ADATVÉDELEM ÉS SZERZŐI JOGOK

Adatvédelem: Miért kell adatainkat védeni? Miért van szükség törvényekre? Mitől védjük magunkat?

A számítógépes adattárolás és az Internet elterjedésével az egyes emberekről egyre több információ gyűjthető be. Gondoljuk végig, hogy milyen oldalakat látogattunk meg az elmúlt időben az Interneten! Mikor vettünk ki pénzt az automatából, mikor fizettünk a kártyával? Voltunk-e orvosnál TB kártyánkkal? stb… Ezeken a helyeken tárolják az adatainkat és információinkat. Ha ezeket az információkat összekapcsolnák, akkor mindent tudnának rólunk. Mi pedig nem tudnánk, hogy milyen információval rendelkeznek rólunk. Kiszolgáltatottak lennénk!

Az adatvédelem jogi szabályozása

Európa többi országában már az1970-es években felismerték ennek a veszélyeit és törvényekkel szabályozták az adatok védelmét. Európában elsőként Svédországban született adatvédelmi jogszabály.
Az *adatvédelem alapjait* hazánkban a Magyar Köztársaság Alkotmánya határozta meg. Az Alkotmány XII. fejezet 59. § kimondja:
(1) A Magyar Köztársaságban mindenkit megillet a jó hírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog.
Hazánkban 1992-ben hirdették ki az 1992. évi LXIII. *Személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvényt.* A törvény célja, hogy :
[1. § (1) bekezdés] személyes adataival mindenki maga rendelkezzen és a közérdekű adatokat mindenki megismerhesse.

Adatvédelmi törvény

Személyes adat bármely meghatározott természetes személlyel kapcsolatba hozható adat. Az adatból levonható, az érintettre vonatkozó következtetés.
Közérdekű adat az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységre vonatkozó, a személyes adat fogalma alá nem eső adat.

<u>Adataink nyilvántartása:</u>
Mindenki tisztában van azzal, hogy vannak olyan adatok, amiket mindenképpen nyilvántartanak. Ennek is meg vannak a törvényi feltételei. Az 1992. évi LXVI törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról szól.
2. § (1) A polgár jogosult megtiltani a róla nyilvántartott adatok kiadását.
(3) Az állami és önkormányzati szervek elsősorban a polgártól kérhetnek adatokat. A nyilvántartás szolgáltatását akkor vehetik igénybe, ha a szükséges adat a polgártól nem szerezhető be.

Milyen szervezetek látják el ezeket a feladatokat?
- Önkormányzati jegyző
- Országos Személyi Adat-és Lakcímnyilvántartó Hivatal
- Belügyminiszter

Milyen adatokat tárol a nyilvántartás?
- A nevet (családi és utónév, nőknél leánykori név)
- Magyar vagy külföldi állampolgárságot
- Születési helyet és időt, anyja nevét
- Személyazonosító jelet, lakcímet
- Halotti anyakönyvi kivonatot (halál helye, időpontja)
- Adatszolgáltatási korlátozást és tilalmat

SZERZŐI JOG

Könyvet, filmet, CD-t, vagy valamilyen programot nagyon könnyű másolni, de sok jogi problémát von maga után. Aminek az összefoglaló neve szerzői jog. Ez a törvény akadályozza és tiltja meg, hogy bizonyos adatokat ne lehessen másolni és saját nyereség céljából eladni, értékesíteni.

A szerzői jogi törvény

Magyarországon a szerzői jogokat az 1999. évi LXXVI. Törvény szabályozza. Ez a törvény védi az irodalmi, tudományos és művészeti alkotásokat. Vagyis a szoftvert is. A szerzői jog azt illeti meg, aki a művet megalkotta. S még rengeteg jog csak a szerzőt illeti meg. A törvény értelmében a számítógépes programalkotás és a hozzá tartozó dokumentáció a szoftver.

A szoftverek védelme

A szoftverek védelmére általában két lehetőség adódik. Az egyik a technikai védelem, a másik a jogi védelem.

- Technikai védelemhez tartozik az illetéktelen hozzáférés elleni védelem és a másolásvédelem.
- A jogi védelemhez tartozik a szerzői jog (copyright), és a szoftverszerződés.

A szoftverszerződésben írják le a jogszabályok által biztosított védelmi intézkedéseket. A kereskedelmi programok esetében a telepítés megkezdése előtt úgynevezett blankettaszerződést kell elfogadni. Itt az elfogadás hozza létre a felhasználói jogviszonyt. Külön érdekesség, hogy a program megvásárlásakor nem a tulajdonjogot vesszük meg, hanem az adott példány kizárólagos felhasználói jogát.

Mit tehetünk a legálisan vásárolt szoftverrel?

- Először is használhatjuk.
- Készíthetünk biztonsági másolatot a szoftverről.
- Megfigyelhetjük és tanulmányozhatjuk a szoftvert.
- A törvény azt mondja, hogy a szoftvert visszafejthetjük. De csak akkor, ha más szoftverekkel való együttműködtetés megvalósításához erre szükség van. Persze a legtöbb cég ezt tiltja a licence szerződésben.

SZOFTVER-LICENCELÉSI MÓDOK

A szoftvereket csoportosítani lehet, mégpedig aszerint, hogy a licence mennyi szabadságot ad a felhasználónak.

