Topon maradni

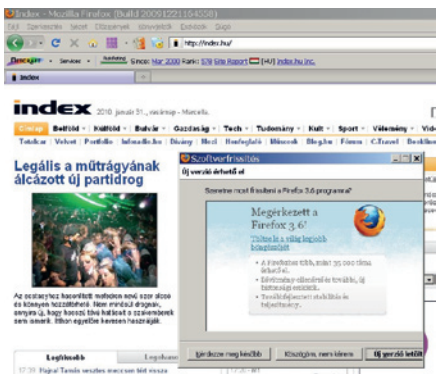
Frissen tartó mechanizmusok

Sorozatunk 31. részében arról értekezünk, mit kell tennünk annak érdekében, hogy rendszerünk friss, vagyis sebezhetetlen maradjon. Korábban (a 18., E, mint Exploit című fejezetben) már jól kiveséztük, hogy a „nulladik napi", frissen felfedezett, még javítással nem rendelkező hibák kivételével a már ismert sérülékenységek kihasználásával terjed a kártevők jelentős része.

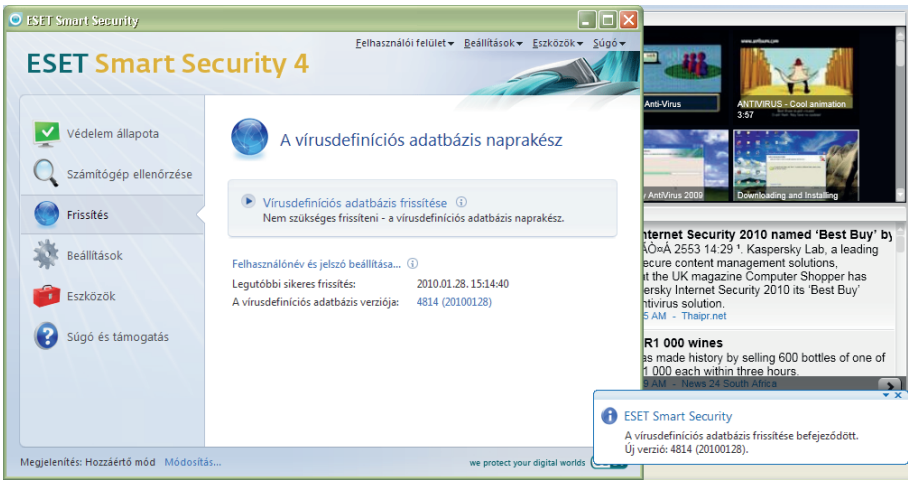
Vajon mekkora erőfeszítést kíván az operációs rendszer és a teljes munkakörnyezet naprakészen tartása a vírusvédelmi programokkal összehasonlítva, ahol automatizálva zajlik mindez? Illetve hogyan végzi, támogatja ezeket a Windows, a Linux és a Macintosh platform? Cikkünkben végül szó lesz majd arról is, mikor nem lehetséges, és mikor rejthet akár veszélyeket is magában a frissítés.

Amit mindig frissíteni kell

A vírusirtó, illetve internet security csomagoknak már évek óta (lassan már több mint másfél évtizede) megvan az a jó tulajdonságuk, hogy automatikusan frissülnek az internetről. Korábban hetente, néhány naponta, ma már jellemzően legalább naponta egyszer, de jobbára többször történik meg mindez. Beállítástól függően észre sem vesszük, vagy csak egy informatív buborék jelenik meg a Tálcán néhány másodpercre, amihez nem szükséges bármiféle teendő, maximum a tudomásul vétel. Ezt a funkciót inkább csak letiltani lehet, bekapcsolni nem is szükséges, hiszen minden AV-rendszerben ez az alapértelmezett tulajdonsága: szolgál, és teszi a dolgát a háttérben (és nem csak AV-termékek használják ezt a



A Súgó → Frissítések keresése útvonalat kell bejárnia annak, aki mindig a legesleg-újabb verzióját szeretné használni a Firefox-nak (a korábbi, még támogatott fejlesztési ágak frissítése automatikusan történik, ha ezt beállítottuk). A Tűzróka sok tekintetben kiemelkedik a versenytársak körül, de itt is érdemes kőbe vésni: 100 százalékig biztonságos böngésző nem létezik

