Szolnoki Tudományos Közlemények XIV.
Szolnok, 2010.

Dr. Szilvássy László[1]

BEHÁLÓZVA – AZ INTERNET LEHETŐSÉGEI ÉS VESZÉLYEI[2]

1.1. BEVEZETÉS

Ma már az élet minden területén hálózatokat használunk. Gondoljunk csak a mobil telefonra, vagy a bank automatákra, de az internetet[3] is egyre többen használják, használjuk napi szinten. Hiába növekszik folyamatosan azok köre, akik napi szinten dolgoznak az Internet segítségével mégsem növekszik jelentősen azok száma, akik ismerik az Interneten rejlő lehetőségeket és még kevesebb azok száma, akik tisztában vannak az Internet veszélyeivel.

1.2. AZ INTERNET RÖVID TÖRTÉNETE

Az Internet egy világméretű számítógép-hálózat, amely kisebb hálózatok ezrei közötti kommunikációt tesz lehetővé egy egységes „hálózati társalgási nyelv” (az Internet Protocol - TCP/IP) segítségével. A szó jelentése: Internet - „hálózatok közötti”.
Az első nagyobb hálózat az amerikai védelmi minisztérium ARPANET rendszere volt, melyet katonai célokra hoztak létre a ’60-as években. ARPA – Advanced Reserch Project Agency – Fejlett Kutatási Programok Hivatala által támogatott program célja egy olyan hálózat létrehozása volt, mely az adatot automatikusan átirányítja, ha egyes vonalszakaszok vagy számítógépek megszűnnek működni. Az ARPA végső célja egy olyan hálózat volt, mely túléli az atomtámadást.
Az 1970-es években több kisebb-nagyobb egyetemi hálózat fejezte ki szándékát, hogy csatlakozni szeretne az ARPA kísérleti hálózathoz. Kidolgoztak egy szabályrendszert, mely lehetővé tette a különböző típusú számítógépek együttműködését. Ezek a szabályok (protokollok) internetworking (röviden INTERNET) néven váltak közismertté.
Az internetre kötött számítógépek rendelkeznek egy internet címmel – IP (Internet Protocoll)

[1] Zrínyi Miklós Nemzetvédelmi Egyetem, Bolyai János Hadmérnöki Kar, Repülő és Légvédelmi Intézet, Fedélzeti Rendszerek Tanszék, okleveles mérnök alezredes, egyetemi docens H-5008 Szolnok, Pf.1., Email: szilvassy.laszlo@zmne.hu
A cikket lektorálta: Dr. Krauszné Dr. Princz Mária Debreceni Egyetem, főiskolai docens, PhD.
[2] Az azonos című előadás rövidített, írott változata
[3] Internet vagy internet. Melyik a helyes? Mindkettő. Az internet (kis kezdőbetűvel) a fizikai hálózatot jelenti, ami a számítógépekből, szerverekből, vezetékekből, összefoglaló néven a hardverből áll. Az Internet (nagy kezdőbetűvel) azt a tartalmat jelenti amit fellelhetünk a világhálón. Ezt az írásmódkülönbséget és ezáltal a tartalom és a hálózat külön elnevezését egy régebbi internetes cikkben láttam és azóta magam is így használom, mert így valóban különbséget lehet tenni írásmódban is a két fogalom között.

címmel, ami hasonlóan a telefonszámokhoz egyedileg azonosít egy számítógépet. Erre azért van szükség, hogy a hálózaton végbemenő kommunikáció során, egy bizonyos számítógépnek küldött információt csak az a gép kaphassa meg. Pl.: 193.224.76.3[4]. Az ilyen típusú azonosítókat elég nehéz lenne megjegyezni, ezért az IP címmel rendelkező számítógépekre hivatkozhatunk neve alapján is, pl.: www.zmne.hu

1.3. AZ INTERNET SZOLGÁLTATÁSAI

Az internet nem azonos a webbel, sokkal több szolgáltatása létezik, mint amit az átlag felhasználó használ/kihasznál. Ezek a következők:

- elektronikus levelezés – e-mail;
- telnet;
- ftp;
- talk;
- IRC;
- Gopher;
- WWW.

