PCI DSS

Проблемы Стандарта Безопасности Данных Индустрии Платёжных Карт

Пятиизбянцев Николай Петрович

Требования PCI DSS

3.2.1 Запрещается хранить полное содержимое дорожки (содержимое магнитной полосы, находящейся на обратной стороне карты, его аналог на чипе либо в ином месте). Эти данные также называются "полная дорожка", "дорожка", "дорожка 1", "дорожка 2" и "данные магнитной полосы".

Примечание: Для ведения бизнеса может быть необходимо хранение следующих элементов данных магнитной полосы:

- имя держателя карты;
- номер платежной карты (PAN);
- дата истечения срока действия карты;
- сервисный код.

Трек 2 – хранить нельзя!

5264832001000336=13011211665400000129

Хранить можно:

Трек 2 – хранить нельзя!

5264832001000336=13011211665400000129

Хранить можно:

номер карты: 5264832001000336

Трек 2 – хранить нельзя!

5264832001000336=13011211665400000129

Хранить можно:

номер карты: 5264832001000336

дату: 1301

Трек 2 – хранить нельзя!

5264832001000336=13011211665400000129

Хранить можно:

номер карты: 5264832001000336

дату: 1301

сервис код: 121

Трек 2 – хранить нельзя!

5264832001000336=13011211665400000129

Хранить можно:

номер карты: 5264832001000336

дату: 1301

сервис код: 121

индекс криптографического ключа: 1

Трек 2 – хранить нельзя!

5264832001000336=130112116654000000129

Хранить можно:

номер карты: 5264832001000336

дату: 1301

сервис код: 121

индекс криптографического ключа: 1

PVV: 6654

Трек 2 – хранить нельзя!

5264832001000336=13011211665400000129

Хранить можно:

номер карты: 5264832001000336

дату: 1301

сервис код: 121

индекс криптографического ключа: 1

PVV: 6654

CVC: 129

Трек 2 – хранить нельзя!

5264832001000336=13011211665400000129

Хранить можно:

5264832001000336=130112116654xxxxx129 ?

Payment Card Industry (PCI) Data Security Standard

Requirements and Security Assessment Procedures Version 3.0

3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.

Запрещается хранение персонального идентификационного номера (PIN), а также зашифрованного PIN-блока.

Payment Card Industry (PCI) PIN Security Requirements Version 1.0

PINs must not be stored except as part of a store-and-forward transaction, and only for the minimum time necessary. If a transaction is logged, the encrypted PIN block must be masked or deleted from the record before it is logged.

Если транзакция регистрируется, зашифрованный ПИН-блок перед записью должен маскироваться

Т.е. хранить можно? Какие требования к маскированию? Один символ достаточно?

Payment Card Industry (PCI) Data Security Standard

Requirements and Security Assessment Procedures Version 3.0

3.2.3 Запрещается хранение персонального идентификационного номера (PIN), а также зашифрованного PIN-блока.

ПОЯСНЕНИЕ:

Данные значения ДОЛЖНЫ быть известны только владельцу карты или банку, который выпустил карту. Если эти запрещенные данные будут храниться и будут украдены, злоумышленник получит возможность совершения мошеннических операций с использованием PIN-кода (например, для получения наличных через банкомат).

PINBLOCK – хранить нельзя (3.2.3 Запрещается хранение … зашифрованного PIN-блока)

Но, PVV - хранить можно (ver.1.0 – 3.2.3 Do not store the PIN Verification Value (PVV) - запрет)

PINBLOCK: блок 16 символов (ПИН+12 цифр номера карты) зашифрован 3DES на TPK/AWK/IWK двойной длины (32 символа)

PVV: блок 16 символов (ПИН+ 11 цифр номера карты) зашифрован DES на PVKA (16 символов), расшифрован DES на PVKB (16 символов), зашифрован DES на PVKA (16 символов)=>децимализация

Компрометация TPK/AWK/IWK => компрометация ПИН (эмиссия+эквайринг)

Компрометация PVKA+PVKB => компрометация ПИН (эмиссия)

Требования по безопасному управлению ПИН-кодами индустрии платежных карт (PCI PIN Security Requirements)

ПИН–коды шифруемые только для передачи между устройством ввода ПИН-кода и считывателем карт должны использовать один из форматов ПИН-блока, указанного в ISO 9564. Там, где применяется формат 2, должен использоваться метод уникального ключа на каждую транзакцию в соответствии с ISO 11568. Формат 2 должен использоваться только в связи с офлайновой верификацией ПИН-кода или для операции по смене ПИН-кода в связи со средой смарт-карты.

