Опубликовано на Швейцария: новости на русском языке (https://nashagazeta.ch)

Как обезопасить банковские вклады? | Comment protéger ses comptes bancaires?

Автор: Надежда Сикорская, Женева , 20.12.2011.

(© Alpict)

В продолжение ставших традиционными Интернет-конференций, проводимых Нашей Газетой.ch при поддержке Газпромбанка, предлагаем вашему вниманию беседу экспертов на тему, которая в последнее время приобрела особую актуальность: о защите банковских вкладов от происков злоумышленников.

|
La sécurité informatique est une grande question d'actualité: dans le cadre des

conférences, organisées par NashaGazeta.ch avec le soutien de GazPromBank, nous vous proposons une discussion sur la protection des données bancaires, menée par des experts en Suisse et en Russie.
Comment protéger ses comptes bancaires?

Помните песенку Лисы Алисы и Кота Базилио из чудесного фильма «Приключения Буратино», в котором мнимые друзья советуют деревянному мальчику, как лучше распорядиться неожиданно свалившимся на него состоянием: «Заройте ваши денежки…» и так далее.

Конечно, те времена прошли, современные «богатенькие Буратино» предпочитают не зарывать свои золотые монетки в землю, не класть в тумбочку и не прятать в люстру, а поручать заботам специалистов - сотрудников банков, инвестиционных компаний и прочая. Впрочем, движет ими то же стремление – сделать так, чтобы денежки «проросли». При этом желательно, чтобы размеры «урожая» не становились бы достоянием широкой общественности.

Однако в последнее время участились случаи утечки этой заведомо конфиденциальной информации, что радует любителей совать нос в чужие дела, но не может не вызывать озабоченности как и самих вкладчиков, так и всех профессионалов, работающих в области финансов. Вот об этом мы и поговорим сегодня с двумя экспертами, подходящими к проблеме каждый со своей точки зрения.

У нас в гостях: **Алексей Константинович Плешков**, начальник Отдела защиты информационных технологий Газпромбанка (Москва, Россия), и **Алексис Сикорский**, Генеральный директор группы New Access, специализирующейся на производстве программного обеспечения для частных банков (Женева, Швейцария).

Наша Газета.ch: Господа, кто из вас знает, когда произошел первый случай хищения банковской информации и может о нем рассказать?

Алексей Плешков: Первые факты хищения банковской информации – по сути, ровесники самих банков и относятся к VIII веку до нашей эры. В этот период в Древнем Риме происходило становление государственности, развивался товарный обмен, денежные и кредитные отношения. Первые римские банки (банк – от итальянского слова «стол», «banco») специализировались на меняльном деле (нумулярии) и на кредитных операциях (аргентарии). Уже тогда переезжавшие в другое поселение сотрудники забирали с собой все созданные ими ведомости и накопленные за время работы материалы и знания. С другой стороны, бедные слои свободного населения и беглые рабы под страхом смерти совершали набеги и грабежи на рыночные площади, где размещались банки (меняльные столы), отбирая у банкиров (менсариев) не только наличные денежные средства, предметы обихода и дорожные карты, но и рукописные ведомости.

Алексис Сикорский: В обозримом прошлом первый серьезный случай кражи данных с целью передачи их «компетентным органам» имел место в 2002 году в лихтенштейнском банке LGT: конфиденциальная информация, касающаяся 1400 клиентов этого банка, была тогда передана германской налоговой инспекции.

В начале декабря 2009 года бывший сотрудник отдела информатики женевского

банка HSBC передал французским властям банковские данные, касающиеся французских налогоплательщиков, обладающих скрытыми счетами в Швейцарии. В список попали около 3000 человек, уклонявшихся от налогов.

В начале февраля 2010 года Германия получила предложение приобрести, за несколько миллионов евро, банковскую информацию о 1500 немецких налогоплательщиках, обладающих счетами в Швейцарии.

