ИНТЕРНЕТ-СЕРВИСЫ «СВЯЗНОГО» ЗАЩИЩАЮТСЯ ОТ КИБЕРАТАК С ПОМОЩЬЮ PT APPLICATION FIREWALL

«Web application firewall — один из необходимых компонентов защиты онлайн-сервисов. Мы протестировали различные решения, как отечественные, так и импортные. Продукт компании Positive Technologies отвечает всем предъявленным нами требованиям. С помощью PT Application Firewall были выявлены атаки, которые не обнаруживались другими имеющимися средствами. Кроме того, мы знакомы с профессиональной командой Positive Technologies, следим за прогрессом этой компании, и это дает нам уверенность, что PT Application Firewall будет достойно развиваться».

Игорь Усачев
заместитель начальника
управления контроля информационных рисков
ГК «Связной»

ПРОФИЛЬ ОРГАНИЗАЦИИ

- **Отрасль:** розничная торговля
- **Название:** «Связной»
- **География:** около 3000 магазинов в 900 городах РФ
- **Сервисы:** интернет-магазин Svyaznoy.ru, «Связной Трэвел», «Дом.Связной», «Связной Страхование», «Связной Сервис», «Связной Клуб», «Связной Работа», «Связной Бизнес», «Связной Поддержка»
- **Решение:** защита онлайн-сервисов
- **Продукт:** PT Application Firewall

ЗАДАЧА

Компания «Связной» — крупнейший в России мультиканальный ритейлер федерального масштаба и лидер по продажам смартфонов в стране. Интернет-магазин Svyaznoy.ru с оборотом 22 млрд рублей посещают около 15 млн человек в месяц. Кроме продажи гаджетов, компания активно развивает свою экосистему интернет-сервисов, включая сайты для поддержки клиентов ритейлера, выбора интернет-провайдера, оформления кредитов и страховок, покупки авиабилетов и др.

Распределенность множества офисов и магазинов требует активного использования интернет-сервисов для автоматизации торговли и управления складом, взаимодействия с поставщиками и партнерами. Однако все это существенно расширяет спектр угроз. За последний год ИБ-эксперты отмечают рост атак на торговые сети: злоумышленники активно блокируют интернет-магазины, сервисы компаний, похищают персональные и платежные данные покупателей. Участились так называемые атаки low and slow — многоступенчатые, медленные атаки малого объема. Также, по данным Positive Technologies, выросло количество целенаправленных атак. При этом в большинстве случаев злоумышленник использует уязвимости веб-приложений.

Популярность сервисов «Связного» делает их лакомой мишенью для атак злоумышленников. Дополнительным фактором риска является жесткая конкурентная борьба в данном секторе рынка. К примеру, DDoS атаки — это популярный сценарий для шантажа и недобросовестной конкуренции, который представляет собой серьезную угрозу для бизнеса.

Все это формирует достаточно серьезные требования к защите веб-приложений «Связного»:

- Защита от известных и новых (0-day) атак на веб-приложения.
- Защита от фрода и целенаправленных атак, целью которых является похищение денежных средств и пользовательских данных.
- Оперативное блокирование ботов, атак «тяжелыми» запросами и других атак, направленных на доступность интернет-сервисов (DDoS) на уровне приложения.
- Высокая производительность и отказоустойчивость: защитная система должна работать в отказоустойчивом режиме с большим объемом трафика и при этом не оказывать влияния на скорость и доступность работы приложений.
- Масштабируемость: в экосистеме сайтов «Связного» постоянно появляются новые ресурсы, которые должны быть обеспечены защитой быстро и легко, без лишних затрат на внедрение и настройку дополнительных средств безопасности.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ:

