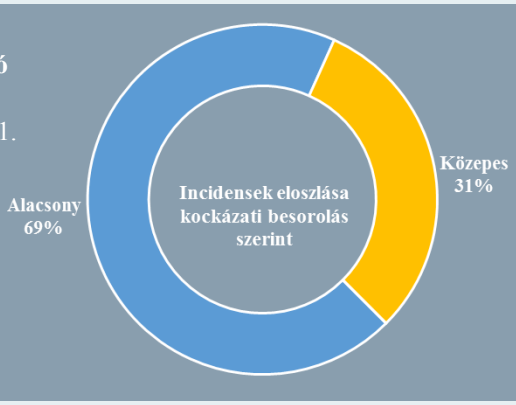
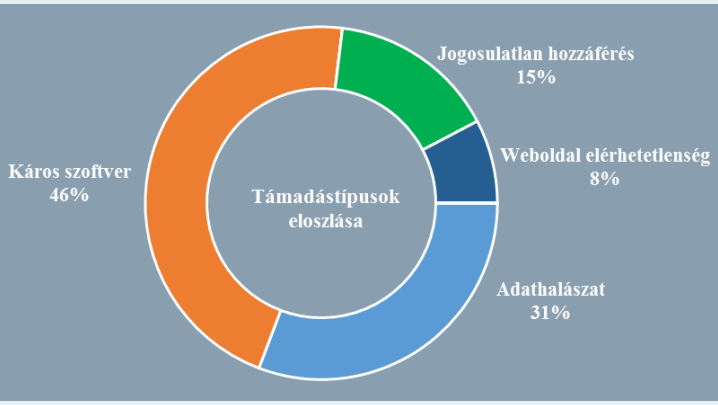
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

2018. 44. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.10.26. - 2018.10.31.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon!

A hivatalos vizsgálat szerint is a brit kémszolgálathoz köthető a Belgacom elleni hackertámadás

(www.securityaffairs.co)

A De Standaard nevű belga újság részleteket közölt Belgium legnagyobb távközlési szolgáltatója, a Proximus (korábbi nevén Belgacom) ellen 2013-ban elkövetett hackertámadás kivizsgálásával kapcsolatban, amely során bizonyítékokat találtak a GCHQ brit titkosszolgálat érintettségére. A cég infrastruktúrája malware (Regin) támadás áldozatává vált, amelyről már korábban gyanították, hogy összefüggésben állhat a Five Eyes országok állami támogatású kémtevékenységével, az Edward Snowden által kiszivárogtatott NSA dokumentumokban pedig ennél is konkrétabban az Egyesült Királyság került megnevezésre. **Bővebben...**

Mesterséges intelligencia alapú bűnüldözés Spanyolországban

(www.zdnet.com)

Spanyolországban bevezettek egy, a Cardiff Egyetem és a Madridi III. Károly Egyetem kutatói által fejlesztett, VeriPol nevű mesterséges intelligencia (MI) alapú rendszert, amely a bűnüldöző hatóságok számára segítséget nyújthat a hamis bejelentések kiszűréséhez. **Bővebben...**

Több ügyfelet érintett a British Airways adatszivárgási incidense, mint korábban gondolták

(www.securityaffairs.co)

A RiskIQ végezte az idén szeptemberében nyilvánosságra került, British Airways-t ért adatszivárgás incidens kivizsgálását, amely szerint a támadással gyanúsított MageCart-bűnszervezet a kezdeti feltevésekhez képest lényegesen több ─ mintegy 185 000 ─ ügyfél személyes adataihoz és kártyainformációihoz fért hozzá. **Bővebben...**

IT biztonsági Tanács

A Symantec legutóbbi **blog posztjában** azzal foglalkozik, hogy hogyan ismerhetjük fel az automatizált közösségi média fiókokat a Twitteren. Ehhez a legszembeötlőbb karakterisztikák számbavétele mellet ─ mint például, hogy a fiókok nevében sokszor szám található, vagy hogy többnyire csupán retweetelik a tartalmakat saját posztok helyett ─ néhány szoftveres segítséget is bemutat. Ilyenek a **Botometer** webes alkalmazás, a **Botcheck.me** Chrome kiegészítő, valamint a **Tweetbotornot** R package.

A Signal az üzenetek feladóit is titkosítja

(www.wired.com)

A biztonsági szempontból piacvezető csevegő alkalmazás, a Signal nyilvánosságra hozta legújabb fejlesztését, miszerint a jövőben nem csupán az üzenetek kerülnek titkosításra, hanem a feladók személye is rejtve marad. Mindez azért fontos, mert bár a rendszer nem logolja a hálózatán történő tevékenységeket, a feladó és a címzett alapján is tehetők megállapítások a platform használatára vonatkozóan. **Bővebben...**

Ezek a kártevők okozták a legtöbb gondot idén

(www.helpnetsecurity.com)

A Webroot összefoglalta azon kártevőket, amelyek a 2018-as eddigi adatok alapján a legnagyobb fenyegetést jelentették a szervezetek és felhasználók számára. Három fő kategória alapján állították össze a listát: botnetek és banki trójaiak, kriptovaluta bányász programok, valamint zsarolóvírusok. **Bővebben…**

Újabb kutatás demonstrálja a kritikus rendszerek sérülékenységét

(www.trendmicro.com)

A Trend Micro legújabb kutatása a víz- és energiaellátást biztosító rendszerek kibertámadásokkal szembeni kitettsége kapcsán jutott riasztó eredményre. A vizsgálatokból készült jelentés ugyanis rávilágít arra, hogy a nevezett területek informatikai rendszerei mennyire könnyen deríthetők fel és használhatók ki nyíltan hozzáférhető, alapfokú eszközök és technikák segítségével. **Bővebben...**