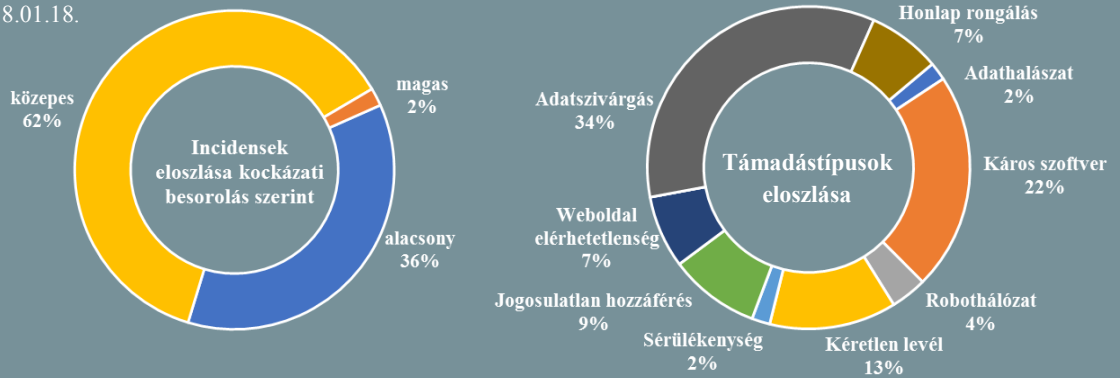


Incidens adatok: 2018.12. — 2018.01.18.



Kövessen minket online az itbiztonsag.govcert.hu oldalunkon, ahol naponta olvashatja legújabb híreinket!

Három milliárd feltört felhasználói fiók a neten

(www.securityweek.com)

Jordan Evan Bloom, egy kanadai férfi azért áll bíróság elé, mert olyan weboldalt üzemeltetett (leakedsource.com), amelyen érzékeny személyes információkat, többek között e-mail címeket és jelszavakat tárolt és árult. Ezek a – közel 3 milliárd felhasználói fiókra vonatkozó – személyes adatok más nagy adatszivárgási incidensekből (pl.: LinkedIn, Ashley Madison) származtak, amelyeket felhasználva a vád szerint mintegy 247 000 kanadai dollár (~50 millió forint) haszonra tett szert. A hatóságok felhívták arra a figyelmet, hogy a korábbi szivárgásokból származó felhasználói adatok továbbra is használhatók lehetnek, amennyiben a szivárgásban érintett felhasználó ugyanazt a felhasználónév és jelszó párost használta más oldalakon is. Az akció nemzetközi összefogással, a holland rendőrség és az FBI közreműködésével zajlott. **Bővebben...**

Átstrukturálási törekvések az ausztrál kiberbiztonsági szervek között

(www.zdnet.com)

Az ausztrál kiberbiztonsági kutatóközpont (CSRC) egy olyan, országos hatáskörrel bíró ügynökség létrehozását kezdeményezte, ami kiegészítené a meglévő kiberbiztonsági feladattal bíró állami szervezetek tevékenységét. „Ausztrália kiber fenyegetettség elhárító képessége és a hatóságok bűnüldöző tevékenységének informatikai támogatása viszonylag gyenge, koordinálatlan és szétszórt” – állítják a tanulmány szerzői. Úgy vélik, a kiberbűnözés elleni harc akkor lesz a legsikeresebb, ha a nyomozati támogató tevékenységek, illetve a kiaknázható IT-biztonsági képességek és a technikai feltételek nemzeti szinten egy intézménynél kerülnek összefogásra és koordinálásra. Ezzel párhuzamosan az Ausztrál Értékpapír és Befektetési Bizottság (ASIC) benyújtott egy törvénymódosítási javaslatot, amelyben a szervezetet nyomozati hatósággá szeretnék minősíteni, egyúttal felhatalmazást kérnek telekommunikációs csatornáknak, a súlyos bűncselekmények utáni nyomozások érdekében történő lehallgatásához, valamint a megszerzett információk külföldi ügynökségekkel történő megosztásához. **Bővebben...**

Így látta az ENISA a tavalyi évet kiberbiztonsági szempontból

(www.enisa.europa.eu)

Az Európai Unió Hálózat- és Információbiztonsági Ügynökség (ENISA) elkészítette a 2017-es év kibereeményeinek értékelését, amely a fenyegetéseken és a kockázatokon kívül a kibertámadások elleni küzdelem eredményeit is összesíti, kiemelve például a bűnüldöző szervek és a kormányok "Darkweb" elleni fellépését. A beszámolóban kiberbűnözői bevételforrásokkal, kibertámadásokkal és a fenyegető csoportok, valamint a támadásokra felhasznált infrastruktúrák változásával is foglalkoznak. Az ENISA idén célul tűzte ki, hogy – az immár hatodik alkalommal – elkészülő éves jelentése ezúttal olvasmányosabb legyen, ne kizárólag az iparág szakemberei számára legyen értelmezhető. Emellett elindították az etl.enisa.europa.eu címen elérhető weboldalt, amelyen 2017 legkiemeltebb internetes fenyegetéseiről, trendjeiről, valamint ezek figyelembevételével javasolt szabályozási, üzleti, oktatási és kutatási ajánlásokról található információ az ENISA/EU döntéshozók számára. **Bővebben...**





