

## «Безопасность на первом месте» или «Соответствие на первом месте»? - Продолжение

27.08.2009

*Продолжение [статьи](#), опубликованной 20 августа этого года, посвященной двум принципиально разным подходам к внедрению стандарта PCI DSS. Речь пойдет об отношении между соответствием PCI, и соответствием требованиям ASV-сканирования.*

*Антон Чувакин, директор направления PCI Compliance компании Qualys, Ph. D.*

### Проверка соответствия ASV-сканированием

Требование 11.2 стандарта PCI DSS предусматривает проведение ежеквартального внешнего сканирования сертифицированным поставщиком услуг сканирования (ASV). Такое сканирование должно показать, что в периметре инфраструктуры отсутствуют PCI-уязвимости. Приведем пример уязвимостей, которые считаются причинами неудачного ASV-сканирования:

- Уязвимости с оценкой в 4.0 баллов и выше по метрике CVSS v2.0 приведут к несоответствию сканируемых IP-адресов требованиям PCI.
- Уязвимости, которые могут привести к реализации атак типа «SQL-инъекция» и «межсайтовое выполнение сценариев», приведут к несоответствию сканируемых IP-адресов требованиям PCI.

Являясь простейшим методом проверки соответствия PCI, ASV-сканирование позволяет организациям узнать о возможных уязвимостях периметра среды данных о держателях карт.

Любой специалист в области безопасности понимает, что новые уязвимости находят в программных приложениях и платформах каждый день, и частое сканирование уязвимостей позволяет организациям обнаруживать их, а потом устранять, повышая, тем самым, уровень безопасности. Это наглядный пример мышления в стиле «Безопасность на первом месте!»

Что с другой стороны ожидает организацию, которая руководствуется принципом «Соответствие на первом месте!»? Что именно происходит, когда такого рода организация проводит повторное сканирование прямо перед отправкой Отчета о Соответствии (RoC) в банк-эквайер и обнаруживает, что недавно были найдены уязвимости в используемом ПО?

К сожалению, многие организации зачастую считают, что столкнулись с ситуацией, при которой «кто-то нарушил их соответствие PCI» (!).

Возможно, раздражение проявится в вопросах вроде: «Ну почему это сканирование обнаружило уязвимости, когда мы как раз хотели сообщить об успешном завершении проекта по достижению соответствия PCI? Почему мы лишаемся соответствия, полученного с таким трудом? А может просто

заменить механизм сканирования на другой, который покажет, что наша система соответствует требованиям PCI?»

В итоге, не так уж важно сколько раз эксперты в сфере безопасности вещали: «Безопасность на первом месте!» Если некоторые организации не принимают безопасности во всей ее сложности, пренебрегая ею годами, то девиз «Соответствие на первом месте!» становится для них определяющим. Ну, по крайней мере, это они понять в состоянии! Потом слоган «Соответствие на первом месте!» превращается в «ТОЛЬКО соответствие!», формальное следование перечням требований заменяет анализ рисков, блок-схемы заменяют осмысление угроз и уязвимостей.

Что происходит дальше? Разумеется, в их систему проникают злоумышленники и крадут карточные данные. А СМИ пишут о них вдохновенную историю! Ну и наконец, Совет PCI SSC штрафует их за то, что у них не было даже соответствия требованиям...

В этот момент на них неожиданно нисходит прозрение - безопасность это действительно важно!

В результате, не так уж трудно выбрать между двумя принципами: «Безопасность на первом месте!» или «Соответствие на первом месте!». Тем не менее, если после прочтения написанного вы всё равно взволнованно скажете: «Соответствие на первом месте!», пожалуйста, убедитесь хотя бы в том, что после этого вы скажете: «А безопасность на втором!».

На этом этапе полезно будет вспомнить о Титанике (который, как мы все знаем, затонул в 1912 году, столкнувшись с айсбергом). Было установлено, что корабль действительно соответствовал всем требованиям безопасности того времени. А основная проблема была в том, что эти требования были написаны в 1894 году, когда размеры и конструкция судов такого типа быстро менялись. В требованиях указывалось, что на все суда водоизмещением более 10 000 тонн требуется установка 16 спасательных шлюпок, и именно столько шлюпок было на Титанике. Другими словами, Титаник полностью соответствовал требованиям безопасности - идеальный пример последствий принципа «Соответствие на первом месте!»

## Об авторе

Антон Чувакин является известным экспертом по информационной безопасности, автор книг «Security Warrior», соавтор «Know Your Enemy II», «Information Security Management Handbook», «Hackers Challenge 3», «PCI Compliance», «OSSEC HIDS», а также многих публикаций по безопасности. В свободное время пишет заметки в своем блоге [www.securitywarrior.org](http://www.securitywarrior.org). Автор многих докладов по вопросам информационной безопасности на конференциях в США, Великобритании, Сингапуре, Испании, Канаде, Польше, Чехии, России и других стран. Защитил диссертацию на соискание ученой степени Ph. D. в Университете Стони Брук, Нью-Йорк, США.

## 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 1.2.1 выпущена в июле 2009 года.