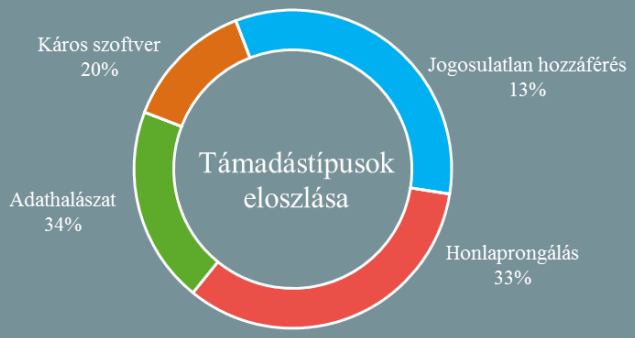
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.06.07. - 2019.06.13.



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

Mégsem annyira biztonságosak az elektronikus személyi igazolványok?

(ehackingnews.com)

Az észt Postimees napilap értesülései szerint hackerek visszaéléseket követtek el észt elektronikus személyi igazolványokkal. Az e-személyik egyre több országban könnyítik meg az állampolgárok életét, lehetővé téve az Interneten keresztül történő ügyintézést. Észtországban a polgárok ily módon már körülbelül 600-féle online szolgáltatást vehetnek igénybe, például lehetőségük van dokumentumok digitális hitelesítésére, vagy éppen mobil számla befizetésére. Mindennek alapja az a bizalom, hogy az e-személyi technológia megfelelő biztonságot szavatol, azaz nem hamisítható, amely azonban egy most kitudódott incidens miatt kérdésessé vált. 2019 februárjában ugyanis egy adathalász kampány során az ország egyik legnagyobb bankját megszemélyesítve a támadók azonosítókat csaltak ki észt polgároktól, amelyek birtokában képesek voltak új profilt regisztrálni a Smart-ID alkalmazásban, amivel számos szolgáltatáshoz hozzáférhettek.

Ki lesz Európa legnagyobb kiberbiztonsági tehetsége 2019-ben?

(www.enisa.europa.eu)

Már javában zajlik a felkészülés az immár hatodik alkalommal megrendezésre kerülő European Cyber Security Challenge (ECSC) 2019 uniós szintű kiberbiztonsági versenyre, amelyen a nemzeti versenyek győztesei képviselhetik majd országaikat. Míg egyes uniós tagállamok már sikeresen lefolytatták az országos fordulót, másoknál csak később kerül megrendezésre saját megmérettetésük. Az idén október 9. és 11. között Bukaresten megrendezésre kerülő ECSC 2019-en a versenyzőknek különféle kihívásokkal kell szembenézniük, többek között mobilbiztonsági, kódolási és dekódolási, valamint forensic feladatokat kell majd megoldaniuk. **Bővebben...**

Közeleg az ENISA-t újradefiniáló rendelet hatálybalépésének időpontja

(www.enisa.europa.eu)

Június 27-én lép hatályba az Európai Uniós Kiberbiztonsági Ügynökségről (ENISA) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről szóló, 2019/881-es számú rendelet. Ennek hatálybalépésével egy olyan új korszak veszi majd kezdetét, amelyben az ENISA az Európai Unió állandó megbízással rendelkező kiberbiztonsági ügynöksége lesz, az ezzel járó kiterjesztett feladatkörrel pedig a tervek szerint nagyobb támogatást lesz képes nyújtani az Uniónak.

Backdoort tartalmazó spamekre figyelmeztet a Microsoft

(zdnet.com)

A Microsoft figyelmeztetést adott ki egy európai felhasználók ellen zajló káros kód kampány miatt. Az e-mailek csatolmányaként egy .rtf kiterjesztésű dokumentum található, amelynek megnyitásakor több szkript segítségével egy trójai program települ a rendszerre, amely hátsó ajtót nyit azon. A tech cég szerint ez a fertőzési mód egy 2017 novemberében befoltozott MS Office sérülékenységet használ ki (CVE-2017-11882), azon felhasználók tehát védettséget élveznek, akik már feltelepítették a hibajavítást. A biztonsági frissítések időben történő telepítése ugyanakkor sok esetben elmarad, amely jelen sérülékenység esetében is releváns lehet, ugyanis – több beszámoló szerint is – ez 2018 egyik leggyakrabban kihasznált sérülékenysége volt. **Bővebben...**

Adathalász naptármeghívóval támadják a mobilfelhasználókat

(threatpost.com)

Újabb, ezúttal Gmail felhasználókat célzó adathalász kampány ütötte fel a fejét – derült ki Maria Vergelis, a Kaspersky egy kutatójának bejegyzéséből. A támadás során a mobileszközök képernyőjén megjelenő Google Naptár meghívó egy adathalász weboldalra mutató hivatkozást tartalmaz, amelyen hitelkártya- és egyéb személyes adatok megadására kérik a felhasználókat. A főleg májusban tapasztalt felugró ablakok formájában megjelenő linkek az adathalászaton kívül egyéb rosszindulatú tevékenységekhez is felhasználhatók, például káros kódok céleszközökre történő letöltésére. Vergelis elmondása szerint ezzel a fajta nem hagyományos támadási vektorral a támadók több áldozatot érhetnek el, szemben a sokak által már jól felismerhető e-mailben érkező adathalász módszerekkel. A kutató arra is rámutatott, hogy ily módon a Google egyéb szolgáltatásain (Photos, Hangouts, Ads, Analytics), de más szolgáltatókon keresztül is elvégezhető a támadás. **Bővebben...**

