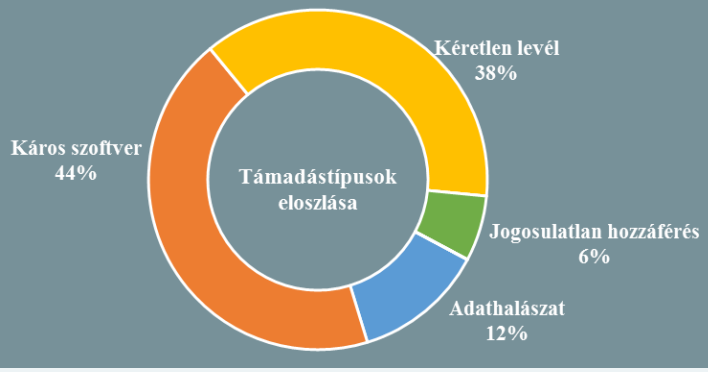
Incidens adatok:
2018.03.30. - 2018.04.05.



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

ENISA a potenciális kiberfenyegetések felkutatásáról

(www.enisa.europa.eu)

Az ENISA kiadta első tanulmányát a kiberfenyegetés-felderítő szolgáltatásokról, az ún. Threat Intelligence platformokról (TIP). A tanulmány célja, hogy azonosítsa a jelenleg elérhető megoldásokban rejlő lehetőségeket és korlátokat, mivel a releváns, kontextusfüggő biztonsági információk nem csupán az eseménykezelő szervezetek, hanem bármely mai, modern vállalat számára is alapvető fontossággal bírnak. Az elemzés részletes áttekintést ad a platformok felhasználóiról, a TIP-ek főbb funkcionális területeiről, valamint a különböző feladatokat ellátó IT-biztonsági csoportok (CTI-k, SOC-ok, CSIRT/CERT-ek, stb.) által használt TIP-ek jelenlegi helyzetéről. A jelentés számos javítóintézkedést és ajánlást fogalmaz meg, például a vállalatok számára javasolják, hogy a megfelelő TIP kiválasztásához fókuszáljanak a saját specifikus követelményeikre, emellett felhívják a figyelmet az ingyenes megoldásokra, amelyeket célszerű megvizsgálni, mielőtt egy költséges szolgáltatás mellett döntenének. **Bővebben...**

A Chrome a háttérben káros kódok után kutat a Windowsos gépeken

(www.motherboard.vice.com)

A Google még tavaly ősszel jelentette be, hogy a böngészőjét egy új biztonsági funkcióval látja el, azonban a biztonsági szakma csak most figyelt fel a Chrome Cleanup Tool-ra. Ez a böngészőbe épített antivírus komponens az ESET víruskereső motorját felhasználva Windows rendszereken – a felhasználó tudta nélkül – gyakorlatilag a teljes fájlrendszert átvizsgálja olyan kártékony programok után kutatva, amelyek a böngészőre nézve fenyegetőek lehetnek. Találat esetén felajánlja, hogy eltávolítja a káros fájlokat, amelyek meta adatairól alapértelmezetten jelentést tesz a Google felé, olyan információkat továbbítva, mint a malware helye a fájlrendszerben, valamint egyéb – nem részletezett – rendszerinformációk, mindazonáltal ez a jelentéstétel opcionális. Időközben több biztonsági kutató is kifejezte aggodalmát az előzetes hozzájárulás hiánya és az eljárás átláthatatlansága miatt. A Google Chrome biztonsági főnöke egy Twitter posztban kiemelte, hogy a szoftver nem gyűjt be felhasználói információkat és csupán hetente fut le, valamint, hogy a fájlokon kizárólag felhasználói beleegyezést követően hajt végre bármiféle műveletet. **Bővebben...**

Már elérhető a leggyorsabb publikus DNS szolgáltatás

(www.bleepingcomputer.com)

Az 1.1.1.1-es IP címen érhető el a Cloudflare és az APNIC által közösen indított ingyenes DNS szolgáltatás, amelyet 2018. április 01-én jelentettek be. A közlemény szerint a cél a leggyorsabb DNS feloldást nyújtó szolgáltatás létrehozása volt, ami egyúttal a magánszféra védelmét is figyelembe veszi. A legtöbb jelenleg elérhető DNS szolgáltatással kapcsolatban ugyanis – a kiszolgálás lassúsága mellett – aggasztónak tartják, hogy egyesek logolják a felhasználói IP címeket és az onnan érkezett feloldási kéréseket, ami lehetővé teszi számukra a felhasználói böngészések nyomonkövetését, majd ezen privát információk továbbértékesítését harmadik félnek. Az 1.1.1.1 esetében azonban az ügyfelek címei egyáltalán nem íródnak diszkre és a tranzakciós logokat 24 óránkként törlik. A performanciára vonatkozó állításokat alátámasztják a DNSPerf által végzett mérések, ami alapján jelenleg valóban ez a leggyorsabb DNS szolgáltatás. A biztonsággal kapcsolatos kijelentések hitelességét pedig a KPMG-vel tervezik validáltatni egy biztonsági audit során. **Bővebben...**

A Google Play Store-on is előfordulnak kriptovaluta bányász alkalmazások

(www.zdnet.com)

