



*Если составить список самых обсуждаемых за последний год ИТ-тем в банковской среде, в Топ-5 обязательно войдут проблемы безопасности систем ДБО, перспективы аутсорсинга банковских систем и систем информационной безопасности, а также облачный вопрос. У медали, как известно, две стороны: преимущества новых технологий несут с собой дополнительные угрозы. О том, как сохранить разумный баланс между выгодами и рисками и о прогнозах рынка ИБ для банковского сектора мы беседуем с **Анатолием Скородумовым, начальником отдела информационной безопасности банка «Санкт-Петербург»**.*

Ж.И.: Анатолий Валентинович, как, на Ваш взгляд, можно оценить эффективность работы ИБ в банковской сфере? Какие показатели являются здесь ключевыми?

А.С.: Оценить эффективность системы ИБ в организации достаточно сложно. Один из главных объективных показателей — это результаты внешних аудитов на соответствие российским и международным стандартам. Появление стандартов и ряда законодательных актов в последние 3–4 года стало своеобразным катализатором повышения общего уровня информационной безопасности в банках. Самые наглядные примеры здесь — закон № 152-ФЗ, требования стандарта PCI DSS. В части продвижения и развития своего стандарта по ИБ достаточно активен Банк России. Необходимо пони-

мать, что, кроме явного преимущества, заключающегося в выполнении требований регуляторов, успешное прохождение аудита несет в себе и опосредованные выгоды для бизнеса в виде увеличения лояльности клиентов, повышения позиций в рейтингах.

Ж.И.: Можно ли утверждать, что требования регуляторов фактически создали моду на высокий уровень ИБ для банковского сектора?

А.С.: Вполне возможно. Но моду задает и современное развитие ИТ-технологий. Среди вопросов повышения уровня ИБ в банках наиболее актуальной проблемой является уязвимость популярных сейчас систем дистанционного банковского обслуживания (ДБО), связанная как с особенностями использования меха-

низмов ИБ, так и с недостаточным пониманием клиентами требований информационной безопасности. Проблемы ДБО в том или ином виде сейчас занимают практически все российские банки: идут поиски конкретных решений, которые на длительный срок могли бы снять вопрос несанкционированного списания средств со счетов клиентов.

Наш банк для защиты систем ДБО внедрил SMS-авторизацию пользователей при их подключении к Интернет-банкингу и проведении платежей. В результате за последние 2 года у нас практически не было случаев несанкционированного списания денежных средств со счетов клиентов, хотя подобные попытки фиксируются достаточно регулярно. Дальнейшее развитие направления защиты систем ДБО является одной из priori-

тетных задач банка в 2012 году. Высокий уровень ИБ рассматривается нами как один из критериев привлекательности наших банковских продуктов для клиентов.

Л.И.: Какие еще механизмы защиты систем ДБО, кроме SMS-авторизации, реализует Ваш банк?

А.С.: В соответствии с действующим законодательством в системах ДБО для юридических лиц мы используем электронно-цифровые подписи, подтверждающие авторство и достоверность присылаемых электронных документов. Также мы планируем реализацию механизма хранения криптографических ключей с помощью сертифицированных USB-идентификаторов — eToken и ruToken. В его основе лежит принцип «вся криптография на борту», позволяющий избежать считывания криптографических ключей в оперативную память компьютера и тем самым минимизирующий риски их несанкционированного использования. В данный момент в банке проходит тестирование этой технологии. На 2012 год запланировано внедрение технологии хранения криптографических ключей на

пластиковых картах с электронным чипом.

Я не говорю о таких стандартных механизмах, как соединение по безопасному протоколу SSL, использование межсетевых экранов и систем антивирусной защиты.

Ж.И.: Один из трендов российского корпоративного рынка – обеспечение защиты используемых топ-менеджментом мобильных устройств. Насколько эта задача актуальна для банковского сектора?

А.С.: Согласен, что эта тема сегодня находится на модной волне, в том числе и в банковской сфере: смартфоны, имеющие доступ к внутренним корпоративным системам, мы используем достаточно широко. И если для стационарных компьютеров организация защищенного удаленного доступа стала привычным делом, мобильные устройства — в буквальном смысле слова подвижный элемент информационной инфраструктуры компании — вызывают трудности. Для защиты удаленного входа в систему со смартфонов и планшетных компьютеров мы по аналогии с системами ДБО планируем использовать технологию одноразовых паролей.

