

Internet

2. rész

Szilvássy László okl. mk. őrgy.



Repülőműszaki Intézet
www.szrfk.hu



Az Internet **VESZÉLYEI**

- Vírusok: védekezés ellenük, otthoni használatra ingyenes programok ajánlása, néhány fizetős alkalmazás és körülbelüli árai;
- Kém és reklám programok: védekezés ellenük;
- Tűzfalak: Windows beépített tűzfala, ingyenes alkalmazások;
- Temporary Internet Files mappa tartalmának ürítése





Veszélyek az Interneten

1. Kártékony programok
2. Jelszófeltörés
3. Elektronikus lehallgatás
4. Hackertámadás
5. Kéretlen e-mail üzenetek
6. Adathalászat és az elektronikus személyazonosság ellopása
7. Megtévesztés



1. Kártékony programok

Kéretlen műveleteket végrehajtó programok. Ilyenek lehetnek a vírusok, a férgek, a trójai és egyéb kártékony végrehajtó programok, valamint a felhasználó engedélye nélkül a rendszerre telepített kém- és reklámprogramok.

- a) Vírusok és férgek
- b) Trójai programok
- c) Kártékony végrehajtó programok
- d) Reklám- és kémprogramok



1. a) Vírusok és férgek

A számítógépes vírusok és férgek kicsi, önmagukat sokszorozni képes kéretlen programok.

Vírusok: mindig valamilyen gazdaprogramhoz kapcsolható, fájlból fájlra terjed.

- viszonylag ártalmatlan
- komoly károkat okozó

Férgék: nincsen szüksége semmilyen gazdaprogramra, gépről gépre terjed.



1. b) Trójai programok

A trójai programok nem fertőznek meg más fájlokat és nem sokszorozódnak.

Gyakran **ismeretlen** helyről letöltött játékokkal, ingyenes programokkal segítségével kerülnek a gépünkre.

Telepítés után valamilyen hátsó ajtót (portot) hoznak létre, melynek segítségével a hackerek átvehetik az irányítást a számítógépünk fölött, vagy jelszavakat és a gépen tárolt egyéb bizalmas információkat küldenek el a tudtunk nélkül.



1. c) Kártékony végrehajtó programok

Bizonyos programok nem sokszorozzák önmagukat és nem nyitnak hátsó ajtót külső hozzáféréshez, hanem valamilyen nem kívánt műveletet hajtanak végre a számítógépen.

Ilyen lehet például bizonyos típusú fájlok (pl.: World állományok) letöltése a számítógépről, vagy a modem telefonos kapcsolatánál a tárcsázandó telefonszám átírása, valamilyen emelt díjas számra.



1. d) Reklám- és kémprogramok

Bármilyen (!!!) program telepítésével beszerezhető, de elegendő egy web hely meglátogatása, vagy egy HTML formátumú e-mail megnyitás ahhoz, hogy „megfertőzze” a gépünket. Egyik leggyakoribb típusa a **böngészőeltérítő** program, amely megváltoztatja a böngésző kezdőlapját.

A **kémprogramok** pedig adatokat gyűjtenek, legtöbb esetben direkt marketing céljából, pl. az Internetes szokásainkról, és ennek függvényében célzott reklám leveleket fogunk kapni.



2. Jelszófeltörés

Egy számítógépes rendszerbe a legkönnyebben egy érvényes felhasználónév és jelszó kombinációjával lehet bejutni. Ha már bent vagyunk rendelkezünk a felhasználó minden jogosultságával.

Jelszó feltörési módszerek:

- személyes információk alapján
- szótáras támadás
- nyers erő módszere



Repülőműszaki Intézet
www.szrfk.hu

9



2. Elektronikus lehallgatás

Az elektronikus kommunikáció elfogására számos módszer létezik. Leggyakoribb a **csomagszimatoló** („sniffer”) program segítségével történő lehallgatás. A csomagok átvizsgálása és összeállítása révén juthatnak bizalmas információhoz.

Sajnos több száz, a hálózati kommunikáció elfogására képes felügyeleti szoftvertermék létezik, néhányuk ráadásul ingyenes is.



Repülőműszaki Intézet
www.szrfk.hu

10



3. Hackertámadások

Több száz konkrét támadási forma létezik, amelyek segítségével egy számítógépes rendszer vagy hálózat hozzáférhetővé válik.

- a) Szolgáltatás megtagadási támadások
- b) Port letapogatás („port scanning”)
- c) Hamisítás („spoofing”)
- d) Vezeték nélküli támadások



3. a) Szolgáltatásmegtagadási kérelem

A szolgáltatásmegtagadási (DoS) támadások során egy rendszert vagy hálózatot kezelhetetlen mennyiségű adattal árasztanak el.

Az elosztott (DDoS) támadások még kifinomultabbak. Ebben az esetben a támadások révén a hackerek több számítógép fölött veszik át az ellenőrzést, és ezeket a gépeket **szolga** vagy **zombi** elnevezéssel felhasználják más rendszerek ellen indított támadásra.



3. b) Portletapogatás („port scanning”)

A port a hálózati alkalmazások által két számítógép közötti kommunikációra használt logikai kapcsolattartási pont.

