персональные данные персональные данные персона № 6 (59), июнь 2013 данные
Информационно-аналитический журнал для операторов персональных данных

«Меры и средства защиты персональных данных»

Защита информации в процессе доступа к сервисам ДБО требует полноценной защиты на каждом этапе

Материал участвует в конкурсе

Дистанционное банковское обслуживание (ДБО) благотворно влияет на рынок на всех уровнях кредитно-финансовой сферы деятельности от кредитных организаций до конечного пользователя. Клиенты финансовых учреждений год за годом обретают все больше возможностей управлять своими счетами, а организации снижают издержки на содержание офисов и получают возможность предлагать клиентам дополнительные услуги. Но от такого взрывного роста выигрывают не только банки и пользователи услуг, но и третья сторона - преступный мир, мошенники и кибермошенники.

Финансовые структуры всего мира проявляют всё большую озабоченность проблемой безопасности при дистанционном банковском обслуживании и, согласно статистике из открытых источников, среди всех видов мошенничества в сети Интернет аферы в системах ДБО стали в 2008-2009 годах самым прибыльными из них. Так в чём причина сложившейся ситуации и почему в ближайшее время не предвидится кардинальных изменений?

Данные в финансовой сфере являются наиболее лакомой целью для преступников, так как их проще всего превратить в деньги, а успешно выведенные из строя сервисы финансовой организации наносят куда более явный материальный и репутационный ущерб, чем, например, утечка коммерческой тайны из компании или персональных данных из медучреждения. В финансово-кредитных учреждениях доля случайных утечек информации гораздо ниже, чем в целом по всем индустриям, а на злонамеренные утечки приходится 68% случаев, согласно данным InfoWatch за 1 полугодие 2012 года. Произвести хищение информации любым способом, как с помощью случайной или злонамеренной утечки, так и с помощью взлома или заражения системы вредоносным кодом, проще всего в ситуации, когда данные пользователей выходят за пределы защищённой среды банка или иного учреждения, а значит, ДБО является самым уязвимым элементом этой сферы рынка.

ДБО можно условно разделить на три вида:

Первый вид ДБО – разнообразные *устройства самообслуживания*. Банкоматы, POS-терминалы и информационные киоски уже давно и прочно вошли в нашу жизнь. Увеличение числа сервисов, предлагаемых клиентам через банкомат, ведет к увеличению «площади атаки» для потенциальных злоумышленников. Кибератаки на банкоматы и сети банкоматов принимают самые различные формы, от грубых нападений с целью выведения системы из строя, как в мартовской атаке на южнокорейский банк Shinhan, до скрытого внедрения вредоносного кода в сами устройства. Согласно отчету экспертов ATMIA за 2012 год, логические угрозы для банкоматов уже вышли на третье место среди основных угроз, и только использование новых технологий в области защиты информации способно остановить или хотя бы замедлить эту тревожную тенденцию - традиционные подходы, требующие широкополосного доступа в Интернет и существенных ресурсов, не работают в условиях ограниченной программной среды банкомата.