

PCI DSS как средство повышения уровня защищенности информационной инфраструктуры

20.03.2009

Стандарт PCI DSS, разработанный совместными усилиями международных платежных систем (AmEx, Discover, JCB, MasterCard и Visa) как ответ на непрекращающиеся инциденты компрометации данных платежных карт, привлекает все больше внимания в российском банковском сегменте.

Антон Карпов, QSA-аудитор Digital Security

МПС пока еще не предъявляют штрафных санкций к банкам в России за несоответствие требованиям стандарта (non-compliance), требуя лишь наличие факта прохождения аудита. Тем не менее, уже сейчас можно отметить печальную тенденцию к готовности воспринимать стандарт как формальный документ и саму процедуру прохождения аудита (и, соответственно, подготовки своей инфраструктуры к аудиту) – как необходимость выполнить ряд процедур «для галочки». Разумеется, не все организации столь категоричны в отношении к стандарту, а те, кто входит в этот круг, поступают так не от хорошей жизни – финансовый кризис коснулся банковского сектора в первую очередь, проблем всегда немало, а тут еще PCI DSS... Тем не менее, я бы в такой ситуации порекомендовал взглянуть на стандарт немного иначе. Не как на навязанные двести с лишним требований, обязательные для выполнения, а как возможность системно подойти к вопросам обеспечения информационной безопасности своих платежных ресурсов.

Как отмечено выше, МПС пока не собираются выставлять штрафные санкции даже за самый жесткий non-compliance, лишь вводя штрафы за отсутствие самого факта прохождения аудита. Это говорит об одном: Visa, MasterCard и другие меньше всего хотят, чтобы вы сейчас же бежали затыкать бреши в своей системе ИБ бессистемно-заплаточным способом. Не стоит бояться проверок QSA. Не нужно опасаться замечаний аудиторов. Хороший QSA-аудитор выявит основные «болевы точки» вашей инфраструктуры, которые не только являются причиной несоответствия различным требованиям PCI DSS, но и существенно снижают уровень защищенности вашей платежной инфраструктуры. Хороший аудитор, в дополнение к официальному отчету (Report on Compliance), содержащему замечания по каждому требованию стандарта, выдаст свои рекомендации по повышению уровня ИБ, наметит шаги, которые необходимо выполнить в первую очередь для устранения самых серьезных проблем. После визита хорошего QSA-аудитора у компании на руках останется не только заполненная таблица соответствия, а в голове будет отсутствовать непонимание того, что с этим делать. План действий, четкое представление того, какие мероприятия следует планомерно проводить в первую очередь, без формальной оглядки на стандарт – вот та информация, которую должен дать хороший аудит. И только

потом, проходя аудит во второй-третий-четвертый раз, можно раз за разом «подкручивать гайки» в соответствии с отдельными требованиями стандарта.

Возьмем для примера требование 11.3 стандарта, согласно которому в компании минимум раз в год, а также в случае существенных изменений структуры сети (например, внедрении новых серверов), должен проводиться тест на проникновение. Под тестом на проникновение понимается проведение атак на сетевом уровне и на уровне приложений на все публично доступные сервисы компании из сети Интернет (т.н. "внешний тест на проникновение") и внутренние ресурсы, входящие в область аудита PCI DSS (т.е. внутренний активный аудит защищенности). Грамотно выполненный тест на проникновение позволяет оценить реальный уровень защищенности информационных ресурсов компании, как с точки зрения внешнего злоумышленника, так и с позиции злонамеренного сотрудника компании – это подтверждается лучшими мировыми практиками в области ИБ. Здесь PCI DSS не говорит ничего нового, лишь заставляет еще раз уделить внимание данному аспекту ИБ. Давно ли в вашей компании проводился тест на проникновение? Грамотно ли он был выполнен, или это было просто сканирование специализированными программными средствами?

Таким образом, хотелось бы, чтобы PCI DSS воспринимали не как навязанную «обязаловку», а как дополнительную мотивацию к приведению в порядок инфраструктуры ИБ, хотя бы в моментах, определенных стандартом. Для разумного минимума ИБ он вполне подходит.

Об авторе

Антон Карпов – аналитик по информационной безопасности компании Digital Security, QSA-аудитор.

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.