Informatikai biztonság alapjai

3. Rosszindulatú programok

Pethő Attila

2008/9 II. félév

Rosszindulatú programok (malware) fajtái

- vírusok,
- férgek,
- trójaiak,
- spyware,
- dishonest adware,
- crimeware,
- stb.

Vírusok

A **számítógépes vírus** olyan program, mely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban.

Többnyire rosszindulatú, más állományokat használhatatlanná, sőt teljesen tönkre is tehet.

Vírusok jellemzői

- gazdaprogram fertőzése,
- önsokszorosítás,
- kis méret,
- legtöbbjük a Microsoft Windows operációs rendszereken okoz gondokat,
- futtatható állományokat képesek megfertőzni,
- általában ártó szándékkal készítették őket,
- rejtetten működnek, esetleg akkor fedik fel magukat, ha feladatukat elvégezték,
- egyre fejlettebb intelligenciával rendelkeznek, például változtathatják saját kódjukat és aktivitásukat.

Típusaik

- EXE-COM vírusok (Jerusalem, Friday 13)
- BOOT-vírusok (brain, 1986)
- MR-vírusok
- Makró vírusok
- New Exe vírusok
- Multi platform vírusok
- Önátíró (polimorf) vírusok
- E-mail vírusok
- zenefájl vírusok

Működési mechanizmusuk

- A memóriába kerülve végrehajtható fájt keres, ha nem fertőzött, akkor rátelepszik.
  - Nem rezidens → rögtön fertőz, ha lehet.
  - Rezidens → türelmesen vár megfelelő gazdavírusra.
- A gazdafájl elindítása után átveszi az irányítást, végrehajtja a feladatát és visszaadja a vezérlést a gazdafájlnak.

Férgek (worms)

- Önsokszorosításra képes programok.
- Nincs szükségük gazdaprogramra, önállóan terjednek.
- Számítógép hálózaton keresztül terjednek.
- Pl. Mydoom féreg: először 2004 Január 26-án látták, leggyorsabban terjedő féreg.

Trójaiak

- Látszólag hasznos funkciót lát el, de mellette más, káros tevékenységet is folytat.
- Nem sokszorosítja megát, célzott támadásra készítik.

Típusaik

- Távoli hozzáférés,
- Adat megsemmisítő,
- Letöltő,
- Szerver Trójai (Proxy, FTP , IRC, Email, HTTP/HTTPS, etc.),
- Biztonsági szoftver kikapcsoló,
- DoS támadást végző,

Védekezés

- Nem szabad bizonytalan származású szoftvert használni.
- Vírusírtó programok használata.
- Tűzfal alkalmazása.
- Rendszeres szoftverfrissítés. → Korábbi verziók hibáit kihasználó rosszindulatú programok nem fertőzhetnek.

Kéretlen levelek (spam)

- A fogadó által nem kért, elektronikusan, például e-mailen keresztül tömegesen küldött hirdetés, felhívás.
- Összegyűjtött e-mail címekre rövid idő alatt, milliós nagyságrendben is képesek küldeni leveleket.

Védekezés

- olvasás nélküli törlés (fennáll a fontos levél törlésének esélye)
- a web oldalakon feltüntetett e-mail címek álcázása a begyűjtés ellen
- spam azonosító program telepítése a felhasználó gépére
- a nyitott mail-továbbító szerverek korlátozása
- SPAM szűrő alkalmazása a levélkezelő felületen
  - kulcsszavak alapján való szűrés
  - öntanuló Bayes-szűrő használata
- a küldő cégek jogi perlése http://hu.spam.wikia.com/wiki/Kezd%C5%91lap

- A *Cisco* szerint 2010-re 30–40%-kal gyarapodhat a spamek száma.[1] Az évre minden korábbi évinél több, összesen 350 milliárd spamet vártak.[2] Az év elején az összes e-mail 95%-a volt kéretlen reklámlevél.[3]
- 2010-ben is a gyógyszereket árusító spamek a leggyakoribbak, a teljes spamforgalom 80%-át adják, további 5–10% a pornótermékeket népszerűsítő reklám.[4] A MAAWG felmérése szerint a címzettek 50%-a olykor megnyitja a spameket, 11%-uk kattint a bennük található linkre, 8%-uk a levél csatolmányát is megnyitja, 4-4% pedig válaszol, sőt továbbítja az üzenetet.[5]
- A mobilspamek piaca a jobb olvasottság és az egyre alacsonyabb tarifák miatt várhatóan tovább emelkedik, két éven belül európai méretű probléma lehet.[6] 2010-re az SMS-ek 10%-a volt reklám tartalmú, egyes ázsiai országokban olykor azonban a 20%-ot is elérte ez az arány.[7]