Смена ПИН-кода держателем по технологии EMV

необходимо использовать (разрешить) на HSM формат ПИН-блока 34(Thales)/2(ISO), который является небезопасным: одинаковые ПИН-коды дают одинаковые ПИН-блоки на идентичных ключах.

При инсайде можно посылать на HSM хостовые команды (KU или KY) и перешифровать ПИН-блок из формата 0(ISO) в формат 2(ISO). Далее злоумышленник сохраняет полученные ПИН-блоки формата 2 и путем их сравнения, находит ПИН по известным значениям.

Payment Card Industry (PCI) Data Security Standard

Requirements and Security Assessment Procedures Version 3.0

3.2.

Эмитенты и компании, обеспечивающие услуги эмиссии, могут хранить критичные аутентификационные данные, если у них есть обоснованная потребность в этом.

Риск неприемлемый для эквайрера

является приемлемым для эмитента!

Стандарт разрешает эмитентам использовать небезопасные технологии (с точки зрения эквайринга).

Payment Card Industry (PCI) Card Production Logical Security Requirements Version 1.0 May 2013

n) The PIN must only be decrypted immediately before it is passed to the final distribution channel (e.g., the telephone or e-mail system).

ПИН должен быть расшифрован только непосредственно перед передачей (например, по телефону или электронной почте)

Банк получил сертификат соответствия стандарту PCI DSS:

Обеспечена безопасность чужих карт.

Обеспечена безопасность своих карт? – неизвестно!

Global

Security Notice

Bulletin No. 4 • 6 December 2013

Risk Mitigation for ATM Cash-Out Fraud

Attacks—Update

The hackers install additional malware to facilitate the capture and export of payment card data for the manufacture of counterfeit prepaid cards. Using stolen PANs, magnetic stripe data, and cardholder credentials, fraudsters may then be able to exploit the prepaid entity system's PIN request functionality to request and receive PINs for the counterfeit cards. These are the same applications that a legitimate cardholder would use to request a PIN. The PINs and counterfeit cards are provided to accomplices to carry out the actual ATM Cash-Outs.

http://www.gemoney.ru/about/pr-office/news-release/article.wbp?article-id=81D346AC-7F00-0001-002D-74404591BCCB

ДжиИ Мани Банк подтвердил соответствие стандарту информационной безопасности PCI DSS международных платежных систем

25.11.2010

Компания «Sysnet Global Solutions» успешно завершила проект по подготовке и проведению сертификации на соответствие требованиям международного стандарта безопасности платежных карт — PCI DSS v.1.2.1 в «ДжиИ Мани Банк».

Получение «ДжиИ Мани Банком» сертификата PCI DSS еще раз подтверждает высокий уровень защищенности и надежности данных клиентов банковских карт», - сказал старший консультант по безопасности компании «Sysnet Global Solutions» Алексей Гребенюк.

http://creditcardsonline.ru/news/2013/07/31/940-klientyi-djii-mani-banka-budut-poluchat-pin-kodyi-po-sms/

Клиенты ДжиИ Мани Банка будут получать ПИН-коды к картам по SMS

31.07.2013

С 14 августа 2013 года ДжиИ Мани Банк вводит в действие услугу по получению ПИН-кода посредством SMS-сообщений. При оформлении карты ДжиИ Мани Банка клиент будет получать ПИН-код в SMS-сообщении. В Банке надеются, что с внедрением такой услуги расчетные карты откроют перед клиентами больше возможностей и помогут им в реализации всех планов и идей.

Данная технология предполагает выпуск карты с PIN, который будет отправлен клиенту - держателю карты в виде SMS-сообщения.

PIN передается держателям карт в ОТКРЫТОМ ВИДЕ.

