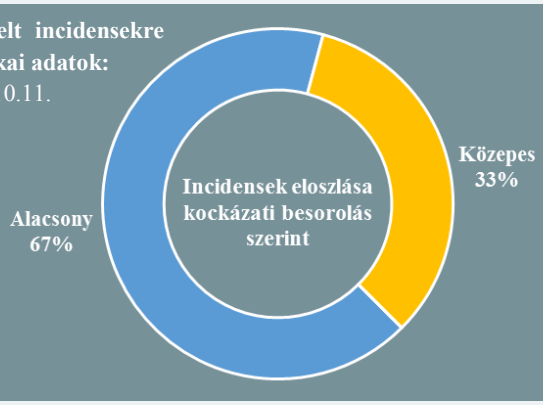
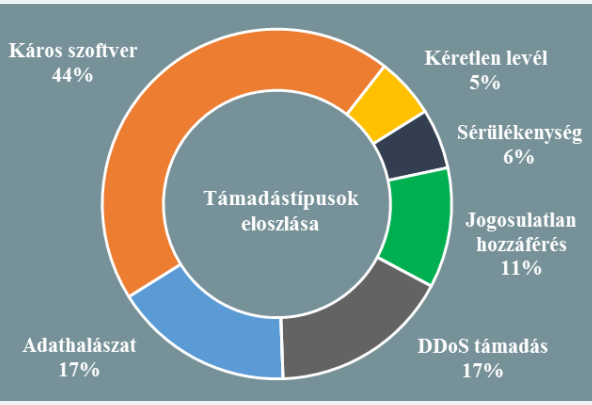
**Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:**
2018.10.05. - 2018.10.11.




**Kövessen minket online az itbiztonsag.govcert.hu oldalunkon!**

## A nyugati világ számára (ismét) Kína jelenti a legnagyobb kiberfenyegetést

**(www.zdnet.com)**

Biztonsági szakemberek attól tartanak, hogy egy ipari kémkedéssel vádolt kínai hírszerző tiszt letartóztatása miatt Kína ismét fokozhatja kibertevékenységét a Nyugat ellen. Az amerikai igazságügyi minisztérium tegnap közleményt adott ki Yanjun Xu ─ más néven Qu Hui, vagy Zhang Hui ─ a kínai civil hírszerzés (MSS) magas rangú tisztviselőjével szembeni vádemelésről, amiért állítólag amerikai légügyi és űrrepülési szervezetektől próbált üzleti titkokat szerezni. Kína még 2015-ben állapodott meg az Egyesült Államokkal a kiberkémkedési műveletek kölcsönös felfüggesztéséről, amelyhez sokáig tartotta is magát. Dmitri Alperovitch, a CrowdStrike biztonsági cég vezérigazgatója szerint a vádemelést Kína valószínűleg igyekszik majd megtorolni, ugyanakkor egyetért a Trump adminisztráció egy márciusi jelentésében foglaltakkal is, miszerint az ázsiai ország alapvetően már tavaly aktivizálta magát a támadások terén. **Bővebben...**

## ENISA jelentés a bizalmi szolgáltatókat érintő incidensekről

**(www.enisa.europa.eu)**

Az ENISA kiadta az elektronikus bizalmi szolgáltatóktól az eIDAS alapján begyűjtött, 2017-es évre vonatkozó incidens adatokat összesítő jelentését. Az összefoglaló főbb megállapításai szerint az incidensek közel fele határokon átívelő és komoly hatással bírt, a leginkább érintett szolgáltatások pedig az e-aláírás és az elektronikus bélyegzők voltak. Egy másik fontos megállapítás, hogy a biztonsági események hátterében elsősorban rendszerhibák és harmadik feleket érintő hibák álltak ─ mindkettő 36%-ot tett ki. Steve Purser, az ENISA alapműveletekért felelős osztályának vezetője szerint a jelentés világosan megmutatja, hogy az európai bizalmi szolgáltatók felügyelete csak nemzetek közötti kooperációval lehetséges.

## Kivizsgálják a Google+ adatszivárgását, de nem a GDPR tükrében

**(www.engadget.com)**

Németország adatvédelmi biztosa bejelentette, hogy vizsgálatot indít a Google+ adatszivárgási incidense kapcsán. Mint a napokban kitudódott, a Google közösségi szolgáltatása közel félmillió felhasználó személyes adatát tette elérhetővé, azonban a vállalat minderről hónapokon át hallgatott, arra hivatkozva, hogy nem igazolt, hogy azokkal történt is visszaélés. Most, az eset nyilvánosságra kerülését követően a cég bejelentette a Google+ megszüntetését, illetve új adatvédelmi megoldásokat vezetett be. Mivel az incidens még a GDPR hatálybalépését megelőzően történt, a tech óriás valószínűleg az adatvédelmi rendelet szigorú szankcióinál enyhébb büntetésre számíthat. **Bővebben...**

## Az ESET bizonyítékot talált arra, hogy ugyanaz a csoport felelős a NotPetya kampányért és az ukrán energiaszektor elleni kibertámadásokért

**(www.welivesecurity.com)**

A biztonsági cég kutatói lényeges hasonlóságokat fedeztek fel a tavalyi NotPetya wiper támadásokkal gyanúsított Telebots csoport által idén bevetett backdoor (Exaramel) és az Ukrajna elektromos ellátórendszere elleni 2016-os támadás során alkalmazott Industroyer nevű malware között, így feltételezik, hogy mindkettő mögött a Telebots áll. Az IT biztonsági szakma részéről mindez már korábban is felmerült, azonban eddig bizonyíték hiányában ez csupán spekulációnak számított. **Bővebben...**

