

Стандарт PCI DSS

В последние годы по всему миру участились случаи взлома банковских информационных систем, а также факты мошенничества и кражи данных держателей карточек. Подобная нездоровая тенденция стала одной из главных причин, побудивших международные платежные системы объединить свои усилия и принять дополнительные меры для защиты своих клиентов. В этих целях в 2004 г. был разработан единый набор требований к безопасности данных — Payment Card Industry Data Security Standard (PCI DSS), объединивший в себе требования ряда программ по безопасности таких платежных систем, как Visa Int., MasterCard, American Express, Discover Card и JCB. Впоследствии, в сентябре 2006 г. для развития и продвижения стандарта PCI DSS был создан специальный Совет по безопасности — PCI Security Standards Council (www.pcisecuritystandards.com). Основными функциями Совета по безопасности являются: разработка и публикация стандартов PCI и всей сопутствующей документации; определение требований к компаниям, планирующим получить сертификацию для проведения аудитов по PCI DSS (QSA) и сканирования (ASV); осуществление этой сертификации; проведение обучающих тренингов для будущих QSA-аудиторов, а также контроль качества проведенных

аудиторами работ. В свою очередь международные платежные системы принимают отчетность по результатам аудитов и оценивают работу QSA.

Сферы применения PCI DSS

Действие стандарта PCI DSS распространяется на все торгово-сервисные предприятия (merchants) и поставщиков услуг (service providers), которые работают с международными платежными системами, т. е. на всех тех, кто передает, обрабатывает и хранит данные держателей карточек. В таблице ниже проиллюстрированы различные типы данных и требования к ним, которые выдвигает PCI DSS.

В зависимости от количества обрабатываемых транзакций каждой платежной системой компании присваивается определенный уровень с соответствующим набором требований, которые должны выполняться в обязательном порядке. Это может быть ежегодное прохождение аудита, ежеквартальные сканирования сети или ежегодное заполнение листа самооценки (Self Assessment Questionnaire — специальная анкета, разработанная PCI SSC для самооценки компаний).

Аудит на соответствие требованиям PCI DSS

Процедура аудита является обязательной для компаний, которые по-



Максим Эмм
Директор
департамента
аудита компании
«Информзащита»



**Наталья
Зосимовская**
Ведущий
специалист
компании
«Информзащита»

дают под Уровень 1, и должна проводиться ежегодно.

В область проверки сертификационного аудита входят прикладные и инфраструктурные информационные системы, обеспечивающие передачу, хранение или обработку данных платежных карточек в рамках следующих процессов:

- авторизация платежных карточек (все поддерживаемые виды);
- клиринг/сеттлмент с международными платежными системами Visa и MasterCard;
- поддержка пользователей данных платежных карточек.

Каждый этап сертификационного аудита включает в себя определенный перечень работ, различающихся по длительности и трудоемкости.

Этап 1. Подготовка и планирование аудита. На данном этапе выполняются следующие работы:

Таблица

	Данные	Хранение разрешено?	Требуется защита?	Требование 3.4 стандарта PCI DSS
Данные держателей карточек	Номер PAN	ДА	ДА	ДА
	Имя держателя карточки *	ДА	ДА	НЕТ
	Код обслуживания *	ДА	ДА	НЕТ
	Дата истечения срока действия *	ДА	ДА	НЕТ
Критичные данные авторизации (sensitive authentication data)**	Полное содержание магнитной полосы	НЕТ	—	—
	Коды CVC2/CVV2/CID	НЕТ	—	—
	ПИН / ПИН-блок	НЕТ	—	—

* Эти данные должны защищаться, если они хранятся вместе с номером PAN.

** Не должны храниться после прохождения процедуры авторизации (даже если они зашифрованы).



- получение от клиента и анализ необходимых документов и других исходных данных;

- определение области проверки, состава ресурсов сегмента обработки платежных карточек, а также задействованных подразделений;

- планирование и согласование времени проведения проверок, задействованных в них сотрудников компании для минимизации воздействия на бизнес-процессы клиента.

Этап 2. Проведение проверок согласно утвержденным процедурам аудита. На данном этапе осуществляются:

- сбор информации по техническим проверкам;

- анализ информации по техническим проверкам;

- сбор и анализ информации для процессных проверок.

Этап 3. Анализ результатов, формирование предварительного Отчета о соответствии (Report On Compliance). Эти действия предусматривают:

- обобщение и компоновку результатов;

- контроль результатов выполнения проверок;

- формирование предварительного Отчета о соответствии.

