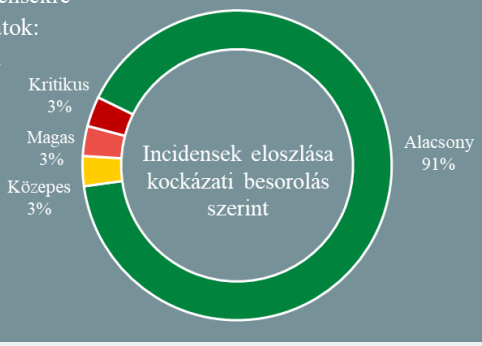
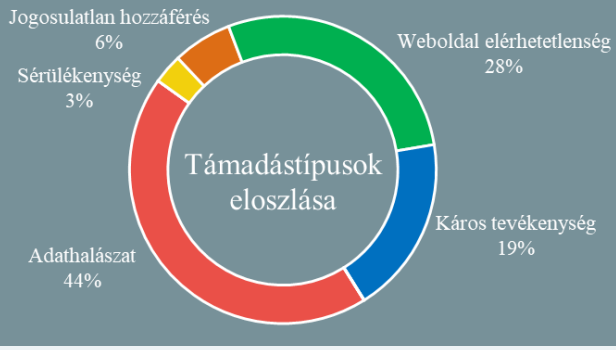
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 25. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.06.12. - 2020.06.18.





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

Hatályba lépett a korai figyelmeztető rendszerről szóló kormányrendelet

(njt.hu)

2020. május végén lépett hatályba az elektronikus információbiztonsági korai figyelmeztető rendszerről (EWS) szóló 214/2020 kormányrendelet. A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet által üzemeltetett EWS egy központosított felügyelettel is rendelkező, illetéktelen hálózati behatolást jelző rendszer (IDS), mely szignatúrák alapján generál olyan jelzéseket, figyelmeztetéseket, amik behatolást, egyéb eseményt, biztonsági vagy adatvédelmi incidenst jelezhetnek a védett hálózatokban. A rendszer ezen kívül képes még a nyers hálózati forgalom incidenskivizsgálási célú mentésére, valamint hálózatforgalmi statisztikai adatok rögzítésére is. **Bővebben...**

Veszélyes új technikát alkalmaz egy új zsarolóvírus

(bleepingcomputer.com)

2019 novemberében került napvilágra a RIPlace névre keresztelt technika, amellyel az ismert antiransomware megoldások ─ többek közt a Windows 10 beépített Controlled Folder Access szolgáltatása is ─ megkerülhetőek. A módszert a végponti védelemmel foglalkozó Nyotron fedezte fel még 2018-ban, amiről akkor tájékoztatta is a nagyobb biztonsági cégeket, akik közül azonban csupán a Kaspersky és a Carbon Black végzett módosításokat. Az eddig csupán elméleti szinten kezelt módszer immáron úgy tűnik formát is öltött, ugyanis a Recorded Future által azonosított Thanos ransomware már be is építette a támadó arzenáljába. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat a Common Sense által biztosított gyerekvédelmi szolgáltatásról.

Konfigurációs hiba miatt elérhető nyomtatók a neten

(shadowserver.org)

A The Shadowserver nonprofit alapítvány alaptevékenysége során napi szintű hálózatfelderítést végez az Interneten keresztül elérhető, támadásoknak potenciálisan kitett eszközök azonosításáért, amelyekről értesíti az érintett hálózatok tulajdonosait, valamint az országkód alapján illetékes nemzeti CSIRT-eket. Az alapítvány 2019 júliusa óta részt vesz az EU-s támogatású VARIoT (Vulnerability and Attack Repository for IoT) projektben, amelynek célja hozzájárulni az IoT (Internet of Things) eszközök biztonságához. Ennek részeként a Shadowserver a nyomtatók távoli elérésére használható IPP (Internet Printing Protocol) szolgáltatást is vizsgálja a monitorozás során, amivel körülbelül 80 000 nyíltan elérhető nyomtatót azonosít naponta.

Melyek a kiberbiztonsági szempontból leginkább veszélyeztetett országok?

(securitymagazine.com)

2020 június 2-án jelent meg az idei Cybersecurity Index (CEI), amely a kiberbűnözéssel szembeni kitettség alapján rangsorolja a nemzetállamokat. Összesen 108 ország került értékelésre végponti és felhő tárhelyek elleni kibertámadások szempontjából, ezek közül jelenleg Afganisztán számít a leginkább veszélyeztetettnek, ezt követi Mianmar, Etiópia, Palesztina és Venezuela. A skála másik végén Finnország található, mint a támadásoknak legkevésbé kitett ország, ezt követi Dánia, Luxemburg, Ausztrália, valamint Észtország. Régiós szinten a legalacsonyabb országonkénti átlagpontszámmal Afrika, a legmagasabbal pedig Európa rendelkezik.

Jelentős hálózati kiesés történt az amerikai T-Mobile-nál

(securityaffairs.co)

A T-Mobile több millió ügyfele tapasztalt problémát hétfőn a hangalapú és szöveges kommunikációban, amelyért egyes hírek szerint egy nagy volumenű elosztott szolgáltatás megtagadást (DDoS) okozó támadás lehetett a felelős. A szolgáltatói közlemény nem említ támadást, csupán azt, hogy egy IP forgalmat érintő hiba történt, azonban az Arbor Networks Digital Attack Mapje DDoS támadást jelzett. **Bővebben...**