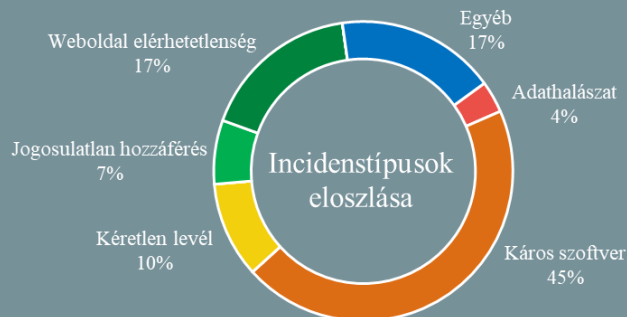


Az NKI által kezelt incidensekre
vonatkozó statisztikai adatok:
2021.10.08. - 2021.09.14.



Kövessen minket megújult [weboldalunkon](#), ahol friss IT biztonsági hírek kerülnek publikálásra!

Európai bankok felhasználóit vette célba egy veszélyes az új trójai kártevő (securityaffairs.co)

Számos szakértő egy új víruskampányra figyelmeztet, amely az európai bankok online felületeinek (e-banking) felhasználóit célozza meg a Hydra elnevezésű kártevővel. A MalwareHunterTeam és a Cyble kutatói szerint az új kampány elsősorban a Commerzbank, Németország második legnagyobb bankjának ügyfeleit érinti. A kiberbűnözők a Commerzbank hivatalos oldalának álcázva hoztak létre egy hamis weboldalt, és megegyező IP címen (91.214.124[.]225) több domaint is regisztráltak. A csalók a hamis weboldalt használták a fertőzött Commerzbank alkalmazások megosztására.

Bővebben...

Androidos felhasználók figyelem, ez nem fog tetszeni

(bleepingcomputer.com)

Egy angol egyetem kutatói aggasztó [eredményre jutottak](#) az androidos telefonok biztonságával kapcsolatban. A kutatók androidos Samsung, Xiaomi, Realme, és Huawei eszközöket, valamint két – az ígéret szerint „Google-mentésített” – Android forkot (LineageOS és /e/OS) vizsgáltak. Eszerint az e/OS kivételével a vizsgált készülékek még minimális használat esetén is jelentős mennyiségű adatot továbbítanak az operációs rendszer fejlesztőinek, és olyan harmadik feleknek, amelyek előtelepített rendszeralkalmazásokkal rendelkeznek (mint például a Google, a Microsoft, a LinkedIn, vagy a Facebook). **Bővebben...**

Az informatikai döntéshozók nem bíznak a kormányzati intézkedésekben, inkább az önvédelemre esküsznek (itsecurityguru.org)

Az Arctic Wolf átfogó [felmérést](#) készített több, mint 1400 angol, amerikai és kanadai cég informatikai döntéshozóinak bevonásával. Az ügyvezetők hozzáállását, különféle üzletet és kiberbiztonságot érintő kérdésekkel igyekeztek feltérképezni. A felmérés több érdekes eredményt is hozott. Például a vezetők mintegy 60%-a az előző évi jelentős kibertámadások miatt nem bízik abban, hogy a kormányzat képes megvédeni szervezeteiket a támadásoktól, így inkább saját magunknak biztosítják a védelemhez szükséges eszközöket. A legnagyobb félelmet az államilag – mint például Kína vagy Oroszország – által támogatott támadások okozzák. **Bővebben...**

Csúcstelefon potom áron? Vigyázat, könnyen lehet, hogy csalás! (heise.de)

Több ismert online webshopban – kínai AliExpress, amerikai Wish – gyanúsán olcsó, csúcstechnológiával (16GB RAM, 10 magos processzor stb.) rendelkező okostelefonokat kínálnak eladásra. A vásárlók gyanakvását a pozitív értékelések és a 30 napos pénzvisszatérítés gyakran elosztatja, azonban a rendelt termék helyett gyakran egy sokkal silányabb eszközt kapnak kézhez. Első ránézésre a rendelt készülék megegyezik a leírással, sőt a beállítások menüben is a meghirdetett specifikációk szerepelnek, ugyanakkor a tényleges telefon mögötti fizikai komponensek és a szoftvercsomag elavultak, számos biztonsági réssel rendelkeznek. **Bővebben...**

Apple felhasználók figyelem: ismét vészhelyzeti frissítést adott ki az Apple! (bleepingcomputer.com)

Az iOS 15.0.2 és az iPadOS 15.0.2 egy aktívan kihasznált nulladik napi hibát (CVE-2021-30883) [orvosol](#), amellyről a tech óriás csupán annyi információt tett közzé, hogy az *IOMobileFrameBuffer* memóriakezelési hibájából fakad, és sikeres kihasználás esetén a sérülékeny eszközön **kernel szintű** jogosultságot nyújthat a támadónak. **Bővebben...**

IT biztonsági Tanács



Az NBSZ NKI [weboldalán](#) megtudhatja miként készítheti fel hatékonyan munkatársait az adathalász támadásokkal szembeni védekezésre.