

Подводные камни процесса достижения соответствия PCI DSS

15.03.2010

На что стоит обратить внимание при выборе QSA-компании для достижения Соответствия PCI DSS?

Илья Медведевский, к.т.н., директор компании Digital Security

Предварительный аудит

Рекомендации по устранению найденных несоответствий: краткие или детальные?

При проведении предварительного аудита на соответствие стандарту PCI DSS QSA-аудитор в своем отчете по каждому обнаруженному несоответствию может привести краткие рекомендации по устранению данного несоответствия, например: «безопасно настроить СУБД Oracle в соответствии с такими-то конкретными лучшими практиками и т. д.». Обычно это входит в базовую стоимость предварительного аудита. Для QSA-аудитора является жестом доброй воли выдать краткие типовые рекомендации даже при официальном сертификационном аудите, результатом которого не явилась констатация факта полного соответствия.

Однако заказчику с уровнем соответствия менее 50% стоит обратить внимание на то, что на практике такой подход означает следующее: при дальнейшей подготовке к сертификации он сам будет изучать обозначенную QSA-аудитором проблему и искать варианты, как именно ему выполнить данное требование. Очевидно, что для заказчика (особенно крупного) это часто бывает затруднительно, поскольку требует серьезных затрат времени и ресурсов. В результате такая схема автоматически приведет к необходимости заказа дополнительного расширенного консалтинга при внедрении решений по устранению несоответствий.

На этом фоне заказчику стоит обратить внимание на возможность получения от QSA-аудитора экспертного заключения по результатам проведенного аудита с детальными рекомендациями по приведению информационной инфраструктуры в соответствие PCI DSS. Такое заключение предоставляется в качестве дополнительной услуги сразу после проведения предварительного аудита в виде отдельного документа объемом 20–100 страниц. Это значительно упростит дальнейший процесс подготовки к сертификации, хотя по своей сути является не более чем полезной опцией предварительного аудита для заказчика.

План приведения к соответствию PCI DSS (Action Plan)

Очень часто заказчик в предложении от QSA может обнаружить фразу: «План приведения информационной инфраструктуры в соответствие требованиям PCI DSS (Action Plan)». При этом сама

фраза зачастую подается очень пафосно в контексте отдельной части коммерческого предложения заказчика, тем самым, пытаются убедить в том, что именно этот документ решит все его проблемы с соответствием. Однако парадокс ситуации заключается в следующем: под достаточно громким названием скрывается сугубо формальный документ на одну страницу (!), который отправляется в международные платежные системы и который обычно заполняется ... самим же заказчиком (QSA-аудитор лишь консультирует заказчика при его заполнении или оказывает в этом некую помощь). Этот документ необходим только в том случае, если аудит был сертификационным (не предварительным), и его результаты не показали полного соответствия. Содержанием данного документа является не более чем перечень из основных этапов достижения соответствия с указанием сроков их планируемого выполнения. Цель у документа единственная – проинформировать международные платежные системы (МПС) о том, когда именно в следующий раз (но не далее, чем через один год) можно обоснованно требовать от компании соответствия PCI DSS. Для формальной процедуры сертификационного аудита Action Plan – это просто форма отчетности и не более того.

В случае предварительного аудита, цель которого – сделать первый шаг на пути к соответствию, заказчик обычно не сообщает о его результатах в МПС, и поэтому формальный Action Plan не является обязательным, так как ни коим образом не приближает к достижению соответствия. Самое главное, что должен понимать заказчик: что несмотря на пафосное название, речь идет не более чем о кратком сугубо формальном документе, который не имеет отношения к содержательной части процесса устранения несоответствий и практически никак не поможет при дальнейшей подготовке к сертификации, разве что обозначит временные ориентиры.

Достижение соответствия PCI DSS

Технический проект, детально описывающий все вносимые в ИТ систему изменения

После проведения предварительного аудита и разработки экспертного заключения с детальными рекомендациями для последующего перехода к стадии внедрения (приведение ИТ-системы в соответствие) заказчику необходим детальный технический проект, описывающий все вносимые в систему изменения для ее приведения в соответствие требованиям стандарта. Без подобного проекта тем более никак не обойтись в случае необходимости внесения масштабных изменений, особенно если речь идет о крупном банке, где в наших реалиях процессинг часто не выделен из информационной инфраструктуры банка, а наоборот, глубоко в нее интегрирован. Данный проект разрабатывается на основе отчета о проведенном на первом этапе аудита и экспертного заключения, выданного QSA-аудитором. Проект разрабатывается либо самим заказчиком (если он планирует самостоятельную реализацию технических мероприятий по достижению соответствия) или компанией – системным интегратором, которого заказчик планирует привлечь для реализации проекта достижения соответствия PCI DSS.

На данном этапе одной из важнейших консалтинговых задач для QSA-аудиора является согласование итогового технического проекта с точки зрения его соответствия требованиям стандарта PCI DSS во избежание возможных дальнейших проблем при внедрении. Это крайне важный этап, про который ни в коем случае не стоит забывать заказчику.

