PCI DSS версии 3.2, что нас ждет?

Кристина Андреева
Инженер по защите информации компании Deiteriy
CISA, PCI QSA

01 июня 2016 года

 | 192012, Россия, Санкт-Петербург, пр. Обуховской Обороны д. 271, лит. А | +7 (812) 361-61-55 | www.deiteriy.com | info@deiteriy.com

Версия 3.2 стандарта PCI DSS?

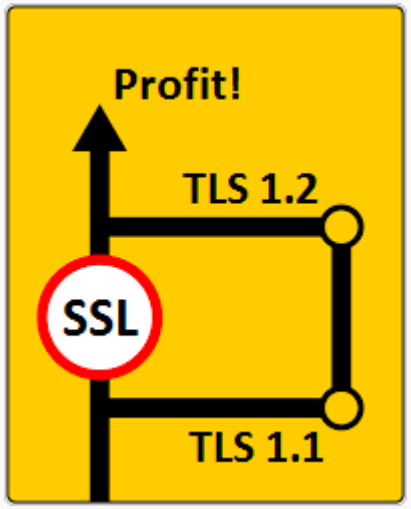
- опубликована 28 апреля 2016 года;
- до **28 октября 2016** года официально действуют **обе версии** – и старая 3.1, и новая 3.2;
- часть новых требований вступит в силу в **феврале 2018** года.

Разновидности нововведений:

- терминологические и косметические;
- для всех организаций, применяющих PCI DSS;
- только для поставщиков услуг (не мерчантов).

Терминология и косметика:

- убраны конкретные примеры «стойких» и «нестойких» протоколов и алгоритмов, поскольку практика показала, что это может измениться в любой момент.



Терминология и косметика:

- «двухфакторная аутентификация» заменена на «мультифакторную».

pas**d

Терминология и косметика:

- видеонаблюдение или СКУД, или обе технологии вместе.

Изменения для всех:

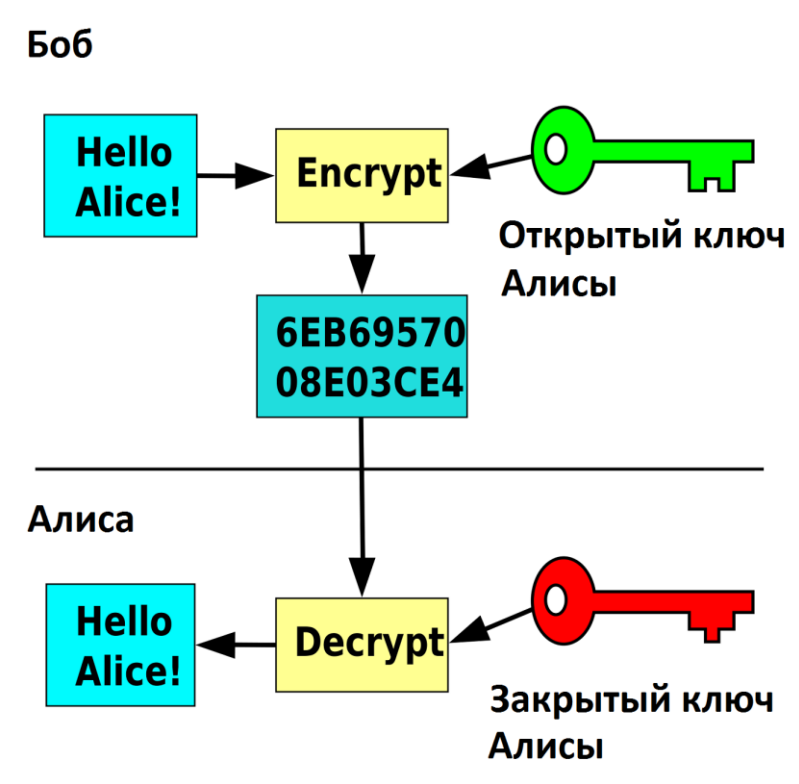
- для любого удаленного доступа к сертифицируемой по PCI DSS среде нужно включить мультифакторную аутентификацию.

Изменения для всех:

- при внесении любых изменений в сертифицированную инфраструктуру следует проверять выполнение требований PCI DSS.

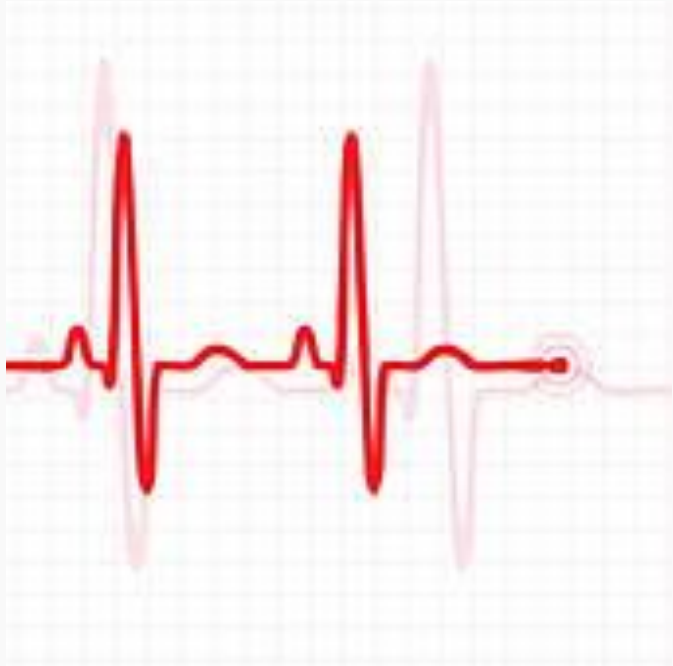
Изменения для поставщиков услуг:

- архитектуру системы шифрования нужно документировать.



Изменения для поставщиков услуг:

- контролировать работоспособность всех систем безопасности.



Изменения для поставщиков услуг:

- тестирование на проникновение для проверки сегментации среды проводить не реже одного раза в шесть месяцев.

Изменения для поставщиков услуг:

- разработать и выполнять программу поддержки соответствия требованиям стандарта PCI DSS.

Изменения для поставщиков услуг:

- раз в квартал проверять, что работники корректно выполняют процедуры анализа журналов протоколирования событий, осуществляют пересмотр правил межсетевого экранирования, применяют стандарты конфигурации для новых систем, реагируют на сигналы систем безопасности, а также соблюдают процедуры управления изменениями

= выборочный внутренний аудит

SSL и TLS:

- до **30 июня 2016 года** все поставщики услуг должны обеспечить поддержку протокола TLS версии не ниже версии 1.1;
- до **30 июня 2018 года** полностью отказаться от использования небезопасных версий протоколов (прощай SSL всех версий и TLS 1.0).

PCI DSS Training:

…кстати, Джереми Кинг лично приедет рассказать о новых версиях стандартов PCI…

21-22 июля 2016 года

Санкт-Петербург

www.paymentsecurity.ru

Вопросы?

E-mail: kristina.andreeva@deiteriy.com

Facebook: Christie Andreeva