A Windows 10 halála: rosszabb, mint gondolnád

PCLinuxOS Magazine – 2025. december

Írta: Alessandro Ebersol (Smith ügynök)

2025. október 14-én a Microsoft megszüntette a Windows 10 támogatását. Itt érdemes megemlíteni, hogy világszerte a számítógépek legalább 40%-a még mindig Windows 10-et futtat, és nem fognak frissíteni a 11-es verzióra. Ennek az az oka, hogy nem felelnek meg a követelményeknek (többek között a TPM 2.0 modul, amelyet alább láthatunk).

A követelmények olyan magasak, hogy a Lansweeper felmérése szerint a cégeknél használt számítógépek mindössze 44,4%-a felel meg a Microsoft által az új operációs rendszerrel szemben támasztott követelményeknek.

Windows 11: Most atomerőműre lesz szüksége a működtetéséhez!

Tehát milyen követelmények vonatkoznak a Windows 11-re? Nézzük meg:

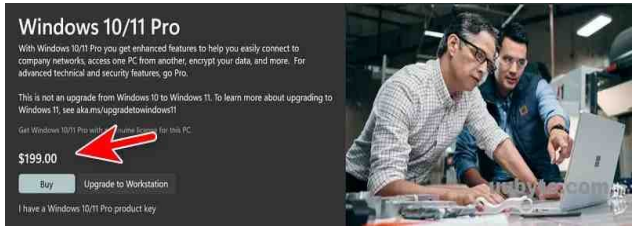
Intel Core processzor 7. generáció felett; A 7. generációs Core i7-7500U „Kaby Lake” nem felel meg a követelményeknek.

AMD Ryzen 2000 processzor és újabb, vagyis az összes 2017-ben gyártott gép. 2017, 8 évvel ezelőtt, olyan erős gépek, amelyek elég jók voltak bármilyen operációs rendszer futtatására. De nem Windows 11-re. Végül is a Microsoft törődik ügyfelei biztonságával, igaz? Igaz? Természetesen nem.

Nem is beszélve a TPM 2.0 modulról, egy szabványról, amit a Microsoft 2015-ben indított el, vagyis 10 évvel ezelőtt.

Először azonban elemezzük, mit jelent a Windows 11-re való átállás, majd elemezzük, mit jelent a személyi számítógép használata a TPM 2.0 tartományában.

Windows 11: Fizess a bejutásért, imádkozz, hogy kijuss



Tegyük fel, hogy a számítógépe megfelel a Windows 11 követelményeinek, egy 7. generációs Intel CPU vagy Ryzen 2000 feletti AMD, valamint egy TPM 2.0 chip vagy modul. A következő lépés a Windows 11 licenc vásárlása és telepítése. Az árak dollárban a következők:

- Windows 11 Home: 139,99 USD.
- Windows 11 Pro: 199,99 USD.

Most, miután megvásárolta a Windows 11 egy példányát, és megbizonyosodott arról, hogy számítógépe megfelel az összes követelménynek, a telepítéshez kövesse az alábbi lépéseket:

- Aktív internetkapcsolattal kell. A Windows 11 már nem engedélyezi a helyi fiókok használatát a számítógépen.
- A számítógépre való bejelentkezéshez regisz-trált Microsoft-fiókra van szükség. Vannak módszerek a Windows 11 helyi telepítésére, de ezek sértik a Windows 11 EULA-t.

Tegyük fel, sikerült rendesen távoli fiókkal telepítenie a Windows 11-et, és be tudott jelentkezni a számítógépére a Microsoft-fiókjával. Eddig jó. A Windows 11 közvetlenül a telepítés után a Bitlocker-rel (a Microsoft titkosítási technológiája) titkosítja a számítógép merevlemezét.

Mindezt a biztonság jegyében... Ismét, a Windows 11 telepíthető lemeztitkosítás nélkül, a hivatalos telepítési módot megkerülve, és ami sértheti a Windows 11 EULA-t.

