20 Декабря 2022 ENOT.io 408 0

PCI DSS: что это, как проходит проверка

PCI DSS или стандарт безопасности индустрии платежных карт (на английском Payment Card Industry Data Security Standard) — международный стандарт безопасности использования, хранения, защиты и применения платежных банковских карт.

Иными словами, PCI DSS является официальным документом, в котором прописаны все требования к любой организации, которая желает, так или иначе, заниматься управлением данными банковских карт в своих бизнес-целях. Впервые этот стандарт безопасности был учрежден платежными системами Visa и MasterCard, а также некоторыми американскими организациями: American Express, JCB и Discover в 2004-ом году.

Стандарты безопасности индустрии платежных карт имеют 12 обязательных требований, разделенных на шесть областей контроля. Все эти пункты считаются законом для всех сертифицированных участников и должны безукоризненно соблюдаться.

Создание и содержание безопасной сети:

Пункт 1. Необходимо установить и обеспечивать функционирование сетевых фильтров, осуществляющих контроль над проходящим через него сетевым трафиком в соответствии с заданными правилами.

Пункт 2. Системные пароли и параметры безопасности используемого оборудования должны быть заменены с заводских на оригинальные.

Защита данных владельцев банковских карт:

Пункт 3. Все данные держателей карт должны находиться под защитой на время их хранения.

Пункт 4. Любые передачи данных карт через общедоступные сети должны происходить только после шифрования.

Поддержание работы программы управления уязвимостями:

Пункт 5. Организация должна использовать свежую версию официального антивирусного программного обеспечения.

Пункт 6. Участник PCI DSS должен заниматься разработкой и поддержанием безопасных систем и приложений.

Пункт 7. В случае необходимости разрешается временное ограничение доступа к хранимым данным любыми лицами.

Пункт 8. Каждый пользователь, имеющий доступ к информационной инфраструктуре организации, обязан иметь собственный персональный идентификатор.

Пункт 9. К данным держателей карт должен быть максимально ограничен физический доступ любых лиц.

Проведение постоянного мониторинга сети и ее тестирование:

Пункт 10. Все сеансы доступа к сетевым ресурсам с данными владельцев банковских карт должны непрерывно отслеживаться и контролироваться.

Пункт 11. Все процессы обеспечения безопасности и ответственные за это системы необходимо регулярно тестировать.

Осуществление политики информационной безопасности:

Пункт 12. Участник стандарта должен разрабатывать, поддерживать и выполнять международную политику информационной безопасности.

Что будет за несоблюдение стандарта?

В случае нарушения требований международного стандарта безопасности на потенциального злоумышленника накладывается ряд штрафов. Размер взыскания определяется по типу безответственной компании, объему и размерам осуществляемых денежных транзакций и количестве повторов нарушения.

Например, за первый проступок может быть назначен штраф в размере 50 тысяч долларов, а за последующий уже 200 тысяч. Санкции к организации, продолжающей не соблюдать установленные требования, будут повторяться ежемесячно до устранения нарушения.

Регулярное пренебрежение любых установленных требований стандарта безопасности может привести к проблемам не только с платежными системами и регулярными штрафами, но и вынудить нести ответственность перед местной правительственной структурой. Платежная система может обратиться к государству, в котором находится нарушитель, и передать информацию о нарушении закона о защите персональных данных.

СПРАВКА: В России к таковому относится федеральный закон 152 «О персональных данных», принятый в 2006-ом году, когда стандарты PCI DSS пришли на российский рынок. Кроме него, к нарушителю может применяться пункт 6 статьи 13.12 и статья 15.36 кодекса об административных нарушениях Российской Федерации. Лица, признанные виновными в нарушениях одной из этих статей, будут нести всю предусмотренную законодательством Российской Федерации ответственность.

Любая компания, желающая обрабатывать данные платежных банковских карт, обязана получать сертификат PCI DSS. Даже если организация не занимается хранением данных, а лишь осуществляет передачу, использует их или может получить доступ к платежной информации, она автоматически обязана пройти сертификацию, так как все вышеперечисленные действия разрешены только участникам платежной системы.

Процесс сертификации делится на несколько способов, зависящих от объема предполагаемых к обработке транзакций. Если количество платежей не превышает суммы в 20 тысяч в год, то можно ограничиться проведением аудита и заполнением специального опросного листа.

В ином случае необходимо осуществить обращение к сертифицированной организации для осуществления полноценной проверки. Проверяющие аудиторы должны будут оценить политику информационной безопасности обращающегося, провести серию тестирований информационной инфраструктуры для проверки ее устойчивости к атакам, составить итоговый отчет.

Если фирма, желающая пройти процедуры проверки, успешно проходит все тесты, ей выдается сертификат соответствия стандартам безопасности платежных систем. В случае обнаружения проблем на каком-либо этапе проверки аудиторы составляют отчет, в котором указываются все необходимые к устранению нарушения. При выявлении серьезных проблем с соблюдением стандартов после устранения нарушений проверка будет выполняться с самого начала.

СПРАВКА: Альтернативно являться участником платежной системы можно через компании-посредники, которые проводят все операции с данными банковских карт самостоятельно. В таком случае сама организация может не проходить сертификацию PCI DSS, так как поставщик платежного сервиса уже имеет сертификат у себя в наличии. Важным остается только следить за соответствием и регулярным обновлением сертификата выбранного посредника.

Например, наш платежный агрегатор ENOT.io имеет сертификацию PCI DSS. Поэтому вы просто ставите наше платежное решение к себе на сайт, и сразу можете принимать платежи.

Интеграция с сайтами и интернет-магазинами

В соответствии с вышесказанным, принимать платежи на своем сайте или интернет-магазине довольно просто. Осуществляется это путем установки на сервер специального модуля по приему платежей для CMS, если таковой у платежного агрегатора имеется. У нас в ENOT.io платежный шлюз есть для Wordpress Woocommerce, Joomla, DLE, Xenforo и для других популярных CMS.

Если у вас самописный движок, то интегрировать прием платежей ваш разработчик может

Стандарт безопасности индустрии платежных карт — важный элемент осуществления любых денежных операций мирового уровня. Сертификат этой системы гарантирует, что данные пользователя будут надежно сохранены и не будут утеряны в случае хакерской атаки. PCI DSS предоставляет хорошую защиту от мошенников и увеличивает при этом платежную конверсию, максимально упрощая сам процесс осуществления платежа.

0

☆ В избр.

ENOT.io

ENOT.io — помогаем принимать онлайн-платежи на сайтах и в интернет-магазинах.

Подписаться

Как принимать платежи с иностранных карт на сайте в 2023 году 1 058

PCI DSS: что это, как проходит проверка 409

Как принимать платежи на сайте и в интернет-магазине 386

Посмотреть все 6 статей

Комментарии

Написать комментарий...

Написать

Блог проекта

Расскажите историю о создании или развитии проекта, поиске команды, проблемах и решениях

Написать

Личный блог

Продвигайте свои услуги или личный бренд через интересные кейсы и статьи

Написать

Рассылка лучших материалов за неделю

Email-адрес

Подписаться

Редакция team@spark.ru | Техническая поддержка help@spark.ru | Продвижение adv@spark.ru | Телефон +7 495 137-07-07

ИП Барабанова Ю.Б. ИНН 500111143150