**Biztonság az Interneten: Windows (1.rész)**

Windows, mint hálózati operációs rendszer - biztonsági mentés - jelszavak.

Az itt következők tanácsot próbálnak adni Windows operációs rendszert futtató személyi számítógépek Internetes biztonságának növeléséhez (Ha hálózatba kötött géppel van dolgunk (vagy akár egy kisebb otthoni hálózatot üzemeltetünk) eltérhetnek a beállítások az itt leírtaktól. Nagyobb hálózat esetén tanácskozzunk a hálózat rendszergazdájával. Nagy valószínűséggel örülni fog, hogy rajta kívül valaki érdeklődik a hálózat biztonsága iránt!). A Windows (3.1, 3.11, 95, 98, tulajdonképpen a ME is) alapvetően egy klasszikus PC környezetből származó operációs rendszerre, az MS-DOS-ra alapul. Ennek az operációs rendszernek, mint az a nevéből is látszik (Disk Operation System - lemezműködtető rendszer) alapvetően az a dolga, hogy a programok futtatásán kívül állományműveleteket végezzen egy (!) gépen. Megalkotásakor az Internet és a számítógépes hálózatok működtetése még csak az úgynevezett nagygépeken (főként katonai és egyetemi) és az ezekhez kapcsolódó terminálokon keresztül volt lehetséges.

A hálózati rendszereknek alapvető tulajdonsága, hogy csak bizonyos jogosultságok (felhasználói nevek és jelszavak) segítségével lehet adatokhoz és a rendszerhez hozzáférni. Ez természetesen más állományrendszert kíván, ahol alapvető kérdés a biztonság.

Az igényre való tekintettel ma már a Windows is képes az Internettel megbirkózni (sőt, elterjedtsége folytán a www tartalom legnagyobb "fogyasztója"), hiszen az internetes szabványok leprogramozhatóak alatta. Mindenesetre az Internetet nem Windowsra tervezték! A Linuxszal foglalkozó részben láthatjuk, hogy az állományrendszer és a jogosultságok tisztázása hogyan működik egy hálózati alkalmazásra is tervezett operációs rendszernél. A Windowsról, mint hálózatot támogató operációs rendszerről tudni kell, hogy csak bizonyos szabályok betartása mellett érdemes használni, ha biztonságban szeretnénk tudni adatainkat (ez természetesen minden operációs rendszerre igaz, csak többnyire máshol "magától értetődő"). Miért fontos ez? Nézzünk körül a gépünkön, hogy milyen állományok találhatóak rajta: komoly munkával megalkotott dokumentumaink, adatbázisaink, személyes és üzleti leveleink, adataink (szinte mindenki az önéletrajzával kezdi a szövegszerkesztést), képek a családról, ismerősökről, magának az internet hozzáférésünknek az adatai, netalán bankkártyánk, mobiltelefonunk, lakásriasztónk, ismerőseink adatai (ha elfelejtem, csak megnézem a megfelelő állományt). Egy ilyen gép mellé nem szívesen ültetünk le egy vadidegent. Amíg MS-DOS és Internet nélküli világ volt, addig ez csak akkor valósulhatott meg, ha fizikailag valaki leült a gép mellé és bekapcsolta. Ma az Internet használatával mindenhol "ismerik a gépünket".

Természetesen nem kell a ló másik oldalára átesni és a számítógépet a páncélszekrényben, kihúzott táp és hálózati kábellel (modemmel) tartani. Ahhoz, hogy használni tudjuk az Internetet, a gépünknek rendelkeznie kell egy azonosítóval, ami alapján megtalálnak a kérésünkre számítógépünk felé érkező adatok (ez az úgynevezett IP cím). Nem mindegy azonban, hogy ezen kívül milyen adatok jutnak el másokhoz, esetleg illetéktelenekhez.