Fókuszban a weboldalak betöltési sebessége mobilon

(www.gadgets.ndtv.com)

A Google szerdán jelentette be, hogy a felhasználói élmény javításának érdekében mobil keresések esetén változást eszközöl a weboldal rangsorolási algoritmusán, miszerint nagyobb hangsúllyal fogja figyelembe venni a weboldalak betöltési sebességét. A 2018 júliusától induló „Speed Update” után a tervek szerint hátrébb fogja rangsorolni azokat a weboldalakat, amelyek lassan töltődnek. A tech óriás azonban egy blog bejegyzésben igyekezett leszögezni, hogy ez csak a „leglassabb élményt nyújtó” weboldalakra lesz hatással, és figyelembe fogják venni az oldal tartalmának relevanciáját, ami emelhet a rangsoron. A cég olyan eszközöket is elérhetővé tett a web fejlesztők számára, amikkel egyszerűen megvizsgálhatják weboldalaikat, hogy azokat hátrányosan érinti-e az új irányelv. **Bővebben...**

IT biztonsági Tanács



A PUA/PUP szoftverek (potenciálisan **nemkívánatos alkalmazások**) gyakran az ingyenesen letölthető programokkal együtt települnek a számítógépekre, a felhasználók tudta nélkül.

Érdeemes minden program letöltés esetén **ellenőrizni a speciális beállításokat és jogosultságokat**, hogy kizárólag a valóban letölteni kívánt szoftvert telepítsük.

Hogy áll az Európai Unió az ICT termékek biztonságával?

(www.enisa.europa.eu)



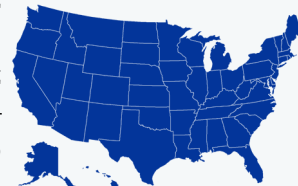
Az ENISA új tanulmányában az uniós tagállamok infokommunikációs technológiai (ICT) termékek esetében alkalmazott biztonsági minősítési eljárásait vizsgálta, összehasonlítva azokat egyes EU-n kívüli országok gyakorlataival. Az ügynökség vezetője szerint az elemzés fontos jellegzetességeket tárt fel, amelyek hozzájárulhatnak egy egységes, európai szintű keretrendszer megalkotásához.

Minderre egyre nagyobb az igény, ugyanis a technológiai piac ugrásszerű bővülése miatt a biztonság terén sok egyenlőtlenség tapasztalható, a tagállamok egyéni szabályozási kezdeményezései pedig csak tovább növelik a töredezettséget. A tanulmány arra a megállapításra jut, hogy a tanúsítvány kibocsátó szervezetek üzleti és jogi szempontból az adott tagországhoz igazodnak és az adott régió szabályozási jellegzetességeit tükrözik. **Bővebben...**

Több USA-beli állam sem nyugszik bele a netsemlegesség eltörlésébe

(www.arstechnica.com)

21 szövetségi állam peres úton kívánja rávenni a Szövetségi Kommunikációs Bizottságot (FCC) a netsemlegesség visszaállítására. "Az FCC döntésének eltörléséhez első lépésként egy felülvizsgálati kérelmet nyújtunk be, ami lehetővé teszi majd az államok legfőbb ügyészeinek, hogy fellebbezzenek." – nyilatkozta Washington állam legfőbb ügyésze, Bob Ferguson. Az FCC december 14-én határozott a netsemlegességet biztosító előírások felszámolásáról, amelyek addig garantálták, hogy az internetszolgáltatók nem prioritizálhatják, blokkolhatják, vagy éppen gyorsíthatják a tartalomszolgáltatók és a felhasználók közti adatfolyamot. Az indítvány szerint a határozat több szövetségi törvénnyel is ellentétes, például az 1934-es kommunikációs törvény (Communications Act), Ferguson szerint emellett kárt okoz az ügyfeleknek és a kisebb cégeknek, valamint visszaveti az innovációt. **Bővebben...**



Még zajlik a Brexit kapcsán feltételezett orosz befolyás kivizsgálása

(www.forbes.com)



A Facebook beleegyezett, hogy mélyrehatóbb vizsgálatot indítson arra vonatkozóan, hogy Oroszország befolyásolta-e az Egyesült Királyság Európai Uniói tagságáról szóló népszavazást, miután a Digitális, Média- és Sport Bizottság bírálta a vállalat eddig meghozott intézkedéseit.

Eszerint a tech óriás szigorú ellenőrzés alá vonja azokat a felhasználói fiókokat, melyekről feltételezhető, hogy hamis hírek terjesztésében vehettek részt. A londoni City Egyetem kutatói ugyanis mintegy 13 500 olyan felhasználói fiókot azonosítottak, amelyekkel a népszavazást megelőzően Brexit-párti üzeneteket tettek közzé, azonban röviddel a népszavazást követően nyomtalanul eltűntek. A kérdéses fiókok közül számos a szentpétervári Internet Research Agency-hez (IRA) köthető, amelyről már korábban ismertté vált, hogy szerepe volt az amerikai választás idején álhíreket terjesztő accountok létrehozásában. Simon Milner, a Facebook területileg illetékes szabályozásért felelős igazgatója a bizottságnak küldött válaszlevelében időt kér a vizsgálathoz, ám ígérete szerint eközben ki is terjesztik azt, hogy további, Brexittel kapcsolatos üzeneteket ellenőrizzenek.

Bővebben...