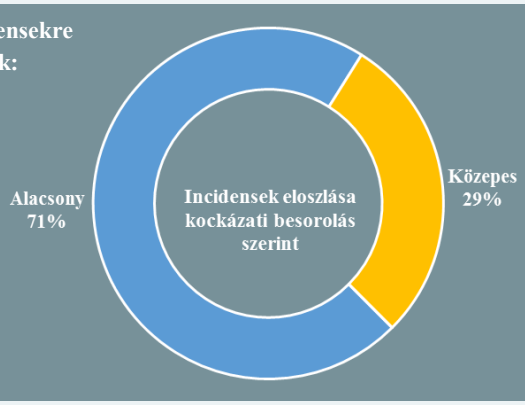
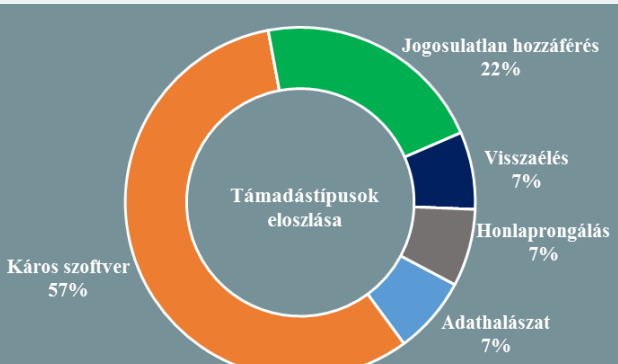
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

2018. 42. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.10.12. - 2018.10.18.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon!

A holland védelmi miniszter elismerte, hogy kiberháborúban állnak Oroszországgal

(www.sputniknews.com)

Hollandia védelmi minisztere, Ank Bijleveld, igenlő választ adott az ország közszolgálati médiaügynökségének (NPO) azon kérdésre, hogy Hollandia és Oroszország aktuális viszonyának jellemzésére használható-e a „kiberháború" kifejezés. Mindez egy áprilisi incidens kapcsán került szóba, amelyben a vádak szerint orosz titkosszolgálati ügynökök informatikai támadást kíséreltek meg a Vegyifegyver-tilalmi Szervezet (OPCW) hágai főhadiszállásának IT rendszere ellen. Az eset nyilvánosságra kerülése után Hollandia növelni kezdte kiberbiztonsági kiadásait, valamint a NATO is felajánlotta kiberhaderejét. Az orosz narratíva szerint mindez csupán provokáció és pusztán egyes politikai intézkedések megalapozásául szolgál.

A cseh hírszerzés megakadályozta a Hezbollah egy kiberműveletét

(www.zdnet.com)

A cseh Biztonsági Információs Szolgálat (BIS) átvette az irányítást több olyan szerver felett, amelyeket a Hezbollah mobil készülékek káros kóddal történő fertőzésére használt ─ írja a ZDNet. Michal Koudelka, a szolgálat vezetője elmondta, hogy a leállított szerverek a Cseh Köztársaság területén működtek, és információik szerint 2017 eleje óta vettek részt a malware terjesztésben. A libanoni félkatonai szervezet módszere abban állt, hogy hamis Facebook profilok felhasználásával, fiatal nőket megszemélyesítve a célpontokkal üzenetváltást kezdeményeztek, majd igyekeztek rávenni őket egy fertőzött üzenetküldő applikáció telepítésére, amelynek segítségével azután információkat nyertek ki az áldozat készülékéről. A kampány célkeresztjében közel-keleti, közép- és kelet-európai férfiak álltak.

Halálos kibertámadásra számít az Egyesült Királyság

(www.zdnet.com)

A brit kibervédelmi központ (NCSC) szerint csak idő kérdése, hogy mikor következik be egy emberéleteket is veszélyeztető támadás az Egyesült Királyság ellen. A szervezet 2016-os megalakulása óta mintegy 1 167 támadással küzdött már meg, Ciaran Martin, az NCSC vezetője szerint ezek nagy része valamilyen módon ellenséges nemzetállamokhoz volt köthető. Az eddigi legkiugróbb eset a WannaCry zsarolóvírus kampány volt, azonban Martin szerint egy ennél sokkal nagyobb pusztítással fenyegető, ún. „1-es kategóriájú" támadásra kell számítani a közeljövőben. Az NCSC saját definíciójában ez a „nemzeti kiber vészhelyzetként" is hivatkozott, nemzetbiztonsági kockázatot is hordozó vészállapot az alapvető szolgáltatások működését akadályozza, és komoly gazdasági és/vagy szociális következményekkel jár, valamint potenciálisan emberéleteket is követelhet. **Bővebben...**

Adatszivárgás történt a Pentagonnál

(www.securityaffairs.co)

Az Egyesült Államok Védelmi Minisztériuma közleményben tudatta, hogy egy adatszivárgás során mintegy 30 000 munkatársuk személyes adatai ─ köztük például bankkártya információk ─ szivároghattak ki. A hivatal szóvivőjének elmondása szerint az incidens néhány hónapja történt, amely során minősített adat nem kompromittálódott. A biztonsági eseményben érintett rendszerről biztonsági okokra hivatkozva nem árultak el többet, ugyanis az adott gyártóval továbbra is szerződésben állnak. A kivizsgálás jelenleg is zajlik, a felhasználók kiértesítését még nem kezdték meg.

Jelentősen emelkedett az Apple eszközöket célzó kriptobányász támadások száma

(www.infosecurity-magazine.com)

A Check Point szerint az iPhone -ok elleni kriptovaluta bányász támadások szeptember utolsó két hetében közel 400%-kal nőttek ─ derül ki a cég legújabb Global Threat Indexéből. A támadások során legnagyobbrészt Coinhive kóddal történt a fertőzés, ami világszinten a szervezetek mintegy 19%-ánál már felütötte a fejét, és 2017 decembere óta folyamatosan vezeti a fenyegetési indexet. A második leggyakoribb miner a Cryptoloot, ami az összesített listán a harmadik helyen szerepel. Maya Horowitz, a Check Point fenyegetés-elemző csoportjának vezetője szerint még vizsgálják, hogy mi az oka annak, hogy a Safari böngészőt használó eszközök most ennyire fókuszba kerültek, ugyanis a támadások ─ az eddigi megfigyelések alapján ─ nem bírnak új funkcionalitással.

IT biztonsági Tanács

Az álhírek kiszűréséhez segítséget nyújthat a NewsGuard böngésző plugin, amely a legnépszerűbb böngésző programokon elérhető.

Működése egyszerű: a program ikonja zöld színre vált, amennyiben egy olyan híroldalt töltünk be, amit a program mögötti felkészült újságírókból és szerkesztőkből álló team már jóváhagyott. Amennyiben egy feltételezett álhír oldalról van szó, az ikon vörös színű lesz. Az oldal működéséről, az értékelések során alkalmazott kritériumokról bővebben itt olvashat.

Arcfelismerő rendszerrel váltják ki a reptéri ellenőrzéseket egy sanghaji repülőtéren

(www.zdnet.com)

A sanghaji Hungcsiao nemzetközi repülőtéren arcfelismerő rendszert alkalmaznak az utasok azonosításához a jegykezelés, a poggyászfelvétel és a biztonsági ellenőrzés során. A tervek szerint a teljesen automatizált rendszert idővel az egész országra kiterjesztik, a pekingi és a nanyangi reptereken már el is kezdték a kiépítését. Az arcfelismerési technológia Kínában már az élet számos területén megvetette a lábát, például létezik olyan étterem, ahol a fizetéshez, egy iskolában pedig a tanulók monitorozásához használják, illetve a hatóságok egy nemzeti megfigyelőrendszer létrehozásán is dolgoznak. **Bővebben...**

A NATO kiberparancsnoksága még az alapelvek tisztázásával küzd

(www.itnews.com.au)

Az Észak-atlanti Szövetség katonai kiberparancsnokságának állománya 2023-ra teljesen feltöltésre kerülhet, készen arra, hogy saját kompetenciából indíthasson kibertámadásokat, azonban ehhez még az alapvető szabályok sem kerültek lefektetésre. A 2018. augusztus 31-én Belgiumban létrejött kiberműveleti központ (CYOC) jelenleg nem rendelkezik saját kiberháborús arzenállal, habár több tagország ─ például az Egyesült Államok, Nagy-Britannia és Észtország ─ is felajánlotta saját kiber képességét a fenyegetések kezeléséhez. Ian West, a NATO kommunikációs ügynökségének kiberbiztonsági vezetője szerint a központ fő célja a fennhatósága alá tartozó kibertér lehető legteljesebb felügyelete, a valósidejű információk begyűjtése ugyanis elengedhetetlen a parancsnoki döntések meghozásához. Amennyiben a szövetségnek sikerül megegyeznie a kiberháborús alapelvekről ─ azaz például, hogy mely kibereseményekről léptethetik életbe az 5-ös cikkelyt ─ az egyes nemzetállamok kiberkapacitásai bevonásra kerülhetnek a szövetséges műveletekbe a CYOC, és végső soron a NATO-erők európai főparancsnokának (SACEUR) irányítása alatt.

Fogyasztóvédők támadják a közösségi médiákat adatvédelmi hiányosságaik miatt

(www.heise.de)

Egy friss német fogyasztóvédelmi tanulmány megállapításai alapján a vonatkozó adatvédelmi szabályok ellenére a közösségi hálók felhasználói kevés kontrollt gyakorolhatnak saját adataik kezelése kapcsán. A Facebook, Instagram, WhatsApp, Twitter, Snapchat és LinkedIn vonatkozásában egyik fő kritikaként fogalmazódott meg, hogy az előírások ellenére az adatvédelmi alapbeállítások nem minden esetben a fogyasztók érdekeinek megfelelően kerültek kialakításra. Mindazonáltal pozitív példaként megemlítendő, hogy a tanulmány szerint a Pinterest és a YouTube döntően megfelelő módon hajtják végre a felhasználókat védő adatvédelmi intézkedéseket. **Bővebben...**

Ausztrália betiltaná a torrent oldalakat

(www.techradar.com)

Az ausztrál kormány az elmúlt években számos komoly intézkedést hozott a szerzői jogokat sértő weboldalak visszaszorítása érdekében, e tekintetben a legmarkánsabb lépés a szerzői jog online jogsértéssel történő 2015-ös kiegészítése volt, amely alapjául szolgált több online kalózportál blokkolásának. A kormány állítása szerint a rendelkezés hatására visszaszorultak a szerzői jogsértések, azonban most újabb törvények útján még jobban kiszélesítenék a blokkolható oldalak körét, sőt azt is megtiltanák, hogy a keresőmotorok (Google, Yahoo, Bing, stb.) egyáltalán megjelenítsék a torrent site-okat a keresési eredmények között. **Bővebben...**