Швейцарию, страну с традиционно безупречной репутацией хранителя банковских тайн, в последние годы сотрясали скандалы, связанные с кражей – уж будем называть вещи своими именами – данных самими сотрудниками банков. Кто эти люди? Что ими руководит?

Алексис Сикорский: Действительно, профиль похитителя данных в последнее время изменился. Раньше главной мотивацией была возможность заработать, и покупатели находились – налоговые ведомства разных стран всегда готовы были дать хорошую цену за информацию о сбережениях своих граждан в швейцарских банках. Против возникшего таким образом черного рынка были приняты соответствующие контр-меры. В последнее же время мы все чаще имеем дело с «борцами за справедливость», которыми движет не личная выгода, но своеобразное понимание общественной пользы. Придавая огласке конфиденциальную информацию, они считают, что вносят свой вклад в борьбу с капитализмом. При этом они прекрасно понимают, что их действия незаконны, и готовы нести за них ответственность.

Зафиксированы ли подобные случаи в России? И как реагируют в российских банковских кругах на происходящее в Швейцарии?

Алексей Плешков: К сожалению, в последние годы в крупных российских организациях также увеличилось количество случаев утечки информации. Эксперты-аналитики связывают это в первую очередь с последствиями мирового экономического кризиса. Многие преданные работники, вынужденные под прессом обстоятельств менять место работы, теряли лояльность к работодателю и не стеснялись, уходя, «забирать то, что плохо лежит». Именно в этот период, столкнувшись с реальными случаями утечек и краж информации на местах, руководители компаний задумались о решении задачи обеспечения информационной безопасности. Российское банковское сообщество в этом смысле может выступать исключением: в 2006 году появился Стандарт Банка России СТО ИББС 1.0, в соответствии с которым банки в нашей стране предпринимают целый комплекс мер по защите информации. Это позволило в период экономического кризиса снизить риски компрометации и утечки конфиденциальной информации, тем самым повысив показатели финансовой привлекательности и рейтинги этих организаций в целом.

Неужели все «борцы за справедливость», о которых говорил Алексис Сикорский, так хорошо подготовлены технически, что могут преодолеть все системы защиты данных и похитить их?

Алексис Сикорский: В случаях, о которых идет речь, в роли воров часто выступают не специалисты в области информатики, а служащие банков или бэк-офисов без особых технических навыков.

А вообще, техническую защиту данных можно сравнить с противостоянием между броневой защитой и ракетами: на каждый новый технологический шаг в развитии брони изготовители ракет отвечают тем же.

В области информационной безопасности происходит такое же соревнование между службами защиты банков и пиратами. Кто выйдет победителем, зависит от того, если говорить коротко, сколько банк вложил на данный момент средств в защиту собственной информации. Однако, сколько ни вкладывай, уязвимым местом всегда будет человеческий фактор.

Интересующимся этим вопросом рекомендую самого знаменитого хакера всех времен, американца Кевина Митника, про него даже написана книга «The Art of Deception: Controlling the Human Element of Security de Kevin Mitnick». Он провел несколько месяцев в тюрьме за различные преступления, связанные с информатикой. По его собственному признанию, он мало пользовался техникой, но обильно – контактами с людьми.

Действовал он так: звонил пользователям информационной системы какого-нибудь предприятия, представлялся сотрудникам службы информатики и спрашивал пароли. Удивительно, но даже сегодня в самых защищенных банках такая тактика будет самой действенной.

Но как же банку защитить себя от предательства изнутри? Ведь нельзя совсем лишить сотрудников доступа к информации?

Алексис Сикорский: Разумеется! Если оставить в стороне чисто технические средства, а говорить об исключительно, так сказать, организационных, то начать нужно, наверное, с разделения ролей администратора банка данных и администратора системы. Кроме того, надо препятствовать переносу информации о клиенте куда бы то ни было, будь то на бумагу или в электронный файл. Даже если бывает нужно иметь доступ к информации, связанной с открытием счета, редко возникает необходимость в ее распечатке. В любом случае, все попытки распечатать информацию, сохранить или перенести ее куда-то могут быть пресечены или, по крайней мере, тщательно отслежены.

