УДК 004.9

ВОПРОСЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

© 2017 А. В. Маричев, И. В. Любимов, Ю. П. Преображенский

Воронежский институт высоких технологий

Аналитический обзор описывает общие и типовые риски информационной безопасности для современной компании. Необходимо постоянно заниматься тренингами, обучающими семинарами для персонала имитировать атаки злоумышленников, чтобы сотрудники уже автоматически реагировали на любые попытки социальных хакеров вторгнуться в информационную инфраструктуру компании. Обзор ориентирован на использование аспирантами или магистрами, занимающимися вопросами корпоративной информационной безопасности.

Ключевые слова: информационная безопасность, защита информации, компьютерные системы.

Любая современная организация, чем бы она ни занималась – юридическая фирма, торговое предприятие или образовательное учреждение, содержит весьма большую информационную инфраструктуру: серверы, рабочие станции, wifi-хотспоты, а иногда даже что-то более экзотическое, например, инфоматы, различные информационно-справочные точки доступа к корпоративной информации и т. д. Безусловно, каждый технологический прорыв, каждый новый гаджет в компании – это, прежде всего, восхищение новым витком развития информационных технологий, причем в этот момент почти никто не думает об информационной безопасности [1, 2]. Умные дома, Интернет вещей, корпоративное облако – эти достаточно новые для обычного человека термины и заставляют вспомнить фантастику, и позволяют в два-три нажатия на экран смартфона выключить свет в офисе, уточнить доставку корреспонденции или разослать всем сотрудникам push-уведомление о предстоящем совещании. Но насколько безопасно использование такого обилия технологий и устройств, каждое из которых – почти полнофункциональный компьютер с обилием программного обеспечения? Рассмотрим, какие потенциальные риски информационной безопасности существуют в современном офисе.

1. Незащищенное WiFi-подключение. В современном мире Интернет-подключение уже не стоит каких-то существенных денег, а безлимитный тарифный план воспринимается как само собой разумеющееся. Не считая крупных торговых центров и прочих openspace-мест, многие организации организуют бесплатное пользование беспроводной сетью, полагая, что это достаточно позитивно. Вместе с тем необходимо помнить, что злоумышленник может без особого труда перенаправить трафик в такой сети через свое устройство, и ваша учетная запись социальной сети или часть другой конфиденциальной информации совершенно незаметно попадет в ненадлежащие руки. Конечно, есть различные способы правильной настройки корпоративной сети, однако многие администраторы в силу лени или слабой квалификации игнорируют подобные рекомендации. Не следует использовать открытый доступ к WiFi ни для чего, кроме как для чтения новостей.

2. Хранение корпоративных секретов на мобильных носителях. Давно закончились времена, когда мобильный носитель формата «3,5» хранил в себе 1,5 мегабайта информации, что было однозначно меньше, чем корпоративная база данных или конфиденциальный проект. Сейчас на флэш-носитель в 128-256 Гб в два щелчка мышью можно уместить практически всю конфиденциальную информацию небольшой и даже средней компании, причем сотрудник может это сделать вполне себе неумышленно, просто «чтобы была». С одной стороны, тотальный запрет использования флэш-носителей (или даже USB-подключений в принципе) внутри компании может снизить данный риск, но

Маричев Артём Витальевич – ВИВТ АНОО ВО, магистр, marichev@vivt.ru.
Любимов Игорь Владимирович – ВИВТ АНОО ВО, системный администратор отдела информатизации и менеджмента качества, lyubimov@vivt.ru.
Преображенский Юрий Петрович – ВИВТ АНОО ВО, начальник отдела информатизации и менеджмента качества, к.т.н., профессор, it_pro@vivt.ru.

все отлично понимают, что это будет означать и для сотрудников, и для специалистов, обеспечивающих безопасность. Первые будут искать изощренные способы, как сбросить себе на флэш-карту важный проект, чтобы доделать его дома или просто создать его резервную копию «для себя» в обход корпоративных запретов, а вторые будут чувствовать на себе всеобщую ненависть и будут вынуждены постоянно проверять состояние операционной системы и компьютеров обычных пользователей. Подобная практика хотя и применяется в ряде компаний, распространения не получила в силу именно психологических препятствий. Как минимум необходимо объяснять сотрудникам, насколько велик риск раскрытия конфиденциальной информации в случае утери или кражи флэш-носителя, а также обязать всех пользоваться шифрованием информации на носителях, чтобы хоть немного уменьшить данный риск. И это все касается только добропорядочных сотрудников организации, если же говорить о так называемых «инсайдерах», то для них использование сменных носителей – 100 % гарантия успеха кражи корпоративных секретов и говорить о борьбе с ними надо в отдельной статье.

