

- [Kezdőlap](#)
- [E-mail tanfolyam](#)
- [Termékeink](#)
- [Miről szól?](#)
- [Gy. I. K](#)
- [Kapcsolat. §](#)
- [A felhasználókról](#)



Számítógépes vírusok? Hogyan lehet végleg legyőzni?

Itt a remek alkalom, hogy néhány nap alatt megbizonyosodj arról, hogy tudatosan véded-e a gépedet, vagy csak a vak szerencse vezérelt eddig. **Ingyenes e-mail kurzusokon** kiképzünk a legfontosabb tudnivalókról, és leleplezünk néhány bennfentes titkot is. **Feliratkozás az e-mail kurzusra itt, jobb oldalt>>>**

E-mail tanfolyam feliratkozás

Keresztnév: *

E-mail: *

Az okos emberek megoldják a problémákat, a zsenik pedig megelőzik őket.

(Albert Einstein)

[Gyakran Ismételt Kérdések](#)

[MSN linkküldőzető "vírus" kiiktatása, megszüntetése](#)

[Automatikus lejátszás kikapcsolása, AUTORUN.INF ellen](#)

[Rendszervisszaállítás kikapcsolása, ha törölhetetlen a kártevő](#)

• Vidi Rita



developed by [Jhack](#)

Vírus Kommandó a Facebook-on

• Létezik biztonságos böngésző?

Posted on július 20th, 2009 Vidi Rita [15 comments](#)

Újabb körkérdesés bejegyzést olvashatsz, három, a témában jártas szakértőt kérdeztem meg arról, hogy mi a véleménye a böngészők biztonságáról, egyáltalán létező, életszerű fogalom-e ez, vagy csak marketingduma? A kérdésem, felvetésem így szólt, a megkérdezettek e-mailben kapták meg, és a választ is így küldték el nekem:

Létezik olyan, hogy "biztonságos böngésző"?



Firefox vs Internet Explorer

Minden böngésző magát kiáltja ki legbiztonságosabbnak, ugyanakkor aki kicsit is mélyebbre lát, tudja, hogy ezek a kinyilatkoztatások sok-sok rejtett, véletlenül ki nem domborított hibát takarhat.

Neked, mint témához szakértőnek mi a véleményed erről: létezik egyáltalán biztonságos böngésző? Vagy ez csak egy üres frázis?

Válaszok, érkezési sorrendben

Csizmazia István [Rambo]

100% biztonságos böngésző mint olyan, nem létezik. Ennek oka, hogy biztonságos program sem létezik. Maximum olyan, aminek a hibáját eddig még nem használták ki.

Jó kompromisszum létezik, és hasznos szokások, megfelelő hozzáállás, hadrafogható pluginok.

Lehet szempont, hogy a szkriptek mennyire tudnak egy böngészőben szabadon, illetve megfelelően lekorlátozva futni – ebből a szempontból a Firefox a NoScript pluginnal mindenképpen kimagasodik a

mezőnyből.

Az szintén egy érdekes kérdés lehet, hogy egy plugin fejlesztőjében mennyire bízunk meg, ugye pont a NoScript és az Adblock plusz vívott egy ilyen csörtét, hogy egymás reklámjait blokkolták, orvul szólas nélkül, [aztán jött a nagy elnézés kérés.](#)

Egy felhasználó maximum megbízhat ezekben, és abban, hogy ha hosszú távon rosszat akarnak neki, akkor jön egy Mark Russinovit és kiborítja a bilit, mint az emlékezetes Sony DRM esetében.

Emellett jó érv még a nyílt forráskódú fejlesztés, ahol biztosan nem rejtenek el hátsó ajtót a böngészőbe, nem módosítják utólagosan a szerződési feltételeket, és akárki használhatja, megnézheti, módosíthatja a forrást, nem kell térden állva könyörögni a javításért.

Vannak cégek – és hitem szerint minden közintézménynek ilyennek kellene lennie – aki szépen lassan kiszállnak a zárt forráskódú világból, és szépen átállnak Outlookról Thunderbirdre, Microsoft Office-ról Open Office-ra, Internet Explorer-ről Mozilla Firefoxra, azt már nem is merem mondani, hogy Windows-ról

Linuxra, és más hasznos célra költik az adófizetők pénzét :-)

A böngészőkben előforduló hibák statisztikájában nem hiszek, ott olyan szinten játszanak a számokkal, amik mindig annak kedvezőek, akinek a statisztika készítője akar.

A Chrome kezdeti szerzői jogi malőrje (minden adat a Google tulajdona) erosen beármányolta az indulást, majd meglátjuk, hova fejlődnek, ők még szerintem nem fociznak a nagyok közt egyelőre.

Az Opera is inkább csak egy szűk rétegé, és a Safari sem "tarolta le" a piacot, bár sok mobil eszközben (pl. nem feltört iPhone) csak ezt tudjuk használni, nincs választásunk.

Mivel nem a teljes képességekről (pl. ACID3 teszt), hanem a biztonságról van szó, tendenciákat azért lehet látni. Hasonlítsuk össze az 1 es 2 évvel ezelőtti tortadiagramot a mostanival, és abból egyértelműen látszik, a FireFox szépen tör előre. Ebből persze még nem lehet mindent eldöntő következtetéseket levonni, hiszen akkor az "Egyen ön is lócitromot, 8 milliárd légy nem tévedhet" jönne. De azért a számok mégis tükröznek egyfajta tudatosságra való törekvést, a biztonság felé történő keresgélést.

