



Веб-ресурсы банка «Приморье» защищены от кибератак

« На сегодня мы обслуживаем значительную часть предприятий Дальнего Востока и Восточной Сибири, представляющих практически все отрасли экономики. Поэтому в условиях роста кибератак, как массовых, так и целевых, нам было необходимо обеспечить защиту ИТ-инфраструктуры и гарантировать клиентам бесперебойный доступ к их личным кабинетам и онлайн-услугам, а также сохранность персональных и платежных данных. Чтобы оперативно развернуть защиту веб-ресурсов и не допустить их деградации, мы решили выбрать именно сервисную модель ИБ »

Евгений Ласковый
Директор департамента информационных
банковских технологий АКБ «Приморье»

Профиль организации

АКБ «Приморье»
Один из крупнейших банков
Дальневосточного региона
<https://www.primbank.ru/>

Отрасль
финансовая сфера

Размер
офисы банка расположены
в Приморском и Хабаровском
краях, Магаданской, Сахалинской
и Иркутской областях, Москве
и Санкт-Петербурге

Параметры сервиса

Web Application Firewall (WAF)
Сервис защиты веб-приложений
<https://rt-solar.ru/services/waf/>

Тип
облачный сервис

Описание
эффективное противодействие атакам
на веб-приложения за счет эксплуатации
многоступенчатых модулей защиты,
включающих анализ трафика
и блокировку атак



Обеспечить клиентам бесперебойный доступ к личным кабинетам и онлайн-услугам и минимизировать риски утечки конфиденциальной информации

Задача

- Оперативно вывести веб-приложение из-под атаки хакеров.
- Обеспечить защиту всех веб-ресурсов, включая основной сайт банка и личный кабинет клиента.
- Выявить трафик, эксплуатирующий уязвимости в веб-приложениях.
- Предупредить несанкционированные изменения внешнего вида веб-приложений.

Решение

- Использовать тестовый контур дистанционного банковского обслуживания для сбора статистики по атакам.
- Кастомизировать правила и политики безопасности для каждого защищаемого ресурса.
- Подключить в кратчайшие сроки к сервису защиты веб-приложений все интернет-ресурсы банка.
- Сформировать отчет о зафиксированных событиях по всем ресурсам.

Результат

Интернет-ресурсы банка оперативно подключены к сервису защиты веб-приложений и выведены из-под удара хакеров. Активные атаки нейтрализованы.

В кратчайшие сроки выполнена необходимая настройка профилей и политик.

Сервис защищает 5 интернет-ресурсов банка, включая личный кабинет клиента, от атак уровня L7 (DDoS-атаки и атаки из списка OWASP Top 10).

В III квартале 2022 года зафиксировано и нейтрализовано более 1,7 млн событий ИБ.

Обеспечена доступность онлайн-ресурсов банка для клиентов, а также сохранность персональных и платежных данных.



Оптимизировать трудозатраты специалистов ИБ-службы банка

Задача

- Подобрать оптимальное решение для защиты онлайн-ресурсов.
- Высвободить время ИБ-специалистов для решения операционных задач.

Решение

- Оперативно подключить защиту веб-приложений по сервисной модели без необходимости найма дополнительных специалистов.
- Отслеживать текущее состояние сервиса, информацию по атакам и формировать отчеты по событиям ИБ в любой момент времени.

Результат

Настройка и эксплуатация сервиса защиты веб-приложений осуществляется специалистами центра противодействия кибератакам Solar JSOC.

Всегда доступна помощь экспертов «Ростелеком-Солар», которые отвечают на запросы клиента согласно регламенту.

При использовании сервисной модели ИБ нет необходимости нанимать специалистов, как, например, в случае интеграции и эксплуатации аппаратного решения.