■ **Владимир ЗАЛОГИН**
директор по специальным проектам ЗАО «С-Терра СиЭсПи»

■ **Мария ЛУРЬЕ**
руководитель отдела маркетинга ЗАО «С-Терра СиЭсПи»

ЗАЩИЩЁННАЯ ВИРТУАЛЬНОСТЬ В БАНКОВСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

АДЕКВАТНЫЙ ОТВЕТ НА НОВЫЕ УГРОЗЫ БЕЗОПАСНОСТИ – ОБНОВЛЕНИЕ НЕ ТОЛЬКО ПОДХОДОВ, ТЕХНОЛОГИЙ И СТАНДАРТОВ, НО И VPN-РЕШЕНИЙ

Технологии и средства виртуализации, как и положено по законам прогресса, совершенствуются по спирали. С каждым новым витком появляются новые задачи, и, как следствие, новые решения. Сегодня особенно остро стоит вопрос безопасности, для решения которого в виртуальной среде требуются немного иные подходы, технологии, стандарты. Переход в виртуальное пространство несет в себе множество преимуществ, в том числе, снижение затрат на создание и эксплуатацию систем, повышение эффективности, производительности, отказоустойчивости системы. Но, в то же время, появляются новые угрозы безопасности.

НОВАЯ ПРОБЛЕМА

В банковских информационных системах (ИС) степень риска возрастает еще больше, так как дистанционным доступом в ИС пользуются множество клиентов банков. И если внутренняя сетевая инфраструктура в финансовых организациях, как правило, хорошо защищена, то защищенность клиентских компьютеров зачастую оказывается недостаточной. Банки предлагают клиентам «хождение строем», то есть рекомендуют применять проверенные временем, унифицированные средства защиты. Но количество клиентов, не желающих выполнять рекомендации по защите, достаточно велико, а контроль со стороны банка затруднен.

До января 2014 года, т.е. до ввода в действие ст. 9 161-ФЗ «О национальной платёжной системы», ответственность за невыполнение рекомендаций банка по информационной безопасности лежала в полной мере на клиентах. Большинство расследованных инцидентов, связанных с хищением средств клиентов ДБО, демонстрировало именно вину клиентов. Но сейчас ситуация изменилась, банки вынуждены нести новые значительные риски по неподтвержденным клиентами транзакциям. Поэтому они озадачены поиском решений, которые позволят повысить уровень безопасности без риска оттока клиентов и без масштабных затрат.

НОВЫЕ ЭФФЕКТИВНЫЕ РЕШЕНИЯ

Основой повышения безопасности взаимодействия клиентов и банков через сеть Интернет является использование инструментов защиты, которые надежны, проверены (временем и регуляторами), и при этом обеспечивают компромисс – клиенты должны «ходить строем» только в определенных местах, без ущемления их свобод и ощутимых затрат с их стороны.

В такой ситуации на помощь могут прийти именно технологии виртуализации. Виртуальный Шлюз и Клиент – новые сертифицированные VPN-продукты от компании «С Терра СиЭсПи» появились в арсенале средств защиты информационных систем в 2014 году. Их применение позволяет создать защищенный туннель через не доверенную сеть (например, Интернет), а также обеспечить взаимную аутентификацию клиента и шлюза.

К преимуществам Виртуального Шлюза можно отнести высокую производительность (до 300 Мбит/сек/ядро на современных процессорах Intel), а также удобство и скорость развертывания, резервного копирования и восстановления. Возможность масштабирования и повышения отказоустойчивости за счет создания кластеров по технологиям RRI и VRRP, поддержка сценариев обеспечения катастрофоустойчивости, применение сертифицированных средств централизованного управления VPN-продуктами – всё это позволяет создать и эффективно обслуживать систему сетевой безопасности банка. Возможность установки виртуального VPN-шлюза на одну аппаратную платформу совместно с про-

дуктами безопасности других производителей (межсетевые экраны, системы обнаружения и предотвращения вторжений, антивирусные средства), обеспечивает надежную эшелонированную защиту.

Рассмотрим несколько вариантов использования виртуальных VPN-продуктов:

1. Для массового применения клиентами банка

Большое разнообразие операционных систем и программных средств, установленных на ПК и ноутбуках пользователей, приводит к неизбежным сложностям, возникающим с установкой и работоспособностью банковского программного обеспечения для работы клиентов с ИС банка.

