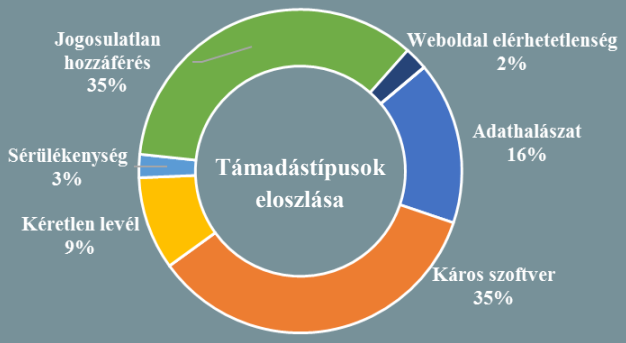
Incidens adatok: 2018.01.01. — 2018.01.11.



Digitális eszközök ellenőrzése határátlépéskor

(www.threatpost.com)

Az amerikai Vám- és Határőrség számára új szabályozás lépett életbe múlt hét pénteken, a határátkelőhelyeken történő digitális eszközök vizsgálatára vonatkozóan. A közzétett új irányelvek értelmében a határőrök továbbra is végezhetnek alapszintű átvizsgálásokat, ami maga után vonhatja a digitális eszközök fizikai ellenőrzését is, például a képek vagy üzenetek megtekintését. Emellett ésszerű gyanú esetén mélyebb szintű vizsgálatra is módjuk van, például eszközök teljes adattartalmának felülvizsgálatára, másolására és elemzésére. Amennyiben a határőrök nem képesek ellenőrizni az eszközön tárolt adatokat, mert azok kóddal, titkosítással vagy egyéb biztonsági eljárással védettek, felszólíthatják az utasokat jelszavaik megadására. Az együttműködés megtagadása esetén az őrök – legfeljebb öt napig – vissza is tarthatják a készüléket. **Bővebben...**

Az amerikaiak többsége még nem hallott a GDPR-ról

(www.helpnetsecurity.com)

Közeledik az Európai Unió általános adatvédelmi rendeletének (GDPR) hatálybalépésének ideje (2018. május 25.), ennek ellenére a MediaPro által végzett felmérés során megkérdezett amerikai alkalmazottak több mint fele ekkor hallott először a szabályzatról. A GDPR nem korlátozódik Európára, az előírásoknak minden cégnek meg kell felelnie világszerte, amennyiben uniós polgárok személyes adatait kezelik, ellenkező esetben igen magas pénzbírságra számíthatnak. A felmérés eredményeként kiderült, hogy nagy problémát jelent az alkalmazottak részéről tapasztalható – és különösen az érzékeny adatok kezelésére vonatkozó – tudatosság hiánya. Steve Conrad, a MediaPro ügyvezető igazgatója szerint ezért is szükséges a munkavállalók képzésére, az adatvédelmi ismeretek elmélyítésére nagyobb figyelmet fordítani. **Bővebben...**

Adatszivárgás egy amerikai kormányzati rendszerben

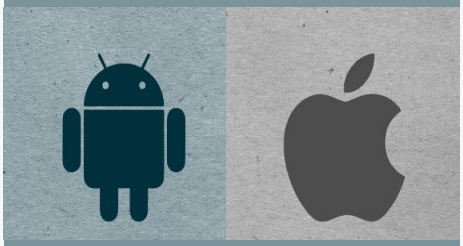
(www.zdnet.com)

Az amerikai Belbiztonsági Minisztérium (DHS) közleményben tudatta, hogy a Főfelügyelői Hivatal (OIG) Case Management Systeméből (CMS) mintegy 247 167, az OIG által folytatott eljárásokkal kapcsolatban rögzített, valamint a hivatal munkatársaira vonatkozó személyes adat vált illetéktelenül elérhetővé. Az esetre úgy derült fény, hogy 2017. május 10-én egy bűnügyi nyomozás során a CMS rendszer egy jogosulatlan másolatát fedezték fel egy korábbi dolgozónál. A DHS december közepén kiértesítette az összes lehetséges érintettet, amelyben kiemelték, hogy a kivizsgálás szerint az incidens nem külső támadás eredményeként és nem az érzékeny felhasználói adatok megszerzése céljából következett be. Az eset miatt az ígéretek szerint komolyabb biztonsági intézkedéseket tesznek. **Bővebben...**

Milyen újítások várhatók az új Wi-Fi szabványtól?

