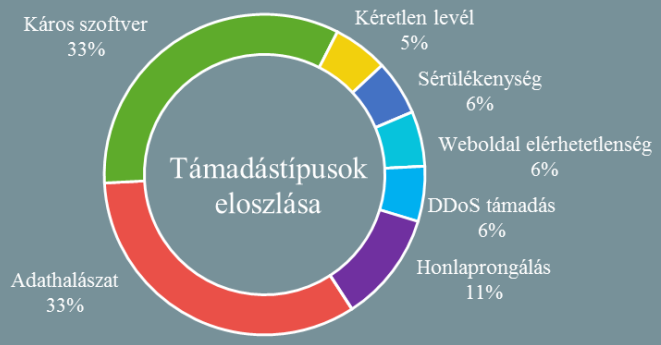
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 22. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.05.24. - 2019.05.30.



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

Az Egyesült Királyság NATO ellen végrehajtott kiberműveletekkel vádolja Oroszországot

(securityaffairs.co)

Az Egyesült Királyság 16 NATO szövetséges országgal osztott meg bizonyítékot arra vonatkozóan, hogy Oroszország az elmúlt 18 hónap során kibertámadást indított ellenük. Jeremy Hunt brit külügyminiszter elmondása szerint az orosz hírszerző apparátus „globális kampányt" folytat a kritikus infrastruktúrák, valamint a központi kormányzati hálózatok ellen, a dezinformációs műveletekkel pedig az Egyesült Államok és Ukrajna választási folyamatait kívánták befolyásolni. Hunt szerint mindezzel megsértették a nemzetközi jogot, ami arányos reakciót tesz indokolttá. **Bővebben...**

Közel egymillió Windows rendszer van veszélyben

(zdnet.com)

Közel egymillióra tehető az interneten keresztül közvetlenül elérhető, BlueKeep (CVE-2019-0708) sérülékenységben érintett Windowsos PC-k száma. A kezdeti becslések több, mint 7 millió potenciálisan érintett eszközről szóltak, azonban mint kiderült a valós szám ennél alacsonyabb, körülbelül 950 000. Ennek oka az lehet, hogy a legtöbb esetben a nyitott 3389-es (alapértelmezett RDP) port nem Windowsos rendszerhez tartozik, vagy azon nem távoli asztal szolgáltatás érhető el. Valós támadásokról mind ez idáig nincs információ, vélhetőleg mert a sérülékenység kihasználására bizonyítás (proof-of-concept) még nem került publikálásra. Robert Graham, a sérülékeny eszközöket felderítő tool (rdpscan) készítője szerint azonban csupán idő kérdése, hogy a támadók saját kihasználási eljárásokkal támadásba kezdjenek. **Bővebben...**

Zsarolóvírussal támadnak MySQL szerverekre

(zdnet.com)

A Sophos felfedezése szerint (legalább) egy kínai hacker csoport olyan, az interneten keresztül elérhető MySQL adatbázisok után kutat, amelyek Windows-os szerveren futnak, mindezt abból a célból, hogy azokat GandCrab zsarolóvírussal fertőzzék meg. Habár korábban ilyen jellegű támadásokra nem volt példa, és a felfedező szerint ez a művelet sem nevezhető széleskörűnek ─ az elmúlt napokban körülbelül 800 alkalommal töltötték le a vírust ─ az eset jó példa arra, hogy miért nem javasolt a MySQL adatbázisok távoli menedzselését az alapértelmezett 3306-os TCP port megnyitásával végezni. Andrew Brandt, a Sophos kutatója lett figyelmes ezekre a támadásokra, amelyekről bővebb információt a Sophos weboldalán közölt.

URL hamisítást tesz lehetővé a DuckDuckGo mobil böngésző sérülékenysége

(www.bleepingcomputer.com)

A DuckDuckGo mobil böngésző androidos verziójának egy hibája lehetővé teszi, hogy egy új weboldal betöltésekor az URL módosuljon a megadottra, azonban maga a HTML oldal ne töltődjön be. Mindez alkalmas lehet a felhasználók megtévesztésére, ugyanis a weboldal tartalma nem fog megegyezni a címsorban szereplővel. A problémát felfedező Dhiraj Mishra biztonsági kutató a HackerOne hibavadász (bug bounty) program keretében 2018. október 31-én jelentette a sérülékenységet (CVE-2019-12329) a böngésző biztonsági csapatának, amelyet 2019. május 27-ig magas biztonsági besorolással kezeltek. **Bővebben...**

Az Apple korlátozná az online hirdetések segítségével történő profilalkotást

(techcrunch.com)

