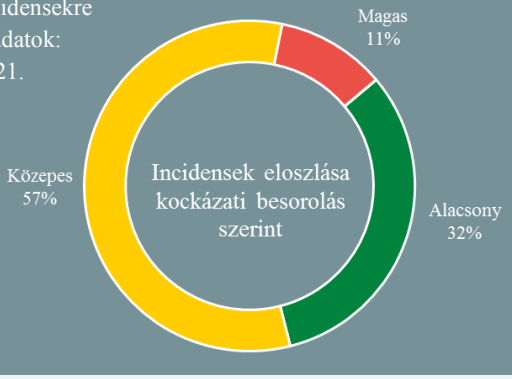
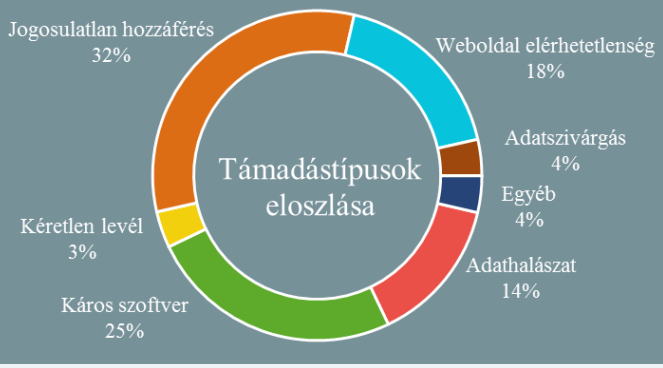
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.03.14. - 2019.03.21.





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

Az EU kiberbiztonsági eljárásrendet határozott meg a bűnüldöző hatóságok számára

(europol.europa.eu)

Az Európai Unió Tanácsa elfogadta az európai bűnüldöző hatóságok válsághelyzet kezelési eljárásrendjét (EU Law Enforcement Emergency Response Protocol), amely a meglévő EU-s válságkezelési mechanizmusokat kiegészítve segítséget nyújt az uniós tagállamok bűnüldöző hatóságainak a nagyszabású, határokon átívelő kibertámadások elleni összehangolt intézkedések végrehajtásában. A protokoll az Európai Bizottság 2017. szeptember 13-i 2017/1584. számú ajánlása nyomán került kialakításra, és központi szereppel ruházza fel az Europol számítástechnikai bűnözéssel foglalkozó európai központját (EC3). **Bővebben...**

Nyílt forrású szavazórendszer fejlesztését tűzte ki célul a DARPA

(motherboard.vice.com)

Az Egyesült Államok Védelmi Minisztériumának kutatóintézete (Defense Advanced Research Projects Agency – DARPA) 10 millió dolláros szerződést kötött egy biztonságos szavazórendszer létrehozására az oregoni Galois céggel. A tervek szerint a rendszer teljes mértékben nyílt forrású szoftverkomponensekből épülne fel, ellentétben a jelenlegiekkel, amelyek bevizsgálása kizárólag a szavazórendszerek ellenőrzésére akkreditált tesztelő laborok által lehetséges. Az úttörőnek számító elképzelés egyik alapköve, hogy a tervezett struktúra biztonságos open source hardverre épüljön, amely a DARPA által fejlesztett új CPU architektúrák felhasználásával valósul meg. **Bővebben...**

A ProtonMail felveszi a kesztyűt az FSZB-vel szemben

(protonmail.com)

A ProtonMail blogján reagált a levelezőszervereit érintő orosz blokádra, amelyben határozott módon foglalnak állást az intézkedéssel szemben, arra hivatkozva, hogy a ProtonMail szolgáltatása nem szerepel a hivatalos orosz tiltólistán, illetve, hogy a tiltás bármiféle jogi eljárás, vagy figyelmeztetés hiányában került bevezetésre. A közleményből kiderül az is, hogy a ProtonMail technikai ellenintézkedéseket hajtott végre, amelyekkel lényegesen csökkentették a blokkolás hatásait, és ígéretet tesznek arra, hogy a későbbiekben is mindent el fognak követni a ProtonMail szolgáltatás Oroszországban történő működésének biztosításához. **Bővebben...**

Ingyenes biztonsági elemző-értékelő szoftverek váltak elérhetővé kritikus infrastruktúra üzemeltetők számára

(securityweek.com)

Az ipari rendszerek kiberbiztonságával foglalkozó Dragos bejelentette, hogy felvásárolja az ugyancsak ezen a területen működő, nagy múltra visszatekintő NextDefense-t, az akvizíció folyományaképpen pedig ingyenesen elérhetővé teszik a Dragos Community Tools nevű biztonsági eszközgyűjteményt. Mindez egészen pontosan két alkalmazást takar, amelyek közül az egyik az ipari rendszereken folyamatos passzív hálózati monitorozást és mély csomagvizsgálatot (Deep Packet Inspection - DPI) lehetővé tévő Dragos Integrity, a másik a CyberLens, amely a gyors csomagfeldolgozás mellett a rendszerelemek vizualizációjára is alkalmas. Megjegyzendő, hogy az ingyenes szoftverekhez a Dragos nem nyújt támogatást.

