УДК 004.58 / 316.776

ПОЛИТИКА ПРОТИВОДЕЙСТВИЯ АТАКАМ, СОВЕРШЁННЫМ С ИСПОЛЬЗОВАНИЕМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В КОРПОРАТИВНОЙ СРЕДЕ

Потапова К.А.

МИРЭА – Российский технологический университет, 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail: ksurashanti@gmail.com

Человеческий фактор в данный момент в мире играет огромную роль. Большинство компаний пытаются решить проблему с помощью аппаратных и программных средств, однако этих способов уже недостаточно. В статье рассмотрены методы, применяемые отделом информационной безопасности при противодействии атакам на компанию, в том числе атакам с использованием методов социальной инженерии. Определено место человеческого фактора в мероприятиях по защите информации и превентивным мерам противодействия, таким как обучение сотрудников и проведение тренингов.

Ключевые слова: социальная инженерия, корпоративные стандарты, финансовые системы, информационная безопасность, тренинги по информационной безопасности

POLICY FOR COUNTERING ATTACKS USED USING SOCIAL ENGINEERING IN THE CORPORATE ENVIRONMENT

Potapova K.A.

MIREA - Russian Technological University, 119454, Russia, Moscow, Vernadsky prospect, 78, e-mail: ksurashanti@gmail.com

The human factor plays a huge role in the world at the moment. Most companies try to solve the problem with hardware and software, but these methods are no longer enough. The article discusses the methods used by the information security department in countering attacks on a company, including attacks using social engineering methods. The place of the human factor in measures to protect information and preventive countermeasures, such as employee training and training, has been determined.

Keywords: social engineering, corporate standards, financial systems, information security, information security trainings.

1. Введение

Корпоративная политика в сфере противодействия информационным атакам многогранна и подразумевает полный комплекс мер, обеспечивающих наибольшую безопасность информации, персональных данных клиентов и сохранность внутренней информации компании [3].

Злоумышленники используют разные подходы для кражи информации. Конечная задача хакера состоит в том, чтобы при помощи взлома компьютерной системы получить доступ к конфиденциальной информации. Один из самых эффективных способов на сегодняшний день — методы социальной инженерии. Также хакеры используют технический метод, когда воздействие производится непосредственно на технику. Не меньшей популярностью пользуется комбинация методов: технического взлома системы и психологического воздействия на сотрудника компании. Популярность использования социальной инженерии при краже данных обусловлена экономическим фактором, так как этот способ не требует серьёзного знания компьютерных технологий и финансовых вложений.

Социальная инженерия – метод несанкционированного доступа к информационным ресурсам, основанный на особенностях психологии человека, где жертвой является не компьютер пользователя, а сам пользователь.

За последние десятилетия значительно усовершенствовались технические методы защиты информации. Было доработано программное обеспечение, которое обеспечивает защиту баз данных и другой информации от неправомерного доступа, обеспечена возможность резервного копирования и хранение наиболее важных данных, была доработана возможность перераспределения ресурсов сети в случае аварии и обеспечено повсеместное разграничение прав доступа к конфиденциальной информации. В то же время, конечно, повышалась и

техническая грамотность пользователей, однако человеческий фактор продолжает оставаться слабым звеном в системе благодаря недостаточному вниманию специалистов по информационной безопасности к уязвимости человеческой психики.

Всё разнообразие атак социальных инженеров можно изобразить на достаточно простой схеме. Она показана на рисунке 1.

Сначала всегда формулируется основная цель воздействия на объект. Чаще всего целью является получение денежной прибыли. Это происходит либо через банковские приложения атакуемого, либо через продажу конфиденциальной информации компании после взлома информационной сети компании с помощью введения в заблуждения жертвы.

После этого наступает этап сбора средств информации о жертве, поиски уязвимостей и слабых мест. Начальные сведения помогут ближе изучить цель и понять, с чем вы имеете дело. Подойдут активные и пассивные методы по методологии разведки на основе открытых источников. К открытым источникам относятся СМИ, публикации в интернете, общедоступные данные аэросъемок и радиомониторинга, публичные отчеты государственных и коммерческих организаций, профессиональные отчеты, конференции, доклады [3].

