# Связь-Банк: как сократить «небрежный» трафик

Андрей Арсентьев
Опубликовано 10 марта 2010 года



Банки традиционно стоят на передовой внедрения современных технологий. Особенно это касается сферы ИБ – от эффективности её работы зависит успех бизнеса банка. На вопросы редакции CIO-World.ru ответил **Дмитрий Карпенко**, начальник отдела защиты информации департамента безопасности ОАО АКБ «Связь-Банк».

**- Дмитрий Эдуардович, как изменилась политика банка в области ИТ в связи с реструктуризацией?**

Кризис, безусловно, внес свои коррективы в работу. В частности, в области ИТ был проведен частичный переход на freeware-решения.

**- Как Вы относитесь к использованию в банках продуктов на основе Open Source? Был ли в Связь-Банке подобный опыт?**

В настоящее время на основе Open Source в банке развернута система антиспама, также апробировано решение по мониторингу активного оборудования и серверов. Кроме того, мы рассматривали аналоги Word, Excel и прочих стандартных программ, необходимых для работы большинства сотрудников.

Однако эта практика не получила своего развития, так как зачастую Open Source-решения просто не дотягивают до удовлетворения потребностей банка в данных продуктах. Лично я остаюсь противником массовой замены проприетарных продуктов на решения с открытым кодом. Open Source лучше использовать для реализации пилотных проектов, понимания нюансов технологий, подбора различных вариантов решения той или иной проблемы.

Но использовать такие продукты в качестве основного решения в столь высокорисковой отрасли, как банковский сектор, неправильно. Хотя бы потому, что не совсем понятно, кто будет отвечать за последствия сбоя «открытого решения». И, например, кто будет его сопровождать, и если Open Source требует работы с базами, то как и когда они обновляются и т.д.

**- Расскажите об истории развития автоматизации в вашем банке. Что на сегодня удалось сделать в этой части?**

Если вспомнить, каким был Связь-Банк 10-15 лет назад, и сравнить с сегодняшней картиной, сразу видно, что и головной банк, и филиалы перешли на централизованное управление. Первым шагом стало внедрение централизованной системы операционного дня в банке на базе серверов, расположенных в головном офисе. Сегодня филиалы по всей России работают в единой системе, и на сегодня перед ИТ стоит задача перевода системы «Клиент-Банк» на аналогичную централизованную платформу.

Централизована работа всех мини-офисов банка, расположенных в отделениях почтовой связи, работающих с «тонким клиентом», технологии которого представляют собой комплекс программных иаппаратных устройств, позволяющих максимально облегчить нагрузку накаждый персональный компьютер на отдельно взятом рабочем месте. Таким образом, «тонкий клиент» фактически переносит всю нагрузку на основной рабочий сервер.

По большому счету, основным толчком для нашего развития послужила, как ни странно, извечная проблема ротации квалифицированных специалистов. При наличии в региональном отделении специалиста высокого уровня его уход из компании вызывает больше проблем, чем увольнение сотрудника в Москве. Ведь найти замену в регионе значительно сложнее.

Именно поэтому было принято решение переходить на систему централизованного управления: сначала была создана централизованная корпоративная сеть, потом мы перешли на работу операционного дня в банке, постепенно начал работать front office по обслуживанию клиентов через централизованную систему. В итоге, филиал за филиалом, за два года все подразделения Связь-Банка перешли на централизованное управление через терминальные серверы и «тонкие клиенты».

**- Какие перспективные направления развития ИТ-функционала Связь-Банка Вы можете назвать?**

Что касается информационной безопасности, здесь основным направлением является защита персональных данных, тем более что федеральное законодательство заняло вполне жёсткую позицию (Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных»).

С точки зрения ИТ цель недалекого будущего – централизация всех процессов в компании. Кризис в этом плане обнажил неявные проблемы: при уходе сотрудников часто остаются неприкрытыми жизненно важные для банка процессы. Показателен наш антивирусный проект, когда было принято принципиальное решение, что на всех компьютерах филиалов устанавливается единое, централизованное решение, и все работы ИТ- и ИБ-специалистов на местах контролируются головным офисом.

В результате система работает всегда, несмотря на внешние обстоятельства: любому новому сотруднику в регионе необходимо лишь проконсультироваться в головном офисе. Если же аналогичная ситуация возникает в центральном офисе, работа продолжается, между всеми филиалами полностью налажен процесс обмена информацией, системы, конфигурации централизованы с точки зрения настроек, а посредством межфилиальных связей всегда можно получить нужную информацию.

Такая взаимовыручка центра и филиалов особенно важна для финансовых организаций, поскольку сбой в работе системы, задействованной в бизнес-процессах, ведет к серьезным рискам для бизнеса.

