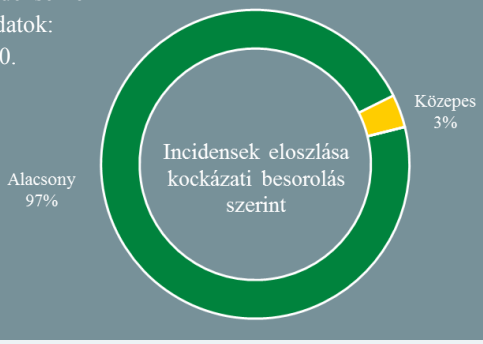
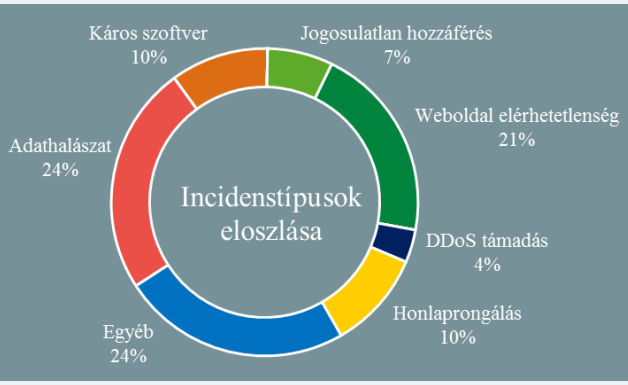
NEMZETI KIBERVÉDELMI INTÉZET

# Nemzetközi IT-biztonsági sajtószemle

2021. 20. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.05.14. - 2021.05.20.




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

## Újabb kritikus infrastruktúrát ért zsarolóvírus támadás, a célpont ezúttal az ír egészségügy volt

**(therecord.media)**

Egy héttel a Colonial elleni ransomware támadás után újabb kritikus infrastruktúránál történt incidens, ezúttal Írország nemzeti egészségügyi szervezetének (Health Service Executive – HSE) IT rendszereit bénította meg zsarolóvírus. A szervezet szerint a kibertámadás következtében egyes szolgáltatások nem elérhetőek, dolgozók nem férnek hozzá betegadatokat kezelő rendszerekhez. Szerencsére mind a sürgős egészségügyi ellátás, mind a COVID-19 oltási program zavartalanul működik. A HSE vezérigazgatója szerint **Conti** ransomware okozta a fertőzést, az incidenskivizsgálást megkezdték, ám eddig zsaroló üzenetet nem találtak a tikosított fájlok között.

## Elérhető a Verizon éves incidenskivizsgálási jelentése

**(zdnet.com)**

A Verizon közzétette a 2020-as év incidenskivizsgálási eredményeit összesítő jelentését (2021 DBIR). Eszerint a webes alkalmazások elleni támadások az összes adatsértési incidens 39%-át tették ki, az adathalászat 11%-kal nőtt, a zsarolóvírusokkal elkövetett támadások száma pedig duplázódott a megelőző évhez képest. A riport összesen 5 358 adatsértési incidenst vett alapul, az adatok 83 közreműködő szervezettől származnak, a világ minden tájáról. **Bővebben...**

## IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat a Sextortion zsarolólevelekkel kapcsolatban.

## Átrendeződések a kiberbűnözői ökoszisztémában

**(therecord.media)**

A Colonial vezeték elleni támadás után az amerikai kormányzat kinyilvánította, hogy keményen kíván fellépni a zsarolóvírus bandákkal szemben, aminek máris érezhető hatásai vannak. Három hacking fórum (XSS, Exploit, RAID) ─ ahol zsarolóvírus hacker csoportok előszeretettel reklámozták szolgáltatásaikat, és toboroztak partnereket ─ teljes mértékben száműzte a zsarolóvírus hirdetéseket. A Colonial elleni támadásért felelős **Darkside** pedig egy üzenetben tudatta, hogy elveszítették az irányítást infrastruktúrájuk felett. Néhány órával később a rettegett **REvil** és **Avaddon** csoportok is változásokat jelentettek be. **Bővebben…**

## Zsarolóvírus támadás ért új-zélandi kórházakat

**(theregister.com)**

Az ír egészségügyi rendszer után most az új-zélandi Waikato kerületi egészségügyi ellátórendszer (Waikato DHB) vált ransomware támadás áldozatává. A 2021. május 18-án, reggel történt támadás következtében a legtöbb IT-rendszert le kellett állítani a kerületi egészségügyi intézményekben, ami hat kórházban is az egészségügyi szolgáltatások jelentős korlátozottságát eredményezte. A betegadatok elérhetetlenné váltak, több műtétet is el kell halasztani. A Waikato DHB vezérigazgatója szerint napokig is eltarthat, amíg a rendszerek újra működőképesek lesznek. **Bővebben...**

## A GitHub már támogatja a biztonsági kulcsok használatát

**(ehackingnews.com)**

Kevin Jones, a GitHub biztonsági mérnöke blogbejegyzésében közölte, hogy a platformon már lehetőség van a hordozható FIDO2 kulcsokat SSH hitelesítésre használni, amely egy jelentős biztonsági előrelépés. A használható biztonsági kulcsok közé tartoznak a YubiKey, a Thetis Fido U2F és a Google Titan eszközei is. Kezelésük egyszerű, elfér a zsebünkben és a számítógéphez USB, NFC vagy Bluetooth segítségével lehet csatlakoztatni. Használhatóak az alkalmazások által generált vagy SMS-ben elküldött egyszeri jelszavak helyett is. **Bővebben...**