Szokott még érv lenni az "én okosan böngészek", ebben nem hiszek, [lásd éppen a Chrome-os bejegyzést](#), bármelyik weboldal vagy banner tartalmazhat ismeretlen kódot, szkriptet.

A hasznos szokások lehetnek a minden böngészés utáni cache ürítés, a session cookiek törlése (amik ugye bizonyos körülmények közt ellophatók), néhány alap plugin használata: NoScript, NetCraft, ShowIP,

Finjan, Aadaptive Referrer remover, Cache Status, Cookie Safe, Live HTTP headers, JS View, Secure Login, XSS Guardian, XSS Warning.

A leginkább biztonságos böngésző egy ezekkel felszerelt és Linux alól futó Mozilla Firefox – legalábbis nekem ez vált be.

--

üdvözzel:

Csizmazia István [Rambo]
antivirus.blog.hu

Buherátor

Onnantól kezdve, hogy az ember túllépett a "Hello Világ!" jellegű problémákon, elvéve találni hibátlan programokkal. Érdemes utánajárni[milw0rm.com], hogy hogyan tudnak még a legprimitívebb fájlkonverterek esetében is veszélyes hibákat elkövetni a programozók – akiket ezzel nem célok megsérteni, hiszen mindannyian emberből vagyunk. Gondoljunk bele, hogy ennek fényében mennyire reménytelen vállalkozás egy olyan szoftvert hibátlanul elkészíteni, amely már-már átvenni látszik egyebek mellet az összes irodai, multimédiás és közösségi alkalmazás, valamint bizonyos értelemben maguknak az operációs rendszernek a szerepét is*!

De a probléma még ennél is összetettebb: hiszen a böngészők ma már nem csak egyszerű, HTML megjelenítésre alkalmas programok. A weben szörfölve ezer szállal függünk a különböző, harmadik féltől származó alkalmazásoktól, különböző beépülő moduloktól és magától az operációs rendszertől, melyeknek szintén hibátlanoknak kellene lenniük ahhoz, hogy biztonságban érezhessük magunkat. Mindez persze nevetséges illúzió.

Azt hiszem, el kell fogadnunk, hogy böngészés közben sebezhetőek vagyunk. Az ezzel összefüggő szemléletváltás már megfigyelhető a Google Chrome és a MS Internet Explorer fejlesztésével kapcsolatban: zárjuk karanténba a böngészőt, hogy ha már úgymint beteg szegény, legalább ne hozzon bajt a rendszer többi részére. Persze a konkrét megvalósítással még csak kísérleteznek, egyensúlyozni kell

viruskommando on Facebook

Kövess Twitteren!



<http://twitter.com/vidirita>

Cikkek

- [Kell-e vírusirtó Linuxra?](#)
- [Hogyan lehet filmeket és zenéket letölteni INGYEN?](#)
- [A nők egyszerűbb jelszavakat használnak](#)
- [PCK epizódok – avagy adatmentési tapasztalatok a szervizből](#)
- [ESET vírusstatisztika – Újra támad az AUTORUN](#)
- [A Biztonságos Internet Napja 2011. február 8.](#)
- [Milyen védelmi szoftverek kompatibilisek egymással?](#)

PC Start

Alapozó oktatóanyag,
hogy végre élmény legyen
a számítógépezés



Kezdőknek,
bizonytalankodóknak,
biztosra menőknek

[Olvass tovább >>](#)

Kategóriák

- [A felhasználó](#) (10)
 - [Kezdő felhasználók](#) (1)
- [Adatvédelem](#) (31)
 - [Adathalászat](#) (8)
 - [adatmentés](#) (6)
 - [adatszívargás](#) (6)
 - [MKB adathalászt e-mail](#) (2)
- [Biztonsági frissítés](#) (6)
 - [Adobe veszélyek](#) (1)
- [Hacker](#) (6)
 - [Hacktivity 2009](#) (2)
- [hírek](#) (16)
 - [80 napos tanfolyam](#) (1)
 - [blog](#) (4)
 - [botrány](#) (2)
 - [dns](#) (1)
 - [gépház](#) (2)
- [hoax](#) (3)

teljes virtualizáció által nyújtott védelem, és a felhasználó jogos igényei – a helyi fájlok elérése, az alkalmazásintegráció, stb. – között. Minden bizonnyal érdekes fejlemények lesznek ebben a témában, de jelenleg legfeljebb biztonságosan használt böngészőkről beszélhetünk: ha nem kattintunk mindenre ami mozog, külön, korlátozott jogú felhasználót, vagy akár szeparált (virtuális) gépet használunk böngészésre, máris sokkal nagyobb biztonságban tudhatjuk magunkat, mint az internetező társadalom túlnyomó része.

*és itt ki is zámám a kérdés köréből a lynx-t és barátait, melyeknek ugyan megvan a maguk romantikája, de mégsem férnek bele a mai modern böngészők koncepciójába.

Buherátor
buhera.blog.hu

Carter

Létezik-e biztonságos böngésző?