3. Использование Интернета сотрудниками. Как ни парадоксально, но жизнь современного офиса почти невозможно представить без Интернета на рабочих местах, вместе с тем достаточно щелкнуть на присланный файл и запустить его, чтобы червь-шифровальщик уничтожил всю работу за длительное время, попутно вымогая деньги за ключ для расшифровки данных. Просто говорить сотрудникам: «Не открывайте ничего из почты», почти бессмысленно, рано или поздно найдется человек, который забудет или отвлечется на что-то в момент открывания письма. Необходимы жесткие (или даже жестокие) тренинги, необходимы постоянные разъяснения, насколько опасно открывать письма, которых вы не ожидаете, либо содержание письма не имеет отношение к корпоративной работе (вызов в суд, о котором вы ничего не слышали, уведомление о заказе, который вы видите впервые, сообщение о просроченном кредит от банка, с которым у вас нет никаких отношений и т. д.).

4. Слабые пароли. Безусловно проще ввести пароль «qwerty» или «123», нежели «QF0op5TYb», но в том случае, если сотрудникам предоставлена возможность самим выбирать себе пароль, львиная доля пользователей выберет либо примитивный пароль из рядом стоящих букв или цифр, либо социально-ориентированный пароль: дату, телефон, имя ребенка, никнейм, кличку кошки и т. д. Бессмысленно ждать от сотрудников ввода действительно стойкого пароля, каждый из них рассуждает: «Меня это не коснется, я никому не нужен, про мой простой пароль никто не догадается». Поэтому первой практикой должна стать дисциплина паролей, выдаваемых администратором. Но в этом случае немедленно возникает другая опасность – пользователи записывают пароли на клочки бумаги и раскладывают их на рабочем месте. Авторы статьи многократно находили ключевые пары под клавиатурами или даже прикрепленными скотчем к монитору. Борьба с данным риском также одна из самых тяжелых испытаний для специалиста в области корпоративной безопасности.

5. И наконец, подробно рассмотрим вопросы социальной инженерии в корпоративной среде. Любая корпоративная информационная инфраструктура состоит из двух компонентов – люди и оборудование. Как известно, любой аппаратный компонент может выйти из строя, любая программа может однажды засбоить, но все равно самое слабое звено в любой системе – человек. Психология сотрудников любой компании – потенциальная мишень для злоумышленника, владеющего навыками и методиками социальной инженерии. Практически все они основаны на речевом или аудиовизуальном воздействии на жертву: телефонный звонок, письмо по электронной почте, либо подложные изображения с одновременным разговором по Skype и т. п.

Большая часть атак на базе социальной инженерии происходит по телефону или посредством электронной почты. Маловероятен приход злоумышленника в офис лично, тогда как отправить электронное письмо или позвонить начинающему специалисту с предложением, просьбой или вопросом – элементарно и ничего не стоит злоумышленнику. Либо жертву обманом вынуждают продиктовать закрытую информацию (например, логин/пароль или закрытый IP-адрес для корпоративной сети), либо выполнить некоторые действия, если злоумышленник выдает себя за ИТ-сотрудника той же компании. Поскольку социальной инженерии подвластны и молодые, и крайне опытные сотрудники (вопрос только в подходе и степени заинтересованности зло-

умышленника), необходимы постоянные тренировки и внутренний аудит безопасности с достаточно жесткими последствиями для нарушителей. Главное, конечно, не переусердствовать и не превратить сотрудников в озлобленных параноиков, но только таким образом можно хоть немного уменьшить данный риск.

Когнитивность человеческого разума позволяет злоумышленнику немного «помочь» жертве с принятием решений в виде ввода ключевых слов, произнесения вслух конфиденциальной информации, вплоть до нажатия на кнопку выключения какого-то устройства. Уговоры, нагнетание психологического напряжения, прямой обман – все это типовые инструменты социального хакера. Рассмотрим базовые приемы, которыми пользуются злоумышленники для воздействия на пользователей.

Один из самых основных методов – претекстинг, т.е. жертву ведут по заранее сформированному сценарию, различия только в подходе к психологии. Либо третье лицо будет просить о помощи, либо, представляясь сотрудником спецслужб, будет угрожать уголовным преследованием за некие действия, либо наоборот, мошенник будет представляться штатным инженером и предлагать помощь в решении проблем в работе компьютера на рабочем месте сотрудника. Одним из важных моментов в данном случае – упоминание имени и фамилии сотрудника, которому происходит звонок, а также упоминание реальных сотрудников компании, особенно, если эти сотрудники являются начальниками по отношению к жертве. К сожалению принципы информационной открытости современных компаний, часть из которых вообще является федеральными требованиями по размещению на сайте определенной части персональных данных, на несколько порядков упрощают для злоумышленника проведения атаки претекстингом. Достаточно изучить сайт компании, и вот мошенник уже отлично оперирует реальными именами, телефонами, должностями, ссылается на реально происходившие в прошлом события и т. д. Непонимание огромной опасности такой атаки – это дамоклов меч для организации.

