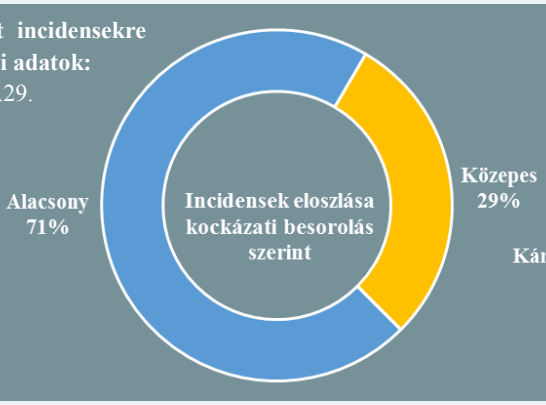
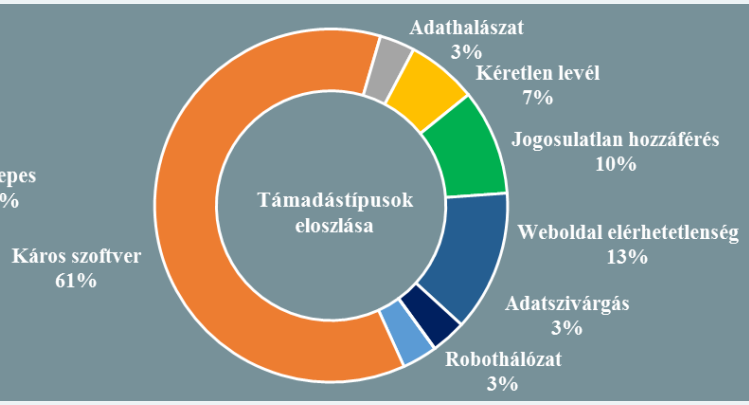
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

2018. 48. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.11.23. - 2018.11.29.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon!

Adatvédelmi konferencia Németországban: a bürokrácia és az elszántság között

(heise.de)

A GDPR átültetése Németországban is akadozik, amelynek egyik oka ─ ahogy arra a szakértők rámutatnak ─ hogy a gazdasági vonzatok még mindig túl erős szerepet játszanak ebben a folyamatban. A problémák megoldására több javaslat is elhangzott egy kölni adatvédelmi konferencián (DAFTA), ahol hangsúlyozásra került, hogy számos téves társadalmi feltételezés, bizonytalanság is gátolja a norma realizálását, ezért az állami szervek részéről továbbra is felvilágosító, tudatosító tevékenységre van szükség. Május 25-e óta nemzeti szinten 185 000, EU-szinten pedig 45 500 adatvédelmi panasz benyújtására került sor az állampolgárok részéről, ami azt mutatja, hogy a panaszjogot nagyon komolyan veszik az érintettek, amely pozitívum. Ugyanakkor negatívumként említhető a hatóságok oldalán tapasztalható, országonként eltérő joggyakorlat és jogértelmezés, amelyet egyes cégek ki is használnak a normák kikerülésére. Ezt a hiányosságot mindenképpen orvosolni kellene a szakértők szerint egy egységes iránymutatással, azonban erre kevés esélyt látnak egyelőre a jövő évi Európai Parlamenti választásokig bezárólag, ami azt jelenti egyúttal, hogy a szóban forgó helyzet 2020-ig valószínűleg megmarad EU-szinten; és ugyanez elmondható a németországi belső helyzetre, mivel a nemzeti jogharmonizációs folyamatok is igen lassan haladnak.

Bizalmas Facebookos dokumentumok kerültek a brit parlament birtokába

(securityweek.com)

A brit parlament Digitális, Kulturális, Média- és Sportbizottsága bizalmas Facebookos dokumentumokat szerzett meg egy már megszűnt fotó kereső alkalmazás (Pikinis) fejlesztőjétől, a bizottság elnöke szerint pedig a hatályos brit jogszabályok értelmében nyilvánosságra is hozhatják azok tartalmát. A kérdés azonban jogi szempontból összetett, ugyanis ─ amint arra Richard Allan, a héten esedékes, dezinformációs témájú nemzetközi meghallgatásra beidézett Facebook vezető felhívta a figyelmet ─ a tech óriás szándékát, miszerint a kérdéses anyagokat titokban tartaná, egy kaliforniai bíróság korábban jóváhagyta. A szóban forgó, 2013/14-ből származó dokumentumokhoz az alkalmazásfejlesztő cég ─ Six4Three ─ egy 2015-ös policy változtatás miatt indított peres eljárás során fért hozzá. A The Observer brit hetilap szerint a bizottság kétszer is felszólította a Six4Three vezetőjét, Theodore Kramert a dokumentumok átadására, valamint egy londoni üzleti útja során a parlament elé is idézték.

Komoly vitákat gerjeszt a thai kormány törvényjavaslata

(www.securityweek.com)

Egy thaiföldi kiberbiztonsági törvényjavaslat felhatalmazást adna a kormányzatnak, hogy magánszemélyek és vállalatok számítógépes eszközeit bírói végzés nélkül foglalja le alapos gyanú, vagy „vészhelyzet” esetén. A tevékenység egy új testület irányítása alatt állna, melynek vezetője a katonai junta feje, Prayuth Chan-O -Cha lenne. Az IT-biztonsági szakma részéről komoly kritikával illetett javaslatot még az év végéig az ország nemzetgyűlése elé kell tárni, amennyiben a kormányzat azt még a jövő év elején esedékes választásokig el szeretné fogadtatni, ugyanakkor a digitális ügyekért felelős miniszter, Pichet Durongkaveroj szerint a részletek jelenleg még kidolgozás alatt állnak. A miniszter ─ igyekezvén csillapítani a lehetséges túlkapások miatti felháborodást ─ kiemelte azt is, hogy a rendkívüli állapoton kívül érvényes lenne a megkötés, hogy bírói végzés szükséges a lefoglalásokhoz. **Bővebben...**

