Az „Ugye megmondtam” hivatal jelenti #1

PClinuxOS Magazine – 2018. február

Írta: phorneker

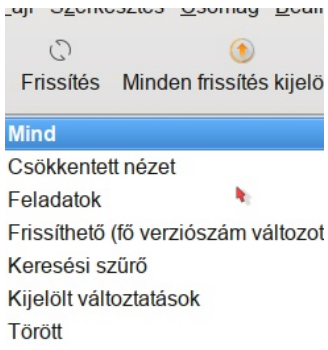
Az elmúlt két hónap során mondtam, hogy csak azért, mert PCLinuxOS-használók vagyunk, még nem vagyunk teljesen védve és biztonságban azoktól a problémáktól, amikkel Windows-ok és Mac OS-X-esek szembesülnek.

Az utóbbi két hétben két új kifejezés került a Linuxban színre: a Spectre és a Meltdown. Említettem, hogy szerencsések vagyunk, amiért nincsenek maleware-ek Linuxra. Ám a Spectre és a Meltdown is történetesen az utóbbi húsz évben készített mikroprocesszorokat érintő tervezési hiba, a **Linux-felhasználókat is érintő** biztonsági kockázatot jelentenek. (Vedd észre, hogy a sorozat címe „Én ugye megmondtam” hivatal jelenti.)

Szerencsére Texstar megfoltozta a 4.4-es, a 4.9-es és az aktuális kernelt, hogy kivédje a potenciális biztonsági problémát, amit a Meltdown és a Spectre okozhat.

Ennél fogva a kernel frissítése a legutóbbi, tárolóban elérhető verzióra kötelező.

A kernel frissítéséhez a PCLinuxOS-ben nyisd meg a Synaptic-ot és kattints az Frissítés-re.



Ha van frissített kernel a tárolóban, akkor azt az „**Új a tárolóban**” résznél találhatod meg. Bármelyik kernel nevű csomagot kiválaszthatod. Mind a **kernel**, mind fejlesztői csomagja kiválasztandó. Kattints az **Alkalmaz**-ra az új kernel telepítéséhez.

A Synaptic automatikusan frissíti a rendszerbetöltőt és jelzi a változtatásokat.

Ezután **indítsd újra a PCLinuxOS**-t (a frissített kernellel), hogy a végrehajtott változások érvénybe lépjenek.

Visszatérve a Spectre és Meltdown témájához, ezek a tervezési hibák az Intel processzorokban **az utóbbi húsz évben** jelen voltak. E tervezési rés segítségével a Cyber-támadók távolról megszerezhettek személyes információkat (jelszót is) anélkül, hogy észrevetted volna, vagy akár bejelentkeztek volna a PCLinuxOS-es gépedre, különösen olyankor, amikor a rendszer újraindítására volt szükség (pl. a Plasma frissítésekor). **Ez annyit tesz, hogy bármilyen, 1998 óta készített Intel-processzoros gép rendelkezik ezzel a tervezési hibával.**

Ennek fényében felmerül néhány komoly biztonsági kérdés.

Ahogy az Igazságügyi Minisztérium, MS elleni 1998. évi monopoliumellenes keresetével kapcsán kiderült, a Microsoft 1990-ben titkos egyezséget kötött a számítógép-gyártókkal, hogy csak Windows-t raknak a merevlemezre és nem ajánljanak fel semmilyen akkor elérhető alternatívát, mint az IBM OS/2 (most Arca Noae's ArcaOS) és a Solaris.

Mi volt ebben az Intel szerepe? Az eredeti IBM Personal Computer (5151-es) Intel 8088-as processzorra épült és nem Motorola 6502-es vagy 68000ás processzorral. Ahogy a személyi számítógépek piaca nőtt, a cégek és a magánszemélyek egyaránt **IBM PC kompatibilitást akartak**, ám azt olcsóbban. (Elég nyilvánvaló, nemde?)

Az 1990-es évek közepére a legtöbb személyi számítógép a piacon Intel processzoros és a merevlemezen Windows-zal telepített volt (mondván, hogy a vevők számára egyszerűbb legyen, én ezt sohasem gondoltam így).

Az eredmény a **Wintel monopólium** lett.

Ez azt jelentette, hogy a Microsoft és az Intel virtuálisan az egész hardver- és szoftverpiacot ellenőrizte. Azt is jelentette, hogy bármilyen hiba felmerülése esetén a két cég nyugodtan ülhetett rajta hónapokig, vagy éppen évekig, mielőtt bármit is tettek volna azzal kapcsolatban.

Ismerősen hangzik?

A Linux és a nyílt forráskód koncepciójának az 1998-as őszi Comdex-en a köztudatba kerülésének hála mindez változni kezdett.

