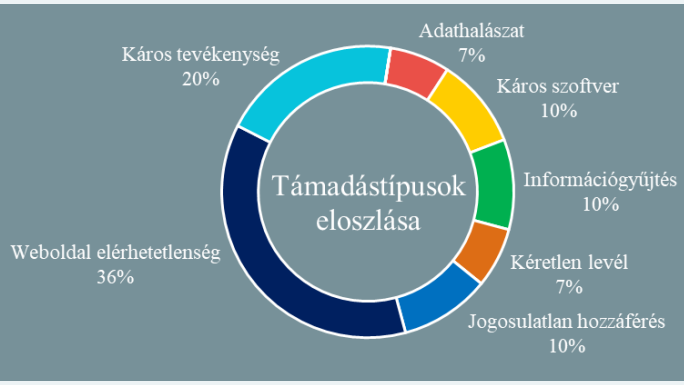
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 46. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.11.06. - 2020.11.12.



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

EU: szigorúbb szabályokról állapodtak meg a felügyeleti technológiák tekintetében

(securityweek.com)

Az Európai Unió jogalkotói, valamint az Európai Tanács ideiglenes megállapodást kötött az ún. kettős felhasználású termékek ─ mint például az arcfelismerő technológia és kémprogramok ─ szigorúbb felügyeletéről, annak érdekében, hogy azok használata ne sérthesse az emberi jogokat. Az új szabályok szerint az európai vállalatoknak kormányzati engedélyre lesz szükségük bizonyos termékek exportjához, amelyeknek szigorúbb kritériumoknak kell majd megfelelniük. **Bővebben...**

Kémfunkciókkal felszerelt banki trójai program terjed Androidon

(thehackernews.com)

Négy hónappal azután, hogy biztonsági kutatók egy latin-amerikai és európai pénzintézeteket célzó banki trójai programot fedeztek fel, kiderült, hogy a művelet hátterében álló elkövetők kémprogram funkciókat is bevetettek a támadások során. A Kaspersky globális kutatási és elemzési csoportja (GreAT) szerint a brazil Guildma nevű kollektíva által alkalmazott „Ghimob" androidos banki trójai program banki, tőzsdei és kriptovaluta alkalmazásokat céloz. A fertőzést követően a Ghimob képes távoli hozzáféréssel tranzakciókat végrehajtani az áldozat nevében, amivel megkerülhetők az alkalmazások biztonsági

IT biztonsági Tanács

Az NBSZ NKI weboldalán javaslatokat olvashat arról, hogyan célszerű kezelni egy, a szervezettől távozó munkatárs e-mail fiókját.

Több millió szállodavendég adata szivárgott ki

(securityaffairs.co)

A Website Planet biztonsági kutatói felfedeztek egy olyan, a Prestige Software Cloud Hospitality szolgáltatásához használt Amazon S3 online tárolót, amely hibás konfiguráció következtében több millió szállodavendég érzékeny adatát szivárogtatta ki. A Cloud Hospitality egy olyan szálláshelyek által használt foglalási rendszer, amely integrálható a Booking.com-hoz hasonló szálláshirdetési platformokkal. Mint kiderült, a cég 2013-ig visszamenően tárolt rendkívül érzékeny ügyféladatokat ─ például a vendégek bankkártya adatait CVV számmal, lejárati információkkal együtt ─ bármiféle védelmi megoldás nélkül, azaz a több, mint 24 GB-nyi adat bárki számára hozzáférhető volt. Jelenleg nem ismert, hogy valójában történt-e illetéktelen hozzáférés, ám a cég ettől függetlenül komoly adatvédelmi bírságra számíthat.

Fejlesztők figyelem: káros kódot tartalmaz egy npm csomag!

(zdnet.com)

A Sonatype kutatói fedezték fel a káros kódot tartalmazó **discord.dll**-t, amely a ZDNet publikációjának elkészültekor még elérhető volt az npm csomagkezelőn keresztül. A biztonsági cég szerint a dll fájlba rejtett kód célja érzékeny adatok kinyerése egyes webböngészőkből ─ mint például a **Google Chrome**, **Brave**, **Opera**, és a **Yandex Browser** ─ valamint a Discord applikációból. A támadás során az érintett programok böngészőtörténet és hozzáférési tokenek tárolására szolgáló LevelDB adatbázisát szerzik meg, és egy Discord csatornát nyitva küldik el a támadóknak. A kutatók szerint a káros kód egy még augusztusban felfedezett malware (fallguys) továbbfejlesztése.

ENISA: fenyegetettségi helyzetkép 2020

(enisa.europa.eu)

Megjelent az európai kiberügynökség 2019 januárja és 2020 áprilisa közötti időszakra vonatkozó kiberfenyegetettségi összefoglalója. Az immár nyolcadik alkalommal elkészített éves jelentés ezúttal új, áttekinthetőbb struktúrában mutatja be a tárgyidőszak főbb kiberbiztonsági trendjeit, a kiemelt témák a korábbiaknál részletesebben, ezúttal különálló dokumentumokként tekinthetők meg. **Bővebben...**