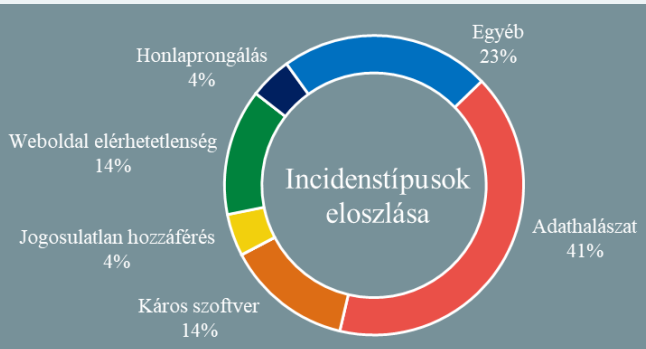
Nemzetközi IT-biztonsági sajtószemle

2021. 49. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.12.03. - 2021.12.09.



Kövessen minket weboldalunkon, ahol friss IT biztonsági hírek kerülnek publikálásra!

Hitelesített Twitter fiókokat vettek célba a támadók

(bleepingcomputer.com)

Miután a Twitter elkezdte tömegesével eltávolítani a kék pipával ellátott, hitelesített fiókmegjelöléseket, úgy vette kezdetét egy újabb adathalász kampány a közösségi platformon. A BleepingComputer által felfedezett hamis e-mailekkel, azokat a felhasználókat vették célba a támadók, akik a Twitteren megadták e-mail címüket és fiókuk rendelkezik még a hitelesítéssel. Az adathalász e-mailekben arra kérik a felhasználókat, hogy amennyiben nem akarják elveszíteni a felhasználói fiókuk hitelesített állapotát, úgy „frissítsék” adataikat. **Bővebben...**

Hamis ügyfélszolgálat „segíti” az áldozatokat az androidos banki trójai telepítésében

(bleepingcomputer.com)

Olaszországi banki adatok megszerzését célozza a BRATA néven ismert androidos távoli elérésű trójai (RAT) program új verziója. A fertőzés egy – látszólag – banktól kapott SMS-sel kezdődik, amelyben arra kérik az áldozatot, hogy telepítsen egy anti-spam alkalmazást, ami könnyen letölthető az SMS-ben kapott linken keresztül. A hivatkozás azonban valójában vagy a BRATA kártevőt letöltő káros weboldalra, vagy egy banki adathalász oldalra irányítja át az áldozatokat. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán az adventi nyereményjátékunkról olvashat bővebb információkat.

Új cookie szabályozás Németországban – ezek lesznek a változások

(heise.de)

A német adatvédelmi törvény célja, hogy megkönnyítse a cégek és a felhasználók számára a cookie-k és más nyomkövetési mechanizmusok kezelését. A szabályozás akkor lép életbe, ha például egy cég hozzáfér egy végkészülékhez, és ott információkat akar elmenteni, vagy tárolt adatokhoz szeretne hozzáférni. Az Európai Bíróság már többször döntött a GDPR szerinti hozzájárulási követelményekről, ami szerint a tényleges hozzájáruláshoz a felhasználónak aktív beleegyezését kell adnia. **Bővebben...**

Több száz sérülékenységet találtak a legnépszerűbb Wi-Fi routerekben

(securityaffairs.co)

A német CHIP IT magazin szerkesztői és biztonsági kutatói összesen 226 biztonsági sebezhetőséget fedeztek fel kilenc ismert gyártó, köztük az Asus, AVM, D-link, Netgear, Edimax, TP-Link, Synolgy és Linksys Wi-Fi routereiben. A lista élén a TP-Link Archer AX6000 áll, 32 azonosított sebezhetőséggel, ezt követi a Synology RT-2600ac 30 db hibával és a Netgear Nighthawk AX12 29 db sérülékenységgel. A leggyakoribb problémákat a firmware-ben elavult Linux kernel, a szintén elavult multimédia és VPN funkciók, a beégetett hitelesítő adatok, a nem biztonságos kommunikációs protokollok, valamint a gyenge alapértelmezett jelszavak – és azok nyílt szöveges tárolása – jelentették. **Bővebben...**

Tartalomvédelmi funkcióval bővült a Telegram

(bleepingcomputer.com)

Az új funkció lehetővé teszi a felhasználók számára, hogy a csoportbeszélgetésekben és a különböző csatornákban megosztott tartalmak esetén, tiltsák azok mentési és továbbítási lehetőségeit. Mindez arra szolgál, hogy a Telegramon közzétett bizonyos tartalmak, kizárólag a csoportban és a csatornákban részvevők számára legyen hozzáférhető. **Bővebben...**