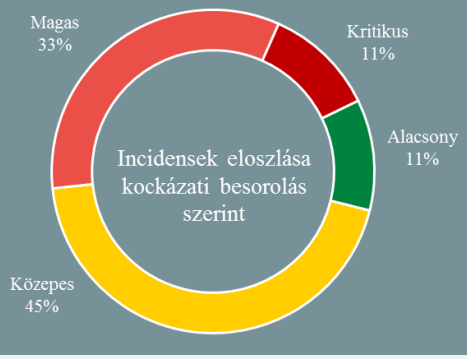
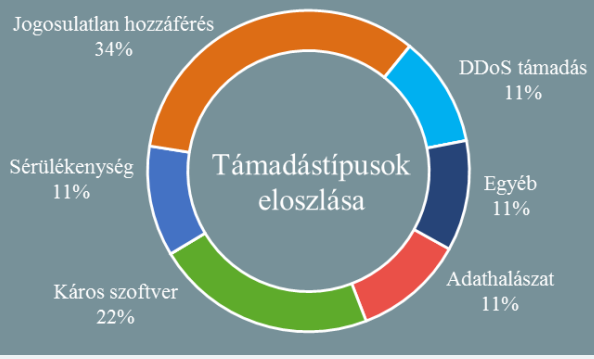
Nemzetközi IT-biztonsági sajtószemle

2019. 14. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.03.29. - 2019.04.04.





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

Szingapúri „álhír törvény": hamis hírek elleni küzdelem vagy állami cenzúra?

(www.techcrunch.com)

Hétfőn került előterjesztésre a szingapúri Igazságügyi Minisztérium (MinLaw) által benyújtott online hamis és manipulatív tartalmakra vonatkozó törvényjavaslat (Protection from Online Falsehoods and Manipulation Bill), amely lehetővé tenné a kormány számára, hogy „kiigazításokat" eszközöljön a kifogásolt online tartalmak esetében. Az elképzelés szerint ilyenkor az eredeti információ is megmaradna, csupán társulna hozzá egy korrekció. A törvényjavaslat további lényeges eleme, hogy az álhírek ("fake news") terjesztését bűncselekményként határozza meg, amely személyenként 50 000 dolláros pénzbírság mellett akár 5 éves szabadságvesztéssel is büntethető, amennyiben pedig a tevékenység automatizált fiókokkal (botokkal) történik, már 100 000 dollár és 10 éves börtönbüntetés is kiszabható. A MinLaw által kiadott sajtóközlemény szerint a törvényjavaslat célja nem a szabad véleménynyilvánítás korlátozása, Phil Robertson, a Human Rights Watch ázsiai igazgató-helyettese azonban attól tart, a törvény célja inkább a rendszerkritikus vélemények elhallgattatása, amelyre már korábban is történtek kezdeményezések.

Hasznos szolgáltatással bővül a Shodan kereső

(darkreading.com)

Az információbiztonsági szakemberek által nagy népszerűségnek örvendő Shodan platform egy új, hasznos eszközzel bővült, amely lehetővé teszi a vállalkozások számára saját interneten keresztül elérhető eszközeik monitorozását. A havidíjas Shodan accounttal rendelkező ügyfelek számára többletköltség nélkül elérhető Shodan Monitor megalkotásakor kifejezetten szempont volt, hogy az eszköz alkalmazása ne igényeljen komolyabb technikai tudást, így minél szélesebb körben használható legyen. **Bővebben...**

Adatszivárgás a Toyotánál: 3,1 millió ügyfél érintett

(gbhackers.com)

Azonosítatlan hackerek jogosulatlan hozzáférést szereztek a Toyota tokiói értékesítési leányvállalatai által közösen használt informatikai hálózathoz, amelyen keresztül mintegy 3,1 millió vásárló szenzitív adatát érték el. A vállalat közleményében jelezte, hogy a megtámadott szervereken banki információkat nem tároltak, azt pedig nem erősítették meg, hogy történt-e ténylegesen adatszivárgás. Bővebb tájékoztatást a jelenleg folyó vizsgálatokra hivatkozva nem nyújtottak, így jelenleg nem ismert a támadás során alkalmazott módszer és a támadók feltételezett kiléte sem.

Hatósági eljárás indult egy olasz kémszoftver fejlesztő cég ellen

(motherboard.vice.com)

A nápolyi rendőrség közleménye alapján a hatóságok razziát tartottak a hivatalosan biztonsági kamera megfigyelő rendszert működtető, azonban a Motherboard információi szerint kémprogramokat is gyártó eSurv nevű cégnél. Egy korábbi publikációjuk szerint a cég felelős több, mint 25, a Google Play Store-ba juttatott káros kódért, amelyekre az eset kapcsán vizsgálódó kutatók összefoglaló néven, Exodus-ként hivatkoznak. A spyware-t több komoly kritika is érte, mert bár a fejlesztő cég rendelkezik érvényes, „passzív és aktív elfogó rendszerek fejlesztésére" szóló szerződéssel, a hatályos olasz jogszabályok értelmében a kémkedési célú szoftverek nem telepíthetők a célpont megfelelő leellenőrzése nélkül. Az Exodus készítői ezt azonban nem végezték megfelelően, ráadásul nem ez volt az egyetlen súlyos hiba. **Bővebben...**

Hamis hírek elleni szolgáltatást vezet be a WhatsApp

(www.reuters.com)

