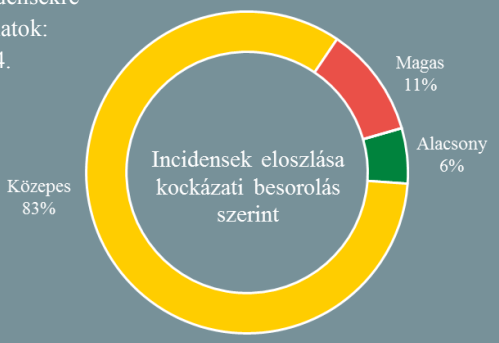
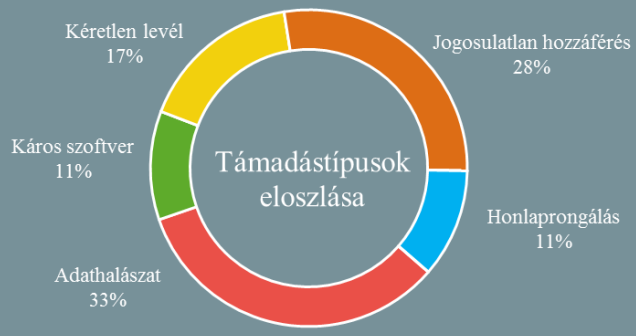
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.06.28. - 2019.07.04.





Kövessen minket megújult weboldalunkon, ahol friss IT-biztonsági hírek kerülnek publikálásra!

Németország és Hollandia közös katonai internethálózatot hoz létre

(zdnet.com)

A NATO védelmi miniszteri találkozóján Brüsszelben német és holland kormányzati tisztviselők megállapodást írtak alá egy közös katonai internet létrehozásáról (Tactical Edge Networking – TEN). A TEN hálózathoz hozzáférő katonák megegyező eszközöket ─ számítógépeket, tableteket, telefonokat ─ fognak használni. Ez az első alkalom, hogy a különböző nemzetek katonai hálózataikat megosztják egymással, ami további NATO tagok számára is példaként szolgálhat. Kezdetben a Bundeswehr digitalizációs projektje (D-LBO) és a holland védelmi minisztérium „FOXTROT" nevű taktikai kommunikációs programja között létesül kapcsolat. A távlati terv az, hogy a NATO tagok szélesebb köre is közössé tegye hálózatait, amely lehetőséget biztosítana további fejlesztések és közös irányelvek kialakítására.

Yandex elleni kiberkémkedéssel vádolnak nyugati államokat

(ehackingnews.com)

A Yandex szerint nyugati titkosszolgálatok több héten keresztül hozzáfértek rendszereikhez, azonban a támadást sikeresen elhárították. A cég azt állítja, hogy a kiberkémkedési célú művelet ügyféladatokat nem érintett, azonban bővebb információt belső szabályzókra hivatkozva nem közölhetnek az esettel kapcsolatban. A Reuters korábbi publikációja szerint a hackerek valamikor 2018 októberében vagy novemberében indították a támadást egy Regin névre hallgató káros szoftver felhasználásával. A programról ismert, hogy az „Öt Szem" (Five Eyes) szövetség tagjai alkalmazzák, így pusztán ez alapján nem lehet eldönteni, hogy az Egyesült Államok, Nagy-Britannia, Ausztrália, Új-Zéland, vagy Kanada állt az akció mögött. **Bővebben...**

Oroszország lehet a felelős az izraeli reptér ellen irányuló támadásért?

(securityaffairs.co)

Izrael Oroszországot vádolja a Ben Gurion reptéren tapasztalt GPS jelek forgalmában keletkezett zavarokért, a Kreml azonban tagadja a vádakat. Június elejétől többször is megszakadt a Ben Guiron reptér forgalmának GPS jelátvitele, amely bár nem okozott balesetet, mégis „jelentős hatást gyakorolt" a reptér működésére ─ állítja a reptéri hatóság. Az orosz izraeli nagykövet elmondása szerint Oroszország nem hajtott végre támadásokat a reptér ellen, a vádakat dezinformációnak titulálta, amelyeket szerinte nem lehet komolyan venni. A szakértők vizsgálatai alapján a GPS rendszerbe történő beavatkozás kizárólag a légtérben közlekedő gépek esetén okozott zavarokat, pontatlan helyadatokat eredményezve ─ derült ki a BBC cikkéből. **Bővebben...**

Javíthatatlan hibát fedeztek fel egy népszerű PGP kulcsszerver hálózatban

(heise.de)

Alapjaiban kérdőjeleződött meg a titkosított levelezést lehetővé tévő OpenPGP egy népszerű kulcsszerver hálózatának (Synchronizing Key Server – SKS) használhatósága. Ismeretlen személyek ugyanis egy célzott támadás során képesek voltak a PGP közösség két prominens személyének (Robert J. Hansen és Daniel Kahn Gillmor) kulcsait „kompromittálni" oly módon, hogy azokat több százezer aláírással látták el. A problémát ezzel kapcsolatban az jelenti, hogy az ilyen, módosított kulcsok importálása a GnuPG kliensek elérhetetlenségét okozzák. A legnagyobb gondot azonban az jelenti, hogy a sérülékenység hátterében egy tervezési hiba áll, amely biztonsági frissítéssel nem orvosolható. **Bővebben...**

Hitelesítési adatokat lop egy androidos horror játék

(bleepingcomputer.com)

