Угрозы информационной безопасности и каналы утечки информации

Автор: Баратова Н.Ш

Перед разработкой систем компьютерной безопасности необходимо оценить потенциальные угрозы и каналы утечки информации, обрабатываемой на ЭВМ, т.е. составить модель нарушителя.

Потенциальные угрозы можно разделить на две основные категории: случайные и преднамеренные.

Виды угроз информационной безопасности:

- **Первая** – это аппаратные средства. Сбой в работе или выход из строя процессора, материнской платы, линий связи, периферийных устройств может привести к частичной или полной потери информации, хранящейся в компьютере.
- **Второй источник угрозы** – программное обеспечение. Угрозу могут представлять исходные и приобретенные программы, утилиты и операционные системы. Для обеспечения сохранности информации штатным пользователям рекомендуется устанавливать лицензионные антивирусные программы.
- **Третий вид угрозы** информационной безопасности – данные, которые хранятся на отдельных носителях или в печатном виде. Необходимо принимать отдельные меры по хранению данных, которые не находятся в компьютерной системе.
- **Четвертый вид угрозы** – пользователи компьютеров и обслуживающий персонал. Люди могут нанести вред информации как случайно, так и специально. Поэтому всегда количество людей, имеющих доступ к информации организации, сведен до минимума.


Угрозы безопасности информации
Случайные угрозы
Преднамеренные угрозы
Стихийные бедствия и аварии
Традиционный шпионаж и диверсии
Сбои и отказы технических средств
Несанкционированный доступ к информации
Ошибки при разработке компьютерной системы
Электромагнитные излучения и наводки
Алгоритмические и программные ошибки
Несанкционированная модификация структур
Ошибки пользователей и обслуживающего персонала
Вредительские программы

Наиболее часто реализуемые угрозы

В связи с повсеместным развитием Интернета наиболее часто атаки производятся с использованием уязвимостей протоколов сетевого взаимодействия. Рассмотрим 7 наиболее распространенных атак.

1. **Анализ сетевого трафика**
2. **Сканирование сети**
3. **Угроза выявления пароля**
4. **Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.**
5. **Навязывание ложного маршрута сети**
6. **Внедрение ложного объекта сети**
7. **Отказ в обслуживании**

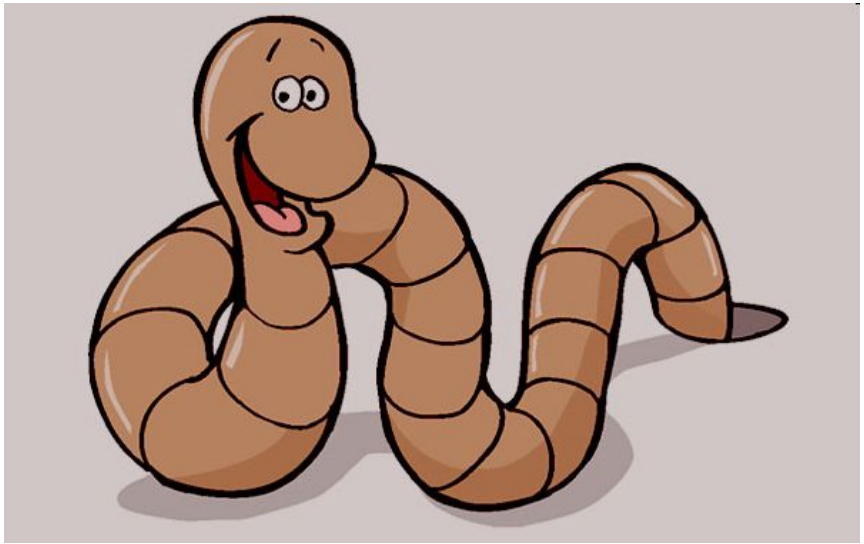
Разновидности атак на сеть удаленного доступа

Под атакой подразумевается попытка нарушения компьютерной безопасности или попытка обхода средств управления безопасности системы. Атаки на сеть могут осуществляться различными методами. Рассмотрим наиболее известные из них.

- Анализ сетевых пакетов.
- Имитация IP-адресов.
- Тайное присутствие третьего лица.
- Отказ в обслуживании (DDOS-атака).
- Атака «троянский конь».

Вирусы-черви

Черви являются подклассом вирусов, но при этом обладают характерными особенностями. Например, червь воспроизводит себя, при этом, он не заражает другие файлы. Кроме этого, вирус-червь внедряется один раз на определенный компьютер, а затем ищет способы распространиться далее на другие ПК. Данная разновидность вируса, чем больше времени находится на компьютере необнаруженной, тем больше файлов заражает. При этом вирус-червь создает только единственную копию своего кода.



Клавиатурный шпион

- **Клавиатурный шпион или keylogger** – это вредоносная программа для перехвата пользовательских паролей операционной системы и определения их легальных полномочий и прав доступа к компьютерным ресурсам. Клавиатурные шпионы различаются только способом перехвата информации. Таким образом, существует три типа клавиатурных шпионов:

ИМИТАТОРЫ

злоумышленник внедряет вредоносную программу, которая имитирует приглашение пользователю зарегистрироваться для входа в систему.

ФИЛЬТРЫ

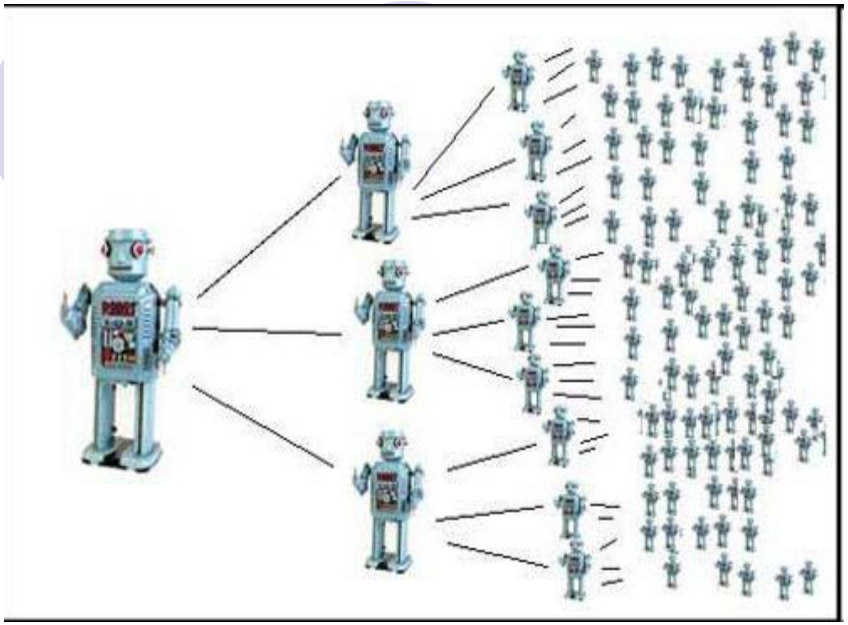
отслеживают все данные, которые пользователь операционной системы вводит с клавиатуры компьютера.

ЗАМЕСТИТЕЛИ

подменяют собой программные модули операционной системы, отвечающие за аутентификацию пользователей.

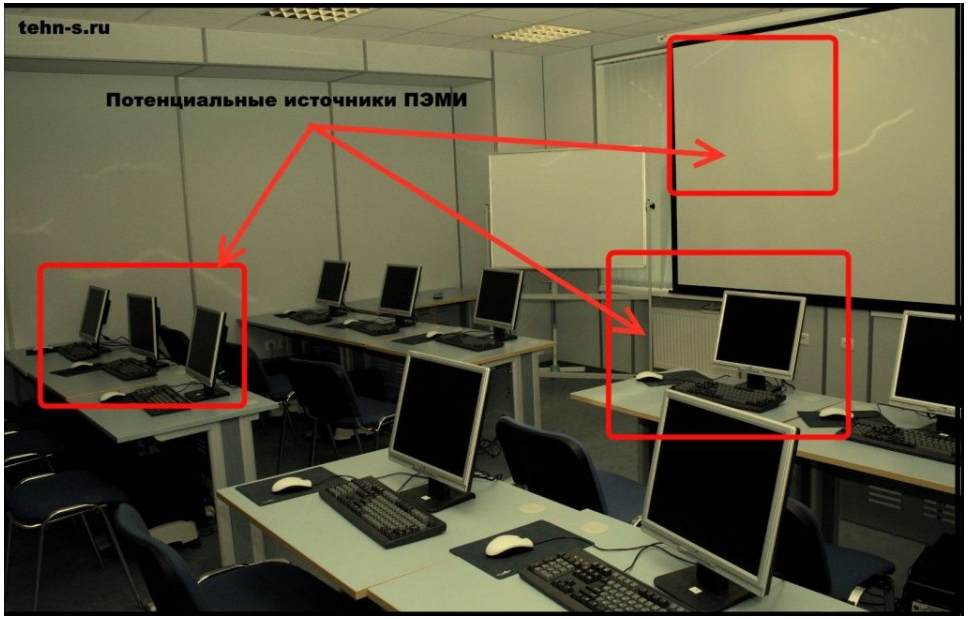
Бот-сеть

Бот-сеть является важным инструментом в руках преступников, в основном используется для передачи огромного количества спама. Bot владельцы часто сдают в аренду свои бот-сети для других преступников, которые рассылают спам, например, рекламные сообщение поддельных лекарств.



Мобильные ОС опережают по безопасности ОС ПК

Наибольшую опасность с точки зрения утечки информации представляют побочные (паразитные, непреднамеренные) излучения технических средств, участвующих в процессе передачи, обработки и хранения секретной информации.



Краткое описание атак с использованием социальной инженерии

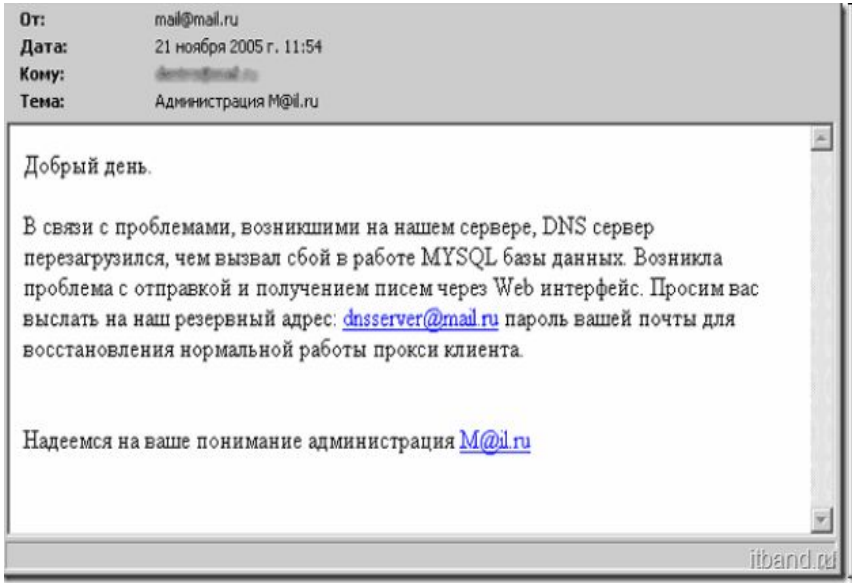
Социальная инженерия описывает, прежде всего, нетехнические угрозы информационной безопасности. Широкий характер этих угроз требует обеспечивать информацию об угрозах и потенциальной защищенности управленческого и технического штата в компании, включая:

- Ведущие менеджеры (Правление компании);
- Технический и сервисный персонал;
- Служба поддержки;
- Служба безопасности;
- Бизнес-менеджеры.

На сегодня существует 8 основных векторов нападения:

- Сетевые угрозы (он-лайн):
- Фишинг;
- Вишинг;
- Фарминг;
- Телефон;
- Анализ мусора;
- Личные подходы;
- Реверсивная социальная инженерия.

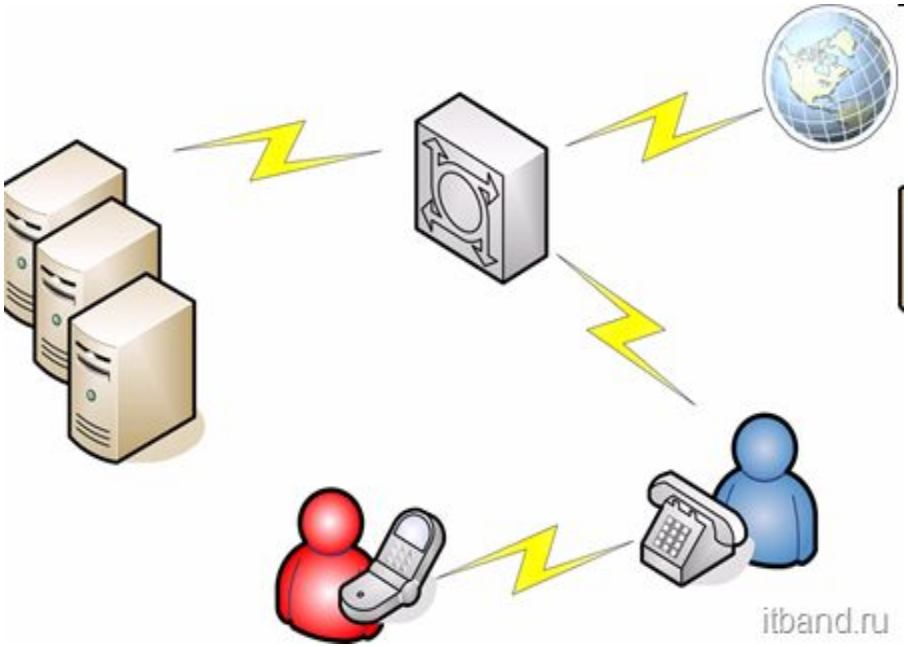
Фишинг (Phishing) — технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т.д.



Фарминг (pharming) – перенаправление жертвы по ложному адресу. Для этого может использоваться некая навигационная структура (файл hosts, система доменных имен – domain name system, DNS).

Угрозы при использовании телефонной связи

Телефон предлагает уникальный способ нападения для хакеров. Это — знакомая среда. Телефонная связь по IP-протоколу Internet (VoIP) — рынок разработки, который предлагает выгоды стоимости компаниям. В настоящее время взлом VoIP, как полагают, является главной угрозой. VoIP-имитация становится столь же широко распространенным явлением, как и электронная почта.



Атаки на мусор

Цели нападения	Описание	Направленность
Бумажные отходы во внешних урнах	Хакер берет бумагу из внешне размещенной урны с мусором, чтобы захватить любую уместную информацию компании.	Конфиденциальная информация
Бумажные отходы во внутренних урнах	Хакер берет бумагу из внутренних офисных урн, совершая обход любых рекомендаций защиты.	Конфиденциальная информация

Реверсивная социальная инженерия

Цели нападения	**Описание**	**Направленность**
Воровство идентификационных данных	Хакер получает пользовательский идентификатор и пароль уполномоченного пользователя	Конфиденциальная информация
Воровство информации	Хакер использует идентификатор уполномоченного пользователя и пароль, чтобы получить доступ к файлам компании.	Конфиденциальная информация Деньги Ресурсы Деловое доверие Деловая доступность

ВЫВОД

Думаю, после прочтения данного материала, вы теперь понимаете, насколько важно со всей серьезностью отнестись к вопросу безопасности и защищенности вашего компьютера от вторжений злоумышленников и воздействий на него вредоносными программами.

Защита от атак социальной инженерии несомненно, одно из самых сложных в разработке мероприятий. Данный тип защиты нельзя построить исключительно техническими методами.

Кроме того, хотелось бы отметить что для построения системы противодействия таким атакам, несомненно, стоит привлекать профессиональных консультантов, а не пытаться строить защиту своими силами