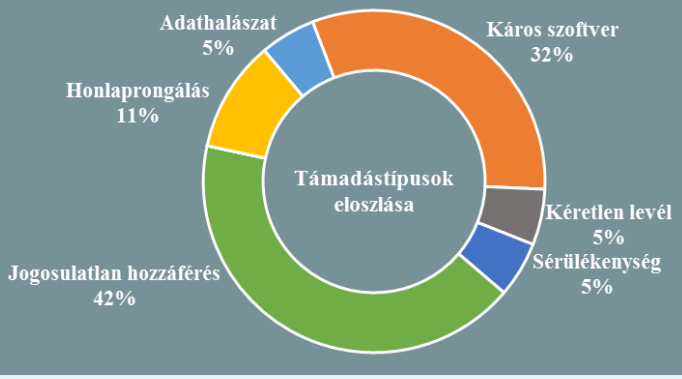
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.04.27. - 2018.05.03.



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

A NATO csapata nyerte a Locked Shields gyakorlatot

(www.ccdcoe.com)

A világ legrangosabb, évente megrendezésre kerülő nemzetközi kibervédelmi gyakorlatán a különböző NATO ügynökségeket képviselő team szerezte meg az első helyet, megelőzve a francia és a cseh csapatokat. „A győztes csapat minden kategóriában kitűnt a gyakorlat során” – nyilatkozta Aare Reintam, a rendezvényt szervező Cooperative Cyber Defence Centre of Excellence (CCDCOE) képviseletében, azt is hozzátéve azonban, hogy úgy véli, minden résztvevő kitett magáért. A körülbelül 4 000 virtualizált rendszer bevonásával zajlott gyakorlat során ugyanis a védekező szerepben lévő „kék csapatoknak” egyszerre kellett megbirkózniuk több, mint 150 komplex IT rendszer felügyeletével, az incidensjelentés készítésével, stratégiai döntések meghozásával, amellett, hogy forensic tevékenység, jogi, valamint a médiával kapcsolatos kihívások is a feladatok részét képezték. Az idei esemény tanulsága, hogy egyre nagyobb igény mutatkozik a technikai szakemberek, a civil és katonai résztvevők, valamint a döntéshozók közötti párbeszéd javítására. **Bővebben...**

A kínai hatóságok hozzáférnek a felhasználók törölt WeChat üzeneteihez

(www.bleepingcomputer.com)

Hatalmas felháborodást váltott ki a Chaohu Municipal Discipline Inspection and Supervision Commission kínai korrupció ellenes bizottság egy közleménye, melyben arról számolnak be, hogy egy nyomozás során egy gyanúsított törölt WeChat üzeneteit szerezték meg. A Bizottság ugyan másnap eltávolította az online közzétett nyilatkozatot, azonban addigra az már széles körben megosztásra került a kínai közösségi oldalakon, és a magánélethez való jog azóta is elsődleges téma a felhasználók körében. A tömeg kritikája elsősorban a Kínai Kommunista Pártot és a WeChat-et fejlesztő Tencent-et éri, utóbbi emiatt nyilatkozat kiadására kényszerült, miszerint a cég nem tárolja a szerverein az ügyfelek chat előzményeit, azok csupán a végponti eszközökön érhetők el. A közlemény azonban csak további elégedetlenséget szított, mivel a törölt üzenetek hozzáférhetőségéről továbbra sem tartalmazott állásfoglalást. **Bővebben...**

Hamis hírek elleni javaslatok az ENISA-tól

(www.enisa.europa.eu)

Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) nyilvánosságra hozta az Európai Bizottság online dezinformációk kezelésére irányuló javaslataival kapcsolatos véleményét, amelyet a NIS (Network and Information Security) szempontjából készítettek el. Az ENISA többek között javasolja a mesterséges intelligencia felhasználását az online dezinformációs kampányok és az ehhez kapcsolódó káros online tevékenységek (pl.: spammelés) detektálásához. Úgy vélik a közösségi médiaszolgáltatóknak a felhasználói bizalom növeléséhez fontolóra kellene venniük a dezinformációs elemzéseik eredményeinek nyilvánosságra hozatalát. Javasolják egyedi szignatúrák alkalmazását a hírekben, azok eredetiségének igazolásához, valamint indítványozzák egy olyan stratégia kidolgozását is, amely szerint a hamis híreket terjesztő weboldalak üzemeltetőit gazdasági retorziók érhetik. **Bővebben...**

Android-alapú keretrendszert jelentettek be az IoT eszközök számára

(www.itnews.com)

A Google idénre tervezi az Android Things 1.0 széleskörű bevezetését, ami az Android operációs rendszer egy, speciálisan az IoT eszközökhöz készített változata – derült ki a cég éves konferenciáján, a Google I/O-n. A kezdeményezés célja, hogy egy egységes keretrendszert biztosíthassanak a különböző okos eszközök számára. A tervek szerint az Android Things kódjának egyes részei nem lesznek módosíthatóak, például, ami a Google -től származó frissítések telepítését hivatott kezelni. A cég ezzel az IoT rendszerek számára jelenleg messze a legnagyobb problémát jelentő biztonsági hiányosságokat szeretné javítani, amitől azt remélik, hogy a kockázatkerülőbb ipari szereplők számára is vonzóbbá tehetik a technológiát.

