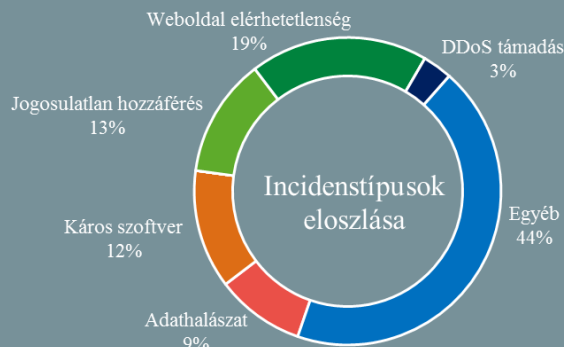


Az NKI által kezelt incidensekre  
vonatkozó statisztikai adatok:  
2021.05.21. - 2021.05.27.



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

## Kétszeres titkosítással trükköznek a zsarolóvírus bandák

([wired.com](#))

A zsarolóvírus támadások során egyre többször tapasztalni, hogy a kiberbűnözők kétszeresen titkosítják a kiszemelt célpont adatait. Dupla titkosítási támadások már korábban is előfordultak, általában két különböző zsarolóvírus csoport egyidejűleg támadta ugyanazt az áldozatot. Az Emsisoft vírusirtó cég azonban azt állítja, hogy több tucat olyan esetről van tudomása, amikor ugyanaz a szereplő vagy csoport szándékosan kétféle zsarolóvírust vet be a támadás során. A biztonsági cég két különböző taktikát azonosított. Az első során a hackerek az adatokat két különböző zsarolóprogrammal titkosítják, így az áldozat, ha képes is dekódolnia a fájlokat, újabb akadályba ütközik, ugyanis az egyszeresen dekódolt állományok még mindig titkosítva lesznek. **Bővebben...**



## Apple felhasználók, frissítésre fel!

([zdnet.com](#))

Néhány héttel a [legutóbbi vészhelyzeti frissítés](#) után, ismét soron kívüli hibajavítás vált elérhetővé Apple termékekhez. Az iOS 14.6 mintegy 30 biztonsági hibát javít, és habár ezúttal nem ismert, hogy a sérülékenységek aktív kihasználás alatt állnának, a frissítés telepítése mindenképp javasolt! Javítást kapott még az iPadOS, a watchOS, a tvOS, macOS rendszerek kapcsán pedig a Big Sur, a Mojave, és a Cataline. **Frissítve...**

## Világszerte folytatódnak az egészségügyi intézmények elleni kibertámadások

([securityaffairs.co](#))

Az alaskai Egészségügyi és Szociális Szolgálat (Department of Health and Social Services) weboldala egy kibertámadás miatt napok óta elérhetetlen. A hivatalos közlemény a jelenleg is folyamatban lévő incidensvizsgálásra hivatkozva ennél bővebb információt nem tartalmaz, szakértők azonban feltételezik, hogy zsarolóvírus okozhatott fennakadást.

## WhatsApp kontra indiai kormány

([theguardian.com](#))

A WhatsApp pert indít az indiai kormányzat új internetes törvénye ellen, arra hivatkozva, hogy az alkotmányellenes, és felhasználói számára lényeges adatvédelmi hátrányt okoz. Az eset hátterében az a februárban benyújtott törvényjavaslat áll, amelynek értelmében az olyan csevegő szolgáltatásoknak, mint a WhatsApp, vagy a Signal, fel kell hagyniuk a titkosított üzenetküldéssel, valamint az üzeneteket egy, a kormányzat számára hozzáférhető, és az adatokat visszakéreshető formában tároló adatbázisban kell elhelyezniük. Az indoklás egyszerű: a bűnüldözés hatékony támogatása, a WhatsApp álláspontja szerint azonban mindez jogszerűtlen tömeges megfigyelésre ad módot. **Bővebben...**

## Figyelem: fontos Pulse Secure Connect VPN frissítés érhető el!

([securityaffairs.co](#))

Az Ivanti egy magas kockázati besorolású sérülékenységről (CVE-2021-22908) adott tájékoztatást, amely autentikált felhasználók számára root jogosultsággal történő tetszőleges kód futtatásra nyújt lehetőséget az érintett Pulse Secure Connect (PCS) VPN-t futtató rendszereken. A sebezhetőség az SMB fájlmegosztás nem megfelelő kezeléséből adódik. A gyártó a **9.1R11.5** verzióban tervezi orvosolni a hibát, amely még nem elérhető, azonban a hiba átmenetileg orvosolható a Windows File Share Browser funkció letiltásával, ami az Ivanti által készített XML fájl telepítésével lehetséges. **Bővebben...**

## IT biztonsági Tanács



Az NBSZ NKI [weboldalán](#) hasznos információkat olvashat a digitális visszaélésekkel kapcsolatosan.