Правила платежной системы Виза

Требования к обеспечению безопасности ПИН-кодов

Участник платежной системы-Эквайер обязан обеспечить безопасность ПИН-кода, используемого для удостоверения личности клиента-физического лица при проведении операции, в соответствии с Руководством по реализации требований к обеспечению безопасности ПИНа в индустрии платежных карт.

В том случае если участник платежной системы-Эмитент получает от Visa незащищенный ПИН-блок, он обязан перевести его в безопасный формат.

То есть,

Эквайрер обязан использовать защищенный формат ПИН-блока,

VISA может его перешифровать в незащищенный формат и отправить эмитенту,

эмитент обязан его перешифровать в защищенный формат:

все кроме VISA обязаны выполнять

PCI PIN Security Requirements

Standard: PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI)

Version: 1.0

Date: January 2013

Author: PCI Security Standards Council

Information Supplement:

ATM Security Guidelines

3.2 ATM Security Overview

The cash in transit or stored in the ATM safe has been the asset traditionally targeted by ATM criminals, sometimes in rather violent ways. However, in the last years, attackers have turned their attention equally to soft assets present in the ATM, such as PINs and account data.

Criminals use this stolen information to produce counterfeit cards to be used for fraudulent transactions—increasingly around the world—encompassing ATM withdrawals, purchases with PIN at the point of sale, and purchases without PIN in card-not-present environments.

Похищенная на банкоматах информация **ПИН и трек** (account data), применяется криминалом для изготовления поддельных карт и используется по всему миру, включая снятия в банкоматах, **покупки в ПОС с ПИН**, а также **покупки** без ПИН в операциях **без присутствия карты**.

Полное непонимание технологии мошенничества:

если у злодея есть трек и ПИН, зачем нужно в ПОС осуществлять покупку, а не снять наличные в банкомате, если есть трек (допустим ПИНа нет), то изготавливают поддельную карту и используют в ПОС, а не в card-not-present, т.к. нет CVV2/CVC2 и 3D Sec.

Standard: PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI)

Version: 1.0

Date: January 2013

Author: PCI Security Standards Council

Information Supplement: ATM Security Guidelines

As organized global crime syndicates target ATMs, the financial industry needs a global ATM security standard to promote the availability of secure ATMs. The main characteristics of this standard are:

Нужен глобальный стандарт по безопасности ATM.

The current versions of *PCI PTS POI Security Requirements* and *PCI PIN Security Requirements* are excellent starting points for these needed standards. However they are currently defined for POS terminals and their adjustment to ATMs is currently under consideration at the PCI SCC.

PCI PTS и PCI PIN являются превосходными отправными точками для необходимого стандарта. Но они применяются только для ПОС и возможность их применения для АТМ только рассматривается PCI SCC.

SCC - что это? опечатка SSC - Security Standards Council.

Документов, в отношении банкоматов со стороны PCI SSC нет, в том числе не подлежат обязательному исполнению PCI PTS и PCI PIN.

Требования PCI DSS

3.4 PAN должен быть представлен в нечитаемом виде во всех местах хранения

Если номер карты скомпрометирован:

Для микропроцессорных карт: недостаточно для изготовления поддельного микропроцессора.

Для карт с магнитной полосой: дополнительно необходимы дата действия карты, CVV/CVC, сервис код и возможно PVV.

Для снижения риска необходим переход на технологию EMV.

Если номер карты скомпрометирован:

Для электронной коммерции: дополнительно необходимы дата действия карты, CVV2/CVC2.

Данные м.б. легко скомпрометированы.

Для снижения риска необходим переход на технологию 3D Secure.

для EMV и 3D Secure

номер карты уже не относится к критически важным данным.

Проведение несанкционированной операции возможно либо при нарушении обычных (существовавших до PCI DSS) требований безопасности, либо при отставании от передовых технологий, таких как EMV и 3D Secure.

PCI DSS защищает устаревшие технологии.

Закрыть PAN в принципе невозможно, т.к. он является идентификатором счета (авторизация, клиринг, диспуты и др.).

EMV и 3D Secure

Появились раньше PCI DSS, на их реализацию уже затрачены значительные средства.

Необходимо дальнейшее их развитие и совершенствование, а не трата средств для защиты устаревших технологий, основанных на возможности осуществить мошенническую операцию, обладая минимальной информацией – номером карты.