Az Apple a közeljövőben új technikai megoldást vezet be a Safari böngészőben, a nyomkövető sütik (tracking cookies) használatával történő felhasználói profilalkotás megakadályozására. A tech óriás egy szerdai blog bejegyzésében arról írt, hogy a hirdetőknek nem szükséges személyhez kötniük a vásárlásokat, elegendő annyit tudniuk, hogy valaki egy hirdetésre kattintva egy online áruházban vásárolt valamit, ezáltal védve a felhasználók identitását, miközben a hirdetőknek sem kell lemondaniuk a hatékony hirdetési kampányokról. A „Privacy Preserving Ad Click Attribution" névre keresztelt technológia mindezt négy fő intézkedéssel valósítaná meg: a kampányazonosító számok korlátozásával meg kívánja akadályozni, hogy a hirdetők egyedi követési kódokat rendeljenek hozzá a felhasználókhoz; a hirdetésekre történő kattintások mérését kizárólag azon weboldalak számára engedélyezné, amelyeken elhelyezték magát a hirdetést. **Bővebben...**

IT biztonsági Tanács

Amennyiben fontos távoli elérést biztosítani MySQL adatbázisunkhoz, alkalmazzuk az alábbi biztonsági intézkedéseket:

- **ne** az **alapértelmezett** TCP portot (**3306**) használjuk,
- a távoli elérésű felhasználói fiókokhoz állítsunk be **fix IP címet** (whitelist),
- bizonyosodjunk meg arról, hogy nincsenek **névtelen felhasználók** (anonymous user),
- tiltsuk le a **root** felhasználóval történő távoli elérést, a többi felhasználó pedig csak **a saját adatbázisához férjen hozzá**,

További javaslatokat weboldalunkon itt talál.

A kínai hadsereg az amerikai kiberfenyegetéstől tartva lecseréli a Windowst

(zdnet.com)

Bár hivatalosan még nem került megerősítésre, a kanadai Kanwa Asian Defense nevű katonai magazin információi szerint a fokozódó kereskedelmi háború és politikai feszültség közepette Peking saját operációs rendszer fejlesztését rendelte el a kínai hadsereg számára. A Snowden, a Shadow Brokers és a Vault7 szivárogtatásoknak köszönhetően a kínai vezetés számára világossá vált, hogy az USA kiterjedt hacker képességei lehetővé teszik, hogy szinte bárhova behatoljon, az okostévéktől a Linux szerverekig, a routerektől az asztali PC-kig. A lehetséges kiberkémkedéstől tartva a kínai kormány a „bizonytalanságon alapuló biztonság" (security by obscurity) megközelítést választva döntött az egyedi fejlesztésű rendszerre váltásról, ami reményeik szerint megnehezíti majd a támadások kivitelezését. **Bővebben...**

Késhet a német közigazgatás 2022-re tervezett digitalizálása

(www.heise.de)

Németország közigazgatási szerveinek – helyi, tartományi és szövetségi szinten – fokozatosan, de legkésőbb 2022-ig át kellene térniük a digitális szolgáltatások nyújtására az ügyfajták nagy része esetében, azonban ez a cél nem biztos, hogy a tervek szerint fog megvalósulni. Az egyik ok a személyi erőforrások hiánya. A szövetségi belügyminisztériumban körülbelül negyven olyan állást kellene betölteni, amelyek szükségesek a szóban forgó munkafolyamatok elősegítéséhez. Egyes vélemények szerint az említett problémához az ország közigazgatási tagoltsága is hozzájárul, ezért a települési önkormányzati, tartományi, illetve szövetségi szervek szorosabb együttműködésére lenne szükséges a kérdésben. Borúlátóbbak úgy vélik, hogy a szóban forgó nehézségek miatt egyáltalán nem is fognak sikerülni a közigazgatás átfogó digitalizálásának tervei.

MS SQL és PHPMyAdmin szerverek veszélyben

(zdnet.com)

A Guardicore Labs kiberbiztonsági kutatói egy MS-SQL és PHPMyAdmin szerverek ellen zajló cryptojacking támadási hullámról adnak hírt. A Nansh0u névre keresztelt malware terjesztő kampány során ─ vélhetően kínai hackerek ─ már közel 50 000 szervert fertőztek meg. A támadók először nyilvánosan elérhető szerverek után kutatnak, amelyeknél próbálgatás útján (brute force attack) igyekeznek hozzáférést szerezni a gyenge jelszóval védett admin fiókokhoz, majd többféle káros kód segítségével TurtleCoin vagy Monero kriptovalutát bányászó malware-t telepíteni a kompromittált rendszerre. A kutatók szerint a támadás atipikus abban a tekintetben, hogy a támadók APT csoportokra jellemző kifinomult technikákat is alkalmaznak: jogosultságkiterjesztésre szolgáló exploitot, digitális tanúsítvánnyal rendelkező rootkitet, illetve a kód visszafejtésének nehezítése céljából VMProtect-et. **Bővebben...**

Szigorúbb adatvédelmi irányelvet mutattak be Szingapúrban

(www.zdnet.com)

Az új adatvédelmi törvény közelgő változtatásainak részeként az adatsértésekkel kapcsolatos intézkedésekre vonatkozó követelmények is módosításra kerülnek Szingapúrban. Az új irányelv értelmében az adatsértést tapasztaló vállalkozásoknak legfeljebb 30 nap áll majd rendelkezésre a biztonsági események kivizsgálásra, amelyek befejezését követően 72 órán belül értesíteniük kell a hatóságokat. **Bővebben...**