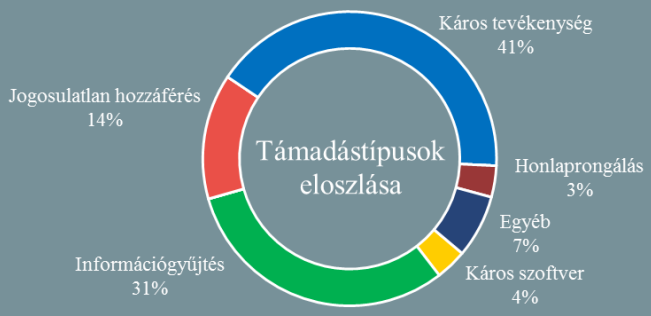
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 38. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.09.11. - 2020.09.17.



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

Útmutató szervezetek számára a sérülékenység jelzések kezeléséhez

(securityaffairs.co)

Az alkalmazott informatikai rendszereket érintő sérülékenységekre vonatkozó információk minden szervezet számára kritikus jelentőséggel bírnak. A brit kibervédelmi intézet (NCSC – British National Cyber Security Centre) friss útmutatójában arra hívja fel a figyelmet, hogy az etikus hackerektől elvárt felelős információ-megosztás támogatása a szervezetek felelőssége is, mégpedig egy jól definiált sérülékenység-közzétételi eljárásrend készítésével és alkalmazásával. **Bővebben...**

Már a Zoomon is elérhető a kétfaktoros hitelesítés!

(securityweek.com)

Fontos biztonsági fejlesztés történt a népszerű videotelekonferencia szolgáltatásnál: immáron elérhető a kétfaktoros azonosítás. A Zoom minden felhasználó számára javasolja a biztonsági funkció engedélyezését, ugyanis a felhasználók védettebbek lesznek a felhasználói fiókok feltörését célzó támadásokkal, valamint az esetleges adatszivárgásokkal szemben. A platform az SMS, illetve telefonhíváson keresztül történő azonosítás mellett lehetőséget biztosít autentikátor alkalmazások használatára is, mint például a Google Authenticator, a Microsoft Authenticator, vagy a FreeOTP. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat a TikTok adatvédelmi és biztonsági beállításairól.

Több ezer Magento online webshopot hackeltek meg néhány nap alatt

(securityaffairs.co)

A Sansec kiberbiztonsági cég szerint közel 2 000 Magento webshopot érintett az eddigi legnagyobb Magecart-stílusú támadási kampány, ami a múlt hétvégén zajlott. A támadók egy speciális típusú káros kódot (skimmer) fecskendeztek a megcélzott weboldalba, abból a célból, hogy a weboldalt meglátogató felhasználók által megadott banki adatokat megszerezzék. Feltételezések szerint a támadások során több tízezer felhasználó érzékeny adatait szerezhették meg így. **Bővebben...**

Gamerek figyelem: adatszivárgás történt a Razernél

(bleepingcomputer.com)

Bob Diachenko biztonsági kutató egy ügyféladatokat tartalmazó, online elérhető adatbázisra hívta fel a gamer eszközöket gyártó cég figyelmét. Az adatbázis megközelítőleg százezer olyan Razer ügyfél adatait ─ többek között a vásárlók nevét, e-mail címét, telefonszámát, rendelési azonosítóját, valamint számlázási és szállítási információkat ─ tartalmazta, akik a cég online webshopján keresztül rendeltek termékeket. A biztonsági kutató augusztus 19-én fedezte fel az adatbázist, elsőként a céggel közvetlenül igyekezett felvenni a kapcsolatot, hogy az adatbázis elérhetősége ne kerüljön nyilvánosságra. **Bővebben...**

Sérülékeny Netlogon kapcsolatokat célzó támadásokra figyelmeztet a CISA

(us-cert.cisa.gov)

Az Amerikai Egyesült Államok belbiztonsága alatt működő kiberbiztonsági ügynökség (Cybersecurity and Infrastructure Security Agency – CISA) felhívja a figyelmet a Netlogon távoli protokoll sérülékenységét kihasználó támadásokra. (A Netlogon (más néven MS-NRPC) egy olyan RPC-kezelőfelület, amelyet tartományhoz csatlakoztatott eszközök használnak.) A szóban forgó sérülékenység (CVE-2020-1472) kihasználásával a támadó hozzáférést nyerhet a támadott tartományvezérlőhöz. **Bővebben...**