

Безопасность на расстоянии

Обеспечение безопасных ИТ-сервисов для удаленных клиентов становится одним из показателей конкурентоспособности финансовой организации

Широкая распространенность и доступность систем дистанционного банковского обслуживания в сочетании с, как правило, низкой защищенностью клиентов привлекает внимание криминальных структур, что делает вопросы защиты пользователей таких услуг чрезвычайно актуальными.

Дистанционное банковское обслуживание (ДБО) — общий термин для технологий предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом (без визита в банк), чаще всего с использованием компьютерных и телефонных сетей. ДБО дает пользователям свободу в плане выбора времени, места, устройства, с которого будет производиться удаленное управление счетом, и экономит их время. Выбирая банк, они нередко предпочитают именно тот, который предоставляет клиентам более функциональную и безопасную систему ДБО. Не так просто бывает обеспечить разумный компромисс этих противоречивых по своей сути требований, в то же время удачное сочетание удобства, функциональности и защищенности способно обеспечить банку определенное преимущество над конкурентами, а потому поиск такого сочетания жизненно важен для современного банка, работающего в условиях острой рыночной конкуренции.

Важно также понимать, что информация, циркулирующая внутри систем ДБО, фактически эквивалентна реальным деньгам, следовательно, создать условия, при которых угроза несанкционированного использования этой информации будет полностью исключена, невозможно, и всегда найдется тот, кто захочет завладеть этой информацией, поэтому данную информацию необходимо защищать.

«В начале 2010 года мы провели анализ информационных рисков, связанных с эксплуатацией комплекса ДБО (как на стороне банка, так и на стороне клиента), и на основе полученных данных приняли решение о необходимости реализации проекта комплексной модернизации системы обеспечения информационной безопасности (СОИБ) ДБО. Решить поставленные в рамках данного проекта задачи было бы невозможно без изменения технологических процессов, связанных с обслуживанием клиентов системы ДБО, а также без модификации внутренних бизнес-процессов», — рассказывает Лев Шумский, заместитель начальника управления инфраструктуры департамента ИТ «Русь-Банка».

РИСКИ И УГРОЗЫ

Интернет был и остается небезопасной и фактически неконтролируемой средой для банков. Угроза перехвата реквизитов доступа пользователей, подключенных к системам ДБО через Интернет, — основное слабое место дистанционных сервисов. Сегодня в ходе проведения атаки мошенники задействуют большое количество звеньев, использующих Интернет в качестве канала для коммуникаций. Правила работы в системах ДБО не являются конфиденциальной информацией, и любой желающий может получить к ним доступ. Единственной возможностью защитить клиента от злонамеренных действий является сохранение конфиденциальности его идентификационной информации. Именно за ней и идет охота.

Большинство атак злоумышленников направлено на хищение закрытого ключа электронной цифровой подписи (ЭЦП) и идентификационных данных клиента, поскольку, завладев этой информацией, злоумышленник может в дальнейшем действовать от имени легального пользователя системы ДБО. В случае хранения ключей ЭЦП на жестком диске или USB-накопителе клиент рискует своими деньгами, поэтому внедрение средств защиты ключей ЭЦП стало одним из важных этапов в реализации всего проекта.

Наименее защищенным элементом ДБО, как показывает практика, является рабочее место пользователя — представителя клиента, внешней по отношению к банку организации. Сотрудникам банка неизвестно, установлено ли на этом рабочем месте антивирусное ПО, с какой периодичностью оно обновляется, какие настройки политик безопасности установлены, использует ли клиент лицензионное ПО, можно ли быть уверенным в безопасности его работы и пр. Обычно банки жестко требуют от клиентов исполнения требований по обеспечению защиты информации рабочих мест, на которых осуществляется работа с системами ДБО, а также выполнения мероприятий по проверке текущего состояния операционной системы на наличие критичных обновлений и т. д. Но для выполнения всех необходимых настроек безопасности требуется определенная квалификация сотрудников ИТ-службы клиента. К сожалению, такие специалисты имеются далеко не в каждой организации.

