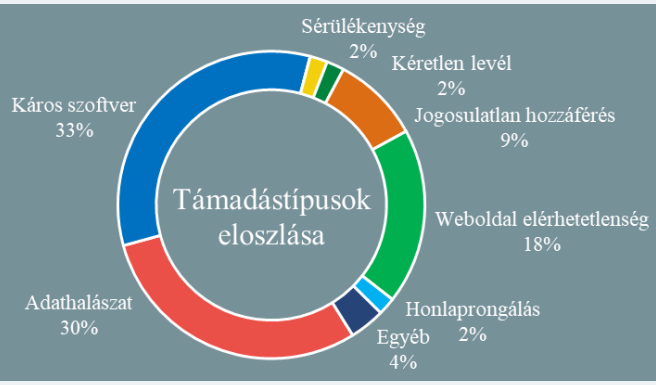
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 24. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.06.05. - 2020.06.11.



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

Kormányzati hálózatra telepített lehallgató eszközöket foglalt le a szlovák rendőrség

(zdnet.com)

Az Aktuality nevű helyi hírportál szerint szlovák hatóságok négy személyt tartóztattak le kedden a kormányzati informatikai hálózatra (GOVNET) telepített gyanús eszközök miatt indított nyomozás során. A letartóztatottak között van a GOVNET-et üzemeltető National Network and Electronic Services Agency (NASES) két magas beosztású tagja, a miniszterelnök-helyettesi iroda egy dolgozója, valamint egy magánszektorbeli személy. A lefoglalt eszközökről feltételezeik, hogy az internetes és telefonos kommunikáció lehallgatására szolgáltak, ezeket jelenleg a Szlovák Nemzeti Bűnügyi Hivatal (NAKA) vizsgálja.

Mobilbanki alkalmazások elleni támadásokra figyelmeztet az FBI

(securityweek.com)

A pandémiás időszak egyik hozadéka, hogy a mobilbankolás népszerűsége még az utóbbi években egyébként is tapasztalható, folyamatosan növekvő trendjéhez képest is jelentősen emelkedett. Az FBI internetes bűnüldözésért felelős központja, az IC3 arra hívja fel a figyelmet, hogy mindez előrevetíti azt is, hogy a mobilbankolást célzó támadások is gyakoribbá válhatnak. Az IC3 szerint a fő veszélyt a banki trójai programok jelentik, amelyek a banki hitelesítő adatok megszerzésére specializálódtak. Ezek ellen leginkább úgy védekezhetünk, hogy kizárólag hivatalos alkalmazásboltokból töltünk le applikációkat és többfaktoros hitelesítést (MFA) alkalmazunk. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat miként törölhető a Cortana a Windows 10 2004-es verziójában.

Néhány órán belül felfedezik a nyilvános szervereken felejtett adatbázisokat

(securityweek.com)

Biztonsági kutatók folyamatosan találnak nem megfelelően konfigurált felhő tárhelyeken szabadon hozzáférhető adatbázisokat. Egy friss kutatás szerint a hackerek — nem meglepő módon — éppoly sikeresek ebben. Kifejezetten gyakran érkeznek hírek olyan szenzitív adatokat tartalmazó adatbázisokról, amelyek publikus felhő tárhelyeken keresztül bármiféle hitelesítés nélkül hozzáférhetőek bárki számára. Biztonsági kutatók egy-egy ilyen találatkor igyekeznek minél előbb felvenni a kapcsolatot az adatbázis tulajdonosával, akik jellemzően hamar korrigálják a hibát. Sok esetben azonban nyitott marad a kérdés, mennyi idő telt el a felfedezésig és ezalatt történt-e illetéktelen hozzáférés. **Bővebben...**

Új zsarolóvírus szindikátus van szerveződőben

(techradar.com)

A Maze zsarolóvírus csoport volt az első, amely tavaly adatszivárogtató oldalt hozott létre (Maze News), ahol a nem fizető áldozatoktól lopott adatokat nyilvánosságra kezdték hozni. A csoport most egy szinttel feljebb lépve egy szindikátus megalakításába kezdett, ahol a zsarolóvírus támadásokat végrehajtó kiberbűnözők információt cserélhetnek és közös infrastruktúrán hozhatják nyilvánosságra az ellopott adatokat. Az első csatlakozó kollektíva a LockBit csoport volt, azonban friss hírek szerint már a RagnarLocker is csatlakozott, akik egyébként rendelkeznek saját adatszivárogtató oldallal. **Bővebben...**

Kibertámadás érte Dél-Afrika legnagyobb magán-egészségügyi szolgáltatóját

(thechronicleherald.ca)

A Life Healthcare keddi közleményében tudatta, hogy egyes informatikai rendszereiket kibertámadás érte. A kompromittálódás mértékét még nem sikerült megállapítani, azonban a betegek ellátása nincs veszélyben, a tartalékrendszerek üzemelnek. A Life Health a harmadik dél-afrikai nagyvállalat, amit kibertámadás ért idén.