

10 Holtbiztos tipp a tökéletes vírusvédelemért



1. tipp - Az operációs rendszer

Bevezető

Üdvözöllek a felelősséggel gondolkodó felhasználók csapatában!

Egy nagyon kemény és markáns megállapítással szeretném kezdeni a felvezetést, már csak azért is, mert ha most sikerül Téged meghökkentenem, akkor jó eséllyel végig fogod venni az anyagot, és soha többé nem fog az egyik legkényelmesebb megoldás hiú reményekkel kecsegtetni, ezáltal semmi nem fogja elterelni a figyelmedet a lényegről.

Íme az általam tett egyik legfontosabb megállapítás: **a vírusvédelmi szoftverek csupán 20%-át jelentik a védelemnek, a maradék 80% a felhasználón múlik.**

Mondok egy példát: egy ismerős fiatal vállalkozó, aki már végigküzdötte magát ezen az anyagon (igen, nem egyszerű eset ezt átvenni, de nagyon megéri, majd meglátod), boldogan dolgozott a laptopján, mert tudta, semmiféle gond nem érheti ezek után. Nem is volt soha semmi problémája. A vírusirtója az egyik legjobb volt, legális szoftverei voltak a gépén, a frissítéseket mindig telepítette, és hasonló alapvető dolgok.

Egy pár hónap után új gépet vett, és a laptopját kölcsön adta egy rokonnak (miután átmentett minden adatot, természetesen). Nos, nem csalás, nem ámítás, az a laptop, ami az ő gondviselő kezei között soha egyetlen vírust sem kapott, az ismerősnél használva, pár nap alatt teljesen összeomlott!

Megszámlálhatatlan vírus, trójai, kémprogram, és egyéb nagyon durva, leirthatatlan kártevők garmadája telítette a rendszert, pár nap alatt!

De ez még semmi, ugyanis most jön a lényeg: a laptopon ott maradt az ismerősöm által eredetileg használt legális vírusirtó, a legális szoftverek, tehát minden, amiről azt hinnénk, hogy kizárólag ezek számítanak valamit a vírusvédelemben.

Nos, ezek járulnak hozzá a legkevésbé a védelemhez. Elég csak a felhasználót lecserélni, és máris összeomlik minden, pillanatok alatt használhatatlanná válik a számítógép, mert nem az gondozza (nem véletlenül használom ezt a szót!), aki addig...

Érted már? Minimális védelmet nyújt egy tudatlan kézben a világ leghíresebb vírusirtója is. Lehet a gyártóknak versenyezniük, kihozhatják a legújabb fejlesztéseket, küzdhetnek nap mint nap a maffiával, hol az egyik, hol a másik kerekedve felül, de a felhasználó marad a kulcsfontosságú tényező.

Igazság szerint, számomra, mint bennfentesnek, úgy tűnik, hogy a vírusirtó gyártók, fejlesztők, a felhasználói tényezőt mintegy menekülési útvonalat tartanak meg. Tényleg szívüket-lelküket beleteszik a szoftverek fejlesztésébe, de tisztában vannak azzal, hogy ez még csak egy kis szelet a tortának, és ha valami nagy katasztrófa történne, akkor még mindig ott marad a felhasználó,

akire lehet mutogatni. Én utálnám, ha engem okolnának. Te hogy vagy ezzel?

A 10 Holtbiztos tippben azokat a lépéseket, trükköket, tippeket fogjuk végigvenni, amik egy csapásra, és örökre megkímélnék Téged a vírusok problémájától. Igen, ezt a meccset örökre lehet tudni, én például már évek óta nem láttam vírust közelről. Pedig kimondottan vírusos oldalakat szoktam megnézni, a forráskódjukban turkálni, mikor megkérnek, hogy segítsék a vírusos oldalakat helyreállítani.

