JAMBRIK ÜGYVÉDI IRODA

NIS 2 implementációjának helyzete

ESIGN Day – 2023.06.30.

dr. Csiky András ügyvéd
www.jambrik.hu

A NIS 2 irányelv megszületése

- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről („NIS 2 irányelv” [Network and Information Systems])

Magyar implementáció

- 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről (Kibertan. tv.),
  - Implementálja a NIS 2 irányelvet és
  - Végrehajtja az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) szóló az Európai Parlament és a Tanács 2019. április 17-i (EU) 2019/881 rendeletet
- A 2023. május 24-től hatályos 10/2023. (V. 15.) SZTFH rendelet a törvény tanúsításra vonatkozó szabályait tölti meg tartalommal

Hatálybalépés

- 2023. május 18-án hatályba lépett egy része a törvénynek
- A részletszabályokat többek között a Kormány és az SZTFH elnöke rendeletben határozza meg
- Május 26-tól *elvileg* már alkalmazandók a megfelelőségértékelő és a „gyártó” (szolgáltató) szervezetekre a biztonsági / eljárási és felügyeleti keretszabályok
- Legkésőbb 2024 elején kerülnek kidolgozásra a részletszabályok
- 2024 végén az ellenőrzésekről szóló rendelkezések is hatályosulnak
- E-kereskedelmi törvény kapcsolódó módosítása 2024. október 18-tól
    - bejelentés-köteles szolgáltatásra vonatkozó szabályok kikerülnek a törvényből: online piactér, keresőszolgáltatás, felhőalapú számítástechnikai szolgáltatás

Érintett szervezetek

Kiemelten kockázatos és kockázatos ágazatokban működő szolgáltatók és szervezetek, *pl.*:

(NIS 2-ben ‚SECTORS OF HIGH CRITICALITY' és ‚OTHER CRITICAL SECTORS')

Hírközlési szolgáltatás (kiemelten kockázatos)

- Az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési szolgáltató
- Adatkicserélő szolgáltatást nyújtó szolgáltató
- Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló törvény szerinti bizalmi szolgáltató

Kihelyezett IKT (Outsourced ICT) (kiemelten kockázatos)

- Kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató
- kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató

Digitális infrastruktúra (kiemelten kockázatos)

- Felhőszolgáltató
- Adatközponti szolgáltatást nyújtó szolgáltató
- Legfelső szintű domainnév-nyilvántartó
- DNS-szolgáltató
- Tartalomszolgáltató hálózat szolgáltatója

Digitális szolgáltatók (kockázatos)

- Az online-piactér szolgáltatója
- E-Ker törvény szerinti keresőszolgáltató
- Közösségi média szolgáltatási platform szolgáltatója
- Domainnév regisztrációt végző szolgáltató

Érintett szervezetek

Alanyi főszabály

Állami vagy magánszervezetek, amelyek az előző dia szerinti ágazatok bármelyikébe tartoznak és amelyek legalább középvállalkozásnak minősülnek [legalább 50 munkavállalót foglalkoztatnak ÉS éves nettó árbevételük és/vagy mérlegfőösszegük meghaladja a 10 millió eurót], valamint az Európai Unión belül szolgáltatnak, tevékenykednek.

Fenti főszabály alóli kivételek

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

Alapvető követelmények

- Biztonsági osztályba sorolási kötelezettség („alap”, „jelentős” vagy „magas”)
- Megfelelő és arányos technikai, operatív és szervezési intézkedések meghozatala (pl. információs rendszerek biztonságáért felelős személy kijelölése)
- Vezetők felelősségi köre, felelősségre vonásuk lehetősége
- Ellátási lánc szerződéseinek felülvizsgálata
- Nyilvántartásba vételi kötelezettség SZTFH-nál (2024. január 1-től lép hatályba)
- Kiberbiztonsági események jelentése
- GDPR alapján már elkészített dokumentumok felülvizsgálata
- Domainnév-nyilvántartás kötelező adattartalmát meghatározza és domainnév-nyilvántartás integritására vonatkozó eljárásrendet SZTFH hagyja jóvá

Tanúsítással kapcsolatos alapfogalmak

- **Gyártó:** az IKT-termék gyártója, IKT-szolgáltatás nyújtója, valamint IKT-folyamat gyártója vagy nyújtója

  (tehát egyben gyűjtőfogalom is)
- **IKT-termék:** valamely hálózati vagy információs rendszer eleme vagy elemeinek csoportja
- **IKT-szolgáltatás:** olyan szolgáltatás, amely teljes mértékben vagy legnagyobb részben információ hálózati és információs rendszerek útján történő továbbításából, tárolásából, lekérdezéséből vagy kezeléséből áll
- **IKT-folyamat:** valamely IKT-termék vagy IKT-szolgáltatás tervezése, fejlesztése, rendelkezésre bocsátása, illetve nyújtása vagy karbantartása céljából végzett tevékenységek összessége

A nemzeti kiberbiztonsági tanúsítási rendszerek

- A megbízhatósági szintek: alap, jelentős és magas
- A tanúsítás vagy önértékelés:
  - jelentős és magas szint esetén nemzeti kiberbiztonsági tanúsítvány kiállítása, független szervezetek által
  - alap szint esetén megfelelőségi nyilatkozat (önértékelés) a nemzeti kiberbiztonsági tanúsítási rendszer alapján
- Kötelezettségek alanya: bármilyen „gyártó” – azaz IKT termék/szolgáltatás/folyamat szolgáltatója

A kiberbiztonsági felügyelet

- **Érintettek:** „kiemelten kockázatos” vagy „kockázatos” ágazatokban működő szolgáltatók és szervezetek
- **Hatósági ellenőrzés** éves ellenőrzési terv alapján, első elkészítése 2025. január 1-ig
- **Kiberbiztonsági felügyeleti díj –** mértéke SZTFH elnöke által rendeletben meghatározandó:

  az érintett szervezet előző üzleti évi nettó árbevételének legfeljebb 0,015%-a, de legfeljebb 10 millió forint
- erre javasolt lehet belső eljárásrenddel is felkészülni

A kiberbiztonsági audit

- Kétévente kötelező lesz
- Független, SZTFH által nyilvántartott auditor által
- Díjkötelesen (külön rendeletben meghatározandó díj)
- Az első kiberbiztonsági auditot 2025. december 31-ig kell elvégeztetni

Szankciók

- **Felhívás:** jogszabályban foglalt biztonsági követelmények vagy eljárási szabályok teljesítésére
- **Határidő tűzése:** biztonsági hiányosságok elhárítására vagy a megfeleléshez szükséges intézkedések meghozatalára
- **Eltiltás:** a biztonsági követelmények teljesülését közvetlenül veszélyeztető tevékenységtől
- Ha a fenti szankciók ellenére a szervezet az előírt követelményeket nem teljesít:
- **Pénzbírság:** majd kormányrendeletben meghatározottak szerint az SZTFH bírságot szabhat ki, amely további nemteljesítés esetén megismételhető

JAMBRIK ÜGYVÉDI IRODA

dr. Csiky András
1095 Boráros tér 7. (Duna Ház)
andras.csiky@jambrik.hu
www.jambrik.hu
+36 1 428 0028

Prezentációt készítette: Jambrik Ügyvédi Iroda részéről dr. Jambrik Gergely, dr. Markó-Tichy Krisztán, dr. Sonnevend-Valle Anna, dr. Csiky András