A WhatsApp új szolgáltatással igyekszik visszaszorítani a hamis hírek terjedését Indiában, röviddel a nemzeti választásokat megelőzően. Az indiai Proto nevű startuppal közösen kidolgozott „Checkpoint Tipline" szolgáltatás a WhatsApp szerint képes kép-, videó-, illetve szöveges formátumú üzeneteket fogadni, majd ezeket „igaz", „hamis", „félrevezető", vagy „kétséges" minősítéssel ellátni. A Proto két alapítója, Ritvvij Parrikh és Nasr ul Hadi szerint a projekt célja a dezinformációs jelenség tanulmányozása, amely lehetőséget ad a félretájékoztató kampányok jobb megértéséhez. A Reuters próbára tette a szolgáltatást egy direkt hamis információkat tartalmazó üzenet elküldésével, azonban jelen publikáció elkészültéig ─ a beküldéstől számított két órán belül ─ nem érkezett válasz a fogadást nyugtázó automata üzeneten kívül. **Bővebben...**

IT biztonsági Tanács

A Microsoft felhőalapú identitás- és hozzáférés felügyeleti szolgáltatása, az Azure Active Directory számára hivatalosan elérhetővé vált a Password Protection nevű biztonsági szolgáltatás, amelynek használatával a rendszergazdák egyszerű módon megakadályozhatják, hogy a felhasználók olyan jelszavakat válasszanak, amelyek könnyen kitalálhatóak, vagy akár már kompromittálódtak is valamely adatszivárgási incidens során. Rendszergazdák a jelszóvédelem üzembe helyezéséről a gyártó oldalán találhatnak részletes információt.

Ezek az eszközök álltak az ASUS frissítéssel fertőző malware célpontjában

(securityaffairs.co)

A Skylight Cyber biztonsági kutatói közreadtak egy listát azokról a hálózati eszköz azonosítókról (MAC cím), amelyeket az ASUS ellátási láncát felhasználó malware támadás során a támadók a célpontok azonosításához használtak. A lista 583 MAC címet tartalmaz, amelyek az esetet feltáró Kaspersky által elemzett backdoorokból származnak. Az orosz biztonsági cég bár korábban kiadott egy online toolt, amellyel bárki megállapíthatta, hogy a saját eszközei érintettek -e a támadásban, azonban a Skylight Cyber fontosnak látta a teljes lista nyilvánosságra hozását, mert úgy vélik, ez szolgálja igazán a biztonsági közösség érdekeit. Azon felhasználók számára, akik megtalálják a hálózati eszközük címét, javasolt a rendszer teljes újratelepítése a gyári beállításokra történő visszaállítással (lásd: alapállapotba állítás).

Az IT biztonsági szakma számára hasznosnak ígérkező sérülékenységi adatbázis van készülőben

(vulncode-db.com)

A Vulncode-DB a fejlesztői információk szerint egy olyan sérülékenység leírásokat tartalmazó nyílt forrású adatbázis, amely az NVD (National Vulnerability Database) és a CVE (Common Vulnerabilities and Exposures) adatbázisok lehetőségeit a sérülékenységekre vonatkozó valós ─ például felhasználóktól származó ─ információkkal egészíti ki. A komplex sérülékenységi információk egy felületen történő közzététele a készítők szerint egyszerre szolgálhat oktatási, valamint kutatási célokat is. A Vulncode-DB jelen (alfa) verziója még több működési hibát is rejt ─ valamint a funkciók tekintetében is meglehetősen hiányos ─ azonban már online elérhető. A projekt gazdái bármilyen szakmai észrevételt, javaslatot, ötletet szívesen fogadnak az érdeklődő szakemberektől.

Helyzetkép a távközlési hálózatokat célzó kiberbűnözési technikákról

(europol.europa.eu)

A telekommunikációs rendszerek a modern társadalmak számára kritikus tényezőnek számítanak, éppen ezért a távközlési ipart érő fenyegetések és sérülékenységek megértése kiemelten fontos az iparági szereplők számára. Ezt szeretné elősegíteni a Trend Micro és az Europol közös kiadványa (Cyber-Telecom Crime Report 2019), amely átfogó, magas szintű képet kíván nyújtani a távközlési hálózatokat célzó kiberbűnözői tevékenységekről (cyber-telecom fraud) és az alkalmazott főbb technikákról. Az összefoglaló alapvetően kétféle típusú fenyegetést tárgyal: a fizikai telekommunikációs infrastruktúrákat célzó, valamint a számítógépes hálózat-alapú támadásokat. A valós eseteket is bemutató anyag konklúziója, hogy az információ csere, valamint az együttműködés az, amivel sikerrel vehető fel a harc az egyre gyakoribb és nagyszabásúbb támadásokkal szemben.

Új trend a papírmentes önkormányzatért és a digitális közigazgatásért

(heise.de)

A németországi Rheinland-Pfalz tartomány egyre több önkormányzata végzi feladatait papírmentesen. Ez nemcsak papírlapok százezreinek ─ és ezáltal jelentős pénzösszegek ─ megtakarítását jelenti, hanem egyébként az ügyintézés is gyorsabbá válik, ami egyúttal környezetvédelmi szempontból is előnyös. Trier városában például körülbelül 1,6 tonna papírt spórolnak meg évente a digitalizált eljárások segítségével, ezen keresztül pedig nagyjából 22 500 eurot takarítanak meg a nyomtatási költségek terén. **Bővebben...**