

## Все, что вы хотели знать о PCI DSS, но боялись спросить

18.02.2009

*У специалистов по карточной безопасности в последнее время возникает все больше вопросов, касающихся внедрения требований стандарта PCI DSS. В частности, задается много вопросов о практике проведения QSA-аудита, а также тонкостей теста на проникновение.*

*Антон Карпов, QSA-аудитор Digital Security*

Любой внешний аудит, проводящийся в компании, обычно ассоциируется у сотрудников этой компании, задействованных в процедуре аудита, с чем-то тяжелым и очень нервным. И действительно: приходят сторонние аудиторы «в белых перчатках», запускают свои глаза и руки в самые основы функционирования инфраструктуры и бизнес-процессов, да и еще много вопросов задают: попробуй не ответить. В случае с PCI DSS эти опасения тем более ожидаемы, ведь стандарт выдвигает ряд довольно конкретных требований к инфраструктуре, в которой передается, обрабатывается или хранится информация о платежных картах и в случае несоответствия хотя бы одного пункта стандарта реальному положению вещей аудитор формально в праве поставить «незачет» по всему стандарту.

Однако, как это часто бывает, не так страшен черт, как его малюют. Международные платежные системы (МПС) в российском регионе пока что требуют под страхом штрафа лишь сам факт прохождения аудита, а не полного соответствия требованиям стандарта PCI DSS. А ряд простых рекомендаций и замечаний, приведенных ниже, помогут компаниям подойти к встрече с QSA-аудиторами максимально подготовленными, заработав минимум «штрафных баллов» за несоответствие и уменьшив, тем самым, список пунктов Плана Мероприятий (Action Plan) на будущий год.

### Сегментация сети и область аудита

Стандарт PCI DSS выдвигает достаточно жесткие требования к защищенности компонентов информационной инфраструктуры компании. Однако следует помнить, что все они относятся только к тем из них, которые входят в область аудита (scope), т.е. «системам, хранящим, передающим или обрабатывающим критичную информацию о платежных картах, а также системам и сетям, имеющим с ними сетевую связь». Компании нередко недооценивают важность выделения области аудита. Вкупе с частым недопониманием того, что имеется в виду под «сетевой связью» (здесь стандарт подразумевает все соединения, не фильтруемые межсетевыми экранами), в область аудита может попасть вся сеть компании. Однако зачастую бывает ситуация, что в процессинге используется одно-два специализированных приложения, с которыми работает буквально несколько человек. В таком случае гораздо проще и эффективнее реорганизовать сеть компании таким образом, чтобы платежные приложения и работающие с ними клиенты были выделены в отдельную логическую подсеть (например, путем выделения отдельного VLAN на коммутаторе), с жестко прописанными

списками контроля доступа в остальные сегменты сети компании. Да и вообще, приведение всей сетевой инфраструктуры к довольно жестким требованиям пунктов стандарта PCI DSS может потребовать значительных усилий, поэтому первое, что рекомендуется как самим стандартом, так и здравым смыслом – это выделить область аудита путем выполнения адекватной сегментации.

## Настройки безопасности информационных систем

Еще один момент, на котором часто «прокальваются» — это конфигурация информационных систем, входящих в область аудита, в первую очередь, конечно, серверов. Своевременная установка обновлений безопасности и регулярное обновление баз антивирусного ПО, разумеется, являются теми требованиями PCI DSS, выполнение которых уже давно вошло в норму в большинстве компаний. Однако в части конфигурации серверных систем стандарт выдвигает более жесткие требования. Так, ряд требований пункта 2.2 говорит о том, что все неиспользуемые или потенциально небезопасные службы и функции должны быть отключены, для удаленного административного доступа следует использовать только протоколы, обеспечивающие передачу аутентификационных данных в зашифрованном виде, а в системных скриптах или конфигурационных файлах не должно храниться никакой критичной информации вроде логинов и паролей.

