Актуальные угрозы при работе с СЭД

Системы «Банк-Клиент» и «Интернет-Клиент» в терминах Федерального закона №161-ФЗ «О национальной платежной системе» являются электронным средством платежа. Выполняя требования статьи 9 указанного закона, Банк «Снежинский» АО информирует вас о случаях повышенного риска при использовании электронного средства платежа. До заключения Договора присоединения просим вас внимательно ознакомиться с возможными угрозами при работе с СЭД (системами «Банк-Клиент» и «Интернет-Клиент)

1. Угрозы, вызванные действиями злоумышленников

Злоумышленники могут получить доступ к компьютеру клиент, на котором установлена система электронного документооборота (далее – СЭД) «Банк-Клиент» и «Интернет-Клиент», или получить доступ к носителю с ключом электронной подписи и тем самым получить доступ к управлению счетом клиента.

Злоумышленники могут способствовать заражению компьютера с установленной СЭД вредоносным программным обеспечением (вирусами).

Наиболее часто заражение происходит при посещении скомпрометированного вэб-сайта, на котором злоумышленниками были внедрены различного рода программы, эксплуатирующие незакрытые уязвимости в браузерах или их модулях. В ходе эксплуатации на рабочий компьютер клиента может загружаться вредоносное программное обеспечение, которое автоматически определяет, с какими приложениями работает пользователь. При обнаружении фактов (следов) работ с СЭД, на компьютер дозагружаются вредоносные модули, предназначенные для кражи авторизационных данных (ключа электронной подписи, логина/пароля). Вредоносные модули способны передать данную информацию злоумышленникам. Современные вредоносные программы имеют широкий функционал и способны работать одновременно с несколькими системами дистанционного банковского обслуживания.

Если хранение ключей электронной подписи осуществляется клиентом на жестком диске компьютера или незащищенном внешнем носителе, то процедура несанкционированного доступа к ним существенно упрощается.

Зараженный вредоносным программным обеспечением компьютер подвержен следующим угрозам:

1.1. Хищение ключей электронной подписи клиента и паролей доступа к ключам электронной подписи клиента.

Злоумышленник, похитивший ключи электронной подписи и пароли доступа к ним, может удаленно (со своего компьютера) создавать от имени клиента платежные документы, подписывать их скопированным ключом электронной подписи, отправлять такие документы в Банк. Документы будут восприниматься Банком как документы, подписанные корректной электронной подписью клиента.

1.2. Удаленное несанкционированное управление ключами электронной подписи с компьютера клиента.

Вход в СЭД осуществляется с компьютера злоумышленника, работа с носителем электронной подписи (например, USB-токеном, подключенным к компьютеру клиента и оставленным в подключенном к компьютеру состоянии), происходит дистанционно.

Злоумышленник может создать от имени клиента платежные документы, подписать их корректной электронной подписью клиента на компьютере клиента. При этом у злоумышленника остаются следующие возможности управления компьютером клиента:

- изменение информации, отражающейся в СЭД (не отражаются проведенные злоумышленником платежи и неверно отражается остаток по счету);
- возможность частичного или полного вывода из строя компьютера клиента (компьютер может вообще не включаться или «зависать» при загрузке или при подключении к СЭД).

Злоумышленник также может создать платежное поручение и сохранить в СЭД в надежде, что клиент не заметит чужое платежное поручение в большом объеме отправляемых платежей, подпишет и отправит его сам.

1.3. Блокирование доступа клиента к сайту Банка (сайту входа в СЭД)

Как только мошенническая операция проведена, и платежное поручение отправлено, злоумышленники могут ограничить доступ легитимного пользователя СЭД.

Злоумышленник блокирует возможность доступа клиента к системе одним из нескольких способов:

- вывод из строя компьютера клиента;
- блокировка локальной вычислительной сети организации клиента, либо блокировка выхода в Интернет организации;
- блокировка доступа к сайту Банка.

1.4. Подмена платежного документа при передаче его на подпись

Злоумышленники могут внедрить в компьютер клиента троянскую программу, изменяющую в подготовленных к отправке платежных поручениях информацию (например, реквизиты получателя платежа, его расчетного счета, наименования банка получателя, сумму платежа). Пользователь видит на экране монитора одну информацию, а на подписание отправляется другая. Параллельно подменяются данные об остатках на счете, выполненных транзакциях и т.д.

2. Угрозы, вызванные действиями/бездействием сотрудников клиента

2.1. Неосторожные действия сотрудников клиента:

- использование чужих компьютеров или иных устройств для распоряжения счетом;
- использование компьютера, на котором установлена СЭД, для посещения интернет-сайтов, отличных от сайта Банка;
- сохранение ключевой информации на жестком диске или в реестре операционной системы;
- хранение носителей с ключом электронной подписи в общедоступном месте;
- неизвлечение носителя с ключом электронной подписи из компьютера после окончания работы с СЭД;
- передача носителя с электронной подписью другому лицу (в том числе IT-специалистам, сотрудникам обслуживающих организаций, в том числе занимающихся сопровождением программного обеспечения).

2.2. Умышленные злонамеренные действия сотрудников клиента

Копирование ключа электронной подписи при получении работающим или уволившимся сотрудником временного неконтролируемого доступа к нему с целью передачи мошенникам.

3. Угрозы, вызванные сбоями в каналах связи

Отсутствие возможности для клиента связаться с Банком и Банку связаться с клиентом из-за сбоев в работе каналов связи.

4. Угрозы, вызванные сбоями в информационных системах Банка

Временная недоступность одного или нескольких сервисов, предоставляемых Банком.

Чтобы не стать жертвой мошенников. Неукоснительно соблюдайте «Требования информационной безопасности при работе в СЭД»! Это существенно снизит угрозу мошенничества с денежными средствами на счете вашей организации при работе в СЭД.

При любых подозрениях на компрометацию ключей электронной подписи, подозрении на использование СЭД без вашего согласия незамедлительно обращайтесь в Единую справочную службу Банка:

тел. 8-800-755-05-05 (круглосуточно, звонок бесплатный).