К примеру, последние годы распространена практика телефонного мошенничества: мошенник просит перевести ему деньги, обманом заставляя поверить в то, что близкий человек жертвы в беде. Этот метод могут применять и к краже корпоративной информации, спрашивая вместо паролей доступа к банковскому приложению данные для доступа к корпоративному ресурсу.

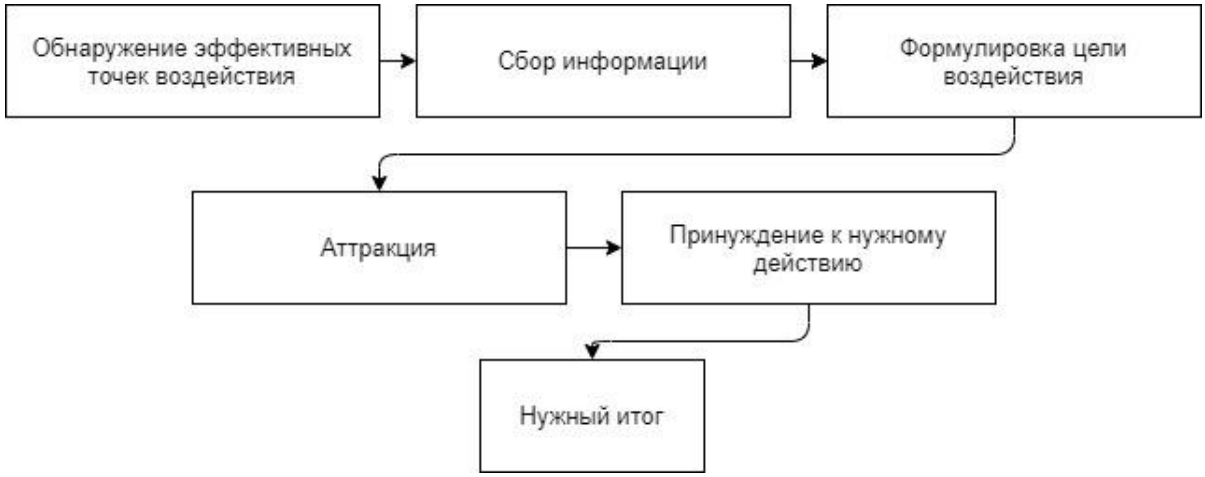

Рисунок 1. Общая схема атаки

Аттракция – это создание нужных условий для воздействия на человека, то есть привлечение его внимания. Лишь после успешного проведения аттракции мошенник может побудить жертву к нужному ему действию.

На рисунке 2 показана распространённая схема мошенничества: злоумышленник размещает поддельную страницу аутентификации, сотрудник компании вводит данные, после чего злоумышленник получает доступ к учётным данным сотрудника.

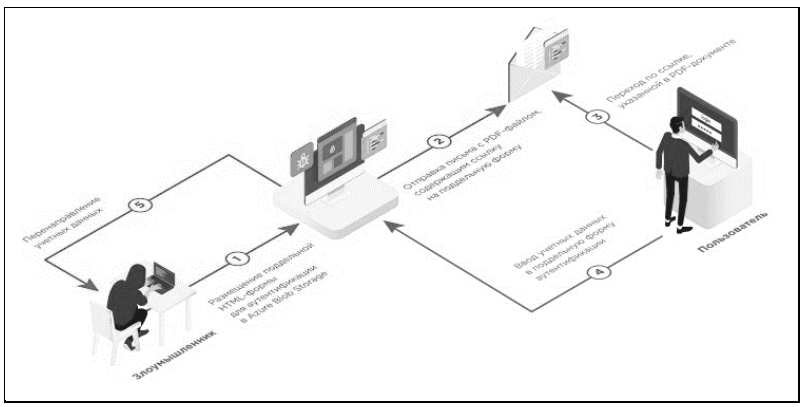

Рисунок 2. Атака социального инженера при помощи поддельной страницы

Другой популярный метод атаки использует речевые терминалы: телефон, VoIP-клиент, микрофоны. Принцип действия IVR-платформ представлен на рисунке 3.

