PCI DSS: актуальные проблемы

В. КОЛОМЕЙЦЕВ: «PCI DSS – живой стандарт, который должен постоянно соответствовать активно развивающемуся рынку пластиковых карт»

Беседовала: Оксана Дяченко

Консультант по ИТ в финансовом секторе компании «Синимекс» Владимир Коломейцев в интервью НБЖ рассказал о проблемах развития стандарта PCI DSS на российском рынке и о том, как компания «Синимекс» позиционирует свою деятельность в этом направлении.

НБЖ: Какие существуют особенности использования PCI DSS на российском рынке?

В. КОЛОМЕЙЦЕВ: По сути стандарт PCI DSS (Payment Card Industry Data Security Standard) является набором требований, соблюдение которых позволяет обеспечить должный уровень защиты данных о держателях карт. Текст стандарта доступен всем желающим и используется как аудиторами при проведении проверок, так и коллективами самих компаний, которые решили получить сертификат соответствия стандарту. А круг таких организаций достаточно велик – торгово-сервисные предприятия, процессинговые центры, банки-эквайеры, организации, выпускающие платежные карты, т.е. все компании, которые хранят, обрабатывают или передают информацию о держателях карт.

На российском рынке пока не введено жестких санкций за несоответствие PCI DSS. Платежная система Visa, к примеру, ввела правила: аудит на PCI DSS является обязательным, однако если выявляются некоторые несоответствия по результатам аудита, то никаких санкций не принимается. Платежная система Master Card пока рассматривает PCI DSS на нашем рынке как рекомендательный стандарт, т.е. на организацию, не получившую статус соответствия стандарту, не налагаются никакие санкции.

Оценка соответствия требованиям стандарта PCI DSS обязательно должна проводиться сертифицированной в индустрии платежных карт компанией (имеющей статус Qualified Security Assessors, QSA).

Сам набор требований стандарта разделен на 12 логических групп. Каждое требование имеет критерий его проверки, и с формальной точки зрения схема работы выглядит просто, однако в реальности возникают различные нюансы, о которых хотелось бы рассказать.

Операции с пластиковыми картами на российском рынке осуществляются достаточно давно, и, следовательно, многие процессинговые системы разрабатывались до появления на нашем рынке стандарта PCI DSS и теперь во многом не соответствуют ему. Например, один из пунктов стандарта запрещает хранить в незашифрованном виде карточные данные, в том числе и номер карты. В свою очередь, зачастую при построении архитектуры хранения данных систем процессингового центра активно использовался номер карты, и при подготовке к аудиту по этой причине перед коллективом, ответственным за подготовку систем банка, встает непростая задача. И если при разработке новой системы реализовать требования стандарта – не такая сложная задача, то менять архитектуру очень дорого – этот процесс итеративный и очень долгий. Поэтому я считаю, что Visa и Master Card проявили себя как стратегические партнеры по отношению к российским процессинговым центрам, они дают время на постепенную адаптацию систем и процессов организации к требованиям стандарта. Это позволит отечественным игрокам индустрии платежных карт связать свое дальнейшее развитие с PCI DSS.

НБЖ: В каком ключе позиционирует себя компания «Синимекс» в этой связи?

В. КОЛОМЕЙЦЕВ: При проведении аудита компания QSA выставляет к банку определенные требования, которые, в первую очередь, адресованы специалистам подразделения процессинга. Работа в индустрии платежных карт подразумевает огромную нагрузку и огромные скорости. Поэтому люди, работаю-

щие в карточном процессинге с большим потоком данных и отвечающие за развитие и поддержку этого направления, испытывают невероятные нагрузки. Представьте, что им еще нужно работать с аудиторами QSA и отвечать за изменения архитектуры систем, владельцами которых они не являются!

В этой связи наша компания взяла на себя функции помощи банкам и другим организациям в поисках решений проблем и проведении изменений, возникающих при подготовке у аудиту PCI DSS. Мы стараемся прийти к нашим клиентам уже с готовыми ответами и решениями. Предварительно эти ответы мы согласовываем с QSA. Ведь стандарт развивается, многие вопросы можно трактовать, и это вызывает у банков проблемы. Приведу пример. У наших клиентов возник вопрос, допустимо ли по стандарту PCI DSS осуществлять шифрование данных на уровне шифрования дисков. У QSA удалось выяснить, что, скорее всего, это будет некорректно, рекомендовано шифровать на уровне ПО.

