14.06.2016

PCI DSS 3.2: что изменилось и к чему готовиться

28 апреля 2016 года на официальном сайте Совета PCI SSC был опубликован пресс-релиз о выходе новой версии стандарта безопасности данных индустрии платежных карт PCI DSS 3.2. Версия получилась внеплановая (обычно новые версии Совет публикует осенью), но при этом изменения в ней считаются минорными. Петр Шаповалов, инженер по защите информации, PCI QSA, компания Deiteriy, разбирает, что поменялось в новом стандарте. Подробности – в июньском номере журнала "ПЛАС".

Помимо совсем мелких корректировок, которые были сделаны с целью исправления различных опечаток, ошибок форматирования, пунктуации и т. д., в новой версии стандарта появился ряд уточнений и дополнений, а также ряд новых требований. Эти требования пока еще являются рекомендательными, но с 1 февраля 2018 года станут обязательными для выполнения. К таким новинкам относятся следующие.

Применимо ко всем организациям:

• для всех изменений в информационной инфраструктуре необходимо дополнительно проверять, что все применимые требования стандарта PCI DSS выполнены для изменяемых компонентов. Иными словами, если вы внесли какое-либо изменение в информационную инфраструктуру, нужно убедиться, что соответствие стандарту не нарушилось (например, обновить схемы сети и потоков данных, провести сканирование на уязвимости и иные подобные мероприятия);
• для удаленного неконсольного административного доступа в область применимости стандарта PCI DSS нужно реализовать мультифакторную

аутентификацию.
Применимо только к поставщикам услуг:
• в случае использования шифрования архитектуру системы шифрования нужно документировать. Алгоритмы, протоколы и процедуры управления ключами необходимо описать и поддерживать в актуальном состоянии;
• требуется контролировать работоспособность систем безопасности. В случае возникновения сбоев в работе таких систем следует выполнить процедуры реагирования и зарегистрировать факт сбоя;
• тестирование на проникновение в части сегментации сети необходимо проводить не реже одного раза в шесть месяцев, а также после внесения любых критичных изменений в информационную инфраструктуру;
• в организации должен быть внедрен высокоуровневый документ, в котором будет описана программа соответствия требованиям стандарта PCI DSS и назначен ответственный работник, который будет контролировать ее выполнение и держать в курсе руководство организации о статусе данной программы;
• не реже одного раза в квартал необходимо проверять, что работники организации корректно выполняют процедуры по ежедневному анализу журналов протоколирования событий, пересмотру правил межсетевого экранирования, применению стандартов конфигурации для новых систем, реагированию на сигналы систем безопасности, а также соблюдают процедуры управления изменениями.

Повторюсь, что до 31 января 2018 года данные требования являются рекомендациями, а уже после наступления этой даты станут обязательными для выполнения. Но поскольку процесс реализации новых требований может занять длительное время и потребовать привлечения дополнительных средств бюджета, участникам рынка рекомендуется начать его выполнение как можно раньше.

Помимо новых требований, в текст стандарта внесены уточнения, включая следующие:

• если в области применимости стандарта PCI DSS используется PA-DSS сертифицированное приложение, но его поддержка производителем прекратилась (например, у ПО появился статус «End-of-life»), то это приложение уже не сможет обеспечивать необходимый уровень безопасности. Поэтому стандарт рекомендует отслеживать статус поддержки при выборе PA-DSS сертифицированных приложений;
• при определении границ области применимости стандарта PCI DSS следует учитывать системы, обеспечивающие непрерывность работы компонентов информационной инфраструктуры: системы резервного копирования и восстановления, отказоустойчивые системы;
• перед переводом в производную среду компонента информационной инфраструктуры необходимо изменять все стандартные настройки и отключать

стандартные учетные записи. Согласно пояснению, это требование касается и платежных приложений;
• добавлено примечание в проверочную процедуру по поиску полного номера карты PAN в логах компонентов информационной инфраструктуры. Уточнение заключается в том, что логи необходимо анализировать и для платежных приложений в том числе;
• добавлено примечание к требованию 3.4.1 по шифрованию дисков: это требование применимо в дополнение ко всем другим требованиям по шифрованию и управлению ключами в области применимости стандарта;
• разработчики должны как минимум ежегодно обучаться методам безопасного программирования;
• добавлено примечание к требованию по системе контроля доступа. Стандарт допускает, что таких систем в организации может быть несколько;
• уточнено, что в качестве системы контроля доступа можно использовать либо систему видеонаблюдения, либо СКУД, либо обе технологии одновременно;
• если в версии 3.1 стандарта PCI DSS должен был контролироваться лишь удаленный доступ вендоров в информационную инфраструктуру, в версии 3.2 внесено уточнение о том, что необходимо обеспечить контроль удаленного доступа любой третьей стороны.

Новое Приложение A2 включило в себя отдельные требования для организаций, которые все еще используют протокол SSL и ранние версии протокола TLS. Это Приложение содержит требования по использованию POS-терминалов (необходимо иметь доказательство того, что POS-устройства не подвержены атакам на небезопасные версии протоколов), а также требование по наличию Плана перехода на безопасные версии протоколов.

[Читать далее >>>]

По материалам PLUSworld.ru