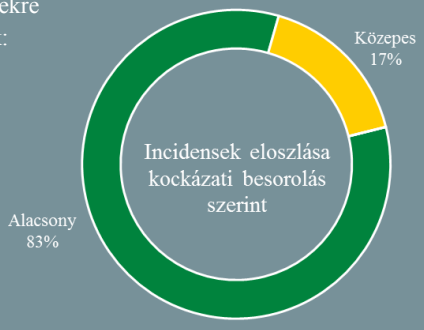
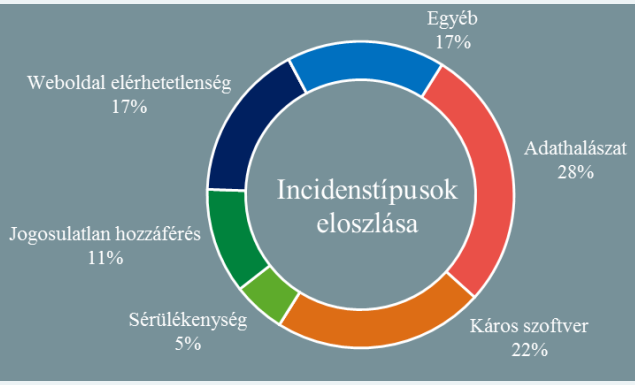
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 11. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.03.12. - 2021.03.18.





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

Oktatási intézményeket célzó zsarolóvírus támadásokra figyelmeztet az FBI

(bleepingcomputer.com)

Az FBI elsősorban felsőoktatási intézményeket, valamint kormányzati szerveket célzó **Pysa ransomware** támadásokra figyelmeztet. A támadások legnagyobbrészt USA-beli és brit szervezetek ellen zajlanak, azonban a tájékoztató szerint külföldi célpontokról is tudni. A Pysa zsarolóvírust terjesztő csoport főképp nyíltan elérhető távoli asztal fiókok (Remote Desktop Protocol – RDP) ─ általában adathalászat útján szerzett ─ jelszavaival jut el a megcélzott szervezet infrastruktúrájába, ahol az elérhető Windows és Linux rendszereket is támadja. **Bővebben...**

Többszörös védelmi megoldás Twitterezőknek

(securityweek.com)

A közösségi platform hétfőn jelentette be, hogy a kétfaktoros azonosítást (2FA) alkalmazó felhasználók számára lehetőséget nyújt arra, hogy akár több biztonsági kulcs használatával extra védelmet biztosítsanak Twitter fiókjaik számára. A webes felület már régóta támogatja a biztonsági kulcsok használatát, azonban az iOS és Android alkalmazásverziók csupán 2020. decemberétől kapták meg a védelmi funkciót. A mostani bejelentés szerint mind a webes felületre, mind pedig a mobilalkalmazásba történő belépéshez több biztonsági kulcs használatára is van lehetőség, ehhez csupán engedélyezni kell a 2FA azonosítási módot.

IT biztonsági Tanács

Az NBSZ NKI weboldalán a Twitter új funkciójával kapcsolatban olvashat hasznos információkat.

Új Mirai variánsra hívja fel a figyelmet a Palo Alto

(securityaffairs.co)

A hírhedt Mirai botnet visszatérésére figyelmeztetnek a Palo Alto kutatói, amely Linuxot futtató IoT és hálózati eszközökre nézve jelent közvetlen fenyegetést. Az új variáns távoli kódfuttatásra lehetőséget adó, már ismert (VisualDoor, CVE-2020-25506, CVE-2021-27561, CVE-2021-27562, CVE-2021-22502, CVE-2019-19356, CVE-2020-26919), illetve zero-day sérülékenységeket is kihasznál. Sikeres hozzáférést követően a támadó rosszindulatú shell szkripteket tölt le az eszközre, amelyek többek között a helyi admin fiókok bruteforce-olásába kezdenek. A támadott eszközök között sérülékeny routerek (D-link, Netgear) is szerepelnek.

Exchange üzemeltetők figyelem: gyors segítség a ProxyLogon probléma kezeléséhez

(bleepingcomputer.com)

A ProxyLogon sebezhetőségeket kihasználó támadások száma meredeken emelkedik, ezért a Microsoft úgy döntött, hogy egy egyszerűen használható megoldással segíti a védekezést. Az **Exchange On-premises Mitigation Tool** (EOMT) névre keresztelt szkript (EOMT.ps1) futtatáskor több dolgot is tesz. Először is ellenőrzi, hogy a telepített Exchange kiszolgáló sérülékeny-e. **Bővebben...**

Adatvédelmi réseket találtak a DuckDuckGo böngészőbővítményben

(ehackingnews.com)

A DuckDuckGo egy széles körben használt böngészőbővítmény, ami a Google Chrome, Microsoft Edge és a Mozilla Firefox böngészők számára érhető el, és legfőbb célja a felhasználók magánszférájának védelme. Az említett bővítményben nemrég olyan biztonsági réseket találtak, amelyek lehetővé tették, hogy egy támadó tetszőleges Javascript programsorokat futtasson távolról (Cross site scripting – XSS) a felhasználó eszközén, illetve a program kommunikációjához nem megfelelő biztonsági szintű kommunikációs láncokat használt, amely így adatszivárgást okozhatott. **Bővebben...**