Банк под замком

Текст: **Александр Федоров,** начальник управления информационной безопасности ЗАО «БИС»

Давно известно: мало заработать деньги, их надо еще и сберечь. Развитие банковской системы, на первый взгляд, решает эту проблему. Все-таки вооруженные ограбления банков – большая редкость. Но, как свидетельствует практика, для грабежа не нужен нож. Для этого даже не обязательно выходить из дома. Современным плохим парням достаточно компьютера, подключенного к сети Интернет.

Банковская система не сможет развиваться без совершенствования систем дистанционного банковского обслуживания. Это – аксиома. Точно так же очевидно, что системы ДБО несут с собой не только удобства, но и немало рисков. В последнее время отечественные кредитные организации в массовом порядке подвергаются атакам высококвалифицированных жуликов, этой своеобразной финансовой саранчи. К примеру, в начале лета этого года была пресечена деятельность организованной преступной группы, которая похищала деньги с помощью компьютерных вирусов. Выяснилось, что общее число зараженных компьютеров составило свыше 1,5 миллионов (!). Данное дело было раскрыто, но это, скорее, исключение из правила, потому что борьба с киберпреступлениями чрезвычайно сложна.

Любители тут не ходят

Утечку финансовых ресурсов организуют не одиночки, а мощные, грамотно сформированные преступные сообщества. Их вполне можно назвать профессиональными. Внутри такое сообщество разбито на группы, изолированные друг от друга, что позволяет им эффективно уводить деньги со счетов и оставаться ненайденными. Ни одна кредитная организация, какой бы мощной службой безопасности она ни располагала, не сможет самостоятельно найти преступников. Казалось бы, что проще? Правоохранительные органы должны дать указания провайдеру, который должен назвать IP-адрес, с которого была произведена атака. Но это теоретически. Существует много вариаций с IP-адресом и немало сетей, например, анонимные прокси и p2p сети, которые и построены таким образом, чтобы сделать пользователя анонимным. Вся информация о клиенте и его IP-адресе скрывается, и получить ее – очень сложная задача.

То, что с киберпреступниками бороться можно только всем миром – сейчас это уже очевидно. Разумеется, можно сказать, что поскольку деньги снимаются с банковских счетов, то и проблему должны решать сами банки. Но такой подход иррационален. Ни один банк не станет иметь дело с компанией-разработчиком, которая предлагает ему незащищенные информационные системы. Только в содружестве с правоохранительными органами (вооруженными, заметим, необходимым законодательством) финансовой организации и компании, разрабатывающей системы дистанционного обслуживания, можно добиться положительного результата.

Задачи ясны

Банки нуждаются во все более совершенных и более защищенных системах ДБО. Для них это вопрос успеха в конкурентной борьбе: очевидно, что клиент пойдет в тот банк, где обслуживание займет меньше времени, при этом идеальный вариант – когда необходимость посещения офиса минимизирована.

Итак, банкам нужны новые ДБО. Но они должны быть надежны. Задача, стоящая перед компанией, разрабатывающей системы дистанционного банковского обслуживания, формулируется четко: стремиться сделать максимально невозможным несанкционированный доступ к счету клиента. Решение этой задачи осложняется тем, что в современных условиях не


Александр Федоров

только юридические, но и физические лица проводят операции постоянно, и движения по счетам идут ежедневно, а не раз в неделю. Банк обязан предоставить своим клиентам возможность проводить транзакции так часто, как это им необходимо, при этом проверки не должны замедлять работу клиентов. Следовательно, мало того, что системы защиты должны быть надежны, плюс к тому, они должны работать в режиме он-лайн 24 часа в сутки 7 дней в неделю, 365 дней в году.

Линии обороны

Системы ДБО, разрабатываемые компанией БИС, имеют многоуровневую защиту. Если раньше считалось достаточным использовать логин-пароль, технологии шифрования и электронной цифровой подписи, то теперь возросшее «мастерство» мошенников требует более серьезных мер.

Существуют три основных уровня защиты, оберегающих банк и деньги его

клиентов. Построены они по понятному принципу: от простого к сложному, а использование их зависит исключительно от желания банка.

Первый уровень – логин, пароль и список одноразовых паролей.

Для начала работы со счетом клиент должен ввести известные ему постоянный логин-пароль, а для подтверждения операции – пароль из полученного им списка одноразовых паролей.

Второй уровень – логин, пароль и sms-сообщение.

Клиент для того, чтобы получить возможность работы со счетом, вводит свой постоянный логин и один из одноразовых паролей, после чего дополнительно получает от банка sms-сообщение с одноразовым паролем для подтверждения операции. Отсутствие какой-либо иной реакции клиента на sms-сообщение означает, что клиент в курсе проводимой операции.

Третий уровень – логин, пароль, sms-сообщение, секретный ключ на внешнем носителе.

Ко всем вышеперечисленным действиям клиента добавляется подключение с использованием внешнего носителя с секретным ключом. Речь идет о специализированной флэшке, выданной клиенту в банке. Специализированный шлюз безопасности «видит» флэшку с ключом, и если идентификация этих данных свидетельствует, что они совпадают с теми, что хранятся в шлюзе безопасности банка, тогда клиента авторизуют, и он получает возможность работать со своим счетом, используя логин-пароль и sms-информирование.

