ИСТОРИЯ УСПЕХА

Приведение системы информационной безопасности ОАО Банк ЗЕНИТ в соответствие с требованиями стандарта PCI DSS

ОАО Банк ЗЕНИТ был учрежден в декабре 1994 года Академией народного хозяйства при Правительстве РФ, нефтяной компанией «Татнефть» и рядом других юридических лиц. Одним из важных направлений деятельности ОАО Банк ЗЕНИТ является комплексное обслуживание корпоративных клиентов. Банк также занимает сильные позиции на рынке инвестиционных услуг и частных инвестиций.

Как член Ассоциации Российских Банков, представленный в Совете Ассоциации, ОАО Банк ЗЕНИТ активно участвует в процессах, идущих в рамках российской банковской реформы.

ЗАДАЧА

ОАО Банк ЗЕНИТ имеет собственный процессинговый центр для обработки транзакций по международным платежным картам. Одной из важнейших задач Банка является обеспечение сохранности данных пользователей. Особое внимание уделяется вопросам защищенности технологических операций и процессам управления информационной безопасностью (ИБ). Оказываемая Банком процессинговая поддержка держателей карт и банков-партнеров должна осуществляться в строгом соответствии с требованиями ИБ, предъявляемыми международными платежными системами, в том числе требованиями стандарта PCI DSS.

Банком ЗЕНИТ перед исполнителем проекта были поставлены задачи разработать и внедрить процессы управления информационной безопасностью в соответствии с требованиями стандарта PCI DSS.

Одним из обязательных условий для Банка ЗЕНИТ было минимальное вмешательство в сложившиеся бизнес-процессы. Это связано с тем, что процессинговый центр Банка работает в непрерывном режиме 24x7, а операции Банка осуществляются по всему миру. При остановке работы процессингового центра осуществление банковских операций было бы невозможно, что не только критично с точки зрения клиентов банка, но и несет в себе определенные репутационные риски.

«Проект комплексный, и задача состояла в том, чтобы не только обеспечить соответствие стандарту PCI DSS, но и требованиям Федерального закона № 152-ФЗ «О персональных данных», и стандарта СТО БР ИББС, **– комментирует Евгений Рудацкий, руководитель направления PCI DSS компании «Инфосистемы Джет».** – *Однако в первую очередь необходимо было выполнить требования стандарта PCI DSS в связи со строгими ограничениями сроков со стороны международных платежных систем».*

Работы по сертификации на соответствие стандарту PCI DSS и оценке состояния системы защиты могут выполнять только специализированные компании, обладающие соответствующим статусом. Исполнителем проекта была выбрана компания «Инфосистемы Джет», обладающая статусами Qualified Security Assessor (QSA, для аудита), Approved Scanning Vendor (ASV, для сканирования сети) и имеющая богатый опыт реализации подобных проектов.

РЕШЕНИЕ

Работы над проектом выполнялись в три этапа: анализ соответствия требованиям стандарта, выявление несоответствий и внедрение специализированных средств защиты, проведение независимого сертификационного аудита. На первом этапе специалисты компании «Инфосистемы Джет» провели полное обследование, в ходе которого решались задачи соответствия не только стандарту PCI DSS, но и требованиям федерального закона № 152-ФЗ «О персональных

127015 Россия, г. Москва,
ул. Б. Новодмитровская, д. 14, стр.1
Телефон: +7 (495) 411-7601
Факс: +7 (495) 411-7602
info@jet.msk.su
www.jet.msk.su

Стандарт PCI DSS разработан в целях повышения уровня обеспечения безопасности в индустрии платежных карт. Организации, которые производят обработку и хранение информации о держателях платежных карт и работают с международными платежными системами, должны каждый год подтверждать соответствие защищенности своих платежных систем требованиям стандарта PCI DSS.

данных», и отраслевого стандарта СТО БР ИББС. По результатам обследования был разработан перечень рекомендаций по повышению уровня безопасности данных о держателях карт.

Наиболее масштабный – второй этап проекта, в ходе которого специалисты интегратора спроектировали и внедрили комплекс организационных и технических мер, направленных на устранение несоответствий, требуемых стандартом:

- внедрение системы мониторинга пользователей баз данных;
- построение процесса анализа и реагирования на события информационной безопасности;
- разработка организационно-распорядительной документации;
- существенная модернизация системы обнаружения вторжений;
- внесение изменений в систему контроля межсетевого взаимодействия;
- построение процессов поиска уязвимостей и управления изменениями ИТ-инфраструктуры банка.

Предложенное техническое решение включало как внедрение новых средств защиты, так и модернизацию имеющихся средств.

«Руководство ОАО Банк ЗЕНИТ принимало активное участие в проекте, что во многом способствовало скорейшему решению проектных задач, – комментирует Евгений Рудацкий, руководитель направления PCI DSS компании «Инфосистемы Джет». – Благодаря этому нам удалось завершить проект в поставленные сроки с минимальным вмешательством в сложившиеся бизнес-процессы банка».

Для оценки защищенности и подготовки к сертификационному аудиту по окончании второго этапа было проведено сканирование уязвимостей и тестирование на возможность проникновения в систему.

Завершающим этапом проекта стало проведение экспертного аудита и итоговая сертификация по требованиям стандарта. Аудит проводила отдельная команда сертифицированных специалистов компании «Инфосистемы Джет». Его результатом стало подтверждение соответствия системы информационной безопасности требованиям стандарта PCI DSS.

РЕЗУЛЬТАТ

Отчет о результатах аудита был направлен в международные платежные системы, которые подтвердили соответствие ОАО Банк ЗЕНИТ стандарту PCI DSS. Полученный Банком сертификат является подтверждением высокого качества совместно проделанной работы.

«Внедренные организационные и технические меры помогают выполнению требований ФЗ-152 и стандарта СТО БР ИББС, а главное, обеспечивают реальную защиту информации, – добавляет **Евгений Рудацкий, руководитель направления PCI DSS компании «Инфосистемы Джет».** – *В настоящее время планируется завершение аналогичных работ в Банке, связанных с отечественной законодательной базой».*