

Как достичь «PCI DSS Compliance»?

Максим Эмм, директор Департамента аудита компании «Информзащита»,
Наталья Зосимовская, ведущий специалист компании «Информзащита»

В минувшем 2008 году журнал «ПЛАС» опубликовал нашу обзорную статью, посвященную стандарту PCI DSS и его требованиям*. Помимо общих вопросов, касающихся данного международного стандарта, в рамках прошлогоднего материала мы также останавливались на интересующей многих участников рынка теме процедуры аудита, приводили собранный статистический материал по основным несоответствиям требованиям стандарта и давали практические советы, как бороться с этими несоответствиями. Итак, прошел год. Нашими специалистами было проведено более 40 аудитов (в том числе и повторных), накоплен еще больший опыт и новый статистический материал. Основываясь именно на нем, мы сочли целесообразным поделиться в данной статье некоторыми выводами и соображениями относительно оптимального с нашей точки зрения пути достижения заветного Compliance.



Начать хотелось бы с того, что сегодня постепенно меняется довольно распространенное даже в прошлом году мнение части банковского сообщества о том, что проходить аудит по PCI DSS, а также выполнять все требования стандарта совсем необязательно, поскольку deadline по соответствию постоянно сдвигается, информации о тех, кого уже



оштрафовали, нет, а возможно и не будет. Все больше и больше компаний понимает, что инициировать довольно непростой и трудоемкий проект по достижению соответствия требованиям PCI DSS жизненно необходимо. И не только по причине того, что могут быть испорчены взаимоотношения с регулятором. Участники рынка приходят к пониманию, что достижение и обес-

печение требуемого стандартом уровня информационной безопасности – это залог сокращения потенциального ущерба от инцидентов безопасности, повышение устойчивости бизнес-процессов и, в конечном итоге, сохранение своей репутации и клиентской базы. Между тем выполнение всех требований стандарта PCI DSS, причем не «для галочки», а именно в том виде, в котором они были изначально задуманы, а может снизить вероятность подобных инцидентов практически до нуля.

Но, как уже говорилось выше, проект по достижению соответствия требованиям стандарта PCI DSS довольно трудоемок. Зачастую организации сталкиваются с проблемой нехватки персонала для выполнения необходимых работ, а также времени, соответствующего опыта и понимания того, что именно и как необходимо сделать. В связи с этим для сокращения сроков достижения соответствия, минимизации затрат на всю программу PCI Compliance (особенно в условиях экономического кризиса) и связанных с этим проблем в ряде случаев целесообразно воспользоваться консалтинговыми услугами сторонней организации, специалистами которой прекрасно знакомы как с проблематикой требований стандарта PCI DSS и их практической реализации, так и являются профессионалами в вопросах обеспечения информационной безопасности и при этом, разумеется, хорошо понимают банковскую специфику.

Scope и Action Plan

Итак, давайте по порядку рассмотрим те проблемные области, где для решения вопросов PCI Compliance возможно вовлечение сторонних консультантов.

Изначально самым главным способом минимизации проблем с достижением соответствия и сокращением затрат на данный проект является минимизация границ аудита (scope), т.е. той области, которая будет проверяться на соответствие стандарту согласно требованиям международных платежных систем.

*См. материал «Стандарт PCI DSS: основные несоответствия и как с ними бороться», «ПЛАС» № 2/2008

Утечка данных из Heartland Payment Systems может стать крупнейшей в истории

Постоянно в прессе появляются новости об утечках данных держателей платежных карт, такие как, например, недавний случай с американским сервис-провайдером Heartland Payment, услугами которой пользуются масса западных коммерческих банков. Через сети этой компании ежемесячно проходит около 100 млн финансовых транзакций. Итак, представители Heartland Payment официально признали, что неким зло-

умышленникам удалось проникнуть в сети компании и получить доступ к данным держателей карт. Представители Visa Inc. и MasterCard Worldwide впервые предупредили о подозрительной активности по транзакциям Heartland Payment еще осенью 2008 года, но внутренний аудит тогда не выявил каких-либо проблем с безопасностью. Однако независимые следователи подтвердили наличие в сети Heartland Pay-

ment как минимум одного вредоносного кода, написанного конкретно под Heartland Payment, который оказался значительно сложнее и опаснее тех, что традиционно распространяются по сети Интернет. В итоге обнаружение кода стало возможным только после привлечения спецслужб США, которые на сегодняшний день уже инициировали масштабное расследование инцидента.

По материалам CyberSecurity

Краеугольным камнем здесь является адекватное сегментирование сети. Зачастую мы сталкиваемся с тем, что сеть процессинга не отделена от общей сети банка. В этой ситуации в область действия требований стандарта попадает вся информационная инфраструктура банка и затраты на достижение соответствия будут в разы или даже в десятки раз выше. В данном случае консультанты могут помочь с идентификацией ресурсов, к которым будут применяться требования стандарта, документированием логических схем движения данных держателей платежных карт, правильной логической и сетевой сегментацией, а также с документированием границ аудита.

После этих подготовительных процедур компания может планировать бюджеты на выполнение работ по всему спектру требований стандарта, имея некоторую гарантию того, что эти бюджеты не придется впоследствии существенно пересматривать. Если при этом компания попадает под требования ежегодного обязательного прохождения аудита, то после определения границ его уже можно проходить, решая параллельно две задачи – выполнение требований регулятора о прохождении аудита и определение всех несоответствий требованиям стандарта для разработки детального плана мероприятий по их устранению (Action Plan).

