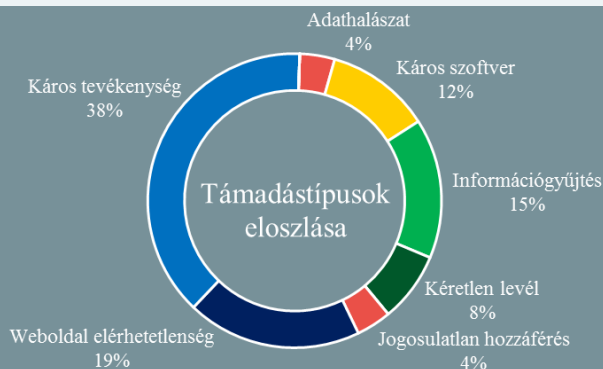


Az NKI által kezelt incidensekre
vonatkozó statisztikai adatok:
2020.10.16. - 2020.10.21.



Kövessen minket megújult [weboldalunkon](#), ahol friss IT-biztonsági hírek kerülnek publikálásra!

Magyar diákokat is vár a lengyel ‘153+1’ kiberverseny

([153plus1.eu/#/](#))

Lengyelország idén második alkalommal szervezi meg a 153+1 elnevezésű kiberversenyt, amelynek fő célja, hogy a fiatal korosztály érdeklődését a kibertér kihívásaira irányítsa. A verseny klasszikus „Capture The Flag” típusú megméretetés, olyan fiatal, az informatikai terület kapcsán érdeklődést mutató diákokat szólít meg, akik szeretnék fejleszteni képességeiket és többet megtudni a kiberbiztonsági kérdésekről. **Bővebben...**

Telegramon elérhető deepfake botnetet lepleztek le ([engadget.com](#))

A Sensity biztonsági cég egy deepfake hálózatot [fedezett fel](#) a közelmúltban a Telegram platformon, amely az elmúlt néhány hónap alatt közel 104 000 nőről készített képre hamis meztelen képeket. Azt hihetnénk, hogy az algoritmus elsősorban hírességek képeiből generált kompromittáló képeket, azonban úgy tűnik a képek “megrendelői” inkább környezetükből választottak — esetenként kiskorú — célpontot. A szoftvert használók többsége (70%-a) Oroszországból származik, ahol a közelmúltban került betiltásra a Telegram. **Bővebben...**

Szingapúr hivatalos azonosításként alkalmazná az arcellenőrzést

([securityweek.com](#))

Jövő évtől kerülhet széles körben bevezetésre az a biometrikus azonosító rendszer, amellyel a szingapúri állampolgárok jelszavak és hardverkulcsok helyett egy gyors arcszkennelés után férhetnek majd hozzá kormányzati, banki és egyéb szolgáltatásokhoz. Az arcfelismerést világszerte többféle formában alkalmazzák — gondoljunk csak a telefonok feloldására, vagy a reptereken történő biztonsági ellenőrzésekre — azonban a szingapúri kezdeményezés eddig messze a legambiciózusabb. **Bővebben...**

Több, mint 50 000 otthoni IP kamerát tört fel egy hacker csoport

([securityaffairs.co](#))

Egy hacker csoport azt állítja, hogy több, mint 50 000 otthoni biztonsági kamerát hekkelt meg, ennek alátámasztásaként pedig privát fotókat tett közzé az Interneten, többek között felnőtt tartalmú oldalakon. A csoport 150 dollárért hozzáférést kínál a teljes gyűjteményhez, sőt, a szingapúri The New Paper szerint VIP tagoknak még azt is megtaníjták, hogyan derítsenek fel online elérhető kamerákat és férjenek hozzá azokhoz. Jelenleg nem ismert, hogy a támadók milyen módon kompromittálták az IP kamerákat, habár a legvalószínűbb egy biztonsági hiba kihasználása vagy gyenge jelszó feltörése lehetett.

A tömegközlekedésben okozott fennakadást egy zsarolóvírus Montréálban

([bleepingcomputer.com](#))

Október 19-én zsarolóvírus támadás érte a montreáli Société de transport de Montréal (STM) tömegközlekedési társaság rendszerét. Bár a támadás okozta kiesések nem befolyásolták az autóbuszok és a metró működését, azonban például elérhetetlenné vált a fogyatékosokkal élő utasok alternatív tömegközlekedési (paratransit) szolgáltatása, ugyanis ez csak online regisztrációs rendszeren keresztül igényelhető. **Bővebben...**

IT biztonsági



Tanács

Az NBSZ NKI [weboldalán](#) hasznos információkat olvashat arról, hogy tehetők biztonságosabbá a Zoom meetingek.