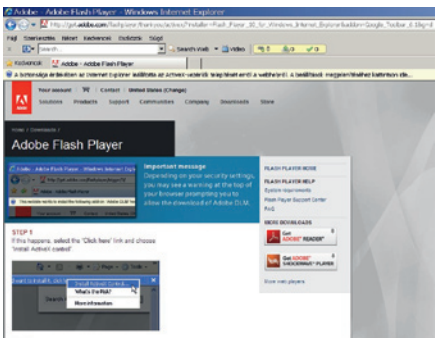


Egy olyan frissítés, amivel nincs semmi probléma. A friss adatbázis mindig újabb kártevők felismerését biztosítja, maga a frissítési procedúra pedig működő internetkapcsolat mellett automatikusan zajlik

szisztémát). A licenc érvényes időszakában van jogosultságunk és technikai lehetőségünk ezeket a frissítéseket igénybe venni.

„Amíg te pihensz, valaki keményen edz, hogy szétrúgja a hátsódat..."

Ennyire nem rózsás a helyzet, ha az operációs rendszereket nézzük, bár még mindig jobb, mintha a teljes feltelepített szoftverkörnyezet naprakészen tartásával hasonlítanánk össze. De nézzük először az előbbit. Kihasználható



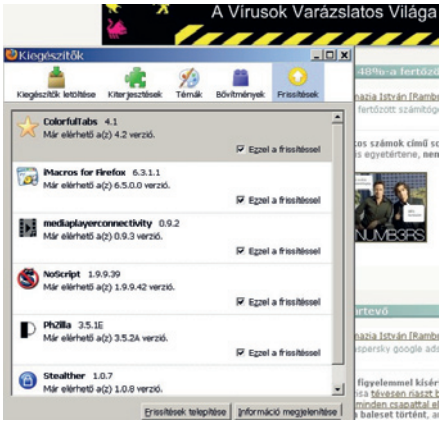
Igen sok sebezhetőséget rejtenek az Adobe szoftverek, ám frissítési gyakoriságuk sajnos nem elég sűrű. A Flash-animációkat megjelenítő FlashPlayer böngészőkomponenst időről időre frissíteni kell, amikor egy-egy ismertté vált támadás tömegesen lepi el a weboldalakat

sebezhetőség minden operációs rendszerben létezik – aki ezt nem hiszi, az mélyedjen el kicsit a milw0rm.org honlapján vagy kövesse a CanSecWest (cansecwest.com) verseny eseményeit időről időre, olvasson BuheraBlogot (buhera.blog.hu) és hasonló oldalakat.

Az nem is lehet kérdés, hogy rendszerünket muszáj frissíteni, frissen és naprakészen tartani, inkább ennek technikai és időbeli nehézségei az érdekesek. Mi most elsősorban a magánemberek, a hétköznapi felhasználók szemszögéből vesszük mindezt szemügyre, de tovább bonyolíthatja a helyzetet egy vállalati felhasználás is, amelyet előtte tesztelni kell az új, friss verzióval is, és csak ha minden hibátlanul működik, akkor lehet frissíteni. Mi most ezzel a nehezítő körülménnyel nem foglalkozunk, figyelmünk középpontjában egy hétköznapi felhasználó áll, aki tud és akar is frissíteni. Reméljük, mindennemű hasonlóság vélt vagy valós személyekkel nem kizárólag a képzelet szüleménye!

Módszerek, eszközök, workaround

A világon legjobban elterjedt, verhetetlen és megkerülhetetlen piaci szelettel rendelkező platform a Windows. Ha hihetünk a statisztikáknak, egyelőre még mindig az XP a legkedveltebb, de várhatóan a Vis-



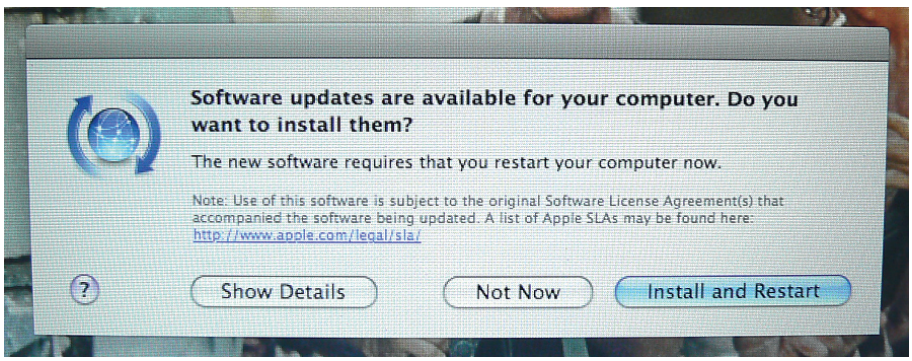
Néhány nélkülözhetetlen Firefox-kiegészítő. Az csak egy dolog, hogy telepítéskor rendre megjelenik a „Csak olyan szerzők kiegészítőit telepítse, akikben megbízik! (A szerző nem ellenőrzött)" felirat. Ám azt sem tudhatjuk, hogy az eleinte korrekt kód melyik frissítés után mit csinál majd a gépünkkel

