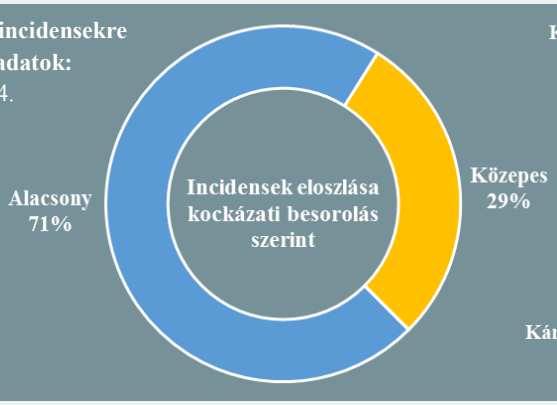
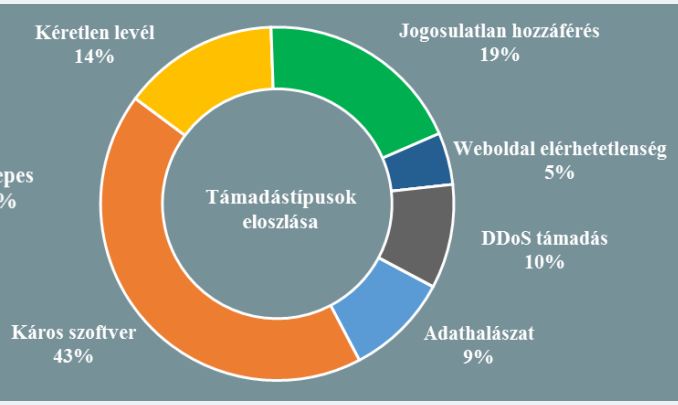
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.09.28. - 2018.10.04.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon!

Változások az Amerikára irányuló orosz online dezinformációs stratégiában?

(www.zdnet.com)

A FireEye úgy véli, Oroszország a 2018-as amerikai időközi választásokkal kapcsolatos dezinformációs műveletek terén feltehetően óvatosabb lesz, mint 2016-ban, az amerikai elnökválasztáskor ─ írja a ZDNet. Az USA-beli kiberbiztonsági cég szerint akkor a fő célok az érzékeny politikai információk megszerzése és nyilvánosságra hozása (pl.: a Demokrata Nemzeti Bizottság e-mailjeinek kiteregetése); a választási infrastruktúra elleni támadások (pl.: szavazói regisztrációs adatbázisok ellen); illetve a közösségi platformokon keresztül történő manipuláció voltak. Egy ehhez hasonló direkt kampány azonban könnyen veszélybe sodorhatja a narratívát, amihez Oroszország következetesen ragaszkodik ─ miszerint nincs köze a 2016-os amerikai elnökválasztás befolyásolásához ─ ráadásul az aktuális politikai helyzettel is elégedett lehet. A stratégia finomítására utalhat az is, hogy az utóbbi időben nem történt a korábbiakhoz hasonló szivárogtatási incidens, hozzátéve, hogy egy ilyen támadás valószínűsége ettől még nem zárható ki. **Bővebben...**

Az új-zélandi határőrség átvizsgálhatja az elektronikus eszközöket

(amp.rnz.co.nz)

A 2018. október 1-jén életbe lépő „Customs and Excise Act 2018" értelmében az Új-Zélandra látogatóknak a hatóságok kérésére hozzáférést kell biztosítaniuk elektronikus eszközeikhez határátlépéskor, a határőrségnek azonban ehhez ésszerű gyanúval kell rendelkeznie. Az ellenszegülők 5 000 dolláros bírságra számíthatnak, a vizsgálatot ─ amely Terry Brown, a határőrség szóvivője szerint a felhőben lévő adatokra nem terjed ki ─ azonban ekkor sem ússzák meg. Kris Faafoi vámügyi miniszter szerint minderre azért van szükség, mivel a szervezett bűnözői csoportok egyre szofisztikáltabb módszereket alkalmaznak a csempészéshez. **Bővebben...**

Egyre többet áldoz az USA a kritikus rendszerek biztonságára

(www.securityweek.com)

Az amerikai energiaügyi minisztérium 28 millió dollárral támogatja a kiberfenyegetéseket megelőző, detektáló és elhárító innovatív eszközök és technológiák fejlesztését. Nem ez az első eset, hogy a minisztérium nagyobb összeget invesztál a kiberbiztonságba, idén már egyszer 25 millió dollárt, nagyjából egy évvel ezelőtt pedig mintegy 20 millió dollárt mozgósítottak ilyen célból. Jelenleg 11 olyan projekt fut, ami az elektromos, olaj és földgáz rendszerek egy kibertámadásoknak ellenálló architektúrájának fejlesztését, valamint a kommunikáció és a felhő szolgáltatások biztonságának növelését célozza. **Bővebben...**

Az eddigi legnagyobb állami támogatású vállalati kémkedésre derülhetett fény?

