Требования PCI DSS к платежным системам и терминалам

Таран Дмитрий, специалист компании Softline

Первый банкомат появился осенью 1996 года, сегодня банкоматы стали универсальным инструментом для осуществления платежей. Однако вместе с ростом использования карточек увеличилось и количество мошеннических операций с их использованием.

Для борьбы с мошенничеством такого рода крупнейшие мировые платежные системы (Visa, Mastercard, Discover) создали отраслевой стандарт PCI DSS (Payment Card Industry Data Security Standard). Стандарт содержит требования по обеспечению безопасности данных о держателях платёжных карт, которые передаются, хранятся и обрабатываются в информационных инфраструктурах организаций. Требования этого стандарта должны быть строго выполнены в процессинговых центрах, где обрабатываются данные платежных карт, и рекомендуются к выполнению банкам-эмитентам, выпускающими пластиковые карты.

Кроме требований PCI DSS банки используют и другие меры защиты банкоматов, информации по транзакциям, а также противодействия мошенникам.

Проблематика соблюдения требований PCI DSS в Республике Беларусь.

На текущий момент, в РБ должны соответствовать PCI DSS (по требованию VISA к октябрю 2011 года) 3 финансовых организации: Белорусский процессинговый центр, ОАО «Приорбанк», ОАО «Банк БелВЭБ». Основная проблематика приведения всех процессов обеспечения информационной безопасности в соответствие с PCI DSS заключается в необходимости реорганизации в компаниях существующей системы разграничения и контроля доступа к информации (ресурсам), выделении дополнительного финансирования для требуемой организации защиты ИТ-инфраструктуры и чувствительных данных.

С другой стороны, в банке могут быть внедрены все необходимые процессы по обеспечению безопасности данных платежных средств, и де-факто соответствовать PCI DSS, но все равно должно быть прохождение сертификации на соответствие стандарту. Сертификацию не проходят, так как на поддержание процессов обеспечения безопасности и на проведение аудита соответствия нужно ежегодно выделять финансирование.

Основные требования PCI DSS к ИТ-инфраструктуре и процессам обеспечения ИБ:

PCI DSS определяет 12 основных требований по 6 направлениям безопасности, которые должны осуществляться в организации:

• Построение и сопровождение защищённой сети

1. Установка и обеспечение функционирования межсетевых экранов для защиты данных держателей карт.

2. Неиспользование выставленных по умолчанию производителями системных паролей и других параметров безопасности.

• Защита данных держателей карт

3. Обеспечение защиты данных держателей карт в ходе их хранения.

4. Обеспечение шифрования данных держателей карт при их передаче через общедоступные сети.

• Поддержка программы управления уязвимостями

5. Использование и регулярное обновление антивирусного программного обеспечения.

6. Разработка и поддержка безопасных систем и приложений.

• Реализация мер по строгому контролю доступа

7. Ограничение доступа к данным держателей карт в соответствии со служебной необходимостью.

8. Присвоение уникального идентификатора каждому лицу, имеющему доступ к информационной инфраструктуре.

9. Ограничение физического доступа к данным держателей карт.

• Регулярный мониторинг и тестирование сети

10. Контроль и отслеживание всех сеансов доступа к сетевым ресурсам и данным держателей карт.

11. Регулярное тестирование систем и процессов обеспечения безопасности.

• Поддержка политики информационной безопасности

12. Разработка, поддержка и исполнение политики информационной безопасности.

Особенности применения требований PCI DSS по защите банкоматов.

Защита банкоматов состоит из двух компонентов — защиты физической и защиты информационной. Основные составляющие информационной защиты — это безопасная среда передачи и шифрования данных (пункт 4), необходимость использования антивирусного обеспечения (пункт 5), ограничение доступа к банкоматам сотрудникам только в соответствии со служебной необходимостью (пункт 7).

Физическая защита банкоматов направлена на обеспечение сохранности наличных денежных средств.

Стандарт PCI DSS в основном направлен на организацию процессов обеспечения информационной безопасности в отрасли платежной индустрии и не

содержит конкретных рекомендаций по техническим средствам и мерам.