Ещё одно преимущество централизации состоит в том, что с внедрением единой системы управления процессами минимизируются финансовые затраты на запуск новых отделений и филиалов, так как техническое решение просто «масштабируется».

**- Насколько бизнес банка зависит от эффективной системы информационной безопасности?**

Точно так же, как зависит от ИТ. Как только в обменном пункте появились компьютеры, время обслуживания одного клиента сократилось в 1,5 раза, не говоря об экономии времени при формировании отчетов.

Что касается информационной безопасности… Как вы думаете, можно жить без информационной безопасности? Можно. Вопрос, как и сколько и какие будут последствия. Можно вести бизнес с платежными картами без соблюдения требований информационной безопасности? Можно. Вопрос, как часто будут вскрывать банкоматы и взламывать системы. Исходя из того, насколько широкое развитие получили платежные карты, думаю, цена пренебрежения информационной безопасностью в данном случае будет для банка подобна смерти.

Другой пример – введение в действие Федерального закона «О персональных данных» №152-ФЗ. Если его нарушить, возникает вопрос, останется ли лицензия у такого банка, если жалоб клиентов будет много или в открытом доступе появятся данные из «ушедших баз». Последствия могут быть очень плачевными.

Часто в российских компаниях ощущается полное непонимание сотрудниками того, как электронное общение со знакомыми о делах организации может нести, как минимум, информационные риски для организации. Даже если проблемы, о которых сотрудник посетовал другу, действительно на данный момент имеются, большинство ситуаций выправляемо.

Но репутация банка в результате доверительной беседы может пошатнуться. Если в рамках отдела и департамента контролировать эти процессы организационными мерами можно, то в масштабах компании, да еще и с разветвлённой филиальной сетью, проблематично. Здесь контроль за подобного рода нежелательными высказываниями, не говоря уже о конфиденциальной информации, должен быть автоматизированным.

**- Когда Связь-Банк задумался о совершенствовании своей системы информационной безопасности?**

Связь-Банк существует с 1991 г., и когда-то всё, что касалось информационной безопасности, относилось к ИТ-подразделению и, по сути, ложилось нагрузкой на плечи системных администраторов. В конце 90-х годов в подразделении по безопасности появился отдельный сотрудник, который должен был заниматься безопасностью в сфере информационных технологий банка в тесном взаимодействии с ИТ-отделом.

Защита информации в банке была всегда и постоянно совершенствовалась. Это непрерывный процесс, поскольку, как известно, совершенству нет предела. Классическая задача всех «безопасников» – знать, что происходит с информацией в организации, кто, что и куда передает.

В вечном споре, имеет ли право сотрудник организации, подписавшийся под тем, что он будет использовать корпоративные ресурсы только в корпоративных целях, но при этом воспользовался ими для своей личной переписки, я склонен встать на сторону тех, кто считает, что к этому сотруднику можно применить меры административного воздействия, вплоть до увольнения, но если человек подаст на компанию в суд, то, наиболее вероятно, он его выиграет. Потому что будет нарушено конституционное право гражданина. И вариант один – максимально автоматизировать этот процесс. Когда стоит автоматизированная система, в ней прописаны определенные правила, не требуется просмотра частной переписки сотрудников посторонними лицами, и, соответственно, конституционные права человека не нарушаются.

**- Недавно ваш банк осуществил пилотное внедрение решения Traffic Monitor Enterprise от InfoWatch. Почему выбор пал на этот продукт ? Какие еще решения вы рассматривали?**

Причина очень простая: изначально, когда искали продукт для проведения серьёзного пилотного проекта, исходили из текущих условий ведения бизнеса в банке. Всилу специфики хранения документов выделить те из них, на которые можно было бы поставить какие-либо метки, было нельзя. Также было нельзя гарантировать, что даже если такие документы выбраны, то те сотрудники Банка, кто работает с ними, будут своевременно вносить метки или сохранять документы в нужных каталогах.

Поэтому для проведения пилотных проектов по системам, работающим с электронными метками, нужно было проводить колоссальную предварительную работу. За это время обработанные документы вполне могли потерять актуальность. В связи с этим мы искали продукт, запустив который, можно было бы начать получение информацию с момента инсталляции. И пусть это будет огромный объем информации, главное - будет то , с чем можно работать.

К моменту старта пилотного проекта альтернативы продукту InfoWatch не было (к счастью, или к сожалению – не знаю). Сейчас на российском рынке появились конкурирующие с InfoWatch Traffic Monitor решения, например, продукты Symantec, McAfee, Websense, однако они по-прежнему не в полной мере отвечают тем требованиям к защите данных от утечки, которые предъявляются нашей компанией к системам такого рода. В некоторых случаях не устраивает ценовая политика, в некоторых – ряд технических особенностей.