(thehackernews.com)

Egy, a Bloomberg által publikált cikk szerint állítólag egy apró, káros kódokat tartalmazó mikrochipre bukkantak egyes Kínában gyártott alaplapokon, amelyeket széles körben használnak ─ például közel 30 amerikai vállalat, köztük az Apple és az Amazon szervereiben. A kérdéses chipeket a világ egyik legnagyobb szerveralaplapokat gyártó cége, az amerikai Super Micro tervezte, és a kínai gyártás során kerülhettek az alaplapokra. A Bloomberg állítása szerint a chipek olyan beágyazott kódokat tartalmaznak, amelyek lehetőséget teremtettek arra, hogy azokon keresztül a kínai állam megfigyeléseket végezzen, illetve a cikk kitér arra is, hogy minderre az Apple és az Amazon már 2015-ben felfigyelt. A hírbehozott vállalatok és a kínai állam mindeddig tagadják az információk valódiságát. **Bővebben...**

Intra: egy Google-ös anti-cenzúra app

(techcrunch.com)

A Google Jigsaw nevű részlege bemutatta az Intra nevű mobil applikációt, amellyel a cég szerint megelőzhetőek a DNS manipulációs támadások, amelyeket egyes országok az állami cenzúra eszközeként hír és közösségi oldalak elérésének blokkolására használnak ─ a TechCrunch cikke ezzel kapcsolatban név szerint említi Törökországot és Venezuelát. Az Intra azáltal nyújt védelmet, hogy gondoskodik a DNS szerver felé irányuló forgalom titkosításáról, ehhez alapértelmezetten a Google DNS szolgáltatását veszi igénybe, alternatívaként beállítható még a Cloudflare publikus DNS-e. A kevéssé ismert Google divízió egyéb cenzúra ellenes appokat is fejleszt, mint például a DDoS védelmi Project Shield, vagy az Outline, ami újságíróknak és aktivistáknak nyújt VPN szolgáltatást. **Bővebben...**

IT biztonsági Tanács

Az US-CERT riasztást adott ki, amelyben javaslatot tesz az APT fenyegetések kezelésére.

Egyre jellemzőbb, hogy a támadók egy megbízhatónak minősített hálózat felől próbálnak bejutni a célkeresztben lévő vállalati rendszerekbe, ami ellen csak szigorú házirendek alkalmazásával lehet felvenni a harcot. Ennek értelmében ─ többek között ─ javasolt kiemelt figyelmet fordítani az alábbiakra:

- Többfaktoros autentikáció, szigorú fiók felfüggesztési házirend és a legkisebb jogosultság elvének következetes alkalmazása;
- az RDP hozzáférések felülvizsgálata, a korlátozott rendszergazdai mód bekapcsolása;
- a felhasználók oktatása a biztonságtudatos magatartásra a kéretlen e-mailekkel kapcsolatban.

Kiberkommandó: szabályellenesen nyolc millió külső tanácsadóknak

(www.heise.de)

A német igazságügyi minisztérium egy, a szövetségi hadsereg (Bundeswehr) egyik IT-projektje kapcsán – 900 és 1 700 eurós napidíjak révén – nyolcmillió eurót fizetett ki tanácsadás jogcímén, nem megfelelő keretszerződések alapján külső vállalkozóknak, szabálytalanul felhasználva ezzel a költségvetési forrásokat és megsértve a közbeszerzési szabályokat. Az érintett projekt (CIT Quadrat) 2012-ben kezdődött és célja a katonaság IT-rendszerének modernizálása volt, és amelyre ezen időszak alatt 350 millió euró került elköltésre. **Bővebben...**

Solid: a Web atyja új korszakot hirdet az adatkezelésben

(medium.com)

Sir Timothy Berners-Lee, az „Egy kis lépés a Web-nek..” című posztjában mutatta be új, Solid névre hallgató nyílt forrású platformját, amely alternatívát kíván nyújtani az aktuális adatkezelési modellel szemben. Jelenleg a felhasználóknak a különböző szolgáltatások igénybevételéhez át kell adniuk személyes adataikat a digitális cégeknek, amely ─ mint fogalmaz ─ a tapasztalatok szerint nem a felhasználók érdekeit szolgálja. Az új koncepció teljes kontrollt ígér mindenkinek a saját adatai felett. **Bővebben...**

Észtország beperli a Gemaltót

(www.reuters.com)

Az észt rendőrség 152 millió euróra perli a Gemaltót, amiért tavaly vissza kellett vonni az észt elektronikus személyigazolványokat egy biztonsági hiba miatt. Az észt Rendőrség és Határőrség (PPA) közleményben tudatta, hogy a Gemalto ugyan elkészítette az igazolványokhoz tartozó egyedi privát kulcsokat, ám a szerződésben vállaltakkal ellentétben elmulasztotta azokat beágyazni a kártyákon lévő chipbe, ami sérülékennyé tette a rendszert külső kibertámadásokkal szemben. Az észt kormányzat 2002 óta állt a céggel ─ és jogelődjével ─ szerződésben, ám a tavalyi történések után inkább a francia Idemiával állapodott meg. **Bővebben...**

Az Egyesült Államok a NATO rendelkezésére bocsátja kiberarzenálját

(securityaffairs.co)

A tervek szerint az USA elérhetővé teszi offenzív kiberarzenálját a NATO számára, az olyan fenyegetések elleni védelem gyanánt, mint amit Oroszország jelent, Washington ezzel olyan országok példáját követi, mint az Egyesült Királyság és Dánia. Jens Stoltenberg NATO főtitkár szerint a tagállamok elleni kibertámadások ─ különösen a balti államok tekintetében ─ egyre gyakoribbá és szofisztikáltabbá váltak **Bővebben...**

Új állami kiberközpont jött létre Kanadában

(cyber.gc.ca)

Kanada védelmi minisztere bejelentette a Kanadai Kiberbiztonsági Központ (Canadian Centre for Cyber Security) megalakulását 2018. október 1-jén. Az intézmény a nemrég nyilvánosságra hozott nemzeti kiberbiztonsági stratégia egyik fontos elemeként jön létre, szervezetileg a Kommunikációs Biztonsági Szervezet (CSE) részeként. A kiberközpont főbb feladatai: a kanadai állampolgárok tájékoztatása kiberbiztonsági témakörben, védelmi technológiák, eszközök fejlesztése és terjesztése, a különböző szektorok közötti információcsere biztosítása, tudatosítás és oktatás, valamint nemzeti kontaktpont szerepkörből eredő feladatok. **Bővebben...**