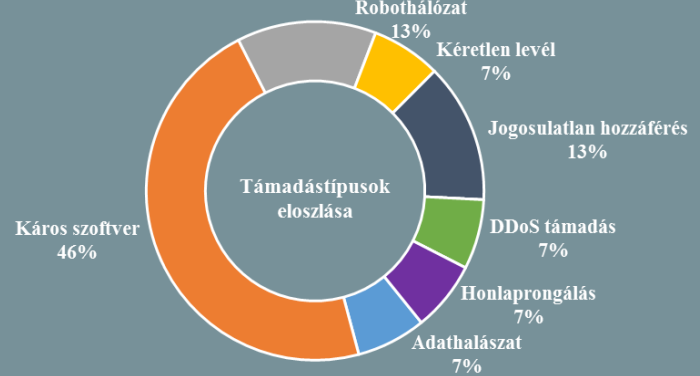


Az NKI által kezelt incidensekre  
vonatkozó statisztikai adatok:  
2018.06.22. - 2018.06.28.



Kövessen minket online az [itbiztonsag.govcert.hu](http://itbiztonsag.govcert.hu) oldalunkon, ahol naponta olvashatja legújabb híreinket!

## Az USA-ban ismét csökkentették a bűnüldöző szervek személyes adatokhoz való hozzáférési lehetőségeit

([www.bleepingcomputer.com](http://www.bleepingcomputer.com))

Számos kormányzati tisztviselő és adatvédelmi érdekképviseleti csoport üdvözölte az amerikai Legfelsőbb Bíróság (SCOTUS), a 2011-ben indult Carpenter kontra Egyesült Államok per kapcsán hozott múlt heti döntését, miszerint a bűnüldöző hatóságoknak bírői végzést kell szereznük, mielőtt a bűncselekmények elkövetésével gyanúsított személyek mobilkészleteikre vonatkozó információkat kérnének be a szolgáltatóktól, vagy más harmadik féltől. Az ítélet alapján az ilyen típusú adatokat inentől kezdve azonos szintű jogi védelem illeti meg, mint ami az eszközökön tárolt adatokat védi. John Roberts, a SCOTUS vezetőjének elmondása szerint a helyadatok hozzáférhetősége közel „tökéletes felügyeletet” tesz lehetővé, ami sérti az amerikai állampolgárok magánélethez való jogának védelmében hozott negyedik alkotmánymódosításban foglaltakat. **Bővebben...**

## Tovább kísért a WannaCry

([www.securityaffairs.co](http://www.securityaffairs.co))

Egy WannaCry témájú adathalász e-mail kampányról (WannaSpam) számolt be a SecurityAffairs hírportál, melynek során a magukat WannaCry-Hack-Teamnek nevező csoport arról próbálja meggyőzni az áldozatot, hogy számítógépük megfertőződött a WannaCry zsarolóvírussal, a fájlok törlése azonban elkerülhető a váltságdíj megtérítésével. Szakértők felhívják a figyelmet egy, a tárgy mezőben szereplő elírásra, amire felhasználói jelzések alapján lettek figyelmesek, és ami segíthet a spam kampány beazonosításában. Eszerint a támadók az angol „Attention” kifejezés helyett az „Attantion”-t használják. Akihez eljut a megtévesztő üzenet, nincs más dolga, mint figyelmen kívül hagyni azt, és törölni az e-mailt. Információk szerint szerencsére egyelőre csak néhányan váltak áldozataivá a WannaSpam kampánynak. **Bővebben...**

## Megjelent az új Wi-Fi szabvány

([www.securityweek.com](http://www.securityweek.com))

A Wi-Fi technológia gondozásáért felelős Wi-Fi Alliance hétfőn jelentette be a Wi-Fi Protected Access protokoll legújabb verziójának, azaz a WPA3-nak a megjelenését. Az új szabvány kétféle üzemmódot támogat, az egyik a WPA3-Personal, mely a próbálgatás-alapú (brute force) jelszótörő támadások ellen nyújt fokozott védelmet, abban az esetben is, ha a felhasználó kevésbé komplex jelszót választ. A másik pedig a WPA3-Enterprise, ami 192 bites titkosítást kínál a kiemelt biztonságot igénylő – például kormányzati – hálózatok számára. A cég emellett további két funkciót jelentett be, az Easy Connectet, mely lehető teszi a felhasználók számára, hogy egy QR-kód beolvasásával adjanak hozzá eszközöket a vezeték nélküli hálózathoz, valamint a Wi-Fi Enhanced Openet. **Bővebben...**

## Törvényt szegnek az EU egyes országai

([www.forbes.com](http://www.forbes.com))

A Privacy International, a Liberty és az Open Rights Group digitális jogvédő szervezetek több, mint 60 NGO-val, közösségi csoporttal és egyetemmel közösen több országban nyújtottak be panaszt az Európai Unióban működő tömeges megfigyelési gyakorlat megszüntetéséért. A szervezetek arra szólítják fel az EU-s kormányokat, hogy a kommunikációs vállalatoktól ne követeljék meg az ügyfelekre vonatkozó személyazonosításra alkalmas adatok (IP címek, helyadatok, stb.) tárolását, vagyis azt, amit az Európai Unió Bírósága (CJEU) már két alkalommal is jogellenes tevékenységnek ítélt. **Bővebben...**



## Komoly teljesítményjavulást hozott a Files Go frissítése

(www.zdnet.com)

