

Опасность внутреннего нарушителя

О. СМОЛИЙ: «Для крупного банка с хорошо организованной защитой информации хакерские атаки равносильны укусу комара. Ущерб от них и от других видов внешних угроз несопоставим с ущербом, который банк может понести от внутренних нарушителей»



Беседовала: Вероника Сошина

С развитием технических средств обеспечить информационную безопасность становится все сложнее, а возможный ущерб от внутренних утечек становится все больше. О том, как в одном из крупнейших российских банков обеспечивается защита от внешних и внутренних угроз, НБЖ рассказал руководитель группы защиты телекоммуникационных систем отдела защиты информации управления защиты информации и объектов банка Олег СМОЛИЙ.

НЕ КОНФИДЕНЦИАЛЬНОСТЬЮ ЕДИНОЙ ...

НБЖ: *Последнее время теме информационной безопасности уделяется достаточно много внимания. Существует ли какая-либо специфика обеспечения информационной безопасности в банке?*

О. СМОЛИЙ: В любой современной организации необходимо защищать три свойства информации – конфиденциальность, целостность и доступность. В зависимости от специфики работы организации приоритеты этих трех «столпов» могут меняться. В банке очень важны такие параметры, как доступность и целостность информации, поэтому при построении систем их учитывают в первую очередь. В отличие от конфиденциальности, важность которой не меньше, обеспечение защиты должно производиться не в ущерб первым двум.

Приведу конкретный пример. Для контроля почтового трафика мы поставили в банке две системы, одна из которых

InfoWatch Traffic Monitor, вторая – Websense DSS. Обе системы позволяют контролировать исходящий трафик на предмет наличия конфиденциальной информации в реальном времени и в случае обнаружения нарушений блокировать передачу подозрительных сообщений. Поиск конфиденциальной информации в сообщениях системы производят по разным алгоритмам, поэтому мы используем для этой задачи обе системы. Дополнительно система InfoWatch Traffic Monitor позволяет вести большой архив исходящей электронной почты банка за длительный период времени с возможностью подробного последующего анализа для расследования случаев утечки конфиденциальных данных.

Обычно при внедрении такие системы ставятся «в разрыв». То есть вся исходящая информация перед отправлением проходит через модули контроля. Письмо сначала проверяется, а затем, если не обнаружено нарушение, отправляется адресату. Если же находится чувствительная информация, то передача сообщения блокируется до принятия решения оператором. При этом получаются как значительные задержки в отправке сообщений, так и возможные ложные реагирования системы и блокирование сообщений по информации, похожей на конфиденциальную. Мы выбрали иную схему реализации: письмо отправляется без задержек, а модулю контроля предоставляется копия, которая анализируется на наличие конфиденциальной информации.

Выбирая такую конфигурацию системы, мы руководствовались тем, что в работе банка очень важны безотказность и своевременность доставки сообщений. Потери от ложной тревоги и возникающей при этом длительной задержки могут оказаться гораздо более значительными, чем в случае утечки информации. Поставив систему информационной безопасности в копию трафика, мы не вмешиваемся в работу почтовой системы, но в то же время мы можем проводить полный анализ исходящей информации без задержки писем.

То есть некоторые особенности в построении архитектуры системы существуют, и возникают они потому, что нам приходится расставлять приоритеты.

НБЖ: *А если обнаружится конфиденциальная информация в письме после его отправления?*

О. СМОЛИЙ: При должной организационной работе такие случаи происходят очень редко. И в основном не по злему умыслу, а по ошибке сотрудников. Здесь важна тщательная работа с кадрами банка, осведомленность в вопросах безопасности, дисциплина и осознанная ответственность сотрудников.

Кстати, нередко сотрудники службы информационной безопасности пытаются выразить риски в численном, то есть денежном выражении. Я считаю такие попытки «оцифровать» риски либо рекламным трюком, либо некомпетентностью. По моему

убеждению, сотрудник службы безопасности может обозначить риски, довести сведения о рисках до владельца информации и руководителя организации, но не может перевести риски в деньги. Это могут делать только бизнес-подразделения, которые являются владельцами информации, и то лишь оценочно. Можно попробовать рассчитать ущерб, который возникнет в случае реализации риска. Но эта оценка будет очень приблизительной, поскольку размер ущерба зависит не только от того, какая информация вышла за пределы кредитной организации, а в большей степени от того, как эта информация была использована.

НБЖ: *Системы безопасности – дорогое удовольствие. Какие средства защиты информации вы считаете первоочередными?*

О. СМОЛИЙ: Защита информации – это, прежде всего, организационный вопрос, а потом уже технологический. Некоторые банки вооружаются до зубов, покупая всевозможные системы по защите информации, а потом не знают, что со всей этой «тяжелой артиллерией» делать. В этом случае инвестиции вряд ли когда-либо окупятся, а результат может оказаться нулевым. Многие утечки информации могут быть предотвращены еще до установки систем DLP путем разработки специальной нормативной базы, обеспечения осведомленности сотрудников, проведения учебных семинаров и прочего. Эти меры позволяют многократно сократить риск утечки информации. К тому же нельзя закрывать выборочно угрозы отдельными средствами, как будто для этого предназначены. Решать проблемы надо комплексно, со всех сторон.

