Orczán Zsolt
ELTE TOFK
orczanz@kincsem.tofk.elte.hu

A DIGITÁLIS TUDÁS ÉS A SZEMÉLYES ADATOK VÉDELMÉNEK OKTATÁSI KÉRDÉSEI

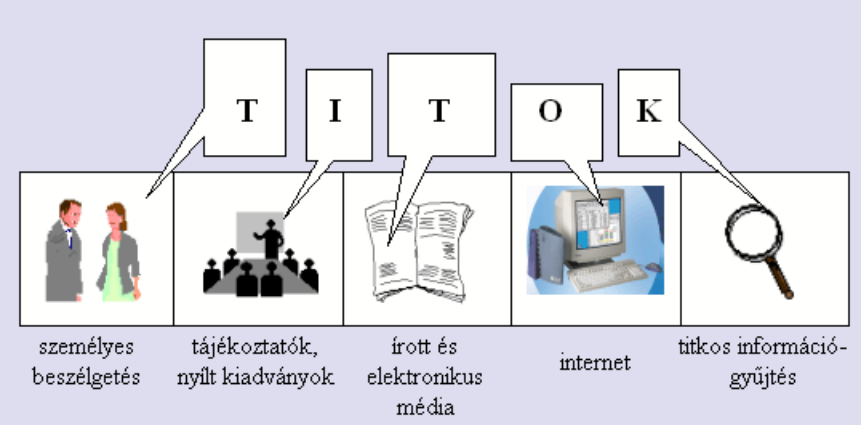
Mondanivalómat egy rövid idézettel kezdem Arthur Orwell 1949-ben megjelent "Ezerkilencszáznyolcvannégy" című regényéből. *„Az embernek annak tudatában kellett élnie, hogy lehallgattak minden hangot, amit kiadott, s a sötétséget leszámítva minden mozdulatát megfigyelték."*

Utópia vagy valóság a térfigyelő kamerák törvénytelen elhelyezése? Elektronikus levelek törvénytelen olvasása, internet forgalmunk nyomkövetése például azért, hogy célirányos reklámcélpontok legyünk? Egyszerre sok egyéb rosszírű kérdés merülhet fel bennünk:

– Mi történik körülöttünk? – Felkészülés a „Tudás alapú információs társadalomra" és felelőtlen gyerekek SPAM- és vírusáradat játéka, vagy esetleg „információs fegyverkezés", amellyel észrevétlenül lehet láthatatlan rabszolgaságba sodorni emberek millióit?

Az információk gyűjtésének sémája sokrétű, az üzleti hírszerzés, előnyszerzés, bankszámla-leszívás, számítógépes adatok meghamisítása, mind-mind előfordulhatnak.

(Forrás: Nemzetbiztonsági Hivatal)



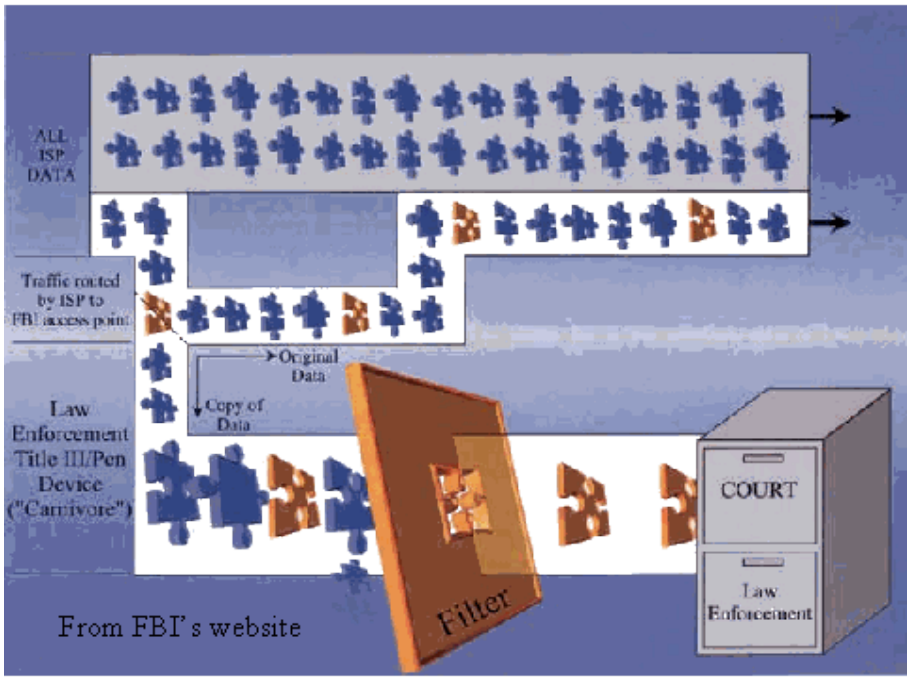
1. ábra: Kommunikációs veszélyforrások

Tekintsük át a veszélyforrásokat, amelyekkel kiszolgáltatottá válhatunk, majd azt a néhány megoldást, amellyel védekezhetünk (*1. ábra*).