Все три уровня защиты в сущности стандартны. Подключение этих уровней (одного, двух или всех трех) – дело банка. Клиент, намереваясь открыть счет, узнает о том, как именно будут защищены его деньги, и на основании этого может сделать вывод: стоит ли размещать свои средства в данном банке. Если клиент полагает достаточным обходиться логином и паролем, он откроет счет в банке, где установлена система ДБО с первым уровнем защиты. Если его это не устраивает – он, вероятно, отправится искать другой банк.

Почему первого или второго уровня может быть недостаточно

В начале статьи речь шла о группе мошенников, которые заразили компьютерным вирусом 1,5 млн компьютеров. Дело это, разумеется, непростое, но эффективное. Вирус, работающий в компьютере клиента, может самостоятельно проводить операции, например, отдать распоряжение о перечислении денег на какой-то заранее определенный мошенниками счет. Тут и пригодится sms-сообщение: без

ввода пароля, высланного по sms, операция не будет авторизована, а клиент, получив известие о том, что с его счетом началась работа, сможет вовремя отдать распоряжение о ее блокировании.

Есть и более изощренные способы грабежа. Например, перечисляемая сумма может быть (без ведома клиента, разумеется) изменена на большую, или средства могут быть направлены на другой счет, а не на тот, что указал клиент. Тут от клиента требуется внимательность: получив извещение от банка, он должен проверить, соответствует ли его распоряжение тому, что видит он в sms-сообщении. Все эти проверки необходимы, особенно если речь идет о солидных счетах. Когда на кону крупные суммы, мошенники не поскупятся на затраты, чтобы заполучить доступ не только к компьютеру владельца счета, но и к его мобильному телефону.

Дополнительные меры

Три этих уровня защиты представляют собой, если так можно сказать, первую линию обороны. Но, разумеется, она не единственная, поскольку практический опыт подсказывает: этих мер недостаточно. В наших системах ДБО используются и другие защитные механизмы, о которых не принято говорить, направленные, прежде всего, на тщательную проверку транзакций. Безусловно, это самая сложная часть защиты.

Формально все благополучно. Клиент получил все предупреждения, подтвердил свое желание произвести операцию. И все-таки повод для сомнений имеется: некоторые параметры операции вызывают повышенное внимание системы защиты. Для того чтобы не пропустить их, применяются так называемые настраиваемые опции. По согласованию с клиентом некоторые операции могут проходить дополнительную проверку.

Механизм дополнительной проверки действует следующим образом: сначала система защиты автоматически приостанавливает проведение операции, попадающей под эти параметры, затем к делу подключается сотрудник службы информационной безопасности банка, который и ведет разбирательство. Соответствующие службы банка должны оперативно связаться с клиентом и получить от него подтверждение на проведение транзакции или отказ от нее.

Разумеется, платеж может быть первым в финансовых взаимоотношениях между клиентом банка и получателем, и сумма может быть больше, чем это бывает обычно. Само по себе это нормально, но стоит подстраховаться. Также понятно, что клиент, в принципе, может работать со своим счетом из любой точки земного шара, и нельзя составить постоянный список используемых IP-адресов. И все же, если система защиты видит, что IP-адрес не принадлежит российскому провайдеру или, допустим, принадлежит анонимному прокси-серверу, она на всякий случай подает сигнал: «Проверьте, IP-адрес вызывает сомнения».

Согласитесь, такая многоуровневая система защиты осложняет жизнь злоумышленникам. Потому что только в том случае, если пройдены три первых линии защиты, если транзакция проверена по всем дополнительным параметрам, и клиент подтверждает намерение ее провести, только тогда операция получает «зеленый свет». Последнее, что хотелось бы отметить в связи с данной темой: наш рассказ о том, как действует система защиты, занял куда больше времени, чем само действие. И это тоже одно из преимуществ системы ДБО, разработанной специалистами компании БИС.

Перспектива

Как известно, защитники и нарушители закона находятся в постоянном противоборстве. Отбив одну атаку мошенника, нужно готовиться к следующей. Перспективные разработки компании БИС связаны с комплексной реализацией мер защиты и переходу к понятию «доверенная среда» для своих продуктов. Речь уже идет не только о том, чтобы противостоять несанкционированному доступу к счетам клиента на программном уровне. Создание «доверенной среды» означает, что поставлен заслон проникновению в банковскую систему.

В настоящее время специалисты компании БИС совместно с одной известной компанией в области защиты информации ведут разработку устройства, которое может стать выходом на принципиально новый уровень защиты информационных систем банка. Речь идет о выходе за программные пределы защиты и переходе к аппаратной реализации российских криптографических алгоритмов.

Работа в системе ДБО будет осуществляться следующим образом: клиент подключает к используемому компьютеру выданное ему в банке устройство, которое автоматически, блокируя операционную систему этого компьютера, формирует внутри себя все параметры предстоящей транзакции. Таким образом создаются условия, полностью исключающие возможность постороннего вторжения. В компьютере, используемом клиентом, может работать вирус, мошенники могут считывать информацию с мобильного телефона клиента – все это им нисколько не поможет, потому что операция ведется автономно, исключительно в пределах девайса, доступ к которому не имеет никто, кроме самого клиента.

Как только эта работа будет завершена, а это произойдет уже в конце текущего года, появятся основания говорить о том, что системы ДБО от компании БИС еще более надежно защищены от внешнего проникновения. Можно будет сказать, что и банковская, и клиентская часть системы ДБО существуют в доверенной среде, следовательно, шансов у мошенников станет еще меньше.