Кроме того, существуют недорогие системы, которые имеют многоцелевое назначение. Например, электронные замки на компьютерах, различные системы для контроля использования отчуждаемых носителей информации на компьютерах. Например, у нас в банке использование USB-устройств запрещено без специального разрешения. Чтобы получить его, нужно оформить заявку, согласовать ее с руководителем подразделения сотрудника, службой безопасности, подразделениями ИТ и т.д. В этом случае автоматизированное рабочее место сотрудника ставится под особый контроль.

Поэтому при обеспечении информационной безопасности нужно все-таки начинать с организационных мер, а уже потом выбирать соответствующие технологические решения, если они необходимы. В таком случае потребность в дорогостоящих системах будет сведена к минимуму.

НБЖ: *Но ВТБ, наверное, все-таки «вооружен до зубов»?*

О. СМОЛИЙ: Я бы сказал, что мы при решении этой проблемы придерживаемся принципа разумной достаточности.

ТОП-МЕНЕДЖЕР ПОДЧИНЯЕТСЯ ОБЩИМ ТРЕБОВАНИЯМ

НБЖ: *Какие угрозы, по вашему мнению, все-таки представляют наибольшую угрозу для кредитной организации – внутренние или внешние?*

О. СМОЛИЙ: По моему опыту, провести границу между внутренними и внешними угрозами не всегда возможно. Например, какой угрозой – внешней или внутренней – являются представители компаний-исполнителей или компаний-аутсорсеров?

НБЖ: *Наверное, это все-таки внутренняя угроза. Ведь банк передает этим компаниям часть своих функций.*

О. СМОЛИЙ: В некоторых случаях банк относит исполнителей к числу внешних угроз, так как от них легче защититься. Например, путем отделения среды разработки от промышленных сред. В данном случае банк действует по принципу «разделяй и властвуй».

НБЖ: *Внутренние угрозы более опасны?*

О. СМОЛИЙ: Еще в 2000 году, когда мы впервые разрабатывали модели нарушителей и угроз, оценив возможности различных типов нарушителей, был сделан вывод, что 80% угроз – это внутренние угрозы.

Противодействовать «внешнему врагу» уже не так сложно – весь мир много лет занимается этим, наработано множество рекомендаций, методик, практик и технических средств. А вот полностью обезопасить банк от внутренних угроз практически невозможно. Например, системный или сетевой администратор имеет доступ практически ко всей информации, а ограничить ему доступ нереально.

НБЖ: *А как же хакерские атаки? Сегодня многие от них страдают.*

О. СМОЛИЙ: Для крупного банка с хорошо организованной защитой информации хакерские атаки равносильны укусу комара. Замечу, «хорошо организованная защита» – это много работы и вложенных средств. Бывают, конечно, и более ощутимые угрозы. Например, DDOS-атаки, которые «накрывают» информационный доступ к банку. Но и от них можно успешно защититься: когда у банка есть своя автономная интернет-система, несколько провайдеров и многоканальная система доступа и при этом строится защита сетевого доступа на уровне провайдеров, то степень безопасности будет достаточно высокой, чтобы гарантировать стабильность работы. На некотором достигнутом уровне развития информационной безопасности вы начинаете уделять больше внимания другому. Ущерб от внешних атак уже несопоставим с возможным ущербом от внутренних утечек. Например, если руководитель высокого уровня, переходя на работу в другой банк, украдет данные по клиентам и потом начнет их, этих клиентов, переманивать, потери могут оказаться немалыми.

НБЖ: *ВТБ работает с корпоративными клиентами. Накладывает ли это какие-либо особенности на систему защиты информационной безопасности?*

О. СМОЛИЙ: Конечно, клиенты ВТБ – это крупнейшие корпорации, многие стратегически важны для страны, а потому мы должны обеспечить защиту информации не только от криминальных структур, но и от интересов спецслужб других государств.

НБЖ: *Но как можно противодействовать утечке баз данных вместе с топ-менеджером? Руководство банка по определению имеет доступ к широкому спектру информации. Как можно помешать уходящему топу «прихватить» ее с собой?*

О. СМОЛИЙ: Конечно, от каких-то малых по объемам утечек информации вообще невозможно защититься. Например, чуть ли не

каждый пятый человек легко запоминает до 30 экранов информации после определенных тренировок.

Но стоит отметить, что у высоких руководителей не всегда есть доступ ко всей информации. В крупных организациях топ-менеджер работает на штатной должности, и его полномочия по доступу к информации определяются в соответствии с его функциональными обязанностями, как и в случае с другими сотрудниками. То есть противодействовать нарушениям можно с помощью разграничения доступа по принципу минимально необходимых полномочий. Кроме того, для предотвращения злоупотреблений и фальсификаций существует известное правило «двух рук», когда документ вступает в действие только в том случае, если на нем стоят две подписи – руководителя и клерка. Существуют и другие механизмы, которые помогают защитить информацию от утечек или несанкционированных изменений. Мы уделяем пристальное внимание их разработке, а также контролю их исполнения, потому что нарушения в этой области могут не только привести к финансовым потерям, но и нанести серьезный ущерб репутации банка.

