

ЗАЩИТА ДБО: ТРАДИЦИОННЫЕ ПОДХОДЫ



АЛЕКСЕЙ ВОРОНЦОВ,
архитектор инфраструктуры информационной
безопасности компании «Инфосистемы Джет»



Защита клиентов дистанционного банковского обслуживания (ДБО) всегда была проблемой нетривиальной и потому интересной для профильных специалистов. И дело здесь не в защите систем ДБО банка, которая, по сути, ничем не отличается от обеспечения безопасности любого дистанционного доступа из недоверенной среды, имеет на вооружении целый ряд «лучших практик» и иногда даже попадает под действие регламентирующих стандартов, таких как СТО БР и PCI DSS. Нетривиальным остается одно — защита самих клиентских мест ДБО.

Компьютеры клиентов — это внешняя по отношению к системам банка территория, она не контролируется ИТ- и ИБ-службами банка. Организационные меры здесь в большинстве случаев не действуют — клиент всегда прав. Можно рекомендовать клиенту поставить на рабочее место, к примеру, антивирусное программное обеспечение, но реально работающих рычагов воздействия, гарантирующих выполнение этих рекомендаций, нет. Клиентские места при этом — самая массовая часть системы ДБО. И несмотря на то, что основной ущерб в случае нарушения ИБ на клиентском месте несёт именно пользователь системы, банкам тоже достаётся их «порция» — пока это только репутационные риски, миграция клиентской базы, участие в длительных расследованиях и разбирательствах. Однако ситуация может измениться в ближайшем будущем — с конца 2012 года, когда вступит в действие пресловутая статья 9 закона № ФЗ-161 «О Национальной платёжной системе» (она гласит, что если клиент уведомляет банк о неправомерном использовании

средств электронного платежа, банк обязан возместить ему сумму операции, совершённой без его согласия).

При этом число атак на клиентские места в последнее время всё возрастает. В этой сфере традиционно лидируют составители вредоносного ПО как способные на самую массовую атаку. По заявлению представителей МВД, в России за 2011 год один из наиболее частых видов киберпреступлений — это атаки именно на пользователей систем «Клиент-Банк». И при получении злоумышленниками того или иного вида доступа к счетам юридического лица ущерб в среднем составлял 3–5 млн рублей на организацию.

Наиболее распространённые способы атак на системы ДБО:

- вредоносное ПО (трояны, клиенты бот-сетей и т.д.);
- фишинг;
- использование атак типа Man-in-the-Middle для проведения подложных транзакций;
- внутренние атаки (для корпоративных клиентов);
- направленные атаки на клиентские места (опять же имеют смысл для корпоративных клиентов).

Соответственно, наиболее распространённые векторы атак на системы ДБО — это:

- хищение ключевой и/или аутентификационной информации с последующим ее использованием либо на месте, либо на удалённом компьютере;
- проведение транзакций непосредственно с компьютера клиента;
- подмена легитимных транзакций подложными.

С точки зрения возможностей защиты клиентские места ДБО можно разделить на два вида в

зависимости от специфики их применения. Первый — это защита традиционных решений «Клиент-Банк» (или «Банк-Клиент»), подразумевающих наличие «толстого» клиента и традиционно используемых при работе с юридическими лицами. Этот вариант предусматривает необходимость установки на рабочее место пользователя соответствующего пакета ПО.

Второй — это защита интернет-банкинга. В данном случае в качестве рабочего места пользователя выступает «тонкий» клиент, подразумевающий отсутствие какого-либо специализированного ПО на стороне клиента Банка. Этот вариант используется прежде всего при работе с физическими лицами, но приобретает всё большую популярность благодаря отсутствию необходимости устанавливать дополнительные программные и аппаратные средства, а также своей мобильности.

