М. В. Кузин

PCI DSS: СТАНДАРТ БЕЗОПАСНОСТИ И РЕАЛЬНАЯ БЕЗОПАСНОСТЬ

Безопасность платежных карт на современном этапе

В 2011 г. компания Verizon Business опубликовала очередной отчет о компрометации данных «2011 Data Breach Investigations Report». В основу исследования, проведенного подразделением Verizon RISK Team во взаимодействии с Secret Service США, легли данные за последние 7 лет о более чем 919 млн. скомпрометированных элементов данных в результате подтвержденного взлома около 1000 информационных систем [1].

Основные выводы данного исследования по фактам компрометации данных в 2010 г. следующие:

- скомпрометированы 3,88 млн. элементов данных;
- подавляющее большинство (96 %) скомпрометированных данных относится к данным платежных карт;
- 43 % атак не требовали никаких специальных инструментов для взлома, еще 49 % были связаны с использованием определенных методов и средств, и лишь в 8 % случаев применялись специальные знания и существенные вычислительные ресурсы;
- 89 % организаций, обрабатывающих и хранящих данные платежных карт, на момент взлома не соответствовали требованиям стандарта безопасности данных индустрии платежных карт PCI DSS (Payment Card Industry Data Security Standard — далее Стандарт), а 11 % соответствовали.

Результаты других исследований и проведенных расследований также подтверждают современные проблемы безопасности индустрии платежных карт. Так, в 2005 г. в результате взлома процессингового центра Card Systems Solutions было скомпрометировано 40 млн. платежных карт. Компания необоснованно хранила треки (данные магнитных полос карт) и при этом не защищала их должным образом, в результате международные платежные системы Visa и Amex отозвали свои лицензии. В 2007 г. хакеры похитили 45 млн. записей с данными платежных карт в результате атаки на крупную розничную сеть TJX. В 2008 г. был взломан RBS Worldpay, что привело к компрометации данных 1,5 млн. держателей карт. А в 2009 г. злоумышленники получили доступ к более чем 100 млн. платежных карт в результате взлома процессингового центра Heartland Payment Systems [2].

Очевидно, что данные факты свидетельствуют о существенных уязвимостях применяемых в настоящее время платежных технологий, раз такие массовые атаки и случаи компрометации данных становятся возможны из года в год. Принципиальных решений в связи с этим может быть два:

1. замена уязвимых технологий более безопасными;
2. сохранение существующих уязвимых технологий и защита их дополнительными методами и системами.

Первый путь связан с миграцией на микропроцессорные карты стандарта EMV для предотвращения несанкционированного копирования (скимминга) магнитной полосы карты и посредством внедрения более надежных систем аутентификации держателя карты при проведении операций без присутствия карты, причем в последнем случае в ряде решений также может использоваться EMV-карта. Повсеместного перехода на микропроцессорные карты до сих пор не произошло. США до настоящего момента не были вовлечены в процесс миграции на микропроцессорные карты, но летом 2011 г. ситуация изменилась. Международная платежная система Visa установила для эквайреров и торгово-сервисных предприятий в США обязательства по обеспечению принятия EMV-карт к оплате для торгово-сервисных предприятий с 1 октября

2012 г., для процессинговых центров — с 1 апреля 2013 г. [3]. Тем не менее о полном отказе от платежных карт на основе магнитной полосы пока не говорится, и крупнейшие международные платежные системы пока не установили никаких сроков и временных ограничений.

Второй путь состоит в защите существующих уязвимых технологий (прежде всего платежных карт с магнитной полосой). Для разработки повышенных требований к обеспечению безопасности данных платежных карт в 2006 г. был создан специальный Совет стандартов безопасности индустрии платежных карт (Payment Card Industry Security Standards Council), в который вошли American Express, Discover Financial Services, JCB, MasterCard Worldwide, Visa International. Стандарт (в настоящий момент версия 2.0) определяет требования безопасности для защиты информации, относящейся к платежной карте, и должен использоваться тогда, когда номер карты хранится, обрабатывается или передается.

Стандарт безопасности PCI DSS — основные требования

Стандарт устанавливает требования по следующим шести категориям [4]:

1. построение и обеспечение безопасности сети;
2. защита данных о держателях карт;
3. обеспечение программы менеджмента уязвимостей;
4. реализация строгих механизмов контроля доступа;
5. регулярный мониторинг и тестирование сетей;
6. обеспечение политики информационной безопасности.