Új-Zéland is kizárja a Huawei-t az 5G hálózat kiépítéséből

(securityweek.com)

A GCSB (Government Communications Security Bureau), Új-Zéland egyik ─ többek között hálózatbiztonsági feladatokat is ellátó ─ hírszerzési ügynöksége bejelentette, hogy megtiltja a Spark New Zealand mobil telekommmunikációs cég számára, hogy az 5G-s fejlesztések során Huawei eszközöket használjon, arra hivatkozva, hogy ez „jelentős biztonsági kockázattal" járna. Annak ellenére született meg a tiltás, hogy a két cég között már történt e téren együttműködés, sőt márciusban be is mutattak egy 5G-s teszthálózatot. Az eset ráadásul diplomáciai szempontból is összetett, hiszen bár Új-Zéland az „Öt Szem" szövetség tagja, legnagyobb kereskedelmi partnere Kína. A Spark csalódottságát fejezte ki a döntéssel kapcsolatban. **Bővebben...**

IT biztonsági Tanács

Az EUROPOL „Don't F***(ake) Up" című **tudatosító kampányával** segítséget szeretne nyújtani a hamis termékeket forgalmazó weboldalak felismeréséhez. Többek közt árulkodó lehet, ha az árak irreálisan alacsonyak; a „Rólunk" és „Kapcsolati" adatok alatt elégtelen információ szerepel; nyelvtani hibákkal találkozunk; a kérdéses weboldal domainjében, a cég, vagy a termék megnevezésében olyan szavak szerepelnek, mint például „genuine/valódi", „original/eredeti", „offer/ajánlat", „discount/árengedmény". Gyanús továbbá, ha rossz minőségű, nehezen kivehető, vagy csak kis méretű képeket tartalmaz az oldal; de mindenek előtt a garanciális és szerződési feltételek, valamint az adatvédelmi szabályzat hiánya.

Blokklánc-alapú szavazórendszert vezethet be Dél-Korea

(zdnet.com)

A dél-koreai technológiai minisztérium (MSIP) az ország választási bizottságával (NEC) karöltve bejelentette, hogy egy blokklánc technológián alapuló, online szavazórendszer fejlesztését tervezik megkezdeni, még idén decemberben. A NEC 2013-ban már lehetővé tette az online szavazást (K-voting), ám ezzel kapcsolatban biztonsági aggályok merültek fel, a kormányzat szerint azonban az új rendszer a technológiából fakadóan már átláthatóbb és biztonságosabb lesz. **Bővebben...**

Sikerült felszámolni egy rendkívül kiterjedt csaló reklám kampányt

(bleepingcomputer.com)

Több tízmillió dollár értékű kárt okozott már az „3ve" néven azonosított online csaló reklám kampány, amelyet amerikai hatóságok, valamint tech vállalatok közös erőfeszítésével sikerült csak felszámolni. A kampány során a csalók hamis online reklám felületek generálását és értékesítését végezték egy összetett infrastruktúra segítségével, ami a csúcsidőszakában legalább 700 000 fertőzést kezelt, mintegy 60 000 fiók és 10 000 weboldal felett gyakorolt irányítást, így összesen több, mint 1 millió IP cím tartozott hozzá. Az akcióban a nagyobb tech vállalatok ─ mint a Google, vagy a Microsoft ─ mellett több kiberbiztonsági cég is részt vállalt, például az ESET, a Symantec, a Trend Micro, vagy az F-Secure.

Az Akamai figyelmeztet: támadási kampány zajlik routerek ellen

(www.arstechnica.com)

Az Akamai „EternalSilence" néven azonosítja a nemrég felfedezett malware kampányt, amely otthoni és SOHO routereket céloz. Az alkalmazott technika (UPnProxy) április óta ismert: a támadók az UPnP szolgáltatások sérülékenységeit használják ki, amelyek segítségével kompromittálják az eszközök NAT tábláit, hogy eltereljék a webes forgalmat, valamint ─ egy új funkcióként ─ hogy megnyissák az alapértelmezett SMB portokat (TCP 139, 445), utat biztosítva a belső hálózat felé. Az Akamai szerint körülbelül 277 000 sérülékeny UPnP implementációt alkalmazó hálózati berendezés érhető el az interneten, ebből pedig már körülbelül 45 ezer fertőzött is. **Bővebben...**

Több tízezer feketekereskedelemmel kapcsolatba hozható domaint szüntettek meg

(europol.europa.eu)

Az IOS (In Our Sites) nevű ─ immár kilencedik alkalommal ─ megindított nemzetközi bűnüldözési művelet jelentős eredménnyel zárult, ugyanis mintegy 33 654, illegális termékek forgalmazására használt domain felett sikerült felügyeletet nyerni ─ adja hírül az Europol. A domainek mellett a hatóságok letartóztattak 12 gyanúsítottat, eszközöket foglaltak le, valamint több mint 1 millió euró értékben zároltattak bankszámlákat és egyéb online fizetési platformokon létesített fiókokat. Az akciót tudatosító kampány is támogatja (Don't F***(ake) Up), amely az uniós állampolgárok figyelmét szeretné felhívni az illegális termékek online vásárlásának kockázataira, emellett tanácsokkal is szolgál a hamis termékeket áruló oldalak felismeréséhez.