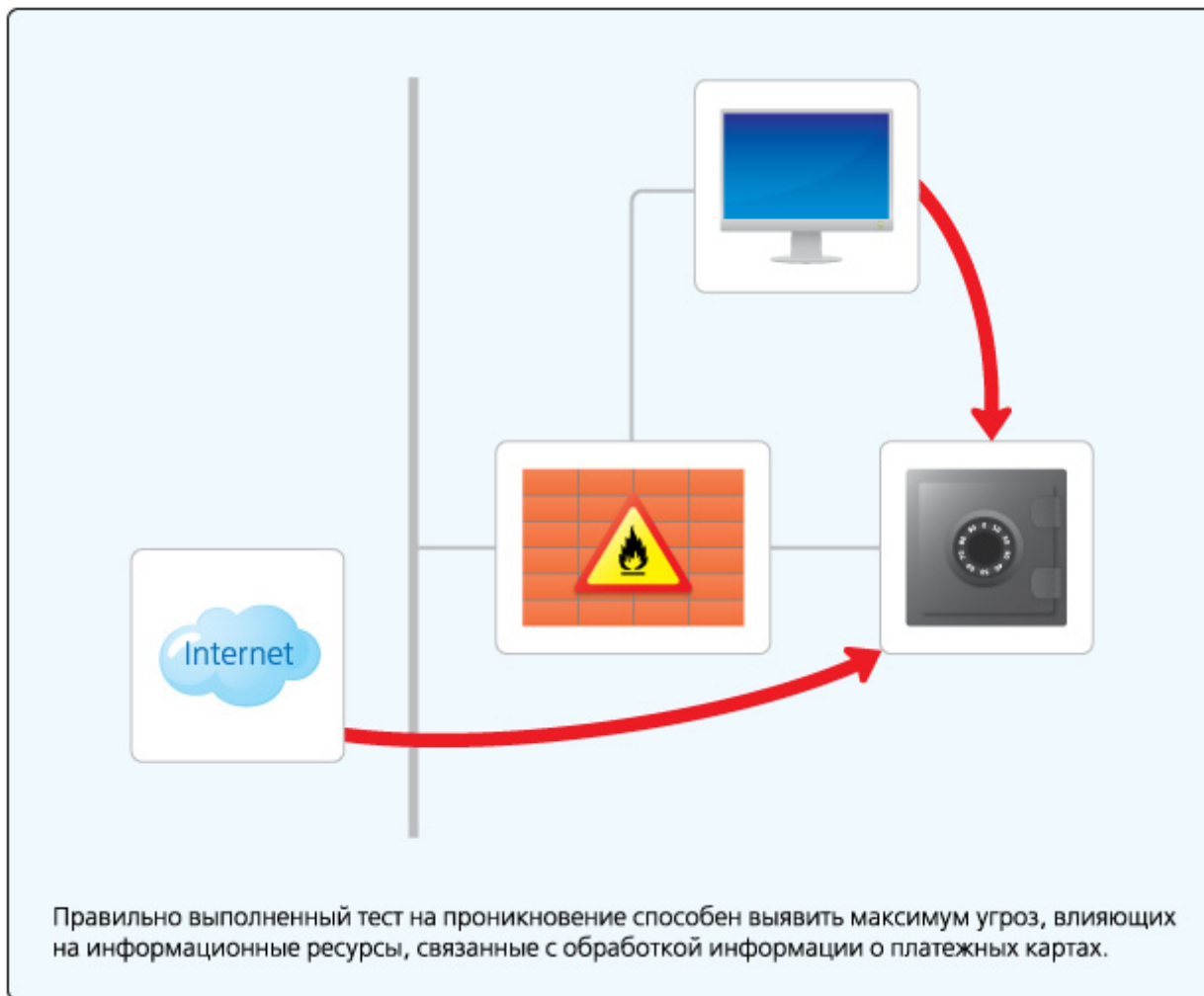
Спросите своего системного администратора, достаточно ли безопасный протокол он использует для удаленного администрирования серверов, и получите ответ, что, конечно же, это ssh для UNIX-серверов или RDP для серверов Windows. Однако попросите убедиться, что на UNIX-сервере при этом в списке запущенных процессов отсутствует telnetd, сетевые службы NFS (ваш администратор использует NFS для чего-нибудь?) или, например, службы печати lpd (вряд ли сервер СУБД используется для вывода чего-либо на принтер). В случае Windows-сервера проверьте, например, что службы uPnP или удаленного доступа к реестру отключены. Вероятно, вы будете сильно удивлены. Вежливо попросите своего системного администратора убрать «все лишнее» - возможно, QSA-аудиторы не будут столь благосклонны.

## Тест на проникновение

Согласно требованию 11.3 стандарта PCI DSS, 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). Тест на проникновение позволяет оценить реальный уровень защищенности информационных ресурсов компании, как с точки зрения внешнего злоумышленника, так и с позиции злонамеренного сотрудника компании (инсайдера).