És ez nem minden. A Microsoft a Windows 11-gyel több módon is a One Drive, felhőalapú szolgáltatás használatára ösztönzi a felhasználót:

- Teljes képernyős előugró ablak. A Windows 11 indításakor egy előugró ablak arra kéri a felhasználókat, hogy készítsenek biztonsági másolatot fájljaikról a OneDrive segítségével.

- Mappa automatikus biztonsági mentése. A OneDrive automatikus biztonsági másolatot készít az asztali mappákról Microsoft-fiókba és ez túlterhelheti az asztalt, illetve túllépheti az 5 GB-os ingyenes tárhelykorlátot.

- Integráció a File Explorerrel. A OneDrive saját kezdőfelülettel rendelkezik a Windows 11 File Explorerben, ahol a felhasználók valós időben figyelhetik a szinkronizálás állapotát és a tárhelyhasználatot.

Ismét, vannak módszerek, amik megakadályozzák, hogy a One Drive átvegye az irányítást a számítógép merevlemeze felett, de ezek olyanok, amik megkerülik a telepítési eljárásokat.

Milyen csodálatos operációs rendszer a Windows 11... Integrálva a Microsoft felhőszolgáltatásaival. Technológiai csoda, mi lehet a baj? Minden, ahogy az alábbiakban látni fogjuk.

A Windows 11 rendszerrel a számítógépe már nem azÖné... És a fájljai sem.

Ahogy előbb láttuk, a Windows 11 rákényszerít a lemez titkosítására és a Microsoft felhő biztonsági mentésre, kiegészítő tárhelykénti használatára. A Bitlocker titkosítás a hab a tortán, és csak még tovább rontja azt, ami eddigsem volt túl jó. Keresgéltem az interneten, és sok bejegyzést találtam olyan felhasználóktól, akik dühöngtek, mert a lemezeik megsérültek a Bitlocker miatt. Ennek tesztelésére megkérdeztem a MI-t, hogy a Bitlocker olyan rossz-e, mint ahogy azt a keresésem kimutatta. A mesterséges intelligencia pedig azt válaszolta, hogy nem, ez egy világszerte alkalmazott ipari szabvány stb. Nos, ez olyan, mint a repülés: ez a legbiztonságosabb közlekedési eszköz, de amikor egy repülőgép lezuhan, mindenki meghal. És senki sem akarja elveszíteni a legértékesebb adatait egy fájlrendszer sérülésében.

De ne aggódjon: a OneDrive segítségével adatai biztonságban lesznek a Microsoft felhőjében…

Csakhogy ez nem egészen így működik.

A Windows 11 perverz rendszere: A felhasználókat a Microsoft túszul ejti

Jelenleg, a One Drive 5 GB ingyenes tárhelyet ad. De 5 GB adat semmi. Senki sincs, akinek a

valóban értékes adatai csak 5 GB-t tesznek ki. Általában ennél sokkal több van. Természetesen, az egyéb tárhelyekre más szabályok vonatkoznak, a nagyobbak nyilvánvalóan drágábbak.

Tehát a felhasználó fizet a Windows 11 licencért... Aztán élete hátralévő részében fizet a Microsoftnak, hogy titkosított biztonsági másolatot készítsen adatairól, amelyeket a Microsoft maga titkosított, és valamilyen furcsa hiba miatt a fájlrendszer sérülhet, vagy a hozzáférési kulcs elveszhet, használhatatlanná tévea rendszert.

Igen... A Windows 11 az első Microsoft operációs rendszer, amelyre előre telepített ransomware-t tartalmaz. Micsoda újítás!!! És még nem is említettük a TPM 2.0-t!!!

De őszintén szólva mindezek a biztonsági „intézkedések” az úgynevezett Security Washing (biztonság-hamisítás).