ЗАЩИТА СИСТЕМ «БАНК-КЛИЕНТ»

Как мы уже говорили, особенностью защиты «толстого» решения является наличие на рабочем месте клиента установленного комплекта ПО, состав которого определяет сам банк. То есть у кредитно-финансовой организации есть возможность выдвинуть ряд требований к программному обеспечению на конечной рабочей станции. Вводить в состав системы «Банк-Клиент» решение по endpoint-защите стало хорошей практикой в банковской среде. Из наиболее часто применяемых методов здесь — пассивный мониторинг активности в программной среде или даже комплексное решение, которое может включать в себя такие модули, как антивирусное ПО, хо-

стовый IPS, базовый персональный межсетевой экран, средства криптографической защиты информации (СКЗИ), возможность многофакторной аутентификации и т.д.

Что следует отметить, как хорошую практику использования традиционных средств защиты банк-клиентов? Список ниже:

Использование СКЗИ. Кроме применения криптосредств для защиты передачи информации по недоверенным каналам связи, хорошей практикой стало использование сертифицированных ФСБ СКЗИ для генерации электронных цифровых подписей (ЭЦП). Основная задача криптосредств в данном случае — обеспечение неотказуемости банковских операций в случае возникновения конфликтов (использование сертифицированных средств позволяет обеспечить юридическое основание при рассмотрении спорных случаев в судебных инстанциях).

Защита ключевой информации. Использование СКЗИ и ЭЦП для совершения банковских операций означает, что ключевая информация является в подобных системах «Клиент-Банк» одним из главных объектов атаки. Обладая этими данными, нарушитель сможет совершать легитимные финансовые транзакции от лица клиента. В связи с этим до-

полнительные меры для защиты ключевой информации всегда являются приоритетными. Среди основных тенденций — уход от применения накопителей и использование различных защищённых способов хранения информации, а также исключение ее хранения в недоверенной среде. Например, желательно использование процессорных смарт-карт и USB-токенов с возможностью совершения криптоопераций непосредственно на аппаратном устройстве.

Двухфакторная аутентификация. Дополнительным уровнем защиты может быть двухфакторная аутентификация сессии работы пользователей с системой «Клиент-Банк». Для этого можно использовать аппаратные и программные генераторы одноразовых паролей, токены и т.д.

Аутентификация на уровне транзакций. Проверка подлинности предполагает не единичную аутентификацию в рамках сессии работы системы «Банк-Клиент», а проверку при каждой из финансовых операций. Эта технология всегда способствует повышению уровня защищённости, но очень редко применяется для корпоративных клиентов. Дело в том, что при проведении большого количества платежей подобный режим вызывает слишком большое число нареканий со стороны самих пользователей системы.

Антивирусное ПО. Так или иначе, вредоносный код — это ос-

новной вектор атаки, в том числе и для корпоративных клиентов. Поэтому рекомендации по использованию комплексов антивирусной защиты на компьютерах с ДБО предлагаются практически всегда. Иногда в практике защиты встречаются случаи, когда антивирусная защита (хотя бы бесплатная) включается непосредственно в комплект поставки ПО «Клиент-Банк».

Использование комплексов Endpoint Security. Дополнительным уровнем защиты от внешнего воздействия систем «Клиент-Банк» является использование автономно управляемых (зачастую — с предустановленными рекомендованными настройками) комплексов Endpoint Security. Кроме антивирусной защиты, они могут включать в себя один или несколько компонентов: персональный межсетевой экран, хостовое средство обнаружения вторжения, средство криптографической защиты.

ЗАЩИТА WEB-БАНКИНГА

В случае web-банкинга всё богатство мер, традиционно используемых для защиты ДБО, оказывается в лучшем случае трудно применимым. Здесь преимущества web-технологий играют злую шутку. Отсутствие жёстких требований к программной платформе и устанавливаемого софта накладывает ограничения на защиту со стороны клиента. При этом риски для этой категории наиболее высоки. Что же традиционные средства защиты предлагают для web-банкинга? Список не



Компьютеры клиентов – это внешняя по отношению к системам банка территория, она не контролируется ИТ- и ИБ-службами банка

такой уж и большой:

Использование протокола SSL.

