# о бедных заказчиках молвите слово

текст Вячеслав Медведев, ведущий аналитик отдела развития компании «Доктор Веб»

**Теоретически, вопрос о том, что нужно для обеспечения информационной безопасности в условиях рынка, решает заказчик (естественно, учитывая действующие в отрасли требования регуляторов). Кто еще, кроме него, знает, что ему нужно защищать, какие угрозы для него актуальны и, самое главное, сколько он может потратить на защиту. Но это в теории. На практике (если не учитывать стоимость необходимых решений) все решает информированность специалистов заказчика и квалификация имеющихся на местном рынке профессионалов.**

Не нужно создавать очередную теорию заговора – необходимая для принятия решений информация никем не скрывается. В условиях конкуренции со стороны вендоров запросить и получить нужные сведения вполне реально. Нужно только задать правильные вопросы. Проблема одна: чтобы задать вопрос, нужно понимать, о чем именно спрашивать.

На деле же выбор средств и методов защиты в большинстве случаев осуществляется на основе знаний, не имеющих никакой связи с реальностью. Не будем в качестве примера знаний об уровне угроз говорить о том, сколько на самом деле вредоносных файлов приходит тем же антивирусным вендорам в день или в месяц – об этом говорилось неоднократно. Посмотрим на иные примеры знаний, скажем, связанные с банкоматами.

В связи с прекращением поддержки Windows XP в СМИ прокатилась волна публикаций, предсказывающих нарастание числа уязвимостей в ОС, установленных на банкоматах, и даже переход на иные ОС. Но действительно ли проблема возникла только сейчас? Будем честными – насколько регулярно до часа X в банкоматы устанавливались обновления безопасности? Эти обновления требуют время от времени перезагрузки. В какой момент перезагрузка понадобится – никому не известно. Да, банкоматы перезагружаются и в ходе регламентных работ, и при инкассации, но применялись ли при этом обновления?

Не меньше «знаний» о необходимости использования защитного ПО. До сих пор далеко не всем известно, что PCI DSS требует именно антивирусного ПО: вопросы по данному требованию встречаются постоянно. Применение ПО, ориентированного на подсчет контрольных сумм, не решает проблемы заражений – антивирусные программы давно отказались от таких подсистем, хотя и имели их на заре своего развития. Подсчет контрольных сумм обеспечивает целостность программ, но не может обеспечить целостность системы в целом.

На данный момент для защиты финансовых структур разработано много действительно хороших стандартов. При грамотном применении они дают необходимый эффект. Проблема в том, что эти стандарты не дают возможности определить необходимость той или иной меры защиты, опираясь на текущий уровень угроз и действительную эффективность предлагаемой заказчику меры защиты. К сожалению, выбор в большинстве случаев осуществляется на основе сложившихся в обществе и ИТ-сообществе мифов. Несмотря на огромное количество общедоступной информации, востребованность ее остается крайне невысокой, в том числе и представителями системы образования.

На сегодняшний день актуальная задача – не выработка требований, а создание системы информирования, доводящей критически важные сведения до специалистов по ИТ-безопасности и сотрудников, ответственных за выбор решений. Кто, скажем, знает о доступности практически единственной специализированной разработки для защиты банкоматов и терминалов – Dr.Web ATM Shield? Не говоря уже о наличии обучающих курсов по принципам защиты банкоматов.

Создание системы распространения ИБ-аналитики в рамках банковского CERT становится сверхнасущной задачей. NBJ