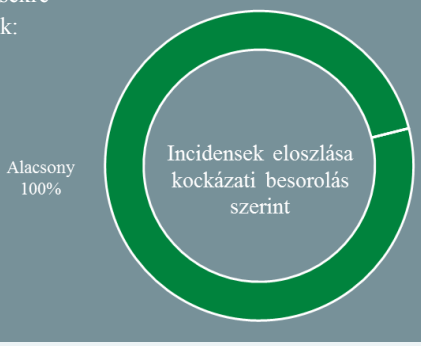
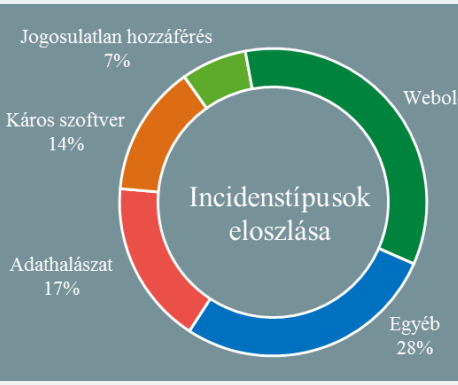
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 24. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.06.11. - 2021.06.17.





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

Amerikai nukleáris fegyverzeti programban közreműködő alvállalkozótól lopott adatokat a Revil zsarolóvírus banda

(bleepingcomputer.com)

A REvil zsarolóvírus csoport egy májusi támadás során adatokat szerzett az amerikai Sol Oriens nevű cégtől, amely többek között nukleáris fegyverzeti tanácsadással is foglalkozik. A Sol Oriens önmeghatározása szerint az amerikai védelmi és energiaügyi minisztérium alá tartozó szervezetek, légügyi és más technológiai cégek számára nyújt támogatást „komplex projektekkel kapcsolatban" ─ írja a BleepingComputer. **Bővebben...**

Régebbi Apple készüléke van? Mielőbb frissítse!

(thehackernews.com)

Az Apple hétfőn soron kívüli frissítést adott ki az iOS **12.5.3** verzióját érintő – aktívan kihasznált – nulladik napi sérülékenységek miatt. Az iOS 12.5.4 három sebezhetőséget javít, köztük az ASN.1 dekóderben észlelt memória gondokat (CVE-2021-30737), valamint két WebKit böngészőt érintő sérülékenységet (CVE-2021-30761, CVE-2021-30762), amelyek kihasználása távoli kódfuttatást tesz lehetővé a támadók számára. Utóbbi két sebezhetőséget a cég szerint aktívan ki is használhatják, bár erre vonatkozó konkrétumokat nem közölt az Apple. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán az SMS-ben érkező kódokkal kapcsolatos csalási módszerről olvashat hasznos információkat.

Új típusú TLS támadás vált ismertté a biztonságos(nak hitt) weboldalak ellen

(thehackernews.com)

A kutatók egy újfajta támadást fedtek fel, amelynek során a TLS szerverek hibás konfigurációit kihasználva a támadó átirányíthatja a HTTPS forgalmat az áldozat webböngészőjéből egy másik TLS szolgáltatás végpontjára, és ezáltal érzékeny információkhoz juthat. A módszert a Ruhr, a münsteri és a paderborni egyetemek akadémikusaiból álló csoport ALPACA-nak nevezte el, ami az "Application Layer Protocol Confusion – Analyzing and mitigating Cracks in tls Authentication" rövidítése. **Bővebben...**

Samsung mobiltelefonok veszélyben: nemsokára kritkus hibajavítás érkezik!

(bleepingcomputer.com)

Mobiltelefonjait érintő kritikus hibák javításán dolgozik a Samsung, amelyeket kihasználva a kiberbűnözők kémkedhetnek utánunk, sőt, akár át is vehetik az irányítást a készülékünk felett. A sérülékenységeket egy mobilbiztonsággal foglalkozó biztonsági kutató, Sergey Toshin fedezte fel, aki január óta már több, mint egy tucat sebezhetőséget jelentett a Samsung hibavadász (bug bounty) programján keresztül. Nagy részüket a gyártó az elmúlt hónapok során javította is, azonban három kritikus hiba még befoltozatlan, és azt sem tudni pontosan, hogy a Samsung mikor teszi elérhetővé a hibajavítást ügyfelei számára. **Bővebben...**

Kiberbiztonsági ügynökséget állít fel Olaszország

(securityweek.com)

Múlt hét során jóváhagyták Olaszországban egy nemzeti kiberbiztonsági ügynökség létrehozását, annak érdekében, hogy növeljék az ország, valamint az EU számítógépes fenyegetésekkel szembeni ellenállóképességét. Mario Draghi olasz miniszterelnök május végén fokozott nemzeti és uniós szintű fellépést sürgetett a kibertérből érkező – leginkább orosz – fellépésekkel szemben, beleértve a kémkedést és az internetes tartalmak manipulálását. **Bővebben...**