A könyv végére azt fogod érezni, hogy néha csak egy hajszal választott el attól, hogy jól csináld a dolgokat, de ez a számítástechnika: nagyon sok mindent ráérzés alapján szinte jól csinálunk, de a tökéletességhez az is kell, hogy ezt rendszerbe foglaljuk. Erről szól ez a könyv, és arról, hogyan tarthatod a számítógépedet és az adataidat maximális biztonságban a vírusok szeme elől alaposan elrejtve.

Azt szeretném kiemelni, hogy természetesen nem elég tudnod a dolgokról, trükkökről, tényekről, ezeket használnod is kell. Igen, kell, és hidd el, nem lesz bonyolult, mert mindent leírtam, kifejettem részletesen, tehát nem kell még napokig elmélkedned, hogy hogyan ültess át a gyakorlatba. A számítógépek számítógépek a világ minden táján, a felhasználók pedig felhasználók akkor is, ha közben még tanulnak, vagy éppen nyugdíjasok, esetleg céget vezetnek.

Vidi Rita

Vírus Kommandó

A 10 Holtbiztos tipp kifejlesztője

Első fejezet: az operációs rendszer



Lehet, hogy meglepetésként fog érni, de a védelem az operációs rendszernél kezdődik, és most kimondottan a Windows operációs rendszerekről fogok beszélni, egy rövid bekezdés erejéig érintve a Linuxot is.

Az operációs rendszer még véletlenül sem azoknak a csillogó-villogó, hasznos alkalmazásoknak a gyűjteménye, amikkel például leveleket írsz, szöveget szerkesztesz, böngészel, videózol. Az operációs rendszer a hardvereidet kezeli, és egy összekötő kapocs a többi alkalmazással. Ha az operációs rendszered labilis,

illegális, rosszul működik, akkor semmi sem lesz biztonságos, megbízható, és jól működő a gépeden. Minden egyes alkalommal, amikor egy rosszul feltelepített, hardvereket nem támogató operációs rendszert indítasz el, akkor ott lebeg a fejed fölött az összeomlás lehetősége. Ilyenkor csak a vak szerencse vezérli a számítógépedet.

Hogyan tud rosszul működni a Windows? Hát nem ugyanúgy kell telepíteni mindet?

Hát nem. A Windows **telepítéssel kezdődik** a dolog, de egyáltalán nem fejeződik be itt, és már magánál a telepítésnél nagy hibákat lehet elkövetni, már a legelső telepítésnél is! (Amikor még szó sincs adatvesztésről.)

Teszem azt, megveszel egy új számítógépet, hozzá egy legális Windows Vistát, feltelepítteted, aztán örülsz. De nem sokáig. A Windows telepítés közben oda kell figyelned arra, hogy több partíció legyen létrehozva, tehát a merevlemez több – legalább kettő – felé kell osztani. Az első, a C: meghajtó lesz a rendszeré, a Windows ide települ. A további partíciókat pedig adattárolásra kell használnod.

A particionálás trükkjével máris elindítod a gépedet a hosszútávon vírusmentes életvitel irányába. Ha anno, a Windows telepítésekor elmaradt a particionálás, tehát kizárólag csak egy meghajtó/helyi lemez található a gépeden, akkor is áll még pár lehetőség előtted:

1. Új merevlemez vásárlása, gépbe helyezése, adatok számára használatba vétele.
2. Külső merevlemez vásárlása, USB-csatlakozón keresztül a géphez csatlakoztatni, és minden adatot ide menteni.
3. Utólagos particionálás (ezt nem ajánlom, csak szakembereknek, mert az adatokra óriási veszély leselkedik ilyenkor, sőt, az egész merevlemezre).
4. Nem csinálsz semmit, viszont elkötelezed magadat arra nézve, hogy az összes többi tippet szigorúan betartod!

