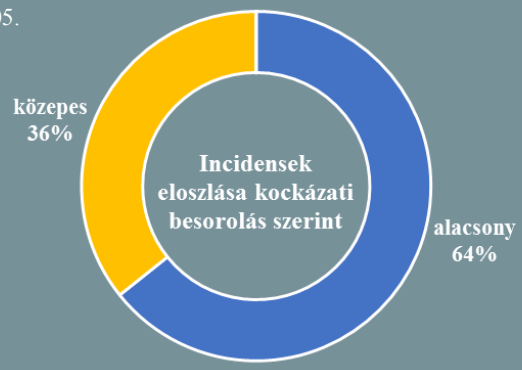
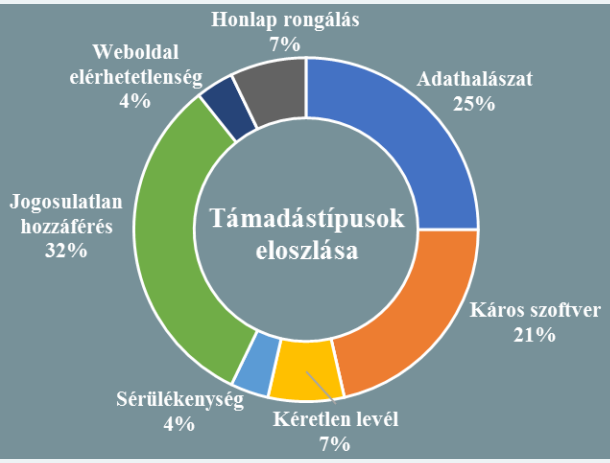
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

2017. 35. hét

Incidens adatok:
2017.08.30. — 2017.09.05.





Riasztó kép egyes európai kritikus rendszerek védelmi állapotáról

(www.theregister.co.uk)

A Egyesült Királyság kritikus infrastruktúráinak több mint egyharmada nem felel meg a kormányzat által állított követelményeknek, derült ki a Coreo Network Security közérdekű adatigénylése (FOI) során. A kérelmeket még 2017 márciusában juttatták el több, mint 338 szervezet számára, beleértve életmentő szolgálatokat, rendőrségeket, energia szolgáltatókat és szállítással foglalkozó szervezeteket is. A válaszadók közel fele (39%) vallotta be, hogy nem végezte el a védelmi javaslatokat tartalmazó "10 lépéses programot". A kormányzat javaslata szerint – amely az EU-s NIS irányelvek implementálására született – egy incidens esetén a kritikus rendszerekért felelős szervezetek komoly bírságra számíthatnak, amelynek mértéke a 17 millió eurót, vagy akár a teljes forgalmuk 4%-át is elérheti. **Bővebben...**

Az új kínai kiberbiztonsági törvény egy másik aspektusa

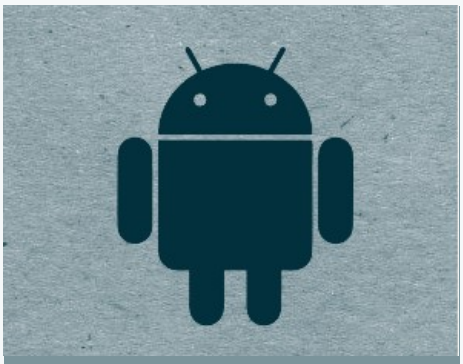
(www.securityaffairs.co)

A törvény lehetőséget teremt a kínai kormányzat számára, hogy az ország területén működő tech cégek szoftvereinek programkódját vagy bármilyen intellektuális tulajdonát elemezzék. A feladatért a Kínai Informatikai Értékelő Központ (CNITSEC) lesz felelős, amely a kínai Állami Biztonsági Minisztérium (MSS) irányítása alatt áll és az egyik feladata sérülékenységvizsgálatok végzése, amelyek eredményeit – egyes információk szerint – hírszerzési műveletek során is hasznosítják. A Recorded Future nevű fenyegetettség felderítő vállalat szerint nagy az esély rá, hogy az új védelmi célú elemzéseket ugyanígy támadó célra is fel fogják használni. Ennek figyelembevételével – a komoly gazdasági motiváló erővel szemben – az érintett cégeknek figyelembe kell venniük a saját hálózattal és szolgáltatásaikkal, valamint a felhasználókkal, ügyfeleikkel kapcsolatban felmerülő kockázatokat. **Bővebben...**

Kibertámadás érte a német kormánypártot

(www.ibtimes.co.uk)

Informatikai támadás érte az Angela Merkel-féle német Kereszténydemokrata párt (CDU) alelnökének weboldalát - közölte az érintett, Julia Kloeckner. Az eddigi vizsgálatok szerint a több ezer illetéktelen hozzáférési kísérlet nagy része orosz IP címekről érkezett. Információk szerint a támadás Angela Merkel és a szociáldemokrata Martin Schultz televíziós vitája előtt zajlott. A BSI szóvivőjének az üggyel kapcsolatos nyilatkozata szerint tudatában voltak a támadásnak és emiatt kapcsolatba is léptek a CDU központjával. A közelgő választások miatt német hírszerző ügynökségek már korábban figyelmeztetést adtak ki, miszerint Oroszország vélhetően megpróbálja befolyásolni a választás eredményét, ahogyan azt tette az Egyesült Államok, majd Franciaország esetében is. **Bővebben...**