Необходимо предпринимать усилия, чтобы номер карты не относился к критичным данным, которые необходимо защищать, а считался лишь одним из реквизитов счета – идентификационным номером.

Слабости PCI DSS

Член Палаты Представителей США Иветт Кларк (Yvette Clark) заявила, что выполнение стандарта не гарантирует безопасности, призвала к его изменению и переходу на новые защищенные технологии, например: «ЧИП и ПИН».

Недостатки PCI DSS:

-защищает устаревшие технологии;

-не обеспечивает должного уровня безопасности данных (PAN);

-неадекватно увеличивает затраты;

-не защищает критичные данные PVV, CVV/CVC, EMV, 3D-Sec;

-не защищает номера карт в банковских АБС (расчеты эквайреров с ТСП).

-умышленное ослабление требований стандарта PCI DSS ради поддержания карточной функциональности (возможность хранения значений PVV, в 1 версии был запрет);

-официальное разрешение нарушения PCI DSS (бесконтактные карты – PAN в открытом виде).

PCI DSS против EMV, 3D Secure?

Зачем платежные системы активно продвигают стандарт и почему денежные средства необходимо вкладывать не в развитие новых безопасных технологий (EMV, 3D Secure), а в защиту старых, морально устаревших?

EMV, 3D Secure – рыночные механизмы (перенос ответственности).

PCI DSS – административные (штрафы).

PCI DSS получил свое наибольшее распространение в Соединенных Штатах Америки. Вместе с тем, прекрасно известно, что именно США является самым отсталым регионом в плане миграции на технологию EMV.

Требования PCI DSS

11.3 Следует проводить внешний и внутренний тест на проникновение не реже одного раза в год, а также после любого значимого изменения или обновления инфраструктуры и приложений (например, обновления операционной системы, добавления подсети, установки веб-сервера).

11.3.b Убедиться в том, что выявленные уязвимости были устранены и проведен повторный тест.

11.3.c Убедиться в том, что тест на проникновение был проведен квалифицированными сотрудниками организации либо квалифицированной третьей стороной, а также убедиться в их организационной независимости (если это возможно; при этом наличие статуса QSA или ASV не требуется).

Требования PCI DSS

Кто проводит тест на проникновение?

Если тест на проникновение проводит не QSA-аудитор, то необходимы дополнительные усилия, чтобы убедить QSA, *«что тест на проникновение был проведен квалифицированными сотрудниками организации либо квалифицированной третьей стороной, а также убедиться в их организационной независимости»*. (11.3.c)

Если тест проводит QSA-аудитор, то данный вопрос решен автоматически.

Требования PCI DSS

Кто проводит тест на проникновение?

Если тест на проникновение проводит квалифицированный специалист, то велика вероятность взлома системы.

Результат: не прохождение PCI аудита, до момента устранения уязвимостей (люди, время, деньги) и необходимость проведения повторного теста (время, деньги). 11.3.b

Если тест проводит неквалифицированный специалист, то всё хорошо: уязвимостей нет, время и деньги экономятся.

ВЫВОД: ЧЕМ ХУЖЕ, ТЕМ ЛУЧШЕ!

Heartbleed Bag

Ошибка переполнения буфера в криптографическом программном обеспечении OpenSSL, позволяющая несанкционированно читать память на сервере или на клиенте, в том числе закрытый ключ SSL.

Ошибка существовала с 31 декабря 2011 (версия 1.0.1 вышла 14 марта 2012) до 07 апреля 2014 (версия 1.0.1g).

Ошибка обнаружена независимо друг от друга группой инженеров безопасности Рику Варджоваара и Джошуа Морин из компании «Codenomicom» и Нилом Мехта из подразделения безопасности Google Security.

Ни один пентестер в рамках PCI DSS за два года не обнаружил данную уязвимость!

Тест на проникновение

Представляет собой попытки использования уязвимостей для определения возможности несанкционированного доступа или других злонамеренных действий.

В случае успешного теста

ВОЗМОЖНА КОМПРОМЕТАЦИЯ ДАННЫХ ДЕРЖАТЕЛЕЙ КАРТ

Global Security Report 2010

Компания Trustwave опубликовала отчет Global Security Report 2010, где приведен анализ основных путей успешно реализованных атак при проведении тестирований на проникновение.