Алексей Плешков: Согласен с Алексисом в том, что нужно подходить к решению проблемы утечки комплексно. Как известно, информационная безопасность – это не состояние, а процесс, протяженный во времени. Чтобы минимизировать риски утечки конфиденциальной информации и банковской тайны в автоматизированных банковских системах (АБС), важно проводить целый комплекс мероприятий - с момента принятия решения о внедрении АБС в банке, заканчивая этапом утилизации использованного оборудования. Причем к любой АБС уже на этапе проектирования должны предъявляться четкие требования, включая требования к подсистеме журналирования событий, наличию средств криптографической защиты, парольной политики, правил разграничения прав доступа, а также требования по наличию в АБС рабочего места администратора безопасности с соответствующими инструментами и интерфейсами.

Широкое распространение в настоящее время получают информационные системы защиты, позволяющие устанавливать на конфиденциальные документы метки, определяющие политику доступ к документу на различных рабочих местах. Системы

обрабатывают сохраненный документ и ставят на него подобие электронного замка, который может быть открыт только на строго определенных компьютерах конкретными сотрудниками. Если данный документ выносят за территорию организации и пытаются открыть на другой компьютере, то электронный замок не позволяет прочитать такой документ. Система защищает также от попыток скопировать содержание документа с меткой в другой документ или сделать скриншот экрана.

Но что может помешать сотруднику с дурными намерениями просто сфотографировать, например, экран с представленной на нем информацией?

Алексис Сикорский: Для этого есть специальные меры безопасности. Можно, например, применить операцию, называемую «маскирование информации». Тогда не экране будет видна не вся информация, а лишь нужные на данный момент элементы ее: подпись, имя без адреса, или особые условия счета без имени владельца. Если же нужно увидеть информацию полностью, можно применить так называемый «floutage», тогда на экране будет видна вся информация, но не одновременно, а фрагментами, словно на них направляется луч фонарика.

Алексей Плешков: Для банков по ряду направлений есть четкие требования регуляторов в части технического оснащения рабочих мест сотрудников. Например, кассовые узлы в обязательном порядке должны быть оборудованы несколькими видеокамерами различной направленности, что, в свою очередь, очень действенно останавливает сотрудника от использования средств видео и фото съемки. Также, с письменного разрешения сотрудника, по согласованию с его руководителем, допускается оборудование рабочего места видеокамерами наблюдения.

Одно из возможных решений – и это касается сотрудников и государственных, и коммерческих организаций - запрет на внос технических средств связи на территорию организации и контроль за выполнением данного требования со стороны обычных сотрудников данной организации. Другим выходом может стать использование специальных экранов на мониторы, не позволяющих сфотографировать отображаемую информацию. Но, к сожалению, во всех перечисленных выше случаях остается риск утечки конфиденциальной информации, вынесенной из организации в голове нелояльного сотрудника (сразу вспоминается старый советский художественный фильм «Щит и меч» с С. Любшиным).

Давайте затронем еще один вопрос, волнующий наших читателей. Многие говорят, что бояться оплачивать товары и услуги в Интернете, опасаясь, что номер их кредитной карточки попадет в руки злоумышленников. Какие меры защиты пользователей применяются в России и в Швейцарии?

Алексис Сикорский: Принцип ответственности при пользовании кредитной картой один и тот же независимо от того, используется ли она в Интернете или в традиционном магазине: владелец карты несет ответственность, только если можно доказать, что он проявил халатность. Иными словами, при незаконном использовании карты рискует коммерсант, а не ее владелец, за исключением случаев, когда выдавший карту банк может доказать не соответствующее нормам пользование ею.

То есть риск, что вам придется платить за что-то, что вы не покупали, практически равен нулю. С другой стороны, учреждение, выдавшее карту, обладает очень

мощной программой, позволяющей контролировать отклонения от привычных для владельца карты покупок. Таким образом, такой регулярный пользователь Интернета, как я, нередко получает звонки от Сотрудников Swisscard, проверяющих, имела ли место та или иная транзакция на непривычном сайте.