Актуальность задачи снижения клиентских рисков существенно возросла в связи с тем, что многие клиенты, не выполнявшие требований банка по обеспечению защищен-



«Обеспечение безопасности предоставляемых дистанционных сервисов является одной из приоритетных задач для нашего банка», Лев Шумский, заместитель начальника управления инфраструктуры департамента ИТ «Русь-Банка»

ности рабочих станций, применявшихся для работы с системой ДБО, при возникновении инцидентов пытались переложить свои убытки на банк, апеллируя к статье 1095 Гражданского кодекса РФ «Основания возмещения вреда, причиненного вследствие недостатков товара, работы или услуги». Данная статья требует обязательного уведомления клиентов о возможных рисках использования тех или иных технологий. Естественно, данный факт с точки зрения бизнеса рассценивается как вероятная угроза, поэтому банк должен получить от клиента обязательство о выполнении всех требований безопасности при удаленной работе со своим счетом.

СУММА ТЕХНОЛОГИЙ

Чтобы соблюсти требования действующего законодательства, нормативных и руководящих документов регуляторов (ЦБ России, ФСБ, ФСТЭК) в «Русь-Банке» было решено использовать только те программно-аппаратные решения, что сертифицированы ФСБ или ФСТЭК. В качестве криптографического ядра были выбраны программные продукты компании «Крипто-Про» — средство криптографической защиты информации

«Крипто-Про CSP» и удостоверяющий центр «Крипто-Про УЦ» на базе технологии PKI. Эти элементы стали первой технологической составляющей проекта модернизации СОИБ ДБО.

Для защиты ключей ЭЦП необходимо было выбрать защищенный носитель. С этой целью был реализован пилотный проект с использованием нескольких продуктов, представленных на российском рынке. Критериями выбора были уровень безопасности ключей ЭЦП, наличие всех необходимых сертификатов, простота настройки клиентской рабочей станции, возможность централизованного учета и управления носителями. В результате тестирования специалисты банка остановили свой выбор на USB-ключе eToken компании Aladdin. Данное решение стало второй технологической составляющей проекта.

«Одной из ключевых задач при проектировании СОИБ является интеграция всех элементов СОИБ между собой и с развернутой в банке системой ДБО», — отмечает Шумский. Основным требованием к интеграционному решению является использование стандартных технологий для взаимодействия с удостоверяющим центром, системой криптозащиты, USB-токенами и системой ДБО.

В качестве интеграционного решения для внедрения был выбран программный комплекс Avanpost IAM CHR_D Pro производства компании «Технологии развития бизнеса». Для оценки эффективности выбранной системы в «Русь-Банке» был реализован еще один пилотный проект, который подтвердил ее эффективность и помог убедиться в скорости внедрения. Использование встроенной в продукт системы электронного документооборота, в свою очередь, обеспечило эффективную организацию бизнес-процессов, связанных с предоставлением клиентам услуг ДБО.

«Выбор системы Avanpost был обусловлен намерением не только повысить безопасность функционирования системы ДБО, но и выстроить комплексную систему управления доступом к информационным ресурсам банка», — рассказывает Шумский.

СТРЕМИТЕЛЬНОЕ РАЗВЕРТЫВАНИЕ

Опытная эксплуатация модернизированной системы стартовала в «Русь-Банке» в мае 2010 года, и уже к концу августа решение было запущено в промышленную эксплуатацию. Все работы по настройке комплекса систем заняли немного более трех месяцев.

«При реализации подобных проектов особое внимание следует уделять организации коммуникаций в рамках проекта, т. к. оказываются затронутыми многие устоявшиеся бизнес-процессы в банке. Это связано с необходимостью объединения технических, юридических и экономических аспектов реализуемого проекта», — комментирует Шумский. — При этом не стоит забывать и о вопросах обеспечения безопасности».

Переход на современные технологии защиты информации позволил «Русь-Банку» получить дополнительные конкурентные преимущества при продвижении услуг ДБО на рынке. Согласно проведенным оценкам, срок окупаемости проекта не превысит 15 месяцев благодаря снижению прямых и косвенных издержек, связанных с эксплуатацией системы ДБО.

В скором времени «Русь-Банк» планирует расширить возможности физических лиц при работе с системами ДБО. В частности, для VIP-клиентов будут сняты существующие ограничения на сумму платежа и его назначение. **СЮ.РУ**