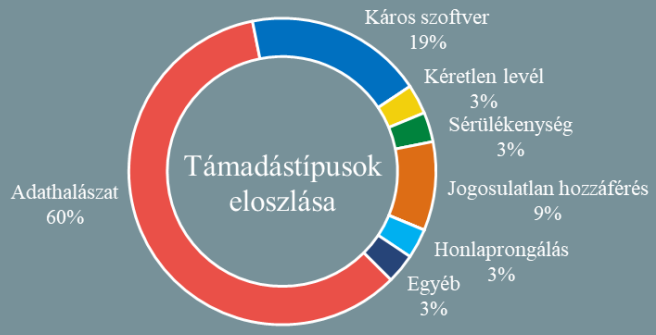
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 22. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.05.22. - 2020.05.28.



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

Orosz szakértők átfogó vizsgálatot folytattak a vállalatok IT-biztonsági védelmi szintjéről

(ehackingnews.com)

A Positive Technologies vizsgálatából az derült ki, hogy még az alacsony szintű tudással rendelkező hackerek is be tudnak törni a legtöbb vállalat hálózatába, egy tapasztalt támadó pedig akár fél óra alatt is képes lehet erre. A vizsgálatok részeként végzett penetrációs tesztek során a szakértők a vállalatok 93%-a esetében hozzá tudtak férni a céges rendszerekhez és kiderült az is, hogy minden hatodik cég esetében azonosítottak támadásra utaló nyomokat, káros linkek vagy kiszivárgott fiók információk formájában. **Bővebben...**

StrandHogg 2.0: Több, mint 1 milliárd androidos telefon appjai hackelhetők

(thehackernews.com)

Norvég kiberbiztonsági szakértők tavaly közöltek információt a Strandhogg-nak elnevezett androidos sérülékenységről, amelynek kihasználásával rosszindulatú applikációk képesek lehetnek a támadott telefonra telepített legitim appok interfészét utánozni, ezzel megtévesztve a felhasználót. A biztonsági problémát felfedező kutatók azonban most egy újabb, hasonló sérülékenységet hoztak nyilvánosságra (CVE-2020-0096), amely még kiterjedtebb kihasználást tesz lehetővé. A biztonsági problémát felfedező kutatók azonban most egy újabb, hasonló sérülékenységet hoztak nyilvánosságra. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat arra vonatkozóan, hogy a 2004-es sorszámú Windows 10 verzió már támogatja a Wi-Fi 6 szabványt.

Virtuális géppel támad a Ragnar ransomware

(securityaffairs.co)

Újabb zsarolóvírus támadási módszert fedezett fel a Sophos biztonsági cég, amelynek segítségével a Ragnar Locker zsarolóvírus képes kijátszani egyes vírusvédelmi szoftvereket. A Ragnar a támadás kezdetén előbb egy Oracle VirtualBox Windows XP környezetet telepít, majd a mappamegosztás segítségével titkosítja a hoszt környezetben található fájlokat. Ilyen támadás érte az Energias de Portugal (EDP) portugál energiaszolgáltatót, amitől a hírek szerint mintegy 10 terányi adatot loptak el. Fontos kiemelni, hogy az ilyen támadásokkal szemben védelmet jelenthet, amennyiben az áldozat hoszt rendszere Windows 10, amin a **Controlled Folder Access** védelmi funkció aktiválva van, ez ugyanis megakadályozhatja, hogy a védett könyvtárak titkosításra kerüljenek.

Álomdnak-e az androidok egységes szintű biztonságról?

(blog.f-secure.com)

Több F-secure tanulmány is arra az eredményre jutott, hogy egyes gyártók esetében (Samsung, Huawei, Xiaomi) ugyanazon készülékek eltérő biztonsági kockázatot jelentenek, attól függően, hogy melyik régióban kerülnek forgalomba. A különbségek elsősorban eltérő alapértelmezett konfigurációkból fakadnak, amelyek attól függően is változhatnak, hogy a készülékbe milyen SIM kártyát helyeztek be. Kínában a Google Play Store tiltása miatt a gyártók saját alkalmazásboltokat üzemeltetnek, amilyen például a Huawei AppGallery. **Bővebben...**

Az eBay portszkenneli a weboldalát látogató felhasználók gépét

(bleepingcomputer.com)

Az eBay weboldalán egy szkript (check.js) lokális portszkennelést hajt végre a látogatók gépén, olyan nyitott portok után kutatva, amelyek távoli támogatást vagy hozzáférést biztosító applikációk jelenlétére utalhatnak. A vizsgált portok — összesen 14, részletes lista a cikkben található — olyan alkalmazásokhoz kötődnek, mint például a Windows Remote Desktop, VNC, TeamViewer, Ammy Admin. A portscan tényét a BleepingComputer saját teszteléssel is megerősítette. Az esetre fényt derítő Nullsweep szerint ugyanakkor Linux alól betöltve az oldalt, már nem fut le a szkript. **Bővebben...**