15 éve a tanácsadói piacon

Kiberbiztonsági (a NIS 2 irányelvnek való megfelelés) tanácsadás

2025. június 27.

KC | Könsberg CONSULTING

1. A JOGSZABÁLYI KÖRNYEZET

2022. december 27. napján megjelent az Európai Unió Hivatalos Lapjában: „Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) 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)". Az európai jogalkotó a kiberbiztonsági intézkedések kötelezettségét szélesebb körben határozta meg, melynek hatálya Ajánlatkérőre is, mint kiemelten kritikus ágazatban szolgáltatást nyújtó szereplőre is kiterjed.

A NIS 2 irányelvnek való tagállami megfelelést szolgálja Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.) elfogadása, amely a hatálya alá tartozó a gazdasági élet jelentős ágazatainak szereplői felé kiberbiztonsági követelményeket határozott meg, valamint megköveteli számukra **az elektronikus információs rendszereik védelme érdekében a kockázatmenedzsment keretrendszer létrehozását és működtetését.**

Az érintett ügyfelek önazonosításból eredő jogszabályi kötelezettségeiknek eleget téve a tavalyi évben elvégezték szervezetük minősítését és a Szabályozott Tevékenységek Felügyeleti Hatósága Kiberbiztonsági Igazgatósága (a továbbiakban: SZTFH) felé történő jogszabályban meghatározott adataik megküldésével kérték/kérhették a hatósági nyilvántartásba vételt.

Az SZTFH által nyilvántartásba vett érintett szervezetek, valamint a Kiberbiztonsági tv. 16. § (1) bekezdés alapján a kockázatos és kiemelten kockázatos ágazatokban tevékenykedő szolgáltatók, szervezetek kiberbiztonsági audit lefolytatására kötelesek.

Az audit során vizsgált követelményeknek való megfelelés bizonyítása érdekében ezen szervezetek elektronikus információs rendszereinek meg kell felelniük a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendeletben (továbbiakban: MKr.) foglaltaknak. A fent hivatkozott kiberbiztonsági audit díjtételeiről és módszertanáról a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról szóló 1/2025. (I. 31.) SZTFH rendelet rendelkezik, amely 2025. február 3. napjától hatályos.

A kiberbiztonsági audittal kapcsolatos határidők 2025.05.31. napjától hatályos jogszabály szerint az alábbiak szerint módosultak:

- a kiberbiztonsági audit elvégzésére az SZTFH által nyilvántartásba vett audit végrehajtására jogosult gazdálkodó szervezettel **megállapodást kötési kötelezettség legkésőbb 2025. augusztus 31-ig;**
- **az első kiberbiztonsági audit pedig legkésőbb 2026. június 30-ig kötelezettség el is végeztetni.**

2. A CÉGÜNK ÁLTAL NYÚJTOTT SZOLGÁLTATÁS BEMUTATÁSA

Cégünk a NIS 2 irányelv, valamint a kapcsolódó hazai szabályozás szerinti megfelelés biztosításának felmérésére teljeskörű tanácsadást nyújt Önnek, hogy jogszabályi kötelezettségeinek az előírt határidőben maximálisan meg tudjon felelni.

Először is fel kell mérjük, hogy Ön és szervezete a kiberfenyegetések által okozható károk mértékével arányos módon jelenleg a NIS 2 irányelv szerinti legfontosabb kötelezettségeinek milyen módon felel meg, ezek az alábbiakat tartalmazzák:

