Информзащита
Системный интегратор

Стандарты в информационной безопасности: панацея или плацебо?

Бабенко Алексей Андреевич, старший аудитор ЗАО НИП «Информзащита»

Справка ТБ

Бабенко Алексей Андреевич окончил факультет прикладной математики и кибернетики Томского Государственного Университета. Старший аудитор Департамента консалтинга и аудита компании «Информзащита», область компетенций — аудит и консалтинг в области приведения в соответствие со стандартами PCI DSS, PA-DSS, ИББС СТО БР, ISO 27001, требованиями 152-ФЗ, безопасности web-технологий. В 2010 году получил статус Qualified Security Assessor, в 2011 — Payments Application Qualified Security Assessor. Активный участник и спикер на различных конференциях, посвященных информационной безопасности. Участник команды SiBears в соревнованиях CTF. В свободное время предпочитает заниматься спортом (баскетбол, джиу-джитсу) и чтением книг.

Стремительное развитие информационных технологий в наши дни вслед за несомненными удобствами привело к появлению новых видов мошенничества и киберпреступлений. По пятам развития ИТ следует информационная безопасность. Приятная тенденция последнего времени — рост понимания ее важности и необходимости. Не последнюю роль в этом играют находящиеся на слуху громкие компрометации информационных систем, в один момент приносящие колоссальные финансовые потери. В отдельных случаях они и вовсе могут привести к необратимым для бизнеса последствиям. В результате, защита информации становится не столько делом организации, сколько критерием надежности для ее партнеров и клиентов.

Стандарты информационной безопасности призваны помочь компании создать требуемый уровень защиты информации, а так же являются критериями измерения уровня текущей защищённости и эффективности процессов управления информационной безопасностью. Кроме национальных стандартов на территории стран СНГ имеют достаточную известность два международных: стандарт ИБ ISO/IEC 27000 и стандарт безопасности данных инфраструктуры платежных карт PCI DSS.

Стандарты серии ISO/IEC 27000, разработанные и опубликованные совместно Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссии (IEC), содержат рекомендации к системе управления информационной безопасностью. Сертификация осуществляется на основе требований, описанных в стандарте ISO/IEC 27001, и производится только аккредитованными компаниями-аудиторами.

Выполнение требований стандарта в странах СНГ не носит обязательный характер, поэтому его распространенность достаточно низкая. На апрель 2012-го года число компаний, обладающих действующими сертификатами соответствия ISO/IEC 27001, в странах СНГ составляло 21. Для сравнения, в Японии, где для ряда компаний сертификация обязательна, 4061 организация обладает действующим сертификатом. При этом стоит отметить, что общее количество компаний в СНГ, внедривших стандарты серии 27000, гораздо выше, поскольку множество организаций, осуществивших внедрение, ставят своей целью не сертификацию, а четко выстроенные процессы управления и подержания уровня информационной безопасности.

Стандарты серии 27000 часто являются первым шагом в развитии систем управления информационной безопасностью. Их использование в качестве ориентира — хорошая практика, которая позволяет построить эффективную систему менеджмента информационной безопасности.

Payment Card Industry Data Security Standard (PCI DSS, Стандарт безопасности данных индустрии платежных карт) был создан Советом по безопасности индустрии платежных карт (PCI SSC), организованным по инициативе пяти крупнейших мировых платежных систем — Visa, MasterCard, JCB, American Express и Discover. Основной целью создания стандарта являлось обеспечение единого уровня информационной безопасности для всех участников индустрии, обеспечивающей обслуживание платежных карт. Безопасность является одним из главных критериев при использовании технологий, связанных с финансами. Поэтому организация защиты данных платежных карт одна из приоритетных задач каждой платежной системы.

В отличие от стандартов серии 27000, стандарт PCI DSS обязателен для применения всеми организациями, обрабатывающими платежные карты. При этом требования к оценке соответствия зависят от суммарного объема обработанных транзакций: от самостоятельной оценки до прохождения сертификационного аудита. Последний проводится компанией, имеющей статус PCI QSA.

Еще одним существенным отличием PCI DSS является его большая детализация. При выполнении требований ISO 27001 защитные меры выбираются по результатам оценки рисков информационной безопасности и их достаточность оценивается сотрудниками организации. При реализации PCI DSS конкретные решения уже определены, а «маневр», в большинстве случаев, допускается только при выборе реализующих технологий.

Кроме того, что платежные системы Visa и MasterCard ввели требования по обязательному соответствию стандарту PCI DSS, были обозначены крайние сроки приведения к соответствию. Это привело к тому, что большинство крупных игроков индустрии платежных карт проделали работу по выполнению требований. В результате, это отразилось на общем уровне защищенности как отдельных участников, так и всей индустрии безналичной оплаты.

Стоит отметить, что стандарт может быть использован организациями, не связанными с индустрией платежных карт, при планировании системы информационной безопасности. Стандарт на постоянной основе обновляется и содержит актуальные меры и рекомендации по снижению угроз информационной безопасности.

Применение стандартов и соответствие их требованиям, несомненно, является хорошей практикой и большим шагом вперед при выстраивании системы информационной безопасности. Однако сам факт соответствия не всегда прямо пропорционален уровню защищённости. Для подтверждения можно вспомнить пример с компрометацией информационной системы крупнейшей в мире розничной сети Wal-Mart, которая на момент инцидента имела действующий сертификат соответствия PCI DSS. Объяснением такому факту могут служить несколько причин. Во-первых, сертификация осуществляется после проведения аудита, который представляет собой оценку состояния на текущей момент времени. В течение года, на который распространяется действие сертификата, в компании перестают работать процедуры, сделанные «для галочки», с целью пройти проверку. Во-вторых, не исключена ошибка самих аудиторов в определении области проверки, состава проверяемых компонентов и общих выводах.

Наконец, всегда стоит помнить, о том, что идеальной безопасности не бывает, и обеспечение безопасности — это постоянный процесс защиты от новых угроз. Стандарты не «волшебная пилюля», а лишь полезный инструмент в достижении максимального уровня защиты.

ЗАО НИП «ИНФОРМЗАЩИТА»
127018 Москва, ул. Образцова, д. 38
Тел.: (495) 980-2345
E-mail: market@infosec.ru
www.infosec.ru

ИНН: 7702148410