В личном плане меня всегда забавляет, когда люди боятся платить карточкой на таком сайте, как Amazon, опасаясь, что украдут ее номер, но легко дают ее какому-то мелкому агенту по найму машин в экзотической стране…

Алексей Плешков: В России до недавнего времени решение о возмещении клиенту банка денежных средств по несанкционированным операциям с его кредиткой зависело только от самих банков. По общепринятой практике ответственность за операции по утраченным (украденным или потерянным) картам возлагалась на держателя. Что касается операций в сети Интернет и по поддельным картам, то лишь часть банков (в том числе Газпромбанк) потерянные средства клиентам возмещают. Многие банки этого не делают, и оспорить их решение можно было только в судебном порядке. И хотя судебная практика, в большинстве случаев, принимала сторону клиентов, само судопроизводство проистекало достаточно длительное время (иногда год и более), что доставляло клиентам много хлопот, отнимало время и силы. Поэтому многие клиенты при незначительных потерях предпочитают в суд не обращаться. Но даже в банках, которые добровольно возвращали деньги, в связи с отсутствием для этого правовых оснований, процесс занимал длительное время (минимум несколько месяцев).

Летом 2011 года в России был принят Федеральный закон «О национальной платежной системе», которым, в частности, регулируется ответственность банка в случае несанкционированных клиентами операций. Клиент, потеряв карту или обнаружив, что карту используют без его согласия, должен незамедлительно проинформировать банк. При строгом соблюдении всех требований направления такого уведомления (они прописаны в законе) банк должен возместить клиенту сумму операции, совершенной без согласия клиента, если не докажет, что клиент сам нарушил порядок использования платежной карты, что и привело к пропаже средств.

То есть законодатель возлагает риск потерь на банк в полном объеме (а не частично, как в западных странах), в том числе по утраченным картам. Однако данные пункты закона вступают в силу только с 1 января 2013 года.

К сожалению, часто наблюдается финансовая неграмотность людей. При выборе банковских продуктов вопросы безопасности являются второстепенными. И даже если банк предоставляет своим клиентам инструменты, позволяющие снизить риск потерь, многие клиенты либо не умеют, либо не хотят ими пользоваться.

Например, в нашем банке у держателей карт – целый комплекс инструментов защиты. Прежде всего, это возможность совершать операции в сети Интернет «Безопасные платежи» с использованием технологии «Verified by Visa» (Проверено Визой) и «SecureCode» (Безопасный Код). Для этого клиент должен подписаться на услугу в любом офисе банка или с использованием банкомата Газпромбанка. При регистрации указывается мобильный телефон держателя. Теперь при совершении операций в сети Интернет, если магазин поддерживает указанную технологию, клиент с сайта магазина будет перенаправляться на сайт Газпромбанка, при этом на

мобильный телефон держателя высылается SMS-сообщение с одноразовым паролем, который необходимо ввести. Если пароль вводится правильно, то операция оплаты одобряется. Злоумышленник, которому станут известны реквизиты карты (номер, срок действия, код проверки карты), все равно не сможет осуществить незаконную операцию. Такая операция возможна только посредством организации высокотехнологичных атак. Например, в результате заражения компьютера держателя вредоносным программным обеспечением (вирусы, Трояны и др.) или перехвата всего информационного потока с компьютера держателя (атака «человек по середине»). Но даже в этом случае есть решение: для того, чтобы минимизировать или даже исключить потери в результате таких неправомерных воздействий, Газпромбанк предлагает услуги системы «Телекард». С ее помощью мы информируем (отправляем SMS-сообщения) держателю карты обо всех произведенных им операциях, что позволяет сразу же выявить несанкционированные. С помощью той же самой системы «Телекард» можно быстро заблокировать карту и избежать дальнейших потерь (не нужно звонить в службу поддержки банка и ждать соединения с оператором, выслушивая голос автоответчика как ваш звонок важен банку, а мошеннические операции при этом будут продолжаться).

