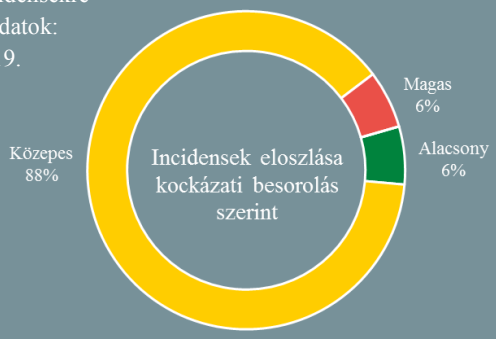
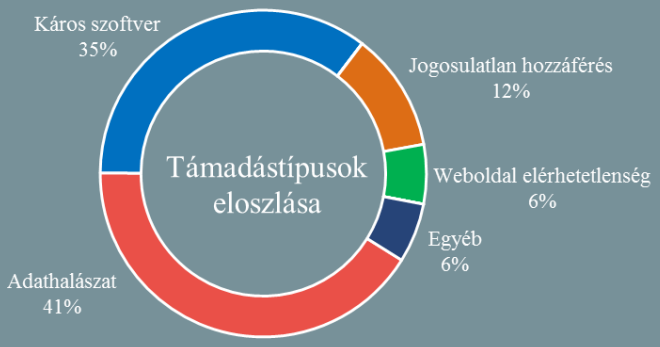
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 38. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.09.13. - 2019.09.19.





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

Ecuador lakosságának nagy része érintett az ország eddigi legsúlyosabb adatszivárgási incidensében

(zdnet.com)

A vpnMentor két kutatója fedezte fel azt az online, bárki számára elérhető Elasticsearch adatbázist, amely Ecuador lakosságának nagy részének szenzitív adatait tartalmazta, köztük az ország elnökével, vagy épp a közelmúltig politikai menedékjogot élvező Julian Assange-zsal. A személyazonosításra alkalmas információkon ─ az érintettek neve, születési dátuma, születési helye, személyi száma, otthoni címük ─ kívül munkahelyükre, gépkocsijukra, iskolai végzettségükre vonatkozó adatok, valamint telefonszámuk is megtalálható volt. Az adatok kormányzati, valamint részben civil rendszerekből származtak, mint például a BIESS bank, vagy az ecuadori autószövetség AEADE. Az ecuadori nemzeti CERT közreműködésével azóta elérhetetlenné tett adatbázisért az eddigi vizsgálatok szerint a Novaestrat nevű helyi vállalat lehet a felelős, akik honlapjuk szerint analitikai szolgáltatásokat nyújtanak a pénzügyi szektornak.

Az ISIS elleni amerikai kiberműveletek nem álltak le

(cyberscoop.com)

Az amerikai kiberparancsnokság által létrehozott ARES összhaderőnemi (alkalmi) harckötelék (Joint Task Force) továbbra is aktív, jelenleg a terrorszervezet afganisztáni tevékenységéről gyűjt információt. A kötelék 2016-ban jött létre, azzal a feladattal, hogy az ISIS informatikai és kommunikációs rendszerei ellen végezzen digitális hadviselést, ennek eleget téve 2017 során több ízben sikeresen támogatták a hagyományos haderő műveleteit. Habár az Iszlám Állam kalifátusa Irakban és Szíriában fizikailag megsemmisült, a szervezet így is aktív milíciákkal rendelkezik a régióban. **Bővebben...**

Utasadatok szivárogtak ki a Lion Air egyes leányvállalataitól

(bleepingcomputer.com)

Több tízmillió utasadat szivárgott ki a Lion Air tulajdonában lévő légitársaságoktól. Az érzékeny információk két, egyenként 21 és 14 millió adatot tartalmazó nyilvántartás formájában voltak szabadon hozzáférhetőek egy Amazon AWS tárhelyen. A kiszivárgott adatok között az utasok személyazonosításra alkalmas szenzitív adatai (többek között utas-és foglalási adatok, személyes elérhetőségek, útlevél adatok) is megtalálhatóak, amelyek többnyire a Malindo Air, valamint a Thai Lion Air 2019 májusi biztonsági mentéseiből származnak. **Bővebben...**

Kína állhatott az ausztrál parlament elleni támadás mögött

(securityweek.com)

A Reuters információi szerint az ausztrál kiberhírszerzési ügynökség (Australian Signals Directorate – ASD) egyértelműen Kínát tartja felelősnek az ausztrál parlament, valamint több politikai párt elleni februári kibertámadásért. Az álláspont nem hivatalos, a nyilvános vád vélhetően a lehetséges gazdasági károktól való félelem miatt maradt el, ugyanis Kína Ausztrália legnagyobb kereskedelmi partnere. Bár Kína korábban is szerepelt a támadás gyanúsítottjai között, ám ekkor még Oroszország és Irán is említésre került, mint lehetséges forrás. További információ, hogy ugyan az incidens nyilvánosságra hozásakor a nyilatkozatok egyértelműen tagadták, hogy a támadás során adatok kompromittálódtak volna, azonban a Reutersnek nyilatkozó anonim források szerint a támadók magánlevelezésekhez és politikai dokumentumokhoz is hozzáfértek.

