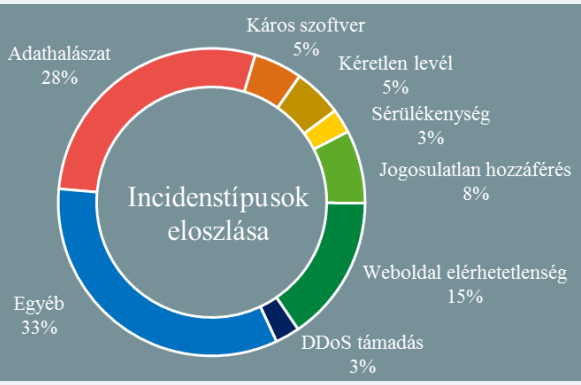
Nemzetközi IT-biztonsági sajtószemle

2021. 18. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.04.30. - 2021.05.06.



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

Még mindig tart a Flubot káros kódot terjesztő támadási kampány

(securityweek.com)

A Proofpoint adatai alapján továbbra is zajlik a FluBot nevű androidos káros kódot terjesztő SMS kampány. Az eredetileg Spanyolországban indult kampány Németország, Magyarország, Olaszország, Lengyelország, majd az Egyesült Királyság után úgy tűnik elérte az Egyesült Államokat. A támadási metódus nem változott, a malware továbbra is egy látszólag valamilyen csomagkézbesítő szolgálattól (FedEx, DHL, Correos) érkező SMS-ek útján terjed, amennyiben az áldozat az üzenetben található hivatkozást megnyitja, és telepíti az azon keresztül elérhető appot. **Bővebben...**

Másfél milliárd Apple eszköz adata van veszélyben egy biztonsági rés miatt

(securityaffairs.co)

Az Apple AirDrop egy kényelmes és praktikus módszer az Apple eszközök közötti vezeték nélküli fájlmegosztásra. Azonban a németországi Darmstadti Műszaki Egyetem kutatói súlyos adatvédelmi hibát fedeztek fel a protokoll működésében. Mint kiderült, egy lehetséges támadónak csupán egy Wi-Fi képes eszközre van szüksége ahhoz, hogy az áldozat eszközének közelében tartózkodva megszerezze a célpont kontakt adatait. A szakértők felfedezték, hogy a hiba az eszközök közötti kapcsolatfelépítési folyamatban található. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat a jelszókezelő szoftverekről.

Kibertámadás ért belga kormányzati webes szolgáltatásokat

(securityaffairs.co)

Masszív túlterheléses támadás ért belga kormányzati IT rendszereket, amely következtében több állami webes szolgáltatás ─ például a kormányzati portál és a rendőrség központi weboldala ─ is elérhetetlenné vált. A támadás az oktatási intézmények, kutatóközpontok, tudományos intézetek és kormányzati szolgáltatások számára internetes kapcsolatot biztosító BELNET hálózatát érte. A szolgáltató tájékoztatása szerint elosztott túlterheléses (DDoS) támadás történt, amelyet sikeresen elhárítottak, így a szolgáltatások ismét elérhetőek. **Bővebben...**

Több százmillió Dell számítógép is veszélyben lehet egy frissen felfedezett sérülékenység miatt

(bleepingcomputer.com)

Konzumer és vállalati Dell gépeket egyaránt érint a **DBUtil** nevű driver sérülékenysége. Az illesztőprogram az elmúlt évtized során szinte minden Dell eszközre telepítésre került, így most potenciálisan több százmillió számítógép esetében okozhat biztonsági problémát. A most nyilvánosságra hozott sebezhetőség, habár biztonsági szakemberek egyetlen CVE azonosítóval (CVE-2021-21551) hivatkoznak rá, valójában 5 biztonsági hibát rejt magában, amelyek legtöbbje jogosultság kiterjesztésre adhat módot illetéktelenek számára. Sikeres kihasználás során kernel szintű jogosultság szerezhető, ami az érintett rendszer teljes kompromittálódását eredményezheti. **Bővebben...**

NSA útmutató IT-OT rendszerek összeköttetéseinek biztosításához

(securityweek.com)

Az informatikai (IT) és a különböző ipari rendszerek (Operation Technology – OT) össszekapcsolása biztonsági okok miatt nem javasolt, azonban bizonyos körülmények között elkerülhetetlenné válhat. Az NSA új segédlete egy ilyen forgatókönyv esetére ad fontos javaslatokat az OT rendszerek védelmének növeléséhez. A szervezetek számára először is mindenképp javasolt az IT-OT összeköttetések tekintetében egy átfogó kockázatelemzés végzése. **Bővebben...**