Említettük korábban, hogy a NOD32 és az ESET Smart Security programok észlelik, ha a Windows frissítések elmaradásban vannak. Emellett az antivírusnak a saját háza táján is söprögetnie kell, és jelezni, ha például az internetkapcsolat átmeneti hiánya miatt meghiúsul a szignatúraletöltés

Egy igazán kiforrott és szerethető frissítési megoldás Ubuntu Linuxon. A szoftverek telepítése és eltávolítása valóban pofonegyszerű, de a frissítések kezelése is példaértékű. A rendszer minden telepített alkalmazás frissítését figyeli, aztán a felugró ablakban egy gombnyomásra el is végezhetjük a frissítést, miközben minden információt részletesen megismerhetünk

ta kedvezőtlen szerepét feledtetni igyekvő Windows 7 egy idő után átveheti majd az első helyet. A sebezhetőségekkel kapcsolatos kérdés például úgy vetődhet fel, hogy egy bűnözőnek milyen payload shell kódot érdemes egy preparált PDF állományba rejtenie a weboldalán? Az egészen biztos, hogy valamilyen távoli kódfuttatást biztosító kódot Windows operációs rendszerre, hiszen kis túlzással amerre néz, mindenhol windowsos gépeket lát, ez éri meg neki. A különféle antivírus cégek havi toplistáján a Conficker féreg még mostanában is előkelő helyen szerepel, és ennek a gyenge adminisztrátori jelszó választása, a külön misét megérő és a fertőzéseket segítő Autorun funkció mellett jócskán kiveszi a szerepét a be nem foltozott Windows rendszerek sokasága.

Mit tud a Windows Automatikus Frissítés és mit nem? A Windows eredetiségét vizsgáló folyamat (WGA, Windows Genuine Advantege) után lehetőség van frissíteni a biztonsági javításokat. A rendszeres frissítés rendre minden hónap második keddjén, az úgynevezett Patch Thuesday napján, azaz a foltozó kedden történik, leszámítva a rendkívüli, sürgős eseteket. A biztonsági frissítések elmaradásának szempontjából sok a szűk keresztmetszet: a felhasználók értik-e a fentieket, érdekli-e őket, legyőzik-e a lustaságukat, elég fontosnak tartják-e, hogy megtegyék, illetve aki tudatosan lopott kópiát használ, az szándékoltan kerüli a licencellenőrzést is kiváltó frissítési folyamatot. A Windows-frissítések egy részéhez a kópia „színétől" függetlenül, a szürkén át az egyértelműen lopott feketéig bezárólag hozzáférhetünk ugyan, viszont a szintén az exploitok célkeresztjében álló Microsoft Office-nál már nem ez a helyzet. Ott csak és kizárólag a legális ügyfelek tölthetik le a biztonsági frissítéseket.



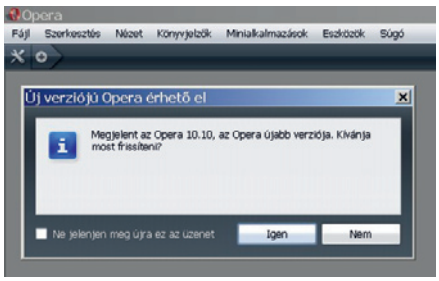
Van felugró frissítés a Macintosh rendszereken is. Ez az OS X-et és az Apple szoftvereket figyeli: iTunes, Safari, QuickTime stb. A hatásköre azonban sajnos ezekkel ki is merül. Emiatt ha egyéb alkalmazást, segédprogramot szeretnénk ellenőrizni, frissíteni, azt mind egyesével és kézzel lehet csak elvégezni

„Az ember vagy előidézi, vagy megoldja a problémát, különben csak szimpla tereptárgy"

