ЗАЩИТА ИНФОРМАЦИИ

Лащенко А.А., Абакумов Д.Е.

Белорусский государственный университет информатики и радиоэлектроники1
г. Минск, Республика Беларусь

Унучек Е.Н.– старший преподаватель

В связи с развитием информационных технологий и компьютеризацией экономики одним из важнейших вопросов в деятельности компании становится обеспечение информационной безопасности.

Информация – это один из самых ценных и важных активов любого предприятия и должна быть надлежащим образом защищена. Цель обеспечения информационной безопасности – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения. Информационная безопасность помогает обеспечить непрерывность бизнеса.

В настоящее время невозможно представить деятельность банка без работы с информацией о его клиентах. Финансово-кредитные организации хранят и обрабатывают информацию о сотрудниках, клиентах, партнерах и других лицах. Безусловно, любая утечка или потеря персональных данных способна привести к невосполнимому ущербу для бизнеса и репутации. Наряду с этим защита персональных данных – это требование законодательства.

Актуальность

Финансовые данные – самая популярная среди киберпреступников цель в информационном пространстве. Криминальный бизнес так же, как и легальный, направлен на получение и максимизирование денежной прибыли, а наиболее выгодные данные находятся в распоряжении финансовых организаций.

Информационная безопасность и защита информации банка должны быть на достаточно высоком уровне, чтобы отражать любые атаки и попытки вторжения со стороны злоумышленников, в том числе со стороны сотрудников самой организации.

Описание проблемы и существующих условий

Утечки информации о кредитных картах, кража персональных данных, программы-вымогатели (например, WannaCry), кража интеллектуальной собственности, нарушение конфиденциальности, отказ в обслуживании – эти инциденты информационной безопасности стали обычными новостями. Среди пострадавших попадаются крупнейшие, наиболее состоятельные и наиболее защищенные предприятия: правительственные учреждения, крупные розничные сети, финансовые структуры, даже производители решений по информационной безопасности.

Среди угроз можно выделить:

Кража конфиденциальной информации – тип атаки, при которой внешние нарушители или неудовлетворенные работники крадут информацию, которая является важной для компании;

Дефейс сайта – тип атаки, при которой страница web-сайта заменяется другой страницей, чаще всего содержащей рекламу, угрозы или вызывающие предупреждения;

Фишинг – тип атаки, при которой злоумышленник получает важную информацию (например, логины, пароли или данные кредитных карт) путем подделывания сообщений от доверенного источника (например, электронное письмо, составленное как легитимное, обманом заставляет получателя кликнуть по ссылке в письме, которая устанавливает вредоносное программное обеспечение на компьютер);

Программа-вымогатель – тип вредоносного программного обеспечения, блокирующего доступ к данным на компьютере, в результате чего преступники вымогают выкуп за то, чтобы разблокировать заблокированные данные;

Потеря данных из-за природных явлений или несчастных случаев.

Чтобы защитить свой бизнес, вам нужно понимать ценность ваших данных и как их можно использовать. Также необходимо определить, какую информацию требуется защищать в рамках законодательства, например, платежная информация или персональные данные. Ниже представлены примеры данных, которые вам необходимо идентифицировать и инвентаризировать:

Кредитные карты, банковская и финансовая информация;

Персональные данные;

Базы данных клиентов, цены на закупку/поставку;

Коммерческие секреты компании, формулы, методологии, модели, интеллектуальная собственность.

Предложения по решению проблемы и перспективы дальнейшего развития будем рассматривать банк «Сбербанк». Информация взята с официального сайта sber-bank.by.

Самые распространенные схемы мошенничества в «Сбербанке» сейчас:

«Звонок из Банка»

Вам звонит незнакомец. Номер входящего звонка очень похож на номер банка, а звонящий представляется работником контакт-центра или службы безопасности банка.

Для реализации мошеннической схемы также используются мессенджеры, прежде всего Viber. Входящий звонок максимально закамуфлирован под звонок сотрудника банка: на аватарке может использоваться логотип банка (полностью или частично), а отображаемый телефонный номер звонящего может быть очень похож на телефон службы поддержки банка.

У мошенников есть возможность звонить с номеров, похожих на официальные номера банка. Злоумышленники меняют цифры в номере, которые вы можете не заметить.

У вас просят конфиденциальные данные

Мошенник сообщает, что «банк выявил подозрительную операцию по Вашей карте» или «поступил запрос на онлайн-оформление кредита на Ваше имя».

Он просит у вас логин и пароль от Сбербанк Онлайн, код из SMS от Банка (сопровождаемый фразой «Никому не сообщайте!»), реквизиты карты (полный номер карты и срок ее действия, CVV- или CVC-код). Это нужно якобы «для сохранности ваших денег».

«Потенциальный покупатель»

Мошенник представляется потенциальным покупателем товара, объявление о продаже которого было размещено вами в сети интернет. По каким-то причинам «покупатель» не может сегодня привезти деньги, но хочет прислать вам залог из другого города по системе дистанционного банковского обслуживания.

