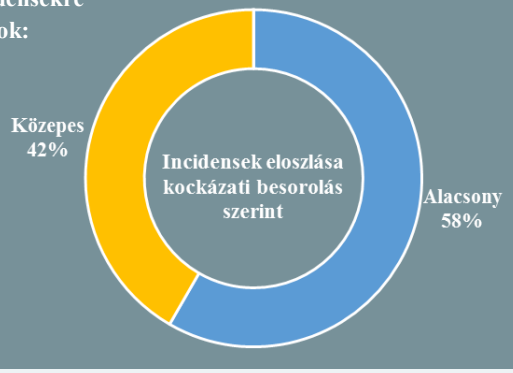
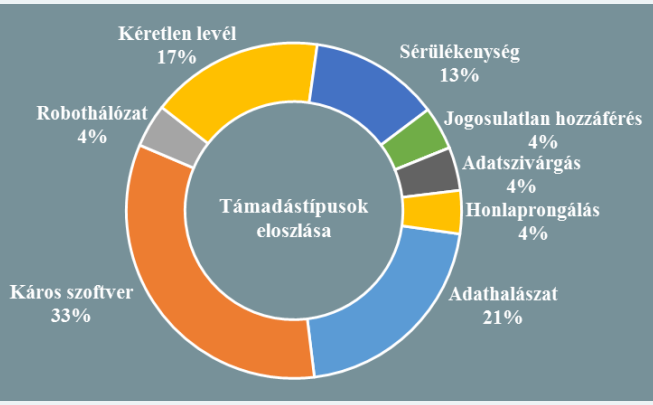
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.05.18. - 2018.05.24.





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

Az Amazon is megjelent a megfigyelési piacon

(www.bleepingcomputer.com)

Az American Civil Liberties Union (ACLU) jelentése szerint a tech óriás az „Amazon Rekognition" nevű, mélytanuláson alapuló arcfelismerő rendszerét aktívan értékesíti bűnüldöző szervek számára. A szervezet tavaly fedezte fel – az egyébként már 2016 óta működő – szolgáltatást, amelynek két ügyfélét sikerült azonosítania, az orlandói rendőrséget, és a Washington Megyei Seriffhivatalt. Ezt követően az információs szabadságáról szóló amerikai törvény (Freedom Of Information Act – FOIA) érvényesítésével sikerült hozzáférniük a hatóságok, és az Amazon közötti írásbeli kommunikációhoz, amelyből többek között kiderült, hogy a vállalat nagy energiákat fektet a szolgáltatás népszerűsítésébe. Az ACLU a magánszférára nézve komoly veszélyként értékeli a rendszert, és tart annak ugrásszerű elterjedésétől, tekintve az alacsony költségét (csupán havi néhányszor tíz dollár), és az Amazon márkaerejét. **Bővebben...**

Lassanként szerveződik az amerikai kibervédelem

(www.bleepingcomputer.com)

Az Egyesült Államokban törvényjavaslatot nyújtottak be ún. „kiber támogató egységek" létrehozására az amerikai nemzetőrség részeként (National Guard Cyber Civil Support). A kormányzók rendelkezésére álló egységek előirányzott feladatai között hangsúlyos szerepet kap a magánszektor szereplőinek helyi oktatása, legjobb gyakorlatok elterjesztése, reakciótervek kidolgozása, és kibergyakorlatok szervezése, emellett kibertámadások esetén szövetségi, állami, és helyi szintű koordinációs szereppel is bírnának. Minden állam rendelkezne egy ilyen szervezettel – beleértve az olyan külbirtokokat is, mint Puerto Rico, Guam, és az Amerikai Virgin szigetek – ehhez államonként egy 50 millió dolláros keretet javasolnak. **Bővebben...**

A Cisco kiberhírszerző csapata potenciális kibertámadásra figyelmeztet

(www.reuters.com)

A Cisco közleménye szerint hackerek legalább 500 000 routert fertőztek meg egy kifinomult káros szoftverrel, aminek célja vélhetően egy átfogó informatikai támadás indítása, például Ukrajna ellen. Úgy vélik mindemögött az orosz kormányzat állhat, amit arra alapoznak, hogy a tömeges fertőzések elemzése során az amerikai kormány által korábban már Oroszországhoz kötött malware mintákat azonosítottak. A szakértők szerint a szóban forgó káros kód (VPNFilter) információszerzésre, de akár aktív támadás indítására is alkalmas. A több nagy IT biztonsági céget is magába tömörítő Cyber Threat Alliance (CTA) nonprofit szervezet több tagja – Cisco, Symantec, Palo Alto, Sophos stb. – is jelezte, hogy elkötelezettek a figyelmeztetés minél szélesebb körű terjesztéséért. **Bővebben...**

Négy fontos európai kibervédelmi szervezet szorosabbra fűzi az együttműködést

(www.enisa.europa.eu)

A Európai Unió Hálózati és Információs Biztonsági Ügynöksége (ENISA), az Európai Védelmi Ügynökség (EDA), az Európai Számítástechnikai Bűnmegelőzési Központ (EC3) és az Európai Unió Számítógépes Sürgősségi Reagálási Egysége (CERT-EU) egyetértési nyilatkozatot írt alá egy közös együttműködési keretrendszer megalkotásához, aminek célja a kibervédelemi törekvések támogatása a leghatékonyabb erőforrás kihasználással, és a felesleges párhuzamosságok kiiktatásával. Ennek során öt főbb területre fókuszálnak, melyek az információ csere, az oktatás és képzés, a kibervédelmi gyakorlatok, a technikai kooperáció, valamint a stratégiai és adminisztratív ügyek. **Bővebben...**

iOS-es eszközökön is használható lesz a Yubico-féle többlépcsős azonosítás

(www.cyberscoop.com)

