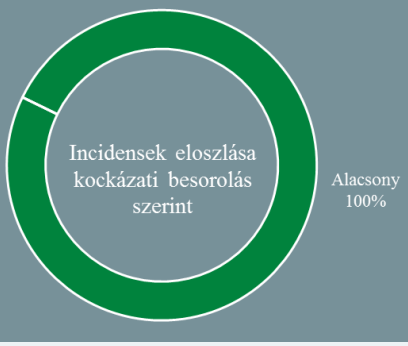
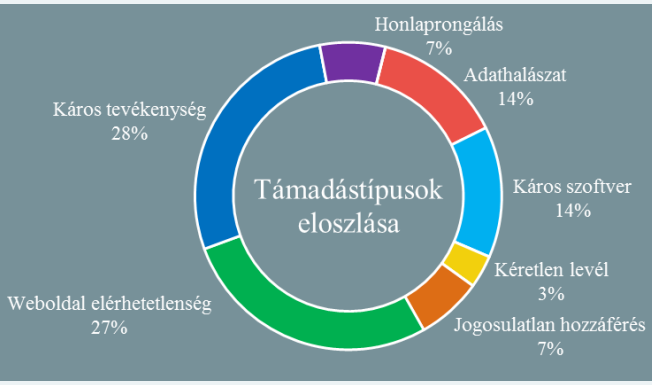
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 31. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.07.24. - 2020.07.30.





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

Komoly biztonsági hibákat találtak népszerű ipari VPN termékekben

(securityweek.com)

Az ipari rendszerek biztonságával foglalkozó Claroty komoly sérülékenységeket azonosított ipari környezetekben ─ főleg az olaj- és gázszektorban ─ népszerű VPN termékekben. A kérdéses eszközök (Secomea GateManager, a Moxa EDR-G902, az EDR-G903, valamint a HMS Networks-féle eWon) titkosított hozzáférési csatornát hoznak létre a vállalati belső rendszerekhez, amit például a rendszerek távoli felügyeletére használnak. A Claroty arra hívja fel a figyelmet, hogy a felfedezett sebezhetőségek között található olyan, ami felhasználható távoli kódfuttatásra, szolgáltatás megtagadásos kondíció teremtésére, vagy az adatok manipulálására, és akár fizikai károkozás is kivitelezhető általuk. Gyártói hibajavítások már elérhetőek, ezek telepítése mindenképp javasolt.

Súlyos adatszivárgás a Dave.com-nál

(securityaffairs.co)

A népszerű digitális banki alkalmazás, a Dave.com elismerte az adatszivárgási incidenst, amely több, mint 7 millió ügyfélrekord kompromittálódásához vezetett ─ miután értesítésre került, hogy az adatokat a "ShinyHunters" néven elhíresült kiberfenyegetési szereplő posztolta egy darknetes hacker fórumon. Többek közt felhasználói azonosítók, telefonszámok, e-mail címek, Risepay és Synapsepay azonosítók érintettek, valamint egyes ügyfeleknél a fizetésre használt bankkártya adatai is, enkriptált formában. Az eddigi vizsgálatok szerint az érzékeny információk egy korábbi üzleti partnertől (Waydev) származtak. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat miként készíthet biztonsági mentés a fájl-előzmények használatával.

Újonnan felfedezett DDoS támadási vektorokra figyelmeztet az FBI

(zdnet.com)

Az amerikai Szövetségi Nyomozó Iroda olyan hálózati protokollokra hívja fel a figyelmet, amelyekről kiderült, hogy felhasználhatóak elosztott szolgáltatásmegtagadással járó támadások során. A figyelmeztetés három hálózati protokollra (**CoAP** – Constrained Application Protocol, **WS-DD** – Web Services Dynamic Discovery- **ARMS** – Apple Remote Management Service) és a Jenkins webalapú automatizációs szoftverre vonatkozik. **Bővebben...**

Nem álltak le a Fancy Bear kiberműveletek

(wired.com)

Az orosz katonai hírszerzéshez (GRU) több agresszív kiberművelet is kötődik, például az ukrán energiaszektor elleni támadások (2015), a legutóbbi amerikai elnökválasztás befolyásolása (2016), vagy épp a NotPetya malware terjesztése (2017). Úgy tűnik a GRU egyik hírhedt kiberkémkedési egysége, a APT28 (vagy más néven Fancy Bear) az elmúlt egy-másfél évben egy nagyszabású, amerikai célpontok elleni hacker támadási kampánnyal volt elfoglalva. **Bővebben...**

Figyelem: QNAP NAS-ok veszélyben

(securityweek.com)

Amerikai és brit kibervédelmi szervek közös riasztásban hívják fel a figyelmet QNAP NAS-ok elleni vírusfenyegetésre. A figyelmeztetés alapja a tavaly felfedezett, QSnatch névre keresztelt malware, amelyet az elmúlt években több támadási kampány során (2014-2017, majd 2018-2019 között) is alkalmaztak QNAP eszközök ellen. Habár a QNAP tavaly novemberben már adott ki biztonsági figyelmeztetést, amiben megelőző intézkedésekre is kitérnek, 2020 júniusi adatok szerint mégis több, mint 62 000 eszköz volt fertőzött világszerte. **Bővebben...**