Очень часто злоумышленники пользуются фишингом для перенаправления сотрудников на поддельные сайты или для "выуживания» (отсюда – fishing) конфиденциальной информации из работника, который всего лишь, на его взгляд, общается с службой технической поддержки, например, банка, который его обслуживает. Наивно полагать, что атака будет направлена против конкретно взятого сотрудника, не попадется один – попадется другой. Практически всегда фишинговая атака предполагает, что сотрудник сообщает человеку, которого он не знает лично и не видит, секретную информацию. Фишинг практически невозможен при личном общении, тогда как голос по телефону или текст электронного письма, содержащего официальный логотип компании, может быть крайне убедителен. Письмо с уведомлением о том, что вы выиграли в лотерею, на ваше имя выпущена золотая карта Visa или вам предоставлена 50% скидка на покупку товаров известного бренда – все это однозначно провоцирует человека на звонок по указанному в письме телефону, что уже запускает механизм мошенничества.

Огромная часть конфиденциальной информации утекает просто при взгляде постороннего человека через плечо сотрудника, особенно часто это происходит в офисах, где клиент априори видит монитор и клавиатуру менеджера. Запрос пароля на экране в огромном числе случаев провоцирует клиента проследить глазами за пальцами сотрудника, все, поле для мошенничества открыто.

Также очень популярен метод, при котором у жертвы удаляется (прячется) достаточно важная информация, причем при попытке восстановления этой информации сотрудник сам с готовностью и большим усердием сообщит звонящему ему «инженеру техподдержки» и свой пароль, и ключевые слова, и местонахождение многой другой конфиденциальной информации, ведь сейчас его основная задача – восстановить файлы. В комплексе с претекстингом – это страшный коктейль социальной инженерии.

Следующим крайне опасным методом является принцип «дорожного яблока». Социальный хакер подбрасывает в места публичного пользования внутри корпоративного периметра флэш-карту, которая содержит исполняемый файл с провоцирующем названием. Во-первых, необходимо помнить, что достаточно просто воткнуть флэш-носитель в компьютер, чтобы состоялся акт вторжения в корпоративную среду, например, при способе инфицирования BadUSB, который уже многократно описан и даже частично реализован. Если же клиент поддастся искушению и запустит программу с

флэш-носителя – можно считать атаку полностью удачной.

Идеология социальной инженерии позволяет проникнуть внутрь системы, не обладая никакими техническими навыками, даже не обладая компьютером и не зная языков программирования, именно это делает ее настолько популярной у современных мошенников. Выманить у одного пользователя ключ и пароль, у другого – лицевой счет, у третьего – необходимую для перевода денежных средств информацию... злоумышленник даже не знает, где эта компания находится, все происходит через Интернет и с помощью телефона или Skype.

Каждая современная компания должна заниматься профилактикой атак методами социальной инженерии среди своих сотрудников. Необходимо постоянно заниматься тренингами, обучающими семинарами для персонала имитировать атаки злоумышленников, чтобы сотрудники уже автоматически реагировали на любые попытки социальных хакеров вторгнуться в информационную инфраструктуру компании.

ЛИТЕРАТУРА

1. Львович И. Я. Факторы угрозы экономической безопасности государства // И. Я. Львович, А. А. Воронов, Ю. П. Преображенский // Информация и безопасность. – 2006. – Т. 9. – № 1. – С. 36-39.

2. Воронов А. А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности // А. А. Воронов, И. Я. Львович, Ю. П. Преображенский, В. А. Воронов // Информация и безопасность. – 2006. – Т. 9. – № 2. – С.8-11.

THE ISSUES OF SOCIAL ENGINEERING IN CORPORATE INFORMATION SECURITY

© A. V. Marichev, I. V. Lyubimov, Yu. P. Preobrazhenskiy

Voronezh Institute of High Technologies

The analytical review describes the common and typical risks of information security for modern companies. You need to constantly engage in trainings, educational workshops for personnel to simulate attacks so that employees have automatically reacted to any attempt by social hackers to invade in the information infrastructure of the company. The review focuses on the use of graduate students or masters, involved in corporate information security.

Keywords: information security, information protection, computer system.