Подавление сетевых атак

Резервное копирование, обновление и установка исправлений

Развёртывание антивирусного программного обеспечения может выполняться на **уровне пользователя** и на **уровне сети**.

По мере выпуска новых вирусов или троянских программ предприятиям рекомендуется **постоянно следить за обновлением антивирусного программного обеспечения до последних версий**.

Рекомендуемые шаги по снижению вероятности атак вирусов-червей.

- **Сдерживание** означает сдерживание распространения червей в пределах сети. Разделите незаражённые части сети на разделы.
- **Противодействие** — исправление всех систем и по возможности выполнение сканирования на предмет уязвимостей в системе.
- **Карантин** — отслеживание всех заражённых компьютеров в сети. Отключите, удалите или заблокируйте заражённые компьютеры в сети.
- **Лечение** — очистка и исправление всех заражённых систем. Для удаления некоторых вирусов-червей может потребоваться переустановка всей основной системы.

Наиболее действенный метод минимизации последствий атаки вируса-червя — **скачать обновления для системы безопасности с сайта поставщика операционной системы** и **установить** соответствующие исправления на **все уязвимые копии систем**.

Можно создать **центральный сервер исправлений**, с которым взаимодействуют все системы по прошествии заданного периода.

Все исправления, которые еще не были установлены, **автоматически загружаются** с сервера исправлений и **устанавливаются** без участия пользователя.

Аутентификация, авторизация и учёт

Сочетание служб **аутентификации, авторизации и учёта** — это метод, позволяющий контролировать вход разрешённых пользователей (аутентификация), какие действия они могут выполнять, находясь в сети (авторизация), а также следить за их действиями во время доступа к сети (учёт).

Аутентификация

В небольшой сети используется локальная аутентификация.

При **локальной аутентификации** каждое устройство использует собственную базу данных комбинаций имён пользователей и паролей.

При наличии большого числа учётных записей пользователей управление этими учётными записями осложняется.

Например, при наличии 100 сетевых устройств все учётные записи пользователей необходимо добавить на все 100 устройств.

В более крупных сетях рекомендуется использовать **внешнюю аутентификацию**, так как она обеспечивает больше возможностей для масштабирования.

Внешняя аутентификация позволяет всем пользователям проходить аутентификацию посредством **внешнего сетевого сервера**.

Варианты внешней аутентификации пользователей

- **RADIUS** представляет собой открытый стандарт с низким коэффициентом использования ресурсов ЦП и памяти. Этот стандарт используется различными сетевыми устройствами.

- **TACACS+** представляет собой механизм обеспечения безопасности, который позволяет использовать модульные службы аутентификации, авторизации и учёта. Этот стандарт использует службу TACACS+, запущенную на сервере безопасности.

Авторизация

После аутентификации пользователя службы авторизации определяют ресурсы, к которым **у пользователя есть доступ**, и операции, которые пользователю **разрешено выполнять**.

Например, «Пользователь „student“ может осуществлять доступ к узлу serverXYZ, используя только Telnet».

Учёт

Записи учёта действий пользователя, включая объекты доступа, продолжительность доступа к ресурсу и все внесённые изменения.

Учёт позволяет **отслеживать использование сетевых ресурсов**.

Например, «Пользователь „student“ осуществил доступ к узлу serverXYZ с помощью Telnet продолжительностью 15 минут».

Межсетевые экраны

Межсетевой экран — одно из наиболее эффективных средств безопасности для защиты пользователей сети от внешних угроз.

Межсетевой экран **разделяет две или более сети** и **осуществляет контроль** проходящего между ними трафика, одновременно предотвращая попытки несанкционированного доступа.

Методы определения разрешённого и запрещённого доступа к сети

- **Фильтрация пакетов** — запрет или разрешение доступа на основе IP- или MAC-адресов.
- **Фильтрация по приложениям** — запрет или разрешение доступа для конкретных типов приложений на основе номеров портов.

Методы определения разрешённого и запрещённого доступа к сети

- **Фильтрация по URL-адресам** — запрет или разрешение доступа к веб-сайтам на основе конкретных URL-адресов или ключевых слов.

- **Анализ пакетов с учётом состояний соединений (SPI)** — входящие пакеты должны представлять собой легитимные отклики на запросы внутренних узлов. Не запрошенные пакеты блокируются, если они не разрешены в явном виде.

Типы пакетов межсетевых экранов

- **Интегрированные межсетевые экраны** — дополняет возможности существующего устройства функциями межсетевого экрана.

- **Персональные межсетевые экраны** — размещаются на узлах и не рассчитаны на защиту локальной сети в целом. Они могут быть реализованы в ОС по умолчанию или установлены сторонним поставщиком.

Типы пакетов межсетевых экранов

- **Аппаратные межсетевые экраны** — это выделенные устройства, называемые устройством защиты.

- **Серверные межсетевые экраны** — это приложения межсетевого экрана, выполняемые в сетевой операционной системе (NOS), например UNIX, Windows или Novell.

Защита оконечных устройств

Защита оконечных устройств — одна из наиболее сложных задач сетевого администратора, поскольку в данном случае имеет значение человеческий фактор.

Компании необходимо разработать и тщательно задокументировать соответствующие политики и ознакомить с ними сотрудников.

Комплексные решения для защиты оконечных устройств используют функции контроля доступа к сети.

В рамках защиты оконечных устройств требуется **защита устройств 2-го уровня** в рамках сетевой инфраструктуры, что позволяет предотвратить атаки 2-го уровня (например, спуфинг-атаки с использованием MAC-адресов, атаки с использованием переполнения таблиц MAC-адресов и атаки по типу «сетевой шторм»).

Такая процедура называется **минимизацией риска атаки.**