

Благодаря экспертизе «Платформикс» персональные данные клиентов банка надежно защищены

Анализ защищенности ИТ-инфраструктуры банка

Заказчик — крупный универсальный финансовый институт, предоставляющий широкий спектр услуг для физических и юридических лиц.

Предыстория проекта

Для финансовой организации жизненно необходимо поддерживать высокий уровень защищенности ИТ-инфраструктуры. Злоумышленники постоянно совершенствуют свои методы, создавая все новые киберугрозы, а утечка данных может грозить как репутационным, так и финансовым ущербом. В этих условиях жизненно важно заблаговременно выявлять потенциальные уязвимости.

Задача

Сознавая важность информационной защиты, заказчик привлек системного интегратора «Платформикс» для плановой проверки защищенности корпоративных информационных систем.

Перед командой интегратора была поставлена задача провести всестороннее тестирование ИТ-инфраструктуры банка, выявить максимальное количество потенциальных уязвимостей и помочь их устранить.

Ход проекта

Проект состоял из нескольких последовательных этапов, включая тестирование на проникновение внешнего и также внутреннего периметра инфраструктуры.

Пентест внешнего периметра инфраструктуры

На этом этапе была произведена разведка, сканирование и анализ сервисов, доступных извне. Для разведки использовались

сетевые сканеры для автоматизированного поиска уязвимостей, а также ручное тестирование с использованием Burp Suite и других утилит для анализа веб-приложений.

Заказчик получил полное описание уязвимостей и методов их устранения

В ходе пентеста были обнаружены несколько минорных багов, которые, хоть и не представляли критической угрозы, всё же требовали внимания, так как даже небольшие уязвимости потенциально способны стать частью более сложной атаки.

Пентест внутреннего периметра инфраструктуры

После сканирования специалисты «Платформикс» сосредоточились на поиске векторов атаки внутри сети. На этом этапе использовалась платформа Kali Linux и такие стандартные инструменты для работы с Active Directory, как BloodHound, утилиты Impacket и NetExec. ИБ-эксперты «Платформикс» также написали небольшой собственный скрипт для сетевых атак. Именно на этом этапе была найдена неочевидная и на первый взгляд незначительная уязвимость, которая впоследствии стала стартовой точкой для компрометации всего домена. Подобные уязвимости часто остаются незамеченными при поверхностных проверках.

В завершение была проведена проверка устранения уязвимостей —

команда проекта убедилась, что все найденные проблемы были успешно устранены, а инфраструктура стала устойчивее к потенциальным атакам.

Результат

Заказчик получил подробный отчет с описанием обнаруженных уязвимостей и возможных сценариев компрометации домена. Команда проекта также предоставила рекомендации по устранению обнаруженных проблем и вместе со специалистами заказчика провела проверку исправлений, чтобы убедиться, что все риски были успешно нивелированы.

В результате банк значительно улучшил уровень своей защищенности и теперь лучше подготовлен к отражению потенциальных атак.



Даже одна уязвимость может стать фатальной для всей системы. Именно поэтому регулярные пентесты и глубокая аналитика — это инструменты, которые помогают избежать серьезных потерь в будущем. В современных условиях пентест становится жизненной необходимостью и позволяет выявить уязвимости до того, как их обнаружат и используют злоумышленники.

Алексей Иванов,
руководитель направления,
«Платформикс»



Создаем, защищаем и развиваем корпоративные ИТ-инфраструктуры

«Платформикс» – эксперт в построении корпоративных ИТ-инфраструктур. Системный интегратор работает на рынке информационных технологий с 1992 года. Компания предоставляет заказчикам полный спектр услуг, связанных с инфраструктурной интеграцией на современном предприятии, ориентируясь на внедрение типовых решений.

Чтобы получить подробную информацию по решениям «Платформикс», пожалуйста, свяжитесь с нами по телефону или письмом

+7 (495) 967 80 50
+7 (800) 600 33 55

info@platformix.ru
platformix.ru