Комплексная защита систем ДБО

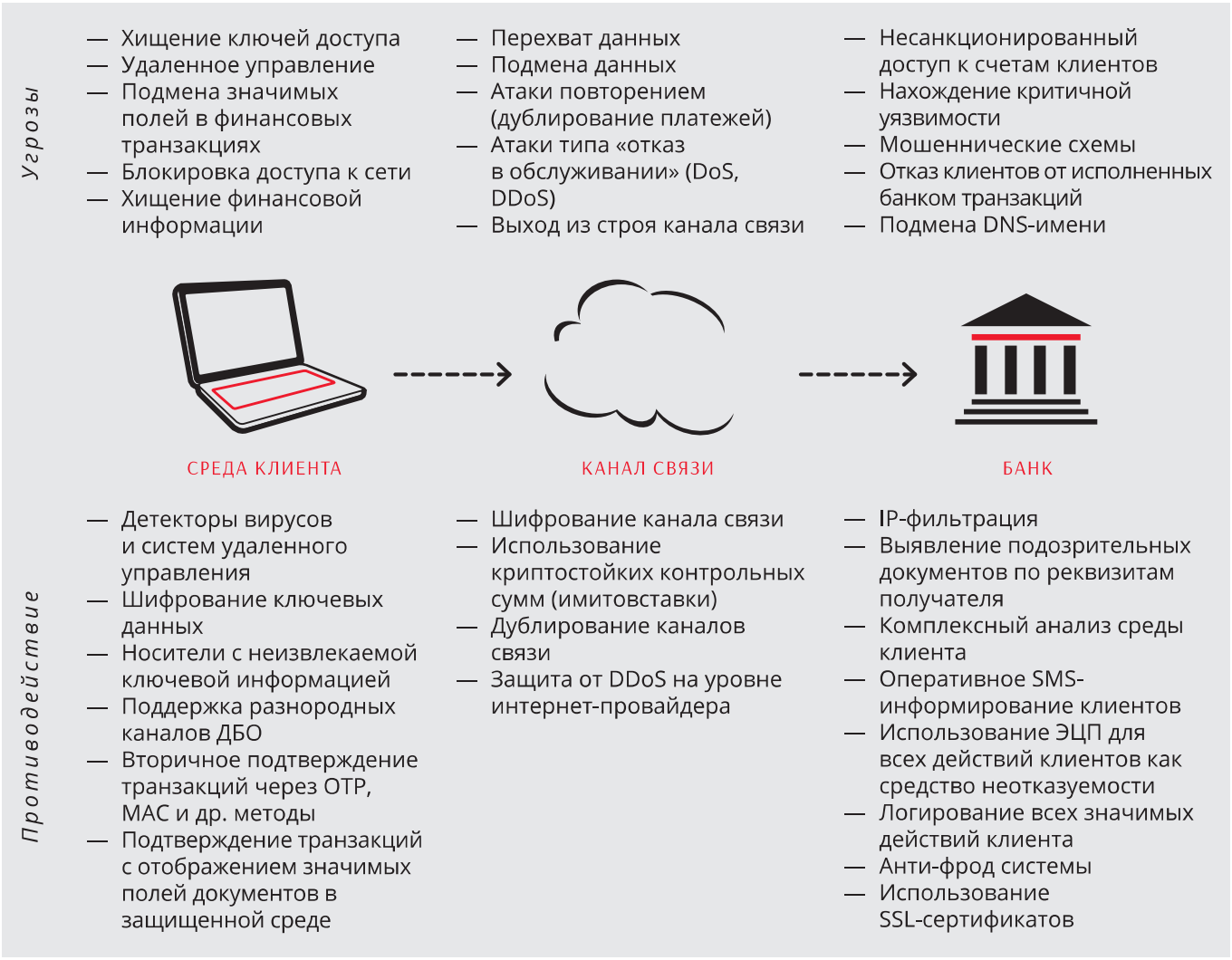
Рынок дистанционного банковского обслуживания (ДБО) продолжает активно развиваться и является обязательным пунктом стратегии успешного банка. На фоне роста популярности услуг интернет-банкинга, увы, увеличивается и число хищений средств со счетов клиентов

Дмитрий Ковалевский
директор по продажам,
BIFIT

Сегодня встречаются как простые примеры халатности, когда к точкам входа в систему ДБО (ПК, ноутбук, планшет или др.) и средствам аутентификации имеет доступ любой сотрудник компании, так и целенаправленные атаки, когда за жертвой ведется длительное наблюдение и производится хищение средств с использованием специального ПО и оборудования. Усугубляет ситуацию еще и то, что средний уровень компьютерной грамотности неуклонно падает при росте процента компьютеризации в Украине. В большей мере проблема связана с упрощением интерфейсов и мифом, что современный ПК + операционная система + обновленный антивирус = 100%-ная защита от всех угроз.

