

Хранить нельзя удалять

14.04.2009

Типичные проблемы выполнения требований стандарта PCI DSS к хранению данных о владельцах платёжных карт.

Сергей Шустиков, QSA-аудитор Digital Security

Стандарт PCI DSS, уже ставший необходимой реальностью для российских компаний, занимающихся обработкой платёжных карт, предъявляет ряд требований к условиям хранения данных о владельцах платёжных карт. Из них стоит выделить два, вызывающих наибольшие трудности.

Первым таким требованием является запрет на хранение критичных аутентификационных данных. Под критичными аутентификационными данными в стандарте понимаются данные, хранимые на магнитной дорожке карты, PIN и PIN-блок, а также CVC2/CVV2. Их хранение после авторизации недопустимо ни при каких обстоятельствах, даже в зашифрованном виде. Исключением является только хранение звукозаписи телефонного звонка в call-центр компании, в течение которого может быть произнесено проверочное значение CVC2/CVV2. К сожалению, приходится констатировать тот факт, что данные магнитной дорожки часто встречаются хранящимися в открытом виде в лог-файлах приложений, управляющих терминальными устройствами. Проблема решается несложно, правда в некоторых случаях потребуется взаимодействие с поставщиком программного обеспечения.

Второе требование гласит, что при хранении данных о владельцах платёжных карт, как минимум номер карты (PAN) должен быть представлен в нечитаемом виде. Нечитаемым PAN может стать в результате его укорачивания, маскирования или шифрования. Единственным обратимым способом хранения номера карты в нечитаемом виде является шифрование. Стоит отметить, что большинство приложений, применяемых российскими компаниями для обработки карточных данных, еще не научились хранить информацию в зашифрованном виде. Для решения этой проблемы можно использовать прозрачные средства шифрования СУБД, например Oracle Transparent Data Encryption. Не следует также забывать и о носителях резервных копий, содержащих карточные данные. Защитить их можно, например, при помощи Oracle Secure Backup. Данные, хранимые на файловом сервере, можно защитить, используя шифрование дисковых массивов. При шифровании на уровне диска следует применять процедуры управления доступом к зашифрованным данным, независимые от средств операционной системы, об этом говорит требование 3.4.1 PCI DSS.

Планируя внедрение систем шифрования данных, стоит помнить о том, что в любом случае, независимо от применяемой технологии, это отрицательно скажется на производительности, поэтому вопрос расширения вычислительных мощностей должен стоять не на последнем месте.

Об авторе

Сергей Шустиков – QSA-аудитор, ведущий аналитик по информационной безопасности компании Digital Security, специализируется на системах менеджмента безопасности. Область профессиональных интересов охватывает разработку систем менеджмента информационной безопасности в соответствии с международными стандартами и проведение аудитов на соответствие требованиям ряда стандартов индустрии защиты информации (PCI DSS, ISO/IEC 27001:2005, СТО БР-ИББС-1.0).

О стандарте PCI DSS

Стандарт PCI DSS (Payment Card Industry Data Security Standard) предназначен для обеспечения безопасности обработки, хранения и передачи данных о держателях платежных карт в информационных системах компаний, работающих с международными платежными системами Visa, MasterCard и другими. Стандарт разработан сообществом PCI Security Standards Council, в которое входят мировые лидеры на рынке платежных карт, такие как American Express, Discover Financial Services, JCB, MasterCard Worldwide и Visa International.

Под действие требований стандарта попадают банки, процессинговые центры, поставщики ИТ-услуг, торгово-сервисные предприятия, и иные организации, обрабатывающие транзакции по международным платежным картам. К части этих компаний международные платежные системы предъявляют требование о прохождении обязательного ежегодного аудита компанией, обладающей статусом QSA.

Текущая версия стандарта 1.2 выпущена 1 октября 2008 года.