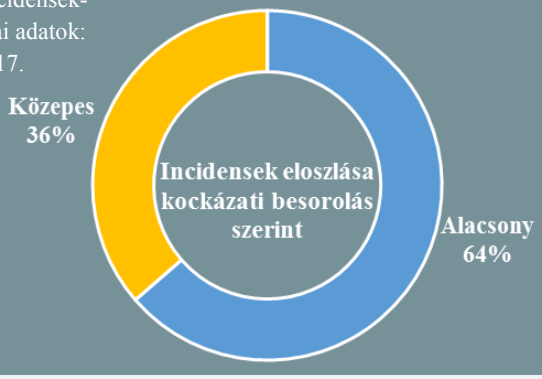
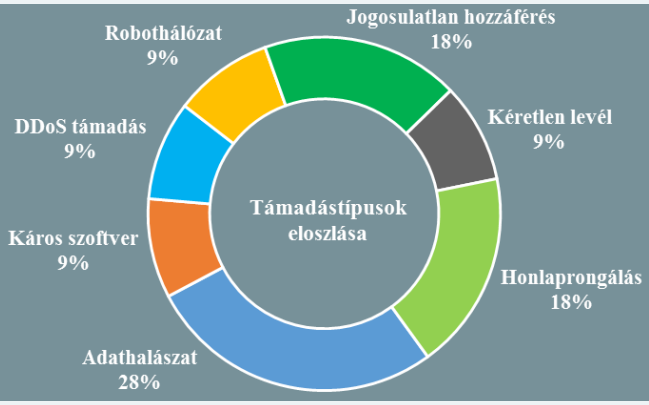
Nemzetközi IT-biztonsági sajtószemle

2019. 03. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.01.11. - 2019.01.17.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon, ahol naponta olvashatja legújabb híreinket!

Nincs központi terv az EU-s választások biztosítására

(wired.co.uk)

Az utóbbi évek incidensei bebizonyították, hogy a politikai választások hatványozottan kitettek az idegen államok érdekei mentén indított kiber műveleteknek, elég csak a legutóbbi amerikai elnökválasztás körüli eseményekre gondolni (lásd: DNC adatszivárgás, valamint orosz dezinformációs tevékenység). Habár ezen események a 2019 májusában esedékes Európai Uniós parlamenti választásokra történő felkészülésre is hatással voltak, egyes szakértők szerint mégsem kellő mértékben. Egy átfogó, központi terv helyett ugyanis jelen állás szerint mind a 27 tagállamnak saját magának kell megbirkóznia a választási rendszereik biztosításával, ráadásul a választásokat veszélyeztető számos veszély között nem feltétlenül egy direkt kibertámadás a legvalószínűbb, a dezinformációs műveletek például jóval gyakoribbak lehetnek. A kevés nemzeteken átívelő kezdeményezés között említhető az „EU vs Disinfo", amely az álhírek felderítésében igyekszik segítséget nyújtani. Liisa Past, az Estonian Information System Authority vezető kutatója pedig az aktuális helyzet előnyére hívja fel a figyelmet, rámutatván, hogy egyetlen választási rendszerrel szemben 27 különböző architektúra nagyban megnehezítheti a támadók dolgát, hiszen a sérülékenységek felmérése időigényes feladat.

Nem fizetne kiberbiztosítási kártérítést a Zurich Insurance a NotPetya támadás után

(securityaffairs.co)

Az amerikai Mondelez élelmiszergyártó óriás mintegy 100 millió dollárra perli a Zurich Insurance biztosító céget, amiért az elutasította a NotPetya zsarolóvírus támadás kapcsán benyújtott kárigényét. A vállalat szerint az ominózus támadás három százalékpontos visszaesést okozott 2017. második negyedéves bevételeiben a szállítási, valamint számlázási rendszerekben okozott károk miatt. A Zurich első körben 10 millió dollárt ajánlott fel, azonban később úgy döntöttek egyáltalán nem indítanak kifizetést egy záradékra hivatkozva, amely szerint ellenséges, vagy háborús eseményre nem vállalnak biztosítást. **Bővebben...**

Útmutató a nemzeti kiberbiztonsági stratégiák megalkotásához

(scmagazineuk.com)

Komoly biztonsági kockázatnak teszi ki magát az az ország, amelyik nem rendelkezik kiberbiztonsági stratégiával, azonban az ENSZ infokommunikációs technológiával foglalkozó ügynöksége, az International Telecommunication Union (ITU) szerint ez a világ 195 országa közül 119-re igaz, amellett, hogy a meglévő stratégiák között is nagy a különbség a minőséget tekintve. Annak érdekében, hogy segítsék ezen alapvető fontosságú stratégia megalkotását, a szervezet egy kifejezetten szabályalkotóknak szánt ajánlásgyűjteményt ad közre „Guide to developing a national cybersecurity strategy" címmel. **Bővebben...**

DNS eltérítéses támadásokkal gyanúsítják Iránt

(fireeye.com)

FireEye egy legkésőbb 2017 januárja óta zajló kiterjedt kibertámadási kampányra hívja fel a figyelmet, amely kormányzati, telekommunikációs és egyéb internetes infrastruktúrák ellen zajlik világszerte, de legfőképp a közel-keleti, észak-afrikai, európai és észak-amerikai régiókban. **Bővebben...**

