Введение

Для банков-эмитентов, взаимодействующих хотя бы с одной из платежных систем (Visa, MasterCard, American Express, JCB и Discover) необходимо ежегодно подтверждать соответствие стандартам PCI SSC. При этом критерий соответствия составляет 100%.
Бизнес-процессы, для которых прохождение сертификация на PCI DSS обязательна:

- Эквайрингс помощью POS-терминалов или устройств самообслуживания.
- Производство и персонализация платежных карт.
- Платежный шлюз электронной коммерции.
- Торгово-сервисное предприятие электронной торговли.

Соответствие стандартам открывает широкие возможности для банка: он получает лицензию на интернет-эквайринг, может подключить банки-аффилиаты, и воспользоваться другими преференциями «участников клуба». В противоположность несоблюдение требований PCI DSS прежде всего может привести к запрету обрабатывать платежи с использованием международных платежных систем. Также на такие банки может быть наложен штраф, и увеличен размер страхового депозита.

Нужно отметить, что PCI DSS не просто список теоретических требований, которые выполняются для галочки. Для их формирования исследуются лучшие мировые практики для поиска оптимальных подходов защиты. Основные задачи:

- Повысить уровень защищенности данных о держателях карт вследствие уменьшения количества потенциально уязвимых бизнес-процессов, приложений, хранилищ данных, рабочих станций, банкоматов и сетевых устройств.
- Снизить затраты на обеспечение безопасности данных о держателях карт.

Актуальной версией стандарта PCI DSS является версия 3.2, опубликованная в апреле 2016 года. Часть новых требований вступит в силу в 2018 года, например, отказ от использования небезопасных версий протоколов (SSL и TLS 1.0).

Решение SoftControl TPSecure было разработано в сотрудничестве с Советом по Разработке Стандартов Безопасности Индустрии Платежных Карт (PCI Security Standarts Council), что позволяет использовать его для приведения информационной системы в соответствие требованиям стандарта PCI DSS 3.2 в части защиты банкоматов и рабочих станций.

Преимущество решений SoftControl

В TPSecure, как и в других решениях SoftControl, в основе лежат проактивные технологии защиты, целью которых является сохранение неизменности системной конфигурации, нейтрализуя саму возможность попадания в систему вредоносного кода. Высокоэффективная технология VIPO, осуществляет мониторинг и контроль активности всей системы с целью предотвращения нежелательных или несанкционированных действий.

Кроме выполнения специальных требований стандарта, TPSecure предоставляет дополнительные возможности:

- Проактивная защита от несанкционированного доступа к данным, изменений объектов файловой системы, реестра, модификации приложений, обеспечивает целостность всей системы. Контролируя запуск и активность всех процессов, TPSecure сохраняет систему в заведомо исправном состоянии.
- Интеграция с другим защитным ПО (любые средства защиты каналов передачи данных, шифрования, антивирусы) позволяет усилить меры безопасности.
- Скрытый мониторинг и логирование всех системных событий уменьшает возможность внесение несанкционированных правок обслуживающим персоналом.
- Контроль доступа к USB накопителям, CD/DVD, COM и LPT портам, контроль автозапуска и возможность задания исключений для определенного накопителя обеспечивает безопасность конечных точек сети.
- Централизованное управление TPSecure позволяет удаленно корректировать настройки клиентских модулей, с возможностью изменения политик контроля приложений и устройств.
- TPSecure оснащен системой самозащиты, которая не может быть остановлена даже при наличии прав локального администратора. Кроме того, клиентский модуль может быть настроен для регулярной отправки своего статуса в консоль администрирования.
- Различные варианты поставки: возможна поставка как стандартного набора компонент и настроек, так и разработка дополнительного функционала по требованию заказчика. При необходимости поставляется исходный код продукта и двоичных библиотек.

Требования PCI DSS

Построение и сопровождение защищенной сети

Требование 1. Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт

РЕШЕНИЕ SOFTCONTROL

TPSecure работает совместно с межсетевым экраном, сохраняет его в заведомо исправном состоянии, предотвращая несанкционированное изменение целостности приложения.