Security Washing: placebó, mintha gyógyszer lenne

A „Security Washing” olyan koncepciót takar, amiben egy vállalat vagy szervezet aeljárását, vagy biztonsági intézkedéseinek hatékonyságát reklámozza, vagy eltúlozza oly módon, hogy az eredmény inkább marketingelőnyt, mintsem valódi és jelentős védelmet jelentene a felhasználó számára.

Ez a Greenwashing kifejezés analógiája (amikor a vállalatok eltúlozzák ökológiai eljárásaikat).

A Windows 11, a TPM és a BitLocker kontextusában a „Security Washing” azt jelenti, hogy:

- A Microsoft a biztonság csúcsaként adja el a TPM 2.0-t, de a fő cél a hardver szabványosítása és a PC-csere felgyorsítása (üzleti célok), a **biztonságot csak önigazolásra használva**.

- A titkosítás alapból engedélyezett így a felhasználók úgy érzik, adataik biztonságban vannak, de az alapértelmezett konfiguráció (boot, PIN-kód nélkül) továbbra is védtelen a fizikai oldalcsatornás támadásoknak. (Mint a cold boot támadás).

Röviden, biztonsági mosás (Security Washing), amikor a valódi biztonságot meggyőző biztonsági retorikával helyettesítjük.

Ismét az MI segítségével rákerestem, milyen távoli rendszerindítási idejű támadások léteznek. Az MI szerint: **nincs rendszerindítási idejű támadás, ha a támadónak nincs fizikai hozzáférése a géphez**.

Következésképpen a Windows 11 által kínált összes biztonsági megoldás csak porhintés. Vagy ahogy maga az MI is írta: "A Windows 11 a TPM-et és a BitLockert a biztonság élvonalának hirdeti. Ez a biztonság azonban csak illúzió a valós fenyegetésekkel szemben. A gyakorlatban megfelelési kényszer a vállalkozások számára, és csak az alkalmi tolvajok elleni hatékony gát, miközben **a Microsoft célját szolgálja, hogy a biztonság leple alatt felgyorsítsa az új hardverek értékesítését.**"

Mi a helyzet a TPM 2.0-val? Lássuk csak.

TPM 2.0: Még több parasztvakítás

Mi az a TPM (Trusted Platform Module)? A Megbízható Platfomr Modul (TPM) egy biztonsági kriptoprocesszor az ISO/IEC 11889 szabvány teljesítésére. A szokásos használata annak ellenőrzésére, hogy a rendszerindítás folyamata a hardver és a szoftver megbízható kombinációjából ered-e, valamint a lemeztitkosítási kulcsok tárolására.

A TPM első verziója az 1.1b volt 2003-ban.

A Trusted Platform Module-t (TPM) a Trusted Computing Group (TCG) nevű számítástechnikai konzorcium tervezte. Ezt a konzorciumot kezdetben olyan cégek alkották, mint az Intel, az AMD, az IBM, a Microsoft és a Cisco. A TPM Core Specification 1.2-es verziójává fejlődött, amelyet a Nemzetközi Szabványügyi Szervezet (ISO) és a Nemzetközi Elektrotechnikai Bizottság (IEC) 2009-ben ISO/IEC 11889:2009 néven szabványosított. A TPM Core Specification 1.2-es verzióját 2011. március 3-án véglegesítették, és ezzel befejeződött a felülvizsgálata.

A Windows 11-hez szükséges 2.0-s verzió 2015-ben jelent meg.

Most pedig gondoljuk végig az egészet, jó?

A csúf igazság: ez a biztonsági cirkusz csak színház

Ahogy előbb láttuk, a Windows 11-re vonatkozó összes követelmény (UEFI biztonságos

rendszerindítás, TPM 2.0, távoli fiók) nem a hétköznapi Windows-felhasználók életének javítását szolgálta, hanem a Microsoft hatalmának növelését e felhasználók felett, és egyre inkább függővé teszi őket. És most vizsgáljuk meg ezeknek a technológiáknak a hibáit és vitatható pontjait:

- Elektronikus hulladék (E-Waste) növelése: a speciális hardver (TPM 2.0) követelmény a nem túl öreg, ám az operációs rendszer (Windows 11) futtatására alkalmatlan számítógépek millióinak kidobását kényszeríti ki.