Kereskedelmi programok: Kereskedelmi céllal készültek, vagyis nagyon behatárolják a felhasználó lehetőségeit.

Freeware programok: Szabadon felhasználhatóak és terjeszthetőek, azaz ingyenes szoftverek. Fontos azonban, hogy visszafejtésük nem megengedett.

Shareware programok: Nagyon hasonlóak a freeware programokhoz, vagyis ingyen beszerezhetőek és terjeszthetőek. De gyakran nem működnek teljes körűen. Ugyanis a teljes programért fizetni kell, és ha nem tesszük meg, akkor néhány programindítás után nem lesz indítható.

Trial programok: Általában kipróbálásra kiadott programok, hasonló a shareware programokhoz. Fontos eltérés az, hogy nem terjeszthetők szabadon.

Félszabad szoftverek: Olyan szoftverek, amelyek kereskedelmiek, de valamilyen felhasználási célra vagy felhasználói csoportnak kedvezőbb feltételekkel kerülnek forgalomba.

Szabad szoftverek: A szabad szoftver nem összetévesztendő az ingyenessel. Ennél sokkal többet kap a felhasználó és sokkal több joggal rendelkezik.

- A program ingyenesen beszerezhető. Bármilyen formátumban (CD, Internet stb.)
- A program szabadon használható.
- A program szabadon terjeszthető.
- A forráskód megismerhető. Ebből következik, hogy a program szabadon módosítható.

A VÉDELMI RENDSZEREK

Az Internet protokollja a TCP/IP tervezésekor nem a biztonsági szempontok játszották a fő szerepet, hanem a lényeg a működőképesség volt. Sajnos az Internet világméretűvé növekedése és a szolgáltatások kiterjedése magával vonta a „bűnözés" megjelenését is. Ezért szükség van arra, hogy az Internethez kapcsolódó számítógépünket megvédjük az idegen behatolóktól. Két védekezési módszer van. A tűzfal (firewall), és a proxy szerver.

A **tűzfal** lehet egy számítógép, vagy egy program. Az otthoni számítógépünkön használhatunk tűzfal programokat, például a ZoneAlarm. (A Windows XP rendelkezik beépített tűzfallal.) A nagyobb hálózatoknál a rendszergazda feladata a tűzfal üzemeltetése. A tűzfal feladata a hálózat figyelése és szűrése. Ezzel az illetéktelen behatolások egy része lefülelhető.

A **proxy** egyrészt tűzfalszolgáltatásokat is nyújt. A másik feladata az Internet megosztása a felhasználók között. A proxy szerver, mintegy átmeneti tároló, a gyakran látogatott oldalakat tárolja. Amikor a felhasználó egy weboldalt lekér, a proxy szerver megnézi, hogy megvan-e az oldal az átmeneti tárolóban. Ha igen, akkor innen tölti be, hogy ne terhelje egy újabb letöltéssel a hálózat forgalmát.

Biztonság és adatvédelem (e-maileknél)

A legfontosabb, hogy az elektronikus levelezés nem biztonságos! Több bizonytalansági tényező van. Nem biztos, hogy a levél feladójaként szereplő név és a személy azonos. A levelünk olyan, mint egy rendes postai levelező lap. Tartalmát el lehet olvasni és módosítani is lehet. Vagyis az olvasó nem lehet biztos abban, hogy a levél tartalma nem változott az útja során. Ma már vannak ilyen módszerek ezekkel a tényezőkkel szemben. Két módszert ismerünk. A digitális aláírás és a kétkulcsos módszer.

Ha **digitális aláírással** van ellátva egy levél, akkor biztosak lehetünk benne, hogy a levél feladója ténylegesen az a személy, aki a levelet küldte. Sajnos a digitális aláírás nem biztosítja, hogy a szervereken keresztül nem módosult a levél, vagy nem olvasták.

A levelek védelméhez használnak titkosításokat. Ezek közül elterjedt a **kétkulcsos módszer**. Ennek lényege, hogy a felhasználónak két kulcsa van, egy nyilvános és egy titkos.

- A nyilvános kulcsot mindenki ismerheti, sőt akinek levelet írunk, annak a nyilvános kulcsával titkosítjuk a levelet.
- A titkos kulcsolt csak a tulajdonosa ismerheti, és ezzel fejtheti meg a titkosított leveleket.

A kulcspárokat, vagy ahogy a Windowsnál nevezik, biztonsági tanúsítványokat a hitelesítés-szolgáltatónál kell beszerezni.

E-mail vírus

Az Internet elterjedésével vírusok új és újabb generációja jelenet meg, amelyek képesek voltak a hálózaton keresztülhaladni és a leveleinkbe férkőzni. Az e-mail vírusok felismerhetőek arról, hogy mellékletet tartalmaznak. A melléklet programot vagy makrót tartalmaz, melyet megnyitva aktivizáljuk a vírust. Ezért fontos, hogy az ismeretlen címről jövő vagy a gyanús mellékletet tartalmazó leveleket megnyitás nélkül töröljük! Másrészt alkalmazzuk vírusirtó programot, mert ezek felismerik és kiiktatják ezeket a vírusokat