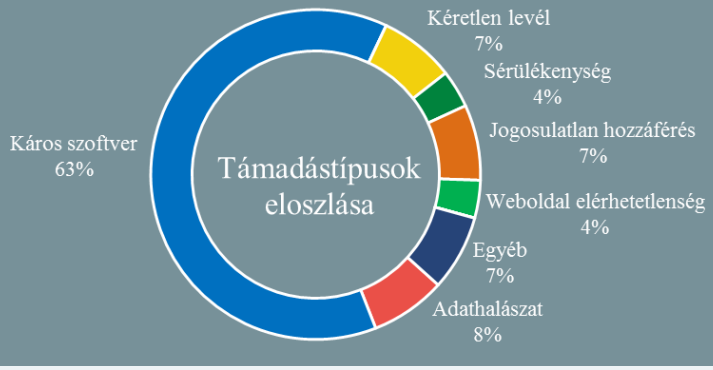
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 45. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.11.01. - 2019.11.07.



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

Megkezdődött: Első alkalommal detektáltak BlueKeep sérülékenységet kihasználó támadásokat

(zdnet.com)

A Microsoft már májusban figyelmeztetett egy kritikus Windows sérülékenység (CVE-2019-0708) lehetséges kihasználására, ami miatt javasolták a biztonsági rést megszüntető frissítés azonnali telepítését. Most úgy tűnik a félelmük beigazolódott: biztonsági kutatók olyan támadásokat észleltek, amelyek a „BlueKeep”-ként hivatkozott biztonsági rés kihasználására törnek. A Microsoft aggodalma nem alaptalan, egyrészt a hiba lehetővé teheti egy önmagától terjedő féreg program alkalmazását, másrészt továbbra is rengeteg (körülbelül 750 000) sérülékeny végpont érhető el az interneten keresztül világszerte. A most észlelt, körülbelül két hete zajló kampány szerencsére „csupán” kriptobányász programmal fertőzi a megcélzott rendszereket. A támadók mindehhez a Metasploit sérülékenységvizsgálati keretrendszer fejlesztői által szeptemberben közreadott demo exploitot használták fel változatlan formában ─ vélhetően megfelelő szakmai tudás hiányában. **Bővebben...**

Átfogó kibertámadás érte Grúziát

(ehackingnews.com)

Október 28-án egy kibertámadás következtében több száz grúz weboldal vált elérhetetlenné ─ köztük a grúz elnök, Salome Zurabishvili hivatalos site-ja is ─ valamint több tévéadó is beszüntette az adást. A grúz belügyminisztérium közleménye szerint a támadás kivizsgálás alatt áll, jelen állás szerint pedig mind belföldi, mind külföldi eredetű is lehetett. eközben a francia La Monde napilap egy lehetséges orosz összefüggésről ír a kibertámadás kapcsán. A lap szerint a grúz hatóságok igyekeznek jó viszonyt ápolni Oroszországgal a kereskedelmi kapcsolatok fenntartásának reményében. **Bővebben...**

QNAP NAS-ok veszélyben

(securityaffairs.co)

Szakértők egy új malware-re (QSnatch) figyelmeztetnek, amely QNAP NAS-okat (hálózati adattároló – Network Attached Storage) vesz célba. A német Szövetségi Információbiztonsági Hivatal (BSI) incidenskezelő szerve, a CERT-Bund szerint a káros kód csak Németországban eddig már több, mint 7 000 eszközt fertőzött meg. Néhány héttel ezelőtt a finn nemzeti kiberbiztonsági szerv (NCSC-FI) már kiadott egy elemzést a malware-ről. **Bővebben...**

Ransomware támadás érte Kanada legészakibb tartományát

(tripwire.com)

Zsarolóvírus támadás érte Kanada Nunavut tartományának állami IT rendszereit. Joe Savikataaq, a tartomány miniszterelnöke november másodikán jelentette be az incidenst egy tweeten keresztül, egy nappal később pedig a helyi kormányzat Facebook oldalán jelent meg poszt, miszerint zsarolóvírus áll a háttérben. Mint kiderült, a káros kód több szerveren és munkaállomáson is titkosította az elérhető fájlokat, amelynek következtében a legtöbb kormányzati elektronikus szolgáltatás érintetté vált. A közleményből nem derül ki, hogy milyen típusú kód pusztított, azonban a CBC szerint a zsaroló üzenet és az alkalmazott fájlok az „Unlock11@protonmail.com” ransomware családra utalnak. A biztonsági esemény kivizsgálása és a kármentesítés jelenleg is folyamatban van, a kormányzat szerint a fájlok többségét képesek lesznek helyreállítani, azonban arra vonatkozóan nem közöltek becsléseket, hogy ez mikorra várható.