1.3.1. Telnet

A *telnet* parancs segítségével bejelentkezhetünk az interneten lévő számítógépek többségébe, ha van hozzá jogosultságunk. Pl.: a Start/Futtatás… beviteli mezőjébe beírjuk a telnet parancsot és annak a számítógépnek a nevét vagy IP címét, amelyhez csatlakozni akarunk. pl.: *telnet 193.224.76.3* vagy *telnet zmne.hu* Természetesen ehhez is, mint minden távoli számítógép eléréséhez megfelelő jogosultságok kellenek, és amikor a hálózatok biztonsága nagyon fontos tényezővé vált, csak indokolt esetben fogunk ilyen jogosultságot kapni.

1.3.2. Ftp

Ftp, mint a neve is mutatja **f**ile-**t**ransfer **p**rotocoll (fájl átviteli szabály) ezzel a paranccsal a hálózat gépei között szöveges vagy bináris állományokat (pl: képeket, hangokat, programokat, stb.) vihetünk át egyik gépről a másikra. Ezt is hasonlóan indíthatjuk, mint a telnetet, de használhatjuk pl. a TotalCommendert, vagy más ftp klienset is, amelyek kiváló csatlakozási lehetőséget biztosítanak. Természetesen ehhez is valamilyen jogosultság szükséges.
A jogosultságok lehetnek:

anonymous: kevesebb jog, jelszó (password): e-mail cím;
„user”: regisztrált felhasználó saját felhasználónév (login) saját jelszó (password).

1.3.3. Talk

Két, egymástól távoli gép felhasználójának online kommunikációját lehetővé tevő protokoll, illetve program.
Előnyei:

- nagyon gyors;
- olcsó;
- nem egyoldalú.

Hátrányai:

[4] Ha az IP címet beírjuk a böngészőnk címsorába megnyílik a www.zmne.hu oldal.

- rossz vonal esetén nagyon lassú, gyors vonal esetén pedig a gépelési sebesség szab határt a kommunikációnak;
- érzelmek kifejezése korlátozott (☺ használata).

1.3.4. IRC (*I*nternet *R*elay Chat)

Valós idejű társalgás. Internet szolgáltatás, amely személyek közti üzenetküldést tesz lehetővé, beszélgető-csoportokban.
Mindegyik csatorna nevén kívül rendelkezik egy változtatható témacímmel (topic). Az IRC hálózatokon a szerverek egymáshoz kapcsolódnak (A felhasználók előtt ez rejtve marad).
Minden felhasználót beceneve (nickname) alapján különböztet meg a rendszer.
Néhány chat-es honlap:

- chat.trefort.hu;
- chat.gyaloglo.hu;
- chat.hu.

1.3.5. Ghopher

A ’90-es évek elején a Minnesota Egyetemen (University of Minnesota) kifejlesztett rendszer. A Ghopher egy karakterorientált, menüvezérelt, információszolgáltató rendszer, melynek segítségével főleg szöveges állományokat lehet letölteni az Interneten lévő adattömegből. A WWW konkurense volt.

1.3.6. WWW (*W*orld *W*ide Web)

Röviden Web-ként nevezzük. Osztott, hipertext-alapú, multimédia képességekkel rendelkező rendszer. Általános információ lekérés, keresés eszköze.
A hipertext a szövegben elhelyezett hivatkozás (internetes kapcsolatok, linkek) közvetlen elérésére utal. A Web használatához szükség van egy grafikus felülettel rendelkező operációs rendszeren futó böngésző (browser) programra.
Home Page
Az Internet polgárai önmagukról *Home Page*-en keresztül nyújtanak információt az érdeklődők számára. Nagyon nehezen alakult ki a *Home Page* magyar megfelelője. Általában *honlap*-nak használjuk, de az angol megfelelői is közismertek *Home Page* vagy *Home Site.*

1.3.7. VoIP (Voice over IP)

Internet Protokoll feletti beszédátvitel vagy IP telefónia – a távközlés egy olyan formája, ahol a beszélgetés nem egy hagyományos telefonhálózaton, hanem az interneten vagy más IP-alapú hálózaton folyik.
Költségei tekintve jelentősen olcsóbb a hagyományos telefonálásnál. Gazdasági szakemberek véleménye szerint 1-2 éven belül jelentős felhasználói tábort hódíthat el a hagyományos szolgáltatóktól.
Legjelentősebb képviselője a Skype (www.skype.hu), Windows Live Messenger.