Доступ к файлам, ключам реестра, процессам приложения может быть заблокирован. Тем самым TPSecure предотвращает несанкционированное изменение настроек межсетевого экрана.

Требование 2. Не использовать пароли и другие системные параметры, заданные производителем по умолчанию

РЕШЕНИЕ SOFTCONTROL

TPSecure использует Active Directory для централизованного управления политиками безопасности и защиты административного доступа.

Защита данных держателей карт

Требование 3. Обеспечить безопасное хранение данных держателей карт

РЕШЕНИЕ SOFTCONTROL

TPSecure обеспечивает защиту хранимых данных, блокируя несанкционированный доступ ко всем объектам файловой системы.

Поддержка программы управления уязвимостями

Требование 5. Защищать все системы от вредоносного ПО и регулярно обновлять антивирусные приложения

РЕШЕНИЕ SOFTCONTROL

TPSecure не только выполняет это требование, но также защищает от всех угроз, известных и неизвестных. Уникальность TPSecure в том, что он обеспечивает проактивную защиту от любого вредоносного ПО (вирусы, черви, трояны и тп), включая такую растущую угрозу, как инсайдерские атаки. TPSecure предотвращает получение доступа и внесение изменений в систему обработки транзакций, будь то в результате хакерской атаки или несанкционированных действий обслуживающего персонала. TPSecure создает профиль системы на основе модулей и компонент самой операционной системы и всех установленных приложений.

TPSecure осуществляет контроль запуска приложений, позволяя блокировать новые или измененные приложения, если их контрольные суммы отсутствуют в профиле системы. Также, TPSecure содержит традиционный антивирусный сканер.

Требование 6. Разрабатывать и поддерживать безопасные системы и приложения

РЕШЕНИЕ SOFTCONTROL

TPSecure предотвращает использование уязвимостей, применяя проверку целостности и запуская потенциально уязвимые приложения в изолированной среде с ограниченными системными привилегиями.

Как следствие, процесс установки обновлений перестает быть процедурой, проведение которой необходимо по мере обнаружения новых уязвимостей. Установка обновлений может быть отложена во времени без ущерба безопасности.

Благодаря гибкости решения, TPSecure обеспечивает целостность системы с минимальным влиянием на процедуры технического обслуживания. Устройство может быть полностью заблокировано, либо приложения могут быть запущены в изолированной среде, либо могут быть заданы индивидуальные и / или групповые политики, чтобы использовать приложения только в определенных целях и / или с заданными параметрами.

Регулярный мониторинг и тестирование сети

Требование 10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт

РЕШЕНИЕ SOFTCONTROL

В случае инцидента, наряду с блокировкой несанкционированной активности, TPSecure регистрирует и посылает уведомление с описанием того, где, когда и какого рода нарушение было пресечено. Для каждого приложения или процесса ведется история активности с возможностью теневого копирования изменяемых файлов. Возможно отследить последовательность действий каждого инцидента.

Требование 11. Регулярно выполнять тестирование систем и процессов обеспечения безопасности

РЕШЕНИЕ SOFTCONTROL

TPSecure упрощает процесс тестирования. Уведомления создаются на каждую попытку запуска неизвестного кода и несанкционированный доступ к файлам, с возможностью просмотра лога активности на конечных точках.

TPSecure может отправлять статус системы защиты на конечной точке. Если по какой-то причине клиент TPSecure был остановлен на конечной точке, отправляется уведомление в консоль администрирования или на электронную почту.

Кроме того, TPSecure позволяет ускорить процесс прохождения тестов на проникновение, предотвращая вторжения и сохраняя целостность, как всей системы, так и отдельных файлов.

Поддержка политики информационной безопасности

Требование 12. Разработать и поддерживать политику информационной безопасности.

РЕШЕНИЕ SOFTCONTROL

Благодаря возможности централизованного получения уведомлений в режиме реального времени, TPSecure вносит существенный вклад в план реагирования на инциденты.