Лекция 13. Социальная инженерия. Цифровая криминалистика.

Цель лекции: познакомиться с понятием социальной инженерии и с основными приемами социальной инженерии; рассмотреть пути защиты компаний от социальной инженерии и цифровую криминалистику.

План лекции:

1. Понятие социальной инженерии
2. Основные приемы социальной инженерии
3. Как защитить компанию от социальной инженерии
4. Цифровая криминалистика

Социальная инженерия (англ. social engineering) - это один из разделов социальной психологии, направленный на то, чтобы внедрять в человеческое сознание некоторую модель поведения и тем самым манипулировать человеческими поступками.

В social engineering все строится вокруг слабостей человека.

С одной стороны, это личностные качества: сопереживание, наивность, доверчивость, лояльность к чужим слабостям, страх.

С другой — качества профессиональные: недостаток знаний, неумение применять их на практике, игнорирование инструкций и должностных обязанностей.

Ежегодный ущерб от киберпреступников, которые используют приемы социальной инженерии, оценивается в десятки миллиардов долларов США.

Одним из самых первых громких дел с применением social engineering'а стало дело **Кевина Митника**. Его начинания продолжили другие: Братья Бадир, хакер по имени Архангел, Питер Фостер. Некоторые истории легли в основу сценариев для художественных фильмов — например, кинолента «Поймай меня, если сможешь» с Леонардо ди Каприо в главной роли основана на реальных фактах.

Основные приемы социальной инженерии

Фишинг. Это сбор пользовательских данных для авторизации (логинов и паролей) в различных онлайн-сервисах. Фишинг популярен, о нем многие знают, но, тем не менее, попадаются на его «удочку». Обычно он представляет собой массовые рассылки спама по электронной почте. Потенциальным жертвам приходят письма якобы от сервисов, которыми они пользуются: платежных систем, онлайн-магазинов и т. п. Эти письма — поддельные, их задача в том, чтобы заставить пользователя перейти по ссылке или кнопке, а затем оставить мошенникам авторизационные данные. Чтобы вызвать больше

доверия, мошенники придумывают серьезные причины для перехода по ссылке: например, просят жертву обновить пароль или подтвердить какое-то действие в системе.

Претекстинг. Методика психологической манипуляции по заранее подготовленному сценарию. Сценарий реализуется во время голосового общения, в ходе которого жертва сообщает киберпреступнику нужную ему информацию или выполняет действие, которое приведет его к желанной цели. Часто социальные инженеры представляют сотрудниками банков, кредитных сервисов, техподдержки или других служб, которым человек по умолчанию доверяет. Для большей достоверности они сообщают потенциальной жертве какую-либо информацию о ней: имя, номер банковского счета, реальную проблему, с которой она обращалась в эту службу ранее.

Плечевой серфинг. Проще говоря, это подглядывание из-за спины. Так легко получить пароли и логины для входа в местах общественного пользования: кафе и ресторанах, парках и залах ожидания в аэропорту или на вокзале.

Сбор данных из открытых источников. Это не только соцсети (хотя сегодня они особенно актуальны), но и информация в поисковых системах, блогах, на форумах, в профессиональных сообществах и сообществах по интересам, на сайтах с частными объявлениями, на офлайн-мероприятиях: конференциях, докладах, мастер-классах.

«Кви про кво». Второе название — «услуга за услугу». Эта техника атаки предполагает общение по электронной почте или телефону. Мошенник представляется сотрудником, например, техподдержки, и предлагает жертве помочь ему устранить определенные неполадки в онлайн-системе или на рабочем месте. Жертва, выполняя его указания, лично передает ему средства доступа к важной информации.

Троянский конь/дорожное яблоко. Метод предполагает подбрасывание «приманки», которая с высокой вероятностью заинтересует потенциальную жертву. Такой приманкой обычно становится носитель информации — например, флеш-карта, CD-диск или карта памяти к телефону. Жертве станет любопытно, что находится на носителе, она вставит их в ноутбук или телефон, а мошенник с помощью специальной программы получит доступ к информации. Приманкой может быть и email-сообщение, которое сулит получение быстрой прибыли, выигрыша, наследства и других вещей, которые точно заинтересуют многих получателей письма и заставят выполнить содержащиеся в нем инструкции.

Обратная социальная инженерия. Методика направлена на то, чтобы жертва сама обратилась к социальному инженеру и выдала ему необходимые сведения. В этой ситуации мошенники часто прибегают к диверсиям: подстраивают поломку компьютера, проблемы с авторизацией и делают так, чтобы сотрудник попросил их помочь с устранением проблемы.

Что такое социальная инженерия, уже понятно по перечисленным методам. Но это далеко не все, чем пользуются кибермошенники. В мире популярен мобильный банкинг, и социальные инженеры применяют свои знания, чтобы получить доступ к карточным счетам жертвы. Так выделилось отдельное направление, которое называют кардингом. За этим определением скрываются махинации с банковскими картами. Если раньше использовались физические способы получения информации (специальные устройства считывали пароли прямо на терминалах), то теперь это проще сделать с помощью методов социальной инженерии, психологическими приемами заставляя жертву раскрыть номер карты, срок ее действия, CVV-код и получить полный контроль над банковским счетом.

Мошенники активно пользуются социальными сетями, в которых пользователи делятся событиями из личной жизни и увлечениями. Чтобы получить доступ к аккаунту (любому, не только в соцсети), хакеры изучают страницу потенциальной жертвы: когда и где она родилась и живет, кто ее родители, ее хобби, какие мероприятия посещает, с кем дружит. Взломав профиль друга жертвы, легко будет установить с ней контакт и получить нужные сведения, прикрываясь благими намерениями.

Еще один инструмент социальных инженеров — СМС-рассылки. В них обычно сообщают о выигранных автомобилях и крупных суммах, об угрозе немедленной блокировки банковской карты и попавших в беду родственниках. Человек, у которого таким способом вызвали интерес, сочувствие или страх, способен на многое, в том числе поделиться секретной информацией, не подозревая, что передает ее в руки мошенников.

Методы работы социальных инженеров

Опытный социальный инженер редко использует одну технику сбора данных. Обычно методы социальной инженерии — это комплекс инструментов, которые применяются в зависимости от обстоятельств. Он:

- представляется сотрудником сервисных служб, проверяющим или руководителем;
- подглядывает из-за плеча, чтобы узнать логин и пароль;
- отправляет фишинговые электронные письма и сообщения в мессенджеры;

- тайно записывает нажатия клавиш, пока жертва работает за компьютером;
- записывает голосовые сообщения, похожие на сообщения роботов;
- просит о помощи, где жертва раскроет важны данные.

Атака методами социальной инженерии

Сбор информации о потенциальном объекте. Чтобы эффективно применить методы социальной инженерии, нужно знать, с чем и кем имеет дело кибермошенник. В компании преступника может заинтересовать количество сотрудников, графики их работы, перемещения, страхи, конфликты на рабочем месте и другое, что делает их уязвимыми.

Выбор жертвы и сбор данных о ней. Наибольший интерес представляют данные для авторизации, аккаунты в социальных сетях, сообщения на форумах, в чатах, сведения о перемещении, личный адрес, связи с другими людьми (родственниками, коллегами, друзьями), общедоступная информация из поисковых сервисов.

Информационная атака. Получение физического или онлайн-доступа к ценной информации, сбор базы логинов/паролей, документы или другая цель, которую преследует кибермошенник. Атака осуществляется после контакта мошенника с жертвой. Установить контакт можно разными способами: в реальном или телефонном разговоре, онлайн (отправив письмо на e-mail или написав в соцсети).

Использование полученных данных. Информацию, которая попала в руки киберпреступнику, можно использовать для доступа к банковскому счету, чтобы скомпрометировать компанию, попросить выкуп за возврат доступа или нераспространение украденного.

Что такое тест на проникновение. Когда упоминается социальная инженерия, определение ее предполагает, что по ту сторону от жертвы всегда стоит кибермошенник. Это не так. Сегодня инструменты социального инжиниринга используются для повышения информационной безопасности предприятия через тесты на проникновение.

Специалисты, которые занимаются тестированием на проникновение, точно также используют психологические и социологические приемы для получения ценной корпоративной информации. Но их цель — закрыть слабые места, выявить пробелы в знаниях сотрудников и повысить сознательность там, где речь идет о конфиденциальных данных и способах обращения с ними.

Как защитить компанию от социальной инженерии

Так как самым уязвимым элементов в системе безопасности остается человек, мероприятия по защите будут затрагивать именно его. Исключением

будет установка последних обновлений для антивирусных приложений и надежного брандмауэра на рабочие машины сотрудников.

Инструкции по работе с информацией

Информация, с которой работает сотрудник, является собственностью компании. То же касается авторизационных данных в корпоративных системах. Некоторые компании уже перешли на регулярную смену прав доступа, но некоторые сотрудники продолжают оставлять логины и пароли на виду, не скрывая их от потенциальных мошенников или легко передаю их третьим лицам без должных оснований.

Инструкции по общению с клиентами/посетителями/техподдержкой

Не важно, кем является человек, который хочет прямо или косвенно получить от сотрудника ценные данные или доступ к ним. Главное, чтобы сотрудник имел четкие инструкции, какую информацию он вправе передавать и на каких основаниях. Третьи лица, которые не связаны с компанией, но интересуются процессами в ней, должны вызывать подозрение и ответную реакцию: о них следует доложить службе безопасности компании.

Повышение осведомленности

Регулярно появляются новые способы информационных атак, методы взлома, в том числе, социальной инженерии. Значит, компании необходимо регулярно обучать персонал принципам работы с корпоративными данными и напоминать об ответственности, которая на них возложена. Сотрудники обязаны знать, к каким последствиям может привести раскрытие конфиденциальных данных с помощью социальной инженерии. Помимо этого, руководству компании следует разработать регламенты и инструкции, касающиеся вопросов хранения, использования, распространения и передачи авторизационных и других данных третьим лицам.

Цифровая криминалистика

Цифровая судебная экспертиза (иногда известная как цифровая криминалистика) - это отрасль судебной медицины, охватывающая восстановление и исследование материалов, обнаруженных в цифровых устройствах, часто в отношении компьютерных преступлений. Термин «цифровая криминалистика» первоначально использовался как синоним для компьютерной криминалистики , но теперь он расширился и теперь охватывает все устройства, способные хранить цифровые данные . Укоренившись в революции персональных компьютеров в конце 1970-х - начале 1980-х, эта

дисциплина развивалась бессистемно в течение 1990-х, и только в начале 21 века появилась национальная политика.

Цифровые судебные расследования имеют множество применений. Наиболее распространенным является подтверждение или опровержение гипотезы в уголовных или гражданских судах. Уголовные дела связаны с предполагаемым нарушением установленных законодательством законов, которые преследуются полицией и преследуются государством, например, убийства, кражи и нападения на человека. С другой стороны, гражданские дела касаются защиты прав и собственности физических лиц (часто связанных с семейными спорами), но также могут быть связаны с договорными спорами между коммерческими организациями, когда форма цифровой криминалистики называется электронным обнаружением (ediscovery) может быть задействовано.

Судебная экспертиза может также применяться в частном секторе; например, во время внутренних корпоративных расследований или расследования вторжений (специальное расследование характера и масштабов несанкционированного сетевого вторжения).

Технический аспект расследования делится на несколько подразделов, связанных с типом задействованных цифровых устройств; компьютерная криминалистика, сетевая криминалистика , криминалистический анализ данных и судебная экспертиза мобильных устройств . Типичный процесс судебно-медицинской экспертизы включает в себя изъятие, визуализацию (получение) и анализ цифровых носителей, а также составление отчета о собранных доказательствах.

Помимо выявления прямых доказательств преступления, цифровая криминалистика может использоваться для приписывания улик конкретным подозреваемым, подтверждения алиби или утверждений, определения намерения , определения источников (например, в случаях авторского права) или удостоверять подлинность документов. Расследования намного шире по охвату, чем другие области судебно-медицинской экспертизы (где обычно цель состоит в том, чтобы дать ответы на ряд более простых вопросов), часто с участием сложных временных рамок или гипотез.

Проверка цифровых носителей регулируется национальным и международным законодательством. В частности, в отношении гражданских расследований законы могут ограничивать возможности аналитиков проводить экспертизы. Часто существуют ограничения на мониторинг сети или чтение личных сообщений. Во время уголовного расследования национальное законодательство ограничивает объем информации, которая может быть изъята. Например, в Соединенном Королевстве изъятие доказательств правоохранительными органами регулируется законом ПАСЕ . В начале своего существования Международная организация компьютерных доказательств

(IOCE) была одним из агентств, которые работали над установлением совместимых международных стандартов для изъятия улик.

При использовании в суд цифровых доказательств подпадает под те же правовые нормы, что и другие формы доказательств; суды обычно не требуют более строгих правил. В Соединенных Штатах Федеральные правила доказывания используются для оценки допустимости цифровых доказательств, PACE Соединенного Королевства и Законы о гражданских доказательствах содержат аналогичные руководящие принципы и многие в других странах есть свои законы. Федеральные законы США ограничивают изъятие предметов, имеющих только очевидную доказательную ценность. Признается, что это не всегда возможно установить с помощью цифровых носителей до исследования.

Список использованной литературы

1. Adam Shostack. “Threat Modeling: Designing for Security”. Published by John Wiley & Sons, Inc., Canada 2014.- 626 p.
2. Richard Bejtlich. “The Practice of Network Security Monitoring”. Published by No Starch Press, Inc., USA 2013. – 380 p.
3. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams and Abdul Aslam. “Enterprise Cybersecurity: how to build a successful Cyberdefense program against advanced threats”. Published by Apress, 2015. – 508 p.
4. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. Инсайд : журнал. — 2015. — № 1. — С. 14—17. — ISSN 2413-3582
5. Carl A. Sunshine. Computer Network Architectures and Protocols. — Springer Science & Business Media, 2013-06-29. — 542 с. — ISBN 978-1-4613-0809-6.
6. Саммонс, Джон (2012). Основы цифровой криминалистики: учебник для начинающих в цифровой криминалистике. Syngress. ISBN978-1597496612