Veszélyforrások

Sajnos egyre ismerősebbé kezdenek válni mindannyiunk számára az olyan különleges kifejezések, betűszavak, mint a következők. Echelon, Carnivore, Altivore, DDOS, Spyvare, Spybot, Keylogger, Reklámrobot, Pásztázó szoftver, Szkript kölykök, Trójai program, Cookie, Sniffer, Vírus, Hacker, Cracker, Ping, Web-bug, Web-bogár, Keylogger, hálózat szkennelés, Telnet, Ftp, Hátsó kapu, Smurf, Spam, Email hoax.

Ezek közül a Carnivore – vagy az Altivore – működési ábrájának bemutatásával jól láthatóvá tesszük az internet hálózat megfigyelését (*2. ábra*). Az Altivore szabadon letölthető program. Szerverre telepítve törvénytelen megfigyelés végezhető vele. Természetes hasonló programok is könnyen elkészíthetők.



2. ábra: Az internet-hálózat megfigyelési sémája (Forrás: FBI)

Védekezési lehetőségek

Szerencsére a védekezési lehetőségek köre is egyre gyarapszik, bár még nem túl sokan élünk. velük. Ilyen lehetőségek: a jó jelszó, a tűzfal, SSL, SSH, PGP, vírusirtók, SPAM detektor, a digitális aláírás felhasználó oldali alkalmazása, a szerverek hitelességének ellenőrzése. Ezek mellet a legfontosabb a felhasználói adatvédelmi tudás és ennek alkalmazása.

Hallgatóink körében kérdőíves felmérést végeztünk a kommunikációs veszélyekről és elhárításukról meglévő ismereteik feltérképezésére. 80 másodéves hallgató találkozhatott a következő felelet-választásos kérdőívvel.

Felmérés az Internet biztonságos használatáról

- Kérem, karikázza be azt az állítást, amivel egyetért!

  Az Internet hálózaton történő levelezés, böngészés, sms küldés, „chat” stb.
  - Könnyen lehallgatható, mert az alapbeállításban semmi sincs titkosítva.
  - Csak a titkosszolgálatok tudják lehallgatni és megfigyelni azt, amit teszek.
  - Még a titkosszolgálatok sem tudják lehallgatni, megfigyelni azt, amit teszek teljesen „névtelen” tudok maradni a „net”-en.

- Kérem, karikázza be az alábbi kifejezések közül azokat, amelyekről már hallott!

vírus	pásztázó szoftver	digitális aláírás
tűzfal	szkript kölyök	hátsó kapu
trójai program	smurf	hálózat szkennelés
jelszó	Keylogger	Carnivore
DDOS	ftp	Altivore
SSL	SSH	cracker
PGP	süti (cookie)	spam
Spyware	sniffer	E-mail hoax
Reklámrobot	hacker	spybot
web-bug		

- Kérem, karikázza be az alábbi kifejezések közül azokat, amelyek a biztonságos felhasználást szolgálják!

vírus	pásztázó szoftver	digitális aláírás
tűzfal	szkript kölyök	hátsó kapu
trójai program	smurf	hálózat szkennelés
jelszó	Keylogger	Carnivore
DDOS	ftp	Altivore
SSL	SSH	cracker
PGP	süti (cookie)	spam
Spyware	sniffer	E-mail hoax
Reklámrobot	hacker	spyboot
web-bug		

- Kérem, karikázza be az alábbi kifejezések közül azokat, melyek felhasználók megfigyelésére, lehallgatására szolgálnak!

vírus	pásztázó szoftver	digitális aláírás
tűzfal	szkript kölyök	hátsó kapu
trójai program	smurf	hálózat szkennelés
jelszó	Keylogger	Carnivore
DDOS	ftp	Altivore
SSL	SSH	cracker
PGP	süti (cookie)	spam
Spyware	sniffer	E-mail hoax
Reklámrobot	hacker	spybot
Spybot	web-bug	

- Mennyire biztonságos az Interneten vásárolni?
  - Biztonságos. Nem kell félni, hogy mások a nevemben visszaéljenek.
  - Körültekintőnek kell lenni, mert már hallottam visszaélésekről, de nekem különösebb félnivalóm nincs, mert az eladó és a szolgáltató garantálja a biztonságos vásárlást.
  - Rendkívül körültekintőnek kell lenni és a gépemen több óvintézkedést, biztonsági szoftvert célszerű telepíteni.