Lehetséges fordulat az amerikai hatóságok kontra adatvédők harcában

(theregister.co.uk)

Egy kaliforniai bíró úgy határozott, hogy az amerikai hatóságok nem kényszeríthetik arra a gyanúsítottakat, hogy arcfelismerés, vagy ujjlenyomat olvasás útján feloldják a telefonuk zárolását. A jelszavak megadását az amerikai polgárok eddig is jogszerűen megtagadhatták, azonban a biometrikus azonosításra ez nem vonatkozott. **Bővebben...**

Négy éves adatvédelmi hibát javított a Twitter

(mashable.com)

Egy Twittert érintő biztonsági hiba vált ismertté, amelynek következtében egyes usereik privát tweetjei publikussá válhattak. Az esetről a Twitter adott hírt, eszerint amennyiben androidos felhasználóik 2014. november 3-a és 2019. január 14-e között a „Protect your tweets" funkció engedélyezése után további beállítást is módosítottak ─ például új e-mail címet adtak meg a fiókjukhoz ─ lehetséges, hogy ezzel az előbbit tudtukon kívül kikapcsolták. **Bővebben...**

IT biztonsági Tanács

A Carnegie Mellon Egyetem (CMU) incidenskezelési segédletet ad közre, amelynek célja egy viszonyítási alapot nyújtani az incidenskezeléshez a szervezetek számára.

A kiadványban az incidens menedzsment különböző aspektusai kerülnek feltérképezésre, mint például a védelem, detektálás, reagálás, valamint mindezek szolgáltatássá formálása.

Az anyag alkalmas arra, hogy egy szervezet magas minőségi standardoknak megfelelő incidenskezelési képességet fejlesszen.

Egyre váratlanabb helyeken bukkan fel az online terrorpropaganda

(wired.com)

A terrorszervezetek ─ mint például az ISIS ─ évek óta hatékonyan használják a streaming szolgáltatásokat, fájlmegosztó platformokat és a közösségi médiát kapcsolattartáshoz, toborzó tevékenységhez. Habár a Facebook, a Twitter, a YouTube, vagy a Telegram megerősített felügyelettel és szigorúbb biztonsági intézkedésekkel egyre jobban képesek visszaszorítani a terrorista tartalmakat, a terrorszervezetek válaszul kevésbé ismert platformok felé fordulnak. Az ISIS eddig jellemzően a Telegramot használta a közlemények terjesztéséhez, azonban 2018 decembere óta ez kiegészült a mintegy 10 milliós ügyfélbázissal rendelkező RocketChattel, amelyet azóta több ISIS-hez köthető csoport (Khilafah News, Halummu, vagy Shumukh al-Islam) is előnyben részesít, sőt már technikai útmutató is készült a RocketChat telepítéséhez és anonim használatához. **Bővebben...**

Jól halad az indiai kibervédelmi ügynökség szervezése

(m.economictimes.com)

India egy kibervédelmi ügynökség felállításán dolgozik, amely az indiai védelmi minisztérium alatt működő Összhaderőnemi Törzs (Integrated Defence Staff ─ IDS) irányítása alatt áll majd, vezetője pedig egy háromcsillagos tábornok lesz ─ nyilatkozta Manoj Mukund Naravane tábornok, az indiai hadsereg keleti parancsnokságának parancsnoka. Elmondása szerint a szervezet nem kizárólag katonai funkciót lát majd el, célja a kibertérből származó bármiféle fenyegetés kezelése lesz. A már véglegesítési szakaszban álló tervek szerint a kötelékébe tartozó egységek decentralizáltan kerülnek elhelyezésre, annak érdekében, hogy egy kibertámadás esetén minden főhadiszálláson legyen kompetens személy. **Bővebben...**

Nyomozati anyagok szivároghattak ki az FBI-tól

(thehackernews.com)

Az oklahomai Department of Securities-hez kapcsolódó, több terrabájtnyi kormányzati irat vált nyíltan hozzáférhetővé a legutóbbi, amerikai kormányzatot érintő adatszivárgásban. A védelem nélküli tárolószerverre egy kiberbiztonsági kutató, Greg Pollock bukkant rá, mely szerveren több érzékeny akta is megtalálható volt, többek közt FBI nyomozati iratok is. A szerverhez bárki, bármiféle azonosítás nélkül hozzáférhetett. A nyomozati iratokon túlmenően elektronikus levelek, társadalombiztosítási számok, 10 000 bróker neve és címe, valamint távoli hozzáférési adatok is elérhetőek voltak. **Bővebben...**

Több, mint 140 nemzetközi járatot érinthetett az Amadeus online fogadási rendszer biztonsági hibája

(bleepingcomputer.com)

A Safety Detective egy biztonsági kutatója komoly hibát fedezett fel az Amadeus online repülőjegy foglalási rendszerben, amelynek következtében illetéktelen személyek képesek lehettek hozzáférni az utasok adataihoz, valamint módosítani is azokat. A rendszer igen népszerű, mintegy 140 nemzetközi légitársaság használja, ezzel a piacon jelentős (44%) részesedést tudhat magáénak ─ olyan ügyfelekkel, mint például a United Airlines, Lufthansa, vagy az Air Canada ─ így a problémában több millió utas vált potenciálisan érintetté. A kutató akkor fedezte fel a hibát, amikor egy izraeli társaság (EL AL) járatára szeretett volna foglalni. **Bővebben...**