История успеха
Абсолют Банк

«Абсолют Банк» усилил защиту веб-приложений от кибератак с помощью PT Application Firewall

АКБ «Абсолют Банк» — крупный федеральный банк с фокусом на высокотехнологичное развитие в приоритетных направлениях бизнеса. Банк специализируется на работе в сегментах с высоким уровнем экспертизы и уникальными IT-решениями: ипотеке, автокредитовании, а также МСБ в цифровом формате, на системном обслуживании компаний холдинга ОАО «РЖД», на комплексных решениях в private banking.

Задача

Как показали исследования Positive Technologies, кредитно-финансовые организации входят в тройку наиболее атакуемых. Чаще всего взлому подвергаются банковские сервисы, с помощью которых пользователи могут оплачивать услуги, открывать вклады и делать переводы. Самые распространенные атаки на веб-приложения финансовых организаций — атаки на клиентов, в частности «Межсайтовое выполнение сценариев» (Cross-Site Scripting), с целью кражи персональных и платежных данных. Кроме того, участились случаи заражения сайта вредоносным ПО: такой способ позволяет киберпреступникам охватить большее число жертв.

Принимая во внимание возможные риски, связанные с киберугрозами, Служба ИБ «Абсолют Банка» решила усилить систему защиты от потенциальных атак на веб-приложения банка. Основным этапом этого процесса стало внедрение межсетевого экрана уровня приложений (web application firewall).

Были сформированы требования к решению. Межсетевой экран должен выполнять следующие функции:

- противодействовать известным атакам на уровне приложения и бизнес-логики,
- выявлять эксплуатацию уязвимостей нулевого дня,
- предотвращать атаки на пользователей,
- анализировать и сопоставлять множество событий для выявления цепочек атак,
- взаимодействовать с внешними системами сбора и анализа событий (SIEM) и оповещать средства защиты от DDoS сетевого уровня,
- вычислять IP-адрес атакующего из запроса,
- обеспечить непрерывную работу приложения.

Для решения поставленной задачи «Абсолют Банк» остановился на межсетевом экране уровня приложений PT Application Firewall. Продукт 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.

АКБ «Абсолют Банк» — крупный федеральный банк с фокусом на высокотехнологичное развитие в приоритетных направлениях бизнеса

Булгаков
Алексей Алексеевич
Руководитель
Службы ИБ

«Ресурсы финансовых организаций всегда в фокусе у злоумышленников. Для нас крайне важны сохранность данных и доступность наших приложений для клиентов, поэтому мы уделяем особое внимание защите клиентских веб-ресурсов от кибератак. Благодаря межсетевому экрану PT Application Firewall мы можем контролировать безопасность веб-приложений "Абсолют Банка" и оперативно реагировать на актуальные угрозы. PT Application Firewall подтвердил заявленные характеристики и зарекомендовал себя как надежное, производительное и функциональное решение».

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

Решение

Для оценки возможностей PT Application Firewall было организовано пилотное тестирование, которое проходило с августа 2018 года по январь 2019 года.

На основе заданных управлением защиты информации «Абсолют Банка» критериев для реализации системы защиты была сформирована программа испытаний PT Application Firewall. В рамках тестирования специалисты Positive Technologies провели обучение по работе с PT Application Firewall для ИБ-сотрудников банка. Также была проверена производительность решения с учетом специфики инфраструктуры банка.

На время тестирования PT Application Firewall был развернут в режиме Sniffer: система анализировала копию веб-трафика, поступающего на защищаемый сервер. Это было нужно для того, чтобы минимизировать влияние на работу защищаемых веб-серверов.

Результаты

По итогам пилотного проекта был проведен анализ актуальности выявленных угроз для защищаемых ресурсов. PT Application Firewall успешно прошел тестирование и показал высокую точность по обнаружению атак на веб-приложения «Абсолют Банка». За время тестирования PT Application Firewall обнаружил более 10 000 атак. До 10% из них — высокого уровня опасности, около 40% — среднего уровня и около 50% — низкого.

Следующим этапом стало внедрение PT Application Firewall. Решение было развернуто в режиме обратного прокси-сервера, когда межсетевой экран блокирует аномальные запросы, направленные на веб-приложения. Благодаря разнообразию защитных механизмов, поддержке различных режимов работы и схем реализации, решение PT Application Firewall гибко встраивается в инфраструктуру банка, не нарушая существующие бизнес-процессы, и обеспечивает непрерывную работу всех приложений.

Служба ИБ «Абсолют Банка» использует PT Application Firewall для непрерывной защиты веб-приложений от атак злоумышленников, направленных на снижение доступности веб-приложений, а также нарушение целостности и доступности обрабатываемой в них информации.

Также PT Application Firewall позволил обеспечить управление SSL-сертификатами и наборами шифров в едином центре управления защитой HTTPS-соединений. Это дало возможность эффективно защищать самописные и сторонние сервисы, разработчики которых зачастую не имеют экспертизы в настройке SSL.

О компании

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

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. 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.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

PT_Absolut Bank_SS_A4.RUS.0001.02.DEC.10.2019