Как SafenSoft TPSecure помогает соответствовать стандарту PCI DSS

Введение

Сообщество PCI SSC, объединившее в себе крупнейшие платежные системы, непрерывно развивает, улучшает и внедряет стандарты безопасности для защиты данных держателей банковских карт. В рамках этой инициативы был опубликовал набор стандартов безопасности, названный Payment Card Industry Data Security Standard (PCI DSS) - Стандарт безопасности данных индустрии платежных карт. Все банки, торгово-сервисные предприятия, поставщики технологических услуг и другие организации, деятельность которых связана с обработкой, передачей и хранением данных о держателях платежных карт, должны проходить регулярную проверку соответствия требованиям стандарта PCI DSS. Компании, не соблюдающие требования стандарта, рискуют потерять возможность обрабатывать платежи с использованием международных платежных систем.
Актуальной версией стандарта PCI DSS является версия 2.0, опубликованная 28 октября 2010 года.
Данный документ описывает, как SafenSoft TPSecure поможет Вам привести систему в соответствие с требованиями стандарта of PCI DSS 2.0, защищая целостность вашей корпоративной сети.

Преимущество решений SafenSoft

Программный продукт SafenSoft TPSecure поможет компании привести систему в соответствие стандарту PCI DSS и снизить финансовые риски и риски ИБ. Когда бы ни была произведена попытка вторжения, она блокируется, а TPSecure отправляет своевременное уведомление, с описанием, где, когда и какого рода нарушение имело место.
В TPSecure, как и в других решениях SafenSoft, в основе лежат проактивные технологии защиты, целью которых является сохранение неизменности системной конфигурации, а не попытки поиска отдельных образцов 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 - Возможность совместной работы с другими средствами защиты (любые средства защиты каналов передачи данных, шифрования, антивирусы) позволяет усилить существующие политики безопасности.
- Скрытый мониторинг и логирование всех системных событий – Непрерывный мониторинг устройств, предотвращающий возможность модификации со стороны обслуживающего персонала.
- Контроль доступа к USB накопителям, CD/DVD, COM и LPT портам, контроль автозапуска и возможность задания исключений для определенного накопителя.
- Централизованное управление - TPSecure управляет удаленно настройками клиентских модулей, с возможностью изменения политик контроля приложений и устройств.
- Система самозащиты – TPSecure не может быть остановлен даже при наличие 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. Возможна поставка исходного кода продукта, двоичных библиотек (SDK).

Соответствие PCI DSS – Как TPSecure помогает выполнить требования

Построение и сопровождение защищенной сети

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

РЕШЕНИЕ SAFENSOFT

- 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 SAFENSOFT

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 SAFENSOFT

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

Поддержка программы управления уязвимостями

Требование 5. Использовать и регулярно обновлять антивирусное программное обеспечение

РЕШЕНИЕ SAFENSOFT

Хотя стандарт говорит об антивирусах, ясно, что суть этого требования – защита от вредоносного кода любого рода. 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 SAFENSOFT

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 SAFENSOFT

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 SAFENSOFT

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 SAFENSOFT

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