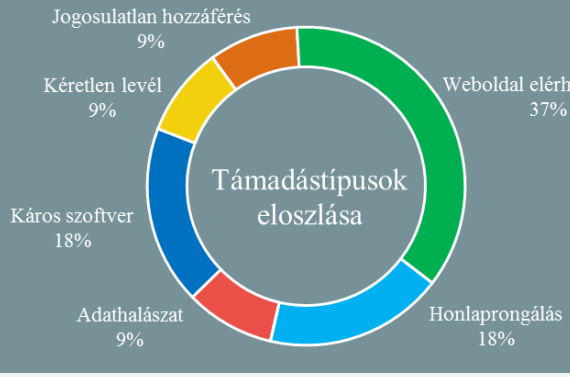
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.07.26. - 2019.08.01.



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

Politikai véleményformálásra használt fiókokat törölt a Facebook

(securityaffairs.co)

A Facebook blogján tette közzé, hogy a közelmúltban több oldalt, csoportot és felhasználói fiókot is törölt „nem hiteles viselkedés" miatt, köztük olyanokat, amelyeket vélhetően a július 21-i ukrán elnökválasztás befolyásolására hoztak létre. A Facebook négy, egymástól függetlenül zajló, a szavazók politikai érzelmeire hatást gyakorló kampányt azonosított, ezek közül hármat orosz APT csoportokkal hoznak összefüggésbe. A műveletek különböző témakörökre fókuszáltak, volt amelyik az ukrán polgárok véleményének befolyásolására koncentrált az orosz-ukrán viszony kapcsán, mások megosztó információkat terjesztettek például a thaiföldi politikáról, Kína és az Egyesült Államok között fennálló geopolitikai helyzetről, vagy például hongkongi tüntetésekről. Az elkövetők többféle eszközt is bevetettek, a hamis profilokat egyes esetekben korábban elhunyt ukrán újságírókat, vagy katonai személyeket megszemélyesítve hozták létre, a tartalmakat pedig hamis követőkkel igyekezték népszerűsíteni.

Bizonyos szolgáltatásokat már biometrikus azonosítással is el lehet érni Oroszországban

(ehackingnews.com)

Az oroszországi Irkutsk térségben már több, mint 70 bankfiók működik a Unified Biometric System (UBS) rendszert integrálva, amely lehetővé teszi egyes banki szolgáltatások távoli elérését arc és hang alapú azonosítás útján. A szolgáltatás igénybevételéhez egy személyes ügyintézés szükséges, ahol az ügyfeleknek az útlevelüket is be kell mutatniuk. A kliensek a regisztráció után telefonos megkeresés útján is nyithatnak számlát, indíthatnak átutalásokat, valamint vehetnek fel kölcsönt. A tervek szerint a szolgáltatások száma idővel bővülni fog, sőt, hamarosan a biztosítók is csatlakoznak. **Bővebben...**

Louisiana állam kormányzója zsaroló-vírus támadások miatt rendkívüli állapotot hirdetett

(zdnet.com)

Három észak-louisianai plébániához (Sabine, Morehouse, és Ouachita) tartozó iskolai körzet zsaroló-vírus támadás áldozatává vált, amelynek következtében az IT rendszerek leálltak. Ez a második alkalom, hogy egy kormányzó rendkívüli állapotot hirdet egy kibertámadás miatt, 2018 februárjában az amerikai Közlekedési Minisztérium coloradói kirendeltségének kellett felfüggeszteni működését SamSam ransomware támadás okán. A rendkívüli állapot célja minden esetben tartalék erőforrások felszabadítása a problémás területeken. **Bővebben...**

A Synology figyelmeztet: NAS termékeket támadnak zsarolóvírussal

(nakedsecurity.sophos.com)

A Synology figyelmeztetést adott ki NAS (hálózati adattároló – Network Attached Storage) termékek tulajdonosai számára, ugyanis a gyártó július 19-én egy NAS eszközöket célzó ransomware támadási kampányt azonosított. A cég szerint a támadók nem sérülékenységet használnak ki, hanem egy egyszerű ─ ám annál hatékonyabb ─ technikát alkalmaznak: a legnépszerűbb jelszavak felhasználásával, próbálgatás útján (brute force) igyekeznek hozzáférést szerezni az interneten keresztül elérhető eszközökhöz, majd egy zsarolóvírus futtatásával titkosítani az áldozat adatait. A Synology a támadások megelőzéséhez több alapfokú biztonsági beállítást is javasol, mint például hosszú és komplex jelszavak alkalmazását, valamint egy új fiók létrehozását az adminisztrátori csoportban az alapértelmezett „admin" fiók helyett. **Bővebben...**

SMS üzenetek útján terjed egy mobilokat fertőző zsarolóvírus

(bleepingcomputer.com)

Egy új androidos zsarolóvírus támadási módszert fedeztek fel, amely képes teljes hozzáférést szerezni a fertőzött eszközök névjegyzékéhez, majd káros hivatkozást tartalmazó SMS üzenetek útján tovább terjedni az áldozat kontaktjainak készülékére. Az Android/Filecoder.C (FileCoder) névre keresztelt zsaroló programot július közepén fedezte fel az ESET, ami akkor a Reddit-es XDA Developers mobil fejlesztői közösségen belül terjedt. A kártevő az ESET szerint Android 5.1, valamint ennél frissebb verziókra nézve jelent fenyegetést, azonban szerencsére hatása ─ a támadási kampány végrehajtásában, illetve a titkosító algoritmus implementálása során elkövetett hibák miatt ─ jelenleg korlátozott, ugyanis a titkosított fájlok helyreállíthatóak. **Bővebben...**

