УДК 004.58 / 316.776

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дашко Д.А., Мешков В.И.
Государственный ВУЗ «Национальный горный университет», nmu.org.ua, dashkodo@gmail.com

Сегодня человеческий фактор в информационной безопасности играет гораздо более важную роль, чем 20 лет назад, когда пользователями Интернета были лишь специалисты. Многие компании, которые думают, что проблему информационной безопасности можно решить просто с помощью аппаратных и программных средств, сильно заблуждаются. Технологии безопасности, которым привыкли доверять, – межсетевые экраны, устройства идентификации, средства шифрования, системы обнаружения сетевых атак и другие – малоэффективны в противостоянии хакерам, использующим методы социальной инженерии.

Ключевые слова – защита от социальной инженерии; информационная безопасность; социальная инженерия.

ВВЕДЕНИЕ

Что такое социальная инженерия в контексте информационной безопасности? Социальная инженерия - термин, использующийся злоумышленниками для обозначения несанкционированного доступа к информации, не связанного со взломом программного обеспечения; цель - обмануть людей для получения паролей к системе или иной информации, которая поможет нарушить безопасность системы.

ПРИЧИНЫ РОСТА КОЛИЧЕСТВА АТАК

Популярность социальной инженерии среди злоумышленников растет потому, что нередко сами работники предприятия - люди являются самым слабым звеном в системе защиты. У данного факта много объяснений, во-первых – нередко часть работников просто недостаточно обучена, и им не хватает знаний, чтобы избежать такой атаки, а также большую роль играет и то, что большая часть предприятий думает только о защите физического периметра от внешних угроз. При помощи сотрудника, обойдя эту внешнюю защиту, злоумышленник обходит самое большое препятствие.

Социальная инженерия является важным аспектом в контексте предприятия в целом, так как системы защиты создают для злоумышленника довольно сложно преодолеваемый барьер, и в данном случае неважно, какого именно работника удалось злоумышленнику обмануть, так как результат – доступ ко всем внутренним ресурсам, минуя барьер защиты, будет одинаковым во всех случаях. Атаки социальной инженерии нередко ориентированы на работников, у которых есть самые большие права доступа к работе с конфиденциальной информацией, однако злоумышленник нередко оценивает и потенциальные знания цели.

Одной из важных причин распространения социальной инженерии как метода атаки – это очень дешевый вид нападения, атакующий может не быть специалистом в сфере информационных технологий. Существенным фактором является также и то, что при использовании методов социальной инженерии результат нередко достигается гораздо быстрее, чем, если бы был использован иной метод для нападения, для сравнения – зачем пытаться взломать систему защиты дверь, если неподготовленный пользователь сам готов нас впустить.

ВИДЫ АТАК

- Претекстинг. Данный вид атак представляет собой набор действий, проведенный по определенному, заранее готовому сценарию (претексту). Данная техника предполагает использование голосовых средств, таких как телефон, Skype и т.п. для получения нужной информации. Как правило, представляясь третьим лицом или притворяясь, что кто-то нуждается в помощи, злоумышленник просит жертву сообщить пароль или авторизоваться на подготовленной веб-странице, тем самым заставляя цель совершить необходимое действие или предоставить определенную информацию. В большинстве случаев данная техника требует каких-либо изначальных данных об объекте атаки (например, персональных данных: даты рождения, номера телефона, номеров счетов и др.)
- Quid pro quo. Данный вид атаки подразумевает звонок злоумышленника в компанию по корпоративному телефону. В большинстве случаев злоумышленник представляется сотрудником технической поддержки, опрашивающим, есть ли какие-нибудь технические проблемы. В процессе "решения" технических проблем, мошенник "заставляет" цель вводить команды, которые позволяют хакеру запустить или установить вредоносное программное обеспечение на машину пользователя.
- Сбор информации из открытых источников. Использование социальной инженерии требует умения собирать о человеке необходимую информацию. Основным способом получения персональной информации стал её сбор из открытых источников, главным образом из социальных сетей. К примеру, такие сайты, как «Facebook», «VK», содержат огромное количество данных, которые люди и не пытаются скрыть. Как правило, пользователи не уделяют должного внимания вопросам безопасности, оставляя в свободном

доступе данные и сведения, которые могут быть использованы злоумышленником. Даже ограничив доступ к информации на своей странице в социальной сети, пользователь не может быть точно уверен, что она никогда не попадет в руки мошенников. Например, бразильский исследователь Нельсон Новаес Нето показал, что существует возможность стать другом любого пользователя «Facebook» в течение 24 часов, используя методы социальной инженерии. В ходе эксперимента исследователь выбрал «жертву» и создал фальшивый аккаунт человека из ее окружения - ее начальника. Сначала он отправлял запросы на дружбу друзьям друзей начальника жертвы, а затем и непосредственно его друзьям. Через 7,5 часов исследователь добился добавления в друзья от «жертвы». Тем самым, исследователь получил доступ к личной информации пользователя, которой тот делился только со своими друзьями.

- Дорожное яблоко. Этот метод атаки представляет собой адаптацию троянского коня, и состоит в использовании физических носителей. Злоумышленник подбрасывает "инфицированный" USB-носитель, в месте, где носитель может быть легко найден (туалет, лифт, парковка). Носитель подделывается под официальный, сопровождается подписью или снабжается корпоративным логотипом и ссылкой на официальный сайт компании. Сотрудник по незнанию может подобрать носитель и вставить его в компьютер, чтобы удовлетворить своё любопытство.

МЕТОДЫ ЗАЩИТЫ ОТ АТАК

К сожалению, невозможно предсказать какую атаку выберет атакующий, в какой период времени, кто будет жертвой, но тем не менее возможно уменьшить успешность атаки используя нижеприведенные методы защиты:

- Тестирование системы защиты - это метод выявления недостатков безопасности с точки зрения постороннего человека (злоумышленника). Используя этот метод, можно обнаружить даже те недостатки защиты, которые не были учтены в самом начале, при разработке политики безопасности. При тестировании могут быть затронуты деликатные вопросы частной жизни сотрудников и безопасности организации, поэтому желательно получить предварительное разрешение на проведение такого мероприятия.

Профессионалам в области безопасности при проведении теста необходимо иметь такое же положение, как и у потенциального злоумышленника: в их распоряжении должны быть время, терпение и максимальное количество технических средств, которые могут быть использованы злоумышленником.

- Осведомленность. Осведомленность является ключевым моментом и вследствие того, что это предварительная, предупреждающая мера, нацеленная на усвоение самими служащими основных принципов и необходимых правил защиты. Разумеется, этот аспект требует обучения и тестирования сотрудников. В рамках данной меры акцентируется внимание на следующих пунктах:

1. Привлечение внимания людей к вопросам информационной безопасности;
2. Осознание сотрудниками всей серьезности проблемы и принятие политики безопасности организации;
3. Изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения.

ЗАКЛЮЧЕНИЕ

Список методов защиты от социальной инженерии можно продолжать бесконечно, но это все равно не защитит от злоумышленников и мошенников всех мастей. Поэтому, типовых противодействий социальным инженерам не существует и не может существовать и каждый инцидент требует индивидуального подхода и всестороннего рассмотрения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Касперски К. Секретное оружие социальной инженерии. (Электрон. ресурс) / Способ доступа: URL: http://citforum.ru/security/articles/soc_eng/ – Секретное оружие социальной инженерии.
2. Шишкова С. Социальная инженерия (Электрон. ресурс) / Способ доступа: URL: http://www.e-xecutive.ru/knowledge/announcement/345004/ – Социальная инженерия
3. Should Social Engineering be a part of Penetration Testing? (Электрон. ресурс) / Способ доступа: URL: http://www.darknet.org.uk/2006/03/should-social-engineering-a-part-of-penetration-testing/ – Should Social Engineering be a part of Penetration Testing?
4. Sarah Granger. Social Engineering Fundamentals, Part I: Hacker Tactics (Электрон. ресурс) / Способ доступа: URL: http://www.darknet.org.uk/2006/03/should-social-engineering-a-part-of-penetration-testing/ – Should Social Engineering be a part of Penetration Testing?
5. Margaret Rouse. What is social engineering? (Электрон. ресурс) / Способ доступа: URL: http://searchsecurity.techtarget.com/definition/social-engineering/ – What is social engineering?