Механизмы безопасности в Системе «iBank 2»

1. Угроза хищений в системах ДБО

С 2008 года российские банки сталкиваются с ростом попыток хищений денежных средств со счетов клиентов с использованием систем дистанционного банковского обслуживания (ДБО) и в частности с использованием системы Клиент-Банк. При этом платежные документы, направляемые в банк от имени клиентов, имели подлинную электронную подпись (ЭП). Чтобы направить в банк документ от имени клиента злоумышленнику нужно получить доступ к ключу электронной подписи. Подобрать ключ ЭП невозможно – при длине ключа 256 бит количество возможных вариантов составляет 10^{78}.

Ключ электронной подписи можно только украсть. Исторически во всех российских системах ДБО использовались ключи ЭП, хранимые в файлах – на дисках, USB-флешках и обычных смарт-картах. Для хищения злоумышленники заражали компьютеры специализированными вредоносными программами. Копия файла с ключом отправлялась злоумышленнику. Аналогично похищались вводимые пользователем пароли доступа.

Для противодействия хищениям ключей электронной подписи Система, предоставляемая Банком, поддерживает специальные устройства – USB-токены с неизвлекаемым хранением ключей электронной подписи.

1.1. Новые угрозы

Весной 2010 г. в нескольких российских банках были зафиксированы первые попытки хищений средств у клиентов, использовавших устройства с неизвлекаемыми ключами электронной подписи (USB-токены). Во всех выявленных случаях злоумышленники пользовались халатностью клиентов, оставляющих USB-токены постоянно и бесконтрольно подключеннымы к компьютеру с доступом в Интернет.

С помощью вредоносных программ со встроенным механизмом удаленного управления (RAdmin, TeamViewer, VNC и др.) злоумышленники подключались к консоли инфицированного компьютера клиента. Далее с использованием ранее перехваченного пароля доступа и постоянно подключенного USB-токена злоумышленники, от имени клиента, заходили в систему ДБО, создавали платежные поручения, подписывали их и отправляли в банк. Одновременно были зафиксированы попытки хищений с использованием вредоносных программ, обеспечивающих дистанционный доступ к USB-портам компьютера клиента. При этом вход в системы ДБО осуществлялся с компьютера злоумышленника, а работа с USB токеном, подключенным к компьютеру клиента происходила дистанционно.

Для преодоления механизма контроля доступа клиента с заданных IP-адресов (данный вид защиты подробно описан в пункте 4) вредоносная программа осуществляла туннелирование TCP-трафика с компьютера злоумышленника до компьютера клиента внутри XMPP-трафика (Jabber и т. п.), производила трансляцию IP-адресов (NAT) и направляла TCP-трафик злоумышленника от клиента в банк.

Важно!

- Новые угрозы не являются специфичными для системы предоставляемой Банком. Удаленный доступ к USB-портам или удаленное управление компьютером

позволяет злоумышленникам получить доступ к распоряжению денежными средствами при работе с любыми системами ДБО.

- Ни в одном из инцидентов ключ электронной подписи не был похищен из USB-токена. Применение USB-токенов сильно ограничивает возможности злоумышленников по хищению средств.

Для защиты от данных типов угроз Банк предоставляет клиентам услугу многофакторной аутентификации. Для подключения данной услуги Клиенту необходимо подключить данную услугу.

1.2. Сокрытие мошеннических платежей

В июле 2011 г. в российских банках были зарегистрированы попытки хищения средств с использованием новой разновидности вредоносной программы. Компонента вредоносной программы устанавливалась на компьютер клиента, используя критические уязвимости в старых версиях Java-машин (JVM). Вредоносная программа не только предоставляла возможность дистанционного управления компьютером, но и подменяла вызовы JVM для сокрытия мошеннических действий. Платежные поручения создавались, подписывались и отправлялись в банки непосредственно на инфицированном компьютере клиента. При этом все мошеннические действия и их результаты оставались скрытыми от клиента:

- При работе на инфицированном компьютере мошеннический платеж не отображался в списке платежных поручений. При работе с обычного компьютера мошеннический платеж отображался.
- При работе на инфицированном компьютере операция списания средств не отображалась в выписке. При работе с обычного компьютера проводка отображалась.
- При работе на инфицированном компьютере остаток на счете модифицировался – не уменьшался на сумму мошеннического платежа. При работе с обычного компьютера отображался реальный остаток.

В результате таких действий попытки хищения могли длительное время оставаться скрытыми.

Для защиты от данных типов угроз Банк предоставляет клиентам услуги многофакторной аутентификации, а так же информирования клиента.