IT biztonsági Tanács

Egy új, ingyenesen elérhető online eszközt tett közzé az Egyesült Királyság Kiberbiztonsági Központja (NCSC).
Az „*Exercise in a Box*” névre keresztelt platform egy olyan e-learning felület, amely segítséget nyújthat a szervezetek számára a kiberbiztonsági fenyegetések és kockázatok megértéséhez, a biztonsági események kezelése során felmerülő hiányosságok felméréséhez, valamint a reagálási képességek fejlesztéséhez. A tanagyagok hasznos információkat nyújthatnak mind a kis-és közép vállalatok, valamint az állami és egyéb kormányzati szervek számára.

Veszélyesek a Németországban értékesített olcsó telefonok

(www.zdnet.com)

A számítógépes rendszerek biztonságáért felelős német szövetségi hivatal, a Bundesamt für Sicherheit in der Informationstechnik (BSI) figyelmeztetése alapján legalább négy – Doogee BL7000, M-Horse Pure 1, Keecoo P11 és a VKworld Mix Plus – Android alapú, alsókategóriás okostelefon-modellben azonosítottak beágyazott rosszindulatú hátsó ajtót (backdoor). Az Andr/Xgen2-CY névre keresztelt hátsóajtós trójai programot a Sophos Labs nevű kiberbiztonsággal foglalkozó brit cég fedezte fel még 2018 októberében. Az akkori információk szerint az uleFone S8 Pro okostelenfon egyik alapértelmezett alkalmazásában, a SoundRecorder-ben találták meg a kártékony szoftvert, amelynek célja a fertőzött telefonról való adatgyűjtés, a C&C szerverrel való kapcsolat felépítése, valamint a későbbi feladatok végrehajtása. **Bővebben...**

Újabb veszély leselkedik a távoli asztallal elérhető szerverekre

(threatpost.com)

Több, mint 1,5 millió Internet felől távoli asztal kapcsolattal (RDP) elérhető szerver ellen indított támadást a GoldBrute botnet hálózat az utóbbi napokban. Ennek során a célkeresztben lévő rendszerekhez gyakori és könnyen kitalálható hitelesítő adatok próbálgatásával igyekeznek hozzáférést szerezni, majd a sikeresen feltört szervereket GoldBrute malware-rel fertőzni és további kiszolgálók ellen felhasználni. Az alkalmazott módszer szerint a botnet minden tagja csupán egy felhasználónév-jelszó párost használ fel egy célpont ellen, amellyel vélhetően a detektálást igyekeznek elkerülni. A nemrég nyilvánosságra került, távoli kódfuttatásra lehetőséget adó BlueKeep sérülékenység mellett jelenleg a GoldBrute jelenti a legnagyobb fenyegetést a Windows rendszerekre nézve, azzal a megjegyzéssel, hogy utóbbi jóval egyszerűbben kihasználható.

Routolási hiba miatt Ismét Kína felé terelődött az Internetes forgalom

(zdnet.com)

Június 6-án az európai mobilinternet forgalom egy jelentős része több, mint két órán keresztül egy kínai internet szolgáltató (China Telecom) hálózatán keresztül haladt, a felhasználók ezáltal lassabb kapcsolatot, valamint egyes szerverek elérhetetlenségét tapasztalhatták. Az incidens abból fakadt, hogy a svájci Safe Host nevű kollokációs szolgáltatásokat nyújtó cég hibás útvonal választási (routing) információkat tett közzé. Nem ez az első alkalom, hogy az internet-szolgáltatók közötti forgalomirányításban használt Border Gateway Protocol (BGP) kapcsán probléma merül fel, sőt valójában gyakran lép fel hiba, annak ellenére, hogy az internet szolgáltatók különböző biztonsági intézkedésekkel folyamatosan igyekeznek csökkenteni a forgalmi hibák esélyét. **Bővebben..**

Komoly biztonsági hiba érinti az eTLS protokollt

(www.heise.de)

Hivatalosan is sérülékeny az Európai Távközlési Szabványosítási Intézet (ETSI) által fejlesztett Enterprise Transport Security (ETS, vagy eTLS) protokoll, amely a biztonságos Internetes kommunikációt lehetővé tévő TLS 1.3 alternatívájaként került volna bevezetésre. A Massachusettsi Műszaki Egyetem (MIT) február végén rendelt CVE számot (CVE 2019-9191) az ETSI szabványához, arra hivatkozva, hogy az eTLS nem rendelkezik a titkos kulcscserét lehetővé tévő Perfect Forward Secrecy biztonsági funkcióval. **Bővebben...**