Ситуация осложняется еще и тем, что мобильные устройства очень разнообразны и не унифицированы в части используемых ОС и существующих стандартов. Проиллюстрирую на примере: около года назад мы обратились к решению проблемы защиты корпоративных смартфонов от вирусов и столкнулись с тем фактом, что антивирусных вендоров, поддерживающих всем известный iPhone, на рынке совсем немного. Думаю, что с течением времени в этой области произойдет стандартизация по аналогии с сегментом стационарных ПК — останутся лишь 2–3 операционные системы, и будут применяться универсальные системы защиты.

Л.И.: Если мы заговорили на «мобильную» тему, стоит посмотреть на нее под другим углом. Услуги ИБ, предоставляемые оператором связи, – в чем, на Ваш взгляд, состоят преимущества и особенности подобного подхода?

А.С.: Наш банк в 2011 году перешел на модель приобретения сервиса по защите от DDoS-атак у оператора связи, поэтому мы можем говорить об этом, исходя из собственного опыта. С технической точки зрения построение подобной системы защиты предъявляет высокие требования к пропускной способности каналов и подразумевает наличие в ИТ-подразделении высококвалифицированных узкопрофильных специалистов. Поэтому банк извлекает определенную выгоду, приобретая сервис по ИБ у оператора. С другой стороны, предоставление этих услуг российскими телекомами пока находится в стадии становления и развития, одна из наиболее актуальных проблем на данный момент — отсутствие про-



зрачного SLA. Но это вопрос ближайших 2–3 лет.

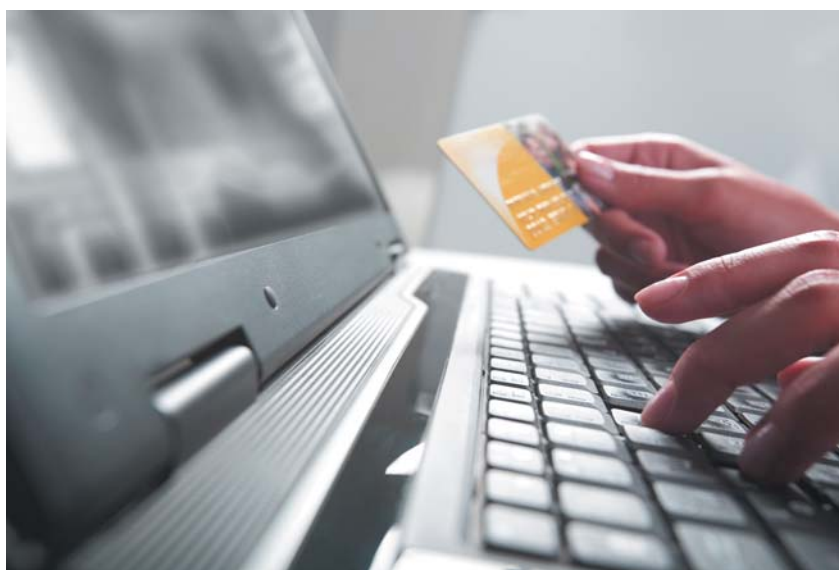
Ж.И.: Возможен ли в принципе аутсорсинг информационной безопасности?

А.С.: Я полагаю, что он не только возможен, но и выгоден. Вопрос только в том, что именно отдавать «на сторону» и кому. Компании-аутсорсеру можно доверить практически весь аудит — внешний и при определенных условиях внутренний, процессы, связанные с формированием модели угроз и оценки рисков, разработку плана обеспечения ИБ и проекты по его реализации. В то же время аутсорсинговая модель реализуема далеко не всегда: если мониторинг инцидентов ИБ ложится в эту схему, то непосредственно разбор конфликтных ситуаций и реагирование на инциденты без наличия собственных служб безопасности и ИБ практически не осуществимы. То же относится к вопросам контроля действий ИТ-администраторов и функционирования систем управления персоналом. Отмечу, что возможности аутсорсинга в сфере обеспечения ИБ достаточно велики, но используются сейчас лишь на 5–10%: бизнес-среда еще не созрела для конкретных действий в этом направлении. Можно констатировать, что исторически компании опасаются доверять внешним контрагентам вопросы информационной безопасности.

