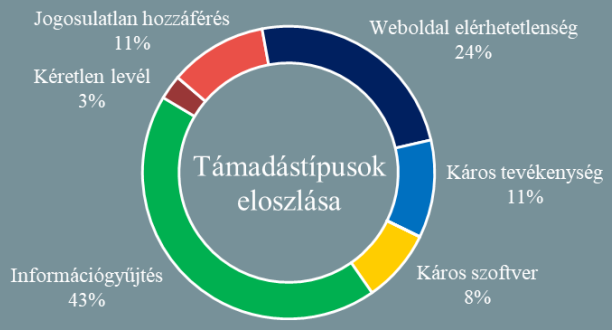
NEMZETI KIBERVÉDELMI INTÉZET

# Nemzetközi IT-biztonsági sajtószemle

2020. 49. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.11.27. - 2020.12.03.


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

## Még nagyobb kontrollt adna az EU az európai polgároknak személyes adataik kezelése felett

**(securityweek.com)**

Az Európai Bizottság adatkormányzásról szóló rendelete (**Digital Governance Act**) az európai adatpiacon történő információmegosztást kívánja elősegíteni. A digitális adatkormányzás célja egy megbízható új rendszer bevezetése, amely a hatályos adatvédelmi elvek figyelembevételével segíti az olyan ipari vagy éppen kormányzati adatok megosztását, amelyek felhasználása valamely okból ─ például szellemi tulajdonjog, üzleti titoktartás vagy magánéleti jogok miatt ─ korlátozott.

## Könnyen kivédhető a WhatsApp felhasználók ellen alkalmazott új támadási módszer

**(lifehacker.com)**

A támadók egy egyszerű, de figyelemre méltó új módszerrel veszik át az irányítást a felhasználók WhatsApp fiókjai felett. Az F-Secure felfedezése szerint, amennyiben egy támadó sikeresen hozzáférést szerzett egy WhatApp felhasználói fiókhoz, a kontaktlistán szereplő névjegyeket megpróbálja üzleti fiókká alakítani, amelyről a szolgáltató egy hat jegyű hitelesítő kódot küld az érintett felhasználóknak. Ilyenkor a támadó az átvett fiók nevében felveszi a kapcsolatot az áldozattal ─ arra hivatkozva, hogy a hatjegyű kód tévedésből került kiküldésre ─ és kéri annak átadását. **Bővebben...**

### IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat a Windows funkciófrissítés teszteléséről.

## Három észt minisztériumnál is adatszivárgás történt novemberben

**(estonianworld.com)**

Az Észt Információbiztonsági Hatóság (RIA) jelzése szerint az ország három minisztériumából – gazdasági, a külügyi és a szociális – is jelentettek adatszivárgást, amely személyes adatok kompromittálódásával is járt. A szociális minisztériumot érintő incidens során például több, mint 9 000 személy fertőző betegségre vonatkozó egészségügyi adata szivárgott ki. A RIA szerint az incidensek közszolgáltatásokban nem okoztak fennakadást. A kivizsgálások jelenleg is tartanak.

## Nemsokára a Chrome figyelmeztet, ha gyenge jelszavakat használunk

**(bleepingcomputer.com)**

Új biztonsági funkción dolgozik a Google, amely automatikusan megkeresi a böngészőben elmentett gyenge jelszavakat. A Chrome biztonsági ellenőrző funkciója figyelmeztetni fogja a felhasználókat, amennyiben a mentett jelszavak között olyan szerepel, amely korábbi adatsértések során kiszivárgott. Mindez egyelőre még csak a Crome Canary verziójában érhető el, miután engedélyeztük a „*Safety check for weak passwords*” és a „*Passwords weakness check*” flageket. A böngésző újraindítását követően a „*Beállítások*” > „*Biztonsági ellenőrzés*” > „*Ellenőrzés most*” lehetőségre kattintva ellenőrizhetők a mentett jelszavak, azok módosítása pedig az „*Ellenőrzés*” (Review) gomra kattintva végezhető el.

## Oracle WebLogic szerverek veszélyben: sürgős frissítés javasolt!

**(thehackernews.com)**

Több robothálózat (botnet) is célba vett nyilvánosan elérhető sérülékeny Oracle WebLogic kiszolgálókat, hogy kriptovaluta bányász programokat telepítsenek és érzékeny információkat lopjanak el a fertőzött rendszerekből. A támadások során az elkövetők egy nemrégiben felfedezett WebLogic Server sebezhetőségét igyekeznek kihasználni, amelyet az Oracle a 2020. októberi Critical Patch Update részeként, majd egy novemberi soron kívüli frissítésben (CVE-2020-14750) javított. **Bővebben...**