С их помощью также могут быть украдены персональные данные, причём как у сотрудников компании, так и у клиентов компании. Наибольшей угрозе подвергаются деньги клиентов банков, так как при использовании определённой связки информации можно попасть в банковское приложение клиента и вывести средства. Поэтому корпорации в том числе должны использовать методы защиты своих клиентов, а не только внутренних данных компании.

В социальной инженерии есть несколько техник, используемых для достижения поставленных задач. Все они основаны на ошибках, допускаемых человеком в поведении [6].

Претекстинг – злоумышленником искусственно создаётся сценарий, который побуждает жертву совершить якобы правильное действие, например, рассказать мошеннику конфиденциальную информацию.

Фишинг – самый распространенный метод атак, проводимых с целью получения доступа к конфиденциальным данным – логина и пароля. Частными случаями фишинга являются ложные веб-сайты, интерфейс которых неотличим от оригинальным, на которых пользователь вводит пароль от оригинального сайта при недостаточной бдительности. В настоящий момент информационная безопасность шагнула очень далеко вперед, как и разработчики поисковых систем. Поэтому большинство сервисов умеют определять фишинговые письма (они отправляют их в спам) и вредоносные сайты [1].

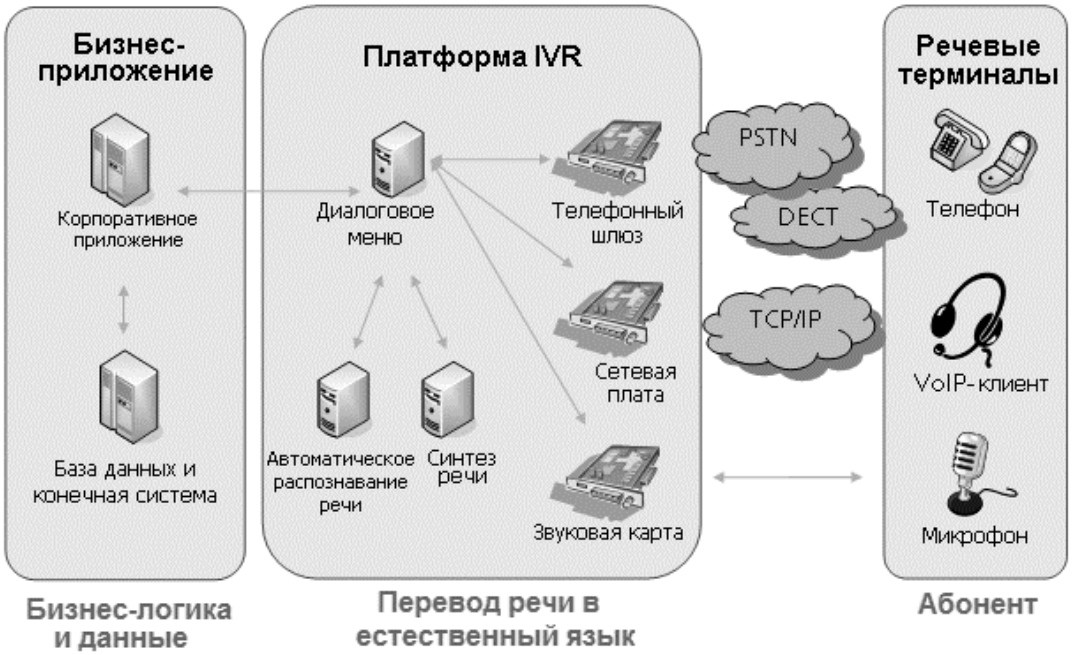

Рисунок 3. Принцип действия IVR систем

Дорожное яблоко – аналог троянского коня, заключается в том, что злоумышленник подбрасывает физический носитель, например, карту памяти, снабжённую привлекательной для жертвы надписью, что побудит жертву ею воспользоваться.

Плечевой серфинг – подсматривание информации из-за плеча жертвы.

Сбор информации из открытых источников – этот метод требует не только знания человеской психологии, но и способность обрабатывать большие потоки информации. Чаще всего информацию о сотрудниках собирают в открытых социальных сетях.