- Ha vásárol az Interneten, milyen „bankkártyát” célszerű használni?

  a) betéti (debit) kártyát b) hitel (credit) kártyát

Felmérésünk alapján a legfontosabb tanítandó témakörök az alábbiak

(A jó jelszó és annak biztonságos használata sokat segíthet)

1. Személyes adataink tárolása a számítógépen (Ne hagyja, hogy a webböngészője megjegyezze a jelszót, hitelkártya számot és más személyes adatait.)
2. Vírusvédelem
3. Egyéni tűzfalas védekezés a hackerek és a crackerek ellen
4. E-mailek kezelése, megnyitása
5. Letöltési óvintézkedések
6. Őrizzük meg titkainkat (Magánéletét őrizze meg magának! Ne adjunk ki könnyen személyes adatokat –csevegő szoba)
7. Biztonsági másolatkészítés
8. Biztonságot ellenőrző szoftverek ismertetése (Securety Check)

És most egy idézettel zárom mondanivalómat, amellyel azt szeretném érzékeltetni, hogy az informatikai adatvédelem kérdése nem új keletű probléma, hiszen az alábbi idézetből kiderül, hogy évszázados probléma megőrizni titkainkat. Hiszen hányszor találkozunk még ma is egyéni pinkódok, jelszavak felelőtlen tárolásával. Franklin Benjamint idézve még ma is elgondolkozhatunk azon, hogy az emberi felelőtlenségnek hol a határa, ezért érdemes megszívlelni cyber biztonságunk érdekében: „Hárman akkor tudnak titkot tartani, ha közülük kettő halott.”

Végezetül csatolok egy mellékletet, amelyet kibővített formában a kar hallgatói és kollégái kapták meg. Az itt közölt változatban nem szerepel az „Információk gyűjtése” téma, mely írásom elején látható, így újfent a mellékletben nem szerepeltettem.

Melléklet

Egyéni védekezés alapjai, amire minden felhasználónak figyelnie kell

1. Biztonságos jelszóhasználat
2. Személyes adataink tárolása a számítógépen (Ne hagyja, hogy a webböngészője megjegyezze a jelszót, hitelkártya számot és más személyes adatait.)
3. Vírusvédelem
4. Egyéni tűzfalas védekezés a hackerek és a crackerek ellen
5. E-mailek kezelése, megnyitása
6. Letöltési óvintézkedések
7. Őrizzük meg titkainkat (Magánéletét őrizze meg magának! Ne adjunk ki könnyen személyes adatokat (csevegő szoba, fórum, e-mail)
8. Biztonsági másolatkészítés
9. Biztonságot ellenőrző szoftverek (Security Check) használata
10. Jelszóváltozások[*]

– A felhasználónak először a régi jelszavát kell beírnia, ha már volt neki. Ezután ennek a jelszónak a kódolt változatát összehasonlítja a tárolt jelszóval. A megfelelő jelszó beírására a felhasználónak csak egy lehetősége van.
– Miután a felhasználó beírta a jelszavát, a *passwd* megvizsgálja, hogyan rendelkezett a rendszergazda a jelszavak „szavatossági idejéről”. Amennyiben az idő nem alkalmas a jelszó megváltoztatására, passwd kilép minden változtatás nélkül.
– Ezek után a program bekéri a felhasználótól az új jelszót, majd megvizsgálja, hogy elég bonyolult-e. Általános szabályként elmondható, hogy a jelszavak jók, ha 6-8 karakterből állnak, és a következő jelkészletekből tartalmaz elemeket:
  - az ABC kis betűi
  - az ABC nagy betűi
  - számok 0 és 9 között

11. Írásjelek

– Fontos odafigyelni, hogy ne tartalmazzon az adott rendszeren használt *„erase”* és *„kill”* kódú karaktereket. A *passwd* nem fogad el nem eléggé bonyolult jelszót. Ha a jelszó elfogadható, a passwd a biztonság kedvéért még egyszer bekéri az új jelszót, és csak akkor hajtja végre a változtatást, ha a két bevitt jelszó megegyezik.

12. Tippek a felhasználói jelszavakhoz

[*] Hivatkozás: kincsem.tofk.elte.hu szerver man passwd parancsra

– Egy jelszavas rendszer biztonsága a kódolási algoritmus erősségétől és a lehetséges kulcsok számától függ. A UNIX rendszerek kódolási módja az NBS DES algoritmuson alapul, és nagyon biztonságos. A lehetséges kulcsok száma a választott jelszó véletlenszerűségén múlik. A jelszavas rendszerek feltörése legtöbbször a gondatlanul megválasztott jelszónak vagy a jelszavak cserélgetésének az eredménye. Ezen okok miatt célszerű olyan jelszót választanod, ami nem szerepel a szótárban és nem szükséges leírnod. Tipikusan rossz választás, ha valamilyen nevet, valamilyen azonosítószámot, születésnapot vagy címet használ jelszóként. Ezeket legtöbbször minden más lehetőség vizsgálata előtt kipróbálja a potenciális cracker. Igyekezzen olyan jelszót választani, ami könnyen megjegyezhető, és így nem kell leírni. Ez például úgy érhető el, hogy két rövidebb szót elválasztunk egy számmal vagy valamilyen karakterrel, például *jel@szo*. A másik módszer, hogy egy könnyen megjegyezhető mondat vagy idézet minden szavának első vagy utolsó betűjét írja egymás után. Így például a *„Morzsa kutyám hegyezd füled”* mondatból *Maqmhdfd* lesz. Feltehetőleg kevés cracker szótárában fog szerepelni ez a szó. Ennek ellenére a még nagyobb biztonság kedvéért érdemes valamilyen saját módszert kitalálni jelszavak készítésére.