ИСТОРИЯ УСПЕХА

Приведение процессинговых систем ЗАО «Компания объединенных кредитных карточек» в соответствие с требованиями PCI DSS

ЗАО «Компания объединенных кредитных карточек» (UCS) – крупнейшая в России процессинговая компания, основные бизнес-направления которой включают эмиссию и эквайринг пластиковых карт таких международных платежных систем, как: VISA International, MasterCard Worldwide, Diners Club International, JCB International. Широкая линейка решений, которые сегодня предлагает компания, тесно связана с процессингом кредитных карт. Компания является одним из лидеров рынка более 30 лет.

Преимущества UCS, как специализированного процессора, позволяют оказывать наиболее качественный и полный сервис всем клиентам, для которых выпуск или прием карт в оплату является стратегически важным.

ЗАДАЧИ

Стандарт PCI DSS разработан в целях повышения уровня обеспечения безопасности в индустрии платежных карт и сформулирован в 12 требованиях. 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.

Когда международные платежные системы обязали своих клиентов соответствовать требованиям стандарта PCI DSS, направленным на повышение уровня обеспечения безопасности клиентских данных, компания UCS одной из первых начала вести работу по усовершенствованию систем информационной безопасности. Руководство компании приняло решение о приведении процессинговой системы в соответствие с требованиями стандарта PCI DSS.

Несоответствие требованиям стандарта наблюдалось по следующим параметрам:

- отсутствие некоторых средств защиты информации, требуемых PCI DSS;
- отсутствие возможности реализации требований стандарта техническими средствами;
- недостаточная документированность процессов управления информационной безопасностью.

Исполнителем проекта была выбрана компания «Инфосистемы Джет» – одна из немногих, обладающих необходимыми для проведения аудита на соответствие PCI DSS статусами Qualified Security Assessor (QSA, для аудита) и Approved Scanning Vendor (ASV, для сканирования сети), а также практическим опытом.

Кроме того, у компаний уже был опыт успешной совместной работы – крупный проект по построению дата-центра «под ключ».

РЕШЕНИЕ

Работа над проектом строилась в три этапа: первоначальный анализ соответствия требованиям стандарта, устранение несоответствий и внедрение необходимых организационно-технических мер защиты, сертификационный аудит.

Первый этап проекта включал в себя предварительную экспертизу процессинговых систем компании UCS. Были обследованы ИТ-система, технологические и бизнес-процессы компании, а также их взаимодействие.

Игорь Ляпунов, начальник Центра информационной безопасности компании «Инфосистемы Джет»:

«Мы провели полномасштабное обследование, которое потребовало большого количества ресурсов, в том числе, человеческих. Мы собрали огромное количество данных, опросили не один десяток сотрудников, согласовали полученные данные – таким образом мы собрали всю необходимую информацию».

Обследование выявило несколько несоответствий требованиям стандарта PCI DSS, например, существовала проблема с внесением изменений в платежную систему – был высок риск нарушений в ее работе. Поэтому в рекомендациях по устранению несоответствий были учтены и эти моменты. По рекомендациям был разработан план приведения в соответствие, содержащий конкретные действия по удовлетворению всех требований.

Второй этап начался с анализа рисков в работе ИТ-инфраструктуры, препятствующих выполнению некоторых требований стандарта PCI DSS. По результатам анализа консультанты компании «Инфосистемы Джет» предложили ряд компенсирующих мер. Эти меры позволили удовлетворить требования PCI DSS, а также сократить затраты заказчика, не уменьшив уровень безопасности.

В рамках второго этапа специалисты компании «Инфосистемы Джет» выполнили проектирование и внедрение комплекса организационных и технических решений для защиты данных о держателях платежных карт. Они разработали необходимую документацию, выполнили внедрение процессов управления информационной безопасностью, требуемых стандартом: процессы управления рисками, инцидентами и уязвимостями. Был реализован ряд технических решений, требуемых PCI DSS либо выступающих в качестве компенсирующих мер:

- внедрена система обнаружения вторжений;
- создана система сквозного мониторинга событий ИБ;
- создана система контроля целостности на всех этапах работы с данными;
- проведена сетевая сегментация;
- внедрен процесс управления инцидентами.

