

5 основных проблем вашей инфраструктуры на пути к соответствию PCI DSS

24.04.2009

Доклад, посвященный основным проблемам, с которыми сталкиваются российские компании на пути к соответствию требованиям стандарта PCI DSS, был сделан 15 апреля 2009 года в московском ЦВК «Экспоцентр» в рамках конференции CARDEX & IT SECURITY.

Сергей Шустиков, QSA-аудитор Digital Security

С 2007 года стандарт PCI DSS стал объективной реальностью для специалистов по информационной безопасности, занимающихся защитой платёжных систем. Большинство организаций, имеющих дело с карточными данными, уже пережили первый опыт общения с QSA-аудиторами и задумались над приведением своей информационной инфраструктуры в соответствие требованиям стандарта. Стоит обратить внимание на часто встречающиеся проблемы, возникающие на пути к соответствию.

Проблема первая – выделение области применения стандарта. Ни для кого не секрет, что требования стандарта к обеспечению ИБ весьма строги. Ситуация облегчается тем, что их действие не распространяется на всю информационную инфраструктуру компании, а только на ту её часть, в которой хранятся, обрабатываются и передаются карточные данные, а также связанные системы. Под связанными стандарт понимает те системы, соединение с которыми не защищено межсетевым экраном. По этой причине, неправильное выделение среды обработки карточных данных от остальной корпоративной сети приводит к тому, что под действие стандарта попадает вся корпоративная сеть компании, и её необходимо защищать в соответствии с его требованиями. Напротив, правильная сегментация поможет минимизировать область применения требований стандарта и значительно сократить затраты.

Проблема вторая – хранение данных. Стандарт запрещает хранение критичной аутентификационной информации (данные магнитной дорожки, PIN и PIN-block, а также CVC2/CVV2) и требует, чтобы как минимум PAN хранился в нечитаемом виде. Под приведением в нечитаемый вид стандарт понимает, в том числе, шифрование. К сожалению, очень часто журналы регистрации событий процессинговых приложений содержат данные магнитной дорожки, а номера карт хранятся в таблицах СУБД в открытом виде. При этом следует отметить, что безопасность должна быть обеспечена во всех местах хранения карточных данных и не стоит забывать файловые сервера и носители резервных копий. В качестве решения данной проблемы могут выступить средства, предлагаемые самими поставщиками СУБД, например Oracle Transparent Data Encryption (TDE).

Проблема третья – разграничение доступа и роли пользователей. Классическая ситуация – отсутствие внятной политики разграничения доступа и, как следствие, бессистемное его предоставление. Мало того, что системные администраторы часто имеют максимальный доступ абсолютно ко всем системам, но подчас уровень доступа обычных пользователей далеко не соответствует принципу

минимальных привилегий. На эту проблему стоит обратить особое внимание, ведь отлаженная процедура предоставления, изменения и отзыва прав доступа, сопровождаемая необходимыми заявками и согласованиями, в России пока еще скорее исключение, чем правило.

Проблема четвертая – мониторинг, а точнее – его отсутствие. При проведении аудита в ответ на вопрос о процедуре управления инцидентами порой приходится слышать, что инцидентов информационной безопасности в компании не было, нет и не предвидится. Это может быть опасное заблуждение, вызванное отсутствием систем и процедур регулярного мониторинга информационной безопасности. Журналы протоколирования событий не изучаются, сетевая активность не анализируется, внутренний аудит не проводится. Сотрудники говорят об отсутствии инцидентов не потому, что их нет, а потому что они их не видят. Учитывая то, что латентность преступлений в сфере информационных технологий крайне высока, без внедрения эффективных механизмов мониторинга их обнаружить невозможно. Одним из наиболее показательных методов оценки эффективности защиты данных о владельцах платежных карт является тест на проникновение. На практике тесты на проникновение в большинстве случаев не проводятся или их качество находится на крайне низком уровне. А ведь качественно выполненный тест, как ни что другое, покажет реальную картину защищенности. Тест на проникновение, выполняемый специалистом, последовательно реализующим цепочку уязвимостей компонентов информационной инфраструктуры, не следует путать с автоматизированным сканированием, которое выявляет лишь уязвимости, лежащие на поверхности. Стоит обратить внимание на то, что требование 11.3 стандарта PCI DSS регламентирует необходимость проведения как внешнего теста на проникновение, так и внутреннего. Внутренний тест на проникновение - это активный аудит защищенности информационной инфраструктуры, выполняемый изнутри согласно модели нарушителя с минимальными привилегиями.

И, наконец – **проблема пятая**. Она заключается в полном или частичном отсутствии, равно как и в низком качестве базы нормативных документов по информационной безопасности. Проблемой являются устаревшие регламенты, которые не только не выполняются, но и очень часто неизвестны сотрудникам компании. Большинство процедур носят неформальный характер, записи об их выполнении отсутствуют. Практика показывает, что без процессного подхода и эффективной системы управления - безопасности не бывает. Система управления информационной безопасностью - это не набор шаблонных документов, которые можно скачать из Интернета или взять у друга, а затем положить в сейф до прихода аудитора. Пылящаяся стопка бумаги не нужна ни вам, ни аудитору. Аудитор, в первую очередь, хочет увидеть небольшие эффективные и удобные для работы документированные процедуры. Это процедуры, которые знают и выполняют на практике сотрудники. Это процедуры, по которым ведутся записи, история которых началась не за одну неделю до аудита.

По опыту, перечисленные пять проблем соответствия PCI DSS встречаются наиболее часто, и именно на них стоит обратить внимание всем, кто встал на путь к соответствию стандарту.

Об авторе

Сергей Шустиков – QSA-аудитор, ведущий аналитик по информационной безопасности компании Digital Security, специализируется на системах менеджмента безопасности. Область профессиональных интересов охватывает разработку систем менеджмента информационной безопасности в соответствии с международными стандартами и проведение аудитов на соответствие требованиям ряда стандартов индустрии защиты информации (PCI DSS, ISO/IEC 27001:2005, СТО БР-ИББС-1.0).

О стандарте PCI DSS

Стандарт PCI DSS (Payment Card Industry Data Security Standard) предназначен для обеспечения безопасности обработки, хранения и передачи данных о держателях платежных карт в информационных системах компаний, работающих с международными платежными системами Visa, MasterCard и другими. Стандарт разработан сообществом PCI Security Standards Council, в которое входят мировые лидеры на рынке платежных карт, такие как American Express, Discover Financial Services, JCB, MasterCard Worldwide и Visa International.

Под действие требований стандарта попадают банки, процессинговые центры, поставщики ИТ-услуг, торгово-сервисные предприятия, и иные организации, обрабатывающие транзакции по международным платежным картам. К части этих компаний международные платежные системы предъявляют требование о прохождении обязательного ежегодного аудита компанией, обладающей статусом QSA.

Текущая версия стандарта 1.2 выпущена 1 октября 2008 года.