Этот протокол позволяет обеспечить проверку подлинности сервера и шифрование сессии. Он применяется повсеместно в связи с тем, что реализован во всех современных браузерах, и позволяет избежать большого количества достаточно простых атак, таких как перехват аутентификационных данных или простые решения класса Man-in-the-Middle. В то же время протокол не обеспечивает защиту при компрометации браузера или подмене сертификатов корневых удостоверяющих центров на клиентских местах. Существуют также версии протокола с определенными слабостями и уязвимостями.

Защита от логирования данных доступа, которая подразумевает использование «виртуальных клавиатур», капч и других способов борьбы с перехватом и/или автоматизированным подбором аутентификационной информации. Увы, постоянное развитие вредоносного кода и различных систем логирования активности пользователя делает эти меры недостаточными. Однако их применение при построении систем web-банкинга не требует больших расходов и потому может рекомендоваться для использования.

Многофакторная аутентификация при доступе.

Прежде всего используются решения с низкой стоимостью владения в пересчете на отдельного пользователя. Это блокноты с одноразовыми паролями, SMS-аутентификация или аутентификация с использованием ПО на мобильных устройствах (смартфонах, коммуникаторах, планшетах). Иногда возможно применение цифровых сертификатов на различных носителях, систем гене-

рации одноразовых паролей и даже биометрии. Но эти решения подразумевают высокие накладные расходы, как правило, лежащие на плечи клиентов при подключении к web-банкингу и потому применимы только в ограниченных случаях (к примеру, для VIP и имиджевых клиентов). Кроме того, некоторые из систем многофакторной аутентификации накладывают дополнительные ограничения

**В СЛУЧАЕ
WEB-БАНКИНГА
ВСЁ БОГАТСТВО
МЕР, ТРАДИЦИ-
ОННО ИСПОЛЬ-
ЗУЕМЫХ ДЛЯ
ЗАЩИТЫ ДБО,
ОКАЗЫВАЕТСЯ
В ЛУЧШЕМ
СЛУЧАЕ ТРУДНО
ПРИМЕНИМЫМ**

на используемые платформы, что может сводить на нет преимущества web-банкинга для клиентов.

В текущий момент наиболее популярным вариантом многофакторной аутентификации при доступе является именно SMS-аутентификация. Она предполагает достаточный уровень защиты при минимальных затратах и хорошо масштабируется (можно привести пример компании Google, использующей этот ме-

тод для доступа пользователей к сервису Gmail). Однако, по сообщениям McAfee Labs, новые версии вредоносного ПО уже научились компрометировать SMS-аутентификацию в ДБО путем реализации атаки Man-in-the-Middle прямо на коммуникаторе пользователя. Учитывая, что доля смартфонов и коммуникаторов растёт, а аудитория, активно использующая мобильные технологии, в достаточной степени совпадает с контингентом пользователей веб- и мобильного банкинга, число атак, реализуемых посредством компрометации смартфонов, будет только расти.

Аутентификация отдельных транзакций.

Дополнительной мерой защиты может выступать использование многофакторной аутентификации не для получения доступа к системе web-банкинга, а для авторизации отдельных транзакций во время работы с ней. Способ обеспечивает частичную защиту от вредоносного ПО, работающего в уже открытой сессии пользователя. Для клиентов-физических лиц (в отличие от юридических) эта защита может считаться приемлемой ввиду удобства ее реализации: количество финансовых транзакций в рамках одной сессии в данном случае редко бывает значительным.

Оповещения о проведённых транзакциях.

