



Осознавая ПОТЕНЦИАЛ онлайн безопасности



Бо Моландер (Bo Molander)

Директор по продажам,
Gemalto E-Banking, Россия

Быстрый рост популярности Интернет- и мобильного банкинга идёт рука об руку с серьёзными сомнениями в безопасности онлайн среды. Большие объёмы финансовых транзакций, которые сейчас совершаются через персональные компьютеры, ноутбуки, планшеты и смартфоны, с неизбежностью привлекают внимание как отдельных злоумышленников, так и организованных преступных групп. И всё чаще банки и финансовые организации сталкиваются с всё более

изощрёнными угрозами. Так, в конце 2012 года сообщалось, что злоумышленники похитили около 36 млн. евро у 30 тысяч корпоративных и частных клиентов банков, используя новую версию вредоносной программы Zeus (названную Eurograbber), которая была разработана, чтобы обойти аутентификацию, осуществляемую с помощью SMS-сообщений, высылаемых банком на мобильные устройства. В свете таких проблем любая организация, которая предоставляет услуги онлайн- или мобильного банкинга либо обеспечивает поддержку электронной коммерции, безусловно, вынуждена принимать эффективные ответные меры. Однако было бы неправильно рассматривать эти проблемы как всего лишь ещё одну внешнюю угрозу, с которой могут справиться исключительно ИТ-специалисты.

Может показаться, что здесь нет прямой логической связи, но обеспечение безопасности операций в Интернет- и мобильной среде в настоящее время открывает большие возможности перед теми, кто работает в финансовом секторе, для обеспечения более прибыльного и стабильного будущего. Хотя, на первый взгляд, реализация стратегии, сочетающей в себе надёжную защиту и удобство конечных пользователей, - это всего лишь ещё одна головная боль в и без того сложных для бизнеса условиях, но она может на самом деле обеспечить платформу для значительного повышения эффективности, качества услуг, прибыльности и конкурентоспособности.

Аргументы в пользу принятия бизнес-ориентированного подхода к безопасности являются ясными и убедительными. Во всех развитых странах накоплен огромный импульс для развития онлайн- и мобильного банкинга, которые обеспечивают клиентам удобство, богатство выбора



и контроль над своими ресурсами. В России уже достигнуты высокие показатели использования Интернета и распространения смартфонов, причем и тот, и другой продолжают расти высокими темпами. Кроме того, в стране с такой огромной территорией и крупными городами, страдающими от автомобильных пробок, привлекательность банковских операций и покупок в режиме 24/7 либо не выходя из дома или на ходу очевидна.

В финансовом секторе потребность в Интернет-банкинге и мобильном банкинге для широкого диапазона групп потребителей очевидна. Более того, за счет успешного развития и продвижения этих услуг, банки получают преимущества для развития бизнеса, выходящие далеко за рамки простого удовлетворения спроса клиентов. Традиционные банковские отделения, в которых клиентов обслуживают лицом к лицу, обходятся слишком дорого, чтобы быть средством для выполнения рутинных операций по поручению клиентов. Поощряя существующих держателей счетов выполнять основную часть своих финансовых операций в режиме онлайн, можно значительно сократить накладные расходы, например, на персонал. Кроме того, за счет сокращения очередей в филиалах или в колл-центрах можно существенно повысить качество услуг, предоставляемых клиентам, которые действительно нуждаются в индивидуальной помощи и консультации. С учетом проблем, с которыми многие банки в России сталкиваются в настоящее время, возможность достичь такого скачкообразного роста эффективности, одновременно предоставляя клиентам услуги, которые они хотят использовать, просто слишком ценна, чтобы её упустить.

Чтобы воспользоваться всеми преимуществами растущего спроса на Интернет- и мобильный банкинг, поставщики должны быть в состоянии продемонстрировать устойчивость и целостность их процессов обеспечения безопасности. Но они должны сделать это, не умень-

шая основного преимущества финансовых операций и покупок в среде Интернета - их удобства. В связи с этим хорошей новостью является то, что существует множество проверенных, готовых к использованию, экономически эффективных и удобных для пользователей решений, которые легко могут обеспечить высокие стандарты безопасности Интернет- и мобильного банкинга, электронной коммерции. Хотя компания Gemalto известна в России больше всего как производитель банковских карт, но это лишь часть гораздо большей истории. Gemalto также является признанным мировым лидером в области цифровой безопасности для финансового и телекоммуникационного секторов, а комплекс решений Gemalto for Banks охватывает как производство карт, так и защиту онлайн-банкинга. Разработанное компанией Gemalto семейство Ezio включает широкий спектр различных методик и устройств, которые предназначены для снижения уровня опасности даже самых продвинутых мошеннических атак, при этом общими характеристиками входящих в Ezio решений для онлайн-банкинга являются масштабируемость, гибкость, модульность и простота реализации. Эти решения разрабатывались с учётом будущего развития технологий - в них заложены возможности беспрепятственной модернизации и поддержки новых продуктов и услуг, внедряемых поставщиками.

Каждое отдельное банковское приложение нуждается в решении по обеспечению безопасности, которое должно удовлетворять специфическим требованиям. Однако ключ к успеху почти всегда заключается в формировании этих решений в соответствии с потребностями различных типов конечных пользователей. Молодые люди, например, проявляют повышенный интерес к использованию смартфонов, планшетов и phablet (смартфонов с увеличенным экраном, сочетающих функциональность смартфона и планшета) для выполнения разнообразных повседневных задач; обычно с энтузиазмом ос-

ваивают новые технологии. В отличие от них клиенты постарше могут предпочитать более традиционных и знакомые методы защиты, такие как зеркало заднего вида на банкомате или транзакции "Чип и ПИН".

Эффективный подход Pick and Mix ("собрать и перемешать") к безопасности обеспечивает специализированный сервер Ezio от Gemalto - многоканальное, multi-token и мультивендорное решение, которое поддерживает все технологии аутентификации: стандартную двухфакторную аутентификацию, такую как одноразовые пароли OTP (One Time Password); двойную (Double) аутентификацию - "запрос/ответ" (Challenge/Response); а также более передовые методы верификации транзакции, такие как динамические подписи (Dynamic Signatures) и разделение доменов безопасности (Secure Domain Separation). Эффективность Ezio Server была подтверждена в ходе испытаний более чем 20 различными производителями устройств аутентификации.

Аналогичный уровень гибкости банки и финансовые организации могут обеспечить, используя выпускаемые компанией Gemalto картридеры различных форм-факторов. Популярность кардридеров на российском рынке, подтверждаемая их внедрением в ряде ведущих банков, отражает значительные преимущества, которые присущи этому типу устройств. С точки зрения банка, они повышают уровень окупаемости инвестиций в EMV-карты. В России популярность таких карт быстро растет: более 100 миллионов новых карт EMV будут выпущены в 2013 году. Как следствие, клиенты, скорее всего, уже знают, что такое персональные кардридеры, и готовы их использовать в качестве удобного средства обеспечения безопасности своих финансовых операций в онлайн-среде. Тем более что имеется широкий выбор беспроводных и подключаемых ридеров для различных приложений. Подключаемые устройства, например, обеспечивают поддержку ряда функций, включая цифровые подписи, имеющие юридическую силу, а также возможности sign what you see ("проверь, что подписываешь"), которые позволяют клиентам просматривать детали сделки, прежде чем подтвердить операцию.

Наряду с кардридерами имеется широкий ассортимент токенов различного дизайна и функциональности - от однокнопочных генераторов одноразовых паролей OTP (на базе событий или времени) до защищённых устройств высокого класса с клавиатурой, которые обеспечивают верификацию транзакций и возможность работы с различными каналами ДБО.



На фоне глобальной финансовой нестабильности, банковский сектор России характеризуется огромным числом и разнообразием организаций, которые вынуждены конкурировать в очень сложной обстановке. Но все эти организации объединяет общее желание увеличить эффективность работы, сократить расходы, повысить стандарты обслуживания клиентов и добиться большего отличия от конкурентов. Для решения всех этих задач предпочтительным является активный подход к переводу клиентов на безопасную модель онлайн-банкинга.

Экономическое обоснование не может быть яснее. Расчеты показывают, что обслуживание одного клиента в традиционном отделении банка обходится в среднем в 10 евро, каждый раз, когда он проходит через входную дверь. В онлайн-банкинге типичные затраты на обеспечение одной рутинной транзакции падают до менее чем одного евро. Учитывая, что сегодня банкам доступны все инструменты, необходимые для преодоления сомнений клиента в целостности как своих денег, так и персональных данных, фундаментальным ключом к успеху является правильный выбор стратегии поставщиками финансовых услуг.

Очевидно, что те, кто рассматривает кибербезопасность как долгосрочную возможность для построения устойчивого будущего, обеспечивают себе самые сильные конкурентные позиции; банки же и финансовые организации, которые продолжают рассматривать вопросы безопасности как еще одну IT-задачу, будут иметь гораздо более неопределенные перспективы.

Для получения подробной информации о решениях Gemalto по обеспечению безопасности электронного банкинга (Gemalto E-Banking security solutions), пожалуйста, посетите www.gemalto.com/ebanking или обращайтесь к Бо Моландеру на bo.molander@gemalto.com.

