

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

31.08.2009

*Заключение цикла опубликованных ранее статей «Безопасность на первом месте» или «Соответствие на первом месте»? посвященного двум принципиально разным подходам к внедрению стандарта PCI DSS. Теперь о том, как можно упростить себе жизнь на пути к PCI.*

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

### Упрощение безопасности под управлением PCI

Обеспечение безопасности процесс сложный, равно как и соблюдение требований PCI. Однако нам нужно подумать над тем, как упростить процесс достижения соответствия с одновременным повышением уровня безопасности для организаций. Итак, как же облегчить процесс достижения соответствия PCI, в то же время, повышая безопасность? Упрощение выполнения требований PCI, и в то же время, повышение уровня защищенности может облегчить жизнь многих экспертов в области безопасности.

Для начала, вспомним былые времена, когда только профессионалы владели магией сканирования сети на предмет выявления уязвимостей. Никто не спорит, что сейчас управлять уязвимостями стало гораздо легче, хотя в то же время нельзя сказать, что это стало легко. Люди, задумывающиеся об упрощении процесса достижения PCI, делятся на две группы.

Первые часто просят о том, чтобы им просто разрешили не выполнять все эти требования. Такие люди склонны отвечать «Да» при заполнении опросных листов (SAQ), даже не задумываясь о том, что действительно нужно сделать для выполнения указанных требований.

Во второй группе обычно знают, что их программа повышения уровня защищенности позволяет организации соответствовать требованиям PCI, и отвечают на вопросы для того, чтобы им легче было это доказать.

Несложно догадаться, что организации, входящие в эти группы существенно отличаются друг от друга. Некоторые представители группы номер 1 спутают межсетевой экран с экраном монитора. Люди из группы номер 2 часто задумываются над тем, как связать свой риск-ориентированный подход к обеспечению безопасности с подходом PCI, ориентированным на внедрение конкретных мер защиты.

Более того, люди из первой группы часто говорят что-то вроде: «Соответствие требованиям PCI это легко - надо просто пройти ASV-сканирование и ответить «Да» на все вопросы листа самооценки». Тем не менее, упростить процесс достижения PCI, не забывая при этом о безопасности, можно даже для тех, кто желает, чтобы вопрос о соответствии PCI исчез как страшный сон. В организации следует

создать благоприятные условия для совершения «правильных» действий (приводящих к снижению рисков) и затруднить совершение «неправильных» действий (увеличивающих риски для бизнеса).

С другой стороны, во второй группе можно услышать такие возгласы как: «У нас хорошая программа повышения уровня защищенности и мы отлично справляемся с информационными рисками. Зачем нам тратить лишнее время на PCI? Ведь наш уровень безопасности и без того высок!» Скорее всего, такого рода организации действительно тщательно работают над безопасностью и хотят использовать свои достижения в качестве доказательств соблюдения требований PCI. В этом случае упрощение достижения соответствия PCI будет заключаться в упрощении процесса проверки соответствия. Разумеется, не надо пренебрегать их программами повышения уровня защищенности!

## **Заключение**

В заключение. Если вы отказываетесь даже попытаться понять информационную безопасность и информационные риски (несмотря на все связанные с этим трудности), соответствие PCI становится инструментом для принятия определенных решений по присвоению рискам «нелегального» статуса. Другими словами, если вы отказываетесь оценивать риски и не хотите планировать внедрение контрмер, позволяющих их снизить, соответствие PCI превращается в простой шаблонный список обязательных для выполнения требований. Какой бы ни была ваша ситуация, существуют пути, позволяющие достичь соответствия PCI, повышая или сохраняя при этом безопасность: упрощение подтверждения выполнения требований, упрощение процесса аудита – это освобождает время на работы по повышению безопасности (в той степени, в которой это необходимо). Также нужно создать условия, в которых принять «правильное» решение будет проще, чем принять «неправильное». Даже выбирать между принципами «Безопасность на первом месте» и «Соответствие на первом месте!» в результате станет легче.

## **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.