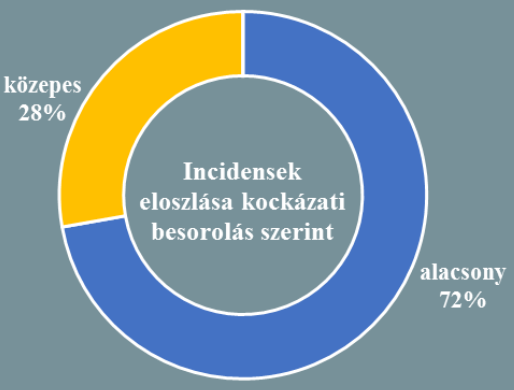
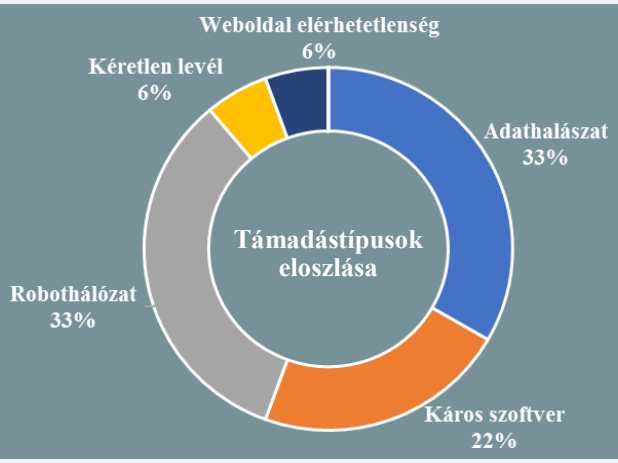
Incidens adatok:
2017.09.20. — 2017.09.26.





Kibervédelmi fejlesztések Ausztráliában

(www.technologydecisions.com)

Az ausztrál kormány a következő hét évre 50 millió dollárt szán egy kiberbiztonsági kooperatív kutatóközpont létrehozására, amit különböző iparági partnerektől további 89 millió dollár egészít majd ki. Ezzel együtt az elvárások is nagyok a Cyber Security CRC-vel szemben, a cél ugyanis egy komplex kibervédelmi képesség megteremtése olyan keretrendszerek és termékek kidolgozásával, ami a vállalkozások és az állampolgárok számára egyaránt védelmet nyújt. Craig Laundy, az ipari fejlesztésügyi helyettes miniszter elmondása szerint a kibervédelmi fejlesztések és a kooperáció kiemelt támogatása megoldást jelent a kritikus infrastruktúrák védelmének biztosítására, mindemellett élénkítő hatással lesz a gazdaságra is. **Bővebben...**

Újabb EU-s kibervédelmi intézkedések

(www.securityweek.com)

Andrus Ansip, az Európai Unió digitális egységes piacért (Digital Single Market) felelős alelnöke szerint a kiber támadások elleni hatékony védelemhez az EU-nak 24 órás reagálási képességet kell kifejlesztenie, amelynek szellemében egy új kiberbiztonsági ügynökség felállítását tűzték ki célul. A jelenlegi ügynökségre építve az új szervezet fő feladata annak elősegítése lesz, hogy a tagállamok képesek legyenek kezelni a kibertámadásokat, illetve kiemelt szerepet kap az európai szintű éves gyakorlatok szervezésében és a hatékonyabb információ megosztás elősegítésében is. Emellett várható egy új EU-s tanúsítási rendszer bevezetése, ami az energetikai, szállításügyi és egyéb hálózatok, valamint új fogyasztói eszközök minősítésére szolgál majd, nagyjából az élelmiszercímkékhez hasonlóan. **Bővebben...**

Kategóriateremtő kibertámadás jöhet

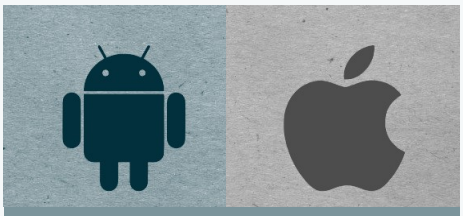
(www.theguardian.com)

Az Egyesült Királyság kibervédelmi központjának (National Cyber Security Centre) vezetője szerint a következő néhány év során nagy az esély egy minden eddiginél súlyosabb kibertámadásra. Ian Levy a Symantec kiberbiztonsági rendezvényén elmondta, hogy a megelőzés csak akkor lehetséges, ha a kormányzati és a gazdasági szektor változtat a kérdéskörhöz való viszonyulásán. Például ahelyett, hogy megszállottan a lehető legjobb biztonsági termékek beszerezésére összpontosítanának, a szervezeteknek sokkal nagyobb figyelmet kellene fordítaniuk a kockázatelemzésre. Fontos lenne jobban átlátniuk az általuk kezelt adatokat, az azok által hordozott értéket és az esetleges sérüléssel okozható károkat. Levy azt tanácsolja a vállalkozásoknak, hogy kevésbé bízzanak a "polcról levett" megoldásokban és támaszkodjanak jobban a munkatársakra a védelem kialakításakor. **Bővebben...**

Az ISIS vélhetően alacsony szintű kiberképességgel rendelkezik

(www.securityaffairs.co)