Разработка и тестирование универсального банковского программного обеспечения для всего многообразия возможных комбинаций – это исключительно сложная задача, требующая огромных ресурсов от разработчиков. Более того, иногда отсутствие такого программного обеспечения вынуждает финансовые организации отказывать в доступе к интернет-сервисам клиентам со «сложными» комбинациями.

Установка на компьютер клиента виртуальной машины с необходимым набором банковского программного обеспечения и средствами защиты информации может помочь в достижении компромисса между разнообразием и типизацией при сохранении необходимого уровня защиты. Ведь одну и ту же виртуальную машину можно установить на компьютеры с различными ОС Windows, MacOS и Linux.

Что получат от такого варианта клиенты? Несомненно, более качественный программный продукт, прошедший всестороннее тестирование в том окружении, для которого он создавался, более эффективный и быстрый сервис технической поддержки, т.к. количество возможных причин для некорректной работы уменьшится.

Что получит банк? Прежде всего, снижение затрат, расширение клиентской базы, снижение рисков. А также возможность сконцентрировать усилия на совершенствовании банковских интернет-продуктов.

Как это работает? Виртуальная машина (ВМ) с установленным необходимым программным обеспечением и VPN-клиентом передается клиенту банка. При запуске такой ВМ на компьютере пользователя устанавливается зашифрованное соединение между VPN-клиентом и VPN-шлюзом, защищающим доступ к ИС банка. Все очень просто. Такую ВМ можно выдавать клиентам банка на специализированном защищенном USB-носителе, который содержит средства усиленной аутентификации. Для доступа к виртуальной машине пользователю потребуется ввести PIN-код.

Предусмотрено определенное количество попыток ввода PIN-кода. Если попыток совершено больше, это приводит к блокировке защищенного носителя. Служба безопасности банка может оперативно блокировать доступ к ИС в случае утраты клиентом контроля над компьютером или защищенным носителем, аналогично тому, как происходит блокировка утраченных платежных карт.

2. Для защищенного удаленного доступа сотрудников банка и сотрудников сторонних организаций, выполняющих работы для банка

Сотрудники банка и специалисты-разработчики от сторонних организаций зачастую имеют достаточно высокий уровень привилегий при доступе к ИС банка и внутренним IT-сервисам, таким как внутренний корпоративный портал, почтовая система, CRM и др.

Желательно сформировать групповые политики доступа к защищаемым подсетям на основе полей в сертификате пользователя, а также использовать вариант с хранением виртуальной машины сотрудника на защищенном носителе с усиленной аутентификацией.

НОВЫЕ ПЕРСПЕКТИВЫ И ТЕНДЕНЦИИ

Справедливости ради, отметим, что на стороне банка применение виртуальных продуктов также может раскрыть новые возможности. Прежде всего, это связано с тем, что надежность каналов связи неуклонно растет и уровень их доступности, в скором времени, может сравняться и даже превысить уровень надежности снабжения электроэнергией.

В таких условиях банк может арендовать IT-инфраструктуру, ИС и средства безопасности как сервис, значительно сократив затраты. В свою очередь, предоставление IT-ресурсов в качестве сервиса уже практически невозможно представить без использования средств виртуализации. На рынке уже доступны предложения использования ИС или их компонентов по сервисной модели.

Одновременное бурное развитие централизованных облачных информационных систем государственных, региональных и муниципальных органов говорит о том, что уровень доверия к модели «IT-как-сервис» уже достаточно высок и вновь создаваемые банки вполне могут рассматривать для себя подобную модель развития.

В заключение хочется отметить, что технологии виртуализации активно развиваются и проникают в сознание обычных пользователей. Терминальный доступ, виртуализированные рабочие места (VDI) и «экспорт приложений» все больше используются в корпоративном секторе.

Несмотря на многообразие угроз, жесткие требования нормативных документов и стандартов безопасности, – на российском рынке есть варианты надежной и легитимной защиты.

* * *

В постоянном совершенствовании технологий, развитии средств защиты наступает новый этап, и компания «С-Терра СиЭсПи» стремится быть на переднем крае, предлагая партнерам современные, надежные, сертифицированные продукты и решения.