NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2022.27. hét

HÍREK

- Helyzetkép: jelentős zsarolóvírus nyomás alatt az egészségügyi ágazat
- Aktívan kihasznált zero-day sérülékenységet javít a Chrome új verziója
- Túlterheléses támadás ért norvég állami weboldalakat és online szolgáltatásokat
- Céges sérülékenységi információkkal próbált pénzt keresni, fülön csípték a dolgozót

Heti IT biztonsági tipp

- Bemelegítünk a HCSC'22-re! Játssz velünk Te is, és nyerj NBSZ NKI ajándékcsomagot!

STATISZTIKAI ADATOK

- Incidensek eloszlása típus és kockázati besorolás szerint
- Események eloszlása csapdatípusok alapján
- Támadott port szerinti eloszlás

PODCAST

HCSC'22: a kedvenc kiberversenyed [házunk tája]

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

Nemzeti Kibervédelmi Intézet

@nki.gov.hu

További érdekességekért, látogasson el **weboldalunkra**!

NEWS

IT biztonsái

HÍREK

IT biztonsági

TIPP

Helyzetkép: jelentős zsarolóvírus nyomás alatt az egészségügyi ágazat

(news.sophos.com)

A Sophos közzétette a mintegy 31 ország, közel 400 egészségügyi szervezetének bevonásával végzett átfogó vizsgálatának eredményeit, amely az egészségügyi ágazat kiberfenyegetettségének — ezen belül is kiemelten a valós zsarolóvírus fenyegetési szint — felmérését célozta. **Bővebben...**

Aktívan kihasznált zero-day sérülékenységet javít a Chrome új verziója

(bleepingcomputer.com)

A legutóbbi biztonsági frissítés által javított, magas kockázati besorolású zero day sebezhetőség (CVE-2022-2294) a WebRTC (Web Real-Time Communications) komponenst érinti, amelyet a Google Threat Analysis Group (TAG) szerint észak-koreai kötődésű hackerek használnak ki széles körben. **Bővebben...**

Túlterheléses támadás ért norvég állami weboldalakat és online szolgáltatásokat

(securityaffairs.co)

A Norvég Nemzetbiztonsági Hatóság (NSM) közleménye szerint a múlt hét során túlterheléses (DDoS) támadás miatt vált elérhetetlenné több norvég állami weboldal. A hatóság szerint a kibertámadásokért egy orosz-barát kiberbűnözői szerveződés a felelős. **Bővebben...**

Céges sérülékenységi információkkal próbált pénzt keresni, fülön csípték a dolgozót

(bleepingcomputer.com)

Legtöbbször a figyelmetlenség a fő emberi kiberbiztonsági kockázat oka, de sajnos azzal is számolni kell, hogy van, aki szándékosan él vissza a szervezeti belsős információkkal. **Bővebben...**

Kémprogramok elleni védelemmel erősít az Apple

(zdnet.com)

Az Apple információkat bejelentette a majdani iOS 16, iPadOS 16 és macOS Ventura rendszerekben bevezetésre kerülő Lezárási mód (Lockdown Mode) elnevezésű új védelmi megoldását, amit elsősorban újságíróknak, aktivistáknak, és kormányzati alkalmazottaknak szánnak, kémszoftverek elleni megerősített védelem gyanánt. Az Apple úttörő megoldásként hivatkozik a funkcióra, Ivan Krstić, a cég biztonsági tervezésért felelős vezetője szerint habár a felhasználók csupán egy rendkívül kis hányadát érintik a szofisztikált célzott kibertámadások, a cég mindent megtesz azért, hogy az ő biztonságukról is gondoskodjon. **Bővebben...**

IT biztonsági Tipp

Folytatódik a **HCSC'22–es nyereményjátékunk**, bővebb információ az NBSZ NKI weboldalán található.

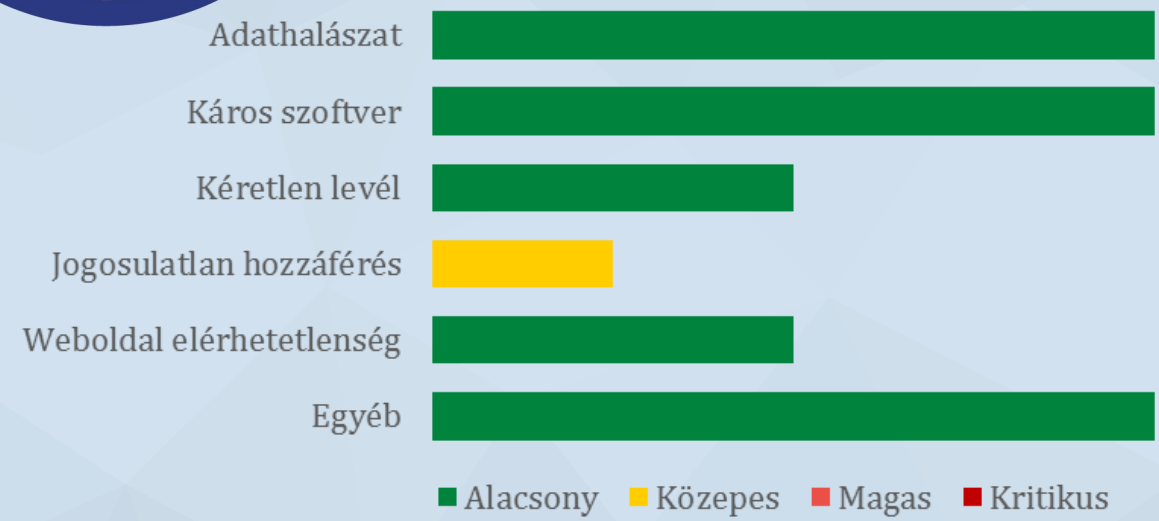
További hírekért, látogasson el **weboldalunkra**!

Statisztikai adatok

2022.07.01-2022.07.07.

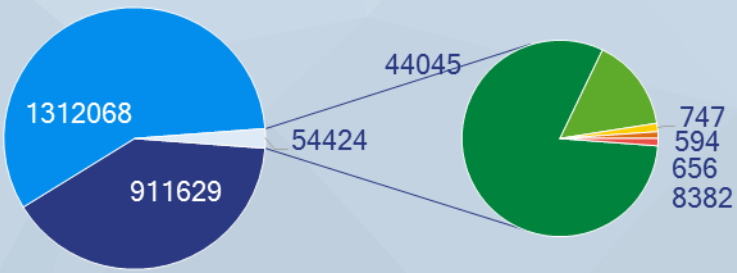
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: közepes

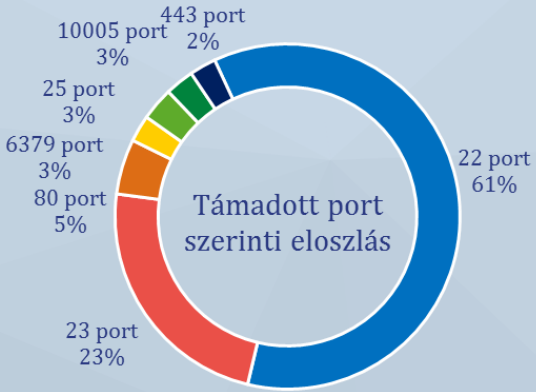


Incidensek eloszlása típus és kockázati besorolás szerint

Az elosztott kormányzati IT-biztonsági csapdarendszerből (Gov1probe) származó adatok:



Események eloszlása csapdatípusok alapján



További információkért, látogasson el **weboldalunkra**!