Консалтинг при внедрении, контрольные проверки и предсертификационный аудит

После того как детальный технический проект достижения соответствия принят и согласован с QSA-аудитором, заказчик переходит непосредственно к этапу его внедрения для последующего устранения всех найденных в ходе предварительного аудита несоответствий. На данном этапе при заключении с QSA-компанией общего консалтингового контракта на приведение к соответствию PCI DSS существуют три возможные опции, на которые заказчику стоит обратить внимание. Особенно эти опции важны в случае в случае крупной организации (банка, сервис-провайдера), для которой внедрение изменений с целью устранения найденных несоответствий является масштабным, сложным и длительным проектом, требующим непрерывного контроля. Небольшим организациям или организациям с высоким исходным уровнем соответствия отдельными опциями можно пренебречь.

1. Консалтинг при внедрении

В этом случае QSA-аудитор (хотя здесь более уместным будет употребить термин QSA-консультант) отвечает на все вопросы, которые возникают у специалистов заказчика или интегратора в ходе реализации проекта по достижению соответствия PCI DSS.

2. Контрольные проверки

Практика показывает, что имеет смысл разбить весь проект на этапы, между которыми расставляются контрольные точки, по которым QSA-консультант имеет возможность контролировать ход проекта, оценивая на объекте все внесенные к моменту проверки изменения (после предыдущей проверки) с точки зрения корректности выполнения требований стандарта.

3. Предсертификационный аудит

Для 100%-ной гарантии успешного прохождения итогового сертификационного аудита при масштабном проекте достижения соответствия PCI заказчику может потребоваться предсертификационный аудит, который выявит мелочи, которые могли быть упущены в процессе реализации проекта достижения соответствия. При этом наличие контрольных проверок в ходе внедрения, очевидно, не отменяет необходимости проведения предсертификационного аудита, хотя оба этих контрольных элемента и являются опцией.

Сертификация

Тесты на проникновение, ASV-сканирование

Про специфику предлагаемых на рынке России и стран СНГ «тестов на проникновение» (то, что в 99% случаев предлагается у нас на рынке под этим ярлыком, было бы некорректно упоминать иначе как в кавычках), обязательных для достижения соответствия PCI DSS, написана уже не одна статья. Заказчику стоит обращать внимание на то, что любая попытка выдать за пентест обычное сканирование (чем часто грешат, к сожалению, в том числе и некоторые QSA-компании) является заведомым нарушением требований стандарта и ведет к лишению QSA-компании этого статуса и проблемам для заказчика, которому данная QSA-компания выдала сертификат, – последний

неминуемо будет отозван Советом PCI SSC. Низкая цена на пентест автоматически означает то, что это будет простой запуск сканера, и свидетельствует об отсутствии необходимой квалификации у компании, которая его проводит. Иными словами, «опасайтесь подделок!».

Что же касается ASV-сканирования, то здесь на нашем рынке наблюдается прямо противоположная, но не менее парадоксальная картина в виде необоснованно дорогого сканирования. ASV-сканирование у большинства ASV-вендоров является автоматической услугой, позволяющей заказчику самостоятельно запустить через web-сайт вендора в удобное для заказчика время сканер и получить отчет об ASV-сканировании. Процедура полностью автоматизирована, из-за этого число проверок практически не ограничено – соответственно, ASV-сканирование, по определению, не может стоить дорого. Разговоры о качестве ASV-сканирования лишены всякого смысла, так как все ASV-вендоры имеют официальный статус и сканируют в строгом соответствии с процедурой, определенной Советом PCI SSC. Во-вторых, даже если кто-то сканирует чуть лучше, а кто-то чуть хуже – в любом случае существует дополнительная ручная проверка – тест на проникновение, не имеющий никакого отношения к ASV-сканированию, который дает дополнительные гарантии защищенности внешнего периметра.

Непосредственно сертификационный аудит, проводимый после выполнения всех перечисленных этапов, является итоговой контрольной проверкой достигнутого соответствия PCI DSS, по большому счету сводящейся к документированию свидетельств выполнения заказчиком требований стандарта, результаты которого QSA-компания обязана хранить не менее трех лет.

Вывод

Как наглядно показывают вышеприведенные примеры из практики, заказчику стоит очень внимательно подходить к выбору QSA-аудитора, поскольку здесь существует масса различных нюансов, имеющих далеко идущие последствия.

Об авторе

Илья Медведевский – Родился в 1972 году в Ленинграде. В 1996 году окончил Санкт-Петербургский Государственный Политехнический Университет по специальности «Информационная безопасность компьютерных систем». После окончания университета поступил в аспирантуру и работал в Центре защиты информации СПбГПУ. В 1999 году защитил кандидатскую диссертацию на тему «Разработка методов и средств анализа информационной безопасности и обнаружения воздействий в распределенных вычислительных системах».

В 1996 году была опубликована первая книга «Теория и практика обеспечения информационной безопасности». Начиная с 1997 года была написана и опубликована серия книг «Атака на Интернет», «Атака через Интернет», «Атака из Интернета», ставших бестселлерами.

С 1994 занимается исследованиями в области информационной безопасности, публикуя их результаты в таких печатных изданиях, как BYTE/Россия, LAN, Открытые Системы, ИнфоБизнес, Системы безопасности, Information Security и многие другие.

С 2002 года является директором компании Digital Security – одной из ведущих российских консалтинговых компаний в области ИБ, а также открытого в рамках компании исследовательского центра DSec Research Group и Сообщества профессионалов PCIDSS.RU.

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 1.2.1 выпущена в июле 2009 года.