Újabb trösztellenes panaszt nyújtottak be az Apple ellen

(zdnet.com)

A Kaspersky trösztellenes panaszt nyújtott be az Orosz Szövetségi Versenyügyi Hivatalhoz (FAS) az Apple alkalmazásboltjának üzletpolitikája miatt. A Kaspersky szerint az Apple App Store házirendjének való megfelelés érdekében a Kaspersky Safe Kids iOS alkalmazás tekintetében két alapvető — a futtatható alkalmazások kezeléséért, valamint a böngészők blokkolásáért felelős — funkciótól is meg kellett válniuk. Az orosz IT biztonsági cég úgy véli, az amerikai tech óriás jelentősen korlátozza a szülői felügyeleti szoftverpiacon a szabad versenyt, egyrészt az alkalmazások kizárólag az App Store-ból engedélyezett letöltése, másrészt az iOS 12 -es verziójában alapértelmezetten telepített Screen Time nevű applikáció miatt. Nemrég a Spotify élt hasonló panasszal a céggel szemben, azt kifogásolva, hogy az Apple olyan különadót vezetett be online áruházán keresztül értékesített alkalmazások bevételére vonatkozóan, ami miatt a harmadik féltől származó applikációk versenyhátrányba kerülnek a cég saját fejlesztésű Apple Music alkalmazásával szemben.

IT biztonsági Tanács

Ingyenesen hozzáférhető az eredetileg Linux/Unix környezetekre készült, valós idejű rendszermonitorozást lehetővé tévő DTrace program Windowsra portolt változata — tette közzé a Microsoft **blogján**. Mindez első körben csak egyes Windows 10 Insider verziókon használható, ám idővel a stabil kiadások számára is elérhetővé válhat.

Orosz kémhálózatot számolt fel a cseh kémelhárítás

(czech.cz)

Miloš Zeman cseh elnök néhány hónappal ezelőtt éles kritikával illette az ország polgári kémelhárítását (Bezpečnostní Informační Služba – BIS), kifogásolva, hogy a szolgálat már hat éve nem volt képes felfedni egyetlen orosz vagy kínai kémet sem. Minderre Michal Koudelka, a BIS vezetője a szervezet weboldalán reagált, miszerint a kérdéses időszakban több orosz és kínai ügynök tevékenységét is megakadályozták, példaként említve egy Csehország területén működő orosz hírszerző hálózat felszámolását. A Respekt nevű cseh hírportál most azt állítja, hogy saját nyomozás útján sikerült bővebb információkat szereznie az esetről. **Bővebben...**

Tízből nyolc kibertámadás során microsoftos sebezhetőséget használtak ki tavaly

(bleepingcomputer.com)

A Recorded Future elemzése szerint továbbra is a Microsoft termékek állnak leginkább a támadók fókuszában, háttérbe szorítva a 2017-ig listavezető Adobe Flash Playert. Miközben a sérülékenységek kihasználását komolyabb technikai ismeretek hiányában is lehetővé tévő programcsomagok (exploit kitek) az utóbbi években egyre kevésbé népszerűek, 2018-ban öt új ilyen exploit kitet azonosítottak (Best Pack Exploit Kit, Creep Exploit Kit, Darknet Angler, Fallout Exploit Kit, LCG Kit). Ezeket számos támadás során felhasználták már: a Falloutot például a GandCrab nevű zsarolóvírus terjesztéséhez is. **Bővebben...**

HTTPS forgalom lehallgatását detektáló eszközt ad közre a Cloudflare

(securityweek.com)

A titkosított webes forgalomba történő közbeékelődés és annak „lehallgatása” több okból történhet, amelyek között legitim szempontok is megtalálhatóak, jó példa erre a vállalati hálózatokon védelmi célból gyakorta alkalmazott proxyk. A Cloudflare álláspontja szerint azonban ezen eljárások egyre szélesebb körű alkalmazása összességében inkább károsan hat az SSL/TLS által nyújtott biztonságra nézve, amelyre korábban már az US-CERT is felhívta a figyelmet. **Bővebben...**

EU-Parlament döntése: jön a digitális ujjlenyomat a személyi igazolványokon

(heise.de)

A személyi igazolványokra a közeljövőben a digitális arckép mellett két ujjlenyomat is felkerül egy chip segítségével – elsősorban közbiztonsági okokra való tekintettel. Az EU állampolgárainak nemsokára a személyi igazolvány igénylésekor két ujjlenyomatot is kell adniuk, az ehhez szükséges végleges jogi aktushoz szükséges teendők már folyamatban vannak a strassburgi fórumokon. Az így kibővített biometrikus adatokhoz a tervek szerint az adó- és vámhatóságok, illetve a rendőri szervek is hozzáférhetnek majd. Ha elfogásra kerül a normatervezet, két éven belül minden tagországban hatályba lépnek ezen új szabályok. **Bővebben...**

Az autóipart vette célba Vietnám vezető hacker csoportja

(cyberscoop.com)

A FireEye információi szerint az APT32 (vagy OceanLotus) néven ismert, feltételezetten vietnámi állami kötődésű hacker csoport február óta több (5-10) multinacionális autóipari vállalat ellen indított informatikai támadást. **Bővebben...**