Например, некоторые клиенты, которым предлагают перейти на обслуживание в другую организацию, могут поддаваться на уговоры менеджера-нарушителя. А некоторые клиенты воспримут предложение как угрозу своему бизнесу, потому что задумаются о том, как другой банк получил сведения о его компании.

НБЖ: *Вы говорили, что криптографические системы обеспечивают достаточно надежную защиту конфиденциальности информации от внешних угроз. Всегда ли удается использовать системы шифрования для защиты?*

О. СМОЛИЙ: Отмечу, что данным вопросом я занимаюсь лишь косвенно и только в отношении систем связи. Криптография и вопросы управления ключевой информацией находится в компетенции моих коллег в нашем подразделении. Но могу сказать, что мы не применяем криптографию одновременно сразу в нескольких плоскостях в отношении одной и той же информации. Здесь действует принцип разумной достаточности. Не вся информация в банке требует использования криптографии. Часто, когда криптографическая защита для информации требуется, ее удобно и достаточно обеспечить на уровне документа. Или шифровать выборочные потоки информации. То есть не тотально защищать шифрованием все каналы связи, а защитить отдельный документ или отдельные каналы связи и участки сети. Например, при передаче информации по публичным каналам связи. Иными словами, мы закрываем криптографическими системами только то, что действительно нужно закрыть. Не допуская излишеств.

НБЖ: *То есть вы закрываете криптографическими системами критичные процессы?*

О. СМОЛИЙ: Да, мы оцениваем критичность каждого процесса и выбираем оптимальное решение для обеспечения его информационной безопасности. Например, возникла задача разработки удаленного рабочего места для возможности работы наших сотрудников на чужих неконтролируемых территориях – в командировках или дома. Для того чтобы сотрудник мог работать с информацией без риска ее утечки или искажения, мы создали так называемую доверенную виртуальную среду. Эта виртуальная среда «запуска-

ется» из зашифрованного образа, и при доступе к банковской информации проходит различные необходимые проверки.

ОДНО ХОРОШО, А ДВА ИНОГДА ЛУЧШЕ

НБЖ: *На какие параметры вы обращаете внимание в первую очередь при выборе решений по информационной безопасности? Как делаете выбор среди разработчиков и производителей?*

О. СМОЛИЙ: Мы делаем выбор, исходя из своих потребностей. Смотрим, что есть на рынке, сравниваем, а потом делаем выбор. Стандартный процесс. Много внимания уделяем вопросам дальнейшего технического сопровождения со стороны выбираемых интеграторов и производителей. Важно не только купить, но и грамотно внедрить и потом без сложностей эксплуатировать.

НБЖ: *Вы не придерживаетесь принципа единообразия – чтобы существовала единая платформа и чтобы проще было производить интеграцию?*

О. СМОЛИЙ: У единообразия есть две стороны. С одной стороны, внедрение единообразных систем, то есть, проще и понятнее, систем от одного разработчика. Например, мы давно нашли взаимопонимание со службой ИТ, что наша сложная телекоммуникационная среда должна быть единообразна для оптимизации структуры управления и сопровождения. В результате сейчас все телекоммуникационное оборудование у нас от одного производителя.

С другой стороны, иногда отсутствие разнообразия ведет к ослаблению надежности или недостатку функциональности. В некоторых случаях единообразие может создать единую точку отказа. Поэтому при выборе решений нужно каждый раз исходить из целесообразности. Например, при организации мониторинга исходящих потоков электронной почты мы пошли как раз по второму пути, о чем я рассказывал чуть раньше, – внедрили две системы различных производителей, которые дополняют друг друга – InfoWatch и Websense.

НБЖ: *Как добиться того, чтобы решения ИТ соответствовали не только техническим требованиям, но еще и требованиям к информационной безопасности?*

О. СМОЛИЙ: Важно понимать, что безопасность – не добавка к существующим информационным системам, а их неотъемлемая часть, нередко определяющая архитектурные решения. Бывает, схемы некоторых решений строятся на основании идей, зародившихся в подразделении безопасности. Например, когда разрабатывалась схема доступа наших зарубежных филиалов к банковской информационной системе. Дело в том, что законодательства стран различаются, и к тому же существуют юридические ограничения, поэтому часть операций необходимо производить на территории России. На вопрос, как это сделать, мы предложили создать виртуальный «филиал». В результате пользователи зарубежных филиалов работают в терминальном режиме, и обработка информации осуществляется в центре в нашей стране.

Такие совместные решения возможны, если сотрудники подразделений безопасности и ИТ говорят на одном языке. Когда есть конструктивный профессиональный диалог, находят оптимальные решения. ¹³³