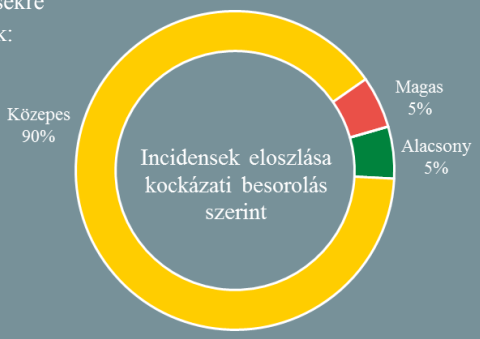
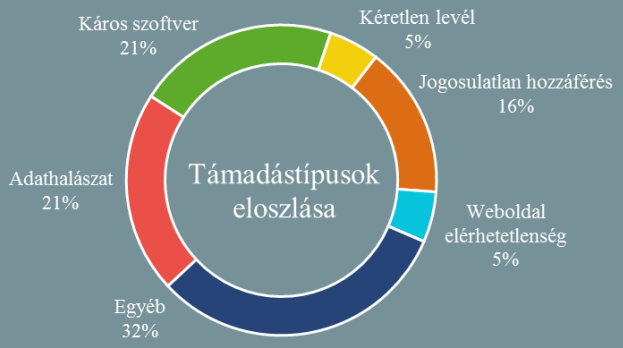
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 21. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.05.17. - 2019.05.23.





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

Újabb ENISA ajánlások az Ipar 4.0 kiberbiztonságának növeléséhez

(enisa.europa.eu)

Az EU kiberbiztonsági ügynöksége tavaly ősz után ismét tanulmánnyal jelentkezik (Challenges and Recommendations for Industry 4.0 Cybersecurity) a negyedik generációs ipar kiberbiztonsági kihívásainak áttekintéséhez, konkrét javaslatokat is téve a főbb problémakörök kezeléséhez. Az összefoglaló az ipar különböző kulcsszereplői – szabályhozók, biztonsági szakértők, üzemeltetők, valamint szabványügyi, akadémiai és K&F szervezetek – számára tartalmaznak hasznos információkat. Az anyag felhívja a figyelmet többek között az Ipar 4.0 szereplői közötti felelősségi körök tisztázásának szükségességére, az ellátási láncot érintő menedzsment folyamatok biztonságossá tételére, a biztonsági szabványok harmonizációjára, illetve a biztonsági célú interoperabilitás alapjainak kialakítására.

Több ezer Linksys router szivárogtat támadásra felhasználható adatokat

(securityaffairs.co)

A Bad Packets szerint egy régóta fennálló sérülékenység miatt több, mint 20 000 Linksys vezeték nélküli router szivárogtat információkat azon eszközökről, amelyek valaha is csatakoztak hozzájuk. Ezek az adatok – az eszközök egyedi azonosítói, nevei, valamint a telepített operációs rendszerre vonatkozó információk – pedig könnyen felhasználhatóak informatikai támadásokhoz, amire jó példa a nemrég nyilvánosságra került ASUS incidens. A kutatók a Binary Edge nevű, internetre csatlakoztatott eszközök felderítésére szolgáló keresőt használták a vizsgálat során, amivel összesen 25 617 routert, ezeken keresztül pedig több, mint 750 000 MAC címet derítettek fel. A fellelt eszközök közül ráadásul mintegy 4 000 esetében még az alapértelmezett felhasználónév-jelszó páros volt beállítva, ami jelentősen növeli a biztonsági kitettséget. **Bővebben...**

Egy Windows 10-et érintő nulladik napi sebezhetőségre derült fény

(zdnet.com)

A „SandboxEscaper” álnevet használó biztonsági kutató kihasználási bizonyítást (PoC) adott közre a GitHubon egy Windows 10-et érintő 0. napi sebezhetőségről. A hiba a Windows Task Schedulert érinti és abból fakad, hogy az nem megfelelően végzi a DACL (discretionary access control list) jogosultságok módosítását, ami egy speciálisan formázott *.job* file segítségével használható ki. A sebezhetőség lokális jogosultság kiterjesztésre (local privilege escalation – LPE) adhat módot, amelyet a hackerek adminisztrátori jogosultság szerzésére használhatnak fel miután egy rendszerhez hozzáférést nyertek. Mindeddig csupán 32 bites Windows 10-en tesztelték, azonban a ZDNet információi szerint elméletileg némi változtatás után bármelyik Windows verzión működhet. **Bővebben...**

A Microsoft egyes applikációk tiltását javasolja

(ehackingnews.com)

A Microsoft még áprilisban közölt egy listát néhány olyan legális alkalmazásról, amely potenciálisan felhasználható a Windows Defender kijátszására. Előfordul ugyanis, hogy a támadók a vállalatok által használt legitim szoftverek – védelmi programok, admin tool-ok – kijátszásával valósítják meg a támadást (lásd: living-off-the-land taktika). A magas biztonsági kockázat miatt a tech óriás azt javasolja, amennyiben nincs kifejezett szükség a közleményben felsorolt alkalmazások elérésére, javasolt a tiltásuk a Windows Defender Application Control (WDAC) segítségével. Mindezek mellett felhívják a figyelmet a biztonsági frissítések telepítésének fontosságára.

Már Androidon is elérhető a Tor Browser

(bleepingcomputer.com)

A Tor Projekt bejelentése szerint elérhetővé vált a Tor Browser stabil verziója a Google Play-en. A cég azért döntött az androidos kiadás elkészítése mellett, mert sok országban szigorú a kormányzati felügyelet és az online cenzúra, a mobil készülékek pedig sok esetben az internethez való csatlakozás egyetlen lehetséges módját jelentik. Habár az androidos verzió jelenleg még nem tartalmazza az asztali kiadások összes funkcióját ─ mindez itt követhető nyomon ─ a fejlesztők szerint lényegében ugyanazon védelmet képes biztosítani. A cég közleménye arról is említést tesz, hogy az Apple szigorú megkötései miatt böngészőjük nem lesz elérhető iOS-en, így alternatívaként az iOS felhasználók számára az Onion Browser használatát javasolják.

IT biztonsági Tanács

A Tenable elérhetővé tette sérülékenység vizsgáló szoftvercsaládjának ingyenes otthoni kiadását, Nessus Essentials néven.

Az ilyen szoftverek segítségével felmérhetőek és azonosíthatóak egy adott infrastruktúrát érintő sérülékenységek.

A szoftverrel összesen 16 IP cím szkennelhető, a professzionális változattal megegyező sebességgel.

Az ingyenes változat korábban Nessus Home néven volt ismert, amely azonban kizárólag személyes használatra adott módot, ami az új változatra már nem vonatkozik, azaz például oktatási célra is felhasználható.

Az Europol koordinálásával felszámolták a GozNym hálózatot

(cnet.com)

Nemzetközi összefogással sikerült megszüntetni egy kiberbűnözői hálózatot, amely a GozNym malware-t felhasználva próbált összesen mintegy 100 millió dollárt ellopni 41 000 áldozattól. Az Europol szerint az eset jó példa a cybercrime-as-a-service (CaaS) alapú szerveződésre, ami azt jelenti, hogy a GozNym hálózat különböző technikai képességeket és kiberbűnözői szolgáltatásokat áruló szereplők felbérlésével jött létre. Ennek részét képezte például a tartalom felügyelet nélküli tárhely szolgáltatás (bulletproof hosting), kódolók, „pénzöszvérek” (money mule), valamint kripterek alkalmazása és spamelés. A nyomozás párhuzamosan több országban ─ Bulgária, Georgia, Moldova és Ukrajna ─ zajlott, végül összesen 10 személy ellen emeltek vádat. Közülük öten Oroszországban tartózkodnak, jelenleg is menekülve az igazságszolgáltatás elől.

Kiberbűnözési információk egy rendszerben

(www.ehackingnews.com)

Az orosz belügyminisztérium egy közös adatbázisba gyűjtené a kiberbűnözéssel kapcsolatos valamennyi rendelkezésre álló információt. A rendszer a kiberfenyegetési információk automatizált begyűjtése mellett állampolgári bejelentéseket is kezelne, amelyeket telefonon, e-mailen, közösségi oldalakon, üzenetküldő alkalmazásokon és SMS-en keresztül is képes lesz fogadni. A portál ─ amelyhez a polgárok és kormányzati szervek ingyenesen férhetnek majd hozzá ─ egyes, már meglévő állami adatbázisokkal is frissítésre kerül, mint például az Egységes Biometrikus Rendszer és a Közszolgáltatási Portál. A fejlesztésért felelős Data Economy által benyújtott tervezet jelenleg a Minisztertanács jóváhagyására vár, amelynek finanszírozására a következő hat évre 1,5 milliárd rubelt határoztak meg.

G Suite jelszavak voltak veszélyben hosszú éveken keresztül

(techcrunch.com)

A Google egy téves beállítás miatt 2005 óta egyszerű szöveges formában tárolta egyes G Suite ügyfeleinek jelszavait. Suzanne Frey, a kereső óriás alelnöke kedden számolt be a biztonsági hibáról, és bár az nem derült ki, hogy mindez pontosan hány G Suite ügyfelet érint, állítása szerint a Gmail felhasználók körében nem volt érintettség az ügyben. A probléma hátterében az állt, hogy a G Suite adminisztrátorok képesek manuálisan új jelszavakat beállítani a vállalati felhasználóknak, ami kifejezetten hasznos dolog például egy új munkatárs érkezésekor, azonban ─ mint kiderült ─ az eljárás hibás implementálásából fakadóan a jelszavakból egy példány titkosítás nélkül került tárolásra. **Bővebben...**

A Google a Gmail-en keresztül követheti nyomon online vásárlásainkat

(www.cnbc.com)

A Google minden olyan online vásárlást ─ valamint foglalási és előfizetési tranzakciót ─ rögzít, amelynél a felhasználók Gmail-es e-mail címet állítanak be a visszaigazoló e-mailek fogadására, attól függetlenül, hogy maga a vásárlás milyen szolgáltatásokon vagy alkalmazásokon keresztül történt. A felhasználók a fiókjukba történő bejelentkezést követően a „Fizetés és előfizetések” menüben a „Vásárlások”, „Előfizetések” és „Foglalások” menüpontok alatt ellenőrizhetik ezeket az ─ akár évekre visszamenőleg tárolt ─ adatokat. **Bővebben...**