КЛАСИФИКАЦИЯ НА ЗАПЛАХИТЕ;ЗАПЛАХИ ЗА ДОСТЪПНОСТТА;ВРЕДОНОСНО ПРОГРАМНО ОСИГУРЯВАНЕ.

Класификация на заплахите.

Заплахите могат да бъдат класифицирани по следните критерии:

- по категорията на ИС (достъпност, неприкосновеност, конфиденциалност)
- по компонентите на ИС-ми, към които са насочени заплахите (данни, програми и т.н.)
- по начина на осъществяване (случайни/преднамерени действия от природен/техногенен характер)
- по разположение на източника на заплахите (вътре или вън от ИС-ма)

Най често разпространените заплахи са:

1. по отношение на достъпността

- повреждане или даже разрушаване на оборудването
- извеждане на системата от режим на експлоатация
- препълване на сървъри
- логически бомби, вируси и троянски коне

1. по отношение на неприкосновеността

- кражба на информация.

1. по отношение на конфиденциалността

- заплаха вследствие разполагане на данни в среда, където няма защита.
- Кражби на оборудване

- Злоупотреби от страна на потребителя

Заплахи за достъпността.

Според компонентите на ИС-ма, към които са насочени, заплахите за достъпността могат да се разделят на:

- Спиране на достъпа на потребителите
- Вътрешен откъс на ИС-ма
- Спиране на работата на подържащата инфраструктура

С потребителите са свързани следните заплахи:

- Нежелание да се работи с ИС-ма
- Невъзможност да се работи със системата следствие на отсъствие на съответстващата подготовка
- Невъзможност да се работи със системата в следствие на отсъствие на техническа поддръжка

Основни източници на вътрешни откази са:

- Отклонение от установените правила на експлоатация
- Излизане на системата от действие вследствие на случайни или преднамерени действия на потребителите или обслужващия персонал
- Грешки при конфигурирането на системата
- Отказ в работата на програмното или апаратното осигуряване
- Разрушаване на данните
- Разрушаване или повреждане на апаратурата

По отношение на подържащата инфраструктура се препоръчва разглеждането на следните заплахи:

- Нарушаване на работата на системите за комуникация, електрозахранването, водоснабдяването, отоплението и климатиците
- Разрушаване или повреда на помещенията
- Невъзможност или нежелание на обслужващия персонал или потребителите да изпълняват задълженията си

Доста опасни са така наречените обидени служители – настоящи и бивши. В повечето случай те се стремят да причинят вреда на организацията, която ги е обидила като например:

- Повреждат оборудването
- Вграждат логическа бомба, която в течение на времето ще разруши програми или данни
- Изтриват данните

Вредоносно програмно осигуряване.

Един от най опасните начини за провеждане на атаки е внедряването на вредоносно програмно осигуряване (ВПО) в атакуемите системи. Можем да разграничим следните аспекти на ВПО:

- Вредоносна функция
- Начин на разпространение
- Външно представяне

Частта от ВПО, осъществяваща разрушителна функция се нарича бомба. Спектърът на вредоносните функции е неограничен и бомбите, както всяка друга програма могат да притежават много сложна логика но обикновено са предназначени за:

- Внедряване на друго ВПО
- Получаване на контрол над атакуемата система
- Агресивно потребление на ресурси
- Изменение или разрушаване на програми или данни

Според механизма на разпространение се различават:

- Вируси – код, притежаващ способността да се разпространява чрез внедряване в други програми.
- Червей – код, способен самостоятелно, т.е. без внедряване в други програми да предизвиква разпространени на своите копия в ИС-ма и да ги изпълнява.
- Троянски кон – вредоносен код, които изглежда като функционално полезна програма