Egy operációs rendszer nem nagy veszteség. Ha összeomlik, újra kell telepíteni és kész. Az persze hozzá tartozik, hogy az újratelepített operációs rendszer mellé még fel kell telepíteni minden egyéb alkalmazást, szoftvert is, mert azok is odavesznek ilyenkor. Ezeknek a kis alkalmazásoknak, fontos programoknak a telepítése, beállítása viszont akár napokig is eltarthat, mert hiszen az a cél, hogy minden ugyanolyan flottul menjen, mint előtte. Nem csodálom, hogy a legtöbb számítógépnél maximum két évente egyszer szánják rá magukat a felhasználók az újratelepítésre, mert egyszerűen akkora kaliberű feladat újra felépíteni a rendszert a nulláról. Erről majd lesz egy anyagom hamarosan, ezzel töredékére le lehet majd rövidíteni az újratelepítés folyamatát.

Ami nagy veszteség, azok az adatok (és a beállítások, mint ahogy fentebb kifejtettem). Ha távol tárolod az adatokat a rendszertől, akkor egy Windows összeomlás esetén is nyugodt maradhatsz, mert minden fontos dolgod megmarad a másik partíción. Tehát erre jó a külön partíció, külön merevlemez.

Ha csak egy partíciód van, tehát a Sajátgépben, vagy a fájlmenedzselő Total Commanderben csak egyetlen meghajtót látsz (C:), akkor kétszer jobban oda kell figyelned a vírusvédelemre, és kétszer felelősebben kell viselkedned. A továbbiakban erre konkrét tanácsokat kapsz majd.

Egy rövidke kitérő a nyílt forráskód felé



Mielőtt még a konkrét Windows témára kanyarodnánk, teszek egy kis kitérőt a Linux felé. A Linux klasszisokkal biztonságosabbnak tekinthető most, mint amilyen bármelyik Windows. Csak nemrég kezdtem megismerkedni a szabad szoftver mozgalommal, a nyílt forráskódú operációs rendszerekkel, holott évek óta környékezem a témát, de mindig volt valami fontosabb dolog, ami miatt mai napig Windows felhasználónak számítok én is.

De nagyon jó hírem van: a Linux szinte ugyanolyan hardvertámogatással bír már, mint a Windows – ez volt az elterjedésének legnagyobb gátja, illetve a marketing tökéletlensége – tehát egy otthoni felhasználó számára is igazi alternatívává lépett elő.

A Linux operációs rendszerek működési elve picit másabb, mint a Windows-é. Úgy fogalmaznám meg egyszerűen, hogy amíg a Windows-okban alapértelmezetten mindent szabad, addig a Linux úgy van megcsinálva, hogy benne alapértelmezetten mindent NEMszabad. Óriási különbség, ha jól belegondolsz, hiszen a Linuxon egyszerűen nem tudnak elindulni maguktól a vírusok. Márpedig a vírusok egyik legfontosabb ismérve az, hogy önműködőek, és

önszorzódóak. Linuxon ez lehetetlen.

Az összes Linuxra írt vírus azon az elven szeretne elterjedni, hogy átveri a felhasználót. Ezért persze van néhány Linux vírus is, de nem milliányi, mint a Windowsnál. Így Linuxra nem is kell vírusirtó például (máris meg van spórolva egy csomó pénz).

Viszont Linuxot használni az üzleti életben munkaállomásként, eddig nem volt egy leányálom. Nem szerette a nyomtatókat, egyes hardvereket, tehát több kárt csinált, mint hasznot, így még mindig nem terjedt el, holott óriási ütemben fejlődik. Leginkább szerverekként, fájl tárolókként használják, ahova nem kell semmi különleges hardver, periféria.

Én elköteleztem magam az mellett, hogy a vírusvédelem zászlaja alatt minden, számítógépet használó felhasználóval és vállalkozóval meg fogom ismertetni a Linux előnyeit, sőt, én magam is átállok, amint elkészül az összes Windows-os oktató anyagom. A tökéletes vírusvédelemhez hozzá tartozik a Windows mentes operációs rendszer sajnos, de amíg ez megvalósul, amíg ez elterjed, addig kénytelenek vagyunk azzal főzni, amink van.

Az áradozás után jöjjön a **Linux hátránya vírusvédelem szempontjából**, ami mai napig probléma:

Ugyanis attól, hogy a fertőzött állományokat Linux alapokon nem lehet lefuttatni, attól még tárolni a vírusos állományokat, fájlokat, vígan lehet rajta. Ez pont olyan, mint bizonyos emberi betegségeknel: vannak, akik csak hordozzák a betegséget, de nem betegszenek meg, viszont simán meg tudnak fertőzni másokat. A Linuxosok nem is tudják, hogy fertőzött fájlokat tárolnak, hiszen náluk nem történik semmi, vírusirtójuk nincs, tehát nem is jelez semmi, ezért fontos, hogy a Linux felhasználók is védekezzenek, náluk elég, ha néha, ritkán, korrekt vírusirtót telepítenek és futtatnak.

Visszatérés a Windowsra



Térjünk vissza a Windowsra: a legjobb az, ha jogilag tiszta, legális, aktivált, eredeti Windowsod van. Tudom, nem olcsó, de a licenelési politikájuknak „hála” a teljes verziókhöz és a frissítésekhez csak és kizárólag a fizetős verziók használói férhetnek hozzá. Egy otthoni felhasználónál is elsődleges, hogy az operációs rendszer licenccadatai meglegyenek, a számlával együtt.

A fizetős verziókhöz jár a terméktámogatás, járnak hozzá az automatikus biztonsági frissítések.

Egyes, vírusbiztonsági szakemberek, mikor a vásárolt vírusirtó mellett mégis megfertőződik a gép, akkor mindig azt a kérdést teszik fel először: "A Windows ugye jogilag teljesen tiszta?" Ugyanis, ha nem az, akkor nincs miről beszélni, mert az egyébként jól működő biztonsági szoftver mellett maga az operációs rendszer egy óriási biztonsági rést jelent.

Felejtse el a régebbi Windows verziókat, a 98-ba már egy 5 éves gyerek is be tud jutni egy kis barkácsolás után. Mai napig találkozom olyan gépekkel – főleg állami, önkormányzati intézményekben – , amiken Windows 98-at használnak, mert a nem tudom milyen külső szoftvergyártó cég csak ehhez tud adatbázis programot írni pl. (méregdrágán, tegyük hozzá).

A mostani Windows XP SP3 szervizcsomaggal már megfelelő ALAP az internetezéshez, folyamatos használathoz. De csak akkor, ha rendszeresen frissül az operációs rendszer. (Érdemes automatikusra állítani a frissítést, Vezérlőpult >> Automatikus frissítés)

A Microsoft felvette az automatikus frissítések közé az Internet Explorer 7-et és az SP3 szervizcsomagot, ami lényegében a Windows XP legutolsó javítása. Ezeknek mindenképpen rendben kell lenniük a csámítógépeken, mert az SP3 szervizcsomaggal a működést tekintve is sokkal jobb lett az XP – bár inkább a háttérműveleteket tekintve – az IE 7 pedig klasszissal biztonságosabb, mint elődje, az IE 6 volt. Ellenőrizd le, hogy milyen böngésződ van – erről beszélünk majd bővebben még – illetve ellenőrizd le, hogy SP3 szervizcsomag van-e feltelepítve. Ha még mindig SP2, netán SP1 szervizcsomagod van, akkor sürgősen be kell szerezned az SP3-at, és telepítened kell! Ez a Microsoft oldaláról le lehet tölteni.

(Itt tudod ellenőrizni a céges gépeken is a szervizcsomag verzióját: Vezérlőpult>>Rendszer. Rögtön a párbeszédpanel főoldalán látni fogod, hogy milyen Windows verziód van, és milyen szervizcsomag van mellette.