Ж.И.: В чем состоят главные риски аутсорсинга ИБ?

А.С.: Традиционным камнем преткновения в этом вопросе является риск утечки конфиденциальных данных: считается, что собственных сотрудников проще контролировать. Второе препятствие на пути массо-

вого распространения аутсорсинга ИБ — сложность процедуры привлечения внешнего контрагента к ответственности в случае установления факта утечки. С одной стороны, обязательства аутсорсера и необходимые параметры услуг прописываются в SLA. С другой, участники банковского рынка понимают, что в случае обращения в суд доказать вину компании-аутсорсера будет непросто: в России отсутствует подобная судебная практика.



Ж.И.: Как она практически отсутствует и в отношении фактов DDoS-атак и мошенничества в системах ДБО.

А.С.: Да, к сожалению, прецедентов, связанных с расследованием нелегального доступа к аккаунтам систем ДБО, также недостаточно для того, чтобы говорить о развитой уголовно-правовой практике противодействия мошенничеству в ИТ-сфере. До внедрения дополнительных механизмов обеспечения ИБ мы несколько раз сталкивались с тем фактом, что у наших клиентов возникали трудности при возбуждении уголовного дела даже в случае несанкционированного списания средств с их

счетов. Распространенная причина — отсутствие признаков состава преступления и подозреваемых. Аналогичный вопрос возникает у правоохранительных органов и в отношении распределенных отказов в обслуживании, обычно приносящих косвенный ущерб: как квалифицировать эти инциденты? Несколько лет назад в правоохранительных органах были созданы специализированные подразделения, занимающиеся преступлениями в сфере высо-

ких технологий. Но их ресурсов недостаточно, да и координация работы между различными подразделениями МВД оставляет желать лучшего. Технологии мошенничества в настоящее время значительно опережают возможности российской правоохранительной системы, и очень небольшое количество подобных дел доводится до суда, поэтому единственная правильная стратегия для компаний — быть на шаг впереди злоумышленников благодаря использованию современных механизмов защиты.

Ж.И.: Для каких отраслей аутсорсинг ИБ станет наиболее приемлемым и выгодным вариантом?



А.С.: На мой взгляд, эта модель интересна как SMB-сектору, так и компаниям Enterprise-уровня. Аутсорсинг ИБ позволяет SMB отказаться от содержания дополнительных специалистов в штате ИТ-службы. Средним и крупным компаниям выгодно отдавать вовне аудиты на соответствие действующим стандартам ИБ, чтобы получать независимую оценку уровня информационной безопасности.

Ж.И.: Ваши прогнозы – будут ли банки идти на использование услуг информационной безо-

пасности из облака? Какие сервисы для банков могут стать облачными?

А.С.: На данный момент я вижу две услуги, которые представляют для нашей сферы интерес с точки зрения их реализации в Cloud-среде. Первая – это облачный удостоверяющий центр, позволяющий банкам отказаться от организации собственных УЦ. Клиенты – как физические, так и юридические – проходят регистрацию, получают криптографические ключи и в дальнейшем авторизуются в системе,

размещенной в облаке. Банк лишь отправляет в Cloud запрос, подтверждающий/отклоняющий аутентификацию клиента. Вторая перспективная облачная услуга – заказ и проведение внешних тестов на проникновение. Cloud-сервисы могут значительно упростить организацию определенных банковских процессов и минимизировать расходы, поэтому нас рано или поздно ждет долгая дорога в облака.

Ж.И.: Когда можно ожидать массового распространения облачной ИБ?

А.С.: Судя по тому, что о вопросах переноса ИТ-инфраструктуры в частную облачную среду говорят уже около 2 лет, а участники рынка пока решаются лишь на единичные внедрения, года через 3–4 мы придем к повсеместному предоставлению из облака традиционных ИТ-услуг. О прогнозах распространения Cloud-сервисов ИБ говорить пока рано.

Ж.И.: Спасибо за беседу!