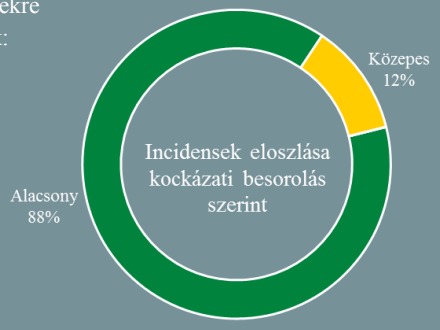
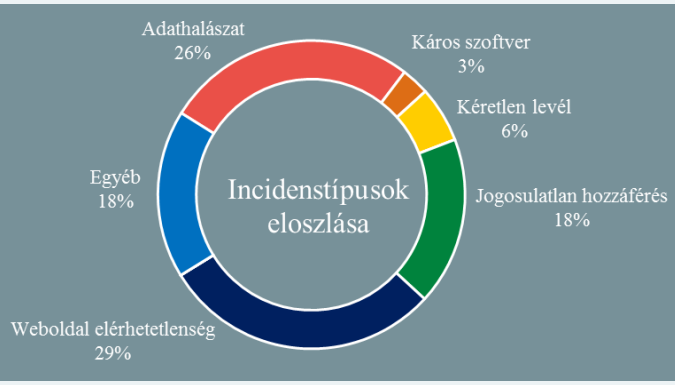
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 09. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.02.26. - 2021.03.04.





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

Többek közt ezért egyre nehezebb egy-egy kibertámadást konkrét nemzetállamhoz kötni

(zdnet.com)

Nyugtalanító trendre világít rá a BlackBerry friss elemzése. Eszerint egyes kiberbűnözői kollektívák ma már olyan potenciállal bírnak, hogy nem ritkán államok is igénybe veszik szolgáltatásaikat. A „cybercrime-as-a-service" (CaaS) üzleti modell lényege, hogy a kiberbűnözők a megrendelő által kiválasztott célpont ellen saját eszközeikkel támadást indítanak, majd a megszerzett információkat átadják a kliensnek. Az ily módon nyert anonimitás érthető módon vonzó a kormányzatok számára, hiszen egy támadás lelepleződése esetén nincsenek állami érintettségére utaló nyomok. **Bővebben...**

Új jailbreak készült IPhone-ra

(techcrunch.com)

Az „Unc0ver" álnevet használó, kifejezetten iPhone-ok feltörésére szakosodott csoport új „jailbreak-eszközt" tett közzé, amely 11-estől 14.3-ig bezárólag minden iOS verzión működik ─ a legújabb modelleken is. Elmondásuk szerint a friss tool a CVE-2021-1782 azonosítóval hivatkozott sebezhetőséget használja ki ahhoz, hogy teljes kontrollt lehessen nyerni az egyébként meglehetősen zárt OS felett. Egyes felhasználók ezt például arra használják, hogy a hivatalos alkalmazásbolton kívülről telepítsenek appokat. Megjegyzendő ugyanakkor, hogy az Apple eszközök jailbreakelése amellett, hogy azt eszközt sérülékenyebbé teszi hackertámadásokkal szemben, garanciavesztést is okoz. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán egy, a Facebookon terjedő kártevőről olvashat hasznos információkat.

Exchange adminok figyelem: sürgős biztonsági frissítéseket adott ki a Microsoft

(bleepingcomputer.com)

Soron kívüli biztonsági hibajavítást adott ki a Microsoft az Exchange valamennyi helyi telepítésű verziójához. A hibajavítás négy, támadók által aktívan kihasznált zero day sebezhetőséget foltoz be. A hibák kihasználásához a támadónak először a 443-as porton keresztül kell hozzáfernie a megcélzott Exchange szerverhez. Amennyiben ez sikeres volt, a négy hiba együttes kihasználásával a támadó teljes kontrollt nyerhet az érintett a szerver felett, azaz a teljes e-mail forgalomhoz hozzáférhet, vagy tetszőleges kód telepítésével a hálózaton tovább is terjeszkedhet. **Bővebben...**

Gootloader: Google keresési találatok közé csempészett oldalakkal terjesztenek kártevőket a bűnözők

(bleepingcomputer.com)

A Sophos szakemberei a „Gootloader" nevű, kártevő-terjesztésre készített keretrendszerrel elkövetetett támadások veszélyeire hívják fel a figyelmet. A Gootloader feltört WordPress webhelyek és rosszindulatú keresőoptimalizálási (Blackhat SEO) technikák segítségével többféle káros kódot ─ németországi esetek alapján akár REvil zsarolóvírust is ─ igyekszik az áldozat rendszerébe juttatni. **Bővebben...**

NSA útmutató a „zéró bizalom" biztonsági koncepció alkalmazásához

(securityweek.com)

A „Zéró bizalom elv" (Zero Trust) azt a biztonsági szemléletmódot jelenti, hogy feltételezzünk, hogy rendszereink kompromittálódása elkerülhetetlen ─ mi több, valószínűleg már meg is történt ─ ennélfogva egyetlen rendszerelem vagy hozzáférési kísérlet sem tekinthető megbízhatónak. Az NSA friss útmutatója (Embracing a Zero Trust Security Model) a Zero Trust koncepció gyakorlati alkalmazásához kíván segítséget nyújtani a szervezetek számára. Eszerint az adatok, rendszerelemek, alkalmazások és szolgáltatások (Data/Assets/Applications/Services - DAAS) hozzáférés-védelmét kell fókuszba helyeznünk, annak szigorú ellenőrzésével ─ és rendszeres újraellenőrzésével ─, illetve a hálózati fenyegetések utáni folyamatos monitorozással. **Bővebben...**