С моей точки зрения, программные продукты InfoWatch интересны не только тем, что они могут заблокировать передачу той или иной информации, но и тем, что можно эффективно собрать данные об инцидентах информационной безопасности и проанализировать их.

При старте проекта ставилась задача продемонстрировать эффективность использования в банке системы «противодействия утечке» и возможные вопросы, которые можно решать при наличии в банке подобной системы. Был установлен

контроль за почтовым каналом (SMTP), веб-трафиком и подключением внешних устройств по различным портам. Основной упор делался на контроль электронной переписки, решение ставилось не «в разрыв», а в режиме теневой копии для дальнейшего анализа того, какая информация покидает пределы организации. Это позволяло не влиять на работу корпоративной сети и сопровождение ИТ, а просто анализировать события в канале, поскольку своевременная реакция на инцидент приводит практически к тем же результатам, что и блокировка. Система не оказала воздействия ни на быстродействие технических средств, ни на качество работы серверов.

**- Чьими силами проводилось внедрение? Расскажите, пожалуйста, о сроках внедрения и полученных результатах.**

Со стороны Связь-Банка внедрение проводилось силами управления информационной безопасности, со стороны поставщика – техническими специалистами «Антивирусного Центра» (техническая настройка и сопровождение работы решения, работа с InfoWatch по доработке решения и проч.). Доработка велась примерно в течение трёх месяцев, и нас приятно удивила готовность специалистов InfoWatch устранять любые неполадки и совершенствовать решение даже под пилотный, некоммерческий проект. Надо попробовать поискать какую-нибудь другую компанию, в особенности западную, в которой при возникновении проблемы сотрудники готовы исправлять еще не проданный продукт. Это основная причина, по которой, во-первых, предпочтение имеют российские продукты, а во-вторых, - именно продукт InfoWatch. Мы убедились: если есть проблема, то она будет этой компанией решаться.

Что касается результатов, то при том, что «пилот» был реализован за полгода, из них в активной боевой стадии – три месяца, за это время был выявлен ряд инцидентов, по одному из которых даже были приняты меры организационного и административного характера. Самое интересное заключается в том, что с момента завершения пилотного проекта прошло более года, но многие наши сотрудники, даже те, кто пришел в компанию после завершения проекта, до сих пор обращаются за разрешением на отправку через корпоративную почту тех или иных документов, которые потенциально могут содержать конфиденциальные данные. Полугодовое использование системы возымело не только колоссальное техническое, но и психологически-организационное действие на сотрудников. Многие эксперты в области безопасности считают, что такой эффект может наблюдаться лишь в течение месяца после завершения проекта, но наша практика показывает – больше года. Думаю, что в итоге количество «небрежного» трафика в компании сократилось процентов на 50.

Сейчас рассматривается возможность выделения средств на коммерческое внедрение программного решения InfoWatch, участвовавшего в пилотном проекте.

**- Охарактеризуйте, пожалуйста, систему ИБ вашего банка. Какие актуальные задачи предстоит решить при ее дальнейшем совершенствовании?**

Мне кажется, что совершенных информационных технологий и идеальной информационной безопасности не бывает в принципе. Вопрос в том, есть ли понимание общих целей и задач у бизнеса, ИТ и ИБ. Поэтому подразделению информационной безопасности в ближайшее время придется решать те задачи, которые будут оказывать содействие развитию бизнеса и совершенствованию

информационных технологий банка. Например, если у бизнеса стоит задача взаимодействия с госучреждениями, это повлечет за собой необходимость использования сертифицированных ИБ-решений, шифрования, с учетом требований ФСБ и т.д. Другое дело, если банк работает только с коммерческими организациями - здесь мы выходим на иной уровень защиты информации.

Кроме того, дальнейшее развитие системы ИБ в нашем Банке, как и в любом другом российском, будет определяться изменением законодательной базы, которая регламентирует сферу информационной безопасности в банковском секторе. Это и Федеральный закон «О персональных данных», и Стандарт Банка России по ИБ, и другие нормативные акты.

Кроме того, в Банке есть подразделение, которое проверяет и контролирует развитие ИТ- и ИБ-инфраструктуры. Этим подразделением проведен мониторинг состояния дел с выполнением сотрудниками требований тех или иных внутренних нормативных документов, регламентирующих деятельность персонала Банка. Уже сейчас можно проводить мероприятия по приведению, в частности, нормативной базы в соответствие с полученными рекомендациями. Думаю, этот процесс приведет к тому, что все отделы будут нацелены на достижение общего результата.