Partneri együttműködés a Google Play vírusmentesítése érdekében

(bleepingcomputer.com)

A Google bejelentette, hogy az ESET, a Lookout és a Zimperium biztonsági cégek segítségével kívánja javítani a rosszindulatú Android alkalmazások észlelésének képességét, még mielőtt azok megjelennének a Play Store-ban, mint letölthető alkalmazások. Az új, App Defense Alliance névre hallgató együttműködés ezt azáltal szeretné elérni, hogy a nevezett cégek víruskereső motorjai integrálásra kerülnének a Google Play Protect (GPP) rendszerbe. Dave Kleidermacher, az Android információbiztonságért felelős alelnökének elmondása szerint az így előálló fenyegetési többletinformáció jelentős javulást fog hozni a káros alkalmazások felismerési képességében. Az App Defense Alliance ugyanakkor kétirányú kommunikációt biztosít a résztvevők között, így a fenyegetésekkel kapcsolatos információkat és a legújabb vírus mintákat a rendelkezésre állást követően a felek képesek lesznek megosztani egymás között.

IT biztonsági Tanács

Egyes új DNS protokollok (DoH, DoT) magasabb szintű biztonság és adatvédelem ígéretével kecsegtetnek, azonban ahhoz, hogy ezek bevezetéséről megfelelő döntést hozhassunk, átfogó képet kell kapnunk a potenciális előnyökről és hátrányokról. Jó ha tisztában vagyunk vele, hogy ezek az olyan ─ biztonsági szempontból lényeges ─ tevékenységekre is hatással vannak, mint például a DNS monitoring.

Az ezzel kapcsolatos kihívások kezelésére az NBSZ NKI weboldalán elérhető egy ajánlás, amelyet az Egyesült Királyság kiberbiztonsági központja, az NCSC adott közre.

Zsarolóvírus támadások Spanyolországban

(bleepingcomputer.com)

Ransomware támadás érte Spanyolország legnagyobb menedzselt szolgáltatásokat nyújtó (MSP) cégét, az Everis vállalatot, valamint az ország első számú rádióadóját, a Cadena SER-t. Habár a támadást hivatalosan nem ismerte el a cég, egy, a BleepingComputer birtokába jutott zsaroló üzenet szerint a BitPaymer zsarolóvírus okozta a fertőzést, azonban a Cadena SER esetében ez még nem került megerősítésre. Az utóbbi időszakban elterjedt taktika, hogy a támadók egy MSP kompromittálásán keresztül juttatnak káros kódot a kliens szervezetek rendszereire, Arnau Estebanell Castellví kiberbiztonsági konzultáns szerint jelen helyzetben is erről lehet szó. Egy a BleepingComputernek nyilatkozó forrás szerint a BlueKeep sérülékenységet is felhasználhatták a támadás során, mindazonáltal jelenleg nem érhető el olyan bizonyíték, ami alapján ezt megalapozottnak lehet tekinteni. Megjegyzendő azonban az is, hogy néhány nappal korábban napvilágra került egy BlueKeepre irányuló támadási kampány.

Pusztító BlueKeep támadásokra figyelmeztet a Microsoft

(zdnet.com)

A Microsoft biztonsági csapata arra figyelmezteti a felhasználókat, hogy a nemrég felfedezett, BlueKeep sérülékenységet kihasználó kriptobányász támadási kampány után újabb, pusztítóbb hatású támadások várhatóak. A nevezett kampányt több biztonsági kutató sem tartotta figyelemre méltónak, azonban a Microsoft szerint ez csupán a kezdet, ezért újfent ─ idén harmadik alkalommal ─ kéri a felhasználókat és szervezeteket, hogy telepítsék a május 14-én kiadott biztonsági frissítéseket.

Új NIST keretrendszer az adatvédelmi kockázatok csökkentésére

(tripwire.com)

Az utóbbi években mind kulturális, mind jogi szempontból változás figyelhető meg az online adatvédelem terén, köszönhető ez részben az olyan súlyos adatvédelmi incidenseknek, mint az Equifax adatszivárgás, vagy a Cambridge Analytica botrány. Szabályozási szempontból mérföldkőnek számít a 2018 májusában hatályba lépett európai általános adatvédelmi rendelet (GDPR), a tengerentúlon pedig a hasonló célokat szolgáló, hamarosan élesedő California Consumer Privacy Act (CCPA). Az amerikai szabványügyi hivatal (NIST) pedig most egy adatvédelmi keretrendszer előzetes tervezetének közelmúltbeli közreadásával igyekszik a szervezetek kockázatkezelési gyakorlatának kibővítésével támpontot adni azon optimális adatkezelési gyakorlatokhoz, amelyek a legkisebb káros következménnyel járnak a személyes adatokra nézve. **Bővebben...**

A berlini fellebbviteli bíróság 2020-ig nagyrészt csak offline állapotban dolgozhat

(heise.de)

Egy hónappal ezelőtt a berlini fellebbviteli bíróság egy erőteljes trójai Emotet támadás után kénytelen volt lekapcsolni teljes számítógépes rendszerét az Internetről. Bernd Pickel, a ház elnöke úgy gondolja, hogy az intézmény 2020-ig nem térhet vissza a normál online állapothoz, ezért a bíróság alkalmazottai számítógépjüket addig gyakorlatilag csak írógépként használhatják. Pickel a Tagesspiegel-nek adott interjújában azonban hangsúlyozta, hogy az igazságszolgáltatás általában az internetes hálózat nélkül működik, valamint jelezte azt is, hogy az incidens során adatvesztés nem történt. **Bővebben...**