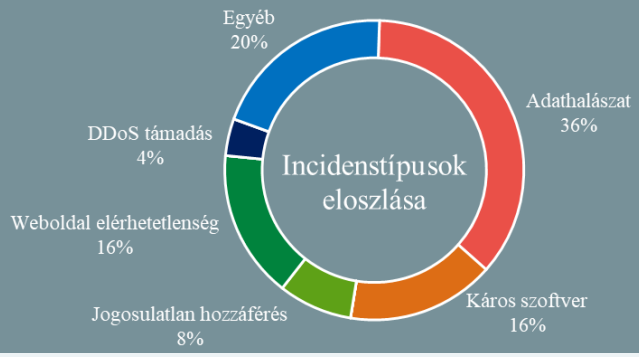
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 36. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.09.03. - 2021.09.09.



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

Fertőzött Office dokumentumokkal veszik át az irányítást Windows rendszerek felett

(thehackernews.com)

A Microsoft figyelmeztetést adott ki a CVE-2021-40444 számú, Internet Explorert érintő kritikus zero-day sérülékenység miatt, amelyet a támadók aktívan ki is használnak. A támadás során a felhasználókat egy fertőzött dokumentum megnyitására próbálják rávenni, amelyhez rosszindulatú ActiveX vezérlőt készíthetnek MSHTML-ben (más néven Trident), ami által kihasználható a távoli kódvégrehajtási hiba, és átvehető a Windows rendszer feletti irányítás. Az MSHTML az Internet Explorer egykori saját böngészőmotorja, amelyet a webes tartalmak megjelenítésére használtak az Office dokumentumokban. **Bővebben...**

Súlyos pénzbírsággal zárult a WhatsApp átláthatósági vizsgálata

(securityaffairs.co)

Az Ír Adatvédelmi Bizottság (DPC) 225 millió eurós bírságot szabott ki a WhatsAppra, az európai uniós általános adatvédelmi rendelet (GDPR) átláthatósági kötelezettségeinek megsértése miatt, arra vonatkozóan, hogy a cég miként osztja meg az európai felhasználók adatait a Facebookal. Az ezzel kapcsoaltos kivizsgálást a DPC még 2018. december 10-én kezdte meg, ami magában foglalta a WhatsApp és más Facebook vállalatok közötti információmegosztást is. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán szeretnénk figyelmükbe ajánlani a **Security Summits** szakmai videókonferencia-sorozatot.

Németország tiltakozik az orosz Ghostwriter kibertámadások ellen

(securityweek.com)

A német külügyminisztérium szóvivőjének nyilatkozata szerint egy ideje Németországot célzó tevékenységekre lettek figyelmesek, amelyek a Ghostwriter nevet viselő APT egységhez köthetők. A német kormány értesülései szerint a szervezet az orosz GRU katonai hírszerző szolgálat kötelékébe tartozik. A támadások sajátossága, hogy „a hagyományos kibertámadásokat dezinformációs és befolyásolási műveletekkel ötvözik” – közölte Andrea Sasse, a német külügyminisztérium szóvivője. **Bővebben...**

Súlyos biztonsági hibákat javít a Netgear

(bleepingcomputer.com)

Új firmware-frissítéseket adott ki a Netgear a vállalati környezetben használt több mint egy tucat okos switch eszközéhez, hogy javítsa a nemrég felfedezett súlyos biztonsági réseket. A sérülékenységek kockázati besorolása magas (10-es skálán 7,4 és 8,8 között helyezkedik el). Az legújabb frissítésben három biztonsági hiba került javításra, amelyek 20 Netgear terméket érintettek, főként intelligens switch-eket. A vállalat tanácsadójának pénteki tájékoztatója szerint az érintett termékekhez új firmware verzió áll majd rendelkezésre, melynek telepítése erősen javallott. **Bővebben...**

BrakTooth: Az új Bluetooth sebezhetőségek akár több millió eszközt is érinthetnek

(securityweek.com)

A Szingapúri Műszaki és Tervezési Egyetem kutatócsoportja egy új, **16 sebezhetőségből** álló családot hozott nyilvánosságra, amelyek a kereskedelmi forgalomban kapható eszközökön alkalmazott **Bluetooth Classic (BT) stackeket** érintik. A kutatók 11 gyártó 13 Bluetooth-eszközének kiértékelése után azonosították a biztonsági réseket, amelyekhez már 20 CVE azonosítót hozzárendeltek, további négy sebezhetőség hozzárendelésére pedig folyamatban van. **Bővebben...**