Bővebben...

IT biztonsági Tanács

A Google különféle adatokat tárol a szolgáltatásaihoz kapcsolódó felhasználói tevékenységekről.

Javasolt ennek áttekintése, amit a Google fiókba való bejelentkezés után a „Saját fiók”, „Adatvédelmi beállítások” menü alatt elérhető „Google-tevékenységének kezelése” menüpontban a „Tevékenységvezérlők”-re kattintva tehetünk meg, ahol egyesével módosíthatjuk is az adatgyűjtési beállításokat, például a helyelőzményekre, hangtevékenységekre, eszközadatokra stb. vonatkozóan.

Intenzív kampányba fogtak az észak-koreai hackerek

(www.bleepingcomputer.com)

A McAfee számolt be a Lazarus Group (vagy más néven Hidden Cobra, Hastati Group vagy Group 77) által indított támadásokról, melyek során érzékeny adatokat igyekeznek megszerezni mintegy 17 országban. A célpontok között kritikus rendszerek, szórakoztatóipari, pénzügyi, egészségügyi és telekommunikációs cégek is megtalálhatóak. Az „Operation GhostSecret”-nek keresztelt offenzíva nagyjából 2018. március közepén kezdődhetett török pénzügyi szervezetek elleni támadásokkal, melyek során korábban használt káros szoftvereket és egészen új variánsokat is bevetettek. A kutatók a támadó infrastruktúra egy részét már azonosították, például a bangkok-i Thammasat Egyetemhez tartozó IP címeket, amelyek miatt már felvették a kapcsolatot a thaiföldi kormánnyal. **Bővebben...**

Új megoldás az IoT és ipari vezérlőrendszerek védelméhez

(www.bleepingcomputer.com)

A Microsoft új, Trusted Cyber Physical Systems (TCPS) nevű rendszere három komponensre támaszkodva hatástalanítja a támadásokat. Az első a Trusted Execution Environment (TEE), ami a modern CPU-kban alkalmazott megoldásokhoz (Intel SGX, ARM TrustZone) hasonlóan hardveres szintű védelmet nyújt. A második egy grafikus interfész, amit egy megbízható – az adott vállalat alkalmazásában álló – humán operátor üzemeltet. Ennek használatával lehetőség van arra, hogy bizonyos műveletekre irányuló beérkező parancsok csak az operátor jóváhagyásával fussanak le. **Bővebben...**

A brit Legfelsőbb Bíróság részben jogellenesnek minősített egy adatgyűjtési törvényt

(www.helpnetsecurity.com)

A National Council for Civil Liberties (NCCL) civil jogvédő szervezet beadványt nyújtott be az Egyesült Királyság Legfelsőbb Bíróságához a nyomozati hatáskör szabályozásáról szóló 2016. évi törvény (IPA) – más néven Snoopers’ Charter – 4. szakaszával kapcsolatban, arra hivatkozva, hogy az sérti az Egyesült Királyság állampolgárainak magánélethez való jogát, továbbá összeegyeztethetetlen az Emberi Jogok Európai Egyezményével. A kifogásolt rész ugyanis lehetővé teszi egyes hírközlési adatok – például az ügyfelek tartózkodási helyére vonatkozó információk és böngészési előzmények – megőrzését és hozzáférhetővé tételét a hatóságok számára. A bíróság ítéletében úgy határozott, hogy a szóban forgó szakasz részben jogellenes, mivel az információ gyűjtése nem korlátozott a súlyos bűncselekmények esetére. Ugyanakkor azt a vádat, miszerint a jogszabály „általános és válogatás nélküli gyűjtést tesz lehetővé” elutasították. **Bővebben...**

A felhasználók tevékenységének követése miatt kétszer lassabban töltődnek be a weboldalak

(www.ghostery.com)

A Ghostery nemrég készített „Nyomkövető Adó” című tanulmánya szerint az Amerikai Egyesült Államokban az 500 legnépszerűbb weboldal közel 90%-a legalább egy, 20%-uk pedig ötven, vagy több nyomkövetőt tartalmazott és a vizsgált oldalak csupán mindössze 10%-a volt nyomkövető mentes. A tanulmány rávilágít arra is, hogy a nyomkövetők lényegesen lassítják a weboldalak betöltési sebességét, aminek a jelentőségét az amerikai netsemlegességet biztosító szabályok hatályon kívül helyezése tovább növeli. **Bővebben...**