IT biztonsági Tanács

Az ausztrál kibervédelmi központ (Australian Cyber Security Centre – ACSC) kiadványa segítséget nyújthat a vállalkozások számára a szervezeti átalakítások idején jelentkező megnövekedett kiberbiztonsági kockázatok enyhítésére. A számos technikai kihívás mellett a kiadvány, az emberi tényező szerepével is foglalkozik, ugyanis az ilyen átmeneti időszakokban a szervezet munkatársai rá lehetnek kényszerítve arra, hogy a szokásos ügymenettől eltérő módon végezzék a munkájukat, és hajlamosabbak lehetnek a számukra ismeretlen személyektől érkező kérések teljesítésére. Emiatt kritikus fontosságú a dolgozók megfelelő tájékoztatása, mivel jó eséllyel találkozhatnak csaló üzenetekkel, hamis adat-, kifizetés és hozzáférési kérelmekkel, különösen, ha a különböző szervezeti egységek egymástól földrajzilag szeparáltan helyezkednek el.

LibreOffice felhasználók veszélyben

(thehackernews.com)

A Microsoft Office irodai programcsomag egyik legnépszerűbb nyílt forrású alternatívája a LibreOffice, amely több platformon (Windows, Linux, macOS) is elérhető. A program használóinak most javasolt különösen óvatosnak lenniük a gyanús csatolmányokkal, ugyanis egy jelenleg még javítatlan sérülékenység (CVE-2019-9848) miatt egy káros kódot tartalmazó dokumentum megnyitása a számítógép kompromittálásához vezethet. A biztonsági hiba a LibreLogo nevű beépített komponenst érinti, amely alapértelmezetten jelen van az irodai programban. A LibreLogo lehetőséget ad arra, hogy a felhasználó bizonyos események bekövetkezéséhez ─ például egérkattintás ─ grafikus elemeket rajzoló rövid szkripteket rendeljen. **Bővebben...**

Büntetés helyett új lehetőséget kaphatnak a fiatal kiberbűnözők Európában

(www.cyberscoop.com)

A Fordham Egyetemen megrendezett Nemzetközi Kiberbiztonsági Konferencián bemutatásra került a „Hack Right" elnevezésű kezdeményezés, ami mentesítené a 12 és 23 közötti korosztályt az első alkalommal elkövetett számítógépes bűncselekményekért járó büntetések alól, azokban az esetben, ha a gyanúsítottak számára nem volt felismerhető az általuk végrehajtott cselekvés illegális jellege. Floor Jansen, a holland rendőrség számítógépes bűnözéssel foglalkozó egység tanácsadója szerint az elkövetők motivációja mögött leginkább az új trükkök kipróbálása, vagy mások – például barátok – lenyűgözése áll azáltal, hogy ártalmatlan szándékkal megszerezik mások jelszavait. Az ilyen esetekben jellemző, hogy az elkövetők nem ismerik fel, hogy az általuk végrehajtott tevékenység társadalmi kontextusban illegálisnak minősül és az okozott károkat sem látják át azok online mivoltából adódóan. **Bővebben...**

Ismert sérülékenység ellenére árulta termékét a Cisco

(thehackernews.com)

A Cisco Systems 8,6 millió dolláros büntetést kapott, amiért annak ellenére tovább értékesítette kamerarendszerét amerikai szövetségi ügynökségeknek, hogy tisztában volt vele, a terméket több kritikus sérülékenység is érinti. Ez az első eset, hogy a „False Claims Act" alapján, kiberbiztonsági elvárásoknak történő nem megfelelés miatt szabnak ki büntetést. Az eset 2011-ben indult, amikor a Cisco egy volt alvállalkozója, James Glenn értesítette a szövetségi szerveket arról, hogy a Cisco Video Surveillance Manager (VSM) termékben évekkel korábban több sérülékenységet azonosított, amelyek azóta sem kerültek javításra. Glenn először 2008 októberében próbálta jelezni a problémát a vállalatnak, azonban akkori munkaadója, a Net Design röviddel ezt követően létszámleépítésre hivatkozva megvált tőle. **Bővebben...**

Új fenyegetési szereplő indít támadásokat közel-keleti olajcégek ellen

(securityaffairs.co)

A Dragos biztonsági szakértői nemrégiben egy új hacker csoportot azonosítottak, akik káros tevékenységeikkel leginkább földgáz- és olajipari szervezeteket, valamint telekommunikációs szolgáltatókat céloznak. A Hexane csoport 2018 közepe óta mutat aktivitást, ami idén, a közel-keleti régióban zajló konfliktusok hatására jelentősen fokozódott. Jellemzően kuvaiti földgáz- és olajipari vezérlő rendszererek (ICS), valamint a tágabb közel-keleti térségben, Közép-Ázsiában és Afrikában működő telekommunikációs szolgáltatók ellen hajtanak végre támadásokat. **Bővebben...**