- gondoskodott-e a szervezete által használt EIR-ek, központi szolgáltatások felméréséről és nyilvántartásba vételéről;
- a szervezet rendelkezésében lévő EIR-eket a Kiberbiztonsági tv.-nek megfelelően biztonsági osztályba sorolta-e;
- teljeskörűen bevezetésre került-e a kockázatmenedzsment keretrendszer szervezete esetében, mely magában foglalja a kiberbiztonsággal kapcsolatos kockázatkezelési tevékenységeket úgy, mint:
  - a rendszerfejlesztési életciklusban a kockázatokkal arányos védelmi intézkedések azonosításán, bevezetésén, értékelésén, működtetésén;
  - valamint nyomon követésén keresztül az új és már használatban lévő rendszerek fenyegetettségeinek folyamatos felderítése, és kockázatainak hatékony kezelése érdekében;
- a szervezet vezetőjeként biztosítja-e az EIR-ek védelmére vonatkozó a Kiberbiztonsági tv-ben foglalt kötelezettségeit, valamint
- a szervezete teljeskörűen felkészült-e a fentiekre, amelyet a kiberbiztonsági audit során független auditor előtt tud is bizonyítani.

A Kiberbiztonsági tv. alapján ezt követően felmérjük az Ön által használt EIR-eket, központi szolgáltatásokat és segítünk a megfelelő nyilvántartásba vételükben a következők szerinti bontásban:

- a szervezete rendelkezésében lévő EIR-ek;
- a szervezete által használt központi rendszerek;
- a szervezete által igénybe vett, központi szolgáltató által biztosított szolgáltatások és támogató rendszerek;
- a szervezete rendelkezésében lévő vagy a szervezet által használt egyéb támogató rendszerek.

A fenti nyilvántartásba vett EIR-jeit adatszolgáltatás és online interjú(k) keretében részletesen feltérképezzük és javaslatot teszünk a biztonsági osztályba való sorolásukra vonatkozóan. A biztonsági osztályba sorolásról ezt követően a szervezet vezetője dönt, és az eredmények a szervezet EIR nyilvántartásában vagy egyéb belső szabályzatába történő rögzítését elvégezzük.

Ezt követően megkezdjük a mindenre kiterjedő NIS 2 irányelv szerinti hiányfeltárást (GAP analízis) – azaz a szervezete információbiztonsági átvilágítását. A GAP analízis célja annak meghatározása, hogy az MKr. szerint kategórizált EIR-jei az előző pontban elvégzett biztonsági osztály követelményeihez képest milyen biztonsági szintet teljesítenek és milyen teendői vannak Önnek annak érdekében, hogy megfeleljen az MKr.-ben előírt biztonsági szint szerinti követelményeknek. A GAP elemzést az Ön redelkezésében lévő összes EIR-re el kell végezni.

A GAP analízis feladatai:

- GAP analízis elvégzése az egyes EIR-ek esetében az MKr.-ben meghatározott fenyegetések kockázatelemzés módszerével történő számbavételével;
- dokumentumelemzés keretében felmérni, hogy az Ön szervezetének meglévő hatályban lévő belső szabályozói (pl. IBSZ, BCP/DRP, GDPR) mennyire támogatják a NIS 2 megfelelést;
- a fennmaradó kockázatok kezelésére cselekvési/intézkedési terv készítése (tartalmazza a szervezet által tervezett rövid védelmi intézkedés leírását, a szervezeten belüli felelősöket és a határidőket).

A GAP analízis - információbiztonsági átvilágítás során kapott adatok alapján:

- azonosítjuk az IT rendszerek (EIR) és folyamatok kockázatait, például az adatvesztési vagy biztonsági réseket;
- pontos képet kapunk a jelenlegi adatvédelmi és biztonsági védelmi intézkedésekről, megjelölve az esetleges hiányosságokat, valamint
- feltérképezzük, hogy milyen lépésekre van szüksége az Ön szervezetének a kiberbiztonsági audit sikeres teljesítéséhez.

Ezt követően a NIS 2 implementációra való felkészítési tanácsadás keretében teljeskörű szakmai segítséget nyújtunk Önnek a NIS 2 irányelvnek és a hazai jogszabályi kötelezettségeknek való megfelelés érdekében a GAP analízis eredményeként meghatározott védelmi intézkedések megvalósításában hiányzó vagy felülvizsgálandó szabályozók, dokumentumok, folyamatok, kontrollok elkészítésében.