Всего определяется двенадцать основных требований по всем категориям:

- установить и поддерживать конфигурацию межсетевого экранирования;
- не использовать пароли и другие параметры безопасности, определяемые поставщиками по умолчанию;
- защищать хранимые данные;
- шифровать передаваемые данные о держателях карт по открытым каналам;
- использовать и регулярно обновлять антивирусное ПО;
- разрабатывать и поддерживать безопасные системы и приложения;
- ограничивать доступ к данным на основе принципа необходимого знания;
- назначить уникальный идентификатор каждому субъекту доступа к информации;
- ограничить физический доступ к данным о держателях карт;
- осуществлять мониторинг доступа к сетевым ресурсам и данным о держателях карт;
- регулярно тестировать системы и процессы безопасности;
- поддерживать политику информационной безопасности.

Приведенные в Стандарте требования призваны обеспечить безопасность данных платежных карт через повышение защищенности автоматизированных систем, в которых эти данные обрабатываются. Соответствие требованиям Стандарта должно означать, что система защищена и компрометации данных в ней произойти не может. Однако вышеназванные компании, в которых были скомпрометированы данные, — Card Systems Solutions, RBS WorldPay, Heartland Payment Systems — до этого проходили аудит и получили статус соответствия Стандарту. Примечательно, что компании RBS WorldPay и Heartland Payment Systems в марте 2009 г. были исключены Visa из списка соответствующих стандарту, но сразу же заявили, что надеются вновь пройти сертификацию уже в апреле и мае 2009 г. — и достигли этого соответствия.

Стандарт безопасности = реальная безопасность?

По определению Международной организации по стандартизации (ИСО) *стандартизация* — это *установление и применение правил* с целью упорядочения деятельности в определенных

областях на пользу и при участии всех заинтересованных сторон, в частности *для достижения всеобщей оптимальной экономии* при соблюдении функциональных условий и требований техники безопасности [5]. Стандарты информационной безопасности призваны обеспечить поддержание желаемых свойств информации, связанных с ее безопасностью, учетом экономической обоснованности и рациональности защиты. С одной стороны, при нарушении требуемых свойств информации наносится некоторый ущерб, с другой — обеспечение защиты информации сопряжено с расходованием средств [6]. Очевидно, требования любого стандарта в области информационной безопасности, в том числе и Стандарта PCI DSS, также процедуры и процессы реализации его требований должны быть рациональными, экономически обоснованными. К настоящему времени практика внедрения Стандарта имеет определенную историю, которая заслуживает особого рассмотрения и анализа.

С учетом приведенных выше фактов взлома крупных процессинговых центров, несмотря на то что формально эти организации соответствовали требованиям Стандарта, возникает ряд вопросов:

- способен ли Стандарт обеспечить безопасность платежных карт?
- почему его внедрение не приводит к уменьшению числа компрометаций и объема скомпрометированных данных?

Эти вопросы волнуют в настоящий момент всех специалистов по безопасности в отрасли, они же явились предметом особого рассмотрения в Комитете национальной безопасности Палаты представителей США (House of Representatives Committee on Homeland Security) 31 марта 2009 г. в слушаниях на тему «Приводят ли Стандарты безопасности индустрии платежных карт к снижению киберпреступности?» («Do the PCI Standards Reduce Cybercrime?») [7].

Позиция представителей PCI SSC и Visa на упомянутых слушаниях заключалась в том, что сертифицированная на соответствие требованиям Стандарта организация соответствует этим требованиям на момент сертификации, но в дальнейшем нельзя гарантировать, что это соответствие сохраняется. При этом после успешного взлома ранее сертифицированных организаций во всех случаях аудит показал, что организация уже не соответствует требованиям безопасности. Представители торговых компаний отметили, что следование требованиям Стандарта вовсе не приводит к состоянию уверенности в безопасности данных держателей карт, при этом реализация требований на практике связана с существенными затратами. А поскольку данные платежных карт все равно должны быть обработаны, т. е. как минимум в этот момент они представляются в незашифрованном виде, то компрометация остается возможной. Кроме того, торговые компании США расценивают Стандарт как некую «заплатку» безопасности, целью которой является перенос потерь на торговые предприятия.

Председатель слушаний обозначила важную позицию — *отсутствие метрик эффективности Стандарта*, которые в принципе должны быть неотъемлемой его частью. Целью Стандарта является защита данных платежных карт. В случае если такая защита будет обеспечена, логично ожидать снижения киберпреступности, мошенничества с платежными картами — такое снижение может являться объективным измерителем эффективности Стандарта. Если же снижения числа преступлений и объема скомпрометированных данных платежных карт не происходит, очевидно, безопасность данных не обеспечивается.

В результате слушаний были сделаны два основных вывода:

1. Стандарт не является достаточным для защиты данных держателей карт, и следование его требованиям не обеспечивает в настоящий момент адекватной безопасности;

2. Стандарт скорее переносит бремя ответственности по мошенничеству, чем реально препятствует компрометации данных.