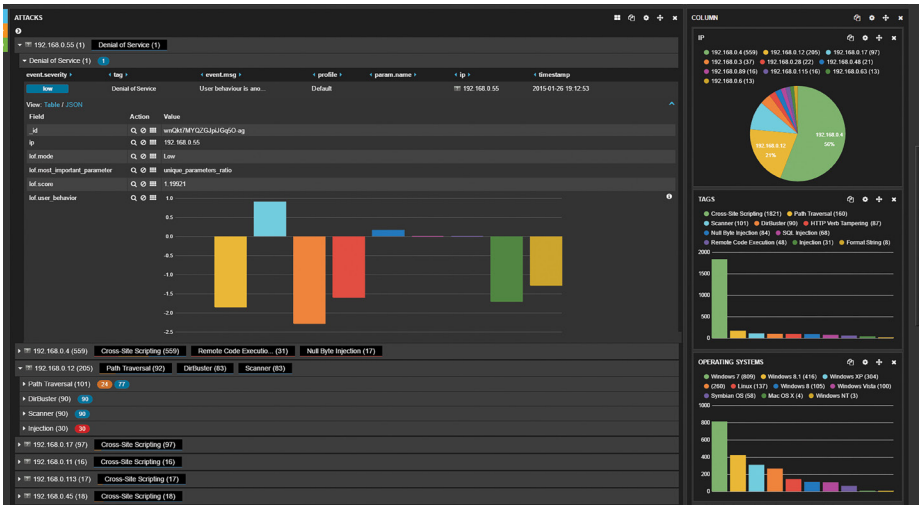
- быстрое самообучение,
- высокая производительность,
- минимальный уровень ложных срабатываний,
- автоматическая блокировка атак нулевого дня,
- блокировка атак на пользователей приложения,
- защита от программ-роботов,
- корреляция событий и построение цепочек атак,
- автоматическая верификация уязвимостей (DAST),
- широкие интеграционные возможности (SIEM и др.),
- обратная связь для исправления уязвимостей

PT APPLICATION FIREWALL:

- единственный продукт класса web application firewalls, сертифицированный ФСТЭК России (сертификат № 3455 от 27.10.2015);
- сертифицирован Министерством обороны (сертификат № 2619 от 21.07.2014);
- внесен в единый реестр российских программ для ЭВМ и баз данных (приказ Минкомсвязи России от 14.06.2016 № 260);
- отмечен аналитическим агентством Gartner. В 2016 году Positive Technologies стала единственным визионером рейтинга Magic Quadrant for Web Application

РЕШЕНИЕ

В ходе поиска решения для защиты главного портала интернет-магазина Svyaznoy.ru, а также ряда других веб-сервисов компании специалисты «Связного» остановились на системе защиты веб-приложений Positive Technologies Application Firewall. Основным критерием выбора стало наличие уникальных механизмов корреляционного и поведенческого анализа, которые позволяют блокировать атаки нулевого дня, а также защищать от фрода, подбора паролей, вовлечения в ботнеты, DDoS-атак и утечек данных. Немаловажным фактором выбора стали также быстрое развертывание решения и удобная настройка защитных механизмов.



РЕЗУЛЬТАТ

Специалистам «Связного» и Positive Technologies удалось выявить более тысячи попыток атак, в том числе с использованием уязвимостей Shellshock, SQL Injection и XSS, а также попытки подбора паролей, загрузки вредоносного кода и использования различных сканеров для поиска уязвимостей в веб-приложениях.

Использование PT Application Firewall помогло существенно снизить риски, связанные с успешной реализацией атак, таких как:

- нарушение доступности сайтов;
- получение несанкционированного доступа во внутренние информационные системы компании, а также полного контроля над приложением и его исходным кодом;
- кража базы данных клиентов, включая номера телефонов, адреса электронной почты, адреса доставки товара и платежные данные;
- получение доступа к конфиденциальной информации компании (счета, договоры, отчеты, закупочные цены, информация о складах, персональные данные сотрудников и т. д.);
- атаки на пользователей приложения с целью похищения их учетных данных;
- мошенничество с бонусными баллами, скидочными картами;
- замена содержимого сайта и размещение порочащей информации.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

POSITIVE TECHNOLOGIES

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