SMS и E-mail оповещения клиента о каждой транзакции могут также рассматриваться как средства борьбы с различными методами перехвата сессий работы с web-банкингом (хотя бы с точки зрения минимизации возможных потерь). Таким образом клиент всегда узнает о начале неправомерного использования его учётных данных. Кроме того, в соответствии с положениями нового закона №

Хищение ключей ЭЦП

С момента развития защиты электронного документооборота, когда было сформировано понятие ЭЦП и приняты стандарты по его использованию, основным направлением атак злоумышленников стали попытки хищения ключей ЭЦП, расположенных на носителях разных типов. Такие хищения осуществлялись как самими сотрудниками компании, так и злоумышленниками с помощью взлома корпоративных сетей и персональных компьютеров, фишинга, внедрения вредоносных программ или социальной инженерии. Практика показала, что парольная политика защиты секретных компонент ключей не привела к значительному уменьшению атак, а лишь снизила вероятность использования ключа при прямой краже носителя. Хищения паролей ключей ЭЦП осуществляются аналогичными способами. Наиболее оптимальной защитой от подобных хищений стала практика хранения ключей на токенах — устройствах, исключающих копирование секретных данных и осуществляющих процесс подписи документа внутри токена. При этом факт хищения ключа легко распознается FMS-системами: признаками мошеннических действий являются получение платежного поручения с не зарегистрированных ранее компьютеров и IP-адресов, нарушение последовательности платежных документов или нестандартное для организации заполнение полей платежного поручения.



ФЗ-161, отсутствие уведомления клиента о совершённой транзакции рассматривается как безусловное перенесение ущерба от мошеннических операций на сторону банка.

Clientless NAC решения. В случае ДБО нельзя использовать полноценный In-Band NAC, поскольку отказ доступа к функционалу ДБО для пользователя с заражённого компьютера, даже реализованный из лучших побуждений, — это потенциально потерянный клиент. Однако предоставить информацию о наличии, к примеру, подозрительной вирусной активности со стороны клиентского компьютера или отсутствии антивирусного ПО никогда не бывает лишним. Ряд Clientless NAC-решений для контроля конечных рабочих мест работает напрямую из браузера и в случае обнаружения серьёзных уязвимостей позволяет выдавать клиенту предупреждение и список рекомендаций по дальнейшим действиям со ссылками на интернет-ресурсы. Другое применение подобных технологий — внутренний мониторинг клиентской базы с составлением списка подозрительных рабочих мест для последующей корреляции этой информации с данными систем финансового мониторинга и антифрода.

Clientless Endpoint защита. Это наиболее сложная технология, являющаяся развитием Clientless NAC решений. Фактически она представляет собой работающий в браузере (с использованием Java-апплетов, ActiveX и др.) полноценный endpoint-клиент, позволяющий без установки дополнительного ПО обеспечивать базовую защиту клиентских мест на время сессии работы с web-банкингом. Данное направление только развивается, практика использования подобных

решений очень невелика, однако их недостатки уже очевидны — это зависимость от версий ПО браузера и клиентских операционных систем, а также высокая стоимость владения.

Организационные меры, побуждающие клиентов к защите. Предложение клиентам ДБО льготных программ на покупку/аренду, к примеру, антивирусного ПО также может рассматриваться как одна из мер защиты клиентских рабочих мест.

ЗАКЛЮЧЕНИЕ

Количество угроз в сфере ДБО только растёт, и появляются новые типы атак, связанные с web-банкингом, вредоносным ПО для мобильных телефонов и др. Отметим, что некоторые из этих угроз еще не существовали год-два назад, с ростом рынка ДБО и банковских интернет-услуг растёт и привлекательность атак на данные услуги. Соответственно, растут потенциальные и реальные потери клиентов, а со следующего года — и реальные денежные потери банков.

При этом существует достаточно большой выбор средств и методов для защиты ДБО. Если говорить об их внедрении для массового использования, особенно для обслуживания физических лиц через средства web-банкинга, можно констатировать, что немногие решения проходят ценз стоимости и возможности масштабирования. В то же время сложившаяся на текущий момент ситуация с развитием киберпреступности и низкий процент раскрываемости подобных преступлений доказывают, что использование банками подобных технологий для защиты своих клиентов более чем оправдано. ■

ЗАЩИТА ДБО ОТ МОШЕННИЧЕСТВА НА УРОВНЕ БИЗНЕС-ПРОЦЕССОВ



АЛЕКСЕЙ СИЗОВ,
архитектор FMRA решений Центра
информационной безопасности
компании «Инфосистемы Джет»