Белорусские банки организуют меры по информационной защите либо на основе собственных инструкций, либо на основе рекомендаций международных стандартов PCI DSS, ISO 27001, ITIL, СТО БР ИББС и т.д. Зачастую в банке организованы меры по защите и канала связи, и антивирусная защита, и другие меры, но они не находят отражения в локальных документах, так как из-за высокой нагрузки на ИТ-персонал организации, сотрудники не имеют возможности заниматься формализацией нормативных документов.

Защита канала связи с банкоматами.

Для защиты канала связи организуются выделенные каналы связи (банкомат-банк), используются средства VPN, обеспечивается шифрование данных на уровне "банкомат-процессинговый центр". Для разграничения доступа к приложениям банкомата используется межсетевое экранирование и средства контроля целостности программного обеспечения банкомата.

Правильная организация указанных мер позволят полностью обезопасить устройство от захвата злоумышленниками и перехвата потока данных держателя пластиковых карточек и информации по транзакциям. Мошенники почти не используют перехват и взлом информации по каналам связи, так как при шифровании информации получить доступ к ней практически невозможно.

Каналы связи, используемые в банкоматах РБ: Wi-Fi, GSM, Ethernet.

Банки, по мере возможности используют Ethernet, а резервные каналы на текущий момент переводят на 3G. Размещать банкоматы предпочитают в ЦБУ, дополнительных офисах и прочих защищенных помещениях. При установке терминалов в торговых точках, используют GSM, CDMA, GPRS.

Преимущественно используется Ethernet, резервные каналы на текущий момент переводят на 3G.

Есть проблемы в использовании медленных каналов связи (CDMA, GPRS — у них невысокая пропускная способность), но это не влияет на защиту банкомата, а создает трудности в работе самого банкомата.

Защита от мошенничества (скимминга).

Широкое использование у мошенников получило использование накладок на банкомат. Через накладку на картоприемник считывается информация пластиковой карточки, а накладка на клавиатуру (или используется миниатюрная видеокамера) позволяет узнать pin-код карточки владельца. В дальнейшем полученная информация используется для записи на заготовки пластиковых карточек (белый пластик) и снятия наличности через терминалы.

В последнее время банки начали выпускать пластиковые карты со встроенным чипом, что повышает степень защиты карточек и не позволяет использовать «белый пластик», но пока повсеместного распространения они не получили.

Такие карточки стоят дороже обычных, и клиент сам может выбирать какую карточку он хочет использовать. Проблема заключается в том, что дополнительная защита чипованной карточки реализуются не во всех банкоматах, а только в тех, которые имеют возможность делать дополнительную проверку по чипу. Из-за высокой стоимости банкоматов, банки не спешат менять парк терминалов, а действуют постепенно, например, с открытием новых офисов покупают новые банкоматы.

В России и Украине процесс перехода на «чипованные» карточки проходит тоже постепенно в связи с вышеуказанными причинами.

Защита программного обеспечения банкоматов.

Киберпреступники также используют вредоносное программное обеспечение для получения доступа к банкомату (вирусы и трояны). Но как утверждают производители банкоматов, это невозможно без участия сотрудников, обслуживающих банкомат. Поэтому в качестве дополнения к брандмауэру в банкоматах используются антивирусы или системы контроля целостности файлов.

Также с антивирусами может использоваться IPS (Intrusion Prevention System) — система предотвращения вторжений. Она не требует обновлений, поддерживая систему в заведомо рабочем состоянии, и не позволяет запускаться приложениям, которые не занесены в список доверенных. Решения, относящиеся к IPS, защищают также и память устройства, что предотвратит атаки типа «Переполнение буфера обмена».

Банки самостоятельно решают использовать или нет системы IDS/IPS (системы обнаружения/предотвращения вторжений), эти системы используются в основном в комплексе с антивирусом. В нашей стране чаще используются следующие системы IDS и антивирусы: Kaspersky, Symantec, Trend Micro, Dr.Web

Есть также специализированный софт, который предлагают производители банкоматов как альтернативу антивирусам.

Для предотвращения случаев сговора мошенника с сотрудником, обслуживающим банкоматы, банки вводят контрольные процедуры, например контроль обслуживания терминала сотрудником безопасности. Если банкоматы обслуживает сторонняя организация, контроль может осуществляться сотрудником банка.

В целом в Республике Беларусь защита банкоматов находится на высоком уровне.