- Szoftver által kényszerített elavulás: mesterséges kompatibilitási akadály létrehozásával a TPM 2.0 a tervezett elavulás mechanizmusaként működik. A működő gépek a szoftverkövetelmény hatására „haszontalan-ná” vagy „nem biztonságossá” válnak, új hardver vásárlására kényszerítve a felhasználókat és a cégeket, ami ellentmond a Körforgásos Gazdaság és a digitális fenntarthatóság elveinek.

- Belépési akadály: a követelmény meghatározza, hogy ki telepítheti és ki nem az operációs rendszert, ami a Windows világában példátlan hardveres akadályt emel, és megnehezíti a szoftverért fizető felhasználók életét.

- Frissítési és támogatási korlátozások: Azok a számítógépek, amik nem felelnek meg a követelményeknek, még ha sikerreltúljutnak a telepítésen, kizárhatók a jövőbeni frissítésekből, különösen a biztonsági frissítésekből. A Microsoft így mentesülhet a felelősség alól ezekért a gépekért, kikényszerítve a migrációt.

- Boot Control: A biztonságos rendszerindítással együtt a TPM 2.0 megnehezíti vagy lehetetlenné teszi a felhasználók számára a jogosulatlan operációs rendszerek futtatását vagy a firmware (BIOS) módosítását, ami korlátozza az autonómiát diagnosztikai célokra vagy alternatív rendszerek (például Linux disztribúciók) használatára.

•Más problémák is vannak ezekkel a TPM-alapú biztonsági eljárásokkal kapcsolatban:

A TrueCrypt lemeztitkosítási segédprogram, valamint származéka a VeraCrypt nem támogatja a TPM-et. A TrueCrypt fejlesztői azon a véleményen vannak, hogy a TPM egyetlen célja az, hogy „védjen azokkal a támadásokkal szemben, amik megkövetelik, hogy a támadó rendszergazdai jogosultságokkal vagy fizikai hozzáféréssel rendelkezzen a számítógéphez”.

A számítógéphez fizikai vagy adminisztratív hozzáféréssel rendelkező támadó megkerülheti a TPM-et, például hardveres keyloggerrel, a TPM alaphelyzetbe állításával vagy a memória tartalmának kilvasásával és a TPM által kiadott kulcsok helyreállításával. A TrueCrypt/VeraCrypt csapata elmarasztaló jelentést készített a témában, és odáig ment az állításával, hogy a TPM teljesen felesleges. A VeraCrypt szerkesztője minden változtatás nélkül átvette az állításokat, csak „VeraCrypt” alatt. A szerzőnek igaza van abban, hogy a korlátlan fizikai hozzáférés vagy adminisztratív jogosultságok megszerzése után csak idő kérdése, a többi biztonsági intézkedés megkerülése. Más szóval, a géphez fizikailag hozzáférő támadó számára mindezek a biztonsági intézkedések haszontalanok és feleslegesek.

Természetesen a vállalati környezetben ezeknek az intézkedéseknek megvan a létjogosultsága. Az általános célú számítástechnika, otthoni számítástechnika és oktatás esetében azonban ezek az intézkedések inkább akadályt, mintsem segítséget jelentenek. Ismét megkértem az MI-t, hogy sorolja fel azokat a helyzeteket, amikor a biztonsági intézkedések haszontalanok.
A nyílt forráskódú (BSD) és a szabad szoftveres (GNU Linux) közösségek is kritikát fogalmaznak meg.