Этап 4. Презентация клиенту предварительного Отчета о соответствии включает:

- представление клиенту обобщенных результатов аудита;

- представление всех выявленных слабых мест в применяемых защитных мерах, а также способов устранения недостатков;

- ответы на вопросы клиента о проведенных проверках;

- согласование спорных вопросов.

Этап 5. Согласование с клиентом и формирование окончательного Отчета (на русском языке):

- окончательное оформление Отчета, корректировка формулировок, контроль ссылок на свидетельства аудита;

- выработка рекомендаций, формирование плана действий (Action Plan).

Этап 6. Уведомление международных платежных систем (МПС) о результатах аудита:

- в случае полного соответствия клиента требованиям PCI DSS в МПС отправляется заключение о результатах проведения аудита — Attestation of Compliance (на английском языке);

- в случае выявления несоответствия требованиям PCI DSS производит-

ся отправка МПС предоставленного и согласованного с клиентом Action Plan.

По результатам аудита подготавливаются отчеты:

- Report on Compliance (Отчет о соответствии);

- Attestation of Compliance (Подтверждение соответствия¹).

Attestation of Compliance направляется в международные платежные системы и содержит общий статус выполнения требований Стандарта банком.

Отчет Report on Compliance представляется банку. Данный отчет содержит общее описание бизнеса компании, описание области проверки и другие сведения в соответствии с официальными процедурами оценки по стандарту PCI DSS 1.2². Кроме того, по каждому из проверяемых требований Стандарта отчет содержит следующую информацию:

- мнение аудитора о том, в полном ли объеме выполнено формально проверяемое требование (In place / Not in place);

- описание способов, которые использовались для проверки требования;

- описание выборки, на которой было проверено это требование;

- в случае если требование не выполнено, дается четкое описание, в какой именно части реализация функции защиты не соответствует требованиям Стандарта.

Основные несоответствия стандарту PCI DSS

Многие вопросы безопасности в компаниях решаются в соответствии с исторически сложившимися практиками, которые не всегда соответствуют требованиям стандарта PCI DSS или даже внутренней политике безопасности компании. Ниже мы привели список наиболее часто встречающихся несоответствий требованиям Стандарта в порядке убывания рисков.

1. Авторизационные данные хранятся в журналах транзакций ATM, POS и т. д.

2. Не определена политика хранения данных, т. е. нет четкой инструкции, где и какие данные платежных карточек хранить и когда их нужно удалять.

¹ В случае полного соответствия PCI DSS.

² PCI DSS Requirements and Security Assessment Procedures 1.2.

3. Не стандартизированы настройки операционных систем и приложений, в том числе с точки зрения обеспечения безопасности.

4. Не устанавливаются вообще или устанавливаются несвоевременно обновления безопасности на серверы процессинга.

5. Регистрация событий не рассматривается как источник информации для мониторинга безопасности и расследования инцидентов.

6. Необходимые для ведения бизнеса сетевые протоколы и политики межсетевое экранирования не задокументированы.

7. Внутреннее сканирование уязвимостей сетевых устройств не проводится.

8. Не обеспечивается должным образом контроль целостности приложений и операционных систем серверов.

9. Если есть собственная разработка ПО, она ничем не регламентирована, и разработчики всегда поддерживают продукционную систему как наиболее компетентные специалисты.

10. Парольная политика применяется в основном только в доменах Windows. На Unix-серверах, базах данных и приложениях парольная политика применяется крайне редко.

11. Обучение рядовых сотрудников в части информационной безопасности недостаточно.

Оценка защищенности

В рамках требования PCI DSS к оценке защищенности можно отнести проведение ежеквартальных сканирований сети и ежегодный тест на проникновение. Сканирование сети нужно проводить ежеквартально (или при любом существенном изменении сетевой инфраструктуры) с привлечением сторонней компании, имеющей сертификат на проведение данных работ и статус Approved Scanning Vendor (ASV). Процесс сканирования регламентирован и проводится в соответствии с PCI DSS Security Scanning Procedures и PCI DSS Technical and Operational Requirements for Approved Scanning Vendors.

Сканирование проводится через Интернет, и сканированию подлежат все публичные IP-адреса компании. К ним относятся:

- системы и сервисы, непосредственно участвующие в обработке данных платежных карточек (например,

сайты e-commerce, платежные шлюзы и т. д.);

- системы и сервисы, компрометация которых может повысить риск компрометации данных платежных карточек (например, электронная почта, DNS и т. д.).

