени отклика (WAF не должен вносить ощутимую задержку при обработке трафика).

Масштабирование и распределенная установка

Новая версия PT AF обладает широкими возможностями по масштабированию и распределенной установке благодаря микросервисной архитектуре продукта и разделению ее на публичную часть (public) и ядро (core). Например, можно установить core поближе к оператору WAF, а в части public в любом количестве разнести инфраструктуру (установить в тот же или соседний ЦОД, в удаленные филиалы или даже облако), при этом собирая информацию со всех в едином окне. При этом важно отметить два момента: каждая часть public анализирует трафик и блокирует угрозы, а также настраивается и масштабируется независимо от других частей и от core.

WAF, работающий «в разрыв»

В расшифровке аббревиатуры WAF изначально содержится слово «Firewall» — дословно это значит «ставить в разрыв». Только так сегодня можно обеспечить бесперебойную работу веб-приложений на установленных показателях: вплоть до 99.999%.

PT Application Firewall 4.0 способен противостоять современным известным и неизвестным угрозам и при этом поддерживать соблюдение требований доступности каждого приложения для его внешних клиентов (вплоть до 99,999% времени). Это стало возможным благодаря новой микросервисной архитектуре продукта: теперь мы можем разносить компоненты системы по разным сегментам, масштабировать каждый из них под любую нагрузку и настраивать независимо друг от друга. То есть PT Application Firewall 4.0 — это не одна высоконагруженная точка агрегации трафика приложений, а гибкая отказоустойчивая система, части которой могут быть разбросаны по инфраструктуре и распределять нагрузку между собой.

Deep machine learning

В PT Application Firewall 4.0 встроена технология глубокого машинного обучения (deep learning, DL) для анализа HTTP-запросов и ответов. Основное отличие глубокого DL от традиционного (machine learning, ML) является то, что в случае с DL пользователю не требуется выбирать значения наиболее важных параметров при анализе выборки. Это означает, что DL работает без глубоких настроек человеком, которых требуют традиционные методы машинного обучения, и более пригоден для работы с большим количеством приложений.

Ответственность за уровень защиты приложения и API

Защита API действительно становится все более актуальной темой для WAF. И дело здесь не только в экосистемах (это лишь частный случай). Приложения все больше взаимодействуют друг с другом и обмениваются данными посредством API. Например, сегодня уже тяжело представить сайт, который предлагает нам единственный способ регистрации через явное указание своих данных, а не предоставляет возможность войти с помощью других сервисов.

Второй важный тренд, если говорить не о пользовательском трафике, — это боты. Сегодня уже 40% трафика генерируется ботами. Да, среди них есть полезные и безвредные: например, поисковые роботы, индексирующие веб-страницы в поисковой выдаче. Однако половина среди этих 40% — зловредные. Потому точное определение и классификация ботов (зловредные или безопасные) — это сложная и большая задача, которая ставится перед WAF.

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays