Некоторые аспекты безопасности в информационных сетях

Существующие угрозы и методы противодействия

Безопасность начинается с мелочей

- UPS
- Сервер должен нормально завершать работу в случаях, когда питание отключилось

Защита от несанкционированного доступа

- Отпечатки пальцев, карты, сотовые телефоны
- Шифрование диска полностью FDE
- (Full Disk Encription)
- Географическая привязка машин, содержащих важную информацию через GPS
- Дублирование информации для сохранности

VLAN

- Виртуальные локальные сети
- Каждый VLAN имеет свой идентификатор
- Количество практически не ограничено
- Стандарт принят в конце 1992 года
- С 2004 года стандарт 802.10 признан устаревшим и заменен на 802.1Q.

VLAN

- Когда локальная сеть в пределах одного здания совместно используется несколькими фирмами, а несанкционированный доступ к информации желательно ограничить
- Также можно реализовывать подобные схемы в рамках Интернет при помощи VPN

VPN

- По типу среды:

- Защищённые = с шифрованием
- Незащищённые – без

VPN по назначению

- **Intranet VPN** для нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи.
- **Remote Access VPN** Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем дома
- **Extranet VPN** Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже
- **Internet VPN** Используется для предоставления доступа к интернету провайдерами, обычно в случае если по одному физическому каналу подключаются несколько пользователей.
- **Client/Server VPN** Он обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Этот вариант похож на технологию VLAN, но вместо разделения трафика, используется его шифрование.

Firewall

- Первые Firewall появились в конце 80-х годов, в 1991 году фирма DEC предложила устройство **SEAL** (Secure External Access Link), устройства же современного типа появились в 1993 году (**TIS** – Trusted Information System).

http://book.itep.ru/6/fwal_63.htm

Firewall

- Система **firewall** заменяет маршрутизатор или внешний порт сети (gateway).
- Защищенная часть сети размещается за ним. Пакеты, адресованные Firewall, обрабатываются локально, а не просто переадресуются.
- Пакеты же, которые адресованы объектам, расположенным за Firewall, не доставляются.

Firewall

- Одно устройство может совмещать в себе функции сетевого экрана, Шлюза, Кэша и Firewall
- Безопасность сети – безопасность самого незащищённого элемента. По этой причине создаётся деметаллизированная зона, куда выносятся эти самые элементы

Firewall

- Обычно сетевым экраном реализуется одна из двух политик безопасности:

- Разрешено все, что не запрещено правилами
- Запрещено все, что не разрешено правилами

Firewall

- Некоторые протоколы желательно отфильтровывать из-за их потенциальной опасности. Допускаются только на специально выделенных машинах.

1. Порт 23 (Telnet), не должен использоваться вообще или использоваться для исследовательских целей на одной ЭВМ
2. Порты 20 и 21 (FTP) лучше закрыть везде, но, в крайнем случае, их можно открыть при необходимости на одном FTP-сервере.

Firewall

3. Порт 25 (SMTP) обычно разрешается только на центральном почтовом сервере.
4. Порт 53 (DNS) открывается только для серверов имен (первичного и вторичного).
5. Порт 520 (RIP) может быть использован для перенаправления потока данных. Если можно обойтись без протокола маршрутизации RIP, это следует сделать.
6. Порты 70 (Gopher) и 80 (WWW) должны быть открыты только для шлюзов соответствующих приложений.
7. Порт 119 (NNTP -служба новостей) должен использоваться только сервером новостей.

Firewall

8. Порт 79 (Finger) желательно закрыть, так как через него может быть получена полезная для хакера персональная информация.
9. Порт 69 (TFTP) безоговорочно должен быть закрыт для любых внешних пользователей. Открытие для внутренних пользователей должно осуществляться в случае крайней необходимости для выбранных IP-адресов.
10. Порт 540 (UUCP) лучше заблокировать из-за его уязвимости (сама услуга устарела и ее безопасность не совершенствуется).

Рекомендуется блокировать

- **NFS (Network File System)**. В случае разрешения доступа к этой услуге через сетевой экран, на удаленной машине можно будет смонтировать файловую систему вашей сети и делать с ней все что угодно…
- **NIS** (Network Information System - сетевая информационная система). Эта система позволяет хакерам узнать нужные им имена узлов и пользователей в вашей сети.
- **X-windows**. По уязвимости эта услуга сравнима с Telnet, допускает удаленный запуск процессов.

Персональные Firewall

Технология	**Решаемая проблема**
Анализ состояния	Блокировка всех нежелательных протоколов
Firewall рабочей станции	Защищает от DoS-атак
Глубокий анализ пакетов (**DPI**)	Выявляет опасное содержимое пакетов в случае разрешенных протоколов
Фильтрация уязвимостей	Блокирует влияние известных уязвимостей
Экранирование уязвимостей	Блокирует уязвимость пока она не удалена. Блокурует уязвимости, которые не могут быть удалены.
Интеллектуальные фильтры	Защищают от атак нулевого дня. Усиливают политику безопасности.
Обычные фильтры	Защита приложений

Эволюция угроз по данным **WWW. World Wide Weaponization**.

Год	Событие
1921	Карел Чапек написал роман RUR о бунте роботов
1948	Джон Фон Нейман опубликовал книгу "Общая и логическая теория автоматов". Обоснование воспроизведения.
1976	Джон Бруннер опубликовал фантастический роман "Shockwave Rider" (о компьютерных взломах)
1982	Сотрудниками фирмы Ксерокс Джоном Шоком и Ионом Хуппом введен термин "червь"
1984	Кохем публикует "A short course on computer viruses" (краткий курс по компьютерным вирусам)
1986	Создан первый вирус для области boot (Brain)
1987	Зарегистрировано первое семейство вирусов Иерусалим
1988	Создан мультиплатформенный червь, способный перемещаться по Интернет
1991	Зарегистрирован вирус Микельанжело, вызвавший шок в прессе, но имевший малую опасность
1992	Создано первое полиморфное семейство вирусов (MtE - Mutation Engine)

Эволюция, продолжение

1995	Первые атаки макровируса W97M документов MS Word
1998	Создан первый Java-вирус (Strange Brew)
1999	Первые успешные атаки червя VBS/Melissa систем, базирующихся на почтовой системе Outlook
2000	Появление вируса VBS/Loveletter - нанесшего наибольший урон. Первое вторжение в ОС Windows (Win32/Qazworm)
2001	Детектирование вируса Sega Dreamcast. Появление вируса, базирующегося на IM (Win32/Goner) Первая атака червя Red против WEB-серверов
2002	Появление вируса, способного заражать Macromedia Flash-файлы (ActnS/LFM.A) Регистрация червя Win32/Sobig
2003	Появление червя Blaster, использующего уязвимости Windows Регистрация кода Win32/SQLSlammer, использующего уязвимости Mirosoft SQL-сервера IRCbots (Internet Relay Chat) начал использоваться для управления botnet

Эволюция, продолжение

2004	Первый червь Perl/Sarty - WEB-червь, использующий Google Первая война malware - Bagle/Netsky.Mydoom Создание быстро распространяющегося почтового червя (Win32/Mydoom) Регистрация первого червя для мобильных средств (SymbOS/Cabir)
2005	Появление червя Lion, поражающего LINUX-серверы Массовое распространение червя Win32/Sober Регистрация троянского коня Win32/TrojanDownloader, маскирующегося под видео кодек Появление первого кода ransomware (Win32/Cpcode trojan) Появление Adware, первого фальшивого антивирусного средства с выпадающими иконками предупреждений
2006	Зафиксирован червь Win32/VB.NEI (Kamasutra), который разрушает или стирает файлы на третий день месяца Появился червь W97/TrojanDropper, атакующий файлы MS Word

Эволюция, продолжение

2007	Выявлена botnet "Storm", вовлеченная в рассылку SPAM (Win32/Nuwar) Созданы программы для удаленного занесения в машины вредоносных кодов Рост популярности целевых атак, использующих файлы MS Office (PPT,XLS, DOC) Получил распространение код Win32/Spy.Zbot для кражи банковской информации
2008	Появился вирус, заражающий Photo Frame Driver CD Червь Win32/Conficker поразил миллионы рабочих станций, использующих Microsoft OS
2009	Зарегистрирована botnet с числом машин в сети более 1.900.000 с центром управления на Украине

Вопросы

- Какие средства защиты можно применить для персональной ЭВМ?
- Каким образом распространяется вредоносная программа?
- Что может быть целью атаки на персональный компьютер?