В Action Plan должны быть прописаны все выявленные несоответствия, а также способы и сроки их устранения. Зачастую компаниям непросто разобраться с тем, каким именно способом следует устранять те или иные несоответствия, т.к. каждое из них – это объект довольно глубокой оценки. Решить эту проблему можно с помощью специалистов компании-аудитора, которые, обладая должной компетенцией, смогут порекомендовать наиболее оптимальный способ устранения несоответствия, определив те области процессингового центра, где целесообразно внедрять определенные технические средства, а также порекомендовать, какие именно средства наилучшим образом смогут решить проблему. Результатам таких работ станут проработанные и задокументированные способы устранения несоответствий стандарту, в том числе, с описанием соответствующих технических решений. Также будут разработаны частные технические задания на реализацию этих решений и выбрано оборудование и/или программные средства. Таким образом, компания будет иметь на руках четкий и подробный план-график, в соответствии с которым все задействованные в проекте сотрудники и подразделения будут осуществлять работы по устранению несоответствий.

Более того, не исключена ситуация, когда выполнить все прописанные в Action

Plan задачи силами самой компании не представляется возможным в принципе. Причины могут быть самые различные: как нехватка квалифицированных специалистов, так и отсутствие должного опыта решения поставленных в Action Plan задач. Ниже мы приведем пару примеров реализации требований стандарта, которые часто вызывают затруднения, и где помощь сторонних консультантов может оказаться крайне полезной.

Проблемные области

Стандарт PCI DSS требует, чтобы на ресурсах, входящих в область его применения, был установлен только необходимый для осуществления бизнес-процессов программный функционал и доступны только необходимые сетевые сервисы. Также в стандарте сказано, что в рамках области аудита должны использоваться только безопасные протоколы (в том числе протоколы управления), а разрешенный действующими правилами фильтрации трафик должен является минимально достаточным для функционирования бизнес-процессов обработки данных держателей платежных карт. Для решения этих вопросов специалистами привлеченной консалтинговой структуры осуществляется идентификация всех открытых портов путем сканирования ресурсов компании-заказчика, определяются и доку-

ментируются минимально достаточный для работы функционал, сетевые сервисы и протоколы. В случае необходимости использования уязвимых протоколов разрабатываются и документируются компенсационные меры. Помимо этого, консультанты могут помочь разработать стандарты безопасной настройки ресурсов, попадающих в область действия стандарта (межсетевых экранов, сетевого оборудования, операционных систем, баз данных, рабочих станций), а также осуществить и протестировать выполненные настройки и их соответствие этим стандартам.

Кроме того, в зоне действия стандарта должна быть осуществлена регламентация и внедрение таких процессов управления информационной безопасностью, как: мониторинг событий ИБ и реагирование на инциденты, контроль технических уязвимостей, контроль эффективности защитных мер, контроль доступа, обучение и повышение осведомленности пер-

сонала компании по вопросам ИБ, управление изменениями и т. д. Следует отметить, что все эти процессы необходимо выстроить и задокументировать с учетом требований стандарта, причем они должны существовать не только на бумаге, но работать и исполняться на практике. Это означает, что формальная отписка в виде документа не обеспечит соответствие PCI DSS. А выстроить и запустить процесс управления ИБ – задача довольно непростая. Так, например, для реализации требований в рамках мониторинга событий информационной безопасности и реагирования на инциденты нужно как минимум: определить критерии выявления инцидентов ИБ для всех типов источников событий (критерии разрабатываются на основе анализа рисков); разработать и задокументировать регламент мониторинга событий ИБ и регламент реагирования на инциденты; обучить сотрудников, протестировать разработанный

план реагирования на инциденты, а также внедрить и настроить в соответствии с документацией систему сбора, обработки и анализа событий ИБ. Как можно убедиться, все это – весьма сложные задачи для самостоятельной проработки, а таких процессов придется выстроить не один.

Также помощь опытных консультантов и аудиторов крайне полезна при проектировании компенсационных мер по снижению рисков, которые возникают при невозможности выполнения того или иного требования стандарта. Точная идентификация оставшихся рисков, разработка минимально достаточного комплекса мер по их снижению, а также документирование всего этого в соответствии с требованиями стандарта являются не всегда тривиальной задачей. А для выполнения таких требований PCI DSS как, например, обязательное шифрование данных держателей платежных карт при их хранении, в том числе в базах данных, иных вариантов, помимо применения компенсационных мер, на текущий момент, практически не существует.

В заключение – пара слов о контроле устранения несоответствий и выполнении требований PCI DSS. Огромным плюсом привлечения консультантов консалтинговой компании, сертифицированной на проведение аудита по PCI DSS является, безусловно, и то, что ее специалисты будут контролировать исполнение всех пунктов плана устранения несоответствий на всем его жизненном цикле, фиксируя в отчете «закрытие» всех выявленных на аудите проблемных зон.

К сожалению, в данной статье мы смогли привести лишь несколько примеров того, каким образом можно оптимизировать затраты на построение системы защиты процессинга, а также обеспечить выполнение требований стандарта PCI DSS. Проблематика достижения соответствия требованиям PCI DSS довольно обширная и глубокая. Поэтому мы в дальнейшем будем продолжать шаг за шагом раскрывать ее наиболее интересные аспекты на страницах журнала «ПЛАС».

ПЛАС

