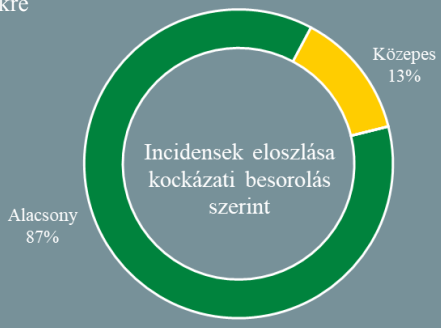
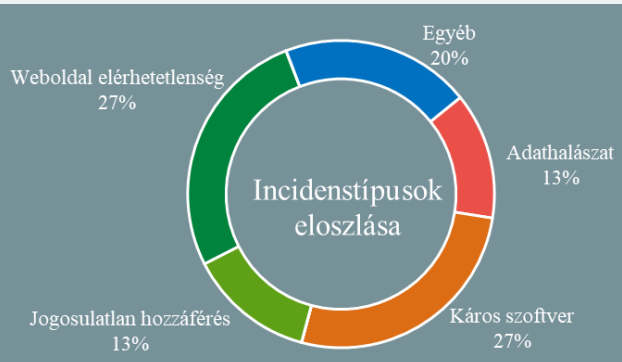
Nemzetközi IT-biztonsági sajtószemle

2021. 30. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.07.23. - 2021.07.29.





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

Ezek voltak az elmúlt két év leginkább támadott sérülékenységei

(bleepingcomputer.com)

Amerikai, brit és ausztrál kiberszervek az FBI-jal közösen biztonsági figyelmeztetést adtak ki az elmúlt évek Top 30 leggyakrabban kihasznált sebezhetőségről az Egyesült Államok kormányzati rendszereiből származó adatok alapján. Az eredményekből egyértelműen látszik, hogy az elmúlt év során fellendült távoli munkavégzést a fenyegetési szereplők is igyekeztek kiaknázni: 2020 leggyakrabban kihasznált sérülékenységei közül négy is összefüggésbe hozható távmunkával (pl.: VPN vagy felhő-alapú szoftverek). **Bővebben...**

Frissítsen, aktívan kihasznált nulladik napi hibát javított az Apple!

(support.apple.com)

Az Apple vészhelyzeti frissítést adott ki több rendszeréhez (iOS **14.7.1**, iPadOS **14.7.1**, and macOS Big Sur **11.5.1.**) egy nulladik napi biztonsági hiba (CVE-2021-30807) **aktív kihasználtsága** miatt. A sebezhetőség hátterében memóriakezelési hiba áll, sikeres kihasználás esetén kernel szintű távoli kódfuttatásra nyílik mód. A sérülékenység az alábbi termékeket érinti: macOS Big Sur, iPhone 6s (≤), iPad Pro (minden modell), iPad Air 2 (≤), iPad (5. generáció ≤), iPad mini (4 ≤), iPod touch (7. generáció). *Az NBSZ NKI javasolja a biztonsági frissítések mielőbbi telepítését!*

IT biztonsági Tanács

Az NBSZ NKI weboldalán bővebb információkat olvashat a biztonsági mentésekkel kapcsolatban.

Bosszantó és elég komoly hibát javítottak a Signalban

(bleepingcomputer.com)

Végre javításra került a Signal Android verziójának egy hónapok óta ismert hibája, amelynek következtében előfordult, hogy az üzenetekhez csatolt médiafájlok mellett további képek is továbbításra kerültek a címzettnek, látszólag teljesen véletlenszerűen. A hibát még 2020 decemberében jelentette Rob Connolly a GitHub-on, azonban a hiba reprodukálásának nehézségei miatt a csevegő platform csak e hónapban tudta javítani. A hosszú javítási időt sok felhasználó nehezményezte, mivel úgy tűnt a Signal nem veszi elég komolyan az egyébként privacy szempontból jelentős problémát. **Bővebben...**

Telegram és Chrome jelszavakra utazik egy mac-es vírus

(bleepingcomputer.com)

Új verzióval tért vissza a macOS-t futtató gépek ellen készült XCSSET nevű malware. A káros kódot fenyegetési szereplők korábban főleg Mac fejlesztők ellen vetették be, azonban a Trend Micro nemrég egy olyan változatot azonosított, ami már a felhasználók egy jóval szélesebb körére nézve is fenyegetést jelent. A mostani változat célja Telegram és Google Chrome felhasználói fiókadatok megszerzése, amit az üzenetküldő alkalmazás esetében meghökkentően egyszerűen valósít meg: kikopizza a teljes Telegram könyvtárat, amelynek birtokában a támadó bejelentkezhet a célpont fiókjába. **Bővebben...**

Adathalász-védelmi funkciót kap a Teams

(bleepingcomputer.com)

A Microsoft közleménye szerint a Microsoft Defender fejlett hivatkozásvédelmi funkciója, a Safe Links integrálásra került a Teamsbe, így a vállalati Teams felhasználók nagyobb biztonságban lehetnek az adathalász vagy egyéb káros célú hivatkozásoktól. Sajnos azonban ennek előfeltétele, hogy a szervezet rendelkezzen Microsoft Defender for Office 365 előfizetéssel. A Safe Links „kattintási időben” ellenőrzi az URL-eket, és megakadályozza a káros hivatkozások megnyitását a Defender naprakész fenyegetési információi alapján. **Bővebben...**