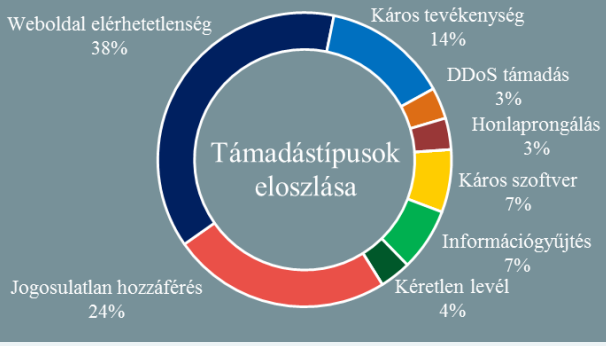
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 42. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.10.09. - 2020.10.15.



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

APT csoportok által kihasznált sérülékenységekre figyeltetnek amerikai ügynökségek

(us-cert.cisa.gov)

Az amerikai Cybersecurity and Infrastructure Security Agency (CISA) és az FBI közös közleményben figyelmeztet egyes APT (Advanced Persistent Threat) csoportok új támadási taktikájára. A támadások középpontjában a nemrég napvilágra került Netlogon sérülékenység (CVE-2020-1472, Zerologon) áll, amelyet további, jellemzően régóta ismert biztonsági hibák kihasználásával együttesen alkalmaznak. **Bővebben...**

Androidos ransomware-re figyelmeztet a Microsoft

(zdnet.com)

Az AndroidOS/MalLocker.B nevű ransomware online fórumokon és 3rd party weboldalakon terjed, magát különböző legitimnek tűnő alkalmazásnak álcázva. Miután a káros kód lefut, a zsarolóvírus zárolja a készülék képernyőjét és egy – a mobil platformokat támadó ransomware-eknél tipikusnak számító – ál rendőrségi bírságot jelenít meg, amelytől az áldozat sehogy sem tud szabadulni. Újszerűséget annyiból jelent, hogy az operációs rendszer mely funkcióit támadja. **Bővebben...**

IT biztonsági Tanács

Az Európai Kiberbiztonsági Hónap (ECSM) kampány keretében készített rövid biztonsági szemléletformáló animációk megtekinthetők az NBSZ NKI weboldalán.

Oroszországot gyanúsítják a norvég parlament elleni támadássa

(bleepingcomputer.com)

A norvég külügyminiszter, Ine Eriksen Søreide közleménye szerint Oroszország áll a norvég parlament (Strotinget) elleni augusztusi kibertámadás hátterében. A szeptember elsejei hivatalos közlemény nem osztott meg részletes információkat a támadásról. Mindössze annyi vált ismertté, hogy a támadók hozzáfértek egyes parlamenti képviselők e-mail fiókjaihoz, amelyekből érzékeny információkat szereztek. Az október 13-ai közlemény szerint a kivizsgálás azóta is nagy erőkkel zajlik az ország kiberbiztonsági szervezeteinek együttműködésével. **Bővebben...**

Jelentős kibertámadást szenvedett el egy londoni kerületi önkormányzat

(zdnet.com)

Kibertámadás érte az észak-londoni Hackney önkormányzatát, amelynek következtében több szolgáltatás és IT-rendszer is elérhetetlenné vált. Az önkormányzat közleménye szerint a brit kibervédelmi központtal (National Cyber Security Centre – NCSC) és külsős szakértőkkel szoros együttműködésben dolgoznak a probléma elhárításán. Az incidens kivizsgálásának ilyen korai pontján a kerületi polgármester közleménye szerint még nem áll rendelkezésre elég információ, azonban az eset feltárása folyamán rendszeres tájékoztatást ígért. **Bővebben...**

Fontos biztonsági fejlesztést jelentett be a Zoom

(bleepingcomputer.com)

A Zoom közleménye szerint jövő héttől minden felhasználójuk számára elérhető lesz a végponttól végpontig tartó titkosítás (end-to-end encryption – E2EE), beleértve az ingyenes verziót használókat is, amennyiben hitelesítik fiókjukat, ami telefonszám megadásával is történhet. A kommunikáció eddig is titkosított módon zajlott a Zoomon, E2EE esetén a különbség az, hogy a session-ök titkosítására szolgáló kulcsok nem központilag a Zoom szervereken generálódnak majd, hanem lokálisan, a meetingeken résztvevők rendszerein. **Bővebben...**