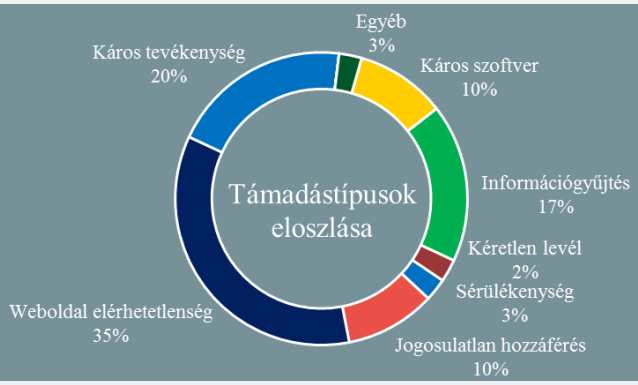
Nemzetközi IT-biztonsági sajtószemle

2020. 50. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.12.04. - 2020.12.10.



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

Az APT28 állhatott a norvég parlament idei megtámadása mögött

(zdnet.com)

A Norvég Rendőri Biztonsági Szolgálat (Norwegian Police Security Service – PST) jelentése szerint az országgyűlési képviselők e-mail fiókjai ellen indított 2020 augusztusi kibertámadás mögött az orosz APT28 (más néven Fancy Bear, Sofacy vagy Strontium) csoport állt. Októberben Ine Eriksen Søreide norvég külügyminiszter már közölte, hogy Oroszországot gyanúsítják a támadással. A PST friss közleménye szerint a fióktörési-kísérletek egy nagyobb, még 2019-ben indított APT28 kibertámadási kampány részét képezték, ezzel vélhetően a Microsoft szeptemberi elemzésére utalva. **Bővebben...**

A fejlesztői frissítés hiánya miatt több népszerű androidos alkalmazás veszélynek van kitéve

(bleepingcomputer.com)

Az Oversecured mobilalkalmazás biztonsági cég még augusztusában fedezett fel egy olyan sebezhetőséget a Google Play Core könyvtárban, amelynek kihasználásával a rosszindulatú alkalmazások kódokat futtathattak más megbízható appokban, ezáltal megfigyelhetővé és ellophatóvá váltak az alkalmazásokba bevitt adatok. (A programkönyvtár rendeltetése alapvetően az, hogy azon keresztül az alkalmazások különböző komponensei futás közben frissíthetőek. Rengeteg népszerű, sokmilliós letöltéssel bíró alkalmazás használja, mint például a Chrome, az Edge, a Facebook, az Instagram, vagy épp a WhatsApp, csak a legnagyobb neveket említve.) **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat arról, miként csökkenthetjük digitális lábnyomunkat.

Ezt jósolja a Kaspersky 2021-re az ipari kiberbiztonság terén

(kaspersky.com)

A Kaspersky ICS CERT közzétette az ipari vezérlőrendszerek (Industrial Control Systems – ICS) kiberbiztonságával kapcsolatos 2021-es előrejelzéseit. A teljesség igénye nélkül: feltételezhető, hogy az elmúlt évek hitelesítő adatok gyűjtésére koncentráló támadási kampányainak eredményeként célzottabb támadások zajlanak majd kritikus rendszerekkel szemben. Ipari hálózatokon népszerű operációs rendszerek (Windows 7 és Windows Server 2008) támogatási ciklusának végeztével, valamint a Windos XP forráskódjának kiszivárgásával rendkívül valószínűnek tűnik egy WannaCry-hoz hasonló esemény. **Bővebben...**

Az NSA figyelmeztet: orosz hackerek VMware sebezhetőségek kihasználására törnek

(bleepingcomputer.com)

Az NSA információi szerint orosz állami támogatású hackerek egyes VMware vállalati távmunka platformokat (Workspace One Access, Access Connector, Identity Manager, Identity Manager Connector) érintő sérülékenységet (CVE-2020-4006) kihasználva támadókampányba kezdtek. A sebezhetőség kihasználásával az érintett eszközökön káros programokat, például web shelleket telepíthetnek és védett információkhoz férhetnek hozzá. Szerencsére gyártói hibajavítás már elérhető, amelyet javasolt mielőbb telepíteni. **Bővebben...**

APT csoport hackelhette meg a FireEye-t

(securityweek.com)

Az IT-biztonsági ipar egy prominens szereplőjét, az amerikai FireEye-t kibertámadás érte, amelyért szerintük egy állami támogatású APT csoport lehet felelős. Kevin Mandia, a cég vezérigazgatója közleményében arról számolt be, hogy nem találtak arra utaló nyomot, hogy a támadók sikeresen hozzáfértek volna érzékeny ügyféladatokhoz. Mindazonáltal a támadók megszereztek olyan ún. "Red Team" típusú hacking eszközöket, amelyekkel a FireEye ─ többek között kormányzati ─ ügyfelei védelmét teszteli. **Bővebben...**