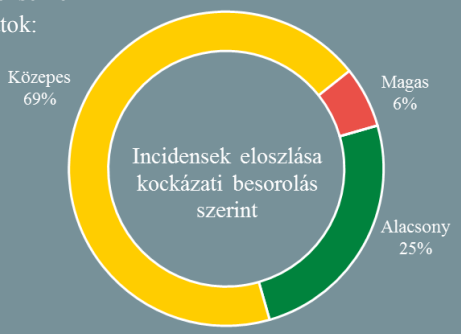
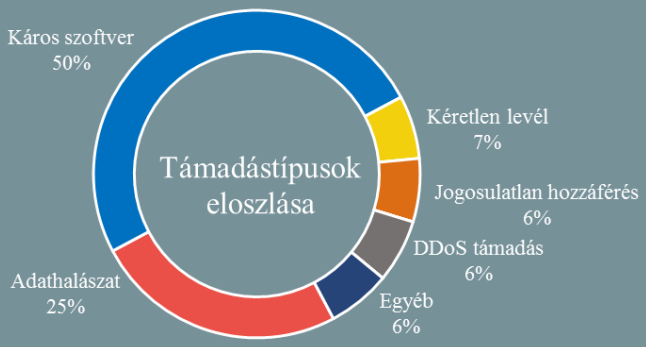
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.09.28. - 2019.10.03.





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

A BSI „IT vészhelyzeti" szolgáltatási csomagot adott ki kis- és középvállalkozások számára

(heise.de)

A német Szövetségi Információbiztonsági Hivatal (BSI) segíteni akarja a kis- és középvállalkozásokat az informatikai vészhelyzetekre való felkészülésben, ennek érdekében kifejezetten a KKV-k számára kialakított „informatikai vészhelyzeti" kártyát, valamint a vészhelyzetek kezelésére szolgáló útmutatókat adott közre. Az „IT vészhelyzeti" kártya felsorolja a munkavállalók számára legfontosabb információkat, tájékoztatást ad arról, hogy vészhelyzet esetén melyik telefonszámot kell tárcsázni, felsorolja azokat az adatokat, amelyekre a hívott félnek szüksége van (például a bejelentő neve, az érintett rendszerek, az incidens ideje és helye), és információt nyújt arról, hogyan kell a hívó félnek viselkednie (például abbahagynia a munkát, dokumentálni a megfigyeléseket). A három oldalas kezelési útmutató az informatikai biztonsági tisztviselőknek és az adminisztrátoroknak szól. **Bővebben...**

További fájlkiterjesztések kerülnek tiltásra a Webes Outlookon

(securityweek.com)

A Microsoft bejelentette, hogy bővíti azon fájlkiterjesztések körét, amelyeket mostantól blokkol a Webes Outlookon, azaz a felhasználók az ilyen kiterjesztéssel rendelkező csatolmányokat nem lesznek képesek letölteni. A tech óriás szerint ezek a mindennapok során kevésbé használtak, így a módosítás a legtöbb szervezet működésére nézve nem lesz hatással. A tiltott kiterjesztések egy része programozási nyelvekhez (PowerShell, Java) kötődik, azonban egyes windowsos alkalmazások kiterjesztései is érintettek, mint például a Windows Sandbox által alkalmazott „.wsb", valamint a digitális tanúsítványoké („.cer", „.crt" és a „.der"). Mindazonáltal kivételek beállítására is van lehetőség.

Újabb SIM kártyákat érintő súlyos sebezhetőségre derült fény

(securityaffairs.co)

A WIBattack a nemrég nyilvánosságra hozott Simjacker nevű, SMS-alapú támadás egy új variánsa. Néhány hete az AdaptiveMobile Security kutatói egy, a mobiltelefonok típusától és operációs rendszerétől független sebezhetőséget fedeztek fel, amely közel egy milliárd eszközt érinthet világszerte. A sebezhetőséget ezzel párhuzamosan egy másik biztonsági cég, a Ginno Security Lab is azonosította, akik egy további, hasonló célokat szolgáló modult (Wireless Internet Browser – WIB) is sérülékenynek találtak. A kihasználási mód is megegyező, egy speciálisan szerkesztett sms-sel a támadott készülék felett teljes kontroll szerezhető. **Bővebben...**

Windows biztonság: a Bitlocker a jövőben elkerüli a hardveres titkosítását

(heise.de)

A Windows beépített meghajtó titkosítója, a BitLocker a jövőben saját titkosítást használ ahelyett, hogy ezt az eszköz gyártójára bízná. Miután az adathordozók hardveres titkosításával kapcsolatban ismételten komoly biztonsági problémák merültek fel, a Microsoft drasztikus lépésre szánta el magát: a szeptember 24-én kiadott összesített frissítés részeként a BitLocker alapértelmezés szerint figyelmen kívül hagyja ezt a funkciót, ehelyett alapértelmezetten szoftveres titkosítást használ. Korábban a BitLocker inkább a hardver meglévő titkosítási szolgáltatásainak használatát választotta, és csak akkor gondoskodott a titkosításról, ha ez nem volt lehetséges. **Bővebben...**

Az Apple törölt egy hongkongi tüntetők által használt appot

(bbc.com)

Az Apple eltávolította alkalmazás áruházából a HKmap Live appot, ami a hongkongi tüntetők és rendőri egységek helyzetének nyomon követésére használható. Az alkalmazás a Telegramos üzenetek alapján jeleníti meg az információkat és többek között a könnygázosított régiókat is láthatják a felhasználók. Az Apple indoklása szerint az applikáció felhasználható a rendőri szervek kijátszására, ugyanakkor tisztázatlan, hogy a tiltás a kínai hatóságok direkt kérésére történt-e. A fejlesztők azzal védekeznek, hogy az applikáció célja csupán az informálódás elősegítése és nem az illegális felhasználás támogatása. Egyesek szerint az alkalmazás törlése az Apple részéről gesztus a kínai vezetés felé. Az app androi dos és webes verziója továbbra is elérhető.