Указанное сканирование не стоит путать с обычным «внешним» сканированием, которое в качестве услуги предлагают большое количество компаний. Особенность сканирования в рамках PCI DSS состоит в том, что оно проводится сертифицированной компанией — ASV — в четком соответствии с требованиями процедур сканирования и направлено на определение соответствия именно требованиям PCI DSS.

Тест на проникновение компании обязаны проводить ежегодно, как на сетевом, так и на прикладном уровне. Тест представляет собой имитацию действий злоумышленника, пытающегося проникнуть в сеть компании и

получить данные платежных карточек и/или взять под свой контроль управление системами, где обрабатываются, передаются или хранятся данные платежных карточек.

Для прохождения теста на проникновение можно привлечь любую стороннюю компанию, обладающую необходимой компетенцией, или выполнить его самостоятельно, но для этого сотрудники компании должны иметь соответствующий опыт и квалификацию.

По результатам теста составляется отчет, содержащий описание методики проведения работ, перечень выявленных уязвимостей и рисков, а также рекомендации по снижению данных рисков. В отчете также описывается ход работ, т. е. все те действия, которые были предприняты, и их результаты.

Проводя регулярные тесты на проникновение и ежеквартальные сканирования сети, компания не только выполняет обязательные требования

стандарта PCI DSS, но и получает объективную оценку защищенности своих структур от внешних злоумышленников, действующих через сеть Интернет, и от действий квалифицированных инсайдеров, имеющих возможность подключения к локальной сети. Кроме того, используя представленные рекомендации, компания сможет повысить общий уровень защищенности сети от наиболее вероятных атак.

Закключение

Хотелось бы отметить, что компаниям, в которых процессы управления ИТ и ИТ-безопасностью реализованы в соответствии с ITIL, COBIT и другими современными стандартами, намного проще выполнить все требования PCI DSS, нежели компаниям, где исторически всей автоматизацией и безопасностью процессинга управляли несколько человек, не документируя свою деятельность. □

Продукты

Новости

Fujitsu Siemens Computers и VMware выпустили совместное решение для работы с приложениями SAP

24 февраля 2009 г. компании Fujitsu Siemens Computers и VMware объявили о совместном решении, которое гарантирует высокое качество обслуживания приложений SAP. Разработанная компанией Fujitsu Siemens Computers новая версия FlexFrame for SAP объединяет VMware Infrastructure, инфраструктуру физического и виртуального центра обработки данных, виртуализированные сети, системы хранения данных и комплексные сервисы в одно законченное и экономически выгодное ИТ-решение.

Среди преимуществ таких интегрированных решений, как FlexFrame for SAP, — легкое и быстрое развертывание, высокое качество обслуживания, повышенная эффективность использования инфраструктуры. Динамически назначая физические или виртуальные серверы приложениям SAP, FlexFrame for SAP обеспечивает оптимальное распределение ресурсов, что позволяет максимально повысить качество обслуживания и

гарантировать удобство пользователей при минимально возможной стоимости инфраструктуры. FlexFrame for SAP увеличивает время безотказной работы приложений, автоматически перезапуская приложения на любой доступной системе — виртуальной или физической — в случае отказа оборудования, а также производит мониторинг всех компонентов приложения SAP и автоматически запускает восстановление в случае отказа.

Как сказал Дитер Герцог (Dieter Herzog), исполнительный вице-президент Fujitsu Siemens Computers, руководитель подразделения технологических решений, «добавление полной поддержки виртуализации стало очередной главой в истории успеха FlexFrame for SAP. С момента своего выпуска данное решение стало сильнее и сильнее, и это подтверждается более чем 200 внедрениями у заказчиков. Теперь, поддерживая VMware Infrastructure, мы помогаем клиентам SAP достичь

нового уровня консолидации серверов и систем хранения».

По словам Брайана Бьюна (Bryan Buun), вице-президента по работе с глобальными альянсами VMware, «со встроенными сервисами Application vServices, такими как VMware High Availability и VMotionTM, VMware Infrastructure сочетает в себе выдающуюся производительность и надежность, сохраняя при этом невысокий уровень расходов на содержание инфраструктуры. Именно поэтому, согласно опросам заказчиков компании, 94% клиентов VMware, развернувших VMware Infrastructure, используют ее в режиме продуктивной эксплуатации. Решения SAP являются критически важными для заказчиков VMware, и руководство компании радо объединению усилий с Fujitsu Siemens Computers для создания гибкого, отказоустойчивого и легкоуправляемого ИТ-решения, которое упрощает виртуализацию приложений SAP и предоставляет заказчикам идеальную платформу». □