Egy 50 000-es telepítéssel rendelkező androidos horror témájú játék igyekszik megszerezni a felhasználók Google és Facebook fiókjainak hitelesítési adatait, majd a régebbi Android verziójú eszközökön ezek birtokában adatgyűjtésbe kezd. A „Scary Granny ZOMBYE Mod" nevű alkalmazás egy valódi horrorjáték, a „Granny" sikerét igyekszik kihasználni, amely egy teljesen legális, jól működő applikáció. Az egyébként teljes értékű játékként is funkcionáló „Scary Granny" csupán két nappal a telepítést követően kezdi meg a kártékony működést. Az alkalmazás a telepítést követően engedélyeket kér, majd egy Google bejelentkezési felületnek álcázott adathalász oldalt jelenít meg, amely segítségével bejelentkezési adatokat képes szerezni. Az applikáció egy további kártékony funkcióval is bír, ugyanis olyan hirdetéseket jelenít meg, amelyek káros oldalakra irányítják a felhasználót. A Scary Granny június 27-én eltávolításra került a Play Store-ból.

IT biztonsági Tanács

Az Európai Unió intézményeinek Számítógépes Vészhelyzeti Reagáló Csoportja (CERT-EU), valamint a francia Nemzeti Kiberbiztonsági Ügynökség (ANSSI) egy ingyenes nyílt forrású CTI (Cyber Threat Intelligence) platformot adnak közre közösen, amely OpenCTI névre hallgat. A közösségi szemléletű portál lehetőséget ad a technikai, valamint a nem technikai CTI információk tárolására, rendszerezésére és vizualizációjára, szem előtt tartva a könnyű kezelhetőséget. A projekt jelenleg is fejlesztés alatt áll, így a készítők előszeretettel várják a visszajelzéseket.

Magas az űrbéli stratégiai eszközök kiber fenyegetettsége

(darkreading.com)

Az államilag szponzorált fenyegetési csoportok kritikus infrastruktúrák elleni támadásainak megnövekedett száma miatt kiberbiztonsági szakemberek a szatellit és űrhajózási rendszerek biztonságáért is aggódnak. A Chatham House nevű agytröszt (think tank) kutatása szerint ugyanis a civil társadalmak nevezett infrastruktúráktól való függése oly mértékű, ami háborús időszakban támadási felületet jelent, békeidőben pedig kémkedési kockázatot hordoz magában, amelyet csak fokoz, hogy a kibertérben indított műveletek a kinetikus támadásokhoz képest jóval alacsonyabb költséggel kivitelezhetőek. Napjainkban már több tucat nemzetállam rendelkezik valamilyen fokú űrbéli kapacitással. **Bővebben...**

Kiberbiztonsági Innovációs Ügynökségét állítanak fel Németországban

(www.euractiv.com)

Az Európai Bizottság elnöki tisztségének betöltésére jelölt Ursula von der Leyen ─ az Egyesült Államok Védelmi Minisztériumának kutatásokért felelős részlegének (DARPA) mintájára a német belügyminiszterrel közösen kezdeményezte a Kiberbiztonsági Innovációs Ügynökség (Agency for Innovation in Cybersecurity) létrehozását, azonban a központ kialakítása a Német Szövetségi Számvevőszék aggályai miatt utódjának feladata lesz majd. A német kormány honlapja szerint az ügynökség célja az ország digitális infrastruktúrájának kibertámadásoktól történő védelme „a technológiai innováció vezetésének biztosításával". Bár július 3-án megszületett a döntés az ügynökség lipcsei székhelyéről ─ amely a tervek szerint 100 új munkahelyet fog teremteni ─, még nem ismert, hogy a szervezet mikor kezdheti meg működését, és ehhez mekkora költségvetés áll majd rendelkezésére. **Bővebben...**

Fiatalkorúakat veszélyeztető Sextortion csaló levelekre figyelmeztet az FBI

(bleepingcomputer.com)

Az Egyesült Államok Szövetségi Nyomozó Irodája (FBI) július 3-án fiatalokat célzó Sextortion csaló levelek kapcsán tett közzé figyelmeztetést a Twitteren, amelyben arra kérik a felhasználókat, hogy ne osszanak meg magukról képeket és videókat olyanokkal, akiket nem ismernek a való életben. Az FBI hivatalos honlapján még májusban nyilvánosságra hozott leírás szerint a Sextortion levelek szövetségi bűncselekménynek minősülnek, amelyekkel fiatalkorúakat veszneknek rá különböző módszerekkel, hogy szexuális témájú képeket és videókat osszanak meg magukról az interneten. Ezek között szerepel a hízelgés, a gyengéd érzelmek táplálásának látszata, a zsarolás és a fenyegetőzés is. **Bővebben...**

Egy iráni APT csoport sérülékeny Outlook verziók ellen indított támadást

(heise.de)

Az amerikai kiber parancsnokság (Us Cyber Command) figyelmeztetést adott ki egy 2017-es Microsoft Outlook sérülékenységet (CVE-2017-11774) kihasználó támadási kampány miatt, amelynek hátterében az iráni kötődésű APT33 (vagy más néven Elfin) fenyegetési csoportot sejtik. Nem minden előzmény nélkül érkezett az információ, a USCYBERCOM már 2018 novemberében osztott meg olyan általuk azonosított malware mintákat a Virustotal-on, amelyek a biztonsági hiba kihasználását célozzák. Tavaly decemberben pedig a FireEye is jelezte, hogy az APT33 kollektíva a Ruler nevű nyílt forrású tesztelő eszköz segítségével támadásokba kezdett.