Amíg a programokat emberek készítik, addig mindig lesznek benne programhibák! Amíg lesznek programhibák, addig lesznek olyan rossz szándékú emberek, akik ezeket ki is fogják használni! Nézzük meg kicsit az ártó szándékúak szemszögéből a helyzetet! Mit szeretnének? Nagy profitot, sok felhasználói adatot! Hogyan lehet ezt elérni? Nagy piacra kell fejleszteni! Tehát meg kell keresni a legtöbb felhasználóval rendelkező operációs rendszer-böngésző párost és ha abban hibát találnak, nagy eséllyel lehet sok-sok százezer felhasználó személyes adatait begyűjteni!

Tehát innen nézve a legveszélyesebb böngésző az, amit a legtöbben használnak!

De a helyzet nem ilyen egyszerű! Azzal, hogy valami kevésbé elterjedt böngészőt használunk, ami esetleg gyengébb felhasználói élményt is nyújt, mint a jól megszokott, máris ott találjuk magunkat, hogy csorbul az érzés! Nem hiába használja és ajánlja a hozzáértőbb felhasználók része a Firefoxot: szép, gyors, jól támogatott, stabil böngészőprogram!

De mint a múlt héten kijött 3.5-ös verziónál is láthattuk, már egy napra rá jelent meg olyan kártékony kód, ami adatlopást eredményezhet! A feszített tempó a fejlesztésben, a sok újdonság mind-mind biztonsági réseket eredményezhetnek!

Az operációs rendszer is sokat tehet a biztonságért. A majdnem tíz éves Windows XP működését a kártékonyprogram-írók nagyobb része már fejből tudja! Zavaró lehet az újabb Vista védelmi rendszerének megkerülése, vagy a teljesen más alapokról induló Linux (~1%-os elterjedtség!) megismerése.

Fontos része még a biztonságnak a megfelelő vírusirtó alkalmazása! Egy jó vírusirtó egyből jelez, ha a böngészőn keresztül kártékony program próbál települni, optimális esetben teljesen meg is akadályozza a működését!

Ezek miatt nem lehet csak a böngészők biztonságáról beszélni önmagában, mindig nagyon sokat számít a futtatókörnyezet, a beállítások.

Legutoljára hagytam a legfontosabbat: a felhasználót! Lehet egy böngésző bármilyen biztonságot, egy vírusirtó bármilyen ügyes, használhatunk akármilyen linux disztibúciót, ha a felhasználó azt látja, hogy meg kell adni a jelszavát és megadja, akkor az összes védelem tehetetlen.

A legfontosabb a jól képzett felhasználó, minden más csak ezek után jöhet.

Összegezve: a legbiztonságosabb böngésző az, amit szinte senki sem használ, de mégis modern, valamint egy nagyon megbízható és ugyancsak friss operációs rendszeren fut. Ez az optimális helyzet sajnos nagyon kevés helyen valósítható meg, így marad a megszokott módszer: Figyelni, gyanakvónak lenni és minden adatot menteni – ez a hármas szabály nagyon fontos!

Carter

Köszönöm az interjúalanyoknak, Rambonak, Buherátornak és Carternek, a részletes és nagyon hasznos véleményeiket!

[Meddig akarsz még szenvedni a lassú géped miatt? Van megoldás, ráadásul könnyű és gyors! Kattints ide, és nézd meg, hogyan tudod begyorsítani a gépedet saját kezűleg!>>>](#)

Mi a TE véleményed? Te hogyan látod? Hiszel a böngészők biztonsági "mutatóinak", vagy gyanakvó vagy és körültekintő?

Várjuk válaszodat a hozzászólások között (itt alább)!

Vidi Rita

- [hallmark](#) (1)
- [lánclevél](#) (1)
- [Internet biztonság](#) (32)
 - [Feltört honlap](#) (10)
 - [Internetbank](#) (2)
 - [IT Security](#) (5)
 - [Jelszó kezelés](#) (3)
 - [torrent](#) (2)
- [SOS megoldások](#) (4)
- [számítógép](#) (40)
 - [Szakember](#) (21)
 - [gyorsítósáv](#) (14)
 - [windows](#) (27)
 - [Windows 7](#) (2)
- [twitter](#) (2)
- [vírus](#) (13)
 - [conficker](#) (1)
 - [Féreg](#) (1)
 - [gumblar](#) (1)
 - [kártevő](#) (1)
 - [Számítógépes vírus](#) (4)
 - [Vírus toplista](#) (6)
- [vírusirtó](#) (33)
 - [nod32](#) (7)
- [Vírusvédelem](#) (61)
 - [Botnet](#) (1)
 - [Nincs kategorizálva](#) (8)
 - [spam](#) (12)

Lassú a géped?

Lassú a géped?

Magától nem fog felgyorsulni!