A jelenleg dúló „kriptoláz” hevében a kiberbűnözők az eszközök könnyű fertőzése miatt egyre növekvő mértékben igyekeznek a mobil platformot is felhasználni profittermelésre, amire a Google hivatalos áruházát is előszeretettel használják. A Kaspersky Lab kutatói számtalan fertőzött VPN, játék és sport alkalmazást találtak a Google Play-en, amelyek közül némelyiket 100 000-nél is több alkalommal töltötték le. Ezek az applikációk, habár jellemzően legitim szolgáltatást is nyújtanak, azt főképp a figyelemelterelés miatt teszik, és fő céljuk az eszköz számítási kapacitásának felhasználása valamilyen kriptovaluta (pl. Monero) bányászásához. A biztonsági cég szerint a futball témájú app-ok a legnépszerűbbek, azon belül egy portugál nyelvű meccsközvetítő alkalmazást töltötték le a legtöbben. A Kaspersky felvette a kapcsolatot a Google-lel, így a fertőzött applikációk mostanra eltávolításra kerültek. **Bővebben...**

IT biztonsági Tanács

Otthoni hálózatunkon célszerű saját WiFi routert használni az internet szolgáltatótól kapott eszköz helyett. Ehhez a berendezést bridge módba kell állítanunk, amelyhez segítséget kérhetünk a szolgáltatótól.

Lehetőleg olyan eszközt vásároljunk, amelyhez a gyártó sérülékenységek esetén a vezérlő rendszert (firmware) érintő frissítéseket tesz elérhetővé.

Kövesse figyelemmel a hírek szerint még idén megjelenő, biztonságos új szabvány (WPA3) megjelenését és az implementálásról szóló gyártói közleményeket.

Ausztráliában szigorítanak a kritikus rendszerek kockázati tényezőinek csökkentéséhez

(www.zdnet.com)

Az ausztrál parlament elfogadta a kritikus infrastruktúrák védelméről szóló törvényt, mellyel a kormányzat a villamos energia, víz, földgáz és a hajózási szektorok, „külföldi befolyástól” való védelmét kívánja biztosítani, azáltal, hogy a miniszterek számára lehetővé teszi, hogy a vállalatokat direkt módon utasíthassák biztonsági intézkedések meghozására, amennyiben nemzetbiztonsági kockázat merülne fel. Az ágazatért felelős miniszter abban az esetben alkalmazhatja a kiterjesztett jogkört és adhat ki utasítást, ha egy szakmai szervezet – mint az Ausztrál Biztonsági Hírszerző Szervezet (ASIO) – kedvezőtlen biztonsági értékelést készít és a kockázat megszűntetése más módon nem lehetséges. Peter Dutton belügyminiszter nyilatkozatában kifejtette, hogy a jogszabály nyomán létrejön a magas kockázatú kritikus infrastruktúrákhoz tartozó rendszerelemek részletes nyilvántartása, mely tulajdonjogi és hozzáférési információkat is tartalmaz majd. **Bővebben...**

Kampányidőszakban kiemelt figyelmet szentelnének a közösségi oldalaknak

(www.theguardian.com)

Sir Julian King, az Európai Bizottság biztonsági unióért felelős biztosa a 2019-es európai választásokra való felkészülés jegyében egyértelmű stratégia létrehozását javasolja arra vonatkozóan, hogy a közösségi platformok miként működhetnek a politikai kampányok idején. Ennek érdekében fontosnak tartja a politikai célú adatgyűjtés korlátozását és nagyobb átláthatóságot vár az internetes – kiemelten a szponzorált – tartalmak megjelenítéséhez használt belső algoritmusok terén. Hasonló szigorító törekvések világszerte megtalálhatók, például Franciaországban, ahol blokkolnák a kampányidőszakokban álhíreket terjesztő oldalakat. Malajziában már hatályba is lépett egy ilyen jogszabály, melynek értelmében az elkövetők 6 év börtönre büntethetők. A kritikusok szerint az ilyen jellegű törekvések veszélyeztethetik, nem csupán a véleménynyilvánítás szabadságát, de a kiadói jogokat is – derült ki egy, az európai ombudsmanhoz benyújtott 13 oldalas beadványból. A HEC Paris kutatói ebben rámutatnak, hogy az EU nem rendelkezik olyan egységes módszerrel, amellyel képesek lennének megállapítani, hogy egy kiadvány tartalmaz-e dezinformációt avagy sem. **Bővebben...**

Európa rosszabbul teljesít az incidenskezelés terén, mint az Egyesült Államok

(www.theregister.co.uk)

A FireEye által készített tanulmány szerint a szervezetek Európában lassabban reagálnak az adatszivárgásokra, mint Észak-Amerikában. Az EMEA térség (Európa, Közel-Kelet és Afrika) vállalatai átlagosan közel fél hónap (175 nap) alatt azonosítják a hálózati behatolókat, ami lényegesen hosszabb idő a tavalyi évben mért 102 naphoz képest. Ezzel szemben az USA-ban – 2016-hoz viszonyítva – 23 nappal csökkent a detektálás ideje. Ezek az európai adatszegések észlelésére vonatkozó megállapítások kiváltképp a közelgő GDPR miatt adnak okot aggodalomra, mivel az európai polgárok adatainak kompromittálódása esetén hatalmas összegű bírságok érhetik a vállalkozásokat. A FireEye jelentésében arról is beszámol, hogy a hackertámadások több, mint fele (56%) esetében fordul elő, hogy a támadók újra lecsapnak az áldozatra, illetve megállapítják, hogy a 2017-es évben Oroszország és Észak-Korea mellett Irán is jelentős kockázati tényezővé vált. **Bővebben...**