Квид про кво – услуга за услугу. Эта атака подразумевает общение сотрудника с мошенником по телефону или электронной почте, в процессе которого мошенник сообщает о какой-то возникшей проблеме, и просит пользователя помочь её решить.

2. Основные методы защиты

Рассмотрим основные рекомендуемые методы защиты. Защита компании должна производится на всех возможных уровнях. В первую очередь обратим внимание на базовые средства защиты информации [4].

Это незаменимый компонент обеспечения информационной безопасности компании. К ним относятся многочисленные антивирусные программы, а также системы фильтрации электронной почты, защищающие пользователя от нежелательной или подозрительной корреспонденции. Корпоративные почтовые ящики обязательно должны быть оборудованы такими системами. Кроме того, необходима организация дифференцированного доступа к информации и систематическая смена паролей [4].

Грамотная защита от DDoS-атак собственными силами невозможна. Многие разработчики программного обеспечения предлагают услугу анти-DDoS, которая способна защитить от подобных нападений. Как только в системе обнаруживается трафик необычного типа или качества, активируется система защиты, выявляющая и блокирующая вредный трафик.

При этом бизнес-трафик поступает беспрепятственно. Система способна срабатывать неограниченное количество раз, до тех пор, пока угроза не будет полностью устранена [4].

Шифрование данных при передаче информации в электронном формате. Чтобы обеспечить конфиденциальность информации при её передаче в электронном формате применяются различные виды шифрования. Шифрование дает возможность подтвердить подлинность передаваемой информации, защитить ее при хранении на открытых носителях, защитить ПО и другие информационные ресурсы компании от несанкционированного копирования и использования [4].

В комплекс технических мер входят и меры по обеспечению физической недоступности объектов компьютерных сетей, например, такие практические способы, как оборудование помещения камерами и сигнализацией [7].

2.1 Тренинги по обеспечению информационной безопасности

Слабым элементом, несмотря на непрерывное усовершенствование технических средств защиты компании, является человек. Именно человеческий фактор служит основной угрозой безопасности персональных данных клиентов компании и распространения внутренней информации о компании.

Во-первых, часто значительная часть сотрудников недостаточна обучена и поэтому невольно способствует краже информации. Во-вторых, достаточно часто само предприятие недостаточно заботится о знаниях своих сотрудников о возможных атаках социальных инженеров, отдавая всё внимание защите физической: например, охрана на входе в здании; и технической: обеспечение обновления антивирусных программ или разграничение прав доступа к информации.

Чаще всего атаки социальных инженеров направлены на работников с наивысшим доступом к работе с конфиденциальной информацией. Однако значительный ущерб компании может навредить и атака на любого работника, так как часто злоумышленники оценивают в том числе потенциальные личные знания цели.

Поэтому, каждый сотрудник компании должен быть проинформирован и проинструктирован, что делать в случае опасности утечки информации или атаки социального инженера. Для этого в компании регулярно должны проводится тренинги сотрудников по обеспечению информационной безопасности. Многие незаслуженно пренебрегают этим методом, тем не менее, он является самым простым и эффективным. Рассмотрим основные рекомендации к обучению:

1. Обучение должен проводить квалифицированный сотрудник отдела информационной безопасности. При недостаточной квалификации преподавателя сотрудники не смогут получить ответы на все интересующие их вопросы, а также сам преподаватель не сможет в достаточной мере акцентировать внимание на важности рассматриваемой проблемы. Также недостаточная акцентуация может произойти в том числе из-за отсутствия личного опыта обучающего сотрудника.
2. Должны быть рассмотрены основные методы атак социальных инженеров на сотрудников компании, такие как плечевой серфинг, претекстинг, фишинг, услуга за услугу, дорожное яблоко и обратная социальная инженерия. Особое внимание сейчас следует уделять плечевому серфингу. Этот метод атаки подразумевает наблюдение за экраном компьютера жертвы в общественных местах. После роста популярности удалённой работы во время пандемии COVID-19, сотрудники часто предпочитают работать в общественных местах, в том числе в кафе и общественном транспорте. Необходимо донести до сотрудников недопустимость работы в общественных местах, если они не уверены, что смогут в должной степени обеспечить безопасность конфиденциальных данных компании.
3. В презентацию обязательно нужно включить меры наказания уголовного кодекса, которые могут последовать за убытки компании по халатности сотрудника. К сожалению, без этой части многие люди не поймут значимость и важность защиты конфиденциальной информации, а также личную ответственность за утечку, последовавшую вследствие их личной невнимательности или халатности.
4. Особое внимание должно быть уделено работе отдела безопасности и быстрого способа связи между сотрудником и отделом. В случае подозрения на любую угрозу сотрудник обязан оперативно сообщить о

потенциальной утечке или угрозе в отдел информационной безопасности. Во-первых, это поможет сотрудникам отдела информационной безопасности оперативно отреагировать на угрозу и как можно раньше принять меры по противодействию атаке. Во-вторых, сотрудник отдела информационной безопасности сможет правильно проинструктировать о дальнейших действиях атакованного сотрудника компании, в том числе оказать последнему психологическую поддержку.

5. После тренингов могут быть проведены пробные атаки изнутри компании, чтобы понять уровень осведомлённости сотрудника. В случае необходимости нужно провести разъясняющую беседу ещё раз.

В ходе обучения рекомендуется в общих чертах донести до сотрудника, чем именно занимается отдел информационной безопасности, так как это повысит доверие внутри компании и обеспечит личную заинтересованность сотрудников в борьбе с мошенниками, использующими методы социальной инженерии.

2.2 Рекомендации по оформлению презентации для обучения сотрудников компаний

Особое внимание должно быть уделено визуальной составляющей презентации. Восприятие речи лучше, если оно подкреплено рисунками и графиками. Важно продублировать главные тезисы на экране.

Ниже перечислены основные рекомендации по оформлению презентации для лекции по информационной безопасности:

1. Хорошо структурированная презентация, в том числе: главный слайд, цели и задачи, основная часть и выводы.
2. Необходимо использовать минимальное пространство слайда. Например, использовать рисунки или акцентировать внимание на заголовке и подпунктах.
3. Дизайн презентации должен быть простым и лаконичным.
4. Каждый слайд должен иметь заголовок.
5. Подведение итогов: кратко рассмотреть все основные положения.

3. Служба информационной безопасности

Служба информационной безопасности - организационно-техническая структура системы обеспечения информационной безопасности, реализующая решение определенной задачи, направленной на противодействие той или иной угрозе информационной безопасности [2].

Сотрудникам отдела информационной безопасности необходимо следить за обеспечением физических средств защиты информации. Это ограничение или полный запрет доступа посторонних лиц на территорию, пропускные пункты, оснащенные специальными системами. Большое распространение получили HID-карты для контроля доступа. Например, при внедрении этой системы, пройти в серверную или другое важное подразделение компании могут лишь те, кому такой доступ предоставлен по протоколу [2].

Сотрудники должны следить за программным обеспечением на компьютере пользователей. Самостоятельно устанавливать и обновлять антивирусные программы. Настраивать фильтрацию электронной почты от нежелательных и подозрительных писем.

Именно отдел информационной безопасности должен понимать, как работает вся структура компании, и каким сотрудникам требуется доступ к полному объёму информации, а каким можно ограничить доступ, в связи с узким полем деятельности.

Нужно настроить рекомендации к паролям и настаивать на регулярной смене пароля раз в несколько месяцев. Например, сделать принудительную смену пароля для доступа в корпоративную сеть, при игнорировании предупреждения пользователь потеряет доступ к данным компании, пока не поменяет пароль на новый, отвечающий всем требованиям отдела информационной безопасности. Это должно быть зафиксировано в нормативных и распорядительных документах, действующих в границах организации.

В отделе должны проводится исследования технологий обработки информации с целью выявления каналов утечки данных и других угроз безопасности информации, формирование модели угроз, разработка политики в сфере информационной безопасности [5].

Состав и численность отдела зависит от размера компании, сферы деятельности, уровня конфиденциальности информации. Численность и состав Службы информационной безопасности должны быть достаточными для выполнения всех задач безопасности и защиты информации [5].

Состав и численность отдела зависит от размера компании, сферы деятельности, уровня конфиденциальности информации. Численность и состав Службы информационной безопасности должны быть достаточными для выполнения всех задач безопасности и защиты информации [5].

4. Заключение

Обучение всегда ведётся на основе корпоративных стандартов компании. В ходе обучения должны быть рассмотрены ситуации, имитирующие атаки и последствия поведения сотрудников в кризисных ситуациях.

Приведена стратегия работы службы информационной безопасности: перечислены основные задачи, а также методы их решения, в том числе необходимость принудительного разграничения прав доступа и регулярная смена пароля всеми сотрудниками компании, независимо от их уровня доступа внутри компании. Необходимо регулярно обновлять программное обеспечение на компьютерах всех сотрудников, а также необходимо регулярно заниматься подготовкой и проводить тренинги по информационной безопасности как для новых сотрудников, так и донесение новых способов атак социальных инженеров и усовершенствования старых методов защиты до остальных сотрудников компании.

Список литературы

1. Артёмов Н., Социальная инженерия – технология «взлома» человека // Медиум: сетевой журнал. 2017 г. URL: https://medium.com/@Emisare/socialnaya-ingeneria-9f16e0ba7fa5 (дата обращения 27.01.2021)
2. ГОСТ 45.127-99. Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. 1999 г. URL: https://meganorm.ru/Index2/1/4293855/4293855564.htm (дата обращения 13.12.2020)
3. Мельников Е. Как понизить роль социальной инженерии в угрозе проникновения // itglobal.com – сетевое издание. 2019 г. URL: https://itglobal.com/ru-ru/company/blog/kak-ponizit-rol-soczialnoj-inzhenerii-v-ugroze-proniknoveniya/
4. Информационная безопасность предприятия: ключевые угрозы и средства защиты // Сетевое издание Комсомольская Правда. 2017 г. URL: https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html (дата обращения 13.12.2020)
5. Служба информационной безопасности // Википедия. 2021 г. URL: https://ru.wikipedia.org/wiki/Служба_информационной_безопасности (дата обращения 25.01.2021)
6. Социальная инженерия // Anti-malvare – сетевой журнал. 2021 г. URL: https://www.anti-malware.ru/threats/social-engineering (дата обращения 20.03.2021)
7. Способы защиты информации // searchinform – сетевой журнал. 2021 г. URL: https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/sposoby-zaschity-informatsii/ (дата обращения 03.03.2021)

Reference

1. Artyomov N., Social'naya inzheneriya – tekhnologiya «vzloma» cheloveka // Medium: setevoj zhurnal. 2017 g. URL: https://medium.com/@Emisare/socialnaya-ingeneria-9f16e0ba7fa5 (data obrashcheniya 27.01.2021)
2. GOCT 45.127-99. Sistema obespecheniya informacionnoj bezopasnosti vzaimouvyazannoj seti svyazi Rossijskoj Federacii. 1999 g. URL: https://meganorm.ru/Index2/1/4293855/4293855564.htm (data obrashcheniya 13.12.2020)
3. Mel'nikov E. Kak ponizit' rol' social'noj inzhenerii v ugroze proniknoveniya // itglobal.com – setevoe izdanie. 2019 g. URL: https://itglobal.com/ru-ru/company/blog/kak-ponizit-rol-soczialnoj-inzhenerii-v-ugroze-proniknoveniya/
4. Informacionnaya bezopasnost' predpriyatiya: klyuchevye ugrozy i sredstva zashchity // Setevoe izdanie Komsomol'skaya Pravda. 2017 g. URL: https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html (data obrashcheniya 13.12.2020)
5. Sluzhba informacionnoj bezopasnosti // Vikipediya. 2021 g. URL: https://ru.wikipedia.org/wiki/Sluzhba_informacionnoj_bezopasnosti (data obrashcheniya 25.01.2021)
6. Social'naya inzheneriya // Anti-malvare – setevoj zhurnal. 2021 g. URL: https://www.anti-malware.ru/threats/social-engineering (data obrashcheniya 20.03.2021)
7. Sposoby zashchity informacii // searchinform – setevoj zhurnal. 2021 g. URL: https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/sposoby-zaschity-informatsii/ (data obrashcheniya 03.03.2021)