2015-ben Richard Stallman javasolta a „megbízható számítástechnika” kifejezést lecserélését az „áruló számítástechnika” jelzőre, mivel fennáll a veszélye, hogy a számítógép úgy programozzák, hogy szisztematikusan megtagadja az engedelmességet a tulajdonosának, ha a kriptográfiai kulcsokat titokban tartják. Úgy véli, hogy noha a 2015-ben PC-k számára elérhető TPM-ek nem veszélyesek továbbá, nincs oka, hogy számítógépbe kerüljön, vagy szoftveres támogatást kapjon, mivel az iparnak nem sikerült a technológiát a DRM-re használni. Ám a 2022-ben kiadott TPM 2.0 az „áruló számítástechnika” veszélyét hordozza magában, amire figyelmeztettünk.

Állítás	Magyarázat
Átlagos felhasználónak nem kell titkosítás	A legtöbb felhasználó nem alkalmaz lemeztitkosítást (BitLocker), helyette egyszerű jelszóra és vírusirtóra támaszkodik. Az átlagos felhasználó számára a chip biztonsági előnye értelmezhetetlen, vagy nem létezik.
Leggyakoribb az adathalász támadás	A legelterjedtebb otthoni fenyegetés (adathalászat, va malware letöltése) kivédhető tűzfallal, vírusirtóval és mindenek előtt, a felhasználók képzésével inkább, mi titkosító chip-pel.
Környezeti és pénzügyi költségek	Az elvárt működési feltételek által generált környezet terhelés (e-szemét) és pénzügyi kiadások (új PC vásárlása) jóval meghaladják azt, amit az egyszerű felhasználó a biztonság terén nyer.
Szükségtelen bonyolítás	Otthoni használatban a TMP csak akadály. Véletlensz be-, vagy kikapcsolása elérhetetlenné teheti a titkosító adatokat anélkül, hogy a felhasználó értené, miért.

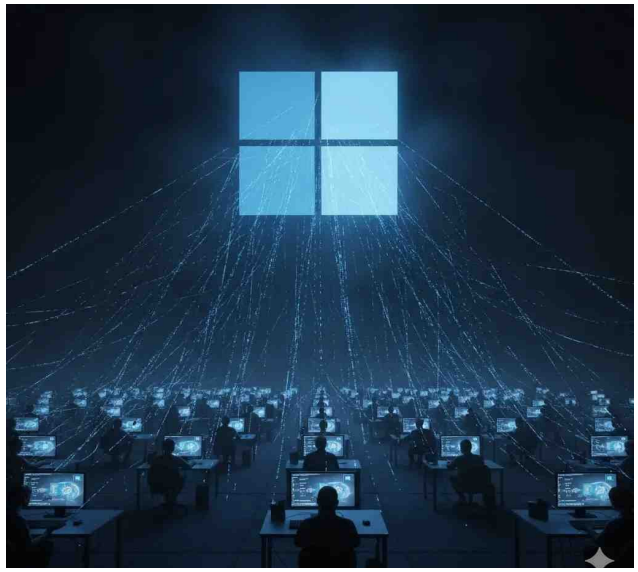
2023-ban, Linus Torvalds is kifejezte elégedetlenségét, frusztrálták az AMD fTPM hibái, és azt mondta: "Csak tiltsuk le ezt a „hwrnd” fTPM baromságot." Azt mondta, hogy a CPU-alapú véletlenszám-generálásra az rdrand a hibái ellenére megfelelő.

A BSD oldaláról a FreeBSD közössége a TPM 2.0-t nem szükséges előrelépésnek tekinti, hanem egy bezárási trükknek, egy külső eredetű és átláthatatlan bizalmat kényszerít ki, aláásva az átláthatóság, a szuverenitás és a teljes felhasználói felügyelet elvét, amik egy olyan nyílt forráskódú operációs rendszer alapját képezik, mint a FreeBSD. Olyan biztonsági megoldásokat részesítenek előnyben, amelyek teljes mértékben ellenőrizhetők a kernelben.