Az Iszlám Államhoz köthető Egyesült Kiber Kalifátus (United Cyber Caliphate - UCC) felhagyott a saját hacker eszközök fejlesztésével, közölte Kyle Wilhoit, a DomainTools kutatója a DerbyCon hacking konferencián tartott előadásában. Az elemző szerint ennek az az oka, hogy vélhetően rendkívül gyenge kódolási képességgel rendelkeznek, amit több általuk fejlesztett titkosított kommunikációra szolgáló alkalmazás és malware elemzésére alapoznak. **Bővebben...**



Mobil rendszerek biztonsága
(www.forbes.com)

A Datavisor által készített jelentés szerint - melynek elkészítéséhez közel 140 millió telepített alkalmazást tanulmányoztak - az Android rendszerek esetében magasabb a hamis alkalmazások aránya (5,8%), mint az iOS rendszereknél (3%). Mindkét rendszerre igaz, hogy főleg a régebbi operációs rendszereket részesítik előnyben a támadók. A jelentés szerint az Androidos rendszerek azért népszerűbbek a támadók körében, mert a nyílt platformhoz egyszerűbben képesek hozzáférni a támadók. **Bővebben...**

A Go Keyboard alkalmazás is privát adatokat gyűjt
(www.ibtimes.co.uk)

A népszerű androidos billentyűzet alkalmazás az AdGuard szerint titokban érzékeny adatokat gyűjt a felhasználókról. Az applikációt – amely ráadásul káros kódot is tartalmazhat – eddig több mint 400 millió felhasználó töltötte le. **Bővebben...**

IT biztonsági Tanács

Az adathalászat továbbra is növekvő tendenciát mutat. A levelek gyakran helyesírási hibákat tartalmaznak, és legtöbbször jelszó cserére vagy számlafizetésre szólítanak fel, de legyünk kritikusak az ismerősök által küldött, legitimnek tűnő üzenetekkel szemben is.
Használhatunk böngésző bővítményeket is, amelyek figyelmeztethetnek a gyanús tevékenységre.

Adathalászat régen és ma
(www.helpnetsecurity.com)

Az adathalászat továbbra is egyike a leggyakoribb számítógépes támadásoknak, mely még mindig növekvő tendenciát mutat. Jelenleg átlagosan naponta 46 000 új weboldalt hoznak létre adathalászati céllal világszerte, derült ki a Webroot elemzéséből. 2017 első felében is folytatódott a trend, miszerint ezek a megtévesztő oldalak csak rövid ideig aktívak – sok esetben csupán 4-8 óráig – annak érdekében, hogy elkerüljék az észlelésüket. Az is megfigyelhető, hogy míg régebben általános sémákat használtak fel a támadásokhoz, mára sokkal kifinomultabb módszerekkel – például a közösségi média oldalakról összegyűjtött információk segítségével – igyekeznek megtéveszteni az áldozatokat, melyet a felhasználók és az anti-phishing rendszerek is egyre nehezebben észlelnek. **Bővebben...**

Mennyire lesz biztonságos az új titkosítási szabvány?
(www.reuters.com)

Nemzetközi nyomásra az NSA visszakozott két, általuk favorizált titkosítási algoritmussal kapcsolatban. A 'SIMON' és a 'SPECK' eljárásokat az Egyesült Államok már 2014 óta próbálja ISO szabványként elfogadtatni, ami ellen az eddigi szavazásokon rendszerint vétót emeltek. Szakértők ugyanis úgy vélték, ezeket nem a megbízhatóságuk miatt javasolták, sokkal inkább azért, mert az amerikai titkosszolgálat képes lehet a feltörésükre. A tiltakozások hatására az NSA végül a robosztusabb verziók mellett döntött, ami a múlt hónap során kedvezőbb fogadtatásra talált, így a javaslat jelenleg a jóváhagyási eljárás végső szakaszában van. **Bővebben...**

Államilag támogatott lehetett a CCleaner fertőzés
(www.motherboard.com)

Szakértők úgy vélik, hogy államilag támogatott hacker csoport állhatott a CCleaner program kompromittálódásával okozott fertőzés hátterében, amely becslések szerint mintegy 2,2 millió felhasználót érinthetett. Kettő biztonsági cég kutatói is kapcsolatba tudták hozni a most használt rosszindulatú programot egy kínai hacker csoporttal, akiknek korábban a Google vállalati infrastruktúrájába is sikerült bejutniuk. Az APT17 más néven 'DeputyDog' egy olyan csoport, amely több mint egy évtizede működik, és korábban már kormányzati szervek, ügyvédi irodák és különböző iparágakból származó vállalatok ellen folytatott sikeres támadást. **Bővebben...**

Kína szigorúan lépett fel a szabálysértőkkel szemben
(www.in.reuters.com)

Kína első alkalommal szabott ki büntetést a június óta érvényben lévő kiberbiztonsági törvény alapján az ország egyes multi tech vállalataira, amelyek között található a Tencent, a Baidu és a Weibo is. Hétfőn kiadott közleményében a Cyberspace Administration of China (CAC) közölte, hogy az érintett vállalatok nem tettek eleget az online tartalmak szűrésére vonatkozó előírásoknak és nem távolították el a hamis híreket, a pornográf, illetve a gyűlöletkeltő tartalmakat. A konkrét összeget ugyan nem részletezik, de a hivatkozott szabályok alapján a felelős személyek egyenként 100 000 jüan (körülbelül 15 000 dollár) mértékű bírságot kaphatnak. A törvény alapján a felügyeleti szerv a pénzbírságon kívül vissza is vonhatja a jogsértő szervezetek engedélyeit és felfüggesztheti szolgáltatásaikat. **Bővebben...**