A Google által kiadott frissítésnek köszönhetően új funkciókkal bővült a Files Go nevű népszerű androidos fájlkezelő alkalmazás, ami eredetileg az indiai felhasználók számára készült – segítségül a korlátozott tárhely kapacitás és a nem megfelelő hálózati lefedettség kezeléséhez – ám mára már globálisan mintegy 10 millió felhasználó telepítette. Az applikáció lehetőséget nyújt internet nélküli peer-to-peer fájlátvitelre egymáshoz fizikailag közel lévő eszközök között, valamint tárhely menedzselésre is alkalmas. A Google által közzétett adatok alapján jelentős a teljesítménybeli javulás, az eszközök közötti kapcsolat felépítés átlagosan 5 másodpercet vesz igénybe, a fájlátvitel pedig – hála az immár automatikusan kiválasztott leggyorsabb csatornának, amely között az 5GHz-es tartomány is szerepel. A fájlátvitel is lényegesen gyorsabb lett, a Google szerint egyes felhasználók 490Mbps-t is mértek, ami körülbelül 100 darab eredeti minőségű kép átvitelére alkalmas, kevesebb, mint 5 másodpercen belül. **Bővebben...**

## IT biztonsági Tanács



Továbbra is népszerűek az ún. „Dark Pattern” módszerek, azaz hogy egyes weboldalak manipulatív módon igyekeznek rávenni a felhasználókat bizonyos tevékenységekre (például adatmegosztásra, vagy vásárlásra), amit sok esetben a weboldal kialakításával érnek el. Ezek során cél lehet a felhasználó figyelmetlenségének, vagy türelmetlenségének a kihasználása zavaros fogalmazással, vagy például a biztonság szempontjából előnyös beállítási lehetőségek elrejtésével.

## Új projektbe fog az EFF, a biztonságosabb elektronikus levelezésért

(www.bleepingcomputer.com)

Az Electronic Frontier Foundation (EFF) bejelentett egy új projektet, amely a két évvel ezelőtt, a Mozillával és a Ciscóval közösen indított Let's Encrypt-hez hasonlóan szeretné a titkosítás bevezetését támogatni, a webszerverek után ezúttal az e-mail kiszolgáltatókra vonatkozóan. A kezdeményezés a STARTTLS helyes használatát állítja középpontba, ami lehetővé teszi, hogy e-mail továbbításakor SSL tanúsítványok használatával titkosított csatornán történjen a levéltovábbítás. A STARTTLS nem új technika, valójában a mai e-mail szerverek 89%-a már részben implementálta is, azonban az EFF szerint nem megfelelően. A tanúsítványok érvényességének ellenőrzése ugyanis többnyire elmarad, ennél fogva harmadik fél képes lehet közbeékelődni a kommunikációs csatornán, emellett egy tervezési hiba folytán arra is lehetőség van, hogy a támadó kikényszerítse a titkosítás elhagyását. **Bővebben...**

## Bűnösnek vallotta magát az oroszokról adatokat szivárogtató NSA-s

(www.cyberscoop.com)

Az NSA egy korábbi szerződéses partnerét, a 26 éves Reality Winner-t tavaly kémkedés vádjával vették őrizetbe. Most beismerő vallomást tett, így valószínűleg elkerülheti az első fokú ítéletben kiszabott 10 éves börtönbüntetést, és csupán 63 hónapot kell letöltenie, azonban jogerős ítélet még nem született az ügyben. Winner, aki korábban az amerikai légierőnél is dolgozott, az NSA-tól minősített anyagokat szivárogtatott ki a The Intercept egyik újságírójának, amik arra vonatkozóan tartalmaztak információkat, hogy Oroszországnak szándékában állt befolyásolni az amerikai elnökválasztást a választási rendszerek gyártói elleni zavarkeltő támadásokkal. Annak ellenére, hogy a szivárogtatás ráirányította a figyelmet egyes választási rendszerek sérülékenységeire, az igazságügy az esetet a kémkedési törvény (Espionage Act) hatálya alatt tárgyalja, amely megvonja annak lehetőségét, hogy az alperes a közérdek tájékoztatására hivatkozzon, sőt az eljárás során a vádlott egyáltalán nem fejtheti ki motivációit az esküdtszéknek. **Bővebben...**

## Az USA kiberdiplomáciai kapcsolatokat építene ki

(www.bleepingcomputer.com)

Az amerikai szenátus külügyi bizottsága szavazott a képviselőházhoz még januárban benyújtott kiberdiplomáciai törvényről (Cyber Diplomacy Act), ami új név alatt állítaná vissza a kiber ügyekkel foglalkozó kormányzati hivatalt és a kiberbiztonsági vezetői tisztséget is, amit Rex Tillerson volt külügyminiszter törölt el nemrégiben. Az Office of Cyberspace and the Digital Economy vezetője diplomáciai feladatokat lát majd el, nagyköveti státusszal fog rendelkezni, személyét pedig a szenátus beleegyezésével az elnök határozza meg. **Bővebben...**

## Bővítik a cseh hírszerzés lehetőségeit

(www.czech.cz)

A távozó cseh kormány a terrorizmus elleni harcra hivatkozva lépéseket tett a hírszerző hatóságok erejének növelése érdekében, ennek részeként lehetővé téve számukra egy új arcfelismerő rendszer kialakítását, és a bankszámla adatokhoz való hozzáférés biztosítását, utóbbival kapcsolatban azonban komoly adatvédelmi aggályok merültek fel. Alena Schillerová pénzügyminiszter a nagyobb lehetőségekhez mérten nagyobb felelősséget is vár a szolgáltatóktól, Andand Šandor biztonsági kutató – egyben az ország katonai hírszerzésének egykori munkatársa – azonban úgy véli, hogy a visszaélések kockázatát nem lehet teljes mértékben kizárni. **Bővebben...**