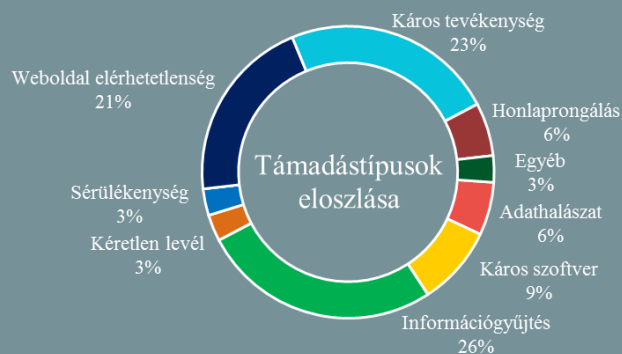


Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2020.10.30. - 2020.11.05.



Kövessen minket megújult [weboldalunkon](#), ahol friss IT-biztonsági hírek kerülnek publikálásra!

Az ipari vezérlőket célzó kibertámadások több, mint 12%-a nemzeti támogatású hackerekhez köthető

(securityweek.com)

A (CS)2AI (Control System Cyber Security Association International) és a KPMG közös [jelentést publikált](#) az ipari vezérlőrendszereket (industrial control systems – ICS) és operatív technológiákat (operational technology – OT) célzó kibertámadásokról. A jelentés alapjául szolgáló felmérést a (CS)2AI több mint 16 000 tagszervezete közül mintegy 600-an töltötték ki, 80%-ban a szervezetek döntéshozói. **Bővebben...**

Hibás proxy konfiguráció miatt belső IP címeket szivárogtatott ki az Applebot

(bleepingcomputer.com)

Az Apple-nek érthetetlen módon közel kilenc hónapba telt orvosolnia egy rosszul konfigurált proxyki-szolgáltató okozta információszivárgási hibát. David Coomber biztonsági kutató 2019 decemberében jelezte először az Apple-nek, hogy a cég webes tartalmakat indexelő programja, az Applebot belső IP címeket szivárogtat. Coomber felfedezte, hogy a probléma háttérben hibás proxybeállítás állhat, ugyanis az Applebot “Via” és “X-Forwarded-For” fejléceket tartalmazó kéréseket küldött a webservereknek, amelyekben megtalálható a proxyszerver IP címe. **Bővebben...**

Egyes esetekben tanúsítvány problémákat okozhat a Windows 10 verziófrissítése

(zdnet.com)

A Microsoft [mege erősítette](#) azon [felhasználói visszajelzéseket](#), amelyek szerint egyes digitális tanúsítványok törölhetőek a Windows 10 1809-esnél frissebb verziójára történő átállásakor. A tanúsítványok elvesztése több szempontból is problémás, különösen most, a távmunka időszakában, ugyanis a legtöbb VPN megoldás (is) ezekre támaszkodva működik. Kiderült azonban az is, hogy a hiba csak bizonyos kondíciók mellett jelentkezik. Eszerint azon rendszerek érintettek, amelyekre a 2020 szeptemberi – vagy ennél frissebb – frissítő csomag (latest cumulative update – LCU) telepítésre került, a verziófrissítés azonban egy olyan kiadásra történik, amely nem tartalmazza legalább az októberi frissítést. **Bővebben...**

FBI: így férték hozzá iráni hackerek amerikai választási rendszerekhez

(bleepingcomputer.com)

A DHS CISA és az FBI [információkat hozott nyilvánosságra](#) arról, hogy iráni hackerek szavazói regisztrációs adatokat tulajdonítottak el amerikai szövetségi portálokról. A támadók először az Acunetix sérülékenységkereső szkennel segítségével derítették fel a célkeresztben álló weboldalakat biztonsági hibáit, majd az azonosított sérülékeny, vagy rosszul konfigurált szerverekről sikeresen töltötték le szavazói adatokat 2020. szeptember 29. és október 17. között. **Bővebben...**

Kevésbé szenzációhajhász sérülékenység elnevezésekért kampányol a CERT/CC

(zdnet.com)

A Carnegie Mellon Egyetem CERT Coordination Center (CERT/CC) egy Twitter bot formájában ([vulnonym](#)) új kezdeményezést indított, amely a feleslegesen ijesztő elnevezések helyett véletlenszerű neveket rendel a biztonsági hibákhoz. A lényegesebb sérülékenységek azonosítására évtizedek óta szolgál a MITRE Corporation által gondozott Common Vulnerabilities and Exposures (CVE) rendszer. **Bővebben...**

IT biztonsági Tanács



Az NBSZ NKI [weboldalán](#) hasznos információkat olvashat a Windows 10 verziófrissítéséről.