**Gyorsítsd be
9 egyszerű
trükk
segítségével!**



Katt ide a folytatásért! >>

Keresőszavak

[7 adathalász adatmentés](#)
[Adatvédelem](#) [antivirus](#) [avast](#) [avg](#)
[biztonság](#) [biztonsági](#) [e-mail](#) [eset](#)
[felhasználó](#) [feltörés](#) [firefox](#)
[frissítés](#) [google](#) [gyorsítás](#)
[gyorsítósáv](#) [gép](#) [Hacker](#) [honlap](#)
[internet](#) [IT](#) [jelszó](#) [kaspersky](#) [kártékony](#)
[lassú](#) [mkb](#) [nod32](#) [security](#) [sicontact](#)
[smart](#) [spam](#) [számítógép](#) [tanulmány](#)
[trójai](#) [twitter](#) [verzió](#) [videó](#) [vista](#) [vírus](#)
[vírusirtó](#) [Vírusvédelem](#)
[windows](#) [xp](#)

Távsegítség

Kapcsolódó bejegyzések:

- [Kell-e vírusirtó Linuxra?](#)

[Internet biztonság](#), [windows biztonság](#), [böngésző](#), [explorer](#), [firefox](#), [internet](#), [körkérdés](#), [mozilla](#)

15 responses to “Létezik biztonságos böngésző?”



1.

[Szalay László dr. július 20th, 2009 - 12:38](#)

Szia!

Kérdezem, hogy tudsz-e segíteni a következő problémán:

Bizonyos, számomra fontos programokat nem tudok megnyitni sem a laptopon, sem az otthoni PC.-n (pl.: .crd, Maxtons, stb). Volt már ilyen, akkor a rendszervisszaállítás megoldotta a bajt. Most sem, akkor sem sikerült a rendszert visszaállítani, mert rákattintva nem csinál semmit. Akkor kaptam egy tanácsot, hogy ay parancssorba mit kel beírni, s akkor beindult. Elmentettem, de nem találom.

Ismered ezt a trükköt?

Üdv és kösz:

Laci.



2.

[Vidi Rita július 20th, 2009 - 12:56](#)

Sajnos nem ismerem ezt a trükköt Laci, légszi nézz szét fórumokon!



3.

[-rb- július 20th, 2009 - 14:34](#)

Remek válaszok!

Annyi kiegészítés, hogy az Open Source megoldásokkal kapcsolatban van 2 NÉPSZERŰ TÉVHIT, ami itt is (úgy mellékesen) elhangzik. Ezekkel kapcsolatban azért érdemes az olvasókkal a teljes igazságot megosztani.

A két népszerű TÉVHIT az alábbi:

- 1) Az Open Source biztonságosabb
- 2) Az Open Source olcsóbb

Azért tartom lényegesnek, hogy leírjuk, hogy ezek a kijelentések “nem fedik fel a valóság minden részletét”, mert az állítások:

- 1) Biztonsági kockázatokat jelentenek a felhasználóknak
- 2) Olyan költségekbe verik őket, amit megúszhatnának

Ha ezt nem akarod megtenni, legalább érdemes elgondolkozni az alábbiakon.

1. TÉVHIT: Az Open Source biztonságosabb.

Ez a tévhit abból az elből indul ki, hogy ha egy program forráskódja nyilvános, akkor több szem előbb megtalálja benne a hibát. Tehát az alkalmazásban kevesebb hiba lesz. Tehát kevésbé támadható.

A valóság azonban az, hogy a hibák megtalálása nem a szemrevételezők mennyiségétől függ, hanem azok minőségétől. Azaz leegyszerűsítve attól függ, hogy a legokosabb ember, aki megnézi, észre veszi-e.

Az olyan open source programokban, mint az, amivel az operációs rendszerek a hálózatra kapcsolódnak is kerülnek elő hibák 15-20 év után is.

Kb. azt látom, hogy amióta (egy bő 5 éve) a biztonság a Microsoftnál is kiemelt fejlesztési és

Segítségre van
szükséged?



(kattints a képre!)

PC Kommandó
Távsegítség >>

[Vírusirtó Lap](#)

- [PC Kommandó dizájn blokk – Saitek audio-200](#)
- [Jó lenne, ha valaki elmagyarázná](#)
- [Adobe Acrobat Reader nélkül nem élet az élet](#)
- [Melyik operációs rendszert válasszam?](#)
- [Meglepetés: Válságelkerülési tanácsok](#)

[HősNők.hu](#)

- [A mennyei prófécia – 1-2. rész](#)
- [Kukucs a mindennapi életbe-szezonmunka](#)
- [Idézet hét elejére 31.](#)
- [Az érzelmek és a gondolkodás hatása az egészségre – 3. rész: viselkedés raszájanái](#)
- [Nyári pénzügyek](#)

[Internet, a szolgáltató szemével](#)

- [A Silihost karácsonyi ajándéka: marketing-könyv + 2 óras teadélután](#)
- [Szigorítottuk a SPAM-szűrésünk – kiváló eredménnyel](#)
- [Interaktív világtérkép a hálózati támadásokról](#)
- [Új Silihost-fejlesztés az Ügyfeleinkért: Google Biztonságos Böngészés integrálása](#)
- [A Facebookon százszor több a SPAM, mint a többi közösségi rendszerben](#)
- [Célpontban az ügyfelek: a Fort Disco malware email- és FTP-szervereket támad](#)

[PC Kommandó](#)

- [Miért kell a Facebook?](#)
- [Használod a Facebook-ot?](#)
- [A nagy SZERVIZ teszt](#)
- [Hogyan védjük szerettünket a hőségtől?](#)

tervezési szempont, az MS termékei LEGALÁBB olyan biztonságosak, mint open source-os társaik. Ez azt is jelenti, hogy sokszor azt igazolja az élet, hogy a megjelenést követő 3-6-12 hónapban kevesebb hibát találnak bennük, mint a megfelelő open source-os rendszerekben.