**Visszatérve a Windowshoz.**

Az MS-DOS, csakúgy, mint a Microsoft egyéb operációs rendszerei zárt forráskódúak, azaz, ha a felhasználó ilyen terméket akar használni a számítógépén, rábízza magát a program (operációs rendszer) készítőjére, fejlesztőjére, nem tudja átírni, saját igényéhez igazítani azt egy bizonyos ponton túl (ilyen főként a kernel, azaz az operációs rendszernek, mint szoftvernek a hardver elemekkel való kapcsolattartásért felelős része). Ez bizonyos szempontból nagyon kényelmes: nem kell érteni a programozáshoz, az operációs rendszer mélyebb ismeretéhez, sőt a DOS-szal ellentétben a parancsszavakhoz sem, elég az egeret mozgatni és klikkelni. Más részről viszont nagy gond: egyes működési hibák sokkal nehezebben látnak napvilágot, a javításuk több időt vesz igénybe, és a kényelmes felhasználó a biztonság illúziójába ringathatja magát, ha nem azzal tölti az idejét, hogy ezekre a hibákra vadászik és igyekszik tenni ellenük.

**Biztonsági mentés**

Mindenki tisztában van a format c: paranccsal és senki nem zárja az előbbieket Enterrel egy jól működő, adatokkal telezsúfolt gépen (Windowsban elég néhány figyelmetlen klikkelés). De biztos mindenki ismer olyanokat, akiknek ez sikerült. Más módokon is lehet katasztrofális adatvesztést produkálni, például ha tartjuk is magunkat ahhoz, hogy a fenti parancsot ne adjuk ki, a merevlemez mechanikája vagy lemezeinek mágneses vagy fizikai rétege is megadhatja magát, áramszünet, feszültségingadozás hatására "megsülhet" a gépünk, vagy olyan vírust sikerül összeszedni, ami visszavonhatatlanul károsítja állományainkat. Esetleg úgy betelik a gépünk, hogy már újraindítani sem tudjuk. Teendőnk az archiválás. Ma már anyagilag is elérhetőek azok mentési technikák, amelyekkel ezt hatékonyan megtehetjük (cserélhető merevlemez, CD író, Zip lemez, kazettás egység, helyi hálózati szerver). Végső megoldásként a kislemezes egység is szóba jöhet, bár kapacitása és strapabírása nem mindig elég. Célszerű többfajta módszert párhuzamosan használni. Vegyük figyelembe, hogy ezek a módszerek (és ez főleg a kislemezes egységre érvényes) nem örökéletűek (pl. lemezeket ne tároljunk a monitor tetején, nehogy átmágneseződjenek). Időnként vizsgáljuk felül a mentett állományainkat. A legjobb megoldás, ha tervezünk egy mentési stratégiát (pl. minden hónapban, második hónapban, nagyobb munkák után, stb.) és ez alapján járunk el.

**Mentendő anyagok:**

*Dokumentumok.*

Ez Windows alatt, ha használjuk a Dokumentumok mappát, egyszerű: ezt a mappát kell menteni adott időközönként. Egyébként azokat a könyvtárat, vagy állományokat, amiket használunk.

*Levelezés.*

Nézzünk utána, hogy a levelező programunk milyen állományokban tárolja a leveleink tartalmát. Ezeket az állományokat (vagy könyvtárat) mentsük. Ha szükség van rá, ezek az állományok visszamásolhatóak (importálhatóak) a mentett állományokból.

*Személyes dokumentumok.*

Ha a bankkártyánk száma vagy jelszavaink megtalálhatóak a gépünkben inkább külön adathordozón tartsuk ezeket, a gép merevlemezéről töröljük. A lemezt tartsuk biztonságos, mások által hozzá nem férhető helyen.