В результате слушаний выяснилось, что цели заинтересованных сторон различаются. Так, PCI SSC является организацией, обеспечивающей разработку Стандарта и необходимое обучение,

но не играющей роли в его адаптации и эволюции на основе практики применения, которая ей не контролируется. Целью платежной системы является продвижение Стандарта среди своих членов. Торговые предприятия стремятся расширить свой бизнес, предоставляя товары и услуги покупателям, и они не только не заинтересованы в реализации требований Стандарта, но и считают его инструментом давления со стороны платежных систем.

Особую озабоченность сертифицируемых на соответствие требованиям Стандарта организаций вызывает тот факт, что успешное прохождение сертификации не гарантирует реальной безопасности. На практике часто имеет место такой сценарий развития событий:

- торговое предприятие А проходит сертификацию на соответствие Стандарту, что подтверждается сертифицированным аудитором QSA (Qualified Security Assessor);
- через некоторое время торговое предприятие А признается точкой компрометации данных платежных карт после успешной атаки со стороны злоумышленников;
- PCI SSC выпускает поправки для аудиторов по процедурам проведения оценки на соответствие требованиям Стандарта по результатам данного инцидента;
- при проверке торгового предприятия А по новым процедурам оно уже не соответствует требованиям.

Практика внедрения Стандарта показала, что одного формулирования требований безопасности недостаточно. Внедрение требований, управление требованиями, учет практических аспектов оказались неэффективными, что и привело к ряду обозначившихся проблем. По результатам исследования, проведенного Society of Payment Security Professionals, почти 24 % организаций, участвовавших в исследовании, потратили более 100 тыс. долл. США в год на оценку и соответствие требованиям Стандарта. А торговые предприятия первого уровня (Level 1), по оценке подкомитета, могут столкнуться с необходимостью ежегодных затрат в 18 млн. долл. США на внедрение требований Стандарта, что превысит возможные потери от мошенничества [7]. Компания Gartner оценила в 2008 г. затраты для приведения автоматизированной системы к соответствию требованиям Стандарта: первый уровень — 2,7 млн. долл. США, второй уровень — 1,1 млн. долл. США, третий уровень — 155 тыс. долл. США. По оценке компании UCS (Россия), приведение системы к соответствию Стандарту составило 1 млн. долл. США, поддержание соответствия — еще 100 тыс. долл. США ежегодно. Только ежегодные обязательные затраты на проведение аудита, пентеста и четырех ежеквартальных сканирований составят около 1 млн. рублей [8].

Эти оценки свидетельствуют о том, что при условии, когда стоимость обеспечения безопасности превышает величину потерь от инцидентов, такая защита становится нецелесообразной. Организации, вынужденные тратить существенные средства для обеспечения соответствия требованиям Стандарта, будут включать данные затраты в себестоимость, что в конечном итоге скажется на держателях карт, иначе бизнес будет нерентабельным.

Недостатки и противоречия PCI DSS

Стандарт следует рассматривать относительно цели его создания как инструмент для защиты данных, а не последнюю линию защиты. Практика показывает, что следование Стандарту не обеспечивает достаточной защиты данных платежных карт. Кроме того, по результатам проведенного анализа можно сформулировать следующие принципиальные недостатки и противоречия Стандарта.

1. *Попытка сокрытия идентификатора (номера карты) принципиально невыполнима.* Безопасность доступа к счету карты не основывается на сокрытии идентификатора, а должна находиться в области усовершенствования процедур и средств аутентификации. Стандарт предназначен для тех организаций и процессов, в которых номер карты передается, обрабатывается или хранится. Номер карты предназначен для обеспечения соответствия счету держателя карты, т.е. является его идентификатором. Безопасность такого доступа обеспечивается процедурами

аутентификации держателя карты, которые должны препятствовать несанкционированному доступу к счету. Логично предположить, что для обеспечения безопасности доступа к счету, при наличии фактов несанкционированного использования карты как инструмента доступа, необходимо усовершенствовать процедуры аутентификации. Такое усовершенствование может включать в себя внедрение механизмов многофакторной аутентификации, например Chip&PIN, CAP-EMV. Однако Стандарт предполагает сокрытие идентификатора (номера карты) как обязательное условие обеспечения безопасности доступа. Очевидно, что принципиально невозможно отказаться от полного сокрытия идентификатора — для проведения транзакции по карте номер необходим, так как является идентификатором счета держателя карты. При современных технологиях платежных карт номер карты не относится к критически важным данным — проведение несанкционированной операции возможно либо при нарушении требований безопасности (хранение полного содержимого магнитной полосы карты и/или результатов криптографического преобразования ПИН-кодов — ПИН-блоков), либо при отставании от передовых технологий, таких как EMV и 3-D Secure.

