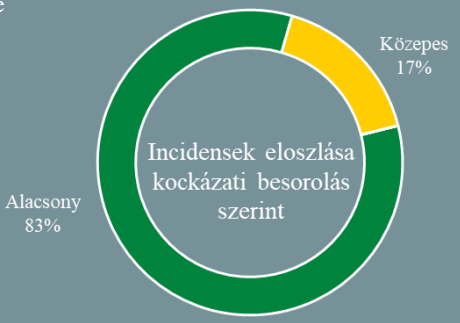
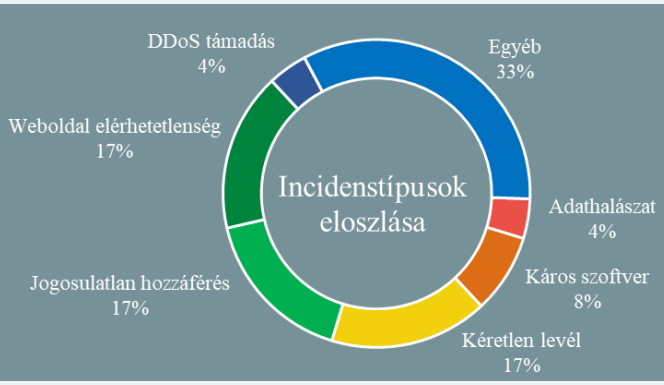
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2022. 03. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2022.01.14. - 2022.01.20.





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

A Microsoft Defender sérülékenysége megkönnyíti a rosszindulatú programok beágyazódását

(heise.de)

Antonio Cocomazzi, a SentinelOne IT-biztonsági kutatója tette közzé a Windows 10-es rendszereken található Microsoft Defender hozzáférési jogosultsággal kapcsolatos sérülékenységét. A biztonsági rés lehetővé teszi a támadók számára, hogy a rosszindulatú programokat elrejtsék a vizsgálatok elől, és így elkerüljék azok észlelését. Ennek oka, hogy a rendszer minden regisztrált felhasználója egy egyszerű paranccsal ki tudja olvasni a Microsoft vírusvédelem vizsgálati kivételeinek listáját. **Bővebben...**

Safarin keresztül kiszivároghatnak a felhasználók Google adatai és böngészési előzményei

(bleepingcomputer.com)

Probléma adódott a Safari WebKit motorjában az IndexedDB API implementációjával, aminek hatására valós időben szivároghatnak ki információk a felhasználó böngészési tevékenységéről. Az IndexedDB egy széles körben használt böngésző API, amely egy sokoldalú kliensoldali tárolórendszer. Általában webes alkalmazások adatainak gyorsítótárazására használják offline megtekintéshez, míg a modulok, fejlesztői eszközök és böngészőbővítmények érzékeny információk tárolására is használhatják. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán bővebb információt talál arról, hogy mi a teendő, ha a hitelesítő alkalmazás nem hozzáférhető.

A DHL lett a legnépszerűbb az adathalászok körében

(bleepingcomputer.com)

2021. utolsó negyedévében a DHL nemzetközi csomagküldő szolgáltató nevével éltek vissza legtöbbször az adathalász kampányok során. Mindez nem meglepő, figyelembe véve az év végi vásárlási szezont (Black Friday, CyberMonday), amikor jelentősen megnő a csomagkézbesítések száma. A DHL több mint 1,6 milliárd csomagot szállít évente, így a csomagküldő nevében küldött értesítésekkel nagyobb eséllyel érhetnek el eredményeket a támadók, főleg azoknál, akik valóban csomagot várnak. Az ilyen jellegű megkeresések gyakran valamilyen vámügyi problémára, például elakadt vagy vámkezelést igénylő csomagokra hivatkoznak, illetve gyakori, hogy a nyomkövetési számot tartalmazó mellékletek, vagy beágyazott linkek megnyitására igyekeznek rávenni az áldozatokat. **Bővebben...**

Gyanús tranzakciókról számoltak be a Crypto.com felhasználói

(zdnet.com) (securityaffairs.com)

A kriptovaluta tőzsdével foglalkozó szolgáltató, a Crypto.com 12 órára felfüggesztette a kifizetéseket és arra kérte ügyfeleit, hogy állítsák vissza kétfaktoros hitelesítő (2FA) adataikat, miután egyes felhasználók szokatlan, gyanús tevékenységet tapasztaltak számlájukon. A Crypto.com Twitter bejegyzése alatt néhány felhasználó arról panaszkodott, hogy számos – általában több ezer dolláros – levonásokat látnak a számlájukon, aminek következtében a szolgáltató kénytelen volt szüneteltetni a kifizetési tranzakciókat. **Bővebben...**

Megkerülhető volt a Box SMS-alapú kétfaktoros hitelesítése

(thehackernews.com)

Nyilvánosságra hoztak egy, a **Box** felhőalapú szolgáltatás többtényezős hitelesítési (MFA – Multi-Factor Authentication) mechanizmusát érintő biztonsági hiba részleteit, amit kihasználva megkerülhető volt az SMS-alapú bejelentkezés. A támadók ezzel a technikával és az ellopott hitelesítő adatokkal akár bizalmas szervezeti adatokat tartalmazó Box fiókokat is kompromittálhattak volna anélkül, hogy ténylegesen hozzáférnének az áldozatok eszközeihez. **Bővebben...**