Androidos alkalmazásokat használtak támadásra

(www.securityaffairs.co)

A múlt hét során közel 300 Androidos alkalmazást távolítottak el a Google Play Store-ból, miután ismertté vált, hogy azokat vélhetően DDoS támadáshoz használták fel. Az ESET IT biztonsági cég még augusztusban figyelmeztetett a lehetséges támadásra, mivel kutatásaik során egy közel 70 000 eszközt tartalmazó botnet hálózat kiépítéséről szereztek tudomást, amelynek kapcsán azonosították a káros tevékenységért felelős alkalmazásokat. Bár ezeket a Google biztonsági csapata eltávolította a hivatalos áruházból – valamint megkezdődött az érintett eszközökről való kivonás is – a felhasználóknak fokozott figyelmet javasolnak és a védelmi szoftverek naprakészen tartását. **Bővebben...**

IT biztonsági Tanács

Egy internetről is elérhető okos eszköz (IoT) vásárlásakor a gazdasági tényezők mellett javasolt a biztonsági jellemzőkre is figyelmet fordítani. Például:

- Van-e autentikáció és meg lehet-e változtatni az alapértelmezett felhasználónevet és a jelszót.
- A gyártó milyen támogatást ad az eszközhöz (és milyen hosszú ideig).
- Kell-e a működéshez portokat nyitni az internet felé.

Az egyetemek is kedvelt célpontok

(www.ibtimes.co.uk)

Megduplázódott az Egyesült Királyság egyetemeit célzó támadások száma, melyek célja főleg a technológiai kutatási (például gyógyszerészeti, mérnöki) eredmények, valamint katonai és személyes adatok megszerzése és vélhetően azok kiszivárogtatása más kormányzatok számára. A felsőoktatási intézmények lényeges kutatási és fejlesztési erőforrásokkal rendelkeznek és az ezzel kapcsolatos információk megszerzése komoly előnyt jelenthet - nyilatkozta Carsten Maple, a Warwick Egyetem kiberbiztonsági kutatási vezetője. A jelentős értékű szellemi tőkéhez mérten azonban sokszor alacsony a kialakított védelemi szint (például elavult operációs rendszerek), amely elsősorban a nem elégséges pénzügyi támogatásnak köszönhető. **Bővebben...**

Figyelmeztetés az SSL implementálásáról

(www.threatpost.com)

Megkezdte a weboldal tulajdonosok e-mailes kiértesítését a Google, a HTTP-ről HTTPS-re történő átállásra való emlékeztetésül. A tech óriás ugyanis októbertől - a Chrome böngésző 62-es verziójának kiadásával - "Nem biztonságos"-ként jelöli meg az SSL-t nem implementáló weboldalakat. Az átállással kapcsolatos tippeket is tartalmazó értesítőket azon webmesterek kapták meg, akik használják a Google ingyenes weboldal keresőoptimalizáló szolgáltatását, a 'Google Search Console'-t. A szigorítás minden olyan webhelyet érint, ahol a felhasználók adatokat tudnak megadni, tekintet nélkül azok jellegére. Biztonsági szakértők kiemelik, hogy a webadminoknak ki is kell kényszeríteniük a HTTPS-t, hogy elkerüljék az esetleges átirányításokat az oldalak nem biztonságos verziójára. **Bővebben...**

Növekvő hangsúly a dark web elleni harcon

(www.securityaffairs.co)

Az Egyesült Királyság Nemzeti Bűnügyi Ügynöksége (NCA) IT szakértőket toboroz a 'dark web'-en működő illegális tevékenységek felszámolásához. A sötét web továbbra is aggasztóan kiemelt szerepet tölt be a feketepiaci tevékenységek, például a drogkereskedelem terén. Egy felmérés szerint ugyanis a brit droghasználók körülbelül negyede szerzett már be ilyen forrásból illegális szereket. Az angol kormányzat emellett a szélsőséges nézetek terjedése miatt is aggódik, mert úgy vélik egyes rejtett platformok komoly szerepet játszhatnak a radikálódásban. Ennek szellemében a bűnüldöző hatóságokkal együttműködve törekednek a társszervezetekkel való együttműködés kiterjesztésére. Az NCA eddigi tevékenysége nyomán mintegy 1 763 letartóztatást eszközöltek belföldön és további 1 300-at a tengerentúlon. **Bővebben...**

Kötelező figyelmeztetés a munkahelyi kommunikáció megfigyeléséről

(www.techcrunch.com)

Az Emberi Jogok Európai Bírósága (ECHR) a munkahelyi magánélet tiszteletben tartásával kapcsolatban mérföldkőnek számító ítéletet hozott. Eszerint a munkáltatóknak mostantól előzetesen figyelmeztetniük kell a munkavállalóikat, amennyiben monitorozni kívánják a munkahelyi elektronikus kommunikációjukat. Az ítélet egy 2007-ben indult per kapcsán született meg, amikor egy román állampolgárnak szüntették meg a munkaviszonyát, mert magáncélra használta munkahelyi infrastruktúrát, ezzel megsértve a vállalat belső szabályait. **Bővebben...**