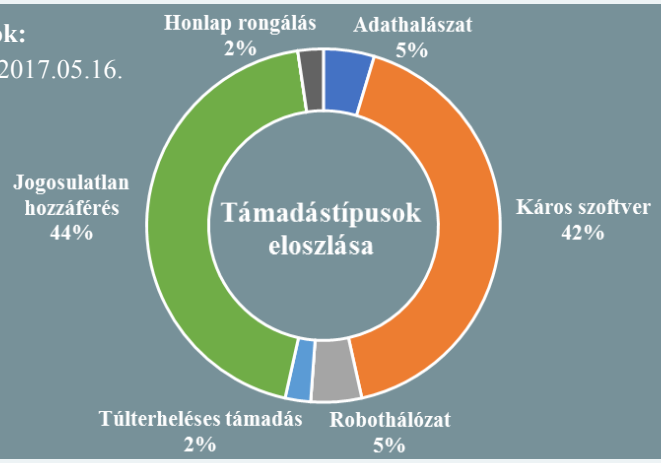
Incidens adatok:
2017.05.10 — 2017.05.16.



WannaCry támadás kormányzati hatása

(www.infosecurity-magazine.com)

A Nemzetközi Szakszervezeti Szövetség (ITUC) felszólította a kormányokat, hogy többet tegyenek az IT biztonság javítása érdekében. Sharan Burrow — az ITUC főtitkára — azt nyilatkozta, hogy a most hétvégén bekövetkezett WannaCry támadás kihangsúlyozta, hogy a kormányok nem tartják be a szigorú kiberbiztonsági normákat és nem fordítanak figyelmet a kritikus iparágakra. A héten Berlinben kerül megrendezésre a Labour 20, ahol megvitatják a globalizáció és a digitális világ munkavégzésére vonatkozó új szabályokat, melyeket majd Angela Merkel - német kancellár - terjeszt fel a júniusi hamburgi G20 csúcstalálkozón. **Bővebben...**

Együttműködés az orosz csalások ellen

(www.nationalcybersecurity.com)

Egyre több bizonyítékot tárnak fel a francia elnökválasztással kapcsolatban, miszerint a francia hálózatokba orosz hackerek hatoltak be. USA és Németország információcserét folytatnak a francia hatóságokkal, miközben egyre több magánkutató cég jut arra a következtetésre, hogy Oroszország beavatkozott a francia elnökválasztásba. Franciaország választási bizottsága szerint, a választással kapcsolatban jelentős mennyiségű adat, valamint hamis információ került ki egy közösségi oldalra. **Bővebben...**

Biztonságosabb jelszavak neurális hálózat segítségével

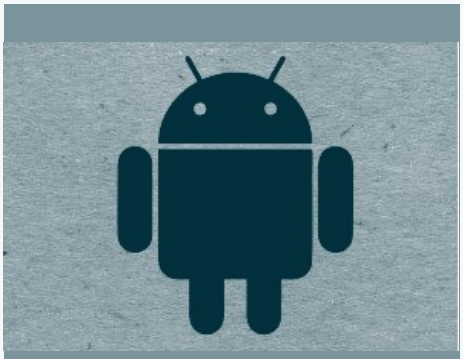
(www.nationalcybersecurity.com)

A Carnegie Mellon Egyetem és a Chicagói Egyetem kutatói a legkorszerűbb jelszómérőt kínálják a felhasználók számára, mely képes valós időben visszajelzéssel támogatni a jelszavak létrehozását. Egy neurális hálózat segítségével az összegyűjtött jelszavak alapján, a jelszómérő rendszer készít egy trendet, így a jelszó karaktereiről képes megállapítani, hogy a támadóknak mekkora kihívást jelent a begépelt jelszó kitalálása, és ennek függvényében különböző módszereket kínál a jelszavak erősebbé tételére. **Bővebben...**

Kockázatkezelésre összpontosít Amerika elnöke

(www.searchsecurity.techtarget.com)

A Trump adminisztráció késedelmei után csütörtökön aláírták az új kiberbiztonsági végrehajtó rendelet, mely egy új irányba tereli a kormányzati kiberbiztonságot. A parancs meghatározza, hogy az IT biztonságot teljes szervezeti szinten kell figyelembe venni, így a szervezeteknek 90 napon belül el kell készíteniük egy mindenre kiterjedő kockázatcsökkentő jelentést a Belbiztonsági Hivatal részére, majd a Menedzsment és Költségvetési Irodának 60 napon belül ki kell adnia az erre irányuló kockázatkezelési költségvetési követelményeket és a NIST Cybersecurity keretrendszer érvényesítéséhez szükséges szakpolitikai változtatásokat. **Bővebben...**



