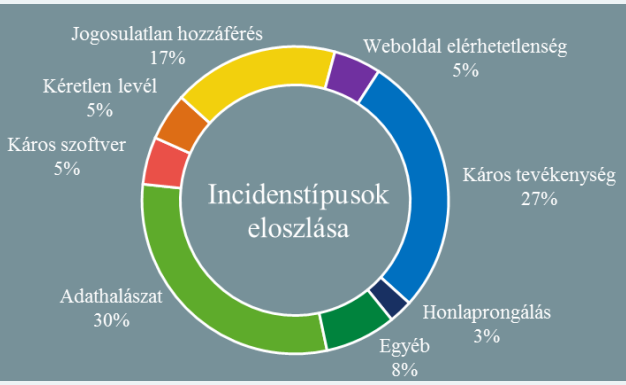
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 02. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.01.08. - 2021.01.14.



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

Kibertámadás érte Új-Zéland központi bankját

(securityweek.com)

Az új-zélandi tartalékbank (Reserve Bank of New Zealand – RBNZ) vasárnapi közleménye szerint "rosszindulatú" adatsértés történt egy harmadik fél által kezelt, szenzitív adatokat tartalmazó rendszerük esetében. Jelenleg nem ismert, hogy pontosan milyen információk érintettek, azonban a bank igazgatója szerint nem kizárt, hogy az incidens során érzékeny személyes és üzleti információk is kompromittálódtak. A szigetország esetében legutóbb tavaly augusztusban történt nagyobb kibertámadás, akkor egy szolgáltatás megtagadásos (DDoS) támadás a helyi tőzsde négy napos leállásához vezetett.

Fillérekért teljes kontroll szerezhető androidos telefonok felett

(zdnet.com)

A darkweben mindössze 29,99 dollárért beszerezhető Rouge RAT nevű káros programmal még a gyengébb képességű hackerek is teljes felügyeletet szerezhetnek az androidos eszközök felett. A távoli hozzáférési eszköz egy keyloggerrel fertőzi meg az eszközöket, amivel monitorozza a felhasználói aktivitást a meglátogatott weboldalakon és az alkalmazások használata során, így az áldozatok bejelentkezési és pénzügyi adatai is a támadók birtokába kerülhetnek. A rosszindulatú program teljes felügyeletet képes szerezni a fertőzött eszköz felett, és olyan kémfunkciókkal bír, mint a GPS követés, képernyőkép készítés, fénykép és kamerafelvétel készítése, hangrögzítés, stb. mindezt úgy, hogy az áldozatok mit sem sejtenek a háttérben zajló tevékenységekről. **Bővebben..**

IT biztonsági Tanács

Az NBSZ NKI weboldalán arról olvashat, hogyan válasszunk megbízható csevegő alkalmazást?

A WhatsApp valójában már évek óta megosztja a felhasználók adatait a Facebookkal, akkor mi változik február 8-tól?

(wired.com)

Amikor a Facebook 2014-ben felvásárolta a csevegő alkalmazást, sokan aggódtak, hogy a két platform között megosztásra kerülnek-e a felhasználói adatok. A WhatsApp két évvel későbbi adatvédelmi irányelvein eszközölt módosítás után mindez már nem volt kérdéses, a csevegő platform egyértelművé tette, hogy a felhasználók adatait elérhetővé teszi a Facebook számára. Igaz, ekkor a korábban regisztrált felhasználóknak még volt lehetőségük ─ bizonyos mértékig ─ kitérni ez elől, ugyanis 30 napig jelezhették, hogy nem járulnak hozzá adataik felhasználásához. **Bővebben...**

Penteszter eszközök rossz kezekben

(zdnet.com)

Évek óta tartó trend, hogy egyre jobban növekszik a nyílt forráskódú programok használata malware támadásokhoz köthetően, a behatolás tesztelő eszközök pedig ezek között is kitüntetett népszerűségnek örvendenek. (Ezek a programcsomagok alapvetően biztonsági szakemberek számára készülnek, informatikai támadásokat szimuláló, ún. penetrációs tesztek végrehajtásához, amelyek a rendszerek védekezőképességének felmérésére szolgálnak.) **Bővebben...**

Hogyan léphet túl az USA SolarWinds sokkon?

(schneier.com)

Bruce Schneier IT-biztonsági szakértő esszében foglalta össze gondolatait az utóbbi évek legnagyobb hatású kiberkémkedési incidenséről, a SolarWinds esetről. A gőzerővel tartó kivizsgálás során eddig már több, mint 250 egyesült államokbeli szervezet ─ köztük jónéhány szövetségi ügynökség ─ érintettségére derült fény, ám ez minden bizonnyal csupán a jéghegy csúcsa. Hatalmas kudarc ez az USA számára az államszervezet kiberbiztonsági felkészültségét tekintve, amelynek nemzetbiztonsági kockázata jelen pillanatban még fel sem mérhető igazán. Joe Biden elnökjelölt első reakciója a megtorlás volt. **Bővebben...**