

Аутентификация в банках: парадокс небезопасности

Ника Комарова

ИНЦИДЕНТЫ УТЕЧЕК КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ, КРАЖ СРЕДСТВ СО СЧЕТОВ КЛИЕНТОВ В БАНКАХ СЛУЧАЮТСЯ ВСЕ БОЛЕЕ ЧАСТО. ФИНАНСОВЫЕ ИНСТИТУТЫ ПОСТОЯННО ГОВОРЯТ ОБ УЖЕСТОЧЕНИИ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СВОИХ СИСТЕМ И ЗАЩИТЕ ОТ ИНСАЙДА. ОДНАКО ИССЛЕДОВАНИЯ ВЫЯВЛЯЮТ ПАРАДОКСАЛЬНУЮ СИТУАЦИЮ В СФЕРЕ КОНТРОЛЯ ДОСТУПА: ЕДВА ЛИ НЕ БОЛЬШЕ ПОЛОВИНЫ СОТРУДНИКОВ РОССИЙСКИХ БАНКОВ ВКЛЮЧАЯ АДМИНИСТРАТОРОВ ИСПОЛЬЗУЮТ КОРОТКИЕ «СЛАБЫЕ» ПАРОЛИ ИЗ СОСЕДСТВУЮЩИХ СИМВОЛОВ, СОВПАДАЮЩИЕ С ИМЕНЕМ ПОЛЬЗОВАТЕЛЯ И Т.П. ПРИ ЭТОМ УЖЕСТОЧЕНИЕ ТРЕБОВАНИЙ К ДЛИНЕ И КАЧЕСТВУ ПАРОЛЕЙ ПРИВОДИТ К ТОМУ, ЧТО, НЕ В СОСТОЯНИИ ЗАПОМНИТЬ ИХ, СОТРУДНИКИ ЗАПИСЫВАЮТ ИХ НА СТИКЕРАХ, КОТОРЫЕ МОЖНО ОБНАРУЖИТЬ ПРЯМО НА МОНИТОРЕ ИЛИ ПОД КЛАВИАТУРОЙ. ОДНИМ ИЗ НАИБОЛЕЕ ДЕЙСТВЕННЫХ СПОСОБОВ РАЗРЕШЕНИЯ СЛОЖИВШЕЙСЯ СИТУАЦИИ ЯВЛЯЕТСЯ ИСПОЛЬЗОВАНИЕ ДВУХФАКТОРНОГО МЕТОДА АУТЕНТИФИКАЦИИ НА БАЗЕ АППАРАТНЫХ ТОКЕНОВ (USB-КЛЮЧЕЙ ИЛИ СМАРТ-КАРТ).

Обеспечение безопасности данных, хранящихся в информационных системах банков, сегодня приобрело для последних критическое значение. Фактически каждая цифра в многочисленных базах данных финансовых институтов имеет реальный денежный эквивалент. Для банка критично четкое определение ролей сотрудников, выполняющих операции со счетами. Отдельным пунктом стоит требование по соблюдению правила «двух рук», когда каждая финансовая операция (перевод денег, изменение реквизитов и т.д.) выполняется одним сотрудником, а подтверждается — другим. И все же в такой системе есть слабое звено. Им является метод идентификации того, что сотрудник, предоставивший аутентификационные атрибуты для доступа в систему, является именно тем, за кого себя выдает. Сегодня вопрос обеспечения строгой аутентификации в банковских учреждениях стоит как никогда остро. С одной стороны, над банками довлеет закон «О персональных данных», где немалая роль отведена проблеме контроля доступа, с другой — общемировые финансовые коллизии повысили риски утечки информации, возведя их в квадрат благодаря массовым увольнениям.

