

Az Európai parlament és a Tanács (EU) 2022/2555 számú irányelvét (rövidítve: NIS2) az Országgyűlés a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvényben (Kibertan. tv.) implementálta a hazai jogrendszerbe.

## KIRE VONATKOZIK A NIS2/KIBERTAN. TV. III. FEJEZETE?

### A Kibertan. tv. kiberbiztonsági felügyelettel kapcsolatos rendelkezéseit a

„Kiemelten kockázatos” és a „Kockázatos” ágazatokban működő szolgáltatóknak és szervezeteknek kell teljesíteni, amennyiben

- az összes foglalkoztatotti létszámuk 50 főnél nagyobb és
- éves nettó árbevételük vagy mérlegfőösszegük meghaladja a 10 millió eurónak megfelelő forintösszeget.

**Kb. 2500 szervezetet érinthetnek a kiberbiztonsági felügyelettel kapcsolatos kötelezettségek.**

#### Kivétel

Az alábbi szervezeteknek méretkorlát nélkül alkalmazni kell kiberbiztonsági felügyelettel kapcsolatos rendelkezéseket:

- elektronikus hírközlési szolgáltató,
- bizalmi szolgáltató,
- DNS-szolgáltatást nyújtó szolgáltató,
- legfelső szintű domainnév-nyilvántartó,
- domainnév regisztrációt végző szolgáltató.

## KIEMELTEN KOCKÁZATOS ÉS KOCKÁZATOS ÁGAZATOK

#### Kiemelten kockázatos ágazatokban működő szolgáltatók és szervezetek

- Energetika (villamos energia, távfűtés, kőolaj, földgáz, hidrogén)
- Közlekedés (légi-, vasúti-, közúti-, vízi- és tömegközlekedés)
- Egészségügy
- Ivóvíz, szennyvíz (Víziközmű szolgáltatás)
- Hírközlési szolgáltatás
- Digitális infrastruktúra
- Kihelyezett IKT (infokommunikációs) szolgáltatások
- Úralapú szolgáltatás

#### Kockázatos ágazatokban működő szolgáltatók és szervezetek

- Postai és futárszolgálatok
- Élelmiszer előállítása, feldolgozása és forgalmazása
- Hulladékgazdálkodás
- Vegyszerek előállítása és forgalmazása
- Gyártás (a tv. mellékletében felsorolt ágazatokra vonatkozóan)
- Digitális szolgáltatók
- Kutatás

## MIKORRA KELL TELJESÍTENI?

- **2024. január 1. – 2024. június 30. között:**
  - az érintett szervezeteknek be kell jelentkeznie a hatósági nyilvántartásába
  - IBF-et ki kell jelölni a szervezeten belül, s az adatait a hatósági nyilvántartásba vételnél is meg kell adni
- **2024. október 18-tól:** az érintett szervezeteknek működtetni kell a Kibertan. tv. VHR alapján elkészített IBIR-t
- **2024. december 31-ig:** kiberbiztonsági audit elvégzésére megállapodást kötni egy auditorral
- **2025. december 31-ig:** első kiberbiztonsági auditot el kell végezteni az érintett szervezeteknek



## MILYEN FELADATOK VANNAK?

### A kiberbiztonsági felügyelettel érintett szervezeteknek az alábbi feladatokat kell elvégezni:

- hatósági nyilvántartásba bejelentkezés
- információbiztonsági felelős (IBF) kinevezése
- IT-biztonsági irányítási rendszer (szabályozás) kialakítása
- IT kockázatelemzés
- IT védelmi intézkedések megvalósítása
- biztonsági események kezelése
- üzletmenet-folytonosság biztosítása
- hardver/szoftver beszerzés/fejlesztés/üzemeltetési követelmények meghatározása
- a fenti követelmények érvényesítése az elektronikus információs rendszerek létrehozásában, üzemeltetésében, karbantartásában vagy javításában résztvevő közreműködők esetében
- IT-biztonsági oktatás tartása a dolgozók részére
- rendszerek és tárolt adatok biztonsági osztályba sorolása
- kiberbiztonsági audit elvégzése külső szakértővel
- biztonsági események jelentése

## ILLETÉKES HATÓSÁG, SZANKCIÓK

### A Szabályozott Tevékenységek Felügyeleti Hatósága /SZTFH/ fogja ellátni az érintett szervezetek felügyeletét.

### Az érintett szervezetnek kiberbiztonsági felügyeleti díjat kell fizetni az SZTFH-nak.

Ha az érintett szervezet a kiberbiztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, az SZTFH jogosult:

- figyelmeztetni
- határidő tűzésével elrendelni az ellenőrzés vagy az audit során feltárt biztonsági hiányosságok elhárítását
- eltiltani az érintett szervezetet a tevékenységétől.

A fentiek eredménytelensége esetén az SZTFH bírság kiszabására jogosult, amelynek összege:

- kiemelten kockázatos ágazatba tartozó szervezetnél max. 10 000 000 EUR, vagy az éves forgalma összegének 2%-ig,
- kockázatos ágazatba tartozó szervezetnél max. 7 000 000 EUR, vagy az éves forgalma összegének 1,4%-ig terjedhet.

## MIBEN TUD SEGÍTENI AZ AAM TANÁCSADÓ ZRT.?

**Kollégáink több évtized szakmai tapasztalattal rendelkeznek informatikai/információbiztonsági projektek lebonyolításában.**

### Végzettségeink:

- Certified Information Systems Auditor(CISA)
- ISO/IEC 27001 Lead Auditor
- Infokommunikációs szakjogász
- Elektronikus információbiztonsági vezető (EIV)

- IT-biztonság helyzetének felmérése (GAP analízis)
- IT-biztonsági kockázatelemzés elkészítése
- Rendszerek és tárolt adatok biztonsági osztályba sorolása
- IT-biztonsági irányítási rendszer (szabályozás) kialakítása, felülvizsgálata
- IT védelmi intézkedések megvalósításhoz szakmai tanácsadás
- Információbiztonsági felelős (IBF) szerepkör ellátása
- Információbiztonsági oktatás tartása

**Számos hazai szervezet részére végeztünk IT-biztonsági kockázatelemzést, auditfelkészítést, illetve betöltjük a IT-biztonsági felelősi feladatkört.**

**Az AAM Tanácsadó Zrt. szervezetén belül ISO 27001 szabvány szerint kialakított, tanúsított IT-biztonsági irányítási rendszert működtet.**