2. *Стоимость реализации требований Стандарта может превысить величину потерь от нарушения безопасности защищаемых активов, что сделает такую защиту неэффективной и в принципе нецелесообразной*. Стоимость защиты должна быть приемлемой и как минимум не превышать убытков в случае ее отсутствия, однако таких оценок при разработке Стандарта не проводилось.

3. *Внедрение требований Стандарта* повлечет дополнительные затраты со стороны эквайреров и торговых предприятий, *что может привести к замедлению развития бизнеса*, если не к полной остановке (например, в российских условиях, где рентабельность и так невелика).

Реализацией мер по принуждению к прохождению процедур сертификации на соответствие Стандарту и выдачей сертификатов на его соответствие занимаются платежные системы. Процессинговые центры и эквайреры имеют договорные отношения с платежными системами и вследствие этого обязаны выполнять все требования Стандарта. Торговые предприятия членами платежных систем не являются, гражданско-правовые отношения они имеют только с эквайрерами. Поэтому ответственность за соответствие торговца требованиям Стандарта возложена на эквайрера, т. е. эквайрер считается соответствующим его требованиям, если все его торговцы прошли процедуры сертификации в платежных системах. Расходы на обеспечение соответствия требованиям могут состоять из затрат на проведение аудита, пентеста, ежеквартальных сканирований сети, мероприятий по приведению автоматизированной системы торговца в соответствие с требованиями, в том числе приобретение оборудования, программного обеспечения (соответствующего, помимо прочего, требованиям стандарта безопасности для платежных приложений PA-DSS), принятие в штат или обучение сотрудников.

4. *В РФ для банков существует ряд юридических аспектов, которые следует отметить*. По требованиям Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Стандарта Банка России СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», носящего в настоящее время рекомендательный характер, банки и так внедряют системы защиты данных в соответствии с этими требованиями, причем сами требования принципиально не отличаются от требований Стандарта. Это означает, что общая стоимость защиты различных используемых банком автоматизированных систем еще более возрастет, однако целесообразность этого не является бесспорной и достаточно обоснованной применительно к российским условиям.

5. *После успешного прохождения аудита на соответствие требованиям Стандарта компания, его прошедшая, не получает никаких гарантий безопасности ни от аудиторов, ни от платежных систем*. В случае же взлома такой компании в дальнейшем статус сертифицированной организации будет, как показывает практика, пересмотрен (отозван).

6. *В Стандарте нет метрик, позволяющих судить об эффективности применения его требований*. Организация может либо соответствовать Стандарту после прохождения аудита (compliance), либо не соответствовать.

7. Наконец, *платежные карты на основе магнитной полосы и традиционные платежи без присутствия карты* (с использованием только номера карты, срока действия и кода верификации карты CVC2/CVV2) *принципиально уязвимы ввиду уязвимости самих технологий*. В связи с этим обеспечить безопасность принципиально уязвимых технологий невозможно.

Выводы

Реализовывать требования Стандарта, очевидно, необходимо, поскольку он носит обязательный характер по требованиям международных платежных систем. Тем не менее как сам Стандарт, так и процедуры сертификации на соответствие его требованиям имеют ряд отмеченных недостатков, препятствующих достижению его основной цели — защиты данных платежных карт.

В связи с этим более перспективным является другой путь обеспечения безопасности, а именно не защита существующих уязвимых платежных технологий, требующая дополнительных инвестиций, а миграция на более современные и защищенные, включая EMV и 3-D Secure, на которые участниками рынка уже потрачены значительные средства.

СПИСОК ЛИТЕРАТУРЫ:

1. 2011 Data Breach Investigations Report. — Verizon Business. URL: http://verizononbusiness.com.
2. *Кузин М.* PCI DSS и реальная безопасность платежных карт // ПЛАС. 2010. Дайджест'2009. С. 16–18.
3. Visa leads U.S. towards EMV implementation. — European ATM Security Team (EAST). URL: http://www.european-atmsecurity.eu.
4. PCI DSS. — PCI Security Standards Council. URL: http://www.pcisecuritystandards.org.
5. International Organization for Standardization. URL: http://www.iso.org.
6. *Герасименко В. А., Малюк А. А.* Основы защиты информации. М.: МИФИ, 1997. — 537 с.
7. *Heather M.* An Analysis of the Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology: "Do the PCI Standards Reduce Cybercrime?". URL: http://www.paymentsecuritypros.com.
8. *Алексанов А. К., Демчев И. А., Доронин А. М. [и др.].* Безопасность карточного бизнеса: бизнес-энциклопедия. М.: Московская финансово-промышленная академия; ЦИПСиР, 2012. — 432 с.