2. Защита ключей электронной подписи

Клиентам, эксплуатирующим системы ДБО с использованием механизма усиленной электронной подписи, следует четко понимать – эпоха хранения ключей электронной подписи в копируемых файлах закончилась. Сегодня необходимо использовать устройства с неизвлекаемыми ключами электронной подписи.

Такие устройства генерируют ключи электронной подписи внутри себя и хранят их в защищенной долговременной памяти. Ключи электронной подписи никогда не покидают устройства и не могут быть извлечены из данного устройства никем, включая разработчика и производителя. Принцип работы устройства: на вход подается электронный документ, а на выходе считывается электронная подпись под этим документом. Усиленная электронная подпись формируется по российскому ГОСТу с использованием встроенного средства криптографической защиты информации (СКЗИ), сертифицированного ФСБ РФ.

Исключение возможности хищения ключей электронной подписи существенно ограничивает возможности злоумышленника. Попытка хищения возможна только в онлайне, когда устройство с ключами электронной подписи подключено к работающему компьютеру. При использовании устройств с неизвлекаемым хранением ключей электронной подписи отсекается значительная часть угроз, существенно снижаются риски хищений денежных средств. Система, предоставляемая Банком, поддерживает USB токены с неизвлекаемым хранением ключей электронной подписи. Использование USB токенов является обязательным условием для подключения клиента к пользованию электронным средством платежа.

3. Многофакторная аутентификация

Для противодействия новым угрозам банк предоставляет клиентам механизмы расширенной многофакторной аутентификации и дополнительного подтверждения платежных поручений одноразовыми паролями.

3.1. Дополнительное подтверждение документов

Возможность дополнительного подтверждения платежных поручений одноразовыми паролями встроено в систему, предоставляемую Банком. Данный механизм не заменяет усиленную электронную подпись под документами, а дополняет ее.

После подписания платежного поручения необходимым количеством усиленных электронных подписей и при превышении пороговой суммы документ переходит в статус «Требует подтверждения».

Для подтверждения такого документа необходимо ввести одноразовый пароль, полученный в SMS- сообщении.

Использование одноразовых паролей значительно снижает риск хищения денежных средств. Для хищения денежных средств злоумышленнику необходимо получить физический доступ к SIM-карте клиента к которой подключена услуга многофакторной аутентификации или подтверждения документов одноразовым паролем либо перехватить SMS-сообщение с применением специальных средств, либо «заразить» телефон жертвы вредоносной программой для получения доступа к SMS- сообщениям жертвы.

3.2. Источники одноразовых паролей

В качестве источников одноразовых паролей в Системе, предоставляемой Банком, используются SMS-сообщения.

К клиенту может быть привязано произвольное количество номеров телефонов для отправки SMS.

Один и тот же номер телефона может быть привязан к нескольким корпоративным клиентам.

Для входа в систему или подтверждения документа сотрудник корпоративного клиента может использовать любой телефон привязанный к его организации.

SMS-сообщение с одноразовым паролем для подтверждения документа содержит критичные реквизиты подтверждаемого платежа: сумму, наименование, счет и БИК банка получателя. Это обеспечивает защиту от подмены отображаемых клиенту реквизитов документа вредоносной программой.

К недостаткам SMS относится возможность задержки доставки сообщения по вине сотового оператора. Это может помешать клиенту оперативно войти в систему и совершить важные платежи.

4. Дополнительные механизмы безопасности

4.1. IP-фильтрация

В системе существует возможность работать только с заданных IP-адресов и IP-подсетей.

Использование механизма IP-фильтрации не защищает от угрозы несанкционированного доступа в систему посредством удаленного управления компьютером. Тем не менее, IP-фильтрация повышает уровень информационной безопасности усложняя защиту системы, что создает дополнительные сложности для злоумышленников.

Список разрешенных IP-адресов и IP-подсетей устанавливается Клиентом при заполнения соответствующего приложения к договору об использовании средства платежа и приему к исполнению соответствующего заявления в банке.

4.2. Email-информирование

Банк предоставляет услугу «SMS-Информирование» для оперативного информирования клиентов по SMS или e-mail о следующих событиях:

- Поступление в банк платежных поручений.
- Движениях средств по счету.
- О входе в систему.
- Списание средств с расчетных счетов.
- Изменениях в настройках рассылки сообщений.

Получение e-mail об указанных событиях позволит своевременно узнать о несанкционированном доступе и оперативно предпринять необходимые меры.

Настройка услуги осуществляется клиентом самостоятельно после подключения данной услуги в Банке