В частности описаны десять наиболее распространенных атак внешнего теста на проникновение.

Атаки с 1-ой по 7-ю могут привести к компрометации каких-либо данных, а атаки 3-я и 6-я прямо говорят о возможности компрометации данных держателей карт.

Тест на проникновение

В банковских системах находятся сведения составляющие банковскую тайну и персональные данные клиентов.

Банк не является собственником данных сведений.

Банковская тайна: ст. 26 ФЗ-№ 395-1 «О банках и банковской деятельности»

Персональные данные: ФЗ-№ 152-ФЗ «О персональных данных»

Для предоставления доступа необходимо разрешение клиента, а не банка!

Соглашения о конфиденциальности недостаточно

УК РФ

Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом -

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного до шести месяцев, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, -

наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до трех лет, либо лишением свободы на тот же срок.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, -

4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, -

УК РФ

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, -
2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, -
3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, -

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

использование вредоносного ПО

На первом этапе аудиторы работают с минимальными знаниями о системе, и их целью является «пробить» периметр, например, установив вредоносное программное обеспечение …

… зачастую приходится разрабатывать вспомогательные средства обхода систем защиты…

Алексей Гребенюк,

старший консультант по информационной безопасности компании FortConsult, QSA.

PCI DSS v.3.0 (11.2.3 ПОЯСНЕНИЕ)

Часто тестировщик использует несколько уязвимостей вместе, чтобы обойти несколько уровней защиты

УК РФ

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

«возможно наступление события при котором пентестер неосознанно (случайно, непреднамеренно) получит доступ к информации разного уровня конфиденциальности.

Если в процессе проведения тестирования на проникновение он и получил к ней доступ, то этот доступ был получен по неосторожности. Следовательно, состав преступления отсутствует.»

Dmitry Evteev

Субъективная сторона преступления, предусмотренная ст.272 УК РФ, характеризуется умышленной формой вины.

Нет умысла – нет преступления.

УК РФ

Статья 25. Преступление, совершенное умышленно

1. Преступлением, совершенным умышленно, признается деяние, совершенное с прямым или косвенным умыслом.
2. Преступление признается совершенным с прямым умыслом, если лицо осознавало общественную опасность своих действий (бездействия), предвидело возможность или неизбежность наступления общественно опасных последствий и желало их наступления.
3. Преступление признается совершенным с косвенным умыслом, если лицо осознавало общественную опасность своих действий (бездействия), предвидело возможность наступления общественно опасных последствий, не желало, но сознательно допускало эти последствия либо относилось к ним безразлично.

УК РФ

Статья 29. Оконченное и неоконченное преступления

2. Неоконченным преступлением признаются приготовление к преступлению и покушение на преступление.
3. Уголовная ответственность за неоконченное преступление наступает по статье настоящего Кодекса, предусматривающей ответственность за оконченное преступление, со ссылкой на статью 30 настоящего Кодекса.

Статья 30. Приготовление к преступлению и покушение на преступление

3. Покушением на преступление признаются умышленные действия (бездействие) лица, непосредственно направленные на совершение преступления, если при этом преступление не было доведено до конца по не зависящим от этого лица обстоятельствам.

QSA, компания, которой Совет PCI SSC предоставил право проведения оценки на соответствие стандарту PCI DSS.

QSA проводит аудит на соответствие PCI DSS, по результатам которого составляется Отчет о соответствии (ROC), в котором содержатся детальные сведения о статусе соответствия организации стандарту PCI DSS.

По запросу МПС QSA предоставляет им ROC.

В ходе аудита QSA выполняет сбор свидетельств выполнения требований PCI DSS (копии документов и записей, снимки экрана, фотографии), которые хранятся в течении 3-х лет и могут быть в любой момент предоставлены Совету PCI SSC.

МПС и PCI SSC знают и контролируют состояние информационной безопасности системы платежных карт России.

ЦБ РФ, ФСТЭК, ФАПСИ:

–контролируют PCI DSS на территории России?

–знают какие банки прошли аудит и сведения о состоянии их информационной безопасности могли быть переданы иностранным компаниям (спецслужбам)?

КИБЕРБЕЗОПАСНОСТЬ НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ?

СПАСИБО!

Пятиизбянцев Николай Петрович