

Аудитор или консультант?

31.07.2009

Правильно ли вы понимаете роль QSA-аудитора, пришедшего к вам на помощь в решении такой задачи, как достижение соответствия PCI? Какое слово точнее описывает ваши отношения – соперничество или сотрудничество?

Сергей Шустиков, ведущий аналитик по информационной безопасности компании Digital Security

Практический опыт показывает, что не все специалисты правильно понимают роли сторон, участвующих в процессе достижения соответствия PCI. Давайте разберемся, что тут к чему, тем самым сделаем попытку ликвидировать почву для произрастания непониманий и трудностей взаимодействия.

Посмотрим на процесс со стороны. С одной стороны мы видим банк, процессинг, платежный шлюз, торгово-сервисное предприятие, или другую компанию, волею судьбы обязанную соответствовать требованиям стандарта PCI DSS. Международные платежные системы предписали компании соответствовать, и иного выхода у неё нет, если она планирует продолжать карточный бизнес. Нам это может нравиться или нет, мы можем долго рассуждать, насколько оправданы действия регуляторов, но для нас это останется таким же объективным фактом, как то, что трава зеленая, а дождь мокрый. Не нами это правило заведено, не нам его отменять, поэтому примем его как должное. Сразу хочу оговориться, что часто всплывающие вопросы «особого пути» России в данном случае я тоже оставляю за бортом, как не имеющие прикладного смысла. Весь мир может соответствовать PCI, мы ничем не хуже.

С другой стороны мы видим QSA-аудитора, призванного объективно оценить степень соответствия компании требованиям стандарта PCI DSS. Для компании он видится проводником стандарта, что правда, видится связующим звеном по рассматриваемой линии с международными платежными системами, что тоже правда, но кроме того, он видится исполнителем карательной воли этих самых регуляторов, что в корне не правда. Возможно, ассоциация с некими карательными функциями возникает из-за термина «аудитор», вызывающего не самые приятые мысли, особенно в сочетании с термином «внешний». Поэтому предлагаю это слово на букву «а» сейчас не употреблять, а воспользоваться нейтральным переводом английского слова «assessor» - «оценщик», а лучше дружественным «консультант». Да да, именно как консультанта необходимо воспринимать этого человека, как друга, который пришел помочь решить проблему.

Теперь рассмотрим, какие же между этими друзьями возникают непонимания. Непонимание первое, явно вызванное негативом от слова на букву «а», заключается в том, что от этого друга-помощника пытаются скрыть проблемы, куда-то его не подпустить, рассказать ему сказки из местного фольклора, и другими хитрыми и не очень способами помешать его работе. Абсурдность ситуации очевидна –

больной, вызвавший на дом доктора, не пускает его на порог, не даёт себя осмотреть и послушать, тайно надеясь на то, что и не болен вовсе, а здоров как бык. Укрывая проблемы от консультанта, компания лишь оттягивает момент, когда ей всё-таки придется ими заняться, а запущенные болезни лечить, как известно, гораздо труднее, особенно если их сокрытие помешало постановке правильного диагноза.

Непонимание второе, основанное, по всей видимости, на нежелании большинства выходить из состояния иллюзорно комфортного равновесия, лучше всего описываемого фразой «авось пронесет». На практике чаще всего выражается в виде попыток компании доказать, что «PCI DSS у нас от сих до сих, а туда и не смотрите даже». Компания начинает ожесточенные бои за каждое место хранения карточных данных и смежные системы, считая своим долгом доказать консультанту, что к этому месту стандарт не применим, и защищать его не надо. Здесь всегда хочется задать известный вопрос: «вам шашечки или ехать?», то есть – какова цель – навести порядок и обеспечить безопасность, тем самым достичь соответствия PCI, или же всеми правдами и неправдами отыскать формальные лазейки не защищать данные и вообще «ничего не трогать, ничего не менять»? Для меня очевидна первая. Опять же, если приводить аналогии из медицины, то глупо выглядит больной, доказывающий доктору, что он и не болен вовсе, а кашель, хрипы в легких и высокая температура – недоразумение, которое лечить не надо, потому что само пройдет.

Чтобы не было в нашей работе подобных комичных ситуаций, следует помнить две очень простые мысли, которые почему-то для многих оказываются весьма сложными для понимания. Первая и основная – цель и у компании и у QSA одна общая – обеспечить безопасность данных о держателях карт и через это достичь соответствия стандарту PCI DSS. Вторая – QSA – это в первую очередь консультант, человек, пришедший помочь решить объективную проблему. Это знающий друг и партнер, который способен оценить ситуацию и предложить способы решения вопросов, с ней связанных. Это справедливо как для проектов по консалтингу и приведению в соответствие, так и для проектов по аудиту.

С уверенностью в том, что понимание неизбежно достижимо, как и соответствие PCI.

Об авторе

Сергей Шустиков – 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 международных и национальных стандартов индустрии защиты информации (PCI DSS, ISO 27001, СТО БР-ИББС-1.0). Занимается научно-исследовательской деятельностью в области системного анализа методов управления в сфере информационных технологий и информационной безопасности. Преподает ряд специальных дисциплин на кафедре Безопасных Информационных Технологий Санкт-Петербургского Государственного Университета Информационных Технологий Механики и Оптики.

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.