Információ veszélyeztetettsége

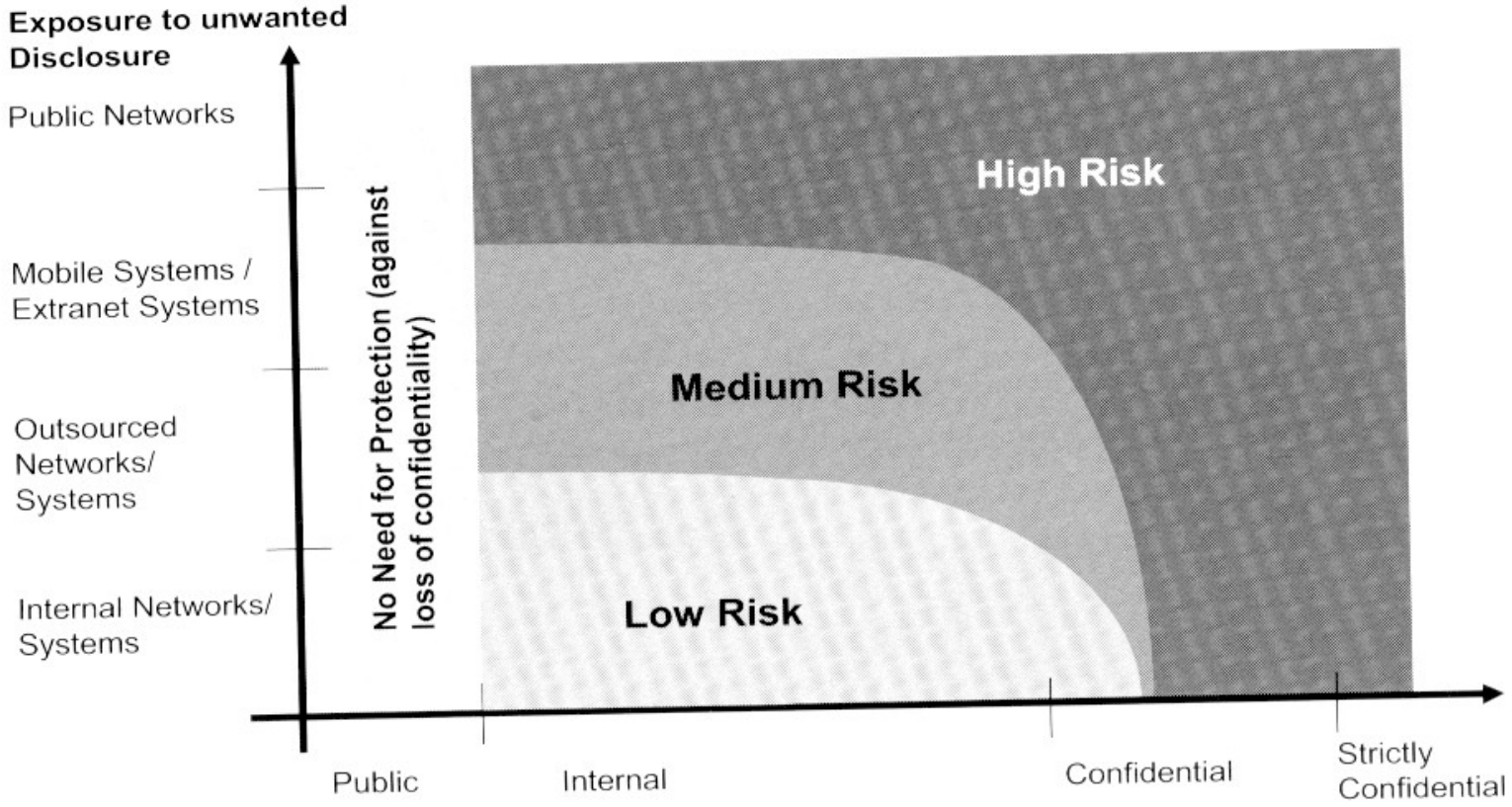

Figure 2: Scenarios and Basic Risk Assessment

Tűzfal

- Védi a privát hálózatot a betörések és a kívülről származó rosszindulatú programok ellen.
- Csak a megengedett információkat engedi ki a privát hálózatból.
- Elválasztja egymástól a hálózat szegmenseit.

Típusai 1.

- Csomagszűrés: az adatcsomagok egyszerű szűrése a cél-port, valamint forrás- és célcím szerint; egy a tűzfal-adminisztrátor által már definiált szabályrendszer alapján történik.
- Állapot szerinti szűrés: felismeri a csomagok közti összefüggéseket és az aktív kapcsolathoz tartozó munkafolyamatokat leállíthatja.
- Proxy szűrés: A szerver csak a proxy IP-címét látja, nem pedig a kliensét. Így a helyi hálózat struktúrája nem ismerhető fel az Internet felől. Megakadályozza a közvetlen kommunikációt a külső és a védett hálózat között.

Típusai 2.

- Tartalomszűrés: egy kapcsolat hasznos adatait kiértékelni, ill. az áthaladó adatokat ellenőrizni tudja.
  - az URL-szűrés és a vírusfigyelés
  - bizalmas céginformációk kiszűrése
  - kulcsszavak alapján nem kívánt weboldalak zárolása
  - nem kívánt alkalmazás-protokollok blokkolása
- Behatolás felismerő és behatolás megelőző rendszerek
- Hálózati címfordítás: Lehetővé teszi belső hálózatra kötött saját nyilvános IP cím nélküli gépek közvetlen kommunikációját tetszőleges protokollokon keresztül külső gépekkel.
- Átjáró: Két különálló hálózat vagy hálózati szegmens közötti átjárást teszi lehetővé.