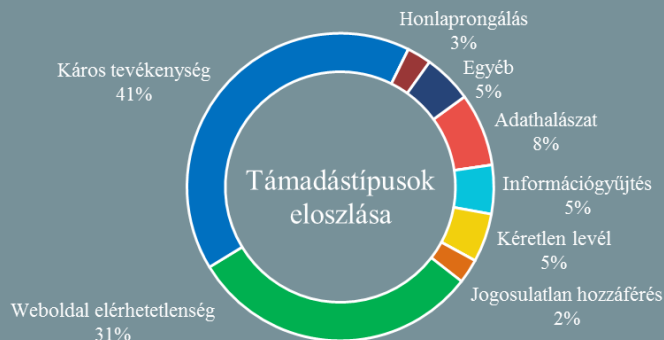


Az NKI által kezelt incidensekre
vonatkozó statisztikai adatok:
2020.08.19. - 2020.08.27.



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

Kibertámadás érte az új-zélandi tőzsdét

([itsecurityguru.org](#))

Az elmúlt néhány nap alatt második alkalommal állt le az új-zélandi értéktőzsde elosztott túlterheléses támadás (DDoS) miatt. A szolgáltatás kiesések a keddi értéknapi utolsó óráiban, valamint szerdán következtek be. Jamie Ahktar, a CyberSmart vezérigazgatójának elmondása szerint az elmúlt évtizedben óriási átalakuláson ment keresztül a pénzügyi szektor, jelentős lépéseket téve az automatizált kereskedelem irányába, például a különböző mesterséges intelligencia alapú technológiák bevezetésével. Azok a szektorok azonban, amelyek teljes mértékben a technológiai megoldásokra építenek a kiberbűnözők és hackerok kiemelt célpontjaivá válhatnak, ezért a biztonságuk elsődleges prioritást kell élveznie.

Bővebben...

Jelentős ráncfelvarrást kapott Androidon a Firefox

([thenextweb.com](#))

Firefox Daylight néven vált elérhetővé az androidos Firefox böngésző új verziója, ami több lényeges újítást tartalmaz. Ezek egy része adatvédelmi célú, ilyen az Enhanced Tracking Protection (ETP), amely megakadályozza a nyomkövető szkripteket (trackerek) a felhasználói adatok gyűjtésében, valamint azok hirdetésekhez való felhasználásában. Az ETP alapértelmezett üzemmódban engedi ugyan letöltödni a szkripteket, azonban azok nem férhetnek hozzá a böngészési adatokat tartalmazó sütihez (cookies). **Bővebben...**

Jön az Office sandbox vállalati Microsoft 365 ügyfeleknek

([bleepingcomputer.com](#))

Nyilvános tesztelési fázisba ért a Microsoft Defender Application Guard for Office alkalmazás, amelynek célja, hogy hatékony védelmet nyújtson a káros kódot tartalmazó dokumentumokkal szemben vállalati környezetekben. Az Application Guard nem más, mint egy sandbox, azaz egy teljesen elkülönített virtualizált környezet. Amennyiben a felhasználó ebben nyit meg egy káros kódot tartalmazó Office dokumentumot, a sandbox automatikusan blokkolni fogja a rosszindulatú tevékenységeket, mielőtt azok hozzáférhetnének a vállalat belső rendszereihez és fájljaihoz, vagy további káros összetevőket töltenének le. **Bővebben...**

Óvatosan a Google Drive-fájlok letöltésével!

([thehackernews.com](#))

Egy rendkívül veszélyes biztonsági hibára derült fény a Google Drive szolgáltatásban, amely lehetővé teszi, hogy rosszindulatú felhasználók egy teljesen legitim fájl "mögé" tetszőleges, akár káros kódot tartalmazó fájl rejtessenek. A probléma a "Verziók kezelése" funkciót érinti. Ez a szolgáltatás lehetővé teszi, hogy a Google Drive fiókunkban lévő fájlokhoz újabb verziót töltsünk fel, anélkül, hogy változna a fájl hivatkozása, ami másokkal történő megosztás esetében rendkívül hasznos.

Bővebben...

Adatszivárgás történt a Freepiknél

([bleepingcomputer.com](#))

Több mint 8,3 millió Freepik és Flaticon felhasználó e-mail címéhez és hashelt jelszavához szereztek hozzáférést ismeretlen elkövetők. (A Freepik a világ egyik legnagyobb online grafikai gyűjteménye.) A cég elmondása szerint a 8,3 millió felhasználó közül 4,5 millió felhasználónak kizárólag az e-mail címét szereztek meg, ugyanis ők a Google, a Facebook, vagy a Twitter fiókjukon keresztül léptek be az oldalak valamelyikére, ezért jelszavuk nem került tárolásra a Freepiknél. **Bővebben...**

IT biztonsági Tanács



Az NBSZ NKI [weboldalán](#) hasznos információkat olvashat arról, miként törölheti adatait androidos készülékéről.