1.4. Veszélyek az Interneten

Az Internet azon kívül, hogy rengeteg hasznos információt tartalmaz – rengeteg haszontalan mellett – nagyon sok veszélyt is rejt magában. Óvatlan, gyakorlatlan felhasználó könnyen lehet hackerek áldozata. Éppen ezért nagyon fontos, hogy alapszinten minden internet fel-

használó tisztában legyen azokkal a veszélyekkel, ami az interneten érheti őket.
Veszélyek az Interneten:

- kártékony programok;
- jelszófeltörés;
- elektronikus lehallgatás;
- hackertámadás;
- kéretlen e-mail üzenetek;
- adathalászat és az elektronikus személyazonosság ellopása;
- megtévesztés.

1.4.1. 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.

1.4.1.1. Vírusok és férgek

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

- Vírusok: midig valamilyen gazdaprogramhoz kapcsolható, fájlról fájlra terjed. Lehet:
  - viszonylag ártalmatlan;
  - komoly károkat okozó.
- Férgek: nincsen szüksége semmilyen gazdaprogramra, gépről gépre terjed.

1.4.1.2. 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 (port-ot) 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.

1.4.1.3. 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) letörlése a számítógépről, vagy a modem telefonos kapcsolatánál a tárcsázandó telefonszám átírása, valamilyen emelt díjas számra.

1.4.1.4. 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.

1.4.2. Jelszófeltörés

Egy számítógépes rendszerbe a legkönnyebben egy érvényes felhasználónév és jelszó kombináci-

ójával lehet bejutni. Ha már bent vagyunk rendelkezünk a felhasználó minden jogosultságával.

Jelszó feltörési módszerek:

- személyes információk alapján;
- szótáras támadás;
- nyers erő módszere;
- 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 szoftver létezik, néhányuk ráadásul ingyenes is. Ezek a szoftverek elsősorban a hálózati diagnosztikai célokra, hálózati hibák felderítésére készültek, de ha rossz kezekbe kerül akkor a hálózaton elfogott csomagokból bizalmas információk, legrosszabb esetben jelszavak is visszafejthetőké válhatnak.

1.4.3. 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.

1.4.4. 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.

1.4.5. 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.

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

Kéretlen e-mailokat 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.

1.4.7. 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.

1.4.8. 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 telefonos megkeresés során megadni bizalmas adatait.

Ilyen esetben legyünk picit bizalmatlanabbak!

1.5. VÉDEKEZÉS

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

1.5.1. Víruskeresők

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

Néhány víruskereső program:

- ✓ Microsoft Security Essential;
- ✓ Norton Antivirus;
- ✓ Kaspersky;
- ✓ McAffe;
- ✓ AVG;
- ✓ NOD32;
- ✓ Panda;
- ✓ Avira.

1.5.2. 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.

- ✓ AdAware;
- ✓ Spybot.

1.5.3. Tűzfalak

A Windows XP később a Vista majd a Windows 7 tűzfala nagyon dicséretes kezdeményezés, mert operációs rendszerbe integrálva ad egy védelmi lehetőséget. Minimális beállításokkal rendelkezik. Windows XP esetében csak a 2. javítócsomagban található meg, de otthoni felhasználóknak melegen ajánlott legalább ezt bekapcsolni.

Egyéb önálló tűzfalak:

- ✓ ZoneAlarm
- ✓ Kerio

- ✓ Comodo
- ✓ Sygate

HIVATKOZÁSOK

[1] The Information Workers' Security Handbook url: http://www.google.hu/url?sa=t&source=web&cd=1&ved=0CBUQFjAA&url=http%3A%2F%2Fwww.netrend.hu%2Fapic%2FInformationWorkersHandbook.doc&rct=j&q=biztons%C3%A1gi%20k%C3%A9zik%C3%B6nyv%20infomunk%C3%A1soknak&ei=zg2zTKb0MsLLswaBoezADQ&usg=AFQjCNHPiV4lb8EKrfRU0uS6fgkYfkCv1w&sig2=TKYd6Y6INKw7A0q3bGOlOA&cad=rja