**5. Противодействие атакам**

Атака на автоматизированную систему (АС) - действие или последовательность действий нарушителя, которые приводят к реализации угроз, путем использования уязвимостей этой АС.

Уязвимости АС:

‑ недостатки аппаратно-программных средств по вине разработчика

‑ добавленные администратором при настройке АС

‑ уязвимости внесенные пользователем

Цель атаки – нарушение одной из функций системы:

‑ конфиденциальности;

‑ целостности;

‑ доступности.

Атака может быть активной (результат - изменение данных) или пассивной (результат — раскрытие данных). При этом факт атаки необязательно означает, что она достигла цели. Степень успешности атаки зависит от уязвимости системы и эффективности контрмер.

Этапы атаки:

1. Сбор информации.

Изучение окружения. Провайдер целевой системы, адреса доверенных узлов, трафик, режим работы организации, телефонные номера и т.д.

Идентификация топологии сети. Количество компьютеров, способ их соединения, организация выхода в глобальную сеть.

Идентификация узлов сети. Разведка IP-адреса узла, его доступности.

Идентификация сервисов и портов. Определяется наличие установленных сервисов (Telnet, FTP, Web- сервера и т.д.) наличие доступа к ним, открытость портов.

Идентификация операционной системы. Тип операционной системы.

Определение уязвимостей узла. На основе ранее собранной информации.

2. Реализация атаки.

‑ проникновение в систему;

‑ контроль над системой.

3. Завершение атаки.

Устранение следов атаки с целью невозможности идентификации атакующего.

‑ маскирование внедренной программы;

‑ изменение контрольных сумм файлов;

‑ очистка журнала регистрации событий.

Общая классификация атак:

‑ регулярные (проводятся на любую систему вне зависимости от состава ее аппаратно-программных средств);

‑ использующие ошибки политики безопасности или администрирования;

‑ использующие ошибки программно-технических средств системы (“баги”).

Противодействие атакам — комплекс организационно-технических мероприятий, направленных на обнаружение, анализ и реагирование на инциденты безопасности, атаки или несанкционированный доступ.

Организационно-правовая составляющая:

- документированная политика безопасности;

- положения о распознавании и противодействии атакам;

- наличие компетентных специалистов.

Реализация положений политики безопасности, в части распознавания и противодействия атакам

Содержание политики безопасности:

- зона ответственности;

- правила использования информационных ресурсов;

- план мероприятий проводимых в случае распознавания атаки;

- ответственность персонала.

Техническая составляющая

Штатные средства - сетевые журналы сетевых устройств, операционных систем и приложений;

Специализированные средства - средства распознавания и противодействия атакам.

Системы обнаружения вторжений (IDS)

Функции:

Обнаружение - идентификация атаки или подозрительной активности в отношении ресурсов сети или хостов и уведомление наблюдающей станции;

Реагирование - блокирование или смягчение происходящего события и профилактика системы от последующих атак;

Предотвращение - остановка обнаруженной атаки частично или в некоторых случаях полностью.

IDS уровня узла (HIDS) - контролирующие отдельный узел (рисунок 5.7);

Сетевые IDS (NIDS) - контролирующие сегмент ЛВС (рисунок 5.7);

IDS уровня рабочей станции - контролирующие отдельную рабочую станцию;

“Системы-ловушки” (honeypots) - эмулирующие отдельный узел или целый сегмент сети, выглядящие заведомо уязвимыми и привлекательными для потенциальной атаки;

Сканеры уязвимостей (vulnerability scanner) - сетевые или уровня узла.

|  |
| --- |
| Рисунок 5.7. – Схема размещения датчиков IDS |

Для противодействия несанкционированному межсетевому доступу брандмауэр должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рисунок 5.8). При этом все взаимодействия между этими сетями должны осуществляться только через межсетевой экран. Организационно экран входит в состав защищаемой сети.

Межсетевой экран должен учитывать протоколы информационного обмена, положенные в основу функционирования внутренней и внешней сетей. Если эти протоколы отличаются, то брандмауэр должен поддерживать многопротокольный режим работы, обеспечивая протокольное преобразование отличающихся по реализации уровней модели OSI для объединяемых сетей. Чаще всего возникает необходимость в совместной поддержке стеков протоколов SPX/IPX и TCP/IP.

|  |
| --- |
| image002  Рисунок 5.8. – Схема размещения межсетевого экрана |

Устройство, подобное межсетевому экрану, может использоваться и для защиты отдельного компьютера. В этом случае экран, уже не являющийся межсетевым, устанавливается на защищаемый компьютер. Такой экран, называемый брандмауэром компьютера или системой сетевого экранирования, контролирует весь исходящий и входящий трафик независимо от всех прочих системных защитных средств. При экранировании отдельного компьютера поддерживается доступность сетевых сервисов, но уменьшается или вообще ликвидируется нагрузка, индуцированная внешней активностью. В результате снижается уязвимость внутренних сервисов защищаемого таким образом компьютера, поскольку первоначально сторонний злоумышленник должен преодолеть экран, где защитные средства сконфигурированы особенно тщательно и жестко.

**Виртуальная частная сеть** (VPN - Virtual Private Network) - объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных (рисунок 5.9).

|  |
| --- |
| image001  Рисунок 5.9. – Схема реализации виртуальной частной сети |

Мероприятия по обеспечению информационной безопасности:

1. Аутентификация взаимодействующих сторон.

2. Криптографическая защита передаваемых данных.

3. Проверка подлинности и целостности передаваемой информации.

Устройства VPN:

1. VPN – клиент - программный или программно-аппаратный комплекс на базе ПК;

2. VPN – сервер - программный или программно-аппаратный комплекс на базе серверного оборудования.

3. Шлюз безопасности - сетевое устройство, подключаемое к двум сетям.

Особенности передачи данных в VPN:

1. Криптозащита всего пакета.

2. Инкапсулирование.

3. Туннелирование.