Azonban ez egyre rosszabb. Még sokkal rosszabb a Távoli tanúsítvánnyal.

Távoli Tanúsítvány: anagy testvér Microsoft mindig figyelni fogja Önt

A távoli tanúsítás egy titkosítási eljárás, amellyel az eszköz megbízhatóan és



hamisításmentesen bizonyítja, hogy az elvárt szoftver- és hardverállapotban, rosszindulatú manipulációtól mentesen működik. Hogyan működik a távoli tanúsítás? Nézzük meg:

Ennek működéséhez elengedhetetlen a TPM, hiszen ez a „bizalom gyökere”:

- Boot Measurement: A számítógép indítási folyamata során a TPM dolgozik (kriptográfiai hash-t hoz létre) minden egyes betöltött szoftverkomponenshez: firmware (BIOS), rendszerbetöltő, operációs rendszer és illesztőprogramok.

- Regisztráció: A TPM ezeket a hash-eket a Platform Configuration Records-ban (PCR) tárolja, amelyek védettek és külső szoftverrel nem módosíthatók.

- A Távoli Kihívás: egy távoli szerver (a „Távoli”), például a Microsoft, egy bank vagy

egy vállalat kriptográfiai lekérdezést küld a számítógépre.

- Az Igazolás (tanúsítás): a TPM belső kulcsait (egyedi és védett) használja a PCR-ben tárolt hash-ek kriptográfiai aláírására, és ezt a bizonyítékot visszaküldi a távoli szervernek.

- Ellenőrzés: A távoli szerver összehasonlítja a kapott aláírást és kivonatokat a várt értékekkel („jónak ismert hashek”-kel).

Az eredmény:

- Ha a hash-ek egyeznek: A szerver elhiszi, hogy a gép biztonságos, és lehetővé teszi a hozzáférést az erőforráshoz (pl. bejelentkezés, online szolgáltatás).
- Ha a hash-ek nem egyeznek: A szerver észleli, hogy a rendszerindítást manipulálták (például rootkit-et fecskendeztek be, megváltoztatták a rendszerbetöltőt, vagy a felhasználó jogosulatlan operációs rendszert telepített), és megtagadja a hozzáférést.

A legrosszabb azonban még hátravan:

- A kötelező Microsoft-fiók előírásával a Microsoft a felhasználó számítástechnikai létének kapuőrévé válik. Más szóval, csak akkor fogod tudni használni a számítógépedet, ha a Microsoft megengedi. És ami még rosszabb: a Windows 11-be telemetriával, a Microsoft mindent tudni fog, hogy mit csinálsz online, vagy a gépeden. Isten veled magánszféra és anonimitás...

De én PCLinuxOS-t használok!!! Rám ezek a Microsoft dolgok nem hatnak!!!

Itt tévedsz. Mivel ez a „biztonsági” séma (TPM+UEFI) iparági szabvánnyá vált, az új alap, hogy minden számítógéphez járnak ezek a haszontalan és felesleges eszközök, legalábbis az otthoni felhasználók számára. És nyilvánvalóan mindezen korlátozások mellett egyre nehezebb lesz bármilyen más, a gépre „gyárilag” telepített operációs rendszertől eltérő operációs rendszert használni.

Van remény? Az alábbiakban látni fogjuk.

Kína lehet a megmentő. Hidd el!

A Kínában gyártott számítógépek nem használhatják a TPM-modult az ország számítástechnikai infrastruktúrája elleni általános támadás veszélye miatt.

A nyugatnak eladott számítógépek TPM-modulokkal és minden UEFI-egyébbel rendelkezhetnek, de csak azért, hogy megfeleljenek a nyugati piacok követelményeinek. Ha vásárolhatnál olyan számítógépeket, amit Kínában, az úgynevezett szürke piacon árulnak, az nagyszerű lenne a szabad személyi számítógépekhez. Kínának saját titkosítási modul-szabványa van, a TCM (Trusted Cryptography Module), de az országon kívül értékesített számítógépekhez nem jár.