Ключ под ковриком

Однако, несмотря на внушительное количество инцидентов в сфере безопасности данных и усиленную пропаганду обязательной работы с персоналом, которую ведут ИБ-специалисты, на практике лишь немногие банки тратятся на тренинги и устраивают стресс-проверки относительно выполнения требований политик ИБ. Свод этих правил, единожды утвержденный начальством, скорее всего, заперт в сейфе службы безопасности и не является в общепринятом смысле «рабочим» документом. Прописная истина для всех, кто знаком с социальной инженерией: хочешь узнать пароль — поищи стикер около монитора, к сожалению, работает. В том числе, и в банках. Как правило, сам логин секретной информацией не является, а пароль каждый второй сотрудник финансового института хранит если не под клавиатурой, то в ящике стола. Иногда, придя в банк к откры-



Хочешь узнать пароль —
поищи стикер около монитора



тию офиса, можно наблюдать, как операционистка звонит своей опаздывающей коллеге с просьбой сообщить ее пароль, потому что иначе никак нельзя открыть операционный день и начать работу. Пароль легко сообщается сотруднику ИТ-подразделения, которому надо несколько раз перезагрузить настраиваемый компьютер. Или коллеге на время отпуска (на всякий случай).

Все это, конечно, рабочие моменты, которые происходят ежедневно в сотнях банков и не приводят к катастрофическим последствиям, но бывают исключения. Гарантий того, что завтра сотрудник не окажется в критической ситуации, нет. Если она потребует от него быстрого решения и быстрых денег, одним из выходов может стать кража средств у работодателя. Ежедневно банки совершают несколько сотен тысяч проводок: денежный перевод в любой валюте на счет фирмы «под закрытие» может быть замечен не сразу, а это оставляет шанс обналить перевод. И дело в шляпе. Понятно, что отжавшийся на противозаконную операцию инсайдер не будет совершать кражу под своей учетной записью. Для этого, не прилагая особых усилий, можно узнать пару чужих паролей и осуществить требуемый перевод «от имени» их владельцев. То есть выдать себя за другого легального пользователя системы, исполнить его роль в проведении операции и остаться неузнанным — и есть основная цель инсайдера. Если система защиты и контроля доступа в банке допускает хотя бы малейшую возможность подобной операции, то ее превращение в жизнь — это лишь вопрос времени.

Admin1981

До сих пор примитивный способ аутентификации с использовани-

ем пары «логин-пароль» является наиболее простым, дешевым и, как следствие, распространенным методом идентификации субъекта в большинстве информационных систем. Если ужесточить требования к длине и сложности пароля, сотрудник начнет записывать его на бумажках. К эскалации проблемы приводит тот факт, что у специалиста крупной организации наберется с десятков паролей к разным системам. Запомнить их все не каждому по силам.

Эксперты Positive Technologies в исследовании «Анализ проблем парольной защиты в российских компаниях» проанализировали 185 тыс. паролей, используемых российскими пользователями для доступа к различным информационным системам, порталам, базам данных. Отчет содержит статистику по паролям, полученную в ходе тестирований на проникновение, аудитов безопасности и других работ, выполненных экспертами компании в 2007-2009 году. Были задействованы различные методики компрометации учетных записей, в том числе с применением специализированных сканеров безопасности, словарных атак и инструментальных аудитов.

Исследование выявило, что основными слабыми местами парольного способа аутентификации являются следующие факторы. Во-первых, использование нестойких паролей, низкое качество парольных комбинаций. Статистика применяемых отечественными пользователями паролей значительно отличается от зарубежной. Российский список паролей на 50% состоит из расположенных рядом символов (1234567, qwerty и т.д.), тогда как западные пользователи больше склонны употреблять слова английского языка (password, love и т.д.). Показательно, что среди 185 тыс. проанализированных паролей не было обнаружено ни одного смешанного — использу-

ющего латинские и кириллические символы.

Несоблюдение элементарных требований к парольным комбинациям подвергает риску всю систему корпоративной информационной безопасности. Согласно исследованию, вероятность компрометации пароля из 4 символов равна ~97%, а при условии использования 9-символьного пароля этот показатель почти в 6 раз ниже и составляет ~17%. Данную проблему могло бы уменьшить внедрение несложных политик безопасности, не позволяющих применять пароли длиной менее 8-10 символов. Добавление правил о том, что пароль не должен содержать комбинации из соседствующих символов и символов одного регистра, позволяет существенно повысить уровень защиты доступа. Однако, как уже было указано выше, порог запоминаемости — это 4-5 паролей, если их больше — принятые меры по безопасности станут стимулом для их обхода.