Однако постоянно следить за SMS-сообщениями не всегда удобно. Да и телефон может быть вне зоны доступа или владелец в момент несанкционированных операций, возможно, просто спит. Для ограничения ущерба в подобных случаях «Телекард» позволяет установить суточный лимит по карте. Например, можно поставить нулевой лимит. А если необходимо совершить операцию оплаты или снятия наличных денежных средств, то с помощью SMS-сообщения лимит поднимается до нужной суммы, после операции лимит снова обнуляется. В таком случае, даже если у держателя похитят карту вместе с ПИН-кодом, снять денежные средства не получится. Если держатель пользуется картой достаточно часто, то каждый раз перед тем как воспользоваться картой отправлять SMS будет довольно неудобно. С помощь «Телекарда» можно минимизировать и это неудобство и управлять своими рисками. Для этого необходимо поставить значение доступного лимита равного той сумме, которой вы часто пользуетесь, и при этом потеря которой не будет для вас слишком болезненна, например, в размере заправки автомобиля и (или) обеда в кафе. Тогда при осуществлении данных оплат не нужно посылать SMS, мошенник же не сможет похитить сумму большую, чем установленный лимит - ведь он не знает, какой лимит вы установили, и может попытаться осуществить первую операцию на большую сумму. Такая попытка будет неуспешной и даст время держателю заблокировать свою карту.

Газпромбанк продолжает развивать инструменты по безопасному использованию платежных карт. Мы планируем внедрение виртуальных карт, по которым можно будет осуществлять операции только в сети Интернет. Денежные средства на такие карты можно будет переводить с помощью систем «Домашний банк» (интернет банк) или «Телекард», что позволит клиентам не держать на картах значительных сумм, а переводить их непосредственно перед использованием.

В заключение нашей беседы прошу вас ответить на вопрос : в каком направлении, на ваш взгляд, будет идти работа над защитой банковских данных в ближайшие пять лет?

Алексис Сикорский: На мой взгляд, в ближайшие годы два фактора определят

развитие контроля за банковскими данными в Швейцарии.

Во-первых, технологии защиты данных улучшаются с каждым днем, как и подготовка сотрудников.

Во-вторых, и это, наверное, самая интересная тенденция, банки обязаны теперь, в силу юридических и процессуальных причин, не только располагать все более полной информацией о каждом клиенте, но и предоставлять эту информацию все более значительному числу сотрудников.

Я думаю поэтому, что хищения информации в банках в ближайшие годы не прекратятся, но соглашения, заключаемые Швейцарией с соседними государствами, сделают их все более бессмысленными.

Алексей Плешков: последнее время в России значимые изменения произошли на уровне законодательства - определены четкие требования по обеспечению защиты получаемой от граждан информации, ее обработке и безопасной передаче по каналам связи. Причем эти требования должны выполняться не только при создании новых комплексных систем. Ранее внедренные системы также должны быть приведены в соответствие с положениями новых нормативных документов.

Еще одно важное направление – тщательный разбор зафиксированных инцидентов, ставших известными фактов совершения злоумышленниками несанкционированных действий по отношению к объектам защиты.

В частности, одним из важнейших направлений сейчас является вектор построения защиты от совершения злоумышленниками мошеннических операций с использованием пластиковых банковских карт или систем дистанционного банковского обслуживания. Хакеры придумывают новейшие технологические схемы для проведения атак на Банки и, к сожалению, психологические и социальные приемы воздействия на клиентов Банков. Именно защита интересов и финансовых средств наших клиентов от действий мошенников является и будет являться для нас наиболее приоритетным направлением на ближайшие годы.

Спасибо за очень интересную и содержательную беседу!

Газпромбанк
Алексис Сикорский
банки в Швейцарии

Source URL: *http://www.nashagazeta.ch/news/12686*