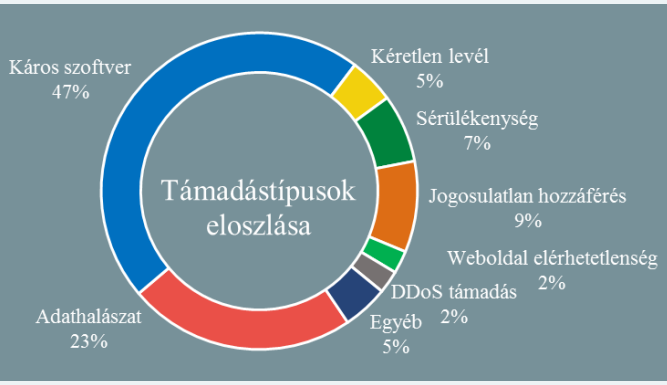
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 17. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.03.17. - 2020.03.23.



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

Az egészségügyi alkalmazásokkal járó magas kockázatokra figyelmeztet a BSI

(heise.de)

A német Szövetségi Információbiztonsági Hivatal (BSI) technikai iránymutatást (TR) dolgozott ki a digitális egészségügyi alkalmazások biztonsági követelményeiről. A hatóság számos veszélyre hívja fel a figyelmet az alkalmazások ezen érzékeny területen történő használatával kapcsolatban. A mobiltelefonos alkalmazások gyakran érzékeny személyes adatokat tárolnak, kezdve az pulzusszámtól, az alvási ritmustól egészen a gyógykezelési tervekig, az orvosi receptekig és leletekig, így egy kompromittálódott okostelefon "felfedheti a felhasználó teljes digitális életét." **Bővebben...**

Apple felhasználók figyelem: egy e-maillel hackelhetők az iOS telefonok

(thehackernews.com)

A ZecOPS kiberbiztonsági kutatói fedeztek fel két nulladik napi (zero day) kritikus sérülékenységet, amelyek sikeres kihasználásával a támadók teljes kontrollt nyerhetnek a sérülékeny Apple készülékek felett. A biztonsági hibák az Apple alapértelmezett levelező alkalmazását (Mail) érintik, és már az iOS6 megjelenése óta jelen vannak egyes iPhone és iPad készülékekben, az egyik hiba ráadásul bármiféle felhasználói interakció nélkül kihasználható. Eszerint ha az áldozat be van jelentkezve a sérülékeny levelező alkalmazásba, a támadónak csupán egy speciálisan szerkesztett e-mail üzenetet kell küldenie az eszköz kompromittálásához. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat a BGP eltérítéses támadások elleni védekező lépésekről.

Ingyenes COVID-19 teszt helyett a Trickbot malware-t kapják a melléklet megnyitói

(zdnet.com)

A Microsoft Security Intelligence csapata szerint az elmúlt napokban ismét jelentős mértékben megnövekedett az új koronavírus témájú káros kódot terjesztő adathalász támadások száma. A biztonsági csapat múlt héten több száz COVID-19-el összefüggő orvosi javaslatokkal és ingyenes tesztekkel kecsegtető e-mailt detektált, amelyek mellékletе káros kódot (Trickbot) rejt. *(A Trickbot kezdetben banki trójai programként indult, mára azonban inkább más káros szoftverek terjesztésére használják a támadók.)* **Bővebben...**

Tanulmány a szoftverbiztonság Európai Uniós fejlesztéséről

(enisa.europa.eu)

A biztonsági események és adatsértések gyakran az alapvető biztonsági elvek és technikák betartásának hiányára vezethetők vissza. A biztonsági szint emelése és az ismert biztonsági fenyegetések enyhítése érdekében a biztonságos szoftverfejlesztés és -karbantartás egyre inkább a megfelelő értékeléstől függ, azaz végső soron a tanúsítástól. Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) e témakörben készített friss jelentése néhány szoftverbiztonsági kulcskérdés tárgyalása mellett áttekintést nyújt a leglényegesebb megközelítésekről és standardokról, valamint azonosítja a főbb hiányosságokat a biztonságos szoftverfejlesztés tekintetében. **Bővebben...**

Kibertámadások kereszttüzében a cseh egészségügy

(reuters.com)

A prágai repülőtér és egy helyi kórház szombaton közleményt adott ki, miszerint kibertámadásokat hárítottak el, beigazolva ezzel a cseh kiberbiztonsági központ, a NÚKIB korábbi figyelmeztetését. A reptér szóvivője szerint a rendszereiket ért támadást szerencsére még a kezdeti szakaszban detektálták, így meg tudták akadályozni annak további kibontakozását. Szintén sikertelennek bizonyultak a Karlovy Vary-beli kórház elleni szombati, valamint az egy nappal korábban több egészségügyi intézményt is érintő támadások. **Bővebben...**