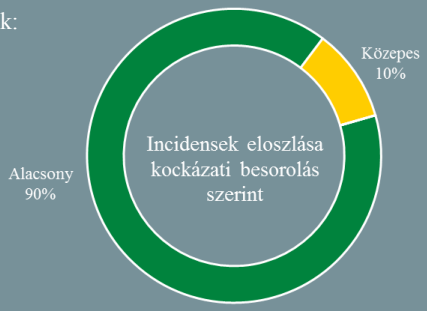
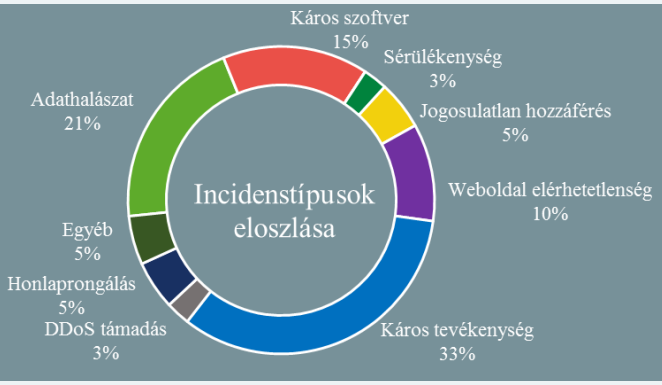
Nemzetközi IT-biztonsági sajtószemle

2021. 03. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.01.15. - 2021.01.21.





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

ENISA útmutató: felhőszolgáltatások biztosítása egészségügy számára

(enisa.europa.eu)

Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) "Cloud Security for Healthcare Services" című jelentésében bemutatja a felhőszolgáltatásokat érintő főbb kiberfenyegetéseket, és javaslatokat fogalmaz meg a felhőtechnológiák biztonságos integrálásához az egészségügyi szektor számára. Az egészségügyi szolgáltatások digitalizálása nem új igény, azonban a pandémiás időszak e téren is sürgetőleg hat. A betegadatok különösen érzékeny jellege azonban megkívánja a biztonsági aspektusok fokozott figyelembevételét. **Bővebben...**

Olyan sokan váltottak hirtelen Signalra, hogy túlterhelődött a szolgáltatás

(bbc.com)

Felhasználók milliói regisztráltak a Signal üzenetküldő alkalmazásra, miután a WhatsApp nemrég módosítást eszközölt a szolgáltatás igénybevételének feltételein. Sokak számára azonban nem volt felhőtlen az első találkozás, a Signal kiszolgálói ugyanis nem voltak felkészülve a felhasználói bázis ilyen mértékű, hirtelen növekedésére, ezért kapacitáshiány miatt akadozott a szolgáltatás. Pénteken arról kezdtek beszámolni a felhasználók, hogy több órán keresztül sikertelen volt az üzenetküldés mind a mobil, mind pedig az asztali alkalmazáson keresztül. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán arról olvashatunk, hogyan kezeljük a szolgáltatóktól beérkező hívásokat.

Kémkedésre módot adó hibákat fedeztek fel videóchat appokban, a Signal is érintett

(bleepingcomputer.com)

Aggasztó biztonsági hibákat fedeztek fel több népszerű videóchat alkalmazásban ─ úgy mint a Signal, a Facebook Messenger, a Google Duo, a JioChat és a Mocha ─ amelyek lehetővé tették, hogy harmadik fél lehallgassa a hívott fél környezetét. A hibák abból eredtek, hogy audió és videó adatok azelőtt kerülhettek továbbításra, hogy arra a felhasználó ─ a hívás fogadásával ─ engedélyt adna. Szerencsére az érintett sérülékenységek már javításra kerültek, ám a hibákat felfedező Natalie Silvanovich arra hívja fel a figyelmet, hogy ez a problémakör további kutatást igényel, ugyanis ő maga például a csoportos hívásokat egyáltalán nem vizsgálta.

DNS over HTTPS ajánlás az NSA-től

(securityweek.com)

Az Amerikai Nemzetbiztonsági Ügynökség (NSA) útmutatást tett közzé szervezetek számára a titkosított tartománynévrendszer (DNS over HTTPS – DoH) vállalati környezetbe történő bevezetésével kapcsolatban. A DNS (Domain Name System) rendszer az ember számára könnyen értelmezhető tartományneveket (domain név) fordítja le IP címekre, amelyeket a különböző hálózati eszközök már képesek kezelni. Sajnos a rendszer mára népszerű támadási felületté vált, főképp mivel a kérések és válaszok egyszerű szöveges formában (plaintext) kerülnek továbbításra. **Bővebben...**

Vállalati dolgozókat célzó csaló hívásokra figyelmeztet az FBI

(bleepingcomputer.com)

Egy éven belül második alkalommal ad ki figyelmeztetést az FBI ún. vishing támadásokról. A vishing kifejezés (voice phishing ─ azaz hang alapú adathalászat) olyan csaló telefonhívásokra utal, amelyek során a támadó magát egy megbízható szervezet képviselőjének kiadva próbálja meg manipulálni a hívott felet, jellemzően azért, hogy az áldozattól érzékeny adatokat szerezzen meg, például jelszavakat vagy bankkártya adatokat. Az FBI most egy világszerte zajló támadássorozatra figyelmeztet, kiemelve, hogy a támadók a korábbiaktól eltérően már nem elsősorban a magasabb pozícióban lévő ─ ezért a szervezeti rendszerekhez feltételezhetően magasabb hozzáférési szinttel rendelkező ─ felhasználókat célozzák, hanem bármely munkatársa célponttá válhat. **Bővebben...**