*Meghajtóprogramok.*

Ezek az állományok felelősek a géphez csatlakoztatott "vasak" működéséért. Alapvetően nem a biztonsági témához tartozó állományok, de egy vírusfertőzés helyreállítása után azért jól jöhetnek Általában a Windows/System könyvtárban csücsülnek, sok más programmal együtt. Kicsit több hozzáértést és figyelmet igényel, de érdemes ezeket az állományokat is menteni, legalább egyszer, főként, ha "jól belőtt" gépről van szó. A Windows Sysbackup könyvtárában is általában megtalálhatóak, általában dll vagy vxd kiterjesztéssel. A Beállítások(Settings)/Vezérlőpult(Controll Panel)/Rendszer(System) alatt az Eszközkezelő(Device Manager) fül alatt az egyes eszközökre kattintva, annak Tulajdonságát(Properties) megtekintve a Meghajtó(Driver) fülön tekinthetjük meg a Meghajtó részletei(Driver Files Details) gomb megnyomásával (jó bonyolult, de nem megijedni), hogy pontosan milyen állományokról van szó (a System könyvtárban nagyon sok más dolog is megtalálható).

*Rendszerleíró adatbázis.*

A Windows rendelkezik egy úgynevezett Registry-vel. System.dat néven találjuk meg a Windows könyvtárban (mellé vehetjük a User.dat-ot is). Ezt is mentsük, a win.ini és a system.ini állományokkal együtt (néhány vírus szeret ezekbe betelepülni, sok munkától kímélhetjük meg magunkat, ha egy rendszerösszeomlás után ezek kéznél vannak). Ezeket érdemes dátum szerint és gyakran menteni, mert napi programjaink is módosítják, módosíthatják. A Sysbackup könyvtárban szintén megtalálhatóak, elvileg frissülnek is itt, de ne feledkezzünk meg róluk.

Akik megengedhetik maguknak, egy cserélhető merevlemezt építhetnek a gépbe a dokumentumaik számára, a programokat tartalmazó mellé. Internetre csatlakozáskor az előbbit el kell távolítani a gépből, lecsatlakozáskor visszatenni és az Internetről letöltött állományokat megfelelő vírusellenőrzés után erre másolni. Kissé macerás, de az illetéktelen Internetes kutakodók ellen elég jó védelmet nyújt. A levelezőprogram viszont csak sok másolgatás és odafigyelés árán barátkoztatható össze vele.

Mindenképpen érdemes egy vírusmentes kislemezből (vagy ha CD-ről is tudjuk a gépet indítani, akár abból, erre aztán ráfér víruskeresőtől kezdve bármi) Indítólemezt (Startup Disk) készíteni, hogy Windows nélkül tudjunk állományműveleteket végezni. A rendszerállományokat érintő vírusfertőzés, de más olyan rendszerösszeomlás esetén, amikor károsodnak az operációs rendszer részei ez elengedhetetlen, ilyenkor vissza tudjuk másolni a biztonsági mentés állományait (károsodott rendszer esetén csak így, esetleg a Windows Biztonsági módjából (Safe Mode) tudunk bármit is tenni). Vírusfertőzés gyanúja esetén ilyenkor kezdjünk víruskereső futtatásával! Rendszerlemezt a Beállítások (Settings)/Vezérlőpult (Controll Panel)/Programok hozzáadása, eltávolítása (Add, Remove Programs) Rendszerlemez (Startup Disk) fülén tudunk készíteni, vagy egy format a: /s parancs után, amennyiben szükséges a CD meghajtóprogramok felmásolásával. A rendszerlemez készítésénél fontos, hogy teljesen vírusmentes legyen, akkor járunk el tehát helyesen, ha közvetlenül az operációs rendszer üres gépre telepítése után (mikor egyébként is felajánlja rendszerünk) elkészítjük, lehetőleg gyári, frissen kibontott lemezre.

**Jelszavak**

Az Interneten akkor tudunk hozzáférni bármihez, ha ahhoz megfelelő jogosultságunk van. A honlapokat azért tudjuk megnézni, mert a távoli szervert üzemeltetető beállította a látható, letölthető állományokon azt, hogy a világon bárki megnézhesse (letölthesse) őket. Ezen túlmenően nem tudunk vele mit csinálni (módosítani, törölni). Azért ez nem ilyen egyszerű (például ott vannak az úgynevezett interaktív oldalak, űrlapfeldolgozó alkalmazások, számlálók, de erre itt nem térünk ki), viszont főképpen ezt használjuk.

