Платежные системы: на лезвии бритвы

Платежные экосистемы компаний в России и за рубежом постоянно подвергаются атакам на POS-терминалы и заражению вредоносным кодом, поэтому вопрос защиты стоит очень остро. С одной стороны, компаниям непросто получать и продлевать сертификаты соответствия со стандартами PCI. С другой — одного соответствия стандартам зачастую оказывается недостаточно, чтобы противостоять серьезным атакам. Кроме того, в вопросах безопасности устройств самообслуживания нельзя ограничиваться следованием стандартам и рекомендациям, какими бы полными они не были. Даже ежечасное обновление вирусных баз не спасает от таргетированной атаки, а ведь атаки на устройства самообслуживания практически всегда — таргетированные. Тем более стандарты — это не антивирусные базы, они не обновляются несколько раз за день.

Удержаться на одном уровне с атакующими киберпреступниками — серьезное испытание для бизнеса, ведь угрозы должны быть обнаружены и нейтрализованы до того, как ими смогут воспользоваться злоумышленники. В случае же обнаружения произошедшего инцидента возникает необходимость в расследовании, а это тоже требует немалых затрат. Нужны серьезные вложения в системы обнаружения вторжений, при этом любое изменение должно рассматриваться как потенциальная уязвимость. Компания Sony, например, потратила на расследование недавнего взлома своих систем около 15 млн долл.

Результатом успешного вторжения в элемент платежной системы обычно является компрометация информации, такой как имена и фамилии держателей пластиковых карт, номера карт, даты истечения срока действия и SSV-коды. Этой информации злоумышленнику достаточно, чтобы получить прибыль — в киберпреступных кругах данные с карточек используются или для создания дубликатов, с которых уже можно снять наличные деньги, или для использования безналичного расчета. Даже если злоумышленники не смогли успешно завершить атаку и продать полученные данные, сам факт компрометации ведет к необходимости перевыпуска миллионов пластиковых карточек, вызывает недовольство клиентов и приводит к финансовым и репутационным потерям.

Михаил Калиниченко
Исполнительный директор ООО «СНС Холдинг»

При применении новейших технологий заражения устройств злоумышленники получают доступ непосредственно к наличным деньгам, хранящимся в терминалах и банкоматах, что увеличивает прибыль и позволяет обходиться без посредников. Однако цена таких технологий велика, особенно если заказывать специализированные сборки вредоносного программного обеспечения под конкретные нужды, так что возрастает и масштаб атаки, необходимой для получения преступниками серьезной прибыли.

За последний год появилось множество троянов, созданных специально для банкоматов. Практически все они обладают функционалом, позволяющим автоматически отключать традиционную защиту, обнаруженную на устройстве в процессе заражения. Именно поэтому полноценному защитному продукту необходимо защищать не только систему, но и себя.

Избежать большинства описанных проблем можно, используя специализированные защитные решения, разработанные для банкоматов и прочих устройств самообслуживания. Safe`n`Sec TPSecure изначально создавался с целью не только обеспечить максимально возможную безопасность защищаемых систем, но и помочь клиентам соответствовать требованиям регуляторов. За прошедшее время Safe`n`Sec TPSecure развился в продукт, учитывающий как требования Центробанка России, так и стандарты PCI DSS. Отметим, что по сравнению с обычными компьютерами у устройств самообслуживания есть особенности, сводящие на нет усилия традиционных защитных продуктов по защите системы. Постоянные обновления антивирусных баз, рутинные для офисных компьютеров, невозможны по техническим причинам, а защиту от инсайдеров антивирусы не способны предоставить в принципе. Происходящие инциденты подлежат расследованию, но как выявить инцидент в период штатного функционирования устройства, если он обошел обычные защитные системы? С системой же защиты целостности программной среды любое несанкционированное изменение будет восприниматься как потенциальная угроза и привлечет внимание.

В области защиты банкоматов перестраховаться невозможно: потенциальные риски слишком высоки, чтобы пренебрегать ими.