Ha Vistát használod, akkor SP1-es csomagnak kell lennie, mert a Vistához még csak egy szervizcsomagot adtak ki (és tették ezzel végre használhatóvá).

Az antivírus szoftverek gyártói megpróbálják tartani a lépést a vírusmaffiával és a hackerekkel, több-kevesebb sikerrel. Ugyanezt a harcot vívják más szoftverek gyártói is, így a Microsoft is. Ha kiderül egy-egy biztonságot érintő baki, akkor "gyorsan" elkészül a szoftveres frissítés, amit automatikusan küldenek a netre fellépő gépekre.

A frissítéssel kapcsolatban beállíthatod a saját szád íze szerint, hogy automatikusan történjen, vagy neked kelljen-e jóváhagynod. **Egyértelműen az automatikus letöltést és telepítést ajánlom**, manapság már nem jellemző, sőt egyáltalán nem fordul elő az, hogy egy frissítés miatt válnak használhatatlanná a gépek. Régen volt egy-két ilyen eset, de ez a probléma ma már nem áll fenn, tehát ez nem kifogás az automatikus telepítés ellen!

A Windowson kívül minden más használatban lévő programodnak jót tesz néha a frissítés. Vannak olyan szoftverek, amiknek automatikusan települő frissítési központjuk van, ezek figyelik a kiadott javításokat, és ha vannak, akkor letöltik ezeket. De van sok olyan program is, ami nem képes frissíteni magát, ezért évente egyszer-egyszer nem árt utána nézni, hogy például a méltán kedvelt képszerkesztőd, vagy egyéb kedvenc, rendszeresen használt szoftveredből létezik-e már új verzió. A vírusirtókat évente szinte teljesen megújítják, tehát ezeket érdemes

újrategytelepíteni évente egyszer, nem elég csak a licenckódokat cserélgetni bennük.

Ha egy program felajánlja, hogy készen áll a frissítések letöltésére, akkor bármi mást is tervezteél éppen végrehajtani, az várhat! Mindig azonnal telepítsd a frissítést, mert ha elodázod, azzal nagyban veszélyezteted a gépedet és az adataidat! A szoftverfrissítéseket általában nem jókedvükben adják ki a szoftverfejlesztő cégek, tehát nem eldöntendő kérdés, hogy alkalmazod-e vagy sem, hanem alkalmazni kell.

Összegezzük a fejezetet:

- Legalább két külön partíció javasolt, illetve ennek alternatív megoldásai.
- A C: meghajtó marad a rendszernek és a programoknak, a további partíciók pedig az adatoknak.
- Jogilag tiszta, automatikusan frissülő Windows operációs rendszer
- XP-nél SP3-as, Vistánál SP1-es szervizcsomag meglétének ellenőrzése.
- Legális szoftverek beszerzése, akár egyszerre, akár folyamatosan ütemezve.
- Szoftverek automatikus frissítéseinek azonnali telepítése (általában pár kattintást igénylő folyamat)
-

És ez volt még csak az első fejezet. Gondolom, most már látod, hogy egy vírusirtó meg egy tűzfal beállításával még sehol sem tartunk, ha a tökéletes védelemre törekszünk. Márpedig én arra törekszem, hiszen akar a bánat állandóan a vírusokkal foglalkozni, van nekem jobb dolgom is! :)

Bár tény, hogy a vírusirtó szoftverek és a tűzfal csupán csak 20%-ot jelentenek a vírusvédelem egészét tekintve, de botorság lenne ezt a 20%-ot kihagyni a rendszerből. Most ezekről lesz szó, mert mint mindennél, ezeknél is óriási tévhitek keringenek a köztudatban.

A folytatáshoz [rendeld meg a 10 Holtbiztos tipp című e-mail kurzusunkat>>](#), minél hamarabb, hiszen tudod:

Egy nap is sok a pokolban...

Üdvözlettel:

Vidi Rita

Vírus Kommandó