„Android For Work"

(www.techrepublic.com)

2017. június 5-től elérhetővé válik a Google Apps Eszközházirend v 7.55, ami lehetővé teszi az „Android For Work" profil használatát. A szervezetnek külön kritériumoknak kell megfelelnie (például a Google Mobile Management - GMM használata) az átálláshoz, azonban az új irányelvvel megoldható a magán és munkahelyi adatok elkülönítése, egy biztonságos környezetben. **Bővebben...**

IT biztonsági tanács

A zsarolóvírus (ransomware) egy kártékony szoftver, amely titkosítja a számítógépen és a mobil eszközökön található fájlokat, amiket váltságdíj ellenében visszaállítanak. Jellemzően fertőzött e-mailekkel terjed, csatolt tömörített állományokban található.

Egy esetleges fertőződés esetén a fertőzött gépet azonnal le kell választani a hálózatról, hogy a hálózat többi gépét ne fertőzhesse meg. Folyamatosan frissítsük biztonsági szoftvereinket és operációs rendszereinket. Készítsünk biztonsági mentéseket, hogy a támadás után vissza tudjuk állítani a fájlokat a legutóbbi mentett állapotra. Csak megbízható forrásból származó e-maileket és hivatkozásokat nyissunk meg.

Trump 2020-as kampánya

(www.cbsnews.com)

Múlt hét kedden jelentették be Donald Trump 2020-as elnökválasztási kampányának új weboldalát, melyen az oldal látógatóinak tartózkodási helyét és eszközeinek adatait gyűjtötték össze Bluetooth segítségével, egy új adatvédelmi irányelv szerint. A CBS News pár órával a felfedezés után felkereste Brad Parscale-t - az oldal webdesign-át készítő cég alapítóját- de addigra eltávolították a tartalmat az oldalról. **Bővebben...**

„A cél szentesíti az eszközt"

(www.techrepublic.com)

A Code 42 új felmérése szerint a biztonsági kockázatok ellenére a döntéshozó vezetők 75%-a használ nem engedélyezett alkalmazásokat, megszegve ezzel a biztonsági protokollokat. A felmérésben résztvevő vezetők elmondása alapján tisztában vannak viselkedésük biztonsági kockázataival, azonban ezt elfogadhatónak találják a termelékenység növelése érdekében. **Bővebben...**

Online csalókra figyelmeztetik a nyaralókat

(www.welivesecurity.com)

Az előző évhez képest közel 20%-kal nőtt azon nyaralók száma, akik online csalások áldozatává váltak. Az elmúlt 12 hónapban 6.000 gyanútlan utazótól közel 6,2 millió fontot loptak. A csalások között kiemelt szerepet kap a szálláshelyek megcélzása, ahol megtévesztő weboldalakkal támadnak, valamint a repülőjegy foglalási oldalak megcélzása, ahol hamis repülőjegyeket árusítanak. **Bővebben...**

Mi az oka a kibervédelem megjelenésének?

(www.nationalcybersecurity.com)

Az internetes világ kialakulása óta számos előnyét élvezhettük a kibertér adta lehetőségeknek, mint a fizikai határok leküzdése és az információk korlátlan elérése. Azonban ezek az előnyök vezettek egy teljesen új bűnözési forma kialakulásához a kiberbűnözéshez. A kiberbűnözés megjelenése óta, az internet által leküzdött akadályokat ellenük fordítva veszélybe kerültek személyes adataink és a magánéletünk, így indokolttá vált a megfelelő védelmi intézkedések, szabályzók és szabályok megalkotása, bevezetése. **Bővebben...**

FTC a hamis támadások ellen

(www.techrepublic.com)

Az Egyesült Államok kormányának független ügynöksége (Federal Trade Commission — FTC) nemrég jelentette be, hogy új lépéseket tesz a hamis biztonsági figyelmeztetések ellen. Együttműködve a szövetségi, állami és nemzetközi partnerekkel, igyekeznek visszaszorítani az ilyen jellegű támadásokat, hogy a felhasználók képesek legyenek a valódi kibertámadásokra reagálni. Ennek ellenére a fogyasztók védelme továbbra is nagy kihívást jelent, hiszen a Pew Research Center tanulmányai szerint az internethasználók fele nem képes továbbra sem azonosítani az adathalász e-maileket. **Bővebben...**