(www.bleepingcomputer.com)

A vezeték nélküli szabványok gondozásáért felelős szervezet (Wi-Fi Alliance) már be is jelentette a WPA3 protokoll néhány jellemzőjét. Négy jelentős újításról adtak most hírt: az első egy webes rendszerek által széles körben használt alapszintű funkció, ami a próbálgatás-alapú (brute force) jelszótörő támadások ellen nyújt védelmet azáltal, hogy néhány elhibázott bejelentkezési kísérlet után automatikusan bontja a kapcsolatot. A második újítás, hogy a saját kijelzővel nem rendelkező eszközök (pl. okos zárak) WPA3 beállításait akár okos telefonnal is menedzselhetjük. A harmadik és negyedik pedig a titkosítást érinti: előbbi gondoskodik róla, hogy minden egyes eszköz és a router vagy AP között titkosított legyen a kommunikáció, utóbbi pedig egy 192 bites titkosítási csomag, összhangban a Commercial National Security Algorithm (CNSA) ajánlással, amely további biztonsági garanciákat fog jelenteni. Már idén megjelenhetnek az első eszközök, amelyek támogatják a WPA3-at. **Bővebben...**



Nincs konszenzus az FBI és az Apple között

(www.arstechnica.com)

Az FBI nyomozói továbbra is nemtetszésüket fejezik ki az Apple, a telefonjai védelmével kapcsolatban tanúsított politikája miatt, a tech cég ugyanis igyekszik folyamatosan nehezíteni a tikosított adatokhoz való hozzáférésen, ami a nyomozóhatóság számára komoly gondokat okoz a bűnözők ellen folytatott vizsgálatok során. Stephen Flatley, az FBI forensic szakértője egy kiberbiztonság témájú konferencián elmondta, úgy véli a cég "ördögi praktikákat" alkalmazva szándékosan igyekszik megnehezíteni a hatóságok munkáját. Eszerint 2017 során mintegy 7 750 készülékhez képtelenek voltak hozzáférni technikai akadályok miatt, annak ellenére, hogy arra törvényi felhatalmazással rendelkeztek. Ugyanakkor pozitívan nyilatkozott a Cellebrite cégről, amely olyan technológiákkal foglalkozik, amelyek lehetővé tehetik az iPhone-okba való bejutást. **Bővebben...**

IT biztonsági Tanács

Erős jelszó megalkotásához több szempontot is érvényesítsünk: használhatunk egy számunkra könnyen megjegyezhető teljes mondatot, ám lehetőleg ne szó szerint vegyük át egy ismert műből.

Emellett tegyük nehezebben kitalálhatóvá speciális karakterek alkalmazásával.

Központi adatbázisba gyűjti Kína a kiberfenyegetési információkat

(www.cyberscoop.com)