A portokat számozással azonosítjuk. A levelező rendszer (POP – Post Office Protocol) a levelek letöltése során a 110-es porton kommunikál a kiszolgálóval. Egy átlagos számítógép rendszeren 65 536 port áll rendelkezésre.

A portletapogatás valójában nem támadás, de lehet belőle az is. Valójában csak nyitott kapu keresése, ahol a támadó bejuthat a számítógépünkbe.



3. c) Hamisítás („spoofing”)

Ez sem számít valódi támadásnak. Az IP-hamisítás a hálózaton át küldött adatok forrás IP-címének meghamisítását jelenti, ezáltal az adatok más számítógépről, vagy más hálózatról érkezettnek tűnnek.

Hasonló az e-mail üzenetek hamisítása is, amikor az e-mail üzenet fejrészét hamisítják meg oly módon, hogy mást jelenítenek meg a valódi küldő helyett.



4. Kéretlen e-mail üzenetek (levélszemét - SPAM)

Kéretlen e-maileket jelent, melyekben valamilyen termék megvásárlására, megrendelésére ösztökélik a címzettet. Párhuzamot lehet vonni a kéretlen e-mail üzenetek és a fizikai postaládánkat elárasztó reklám újságok között.

A végeredmény mindkét esetben ugyanaz: kuka.



5. Adathalászat és az elektronikus személyazonosság ellopása

Bankok, kereskedelmi cégek nevében írott levelek formájában keresik fel a felhasználókat és adataik (számlaszámuk, felhasználó jelszavuk, belépési kódjuk) megadására kérik őket, vagy valamilyen web helyre irányítják a felhasználót, ahol űrlapot kell kitölteni a bizalmas adataikkal, ilyen módon jutnak hozzá az adatainkhoz.



6. Megtévesztés

Szorosan kapcsolható az előző tevékenységi formához, mert mindkettő a felhasználók jóindulatát, hiszékenységét próbálja kihasználni. Ebben az esetben a hacker a bank, vagy telefontársaság munkatársának adja ki magát és próbál hozzájutni felhasználónevünkhöz és jelszavunkhoz.

A BBC News felmérése szerint a számítógéppel dolgozók 70%-a hajlandó volt megadni bizalmas adatait.

Ilyen esetben legyünk picit bizalmatlanabbak!



Védekezés

- Víruskereső programok
- Kém és reklám program kereső és eltávolító alkalmazások
- Tűzfalak



Víruskeresők

Nevükkel ellentétben nem csak megkeresik a vírusokat hanem hatékonyan el is távolítják azt számítógépünkről.

Néhány víruskereső program:

- Norton AntiVirus
- McAfee
- Panda
- NOD32
- Antivir
- VirusBuster



Repülőműszaki Intézet
www.szrfk.hu

19



Kémprogram eltávolítók

A víruskereső programok gyártói is kínálnak olyan összetett, megoldásokat, amelyben a víruskereső és a kémprogram eltávolító, sőt még a tűzfal program is egy jól összehangolt egységet képez. Terjedelem és idő hiányában ezeket felsorolni nincsen lehetőségem, így néhány önálló alkalmazást említek csak meg.

- Ad-Aware Se
- Spybot
- Spy Swepper



Repülőműszaki Intézet
www.szrfk.hu

20



Tűzfalak

A Windows XP tűzfala nagyon dicséretes kezdeményezés, mert operációs rendszerbe integrálva ad egy védelmi lehetőséget. Nem konfigurálható, csak a 2. javítócsomagban található, de otthoni felhasználóknak melegen ajánlott legalább ezt bekapcsolni.

Egyéb önálló tűzfalak:

- ZoneAlarm
- Kerio Személyi tűzfal
- Sygate Personal Firewall



Most pedig nézzünk meg néhány képet a víruskereső alkalmazásokról





Repülőműszaki Intézet
www.szrfk.hu

23



Repülőműszaki Intézet
www.szrfk.hu

24







Temporary Internet Files

Ez a böngésző Itál használt mappa, melybe egy oldal letöltése során a képeket, html oldalakat elhelyezi. Ha a böngésző jól van beállítva akkor kilépéskor kiüríti a mappa tartalmát.

Nézzük hogyan kell beállítani!



Temporary Internet Files törlése 1.

Internet Explorer indítása után

Eszközök/Internetbeállítások... menüpont indításával, majd a megjelenő párbeszéd ablakon a **Speciális füles** lapon „**Az ideiglenes internetfájlok törlése a böngésző bezárasakor**” pont előtt a jelölő négyzetet bejelölni.





Temporary Internet Files törlése 2.

Valamilyen fájlkezelő program segítségével meg kell jeleníteni a rejtett fájlokat, majd a következő útvonalon meg kell keresni az ideiglenes mappát és a tartalmát törölni kell.

Ez az útvonal csak Windows 2000 és XP rendszerekre igaz

c:\Documents and Settings\Felhasználónév\Local Settings\Temporary Internet Files



Repülőműszaki Intézet
www.szrfk.hu

29



Temporary Internet Files törlése 3.

Valamilyen takarító program segítségével.

Pl.: CClener segítségével



Repülőműszaki Intézet
www.szrfk.hu

30





Köszönöm a figyelmet!