Ссылка

Для проверки поступления перевода мошенник направляет вам ссылку на фишинговый сайт, который очень близок по дизайну на используемый вами интернет-банк или страницу для ввода реквизитов карточки для получения уже отправленного перевода денежных средств. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

QR-код

Вместо ссылки мошенник может направить вам QR-код, который также хранит в себе ссылку на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

«Сообщения в социальных сетях»

Мошенник незаконным путем получает доступ к страничке в социальной сети и отправляет сообщения с просьбой финансовой помощи от имени ее владельца друзьям.

Просьба может быть самая разная: от «Скинь мне денег на карту, по дружбе» до нехватки денег на большую покупку. В редких случаях мошенник даже просит произвести оплату самостоятельно, обещая возместить затраты при личной встрече.

«Розыгрыши/раздачи/опросы от Банка или иных организаций»

Мошенники оставляют выдуманную рекламу в популярных социальных сетях об опросе от имени Банка и «Раздаче призов первой 1000 прошедших опрос!». Цель опроса – изучить мнение клиентов. После прохождения опроса организатор обещает денежное вознаграждение.

Однако, после прохождения опроса необходимо заплатить небольшую комиссию, связанную с перечислением вознаграждения.

«Отмена оформленного заказа»

Мошенник представляется работником торгово-сервисной сети (интернет-магазина, сервисного предприятия, службы доставки и др.) и сообщает, что на имя держателя карты оформлен заказ на покупку/доставку товара/услуги. Получая ответ о том, что заказ не оформлялся – дальнейшие действия могут быть следующими:

– мошенник предлагает сделать отмену оформленного заказа и уточняет информацию банке, в котором обслуживается держатель карты (т.е. какого банка карточку вы используете);

– в процессе разговора (если сообщено название Банка) мошенник инициирует процедуру смены логина/пароля в личном кабинете интернет-банка или добавления нового доверенного устройства;

– от Банка приходит SMS с кодом и его просят сообщить;

– узнав SMS-код, мошенник получает доступ к вашему личному кабинету в интернет-банке.

«Оформление кредита»

Мошенник в телефонном разговоре представляется работником белорусского банка или сотрудником правоохранительных органов, который сообщает свое звание или личный номер.

В ходе разговора мошенник сообщает об оформлении на имя собеседника кредита, для погашения которого необходимо срочно получить новый кредит в любом ближайшем отделении банка (любого банка). При этом также сообщает, что документы по оформленному клиентом новому кредиту будут использованы в суде как доказательство понесенного материального ущерба или в качестве смягчающих обстоятельств.

При этом мошенники держат потенциальную жертву в постоянном напряжении, запугивают, убеждают сохранить звонок в тайне (напоминают об уголовной ответственности), переключают на разных сотрудников, не дают отключить телефон и закончить разговор.

Кроме того, якобы для защиты телефона мошенники просят установить приложение AnyDesk «удаленный рабочий стол» из Google Play или Apple Store, позволяющее получить удаленный доступ к телефону для последующего несанкционированного проникновения в дистанционный банковский сервис и перевода денежных средств клиента на счет мошенника после зачисления суммы полученного кредита.

В результате данной схемы клиенты сами получают кредиты для мошенников в разных банках.

Взаимодействие с «контрагентами»

Мошенникам становится известна информация о предстоящей коммерческой сделке между двумя организациями (для примера: одна организация – поставщик товара/услуг, вторая организация – приобретатель). Далее мошенники собирают дополнительные сведения о данной сделке и отслеживают статус оформления пакета документов по ней.

В период с момента завершения оформления сделки и до фактической отгрузки товара (получения услуг) мошенники от лица поставщика (используя его логотип, юридические реквизиты и т.д.) направляют приобретателю сообщение/письмо об отсутствии необходимого объема товара, но в то же время наличия необходимых объемов у другого «контрагента». Предлагается заключить 3-х сторонний договор или дополнительное соглашение к ранее заключенному договору с указанием новых реквизитов для перечисления денежных средств. После этого приобретателем по новым реквизитам перечисляются денежные средства третьему лицу (мошенникам). Если после перевода денежных средств приобретатель все еще не подозревает о мошеннической схеме, через некоторое время в его адрес могут поступать новые заманчивые предложения от «контрагентов» (для примера: возможность отгрузки дополнительной партии товара по сниженной цене).

Что должны сделать банки:

– Внедрить как можно больше вариантов аутентификации клиента и подтверждения платежа. Если клиент хочет иметь 10 независимых ключей, то пусть имеет. Если хоть один потеряет, то дальше ногами топает в банк. Позор банкам, которые позволяют поставить приложение и получить доступ к деньгам мошенникам, которые предварительно сменили телефон клиента в банке.

– Сделать их реально независимыми. Или часть из них. Должно быть по желанию клиента хотя бы три независимых ключа. Потерял любой из трёх — топай в банк.

– Запретить удалённо менять номер телефона или авторизировать перевыпущенную сим-карту. Можно не всем. Но хотя бы дать клиентам такую возможность повышенной безопасности.

– Внедрить системы уведомлений не только через СМС, а HTTP-уведомлений и писем на email. Если сим-карту или смартфон увели, то клиент уже не получит уведомление.

Самым распространенным способом мошенничества является социальная инженерия – методы обмана и введения клиентов в заблуждение с целью кражи денежных средств.

Список использованных источников:

1. https://www.sber-bank.by/page/fin_bezopastnost
2. https://habr.com/ru/post/348892/
3. https://pirit.biz/reshenija/informacionnaja-bezopasnost