Más a helyzet, ha olyan erőforrást akarunk használni, ami jelszót, külön jogosultságot igényel (ilyen tulajdonképpen maga az Internet hozzáférés). Ezt egy felhasználói név, valamint egy hozzá tartozó jelszó birtokában tehetjük ezt meg. A felhasználói nevet általában nem is akarjuk titokban tartani (legalábbis a szolgáltatónk felé), a jelszavakkal viszont körültekintően bánjunk. A jelszavaknak alapvető fontosságuk van az Interneten és tartozik hozzájuk néhány szabály.

A jelszónak megfelelő hosszúságúnak kell lennie (rendszere válogatja, általában minimum hat karakter). Ne legyen értelmes szó. Számokból, betűkből (nagy és kisbetű is) és speciális karakterekből áll, keverve (nem felrázva - egy titkos ügynök azért tud valamit biztonság terén). Soha ne legyen a jelszavunk a felhasználói név. Ne adjuk meg jelszónak a születési dátumunkat, kutyánk nevét és hasonló, "triviális" jelsorokat. Az internetes illegális tevékenység nagy részéért az ilyen jelszavak a felelősek!

A jelszavak kódolása minden operációs rendszer része, így azokat elviekben a rendszeradminisztrátorok, rendszergazdák sem ismerik. Vannak módok viszont, hogy a jelszavunk kitudódjon, ha rosszul kezeljük őket (esetleg annak a rendszernek az adminisztrátora hibázik a beállítások során, ahol a jelszavunk érvényes). Ilyenkor maga a jelszó, vagy a kódolt formája válik elérhetővé az adott gépbe betörő kalóz számára. Utóbbi esetben a jelszó hosszabb időt (számítógépes kapacitástól függően) kívánó procedúrával (kódtörés, megfelelő szoftver segítségével) feltörhető.

A jelszavainkat rendszeresen változtassuk meg. Rendszergazdák havonta legalább egyszer változtatnak jelszót, nekünk ennél kevesebb is elég, de ne mulasszuk el (például fél évenként). A megváltoztatott jelszónak ne legyen köze az eredetihez (Gipsz Jakab például a gipszj felhasználó név mellé a gipszjakab jelszót adta meg - ez magában egy meggondolatlan cselekedet volt - és később ezt gipszjakab1-re módosította - meglehetősen balgán járt el).

Egyes rendszerek figyelmeztetnek, ha nem a fentieknek megfelelően cselekszünk, de nem mindegyik!

Jelszót akkor is érdemes változtatni, ha gyanúsan több áll a számlánkon, mint amennyit valóban használtuk az adott szolgáltatást. Ne legyünk restek ilyenkor a szolgáltató rendszergazdájával is felvenni a kapcsolatot.

Inkább kerüljük, hogy leírjuk a jelszavunkat. Ha mégis erre van szükség - főleg ha ritkán használtról van szó - írjuk le, de semmiképpen ne járkáljuk a homlokunkra tetovált jelszóval. Szóval jól rejtsük el, ha le kell írni a jelszót. Gyakori hiba, hogy a jelszót kis öntapadós papíron a monitorra teszik. Ez csak akkor megengedhető, ha biztos, hogy nem látja senki.

Ne felejtsük el, hogy a Windows állományaihoz bárki hozzáfér, aki a gép mögött ül. Léteznek olyan programok, amelyek jelszóval védik le az általunk kiválasztott állományokat. Főként olyan gépnél ajánlott, amit többen használnak, de legtöbbször ez megtakarítható.

A Windows szereti a kényelmet, ezért felajánlja általában a jelszavak megjegyzését. Ne engedjük meg neki (vegyük csak azt az esetet, hogy a gépet fizikailag ellopják), inkább gépeljünk egy kicsit többet.