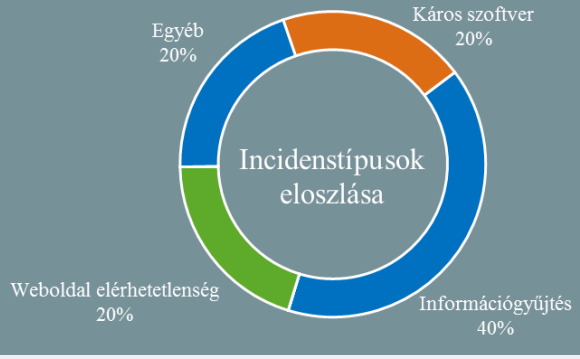
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 33. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.08.13. - 2021.08.18.



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

Nem igazán érnek célt a tudatos jelszóhasználatra nevelő képzések

(bitdefender.com)

Hiába jól ismert tény, hogy a jelszavak újrahasznosítása - azaz amikor több szolgáltatáshoz ugyanazt a jelszót használjuk - egy olyan rossz gyakorlat, ami lényeges biztonsági kockázatot hordoz magában, úgy tűnik a felhasználói megszokások erősebbek. A My1Login nemrég felmérést készített a jelszavak használatával kapcsolatban, ami aggasztó eredménnyel zárult. Mint kiderült, a megkérdezettek kétharmada (62%) ugyanazt a jelszót használja munkahelyi rendszereken, mint otthon, 87%-uk pedig ugyanazt a jelszót használja a különböző céges alkalmazásokhoz. **Bővebben...**

Jogosulatlan hozzáférés a T-Mobile szerint is történt, csak azt nem tudni még, hogy mihez

(arstechnica.com)

Az amerikai T-Mobile 2021. augusztus 16-án közleményt adott ki arról, hogy illetéktelenek hozzáfértek a cég belső infrastruktúrájához. A szolgáltató szerint a támadás során céges adatok kompromittálódtak, azonban ügyfeleik érintettségét nem erősítették meg. Az eset előzménye, hogy egy nappal korábban a Vice magazin egy fórumposztról cikkezett, miszerint egy hacker 100 millió T-Mobile felhasználó érzékeny adatait ─ köztük például az érintettek adóazonosító számát (Social Security Number - SSN), nevét, címét, vezetői engedélyének számát, illetve egyes eszközeik IMEI azonosítóit ─ kínálja eladásra. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat az otthoni Wi-Fi routerek biztonságos használatával kapcsolatban.

Több tucat STARTTLS-hez kapcsolódó sebezhetőséget fedeztek fel, rengeteg e-mail kliens érintett

(thehackernews.com)

Biztonsági kutatók nem kevesebb mint 40 különböző sebezhetőséget azonosítottak egyes levelezőprogramokban és kiszolgálókban alkalmazott STARTTLS implementációk kapcsán, amelyek utat nyithatnak célzott közbeékelődéses (man-in-the-middle - MitM) támadásoknak, lehetővé téve egy behatoló számára a postafiókok tartalmának meghamisítását, és a hitelesítő adatok ellopását. **Bővebben...**

Elsőre nem sikerült patch-elni a kritikus hibát, új javítás érkezett a Pulse Secure VPN-hez!

(thehackernews.com)

A Pulse Secure biztonsági javítást adott ki a Connect Secure VPN termék összesen hat sebezhetőségének befoltozásához. A biztonsági hibák közül az egyik kritikus kockázatú sérülékenységet (CVE-2021-22937) a gyártó hivatalosan már 2020 októberében kijavította, azonban ─ mint arra az NCC Group rámutatott ─ a biztonsági frissítés csupán egyetlen paraméter megváltoztatásával megkerülhető. A kritikus sebezhetőség a már hozzáféréssel rendelkező támadók számára root-szintű távoli kódvégrehajtást tehet lehetővé, továbbá képesek lehetnek megkerülni a webes alkalmazáson érvényesített korlátozásokat, és tartós „hátsó ajtót” biztosítani önmaguknak. **Bővebben...**

Több zsarolóvírus banda is a „PrintNightmare” sérülékenység kihasználására tör

(cyberscoop.com)

A Microsoft több, mint egy hónapja tett közzé információkat az úgynevezett „PrintNightmare” sérülékenységről (CVE-2021-34481). Ez a sebezhetőség azon alapszik, hogy a Windows feladatütemezője nem megfelelően kezeli az együttműködést a számítógépek és a nyomtatók között, lehetőséget adva arra, hogy a támadók rendszer-szintű hozzáféréssel futtassanak kártékony kódokat. **Bővebben...**