IT biztonsági Tanács

Idén októberben is megrendezésre kerül az európai kiberbiztonsági hónap (ECSM), amely 2019-ben különböző témaköröket felölelve a tudatos online viselkedés kialakítására (kiberhigiénia), valamint a kialakulóban lévő technológiákra összpontosít. A kampány fő célja, hogy az európai felhasználók tisztában legyenek az online kockázatokkal, és ezeket számításba véve magabiztosan használják a digitális tér adta lehetőségeket.

A kiberhónapban zajló eseményekről és rendezvényekről a kiberhónap hivatalos magyar nyelvű weboldalán tájékozódhat, további érdekes információkért pedig kövesse a @kiberhónap Magyaroszág, illetve a @Nemzeti Kibervédelmi Intézet Facebook oldalt.

Teljes készültségben az iráni olajszektor

(securityweek.com)

Az iráni energiaügyi miniszter teljes készültséget rendelt el az ország olajipari vállalatai számára a lehetséges fizikai, valamint kibertérből érkező támadásokkal szemben. Bijan Namdar Zanganeh szerint a fokozott előkészületekre az Amerikai Egyesült Államok által folytatott „teljeskörű gazdasági háború" miatt van szükség, az iráni vezetés ugyanakkor tagadja a médiában megjelent híreket, amelyek szerint szeptember 21-én egyes iráni olajipari egységek kibertámadást szenvedtek volna. Mindeközben több nemzet is Iránt vádolja a szaúdi olajszektor ellen szeptember 14-én elkövetett, a termelésben jelentős visszaesést okozó támadásokért.

Komoly veszélyben a PDF file-ok biztonsága

(thehackernews.com)

Kutatók felfedeztek két új módszert, amelyekkel megkerülhetőek a PDF fájlok beépített védelmi mechanizmusai, a titkosítás és a jelszó védelem. Az összefoglalóan PDFex-nek nevezett támadás valójában nem a fájl feltörését teszi lehetővé, hanem azt, hogy a támadó távolról képes legyen kinyerni a fájl tartalmát. A PDFex támadás lehetővé teszi egy jelszóval védett enkriptált fájl módosítását oly módon, hogy amikor megnyitják a fájlt, az automatikusan elküld egy nem titkosított másolatot a támadó szerverére. A kutatók összesen 27, széles körben használt PDF olvasón tesztelték ezt a támadási technikát és mindegyiket sérülékenynek találták legalább egy módszerrel szemben. A sérülékeny szoftverek között megtalálható az Adobe Acrobat Reader, a Foxit Reader, az Okular, az Evince, továbbá a nagyobb böngészők beépített PDF olvasói is, köztük a Chrome-mal, a Firefox-szal, a Safarival és az Operával. A támadásról bővebb technikai információ a kutatók által készített weboldalon érhető el.

Kína új haditechnikai fejlesztései

(moderndiplomacy.eu)

Kína jelentős összegeket invesztál a kettős ─ mind civil, mind katonai ─ felhasználású technológiákba. Mindez Xi Jinping elnök két éve meghirdetett programjának megfelelően történik, amely 2035-ig a Kínai Népi Felszabadító Hadsereg teljes megújítását tűzte ki célul. Ennek mentén Kína 7.5%-ra emelte a katonai költségvetését, a kettős felhasználású kutatásokat pedig 13.4%-ra. Az amerikai hírszerzés szerint a legnagyobb támogatást jelenleg a mesterséges intelligencia (MI) kutatás, az e-számítási eszközök fejlesztése, a kvantumtechnológia és a hiperszonikus fegyverek fejlesztése kapja. Az MI és kvantumtechnológia által nyújtott elemzőképesség felhasználása a modern, többdimenziójú hibrid műveletek során elkerülhetetlenné válik, azonban mindez ─ a katonaitól egyre kevésbé elválasztható ─ civil politikai és stratégiai döntéshozói folyamatokra is érvényes. A Modern Diplomacy-n megjelent elemzés részletesen foglalkozik az aktuális Kínai technológiai törekvésekkel és a jövőbeli fejlesztési tervekkel. **Bővebben...**

Négy zsarolóvírushoz is elérhetővé vált dekriptor

(zdnet.com)

A FortuneCrypt, Yatron, WannaCryFake és az Avest zsarolóvírusok áldozatai számára jó hír, hogy visszaszerezhetik a titkosított fájlokat. A FortuneCrypt, Yatron, és Avest ransomware-ek által kódolt fájlok dekriptora a No More Ransom, a WannaCry telefonos verzióját WannaCryFake) visszakódoló program pedig az EMSISOFT weboldaláról érhető el.