Bármelyik telefon feltörhető egy SMS-sel

(securityaffairs.co)

Egy SIM kártyákat érintő kritikus sérülékenységre derült fény, amelyre SimJacker-ként hivatkoznak és az eddigi legszofisztikáltabb olyan támadási módszernek tartják, amely a mobilhálózati technológia egy alapvető elemére irányul. A sebezhetőség egy legalább 30 országban alkalmazott technológiát, a SIM kártyába ágyazott S@T Browser (SIM Application Toolkit) utasítás csomagot érinti, a sebezhetőség kihasználása ezért készülék-független. A támadók távolról többféle tevékenységet is végezhetnek a felhasználó tudta nélkül: az eszközre vonatkozó helyinformációkat, IMEI adatokat kérdezhetnek le, hamis üzeneteket küldhetnek az áldozat nevében, hívásokat indíthatnak, vagy akár egy káros weboldal megnyitásával káros kódot telepíthetnek a készülékre. Mindezt rendkívül egyszerűen, egy káros kódokat tartalmazó SMS megküldésével érhetik el. A felfedező AdaptiveMobile Security szerint a módszert egy kormányok számára kiberkémkedést végző cég fejlesztette ki, és már legalább két éve aktívan használja is. **Bővebben...**

IT biztonsági Tanács

Több, mint 8 000 Google Naptár bejegyzés érhető el nyilvánosan az interneten, köztük szenzitív vállalati információkkal. Mindez nem egy sérülékenység eredménye, ugyanis a Google Naptárban már hosszú ideje lehetőség van publikussá tenni a naptár bejegyzéseket, ami azonban egyúttal azt is jelenti, hogy azok a Google keresővel is visszakereshetővé válnak.

A szolgáltatás használóknak érdemes a honlapunkon leírtak alapján felülvizsgálniuk a beállításokat és – amennyiben nem indokolt – a megosztás megszüntetése.

Szigorúbb kiberbiztonsági követelményeket támasztanak az orosz bankokkal szemben

(ehackingnews.com)

A Bank of Russia közleménye szerint 2019 végéig új IT-biztonsági követelményeket szab az ország pénzintézetei számára, a nem megfelelés pedig bírságot fog maga után vonni. Artem Sychev, a Bank of Russia Információbiztonsági Osztályának helyettes igazgatója elmondta, a jegybank álláspontja szerint egy bank pénzügyi stabilitása nagyban függ attól, hogy mennyire képes reagálni az információ biztonsági problémákra. Az egyes pénzintézetek kockázati profiljának meghatározásához a jegybank négy fő tényezőt vesz majd figyelembe, amelyek között szerepel a nem engedélyezett tranzakciók aránya, ugyanakkor tekintetbe veszik a pénzintézet egyéb jellemzőit is, mint például a jövedelmezőség, vagy a vezetés minősége. A kockázati profil alapján azután a központi bank ajánlásokat fog meghatározni, azon szervezetek pedig, amelyek alacsony minősítést kaptak, fokozott felügyeletre és akár bírságra is számíthatnak.

A hálózati eszközök továbbra is hemzsegnek a sérülékenységektől

(thehackernews.com)

Az Independent Security Evaluators (ISE) „SOHOpelessly Broken 2.0” című tanulmányában összesen 125 különböző sérülékenységről számol be, amelyeket 13 SOHO router és NAS eszköz kapcsán azonosítottak, a potenciálisan érintett eszközök száma több millióra tehető. A kutatók elmondása szerint 12 eszköz esetében távolról, hitelesítés nélkül átvehető az irányítás. Az érintett gyártók (Buffalo, Synology, TerraMaster, Zyxel, Drobo, ASUS, Asustor, Seagate, QNAP, Lenovo, Netgear, Xiaomi, Zioncom) már korábban tájékoztatásra kerültek, legtöbbjük azóta már javítást is adott ki, azonban a Drobo, Buffalo Americas és a Zioncom Holdings még csak nem is reagált a megkeresésre.

Felfüggesztették a Huawei FIRST tagságát

(forbes.com)

Az amerikai kormányzat részéről intenzív támadás alatt álló Huawei-t átmenetileg kizárták a Forum of Incident Response and Security Teams (FIRST) közösségből. Mindez komoly veszteség a kínai tech cég számára, ugyanis a FIRST számít a legprominensebb nemzetközi információbiztonsági közösségnek, ahol az incidensekkel kapcsolatos információk országok közötti megosztása mellett számtalan technológiai, módszertani kérdés kapcsán zajlik diskurzus. A Huawei ráadásul egyúttal a Special Interest Groups-hoz történő hozzáférését is elveszíti, amely sérülékenységek és fenyegetésekkel kapcsolatos információk megosztására szolgál, emiatt pedig vélhetően a Huawei eszközök biztonsági frissítései is lassabban fognak elkészülni. **Bővebben...**

A hosszabb élettartamú okostelefonok sokat jelentenének környezetvédelmi szempontból

(reuters.com)

Új uniós előírások bevezetését javasolja a nonprofit szervezetekből álló Európai Környezetvédelmi Iroda (EEB), ugyanis egy általuk végzett kutatás szerint az okostelefonok élettartamának akár csak egy évvel történő meghosszabbítása is jelentősen csökkenthetné az Európai Unió szén-dioxid kibocsátását. Az új előírások értelmében az elektronikai eszközök előállítása során az energiafogyasztás helyett nagyobb figyelmet kellene fordítani az ún. éghajlatváltozási költségekre, valamint biztosítani az állampolgárok számára a „javítás jogát”, ami megkövetelné az eszközgyártóktól a tartósabb, könnyen javítható alapanyagok felhasználását. **Bővebben...**