История успеха
Кредит Европа Банк

«Кредит Европа Банк» доверил PT Application Firewall защиту своих веб-ресурсов от кибератак

О компании

АО «Кредит Европа Банк (Россия)» — российский Банк с иностранным капиталом, основанный в 1997 году, принадлежит к международной финансовой Группе FIBA, осуществляющей свою деятельность в 12 странах мира. Филиальная сеть Кредит Европа Банка насчитывает 49 отделений в 22 городах и 5 часовых поясах РФ, а также 508 банкоматов и более 26 000 точек продаж (присутствие банка в 2019 году), расположенных в 77 городах России. На сегодняшний день Банк обслуживает более 6 000 000 клиентов физических лиц, 5 600 корпоративных клиентов и 15 500 предприятий малого и среднего бизнеса (на 31.12.2019).

Задача

«Кредит Европа Банк» оказывает услуги розничным и корпоративным клиентам, а также предприятиям малого и среднего бизнеса. Для реализации услуг банк использует несколько десятков веб-ресурсов, в числе которых официальный сайт, интернет- и мобильные банки для физических и юридических лиц, промостраницы и другие веб-приложения. Связанные с ними риски подразумевают повышенные требования по информационной безопасности.

Взлом веб-приложений — один из наиболее часто используемых методов проведения кибератак на организации и частных лиц. Самые приоритетные цели для злоумышленников — веб-ресурсы финансовых организаций. Чаще всего взлому подвергаются банковские сервисы, с помощью которых пользователи могут оплачивать услуги, открывать вклады и делать переводы. Как показывают исследования Positive Technologies, среди киберпреступников больше всего распространены простые и эффективные атаки — внедрение SQL-кода (SQL Injection), выход за пределы каталога (Path Traversal) и межсайтовое выполнение сценариев (Cross-Site Scripting). Для отражения подобных угроз необходима всесторонняя и непрерывная защита приложений.

АО «Кредит Европа Банк (Россия)» — российский Банк с иностранным капиталом, основанный в 1997 году, принадлежит к международной финансовой Группе FIBA, осуществляющей свою деятельность в 12 странах мира

Александр Сагалаков

Начальник группы безопасности информационных систем АО «Кредит Европа Банк (Россия)»

Кредит ЕвропаБанк

«Мы рассматривали WAF-ы разных производителей, но остановили свой выбор на межсетевом экране уровня приложений PT Application Firewall от Positive Technologies. Специалисты компании ежегодно исследуют безопасность финансовых организаций, а также уязвимости и угрозы мобильных банков, а значит, как никто другой понимают, как киберпреступники атакуют банковскую отрасль. Кроме того, решение неплохо зарекомендовало себя в защите ресурсов других российских банков»

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ PT APPLICATION FIREWALL

Комплексный подход в борьбе с современными веб-вызовами:

- автоматическая блокировка атак нулевого дня,
- выделение трафика уровня приложений из общего сетевого трафика и его анализ,
- интеллектуальный анализ в сочетании с сигнатурными методами,
- защита на стороне клиента,
- защита от DDoS-атак на уровне приложения,
- антивирусная защита на лету,
- встроенный сканер уязвимостей и виртуальный патчинг,
- возможная интеграция с различными классами решений: NGFW, IDS, IPS, DLP, SIEM, анти-DDoS, антивирусы. NGFW, IDS, IPS, DLP, SIEM, анти-DDoS, антивирусы.

«Кредит Европа Банк» решил усилить защиту от потенциальных атак на свои веб-приложения и внедрить межсетевой экран уровня приложения (web application firewall, WAF). Отдел информационной безопасности банка сформировал требования к WAF:

- Межсетевой экран должен выявлять любые виды атак, направленные на получение доступа к информации, содержащей карточные данные клиентов, к платежной информации клиентов и к серверам веб-ресурсов с последующей компрометацией сети банка.
- Обеспечивать противодействие не только известным атакам на уровне приложения и бизнес-логики, но и выявлять эксплуатацию уязвимостей нулевого дня, анализировать и сопоставлять множество событий для выявления цепочек атак.
- Учитывать специфику атак на ресурсы финансовой отрасли.
- Иметь удобный интерфейс и возможность гибкой настройки, а также хорошую техническую поддержку.

Решение

PT Application Firewall предназначен для выявления и блокирования современных атак на веб-порталы, ERP-системы, мобильные приложения, системы дистанционного банковского обслуживания. Благодаря комбинации инновационных технологий и уникальных механизмов PT Application Firewall обеспечивает непрерывную проактивную защиту веб-приложений от большинства атак, включая OWASP Top 10, автоматизированные атаки, атаки на стороне клиента и атаки нулевого дня. PT Application Firewall поддерживает различные режимы и схемы работы, а также может быть реализован в отказоустойчивой конфигурации с балансировкой нагрузки.

Проект по внедрению проводился совместно со специалистами «ДиалогНаука». Для оценки возможностей PT Application Firewall было организовано пилотное тестирование, которое проходило в 2019 году. В качестве объекта защиты был выбран один из рекламных сайтов банка. PT Application Firewall успешно прошел тестирование, поэтому следующим этапом стало полноценное внедрение межсетевого экрана уровня приложений в инфраструктуру.

Андрей Шконда

Старший специалист группы безопасности информационных систем АО «Кредит Европа Банк (Россия)»

Кредит ЕвропаБанк

«PT Application Firewall уже на пилотном проекте показал себя как надежное решение, соответствующее всем заявленным нами требованиям. В последующей работе мы увидели и другие положительные характеристики. PT Application Firewall быстро и бесшовно интегрировался в инфраструктуру банка. В продукте есть возможность гибкой настройки правил защиты веб-приложений и событий, а также удобный и функциональный интерфейс дашборда администратора. Также отметим отличную работу технической поддержки, которая помогает создавать индивидуальные правила для уникальных случаев»

Благодаря разнообразию защитных механизмов, поддержке различных режимов работы и схем реализации PT Application Firewall гибко встроился в инфраструктуру банка, не нарушая существующих бизнес-процессов, и обеспечивает непрерывную работу всех приложений.

PT Application Firewall был развернут в режиме обратного прокси-сервера, когда межсетевой экран блокирует аномальные запросы, направленные на веб-приложения.

Результаты

Под защиту PT Application Firewall были переведены несколько десятков веб-ресурсов «Кредит Европа Банка», включая официальный сайт www.crediteurope.ru, интернет- и мобильные банки для физических и юридических лиц, различные лендинговые страницы и другие информационные ресурсы.

PT Application Firewall удалось выявить и заблокировать такие попытки атак, как сбор информации о внутренней конфигурации веб-ресурса, SQL Injection (внедрение SQL-кода), XSS (межсайтовое выполнение сценариев), Signature Forgery (подделка подписи), а также попытки подбора паролей и использования различных сканеров для поиска уязвимостей в веб-приложениях. В среднем за месяц WAF выявляет около 8500 событий безопасности высокой степени риска (по собственной шкале PT AF), около 3000 — средней и 10000 низкой степени риска.

В дальнейших планах последовательное подключение к WAF всех остальных приложений банка.