2018 egy újabb kínai kiberbiztonsági törvénnyel kezdődik, ami jelentős hatással lehet a nagy amerikai technológiai cégekre. A "Public Internet Cybersecurity Threat Monitoring and Mitigation Measures" alapján előírják a kiberfenyegetésekkel kapcsolatos információk jelentését mindazon vállalkozások számára, amelyek Kínában üzleti tevékenységet folytatnak. Nem csupán az adott vállalatot ért fenyegetésekről kell beszámolniuk, hanem minden, a tudomásukra jutott releváns információt át kell adniuk a Ministry of Industry and Information Technology (MIIT) számára, amelynek elmulasztása komoly retorziót vonhat maga után. Az ilyen módon begyűjtött információk egy nemzeti adatközpontban kerülnek eltárolásra, amelyet részben a kínai hálózatbiztonsági vészhelyzeteket elhárító csoport (CN-CERT) kezel. A szabályzásban érintett vállalkozások köre igen széles, vonatkozik az internet szolgáltatókra, telekommunikációs cégekre, valamint az egyéb internetes vállalatokra is, mint a Facebook, az Apple, a Microsoft, vagy a Google. **Bővebben...**

Életbe lépett az online gyűlöletbeszéd elleni német törvény (NetzDG

(www.engadget.com)

A mai naptól kezdve Németország pénzbírsággal sújtja majd azon közösségi platformokat, amelyek nem távolítják el a gyűlöletkeltő témájú tartalmakat 24 órán – vagy az ún. "összetett eseteket" tekintve 7 napon – belül. Eddig nem lehetett tudni, hogy a tech cégek megfelelnek-e a jogszabályban előírtaknak, mivel a törvény ugyan 2017 októberében hatályba lépett, azonban a tavalyi év végéig még tartott a türelmi idő. A kiszabható büntetés mértéke akár az 50 millió eurót is elérheti. **Bővebben...**

2017-es kibertámadások az Egyesült királyság vállalatai ellen

(www.infosecurity-magazine.com)

A Beaming internetszolgáltató adatai alapján az előző évben több százezer kibertámadás érte az Egyesült Királyság vállalatait, melyek javarészt az internetre csatlakoztatott eszközök ellen irányultak. A szolgáltató több ezer, ügyfeleit ért támadást elemzett valós időben. Az eredmények szerint a vállalati hálózatokba történő bejutásra naponta átlagosan 633 kísérletet tettek, mindez egy évre vetítve 231 028 próbálkozást jelent, ami nagyjából megegyezik a 2016-os adatokkal. Kiderült, hogy a támadások körülbelül 70%-os arányban olyan célpontok ellen irányultak, mint a hálózati biztonsági kamerák, valamint egyéb IoT eszközök. Sonia Blizzard, a Beaming ügyvezető igazgatója szerint a tavalyi év volt az eddigi legrosszabb, az Egyesült Királyság szervezeteit célzó számítógépes fenyegetések szempontjából. Blizzard a kockázatok csökkentése érdekében javasolja a határvédelmi eszközök időszakos felülvizsgálatát, anomália alapú detektálás alkalmazását és a személyes e-mail fiókok, valamint a fájlmegosztó alkalmazások hozzáférhetőségének korlátozását. **Bővebben...**

Kiberközpontot állított fel Vietnám

(www.reuters.com)

Az ázsiai ország egy 10 000 főt számláló kibervédelmi katonai egységet hozott létre. Egy magas rangú vietnámi katonai tisztviselő szerint a 'Force 47' elnevezésű központ már működésbe is lépett és elsődleges feladata a kommunista rezsim által károsnak minősített tartalmak visszaszorítása. Az intézkedés előzményének tekinthető az augusztusi közlemény, mely szerint a jövőben nagyobb hangsúlyt fektetnek az online platformok ellenőrzésére. Emellett egy olyan törvénytervezet kidolgozását is megkezdték, amely – kínai mintára – előírná az online platformok (pl: Facebook, Google) számára az állampolgárok adatait tároló szerverek, az országhatárokon belül való elhelyezését. Az elképzelés azonban olyan komoly vitákat váltott ki, hogy emiatt a nemzetgyűlés még nem hagyta jóvá. Az ellenzéki véleményekkel szemben való szigorú fellépésre jellemző példa, hogy múlt hónapban a bíróság 10 év szabadságvesztésre ítélt egy népszerű bloggert. **Bővebben...**