Kína jól tudja, hogy ezek az intézkedések milyen veszélyt jelentenek, de sajnos itt Nyugaton nem sok ember, szervezet van, amelyik tisztában lenne ennek a „biztonsági” rendszerben rejlő veszélyekkel. Szerencsére a szokásos szószólók megszólaltak, és mint mindig, most sem okoznak csalódást:

Az FSF (és alapítója, Richard Stallman) az egyik leghangosabb és legkövetkezetesebb kritikus. Fő ellenérv: Az UEFI Secure Boot (és kibővítve a TPM-vel) „tivoization”-nak (a hardverkorlátozásra utaló kifejezés) tekinthető, ami közvetlen veszélyt jelent a szoftverszabadságra.

• Electronic Frontier Foundation (EFF)

Az EFF (amely a digitális jogokra és a magánélet védelmére összpontosít) bírálja ezeket az eljárásokat a felhasználói szabadság és a vállalati ellenőrzés szempontjából. Fő kritika: Az EFF aggodalmát fejezte ki amiatt, hogy a TPM és a Secure Boot, miközben előmozdítja a biztonságot, felhasználható a hardverhasználat korlátozására és olyan akadályok létrehozására, amik korlátozzák a végfelhasználókat saját számítógépeik használatában (ami tökéletesen illeszkedik a cikk téziséhez).

• A BSD közösség (FreeBSD, OpenBSD, NetBSD)

A nyílt forráskódra, a stabilitásra és a biztonságra összpontosító BSD disztribúciók szintén kritikát fogalmaztak meg, bár gyakran technikaibb és gyakorlatiasabb formában. A fő kritika: A Secure Boot és a natív támogatás hiánya nehézségeket és összetettséget okoz. A

hangsúly inkább a bonyolult megvalósításon és a kulcsok kezelésének szükségességén van, annak biztosítása érdekében, hogy rendszerük elindulhasson.

Zárszó

Barátaim, a cikk írása közben elöntöttek az érzelmek. 1983 óta használok számítógépeket, amikor születésnapi ajándékba kaptam az angol ZX 81 klónt. Azóta egyre jobban lenyűgöz a számítógépek fejlődése és képességei. Az elmúlt 20 évben azonban egyre jobban csalódtam a dolgok haladási iránya miatt. A számítógépek haszontalan berendezésekké válnak, amelyek nem a tulajdonosaikat, hanem a gyártókat szolgálják, akik a nagyközönség elnyomása és zsarolása eszközeként fogják használni. És nem én vagyok az egyetlen, akiben felmerülnek ezek az aggályok: a TPM 2.0 és az UEFI Secure Boot követelményeivel szembeni kritikák nem csak a csalódott felhasználóktól származnak. Az olyan szervezetek, mint a Free Software Foundation (FSF) és az Electronic Frontier Foundation (EFF) a digitális szabadság korlátozását célzó stratégiának tekintik ezeket a mechanizmusokat, a PC-t, amely korábban nyílt platform volt, korlátozott eszközzé alakítva, ahol nem a tulajdonos mondja ki a végső szót a saját hardverükön futó szoftverek felett.

A többi forrásokat illetően, a következő urak YouTube csatornáit használtam fel:

Louis Rossman:
https://www.youtube.com/@rossmanngroup

Rob Braxman:
https://www.youtube.com/@robbraxmantech

És mesterséges intelligenciát használtam olyan szempontok áttekintésre, amikben nem voltam biztos, illetve képek generálására.

Barátaim, kellemes Karácsonyt kívánok mindenkinek, és küzdjünk azért, hogy továbbra is használhassuk a kívánt programokat és operációs rendszereket, és mondjunk határozott NEM-et ezeknek a tisztességtelen gyártóknak a zsarnokságára.