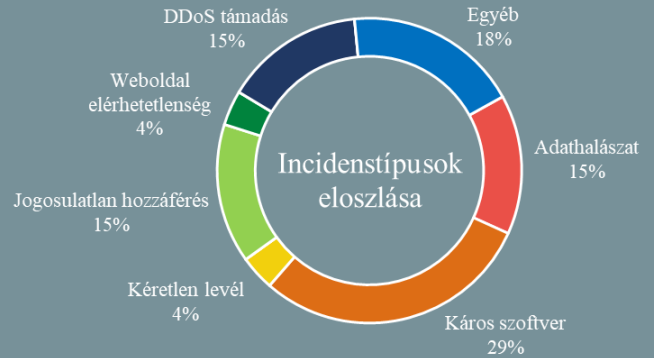
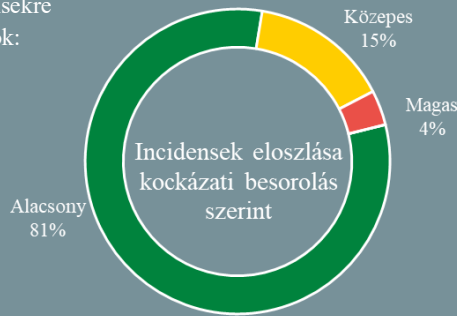


Az NKI által kezelt incidensekre  
vonatkozó statisztikai adatok:  
2022.03.25. - 2022.03.31.



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

## Új transzatlanti adattovábbítási egyezményt köt az Európai Unió és az Egyesült Államok ([securityweek.com](#))

Joe Biden amerikai elnök és Ursula von der Leyen, az Európai Bizottság elnöke jelentette be, hogy sikerült egyeztetni az álláspontokat a transzatlanti adattovábbítás kapcsán korábban felmerült adatvédelmi aggályok enyhítéséhez. *(A jobbizonytalanságot az Európai Unió Bírósága 2020. július 16-án hozott döntése okozta, amely érvénytelenítette az EU és az USA közötti adattovábbítás keretrendszerét, a Privacy Shieldet...)* **Bővebben...**



### A Yandex iOS felhasználók adatait küldi Oroszországba ([infosecurity-magazine.com](#))

Zach Edwards, a Financial Times kutatója szerint a Yandex több tízezer alkalmazásból gyűjt felhasználói adatokat orosz szerverein, köztük olyan iOS felhasználók adatait is, akik soha nem is használták a [Yandex](#) alkalmazásait. A [jelentésből](#) kiderül, hogy miként használják a harmadik féltől származó alkalmazások a Yandex cég által létrehozott fejlesztői eszközöket az iOS felhasználók adatainak gyűjtésére. **Bővebben...**

### IT biztonsági Tanács



Az NBSZ NKI [weboldalán](#) a biztonságos malware elemzési módszerekről olvashat **bővebben**.

### Ezek a főbb kiberbűnözési trendek az FBI jelentése szerint ([fbi.gov](#))

Az FBI Internet Crime Complaint Center (IC3) minden évben elkészíti az ún. **Internet Crime Reportot**, amely a tárgyévre vonatkozó kiberbűncselekmények típusairól és az általuk okozott károk mértékéről ad információt. A 2000-ben megalakult IC3 főként kiberbűncselekmények elszenvedőitől kapott bejelentésekből dolgozik, elsősorban — de nem kizárólag — az Amerikai Egyesült Államok területéről, így az általuk készített éves jelentés alapján egy általános képet kaphatunk a főbb kiberbűnözési trendekről. **Bővebben...**

### Az Anonymous állítólag egy minden eddiginél súlyosabb adatszivárogtatásra készül ([securityaffairs.co](#))

Az Anonymous hacktivisták kollektíva folytatja az orosz szervezetek elleni kibertámadásait, a hírek szerint két ipari cég is áldozattá válhatott. Az [orosz központi banktól](#) szerzett adatok után az Anonymous egy **110 GB**-nyi dumpot tett közzé a DDoSecrets adatszivárogtató oldalon, amelyet állítólag a moszkvai székhelyű **MashOiltól** szereztek meg. A [hackread.com információi szerint](#) több mint 140 000 belső vállalati e-mail található az adathalomban. Szintén belső levelezést tartalmaz az a **2.4 GB-os** adatsomag, ami a hackerek állítása szerint a **Rostproektől** származik. **Bővebben...**

### Akár egy weboldal meglátogatásával is fegyver válhat a böngészőnkől ([bleepingcomputer.com](#))

A MalwareHunterTeam több száz kompromittált WordPress weboldalt fedezett fel, amelyeken az elhelyezett rosszindulatú szkriptek ukrán kormányzati oldalak elleni szolgáltatás-megtagadással járó támadásokhoz (DDoS) használja fel a felhasználók böngészőit. A célzott weboldalak között ukrán kormányhivatalok, az agytröszt, az ukrán Nemzetközi Légión toborzóoldalai, pénzügyi oldalak és egyéb ukránpárti weboldalak szerepelnek. **Bővebben...**