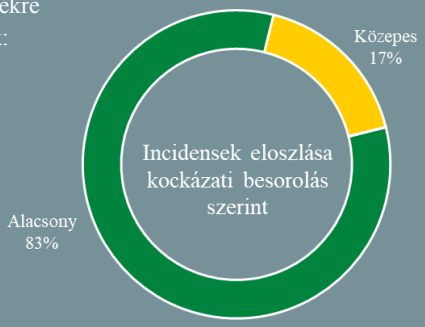
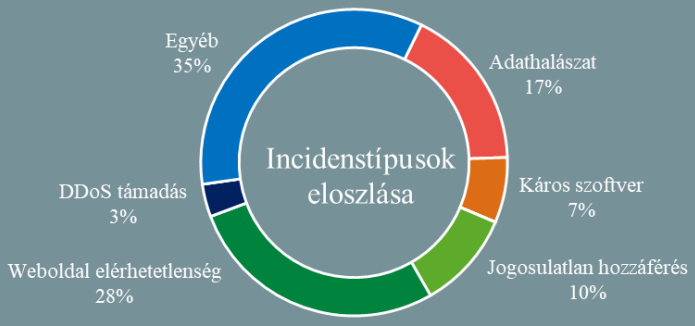
NEMZETI KIBERVÉDELMI INTÉZET

# Nemzetközi IT-biztonsági sajtószemle

2021. 10. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.03.05. - 2021.03.11.




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

## Zsarolóvírus támadás érte a spanyol foglalkoztatási szolgálat rendszereit

**(bleepingcomputer.com)**

Ryuk zsarolóvírus támadás bénította meg a spanyol Állami Állami Foglalkoztatási Szolgálat (Servicio Público de Empleo Estatal – SEPE) rendszereit, amelynek során több, mint 700 kirendeltség állt le. Jelenleg az elsődleges szolgáltatások ─ köztük a szervezet weboldalának ─ helyreállítása zajlik. A SEPE igazgatója, Gerado Guitérrez szerint személyes adatok, illetve a munkanélküli járadékok folyósítására szolgáló rendszerek nem érintettek az incidensben. Mivel azonban jelenleg időpont tegyeztetés nem lehetséges a kirendeltségekbe, a kérelmek beadási határidejét a leállás végéig meghosszabbítják.

## Apple felhasználók figyelem: fontos biztonsági frissítés érkezett!

**(securityaffairs.co)**

Soron kívüli hibajavítást adott ki az Apple egy kritikus kockázati besorolású sérülékenység (**CVE-2021-1844**) javításához, amely a támadók számára távoli kódfuttatást tehet lehetővé. A sebezhetőség ráadásul viszonylag egyszerűen, egy speciálisan szerkesztett weboldallal kihasználható. Javítás az iOS 14.4, iPadOS 14.4, macOS Big Sur, watchOS 7.3.1 (Apple Watch 3-as és ennél későbbi széria), valamint a macOS Catalina és macOS Mojave rendszereken futó Safari webböngészőhöz érkezett.

*Az NBSZ NKI javasolja a javított verziókra (**iOS 14.4.1, iPadOS 14.4.1, Safari 14.0.3**) történő frissítést.*

**IT biztonsági Tanács**

Az NBSZ NKI weboldalán a TikTok új funkciójának használatáról olvashat, amely hasznos segítséget nyújt a zaklató kommentek kiszűréséhez.

## ProxyLogon: A norvég parlament levelezőrendszerét is feltörték

**(bleepingcomputer.com)**

Hackertámadás érte a norvég országgyűlés levelezőrendszerét, amelynek során a Microsoft Exchange levelezőrendszer sérülékenységeit (ProxyLogon) használták ki. A hivatalos közlemény szerint ─ habár a támadás kiterjedtségét még nem sikerült megállapítani ─ az adatlopás ténye már igazolt. Marianne Andreassen, a Storting adminisztrációs vezetője elmondta, jelenleg nem feltételeznek összefüggést a mostani és a 2020 decemberi támadás között.

## Biztonsági kamerákhoz fértek hozzá hackerek nagynevű vállalatoknál

**(bleepingcomputer.com)**

Hackerek hozzáfértek, többek közt a Teslánál, a Cloudflare-nél, az Equinox-nál, további számos egészségügyi szervezetnél, valamint bankoknál és börtönöknél telepített biztonsági kamerák élő képéhez. A *#OperationPanopticonként* hivatkozott támadás során a hackerek ráadásul egyes cégek esetében teljes (root szintű) hozzáférést szereztek a belső rendszereken is ─ ez az elkövetők által posztolt információk alapján vélhetően a Cloudflare és a Tesla esetében is így történt. A támadásról már tudni, hogy az a Verkada rendszereit érte, amely cég rendkívül széles ügyfélkörnek nyújt biztonsági kamerarendszer szolgáltatást. **Bővebben...**

## Utasok millióit érinti a SITA rendszerei elleni kibertámadás

**(securityaffairs.co)**

A SITA, a légiközlekedési ágazat számára elengedhetetlen szolgáltatásokat nyújtó nemzetközi informatikai vállalat több légitársaságot érintő kibertámadás áldozatává vált. A cég világszerte mintegy 400 tagnak és 2 800 ügyfelének nyújt szolgáltatásokat, amely így a világ légitársaságainak 90%-át fedi le. A vállalat beszámolója szerint egy rendkívül precíz és kifinomult támadás érte a szervezet rendszereit. Több légitársaság is érintett az esetben, köztük például a Lufthansa, a SAS-Scandinavian Airlines, Air New Zealand és a Singapore Airlines is. **Bővebben...**