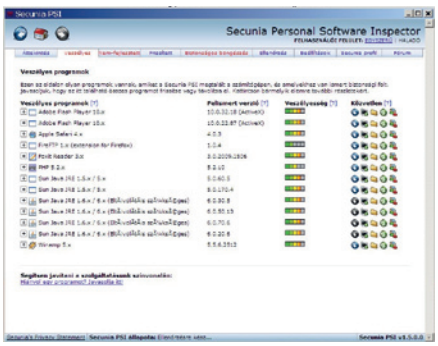
Vegyük úgy, hogy a Microsoft termékek foltozása (Windows, Office) megoldódott a frissítésekkel, de felvetődik ugyanakkor egy másik szempont: mi lesz a többi alkalmazói programmal? Nos, ezek különböző módon, több-kevesebb sikerrel igyekeznek tudatni velünk: emberek, itt a javított, új verzió, vegyétek és használjátok. Van, ahol kézzel kell a Súgó – Frissítések keresése menüpontot használni (például Mozilla Thunderbird, SwishMax), van, ahol automatikusan érkezik a figyelmeztetés a program indításánál (például CCleaner, Winamp), és van olyan szoftver is, ahol nemcsak az ablak vagy a link jön, hanem előzékenyen el is indul maga a frissítés (például Opera, uTorrent). Na és persze előfordul olyan alkalmazás is, ahol a fentiek egyike sem jelenik meg.

Ha csak egyszer is számba vesszük, mennyi és milyen programokat telepítettünk, reklámálnak-e ezek, hogy haladéktalanul frissítsünk, mennyi idő telik el, amíg magunktól észrevesszük az újabbat, rájöhetünk, ez egyedül nem megy. Kéne valami segítség a káoszban való eligazodáshoz, menedzselni ezeket a kulcsfontosságú folyamatokat. Ilyenkor jöhet jól egy Secunia Personal Software Inspector (hopp.pcworld.hu/3301), egy SUMo (www.kcsoftwares.com) vagy egy UpdateStar (hopp.pcworld.hu/5291) program, amelyek képesek levenni vállunkról a terhek egy jelentős részét.

A három megnevezett termék közül talán a legelső a legjobb. Mind a Secunia online vizsgálata, mind pedig a letölthető programja jól felkészült a rendszerünk naprakészségének figyelésre, és sebezhetőségi adatbázisa mind frissességben, mind a széleskörű szoftver-lefedettségben bizalomkeltő.



Sok szoftver működik úgy, hogy maga figyeli a saját megjelenő frissítéseit, és figyelmeztet, ha újabb verzió áll rendelkezésre. Így biztosan eljut az üzenet a felhasználóhoz, és a letöltés, valamint az upgrade folyamat is egyszerűen, keresgélés nélkül végezhető el



A Secunia Inspector figyel, figyelmeztet, és az esetek nagyobb részében a letöltési linkeket is felajánlja, ám egyesével manuálisan kell minden frissítést elvégezni. Néha azonban még így is kialakulhat kaotikus helyzet, ha például 6-8 különféle Java verzió is fent van egy időben

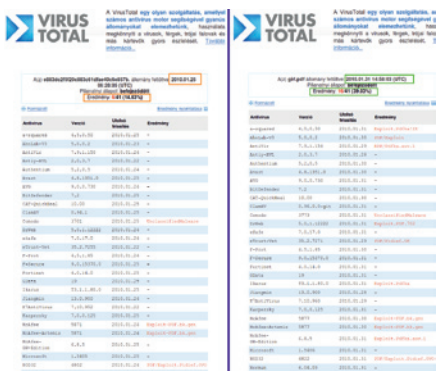
A Secunia a megfelelő állapotú, a frissítést igénylő, és a tovább nem fejlesztett kategóriákat is megkülönbözteti, valamint a sebezhetőségek veszélyessége szerint is képes osztályozni. Az évek óta nem fejlesztett szoftverek esetében érdemes másik helyettesítő program után nézni

Linux-frissítések – én így szeretlek

Semmilyen teret nem szánunk olyan meddő vitának, mint hogy melyik OS a legjobb – ez amúgy is feladatfüggő, nincs ilyen bokszmeccs. Viszont ha a frissítési procedúrát vizsgáljuk, tőlünk az Ubuntu Linux kapná meg az aranyérmet. Ennél egyszerűbb ugyanis már nem is lehetne. Egy gombnyomás (vagy beállítjuk, hogy automatikusan pattanjon fel egy ablak, ha érkezik frissítés) és egy [Enter] egy adminjelszó után, és máris naprakészen tudhatjuk az egész rendszert. Az is nagyon jó pont, hogy mennyire informatív a folyamat – pontosan tudhatjuk, mit hagyunk jóvá, mi frissül, mi történik. Nemcsak azt látjuk, hogy a KB123456 nevű nagyon fontos frissítés készen áll, hanem külön keresgélés nélkül is tudjuk, mi ez, mit csinál, melyik szoftverhez kapcsolódik, és ott a checkbox, dönthetünk, kérjük-e egyáltalán.

