



HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2022.48. hét



HÍREK

- Figyelem: TikTok kihívást kihasználva terjesztenek káros kódot!
- Adathalász támadások várhatóak a Twitter adatszivárgások nyomán
- Folyamatosan támadják a Fortinet sérülékenységet
- Több újítást is hozhat a Twitter 2.0, ilyen például az üzenetek titkosítása
- Rosszindulatú kölcsönalkalmazásokkal verik át a felhasználókat



Heti IT biztonsági tipp

- IT biztonsági adventi kalendárium [2022]



STATISZTIKAI ADATOK

- Incidensek eloszlása típus és kockázati besorolás szerint

További érdekességekért és IT
biztonsággal kapcsolatos
tartalmakért látogasson el
közösségi oldalainkra!



[Nemzeti Kibervédelmi Intézet](#)



[@nki.gov.hu](#)



További érdekességekért, látogasson el [weboldalunkra!](#)

NEWS

IT biztonsági HÍREK IT biztonsági TIPP

Figyelem: TikTok kihívást kihasználva terjesztenek káros kódot! (therecord.media)

A Checkmarx [új jelentése](#) szerint kiberbűnözők egy népszerű TikTok kihívást kihasználva terjesztenek káros kódot. A Checkmarx nemrég egy másfajta veszélyre hívta fel a figyelmet az egyik új kihívás ("Invisible Challenge") kapcsán. **Bővebben...**

Adathalász támadások várhatóak a Twitter adatszivárgások nyomán (bleepingcomputer.com)

Egy hacker fórumon ingyenesen elérhetővé vált a júliusban még 30 000 dollárért árult, 5,4 millió Twitter felhasználó publikus és privát adatát is tartalmazó adathalom. **Bővebben...**

Folyamatosan támadják a Fortinet sérülékenységet (securityweek.com)

A Cyble nevű vállalat biztonsági kutatói október elején hozták nyilvánosságra a FortiOS, FortiProxy és FortiSwitchManager termékeket érintő kritikus kockázati besorolású sebezhetőség [\[CVE-2022-40684\]](#) leírását. **Bővebben...**

Több újítást is hozhat a Twitter 2.0, ilyen például az üzenetek titkosítása (thehackernews.com)

A Twitter vezérigazgatója, Elon Musk hivatalosan is megerősítette, hogy a tervek szerint hamarosan érkezik a platformon küldött üzenetek végponttól végpontig terjedő titkosítása (E2EE). **Bővebben...**



Rosszindulatú kölsönalkalmazásokkal verik át a felhasználókat (bleepingcomputer.com)

A Lookout biztonsági cég egy új jelentésében 251 db androidos és 35 db iOS-es hitelfelvétellel kapcsolatos rosszindulatú alkalmazás került azonosításra, amelyeket összesen 15 millióan tölthettek le, főként indiai, közép-amerikai és afrikai felhasználók. Az alkalmazások időközben már eltávolításra kerültek a hivatalos alkalmazásboltokból (Google Play Store és App Store), azonban a már letöltött appokat manuálisan kell eltávolítani az eszközökről. **Bővebben...**

IT biztonsági tipp



Az NBSZ NKI [weboldalán](#) elérhetővé vált az adventi naptárunk, ami minden napra egy IT biztonsági rejt.



További hírekért, látogasson el [weboldalunkra!](#)

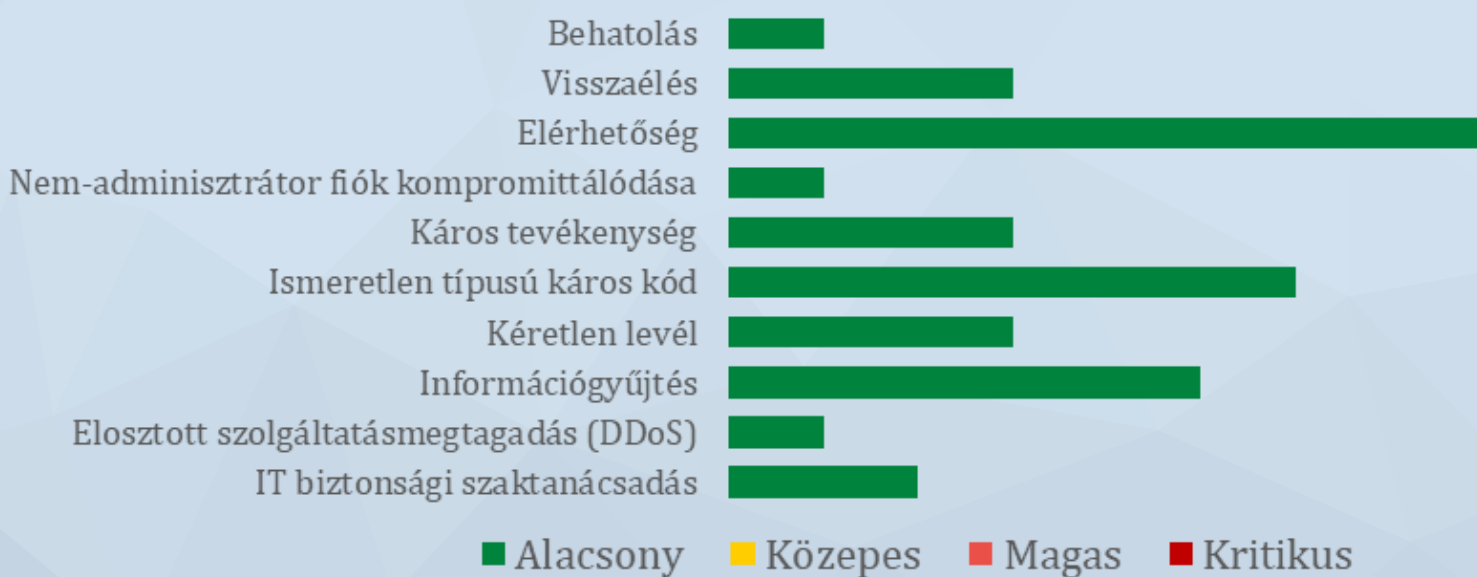
Statisztikai adatok

2022.11.25.-2022.12.01.

Az NBSZ NKI által
kezelt incidensekre
vonatkozó statisztikai
adatok:



Fenyegetettségi
szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