Мы накапливаем подобные вопросы от наших клиентов и к новым заказчикам приходим со все большим количеством готовых ответов. При этом мы подчеркиваем, что никто лучше банков не знает их собственных проблем, поэтому практически невозможно прийти в банк и научить его, как правильно проходить PCI DSS. У каждой кредитной организации уникальная архитектура, выстроенная таким образом, чтобы иметь конкурентные преимущества перед другими банками. Можно сказать, что каждый банк в части архитектуры построения ПО уникален. Поэтому прийти с полностью готовыми ответами на все вопросы не получится. Нельзя создать стандартный набор рекомендаций для всех сразу.

Для каждой кредитной организации главное – время и клиенты. Мы помогаем банкам решать их проблемы, таким образом экономим им время, разгружаем специалистов. Причем мы не просто приносим готовые ответы от аудиторов, некоторые из них нами перерабатываются и прорабатываются и только потом предлагаются заказчикам.

И хотя наша компания не может прямо помогать банкам привлекать клиентов при прохождении аудита PCI DSS, мы можем помочь не потерять их.

НБЖ: Вы не хотите приобрести статус QSA?

В. КОЛОМЕЙЦЕВ: Компания пока не планирует получать статус QSA, возможно, это вопрос будущего. На данный момент наша задача – помощь банкам в подготовке к аудиту, экономия времени и сил наших клиентов, которые они смогут высвободить для реализации важных бизнес-задач.

НБЖ: Каким вы видите развитие рынка PCI DSS?

В. КОЛОМЕЙЦЕВ: Прохождение аудита на соответствие стандарту PCI DSS – это регулярная ежегодная процедура. Причем скоуп систем, подлежащих аудиту в рамках PCI DSS, в недалеком будущем будет только расти, поскольку для реализации амбициозных бизнес-проектов требуется все большая интеграция карточных продуктов с остальными системами банка.

В этой постоянной процедуре проверки соответствию стандарту PCI DSS мы также хотели бы участвовать и предоставлять услуги организациям, перед которыми встала задача прохождения аудита. Сейчас компания прорабатывает подобные возможности. Например, становится очевидным, что некоторые наши клиенты уже на уровне проработки архитектуры включают требования PCI DSS, особенно это касается каналов ДБО.

Мы видим, что PCI DSS быстро развивается, это живой стандарт, который должен постоянно соответствовать активно развивающемуся рынку платежных карт. Все время растет перечень услуг, связанных с картами, а следовательно, расширяется и сфера использования PCI DSS. Если раньше PCI DSS в основном обсуждали банки, крупные компании, то сейчас все больше вопросов аудиторам задают интернет-магазины, интернет-порталы. Дело в том, что вопрос предоставления качественных услуг клиенту начинает упираться в этот стандарт.

НБЖ: Как можно решить проблему согласования англоязычной и русскоязычной версий стандарта?

В. КОЛОМЕЙЦЕВ: Стандарт PCI DSS разработан Советом по стандартам безопасности индустрии платежных карт на английском языке. Компании QSA работают с английской документацией, а требования к банкам, в свою очередь, выставляют на русском языке.

Думаю, что по мере усложнения стандарта начнут появляться различные трактовки PCI DSS даже на уровне согласования русскоязычной и англоязычной версий. Функцию согласования различных трактовок могла бы взять на себя компания, обладающая статусом QSA. Хотя, пожалуй, наиболее оптимальным решением было бы создание коллегиального органа по согласованию стандарта.

НБЖ: Как вы оцениваете перспективы PCI DSS в России, особенно в связи с разработкой стандартов безопасности Банком России?

В. КОЛОМЕЙЦЕВ: Я убежден, что PCI DSS имеет широкие перспективы по распространению среди организаций в нашей стране. Благодаря требованиям стандарта банки и другие организации находят более эффективные способы зашиты данных своих клиентов и таким образом понижают собственные риски пострадать от мошеннических действий. Тем более что стандарт – это не только защита, но и договор о правилах работы на рынке, ведь любая стандартизация упрощает интеграцию между организациями.

Хочу подчеркнуть, что Банк России не только выпускает собственные стандарты безопасности, но и ведет серьезную разъяснительную работу в этом направлении. И у нас есть ощущение, что PCI DSS будет включен в требования Банка России в том или ином виде, т.е. можно говорить о тенденции сращивания стандартов. Отечественные банки взаимодействуют с огромным количеством контрагентов за границей, поэтому прохождение сертификации намного упростит их работу, в том числе и из-за возросшего к ним доверия со стороны партнеров. И в ЦБ РФ это понимают.

Я думаю, что требования Банка России будут включать сугубо российские специфические требования, обязательные к исполнению, и требования, взятые из стандарта PCI DSS (как рекомендательные, так и обязательные). Сращивание с глобальным рынком пластиковых карт и соответствие международным стандартам безопасности – это чрезвычайно позитивная для России тенденция. NBJ