A Yubico kiberbiztonsági cég bejelentette, hogy – miután az Apple korábban nyitott az NFC (Near Field Communication) technológia szélesebb körű felhasználására – a kétlépcsős azonosítást biztosító megoldásuk elérhető lesz iOS-en is. A YubiKey termékcsalád a kétfaktoros hitelesítést egy hardverkulcs segítségével végzi, ami asztali munkaállomásokkal USB, mobil eszközökkel pedig a rövid (maximum néhány centiméter) hatótávú rádiós kapcsolatot biztosító NFC szabvány szerint kommunikál. A cég most hozzáférhetővé tett egy iOS applikáció készítőknek szánt fejlesztőkészletet (SDK), ami lehetőséget biztosít, hogy alkalmazásaikat felkészítsék az NFC-n keresztüli autentikációra. **Bővebben...**

IT biztonsági Tanács

Elérhető a CIS kritikus biztonsági kontrollok 7.0-ás verziója. A SANS **ajánlása** szerint ezek közül fontos **legalább** az alábbi első hat kontrollra figyelmet fordítani, mert a Pareto elv alapján már ez is 80%-kal növeli a védelmi szintet.

1) Hardver assetek nyilvántartása és kontrollja.
2) Szoftver assetek nyilvántartása és kontrollja.
3) Folyamatos sérülékenység menedzsment.
4) Admin jogosultságok ellenőrzött használata.
5) Mobil eszközök, laptopok, munkaállomások és szerverek biztonságos konfigurálása.
6) Az audit logok karbantartása, monitorozása és elemzése.

Az amerikai hadsereg digitálisan dokumentálta volna a teljes emberi életutat

(www.motherboard.vice.com)

2003-ban a Fejlett Védelmi Kutatási Projektek Ügynöksége (DARPA) egy olyan projektet indított, aminek a célja nem kevesebb volt, mint rögzíteni egy személy minden mozgását, beszélgetéseit, és bármit, amit az illető tapasztal – hall, lát vagy olvas – azaz teljességre törekvően rögzíteni egy személy életének minden történését. A digitalizált életesemények visszakereshető formában történő tárolására szolgáló elektronikus naplózási rendszerre a beszédes „LifeLog” néven hivatkoztak. A hatalmas mennyiségű személyes információ gyűjtésének célja többek között a mesterséges intelligencia fejlesztéshez való hozzájárulás lett volna. Egy évvel a projekt kezdete után azonban a DARPA egy másik – nyíltan megfigyelésre szánt – rövid életű projektje (Total Information Awareness) miatt a személyes adatok kérdését egyre jobban felkapó média nyomására hirtelen vége szakadt. Dr. Douglas Gage, a LifeLog projekt vezetője szerint azonban a koncepció a mai okos telefonokban, és a közösségi média hálózatokban lényegében tovább él. **Bővebben...**

Átvették az irányítást a VPNFilter botnet hálózat felett

(www.bleepingcomputer.com)

Az FBI bírósági engedély birtokában sikeresen átvette az irányítást a becslések szerint több, mint félmillió hálózati eszközből álló VPNFilter botnet hálózat vezérlőszerveréhez tartozó domain felett – írja a BleepingComputer. A Cisco korábban arra figyelmeztetett, hogy a hálózatot vélhetően egy Ukrajna elleni nagy volumenű kibertámadás indítására akarják felhasználni, amit az ukrán titkosszolgálat (SBU) szerint nagy valószínűséggel 2018.05.26-ra időzítették volna, amikor az ország az UEFA-kupa-döntőt rendezi. A Szövetségi Nyomozó Iroda közleményében azt is jelezte, hogy az eddig elvégzett vizsgálatok alapján a botnet az Oroszországhoz kötött, hírhedt kiberkémkedési egység, az APT28 (más néven Sednit/Fancy Bear/Pawn Storm/Sofacy, stb.) irányítása alatt állt. Emellett közzétettek egy listát is a VPNFilter malware-re sérülékeny hálózati eszközökről, amellyel kapcsolatban arra kérik az érintett típusú eszközök tulajdonosait, hogy indítsák újra berendezéseiket, az újrakapcsolódási kísérletek elemzésével ugyanis a szakértők hitelesebb képet alkothatnak a botnet valódi méretéről, és az így előálló információkat továbbíthatják az érintett internetszolgáltatók, valamint magán- és közszektorbeli partnereik részére. **Bővebben...**

Továbbra sem könnyű rávenni a Pentagont, hogy foglalkozzanak a biztonsággal

(www.cyberscoop.com)

Ron Wyden amerikai szenátor megelégelte, hogy az Egyesült Államok Védelmi Minisztériumának weboldalai nem biztonságos kapcsolaton keresztül érhetők el. Emiatt levélben arra kérte Dana Deasy-t, a Pentagon információbiztonsági vezetőjét, hogy a minisztériumhoz tartozó összes honlapon egységesen alkalmazzanak megbízható webes tanúsítványokat és HTTPS titkosítást. Ez jelenleg ugyanis csupán az oldalak egy kis hányadánál valósul meg, annak ellenére, hogy egyes hivatalos dokumentumok arról tanúskodnak, hogy a szervezetnek legkésőbb 2016 végégig be kellett volna vezetnie a HTTPS kizárólagos használatát. Wyden szerint a helyzet sürgős megoldást kíván, mivel ismertté vált, hogy a Google Chrome 2018 júliusától minden hagyományos HTTP-n keresztül elérhető oldalt „nem biztonságos”-ként jelöl meg, ami komoly presztízsveszteséget jelentene a Pentagonnak. **Bővebben...**