Во-вторых, халатное отношение к вопросам безопасности со стороны администраторов. Несмотря на использование длинных паролей, сисадмины в 15% случаев выбирают «словарные» комбинации либо пароли, совпадающие с именем пользователя (10%), а в 2% случаев пароль отсутствует вовсе. Подбор такого пароля методом словарной атаки, как правило, не составляет особого труда и не занимает много времени. При этом пароль администратора как привилегированного пользователя позволяет иметь фактически неограниченный доступ ко всем типам данных включая конфиденциальную информацию, персональные данные сотрудников и документы, содержащие коммерческую тайну. Риск, которому подвергает компанию рядовой пользователь, применяя нестойкий пароль, безусловно, высок. Но он не идет ни в какое сравнение с тем ущербом, который может понести компания вследствие несанкционированного доступа с последующей утечкой конфиденциальных данных «от лица» администратора.

В-третьих, несоответствие паролей стандартам безопасности. В настоящее время актуальна тенденция к переходу российских компаний кредитно-финансового сектора на международные стандарты. Поэтому в отчете Positive Technologies рассматривается проблема использования паролей в контексте со-

ответствия требованиям стандарта по защите информации в индустрии платежных карт PCI DSS (Payment Card Industry Data Security Standard). Как известно, PCI DSS был создан в связи с ростом краж и утечек конфиденциальной информации, в частности реквизитов доступа к счетам пользователей платежных систем. Данный стандарт является обязательным во всем мире, в том числе на территории стран CEMEA, куда входит и Россия. Действие PCI DSS распространяется на всех, кто передает, обрабатывает и хранит данные держателей карт (VISA, MasterCard, American Express). По результатам исследования Positive Technologies, 74% паролей, используемых в корпоративном секторе, не соответствуют уровню безопасности, декларируемому PCI DSS. Из этого следует, что теоретически больше половины финансово-кредитных организа-

на тему ответственности за разглашение пароля и т.д. Но любые внезапные проверки просто заставляют работников отлепить стикеры с паролями от монитора и поместить их под клавиатуру или в лучшем случае — в ящик стола.

Аутентификация: как это должно быть

Исходя из постулатов комплексного подхода к обеспечению информационной безопасности, организационные мероприятия необходимо дополнять соответствующими техническими мерами. Отказ от слабых паролей в пользу двухфакторного метода аутентификации на базе аппаратных токенов (USB-ключей или смарт-карт) признан наиболее оптимальным способом решения данной задачи. Двухфакторный способ



К физическому носителю парольной информации сотрудники компаний относятся более ответственно



ций, попавших в базу исследования, не смогли бы пройти обязательную ежегодную процедуру аудита на соответствие PCI DSS, а это повлекло бы за собой штрафные санкции со стороны международных платежных систем.

Резюмируя результаты исследования, можно утверждать, что уровень защищенности корпоративных информационных систем отечественных компаний по-прежнему остается очень низким. Более того, он в значительной степени зависит от «человеческого фактора». Пренебрегая элементарными политиками безопасности, службы ИБ оставляют на совести пользователя обеспечение защиты данных, с которыми тот работает. Немного улучшают ситуацию регулярные семинары для сотрудников, направленные на повышение их грамотности в вопросах информационной безопасности, с обязательным «запугиванием»

подтверждения подлинности аутентификационных реквизитов базируется на следующих факторах: «то, что я имею» и «то, что я знаю». Для того чтобы получить доступ в систему, пользователь должен, во-первых, предъявить «ключ» — обычно токен или смарт-карту, подтвердив факт обладания, а во-вторых доказать, что этот «ключ» принадлежит ему, указав PIN-код к нему. Подобные технологии позволяют повысить уровень информационной безопасности в организации и существенно облегчить жизнь ее сотрудникам. На одном токене можно хранить пароли ко всем системам и приложениям (так называемая политика «единого входа» — Single Sign On), с которыми ежедневно приходится работать пользователю.

Опыт показывает, что к физическому носителю парольной информации сотрудники компаний относятся во много раз ответствен-

нее, чем к абстрактному паролю. Психологическая тонкость состоит в том, что токен выдается под расписку, сотрудник несет за него материальную и своего рода моральную ответственность. Кроме того, токен персонализирован, а следовательно, все действия с его использованием будут выполняться «от лица» владельца и могут быть отслежены в системе.

В правильно спроектированную систему двухфакторной аутентификации можно заложить и другие полезные возможности. Например, имплантировать в токены или смарт-карты RFID-метки для прохода через систему контроля и управления доступом (СКУД), что позволит обеспечить политику «чистых экранов», когда пользователь не может выйти из помещения (покурить, попить чаю и т.д.), не вынув токен или смарт-карту из компьютера. А в момент извлечения операционная система блокируется до следующего подключения с вводом PIN-кода.

Доступ из «недоверенной среды»

Также не стоит сбрасывать со счетов риски удаленного доступа к информационным ресурсам мобильных сотрудников. Обеспечение аутентификации из «недоверенной среды» — нетривиальная задача для банка. Проверить паспортные данные у человека, который пытается получить доступ по VPN, невозможно, впрочем, как и проконтролировать наличие вовремя обновленного антивирусного ПО на его рабочей станции, а также качество соблюдения банковских регламентов по безопасности. Риск кражи пароля при удаленном сценарии доступа возрастает на порядок: для его перехвата в ходе сеанса связи по открытым каналам используются самые различные средства, начиная от «шпионского» ПО и заканчивая атаками типа «человек-по-середине». Обеспечить должный уровень безопасности в данной ситуации можно двумя способами: с помощью расширения функциональных возможностей уже используемых внутри банковской организации USB-ключей либо за счет аутентификации пользователей при помощи одноразовых паролей (OTP, One-Time Password).

В первом случае аутентификация будет максимально безопасной, пос-



кольку она основана на применении аппаратной криптографии, реализованной в USB-токене. Основное неудобство заключается в необходимости установки драйверов, что может оказаться невозможным при работе из интернет-кафе, гостиницы, с коммуникатора и т.д. В ближайшее время, правда, планируется выход на рынок токенов, которые не требуют установки драйверов, однако эта технология пока не отработана и потребует «обкатки», прежде чем стать массовой. Во втором случае все несколько проще: сотруднику выдается специальное устройство — генератор одноразовых паролей (OTP-токен), оснащенное кнопкой и небольшим дисплеем. При нажатии на кнопку устройство выдает последовательность из шести цифр, которую пользователь вводит в специальную веб-форму для пароля. В целях повышения надежности такого способа аутентификации можно совместить одноразовый пароль с запоминаемой частью, тогда даже если кто-то украдет устройство, он не сможет получить доступ к данным. Перехваченная или подсмотренная злоумышленником последовательность чисел, созданная при нажатии на кнопку устройства, также ничего не даст, так как действительно лишь единожды.

Примером успешного перехода на средства строгой аутентификации может служить опыт ряда кредитно-финансовых учреждений. «В условиях недостаточного экономического роста необходимо сохранять конкурентоспособность, минимизируя широкий спектр рисков, к числу которых относится возможность обо-

да сотрудниками установленных ИБ-политик, — комментирует ситуацию Сергей Коханько, начальник отдела информационной защиты и безопасности «Первого Республиканского Банка». — Снижение влияния «человеческого фактора» за счет внедрения технологичных и прозрачных в управлении средств аутентификации позволило нам решить ряд задач в этой области».

В исследовании «Аналитического банковского журнала», в котором приняли участие эксперты из Промсвязьбанка, Россельхозбанка, Раффайзенбанка, Коммерцбанка (Евразия), банка «Возрождение» и других финансовых институтов, токены признаются одним из лучших средств обеспечения контроля доступа к информационным ресурсам. «Аппаратные средства строгой аутентификации являются наиболее действенным и одновременно гибким средством противодействия несанкционированной деятельности», — отмечает Иван Янсон, заместитель руководителя службы информационной безопасности Промсвязьбанка. В резюме исследования АБЖ делает вывод, что наиболее широкие перспективы на рынке средств аутентификации открываются для производителей токенов с аппаратной реализацией российской криптографии и интеграцией в инфраструктуру открытых ключей, что обеспечивает высокий уровень защиты банковских систем и соответствует требованиям регуляторов. Последнее особенно актуально в преддверии вступления в силу закона «О персональных данных». ●