Особое внимание было уделено решениям по управлению доступом к информации и информационным ресурсам.

Многие действия приходилось выполнять «по-живому» – без остановки даже отдельных компонентов – ведь работу процессингового центра остановить нельзя.

Дмитрий Сидоров, директор Дирекции IT UCS, заметил: «Мы пользовались технологией параллельных решений, когда новый процесс внедрялся параллельно со старым, велась верификация результатов старого и нового процессов, и если результаты верификации совпадали, то новый процесс уже внедрялся на место старого. Ни одного серьезного сбоя не было».

При реализации проектов, затрагивающих изменение привычных для пользователей бизнес-процессов, очень важным аспектом является работа с коллективом, особенно участие руководства компании-заказчика в проекте, донесение и разъяснение сотрудникам важности и необходимости такой перестройки. Руководство UCS принимало активное участие в проекте, что во многом способствовало сплочению коллектива и скорейшему разрешению любых проблем.

United Card Service

Дмитрий Сидоров, директор Дирекции IT ЗАО «Компания объединенных кредитных карточек» (UCS):

«Сертификат на соответствие требованиям стандарта PCI DSS подтверждает высокий уровень защиты персональных данных в нашей компании. Он дает большие преимущества нам, и, что еще более важно – нашим клиентам. Среди них много крупных банков, каждый из которых может пойти по собственному пути развития бизнеса. И мы, в свою очередь, готовы сопровождать их на всех этапах. Например, теперь мы можем осуществлять полный аутсорсинг базы счетов банка, будучи уверенными в безопасности нашей процессинговой системы. Специалисты компании «Инфосистемы Джет» помогли нам достичь согласия с требованиями стандарта, и мы готовы рекомендовать их как экспертов высочайшего уровня».

Третий этап проекта – проведение независимого аудита на соответствие требованиям стандарта PCI DSS – был выполнен отдельной командой сертифицированных специалистов компании «Инфосистемы Джет». Аудиторы заполняли анкеты, проводили интервью, проверяли внутренние документы компании и настройки средств защиты информации. По итогам аудита было дано подтверждение соответствия процессингового центра компании UCS требованиям стандарта PCI DSS.

РЕЗУЛЬТАТ

Отчет о проведенном аудите был отправлен экспертам компаний VISA и MasterCard, которые подтвердили статус соответствия компании UCS международному стандарту PCI DSS.

Компания «КОКК» (UCS) одной из первых в Российской Федерации получила сертификат соответствия, свидетельствующий о полном выполнении требований последней версии стандарта PCI DSS 1.2.

Теперь «КОКК» отвечает постоянно растущему уровню требований клиентов и партнеров, а также может свободно оперировать на западном рынке.

Более того, требования стандарта PCI DSS во многом пересекаются с требованиями СТО БР и «Закона о персональных данных», которому должны соответствовать все организации, обрабатывающие персональные данные. Поэтому некоторые внедренные организационные и технические меры также помогают выполнению требований ФЗ-152 и стандарта СТО БР, а главное, обеспечивают реальную защиту клиентских данных.

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

О ЦЕНТРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ «ИНФОСИСТЕМЫ ДЖЕТ»

Центр информационной безопасности компании «Инфосистемы Джет» на сегодняшний день самое крупное подразделение, занимающееся информационной безопасностью, среди всех российских системных интеграторов. В Центре работает более 130 высококвалифицированных специалистов.

Компания «Инфосистемы Джет» работает на рынке информационной безопасности с 1994 года и выполняет полный цикл работ по защите корпоративных систем любого масштаба и сложности – от обследования и анализа рисков до внедрения и сопровождения средств и систем информационной безопасности. За это время было выполнено более 2000 контрактов, в т.ч. более 200 крупных проектов федерального масштаба.

Благодаря наличию широкого спектра решений и услуг, сертифицированных специалистов и богатому опыту, а также четко организованной работе проектного офиса, Центру доверяют проекты крупные компании, в том числе и транснационального масштаба, с численностью сотрудников в десятки тысяч человек.