Этому требованию стандарта почему-то традиционно уделяют минимум внимания, часто путая тест на проникновение с обычным сканированием внешнего периметра сканерами безопасности, к которому иногда добавляется попытка проникновения в сеть компании с использованием методов социальной инженерии (почтовая рассылка потенциально вредоносного ПО). Однако еще в апреле 2008 года регулирующий орган PCI Security Standards Council (SSC) выпустил объяснительный документ-комментарий к пункту 11.3 стандарта под названием «Information Supplement: Requirement 11.3 Penetration Testing». В этом документе отдельно подчеркивается различие между тестом на

проникновение и сканированием сети с использованием сканеров уязвимостей. Сканирование не является достаточной мерой и его проведение не может являться выполнением требований пункта 11.3 стандарта. Кроме того, в документе описывается приблизительная методология и область теста на проникновения, отдельно указывается как необходимость проведения теста на проникновение из внешней сети (Интернет), так и аудит защищенности внутренних ресурсов, связанных с карточной информацией, из локальной сети компании.



Стоит отметить, что грамотно выполненный тест на проникновение, как из сети Интернет, так и внутренний активный аудит защищенности, помимо того, что является единственной возможностью корректно выполнить требование пункта 11.3 стандарта PCI DSS, как ничто другое поможет детально выявить реальные уязвимости, присутствующие в сети компании и могущие стать причиной утечки конфиденциальной информации о платежных картах. Выполнение рекомендаций и устранение уязвимостей по результатам сделанного «по всем правилам» теста на проникновения и внутреннего активного аудита защищенности сети компании существенно повысит общий уровень защищенности информационной инфраструктуры, а значит, приблизит компанию к успешному прохождению аудита PCI DSS. Вот почему PCI SSC уделяет этому моменту так много внимания.

## Мониторинг и тестирование информационной инфраструктуры

Разделы 10 и 11 стандарта PCI DSS целиком посвящены вопросам мониторинга и тестирования компонентов информационной инфраструктуры, входящим в область аудита. Это еще один важный момент, которому неспроста уделяется много внимания. Из канонических вопросов безопасности все обычно помнят только о самом главном: «что делать, чтобы нас не взломали» (что, на самом деле, должно читаться как «что делать, чтобы взломать нас было весьма трудно»). Однако мало кто помнит о втором, не менее важном: «что делать, если нас все-таки взломали». Зачастую (и это не относится исключительно к PCI DSS) компании считают, что у них не происходит инцидентов только потому, что нет никакой возможности эти инциденты отследить. Вот почему стандарт PCI DSS требует, чтобы была развернута централизованная система протоколирования событий (лог-сервер), изменения в конфигурации систем (в том числе нарушение целостности журналов регистрации событий) генерировали системные уведомления администратору, а в сети была развернута и должным образом сконфигурирована система обнаружения и предотвращения вторжений (IDS/IPS).

Просто представьте, что в вашу сеть проникли злоумышленники. Задайте себе вопрос, как вы сможете отследить их проникновение. Смогут ли они модифицировать журналы регистрации событий на взломанном сервере? Смогут ли они незаметно передать украденную информацию через ваши сетевые устройства на внешний хост в Интернете? Ответив на эти вопросы, вы не только лучше поймете требования стандарта PCI DSS, но и значительно повысите уровень защищенности своей сети.

## Сопроводительная документация

Немаловажный вопрос, который фактически охватывает все требования стандарта – это наличие базы нормативных документов, регламентирующих администрирование инфраструктуры и обеспечение информационной безопасности. Всем известно, что безопасность – это непрерывный процесс, а налаженный процесс невозможен без наличия документированных процедур и свидетельствующих об их корректном выполнении записей.

Политика информационной безопасности компании, стандарты конфигурации системных компонентов, документированные процедуры безопасности, регулярно тестируемые планы реагирования на инциденты – вот минимальный набор документов, который сможет убедить аудитора в наличии системного подхода к обеспечению безопасности информации о платежных картах.

Любое действие, способное повлиять на защищенность инфраструктуры, будь то предоставление пользователю доступа к данным, внесение изменений в конфигурацию сети или же установка обновления программного обеспечения, должно выполняться в соответствии с регламентом, и оставлять документальный след – заявку о предоставлении доступа, запись в журнале изменений или электронном лог-файле.

## Заключение

В этой статье были охвачены лишь основные моменты, на которые следует обратить внимание при подготовке к аудиту PCI DSS. Не стоит бояться, ожидая на пороге QSA-аудиторов, вооруженных ручками и бумагой. В конце концов, цель хорошего аудитора – не поставить жирный минус напротив как можно большего количества требований стандарта, а помочь вам сделать вашу сеть защищеннее.

## 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.