A nyílt forrás koncepciója mögött (akár a Debian társadalmi szerződésénél) az az elv húzódott meg, hogy biztosítani kell a technológiai átláthatóságát. Azaz, bármilyen probléma felmerül, a lehető leghamarabb meg kell oldani és nem elrejteni a nyilvánosság elől.

Ez miért fontos? Ne nézzük visszább csak a WannaCry maleware-ig, és amit az Egyesült Királyságban egy kórház rendszerével tett. Az olyan kritikus helyeken működő számítógépek esetén, mint egy kórház, vagy egy nukleáris létesítmény, **elvárjuk a rendszerek megfelelően működését és a gondossá-got, illetve elvárjuk, hogy ezen rendszerek integritása ne sérüljön**, azaz úgy

vigyázzanak a gépekre, mintha az életünk függne tőlük, **mivel függ** is!

A kérdés itt ez:

Az Intel miért titkolta a tervezési hibát a nyilvánosság elől az utóbbi húsz évben?

Vajon ez teljes nemtörődömség az Intel részéről, vagy **égbekiáltó becstelenség.** A monopóliumok általános viselkedése az utóbbi két évszázadban az utóbbit mutatja. Egy problémát ilyen sokáig titkolni és pénzt csinálni belőle egyértelmű bizonyítéka a becstelenségnek ebben az esetben.

Annak köszönhetően, hogy a problémát szoftveresen javították (ahogy Texstar tette a kernellel), most rajtunk a sor, hogy alkalmazzuk a javításokat. Amit az Intel a cégektől akar, hogy **cseréljék le a régebbi számítógépeket újakra.**

Valaki mondhatná, hogy ezt a bejelentést a személyi számítógépek szűkülő piaca indukálta, alapvetően a mobil eszközök növekvő piaca miatt. Ugyanakkor a mobil eszközök piacának is megvan a része a fokozódó kínokban (konstrukciós hibák és maleware-k formájában, amik most az iOS és Android eszközöket érinti).

Úgy vélem, hogy a vevőknek elegük van abból a sok sz****ból, ami technológiai cégekből ered (legyen akár hardveres, vagy szoftveres természetű, csakúgy mint a hálózatból amihez kapcsolódnak) és különösen a Szilikon-völgyből.

És nem csak én gondolom így. Csak nézd meg Richard Stallman személyes honlapját (http://stallman.org) és észrevételeit a technológiával kapcsolatban. 1970 óta vesz részt a számítástechnikában és a nyílt forrású mozgalom egyik alapítója.

Szintén nézd meg a Free Software Foundation weblapját (https://www.fsf.org) és a Defective by Design (hibásra tervezett) weblapját.

Mivel nem bízhatunk a kormányunkban (állami és szövetségi szinten), hogy végzi a dolgát és megvédi a fogyasztókat (hol van ilyenkor Ralph Nader, amikor kellene?). Nekünk kell megoldani ezt a kérdést és képesnek kell lenni egységben és a többség egyetértésével meghozni a saját döntéseinket.

Megvan a saját véleményem a Microsoft kontra Igazságügyi Minisztérium 1998-as monopólium ellenes peréről, az Internet archívumában megtalálható.

Nos, mit csinálok a magam és a cyber-eszközeim védelmében?

Először is nem futtatom a laptopom a nap 24 órájában. Ez annyit jelent, hogy nem kell bekapcsolva tartani folyamatosan. Valójában akkor kapcsolom be, amikor kell és amikor nem használnom, kikapcsolom.

Azzal, hogy nincs folyamatosan bekapcsolva a gép, a számítógépes bűnözőknek nehezebb támadást végrehajtani … és ez jó dolog.

Másodszor, van egy több évtizedes vélekedés, ami még most is érvényben van. **Ha egy ajánlat túl szép ahhoz, hogy igaz legyen, valószínűleg nem az.** Legyen az akár egy levélszemét, vagy egy fertőzött email, az elv érvényes. Ugyanez van az ismeretlen telefonhívásokkal. Azok egyenesen az üzenetrögzítőre mennek. Ha fontos, a hívó hagy üzenetet. Ha nem, akkor valószínűleg nem fontos (vagy éppen nem törvényes).)

Harmadik, ha nem lehet eldönteni, hogy egy történet igaz-e, vagy álhír, az utóbbit feltételezem és nem hiszem el addig, amíg **el nem szállt a minden kétség** az információ hitelességét illetően.

Azok számára, akik még emlékeznek a „**Centennial**” TV-sorozatra (1980 körül) itt egy idézet, ami talán most is megállja helyét. A legutolsó idézetek egyike az utolsó részből, úgy az epizód vége felé találtam:

„Vissza kell néznünk a múltunkba és visszatérni az alapokhoz, ha szeretnénk, hogy legyen jövőnk,”