Ha ehhez hozzávesszük azt is, hogy a rendszerek meddig maradnak nyitottak egy ilyen sérüléssel szemben, akkor még szembetűnőbb a különbség. Azt a végfelhasználók is tudják, hogy a Windows "javítja magát", azaz a legújabb frissítések maguktól települnek.

És van egy másik fontos szempont is. Ezt minden cégvezetőnek (és állami hivatal vezetőjének) tudnia kell:

A biztonságban a leggyengébb láncszem az ember!

Egy nagy gyártónál (nem csak az MS, de az Adobe, IBM, Novell, ...) ha megtörténne olyan, hogy a gyártó egyik alkalmazottja nyit egy hátsó kaput a rendszeren, és ez kiderül, abból világraszóló botrány lesz.

Ha a te rendszergazdád megteszi ezt (a forrás megvan, ott írja át, ahol akarja, úgysem tudod ellenőrizni), akkor az egy lokális kis botrány lesz. Amibe a te céged, állami szervezeted bele fog bukni.

És ehhez nem programhiba kell, csak egy rosszándékú, lusta rendszergazda, aki megérzi, hogy ki akarod rúgni.

Ez mekkora biztonságot ad?

2.TÉVHIT: Az Open Source olcsóbb

Először is az OpenSource nem azt jelenti, hogy ingyenes.

Például a MS lehetővé teszi az állami szerződésekbe, hogy az állam, ha akar, belenézzen a Windows forrásába is.

Sőt a Microsoftra és másoknak is vannak open source, de fizetős termékei.

Nézzük helyette az INGYENES-t. (Ami gyakran valóban OpenSource.)

Mibe kerül, ami ingyen van?

Általában pénzbe. Időnként sok pénzbe. Talán nem ismeretlen az olcsó fénymásoló, drága festék modell senki előtt.

Egy cég/szervezet informatikai költségeinek 80% a fenntartásra, üzemeltetésre megy el. A 20% az új projektekre (ebbe beleértve hardver, szoftver és szolgáltatás költségeket.) Legyen ennek 1/3 része a szoftver beszerzési költsége. Ekkor az IT kiadások 5-6%-ról beszélünk.

Az OpenSource tehát akkor tud olcsóbb lenni a nap végén, ha annak üzemeltetése, ide értve a felhasználók segítségét is, legalább 5-6%-kal olcsóbb tud lenni, mint fizetős társaie.

Ez ma messze nincs így. A Microsoft, IBM, HP, Novell, ... rendszerek üzemeltetése fele/harmada áron megoldható, mint a jelenlegi ingyenes rendszereké.

Ha valaki nem ismeri, hogy miként működik egy vállalat informatikája, az gondoljon bele csak az alábbiakba:

- Mibe kerülne magának elindulni és áttérni önerőből más gyártó termékeire.
- Hol találna olyan munkaerőt, aki ismeri pont azt a terméket.
- Ki tudna segíteni a környezetében, ha elakadt valamiben. (Kollégák, rokonok, ismerősök.)
- Kit hívna, ha elromlana az a rendszer.
- Hogy váltana rendszergazdát, beszállítót? Mit szólna az új rendszergazda ahhoz, ha más által összeprogramozott rendszert kellene üzemeltetnie? Mit gondol ki lenne a hibás, ha valami nem megy: az új üzemeltető, vagy a régi, akit kirúgott?

Az sem utolsó szempont, hogy van egy gyártó, aki bevonható egy probléma elhárításába. Sőt végső soron felelőssé tehető. Ez a kalákában fejlesztett rendszereknél nincs így...



4.

[evenorbet július 20th, 2009 - 15:02](#)

Kedves -rb-!

Legalább odáírhattad volna, hogy te Microsoft programokkal kapcsolatban nyújtasz tanácsadást és kapcsolatban állsz a Microsoft-al. Bár az írásod alapján csalódtam volna, ha nem így lett volna. :)

- [Laptop vásárlás előtt – Mit jelentenek ezek?](#)

Ajánlott oldalak

- [Hatékonyság Blog](#)
- [Ingyenes számítógép tanfolyam](#)
- [Okos Vállalkozás Blog](#)
- [Önbizalom növelés nőknek](#)
- [PC Kommandó](#)
- [Rendszergazda Blog](#)
- [RizsaNélkül.hu](#)
- [Vírusirtó](#)

Feliratkoztál már?

Iratkozz fel, és megkapod a legjobb magyarázatokat a vírusvédelemmel kapcsolatban!

Keresztnevé:

E-mail:

5.



[buherator július 20th, 2009 - 15:08](#)

@-rb-

Alapvetően egyetértek az általad leírtakkal, és nem is szeretnék belemenni egy foss/proprietary flame-be, de

1) Biztonság != hibák száma

2) Nem csak a Windows "javítja magát" sőt, Windowson a third party komponensek központi frissítése szinte lehetetlen. vö.: apt-get

3) open source != sufinituning. A legtöbb nagy FOSS projekthez jár support, felügyelt a fejlesztés stb. Az meg hogy mi a drága mindig szituáció függő, nem túl bölcs dolog általánosítani.

6.



[Krisztián július 20th, 2009 - 15:27](#)

Hja, ha az emberi hülyeséget is számításba vesszük, nincs tökéletes védelem...

Egyébként egy érdekesség az emberi hülyeséghez:

<http://pcforum.hu/hirek/11427/A+vilag+legbenabb+jelszavat+hasznaltak+a+Twitter+vedelme.html>

No komment

7.



[Vidi Rita július 20th, 2009 - 16:01](#)

Krisztián! Nyugodtan olvass vissza itt a blogon is :)

<http://www.viruskommando.hu/blog/adatvedelem/jelszo-jelszo-password-password/>

8.



[Cszmazia István \[Rambo\] július 20th, 2009 - 16:06](#)

Szia -rb-!

Az egyik mondandomat Buherator kollega mar lelotte a 3-as pontjaban, hogy nem sufinituningrol beszélünk. Pl. Linux esetében nem kell okvetlenül szakallas kockasínges autistakra kell gondolni terméktámogatás címen, ehhez elég megnezni pl. az Ubuntu vagy a SuSE cegek számára – külön díjert természetesen – nyújtott színvonalas supportját.

A másik dolog ez lenne, idezlek hozzá: "Egy nagy gyártónál (nem csak az MS, de az Adobe, IBM, Novell, ...) ha megtörténne olyan, hogy a gyártó egyik alkalmazottja nyit egy hátsó kaput a rendszeren, és ez kiderül, abból világraszóló botrány lesz."

Nem kell ehhez az egyik alkalmazott, elég hozzá a cég egész vezetése. Sajnos ez naív tevényt, ma sem tudhatjuk, hogy egy Google mire használja az összes adatunkat, vagy itt van a Google cenzurázott kínai keresoje: lefekudtek a politikai megrendelésnek vagy nem? Nezd meg, hogy egy Yahoo mit meg nem tesz, ha a saját érdekeit vedi az allampolgárral szemben:

<http://computerworld.hu/yahoo-segített-politikai-aktivista-bebortonzeseben.html>

Vagy ha mar Windows es Microsoft, ebbol milyen vilagraszolo botrany kerekedett? Sajnos semmilyen:

http://hup.hu/cikkek/20080913/gyenge_titkositas_a_windows_vedett_tarolojaban_francia_beallitasok_mellett

Emellett pedig koztudomasu, hogy pl. az iPhone kuldozgetett forgalmi adatokat az Applenek,

http://antivirus.blog.hu/2007/11/20/amikor_a_telefon_hazatelefonal

A Windows Media Player pedig regebben vagy meg ma is?! hacsak ki nem kapcsolják, a mediak adatait kuldozgeti, es belebuktak? Nem ugy nez ki.

<http://index.hu/tech/jog/wmp/>

De emellett meg minden forgalmi adatod naplozodik az internetszolgaltonal is, akiket ugyebar a torveny kotelez a titkosszolgalatok feketedobozainak elhelyezesere.

Szoval szerintem a biztonsag olyan, mint a buddhista tokeletesség, elerni sosem lehet, de torekedni azert lehetosegeink es tudasunk szerint kell ra: megbizhatonak velt eszkoz valasztasaval, saját adatait titkossitasaval es gyakori mentesevel, digitalis alairással, egyeb megfelelo magatartással, stb. Addig is marad mindannyiunknak a biztonsag helyett a biztonsag illuzioja ;-)



9.

[-rb- július 20th, 2009 - 16:36](#)

Kedves evenorbert!

Nem írtam le, mivel foglalkozom. Nézd el nekem, hogy nem láttam, eddig, hogy ez itt szokás! (Nálad sem láttam, de azért ez a nevedre kattintva egyértelműen kiderül...)

Hát leírom hát kérdésedre:

Cégeknek segítek, hogy hatékonyabban működjenek informatikai megoldások segítségével. Kifejezetten KKV-knak abban, hogy saját árszínvonalukon megkapják azt a hatékonyságot, amit az informatika a nagyoknak már biztosít!

Ez pedig legátfogóbb módon és a legjobb ár/érték aránnyal, a legkisebb kockázattal, a legtöbb szakértőtől, a legtöbb esetben ma MS megoldásokkal biztosítható.

Ez nem jelenti azt, hogy ne lennének remek OpenSource megoldások is. Magam is használlok ilyeneket. Az egyik blogom is WordPressen fut. (Katt a nevemre és lásd!) Sőt a Microsoft is futtat számos ilyen projektet a neten. Sőt az MS-től függetlenül, MS technológián is sok ilyen projekt van.

Tehát semmi ellenvetésem az Open Source-al szemben. Sőt szeretem az Open Source-ot!

Ezzel együtt azt gondolom, hogy az Open Source / nem OS kérdés az IT szakma belügye. Ha az üzletet ez kell, hogy érdekelje, ott valamit nem csinál jól az IT / tanácsadó.

Mutass nekem egy olyan felhasználót, aki böngészőt, vagy operációs rendszert akar magának fordítani!

Egy rendszer konfigurálhatósága, kiterjeszhetősége elsődlegesen nem a forráskódján keresztül kell, hogy megvalósuljon. Pontosabban baj, ha azon keresztül valósul meg. Különben nincs felelős...

Az eredeti bejegyzésemben mindössze a két kijelentés igazságtartalmát vontam kétségbe. (Szerintem más miatt jó az Open Source. És az előnye mellett vannak hátrányai is szép számmal.)



10.

Újvárosy Attila [július 20th, 2009 - 16:53](#)

Kedves -rb-!

Nem értek veled egyet, több dologban sem. Az első állításod szerint, az nyílt forráskódú programok nem biztonságosabbak, "15-20 év után is kerülnek elő hibák". Példák nélkül ez eléggé sarkított, mert folyamatos fejlesztés alatt állnak a programok, javítások/frissítések pedig rövid időközönként megjelennek.

Az általad leírt "lusta rendszergazda" -ha létezik- bárhol előfordul, az általa kezelt hálózatot, jelszavakat ismerve zárt forráskódú programokban is tud kárt okozni, csakhogy ez bűncselekmény.

A második kijelentésed, miszerint "drágább az OpenSource" szerény véleményem szerint, finoman szólva butaság. :)

Tévhitben vagy, nem kell "áttérni a cégeknek", vagy "új munkaerő". Az APEH-nek is volt ilyen problémája, kiírtak egy pályázatot, melyen benne volt a pályázat leendő nyertesének neve, (... Microsoft szerű program...).

A Microsoft nem egyenlő az informatikával. Egy ténylegesen hozzáértő rendszergazda kell (nem Microsoftos "rendszer-adminisztrátor") és különben is hiba esetén szerintem egy komoly vállalat nem telefonál haza a szülőknak, rokonoknak és ismerősöknek; rendszereket sem kell "összeprogramozni", feltelepítjük, beállítjuk, karbantartjuk...)

Az esetek jelentős százalékában pedig nem "lehet a gyártót felelősségre vonni", mivel vagy nem volt jól beállított/karbantartott a rendszer, vagy egy szüneten lévő alkalmazott okozta a galibát, akarva vagy akaratlanul...



11.

[-rb- július 20th, 2009 - 17:03](#)

@buherator

Köszönöm, hogy válaszolsz a megjegyzésemre!

Némi kiegészítése:

1) Ez igaz. Biztonságra nem is tudok jó definíciót. Ha tudsz, dobd!

Talán a biztonsági kockázat van a legközelebb. Ez meg nem csak a rendszertől függ. Hanem például a rendelkezésre álló időtől, a szükséges eszközöktől, a szükséges felkészültségtől és a védett értéktől is.

2) Ez MS esetében úgy néz ki, hogy a 3rd party frissítést nem a Windows végzi. Sőt vállalati környezetben a Windows-ok nem is érik el az internetet, hiszen azt tűzfal védi. Az MS menedzsment megoldásai pedig képesek tetszőleges rendszer konfiguráció, vagy 3rd party alkalmazás frissítésére is.

Ezen kívül megcsinálnak egy adag más dolgot is, ha akarod: szoftver leltár, távoli segítségnyújtás, virtualizáció, esemény napló konszolidálása, hardver felügyelet, ...

3) Ebben is maximálisan igazad van.

Itt éppen az Open Source és a FREE fogalom keveredése miatt szólt a kritika. Sőt, ami FREE, nem feltétlenül olcsó.

Természetesen Open Source-ban is vannak nagyon jó szakemberek és cégek is. Néhány barátom zseniális dolgokat pakolt össze például.

Az ügyfelem szempontjából az a kérdés, hogy mi biztosítja, hogy ő éppen ilyen szakembert fog ki?

A Novellnek, meg az IBM-nek elhiszem. (Ők támogatnak hivatalosan Linuxot a nagyok közül) De az ő 1000 eurós napidijaikkal nincs olcsó FREE rendszer bevezetés...



12.

[-rb- július 20th, 2009 - 17:05](#)

Szia Csizmazia István [Rambo]!

A kommenteddel teljesen egyetértek!

A biztonság olyan idea, mint a mindig az égen maradó repülőgép. :-)



13.

[-rb- július 20th, 2009 - 17:38](#)

Kedves Újvárosy Attila!

Köszönöm, hogy kritikára méltatsz!

(Az külön öröm, hogy az első post, amit megtaláltam tőled "Ujjlenyomat-olvasó Ubuntu alatt" az épp áprilisban a születésnapomon született :))

A felvetéseiddel kapcsolatban:

- A 15 éves hiba emlékeim szerint a TCP/IP stack-ben jött elő 1-2 éve, és az "ősidők óta" tartalmazta a sérülékenységet, amivel vissza lehetett volna élni. Ezt arra hoztam példának, hogy attól, hogy valamit bárki megnézhet, nem következik semmi a biztonsággal kapcsolatban. (Az sem, hogy biztonságosabb az Open Source, és az sem, hogy nem. Ezt írtam le reményeim szerint.)