Macintosh – tűzre, vízre vigyázunk

A fentiekhez hasonlóképpen automatizált és kényelmes az OS X frissítések jövetele és kezelése is. Elfogad, adminjelszót beüt, örül – ennyi. Ha azonban összevetjük a Windows- és a Linux-frissítések tulajdonságaival, azt láthatjuk, hogy bár kényelmi szintje a Linuxéhoz hasonlít, de sok tekintetben a Windows rendszerrel rokon. Sajnos nem kényeztet el minket, van ugyan automatikusan felpattanó ablak, de az ebben megjelenő frissítések csak az Apple programjainak frissen tartását végzik: OS X, iTunes, Safari, Quick Time. A további alkalmazói programokat nekünk kell figyelni, és egyesével, manuálisan frissítgetni.



Jól látszik a két, egy hét különbséggel elvégzett VirusTotal vizsgálatnál, hogy ennyi idő elteltével mennyivel több (6/41, illetve 16/41) vírusirtó motor képes már detektálni egy viszonylag friss kártevőt

Amikor nem biztos, hogy nyerünk vele

Térjünk most már vissza a Windowshoz. Aki nem használ ki minden egyes új funkcionalitást az új verziókban, elhűlve tapasztalhatja, milyen hihetetlen tempóban híznak az új változatok. Néhány példa csak: a Nero 3 mérete anno még csak 1,8 MB volt, mára a Nero 9.4.26 már 204 MB-ot foglal. Az Acrobat Reader 2 még 1,4 megabájttal beérte, a 9.2-es Reader már közel 25-öt kíván, de itt az iTunes 4.1, ami csak 19,1 MB volt, ezzel szemben az iTunes 9.0.2 mérete már 93,6 MB. És ne felejtsük, ezek még nem a merevlemezen elfoglalt helyet, hanem csak a telepítőcsomag nagyságát jelentik.

Ha a frissítés nem kötelező, és elégedettek vagyunk a használt verzióval, akkor nem muszáj ugyan frissíteni, persze ilyenkor a merevlemezen elfoglalt hely és az ismertté vált sebezhetőségek néznek egymással farkasszemet. Ha nem vállaljuk az új „fatware" telepítését, akkor esetleg kereshetünk alternatív megoldást: kisebb, gyorsabb, biztonságosabb, esetleg olcsóbb vagy akár ingyenes kiváltó programot.

Amikor lehetetlen frissíteni

Egy példával azt is illusztráljuk, amikor bár megvan a jó szándék, és nem jelent közvetlen szívszélhűdési veszélyt az új verzió merevlemezen elfoglalt tárhelye, mégsem tudjuk sikeresen elvégezni a hőn áhított frissítést. Ez lehet például a telepítő hardverkörnyezet vizsgálata. Esetünkben a VMware Player, az ingyenes virtuális gépkezelő szoftverre kapunk figyelmeztetést a Secunia PSI-től, egészen pontosan a „Veszélyes szoftverek" között szerepel a gépen található 2.0.5 változat. A 3-4 éves celeronos gépen ez tökéletesen eldolgozik, igaz, a közben felfedezett biztonsági rések problémákat okozhatnak (kódfuttatás, a host gép lefagyasztása stb.). Pontosan ezért kíséreljük meg a frissítést a javasolt 3.0.0.203739 változatra. Az csak egy dolog, hogy a telepítés a korábbi verzió uninstallálása nélkül nem is működik, a csalódás azonban akkor következik be, amikor kiderül, ezen a hardveren ez az új verzió nem működőképes. Ekkor marad a régi: használni még lehet, de marad a kompromisszum, mégsem lesz mindenünk a legfrissebb, és igen, a gépünk tartalmazni fog támadható, elavult programokat. Vagy mehetünk új számítógépet venni, esetleg virtuálisgép programot cserélünk, és váltunk MS Virtual PC-re vagy a Sun VirtualBoxra.

Talán már érzékelhető, hogy akkor sem egyszerű ez a frissítgetés, ha valaki tényleg mindent elkövet. A következő havi fejezetünkben pedig arról lesz majd szó, mikor rejthet akár közvetlen veszélyt egy frissítés.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu