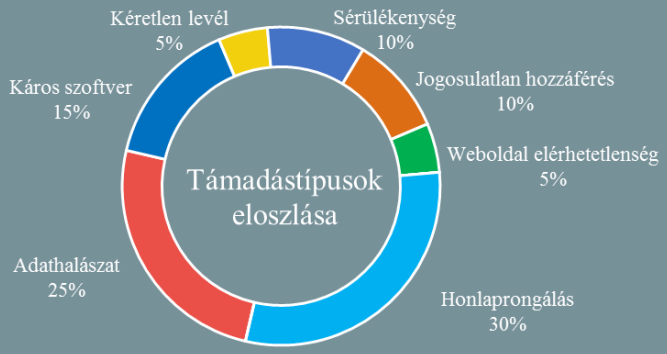
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.08.02. - 2019.08.08.



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

Inkább takarja le a kamerát – üzeni az orosz minőségbiztosítási hivatal

(www.ehackingnews.com)

Az orosz termékek és szolgáltatások minőségbiztosításával foglalkozó szerv, a Roskachestvo felhívja a figyelmet a digitális higiénia fontosságára. Ennek kapcsán több javaslatot is megfogalmaztak: a vírusirtók és az alkalmazások naprakészen tartása mellett például erősen javasolják a digitális eszközök kameráinak és mikrofonjainak lefedését, amikor azok nincsenek használatban. Erre a célra megfelelő egy hagyományos, vagy szövetbetétes ragasztószalag, vagy egy speciális függöny. A kép- és hangrögzítő eszközök eltakarását az olyan kémszoftverek miatt tartják indokoltnak, mint a hírhedt Pegasus, amelyek képesek távolról aktiválni a rögzítő funkciókat, még akkor is ha az alkalmazások számára a felhasználó letiltja a kamerához és a mikrofonhoz történő hozzáférést. **Bővebben...**

Útmutató készül a .zip tömörítés biztonságos használatához

(cyberscoop.com)

Az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete (NIST) hamarosan nyilvánosságra hozza útmutatóját a .zip kiterjesztésű tömörített fájlok biztonságosabb módon történő megosztására vonatkozóan ─ derült ki egy, a CyberScoop birtokába jutott levélből. Az útmutató elkészítését Ron Wyden amerikai szenátor kezdeményezte júniusban, arra hivatkozva, hogy a kormányzati alkalmazottak abban a tévedésben használják a .zip fájlokat érzékeny információk e-mailben történő megosztásra, hogy a tömörítő programok beépített titkosító funkciói megfelelő védelmet nyújtanak, ugyanakkor a valóban biztonságos ingyenes eszközökről és módszerekről nem szereznek tudomást. **Bővebben...**

Újabb sérülékenységet azonosítottak az új WPA3 protokollban

(thehackernews.com)

Az egy évvel ezelőtt bemutatott WiFi Protected Access III (WPA3) protokoll újításai között szerepel a korábbi WPA2-es szabványhoz képest biztonságosabb kapcsolat felépítést lehetővé tévő, ezáltal az offline szótár alapú támadásokkal szemben védelmet nyújtó SAE (Simultaneous Authentication of Equals) eljárás, vagy más néven Dragonfly. Mathy Vanhoef és Eyal Ronen biztonsági szakemberek azonban a szabvány megjelenését követően kevesebb, mint egy éven belül máris több súlyos biztonsági problémát azonosítottak (DragonBlood), az akkor felfedezett side-channel információ szivárgás sérülékenységek például lehetővé tették a Wi-Fi jelszavak kinyerését. **Bővebben...**

Újabb iskolákat ért kibertámadás az Amerikai Egyesült Államokban

(securityaffairs.co)

Az amerikai iskolák ellen zajló támadási hullám tovább folytatódik, ezúttal Alabamában, a houston megyei iskolakörzet intézményei számára okozva fennakadásokat, egy kiterjedt káros kód támadás következtében ugyanis az augusztus elsejére tervezett évnyitót nyolcadikára kellett halasztani. A támadással kapcsolatban mindössze annyi ismert, hogy a fertőzés az iskolák teljes számítógépes hálózatát érintette, emellett a telefonos rendszerek is elérhetetlenné váltak. Habár a problémát okozó vírusról nem közöltek részleteket, feltételezések szerint egy zsarolóvírus okozhatta a fertőzést. Az iskolák a kiberbűnözők számára kiemelt célpontnak számítanak, egyrészt a nagy mennyiségű személyes adat, másrészt a megfelelő kiberbiztonsági „higiénia” hiánya miatt.

Wi-Fin keresztül hackelhetők az androidos telefonok

(thehackernews.com)

Több kritikus sérülékenységet azonosítottak Qualcomm chipsetekben, amelyek lehetővé tehetik a Wi-Fi hatókörben lévő androidos eszközök kompromittálását, bármiféle felhasználói interakció nélkül. A Tencent Blade biztonsági kutatói fedezték fel a Qualcomm chipek WLAN és modem firmware-ét érintő sebezhetőségeket, amelyekre összefoglalóan **QualPwn**-ként hivatkoznak. Ez alatt egészen pontosan két Qualcomm chipet érintő kritikus sérülékenységet (CVE-2019-10539, CVE-2019-10540), valamint a Qualcomm Androidhoz készült Linux kernel driverét érintő sebezhetőséget (CVE-2019-10538) értik. Ezek együttes kihasználásával a támadó teljes irányítást nyerhet a támadott Android eszközök felett. Habár a kutatók csupán a Qualcomm Snapdragon 835 és Snapdragon 845 chipekkel ellátott Google Pixel 2 és Pixel 3 eszközökön tesztelték a QualPwn támadást, a biztonsági probléma a Qualcomm által kiadott számos további chipsetet is érint. **Bővebben...**

IT biztonsági Tanács

Az Egyesült Királyság kiberbiztonsági központja, az NCSC ajánlást adott közre egy alapszintű windowsos biztonsági monitoring rendszer összeállításához.

A „Logging Made Easy” (LME) összefoglaló alapján egy felhasználókat és szervereket is érintő naplózási megoldást nyerhetünk nyílt forrású, ingyenes eszközök felhasználásával. Minderről bővebb információt az NBSZ NKI weboldalán itt találhat.

Pusztító malware terjed Németországban

(zdnet.com)

A múlt hét során egy új zsarolóvírus kezdett pusztítani Németországban. A GermanWiper nevű ransomware, bár zsaroló üzenetet jelenít meg, valójában nem titkosítja a fájlokat, hanem a tartalmukat teleírja nullákkal (0x00), ezzel helyreállíthatatlanul roncsolva őket. Kihangsúlyozandó tehát, hogy az áldozatnak semmiképp nem szabad kifizetnie a váltságdíjat, mivel amennyiben a fertőzés bekövetkezett, a fájlok helyreállítása csupán offline biztonsági mentés megléte esetén lehetséges. A malware eddig csupán német nyelvterületen ütötte fel a fejét, ezen belül elsősorban Németországban. Itt ugyanakkor egyre több felhasználót érint a fertőzés, az ID-Ransomware statisztikája szerint jelenleg az öt leggyakoribb káros kód között szerepel. **Bővebben...**

Külsős alkalmazottakkal ellenőrizteti a Microsoft a Skype Translatoráltal végzett fordításokat

(vice.com)

A Microsoft egyes szerződéses partnerei privát Skype beszélgetésekhez férnek hozzá ─ derül ki a Motherboard birtokába jutott belső anyagokból. Habár a Skype weboldalán szereplő információk szerint a cég 2015-ben bevezetett, mesterséges intelligenciát alkalmazó fordító szolgáltatásának (Skype Translator) javítása érdekében hanganyagokat gyűjthet elemzés céljából, azonban arról már nem ad tájékoztatást, hogy ez részben humán erőforrással történik. Ennek során a munkatársak egy audio anyagot kapnak fordításra, majd ezt össze kell hasonlítaniuk több gépi verzióval, és ki kell választaniuk a legpontosabbat. A Motherboard birtokába jutott hanganyagok között több kifejezetten személyes témájú beszélgetés is megtalálható, egyes fájlok emellett a Microsoft személyi asszisztens programjának, a Cortanának kiadott hangparancsokat is tartalmaznak. **Bővebben...**

Az RDP kliensek egy korábban felfedezett sérülékenysége a Hyper-V Manager-t is érinti

(vice.com)

A Check Point Research szerint több millió Microsoft Azure felhasználó válhatott támadhatóvá a távoli asztal elérést biztosító Remote Desktop Protocol (RDP) egy sérülékenysége miatt. A biztonsági cég tavaly februárban 25, RDP klienseket érintő sérülékenységet azonosított, azonban ─ mint most kiderült ─ ezek közül egy könyvtárbejárás támadásra módot adó sebezhetőség a Microsoft felhő alapú platformján, az Azure-on is alkalmazott Hyper-V virtualizációs megoldásnál használt kliens szoftver (Hyper-V Manager) esetében is érvényes. Ennek oka az, hogy a vendég és a hoszt környezet közötti vágólap szinkronizálás lehetővé tételéhez a Microsoft az RDP-hez korábban már kialakított funkciókat emelte át. **Bővebben...**

0-day sérülékenységet találtak egy népszerű játékkliensben, azonban úgy tűnik nem kerül javításra

(bleepingcomputer.com)

A közel 100 millió regisztrált felhasználóval bíró videojáték kliens, a Steam windowsos változatában nulladik napi (0-day) sérülékenységet fedeztek fel, amelynek kihasználása lehetővé teheti, hogy a támadó adminisztrátori jogosultságot szerezzen. A sebezhetőség abból fakad, hogy a kliens „SYSTEM” jogosultsággal futtatja a „Steam Client Service” folyamatot, amely ugyanakkor elindítható és leállítható „USER” szintű jogosultsággal is. **Bővebben...**