## Mobilfizetéses lopások Kínában

**(www.engadget.com)**

Két nagy kínai mobilfizetési platform ─ az Alipay és a WeChat Pay ─ ügyfelei jogosulatlan App Store-os vásárlásokat jelentettek az utóbbi napokban, amelyeket a vállalatok szerint lopott Apple ID-kkal hajtották végre. Az Alipay kivizsgálást kért az Apple-től, valamint javasolta ügyfeleinek, hogy korlátozzák a jelszavas azonosítás nélkül elkölthető összegeket. Az Apple szóvivője az eset kapcsán felhívta a figyelmet a cég support oldalán javasoltak figyelembevételére, mint például: megfelelően erős jelszó használatára; a biztonsági kérdéseknél nehezen kitalálható válaszok megadására; illetve a kétfaktoros autentikáció alkalmazására. Mindeddig nem tisztázott, hogy a két vállalat mintegy 1,5 milliárd ügyfele közül pontosan mennyit érintett az eset. **Bővebben...**

## IT biztonsági Tanács

Az „Öt Szem” országok kiberbiztonsági szervei közös **jelentésükben** számba veszik a legnépszerűbb nyilvánosan elérhető hacking eszközöket, áttekintést adnak az általuk okozott fenyegetésről, valamint javaslatokat tesznek a hatékonyságuk korlátozására, illetve a detektálásukra. Elsőként a JBiFrost, egy távoli elérést biztosító trójai (RAT) kerül bemutatásra, amely a legtöbbször kéretlen levelek útján fertőz. Ennek a jelenlétére (is) utalhat, amennyiben például nem lehet csökkentett módban indítani a számítógépet; nem indul a Windows Registry Editor vagy a Task Manager; jelentősen megnő a lemezaktivitás és/vagy a hálózati forgalom; szokatlan nevű fájlok és könyvtárak jelennek meg. A védekezés alappillérei az adathalászat elleni intézkedés, az operációs rendszer naprakészen tartása, valamint a rendszeres víruskeresés.

## Új hacker csoportról ad hírt a Symantec

**(www.symantec.com)**

A Symantec által „Gallmaker” néven azonosított, eddig ismeretlen hacker csoport katonai és kormányzati célpontok ellen folytat kiberkémkedést ─ állítja a biztonsági cég új jelentésében. A csoport legalább 2017 decembere óta aktív, legutóbbi tevékenységét 2018 júniusában detektálták. A jelentés két konkrét kampányról tesz említést, eszerint a csoport egy ─ meg nem nevezett ─ kelet-európai ország külföldi nagykövetségei, valamint közel-keleti katonai szervezetek ellen folytatott támadásokat. A biztonsági cég szerint a kollektíva minden bizonnyal állami támogatással bír, azonban ezzel kapcsolatban nem közöltek konkrét információkat. **Bővebben...**

## Egyre több kétség merül fel a kínai kémchipekkel kapcsolatban, eközben a Bloomberg újabb történettel áll elő

**(www.theregister.co.uk)**

A Bloomberget rengeteg kritika érte a kínai kémchipről készült cikk miatt, nemrég pedig egy idézett biztonsági kutató is komoly kétségét fejezte ki azzal kapcsolatban, hogy megtörtént-e az állítások publikálás előtti megfelelő ellenőrzése ─ írja a The Register. Joe Fitzpatrick, a szóban forgó szakember többek közt kifogásolta, hogy az általa felvetett, pusztán elméleti támadási metódust a cikkben névtelen forrásoktól származó tényként kezelték. A hírügynökség azonban most egy új publikációban azt állítja, egy másik amerikai telekommunikációs nagyvállalat is felfedezett egy hasonló hardveres támadást. A történet főszereplője ezúttal is a Super Micro. **Bővebben...**

## Információs hadviselés az ausztrál védelmi erők fókuszában

**(www.csis.org)**

A washingtoni székhelyű CSIS (Center for Strategic and International Studies) think-tank legújabb tanulmányában az ausztrál hadsereg (Australian Defence Force - ADF) információs hadviseléssel kapcsolatos képességeit veszi górcső alá. Az Indiai- és Csendes óceán térségében zajló együttműködés részeként az információs hadviseléssel kapcsolatos képességek kifejlesztése is hangsúlyos szerepet kap, ennek külön jelentőséget is biztosítanak azok az információs hadviselésen alapuló események, amelyekre a térségben a közelmúltig nem volt példa. Mivel az „Öt Szem” (Five Eyes) szövetség két jelentős tagja (USA, Ausztrália) is jelen van az Indo – Pacific térségben, ezen képességek pontos megértése és hatékony alkalmazása egyformán fontos mindkét fél számára.

## Polgárjogi aktivisták a svájciak indokolatlan ellenőrzése ellen

**(heise.de)**

Svájci polgárjogi aktivisták a strasbourgi székhelyű Európai Emberi Jogi Bírósághoz kívánnak fordulni az ország állampolgárait érintő, indokolatlan adatkészletezés okán, amellyel összefüggésben a Nagy-Britanniában hasonló tartalommal megalkotott jogszabály ellen hozott strasbourgi ítéletre is hivatkoznak. A jogi problémát felvető civil szervezet 2014 óta harcol az anomáliát jelentő törvény ellen, amely a telekommunikációs szolgáltatásokat nyújtó társaságokat arra kötelezi, hogy átfogó forgalmi adatokat tároljanak, ideértve a mobiltelefonok helyinformációit, illetve a WLAN hálózatok bejelentkezési adatait. A svájci szövetségi bíróság a panaszt ugyan márciusban elutasította, azonban megjegyzendő, hogy a brüsszeli és strasbourgi európai bíróságokon közel két tucat hasonló ügy van folyamatban.