- Butaságnak minősíted az egyik kijelentésemet, amit nem találok. Ráadásul nem is indokolod, hogy miért. Segítenél nekem, hogy hol mondtam, hogy "drágább az OpenSource"? Reményeim szerint én csak kritériumokat állítottam ahhoz, hogy mikor tehetünk meg egy ilyen kijelentést. Ehhez hozzátettem azt a becslést, hogy 5-6% lehet az össz költségekben a licence beszerzés költsége. Ha valami az üzemeltetésben ennél többel olcsóbb, akkor összességében az az olcsóbb.

Ez annyira nagy butaság?

- Az APEH-os rész nem értem. Nem voltam ott, nem tudom, mire gondolsz. Kifejtenéd?

- Hogy egy Microsoftos rendszer üzemeltetését egy "rendszer-adminisztrátor" is meg tudja csinálni, nem kell hozzá "ténylegesen hozzáértő rendszergazda", ezzel teljesen egyetértek. Ezért lehet többek közt olcsóbban üzemeltetni egy Microsoft-os rendszert. Ha meg nagy a baj, akkor ott van mögötte a support.

- A Microsoft != informatika, ezt aláírom. Miért lenne? Persze, hogy nem ugyanaz...

- Hogy a gyártónak mi a szerepe, azt nagyon különbözően látjuk. Gyanítom, a gyártók is. Én azt a lepattintós stílust nem tapasztaltam, és nem irigyellek, ha neked ilyen partnerekkel kell

dolgozod. Leírom, mi az én tapasztalatom, és mi hogy dolgozunk support témákban:

- * Első, hogy a lehető leghamarabb működjön.
 - * Második, hogy ha működik, akkor az hosszú távon is stabilan működjön.
 - * Harmadik, hogy ne ismétlődjön meg a hiba.
 - * Ha a fentiek megvannak, akkor beszélünk az ügyfeleinkkel arról, hogy kinek a hibája volt. (Helyben állított el valaki valamit, termék hiba volt, mi vétettünk-e hibát.)
 - * Ha hiba bejelentés van, akkor az elhárítás "best effort" alapon történik. Azaz több szintű támogatásunk van, és egyel magasabb szinten is elkezdünk a problémával foglalkozni, mint ahol azt nagy biztonsággal meg tudják oldani.
- Ez azt jelenti, hogy ha véltetően magunk is megbírkózunk vele, akkor is bevonjuk a gyártó támogató mérnökeket, hátha ők még előbb boldogulnak.
- Így nem példa nélküli, hogy ha kell a Microsoft (de más partnert is említhetnék) olyan javítást készít, ami csak számunkra készül.

A lényeg, hogy az ügyfél üzlete menjen!

Én a saját gyakorlatomban nem látom ezt a felelősség elkenést, amiről írsz. Ez tényleg ilyen tipikus, ahogy írod?



14.

Újvárosy Attila [július 20th, 2009 - 18:41](#)

Kedves -rb-!

Elnézést a kései válaszáért, és úgy látom bocsánatot kell, hogy kérjem több dologban is. Én értettem félre néhány dolgot az OpenSource-os kijelentéseiddel kapcsolatban. A TCP/IP-s hiba az más, igazad van. Én azt hittem, valamilyen nyílt forráskódú program hibáját írod, de látom ez nem igaz.

A második kijelentésedből összességében azt szűrtem le, hogy drágább az fenntartása egy nyílt forráskódú vállalati rendszer fenntartása, elnézést a pontatlan idézésért. Ezen kijelentésemet a teljes második pontokra értettem.

Az APEH-os résznél én sem voltam ott, de például a számítógépes adóbevalláshoz szükséges programot először Microsoft operációs rendszerekre írták meg, minekutána az adóhivatal - tudomásom szerint- beperelte egy vállalkozó, mivel ő Machintos-t használ és ezzel őt kizárták ebből a lehetőségéből. Sajnos ezeket forrásokkal nem tudom most alátámasztani.

Az általam tapasztalt hibák -amiket én is láttam- azok tényleg vagy hibásan beállított rendszer miatt volt, vagy pedig böngészőbe -véletlenül- letöltött kártevők. Nem felelősség elkenés, hanem emberi tudatlanság, akár a rendszergazdáknál is, a támogatással általában nincs semmi gond.

A pontjaiddal egyetértek, viszont egy sokoldalú "linux rendszergazda" meg tud birkózni a problémákkal, és support is van a Közösség révén.

Összegezve én értettelek félre, és több dologban is igazad van/volt, annak tudatában, hogy nem vagy elvből "OpenSource-ellenes" másabb véleményem van.

Az OpenSource sem mindig biztonságosabb (emberi tényezők, esetleges hibák), viszont ez ellenpólusával is így van.

Utólag is boldog születésnapot...:)



15.

Szekeres Júlia [augusztus 7th, 2009 - 21:39](#)

Ezt most találtam, _nagyon_ komoly!

<http://www.saveie6.com/index.php>

Leave a reply

Név (szükséges)

Email cím (nem tesszük közzé) (szükséges)

Honlap

Hozzászólás küldése

•

Powered by WordPress - Az oldal tartalma szerzői jogvédelem alatt áll, jogtulajdonos: PC Kommandó Kft. Vidi Rita

[Kapcsolat, cégalapítás](#)

[Impresszum](#)

[Önbizalom](#)

[Önbizalom növelés nőknek](#)

Designed by [My Mobiles](#)