Основной товар банков — это доверие. Любые негативные инциденты снижают

ФОТО: АРХИВ ДМИТРИЯ КОВАЛЕВСКОГО



рыночную привлекательность, а значит — требуется уделять больше внимания безопасности и защите клиентов. Общий уровень защиты системы ДБО равен уровню защиты самой незащищенной части этой системы. Из этого следует, что обеспечивать безопасность необходимо комплексно. Рассмотрим три условных сегмента защиты: сторону клиента банка, канала связи и сторону банка.

СТОРОНА КЛИЕНТА БАНКА

Это самая разнообразная и бесконтрольная часть системы ДБО. Можете не фантазировать на тему построения защищенной рабочей среды у своих клиентов — правильно эту среду всегда считать недоверенной. Самый большой бич систем ДБО — вирусы и удаленное управление, которые не останавливаются антивирусами и фаерволами. Системы антивирусной защиты и фаерволы лишь создают трудности для хищения средств. Те же вирусы легко могут быть адаптированы под текущую версию антивируса, что не позволит выявлять их активность. От момента заражения компьютеров до момента добавления сигнатур в антивирусные базы могут пройти месяцы. Не спасают клиентов и компьютеры под управлением Mac OS X, которые по какой-то причине считали неприступными для вредоносного ПО, пока не вскрыли крупнейшую зараженную вирусами сеть (ботнет). К слову, она уже приблизилась к отметке 900 тыс. Mac OS X устройств.

Конечно, использование свежего ПО и регулярное обновление антивирусов

Безопасность не должна мешать ведению бизнеса, но в то же время нужно осознавать, что попытка защититься от злоумышленников только одним механизмом или устройством может нанести фатальный ущерб банку. Система безопасности должна быть комплексной и обслуживаться компетентными людьми, т.к. именно человеческий фактор является решающим и при зарабатывании, и при потере денег

немаловажно, но клиентам рекомендуют еще один простой рецепт — использовать носители с неизвлекаемыми ключами, такие как USB-токены/смарт-карты, и иметь дополнительный канал подтверждения операции для значимых платежей (через SMS, смартфоны, OTP/MAC-токены, EMV-CAP-ридеры или др.).

Как выглядят USB-токены и смарт-карты уже многие представляют. Стоит отметить лишь то, что не все USB-токены и смарт-карты в Украине могут неизвлекаемо хранить ключи и в ряде случаев представляют собою необоснованно дорогое хранилище данных с паролем. Производители этого не скрывают, но и не афишируют этот тонкий момент.

Кроме того, такая защита от копирования ключей нужна не только клиенту. Она еще и гарантирует банку защиту от обвинений в том, что у сотрудников осталась копия ключа, и это стало причиной хищения средств клиента.

На дополнительных методах подтверждения транзакций остановимся подробнее:

- **Подтверждение по SMS** — самый доступный и понятный метод, который не требует капитального вложения, но имеет высокую стоимость одной операции (в зависимости от контрактов колеблется от 0,07 до 0,25 грн). Стоит еще отметить, что операторы связи не гарантируют отсутствия прослушивания канала и тем более 100%-ную доставку сообщений. Идеально подходит для финансово неактивных клиентов, которые не делают ничего дополнительно для своей безопасности.

- **Приложение для смартфона** — новый перспективный способ с низкой себестоимостью и без затрат на транзакции. Не следует забывать, что смартфон, независимо от марки и ОС, является также недоверенной средой. Так, например, за 2012 год было обнаружено уязвимостей у iPhone — 56, у Android — 6, у BlackBerry — 3 и у Windows Phone — 1. Поэтому такой метод подтверждения нельзя назвать 100%-но защищенным.

- **OTP-токены** являются представителями защищенного канала подтверждения. По сути, это криптографические часы, которые на основании некоего секрета, времени и дополнительных данных показывают на встроенном экране одноразовый пароль. Слабое место таких устройств — то, что в параметры генерации не включаются значимые поля транзакции, что позволяет произвести подмену транзакции.

- **MAC-токены** — аналогичные OTP-токенам устройства, но уже с возможностью уточнения значимых полей операции. Выбор таких устройств очень велик и отличается кроме форм-фактора еще и методом ввода данных. Можно встретить как устройства с клавиатурой для ввода данных вручную, так и VIP-решения, как, например, AGSES-карты, которые считывают значимые поля с экрана компьютера, отображают данные на собственном экране в защищенной среде и требуют проверить отпечаток пальца для выдачи одноразового пароля.

EMV-CAP-устройства похожи по принципу на MAC-токены, но концептуально отличаются тем, что механизм генерации одноразового пароля находится не в устройстве, а в любой подключаемой платежной карте со смарт-чипом. Для таких устройств подходят платежные карты VISA, MasterCard, American Express и др.

Отдельно стоит выделить устройства, которые представляют из себя **USB-токен с экраном**, как например TrustScreen. Такое устройство не только «умеет» подписывать документ внутри себя, но и отображает подписываемую информацию, делая тем самым невозможной незаметную подмену значимых полей документа. Подтверждение подписи документа совершается нажатием на клавишу устройства. Такой механизм исключает возможность подписи по удаленному доступу или с использованием вирусов. Для удобства использования предусматривается пакетное подписание документов и автоматическое (без нажатия на клавишу устройства), но в этом случае ЭЦП будет содержать пометку, что пользователь не ознакомился с содержанием каждого документа или не подтверждал подписание документа собственноручно.

Каждый из названных методов подтверждения транзакции имеет свою целевую аудиторию из клиентов банка. И если при подключении SMS-канала все очень прозрачно и понятно, то при выборе устройств стоит учитывать стоимость серверной части, политику лицензирования и возможность замены производителя устройств.

КАНАЛ СВЯЗИ МЕЖДУ БАНКОМ И КЛИЕНТОМ

Если относительно эффективности защиты клиентской сети у экспертов IT-безопасности есть расхождения во взглядах, то насчет необходимости защиты канала связи мнения совпадают. Банк обязан обеспечить защиту канала от прослушивания, навязывания информации и максимально обеспечить доступность сервисов. Поэтому стоит выбирать систему ДБО с наличием шифрования канала связи и защитой от навязывания информации.

Как правило, у нас в стране на проблему доступности сервиса обращают внимание только в момент его отсутствия по причине сбоя у провайдера, физического повреждения канала связи или заказной DDoS-атаки.

Вопрос построения защищенного канала связи очень важный и требует комплексного подхода. Он включает разработку инфраструктуры сети, дублирование каналов связи, балансировку нагрузки и т.д.

Если говорить про DDoS-атаки, то защиту от них невозможно осуществлять только со стороны банка, т.к. иногда атаки настолько велики, что не выдерживает даже оборудование провайдеров. В этом случае лучше обращаться к организациям, которые предоставляют услуги по противодействию DDoS-атакам.

СТОРОНА БАНКА

Современные системы ДБО имеют как достаточно простые в пояснении черные/белые списки IP-адресов/назначений, платежей/счетов получателя или разнообразные лимиты на снятие, так и системы выявления вредоносного ПО, удаленного доступа.

Кроме этого, есть целые комплексы фрод-мониторинга, которые анализируют все информационные потоки в банке и принимают решения как в автоматическом режиме, так и под контролем сотрудников банка. К выбору таких систем нужно подходить очень тщательно, т.к. бюджеты по таким системам значительны, а результаты могут не оправдать затраты.

Конечно, все это разнообразие механизмов и комплексов не заменяет друг друга, а только дополняет общую систему безопасности. Подбор оптимального сочетания систем защиты и ее настройка требуют индивидуального подхода.

BIFIT

BIFIT
www.bifit.ua
e-mail: info@bifit.ua
тел.: +38 (044) 585-12-21
+38 (056) 726-01-20
+38 (056) 797-60-97
Skype: bifit-ua