MELASZ

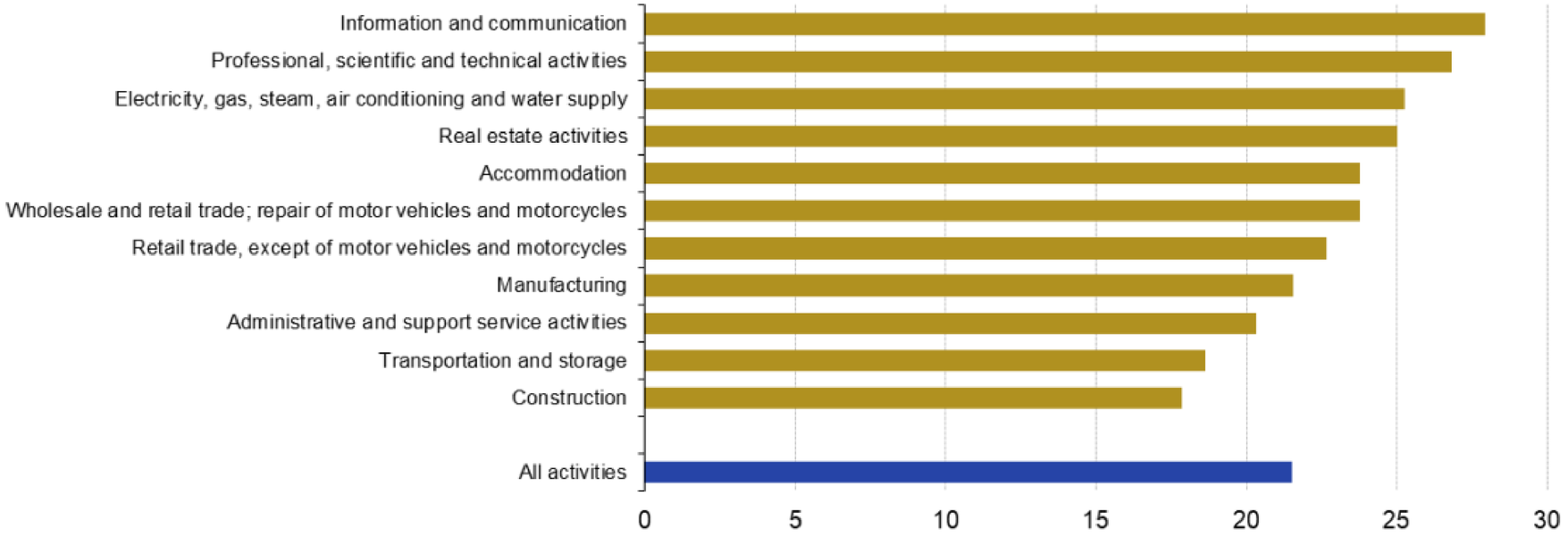
A NIS2 bevezetésének aktuális kérdései és tapasztalatai a hatóság szemszögéből

Budapest, 2025.06.30.

Szabó Dorina Barbara

Helyzetkép – hatalmas fejlődési lehetőség

Enterprises experienced ICT related security incidents leading to consequences, by economic activity, EU, 2023
(% of enterprises)

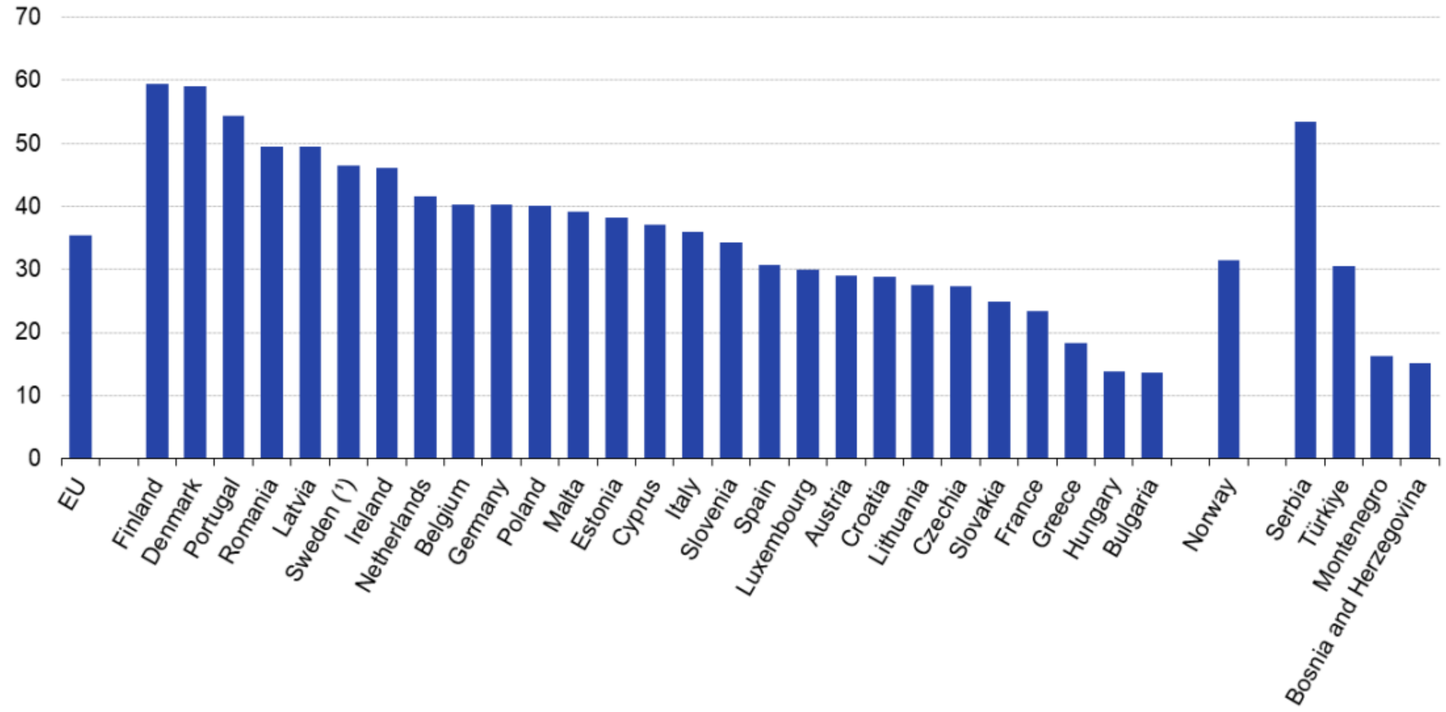


Source: Eurostat (online data code: isoc_cisce_icn2)

eurostat

Helyzetkép – hatalmas fejlődési lehetőség

Enterprises with documents on measures, practices or procedures on ICT security, 2024
(% of enterprises)



(1) Break in the time series
Source: Eurostat (online data code: isoc_cisce_ra)

eurostat

Európai Uniós jogszabályi környezet

2016/1148 EU irányelv

NIS (Network and Information Security)

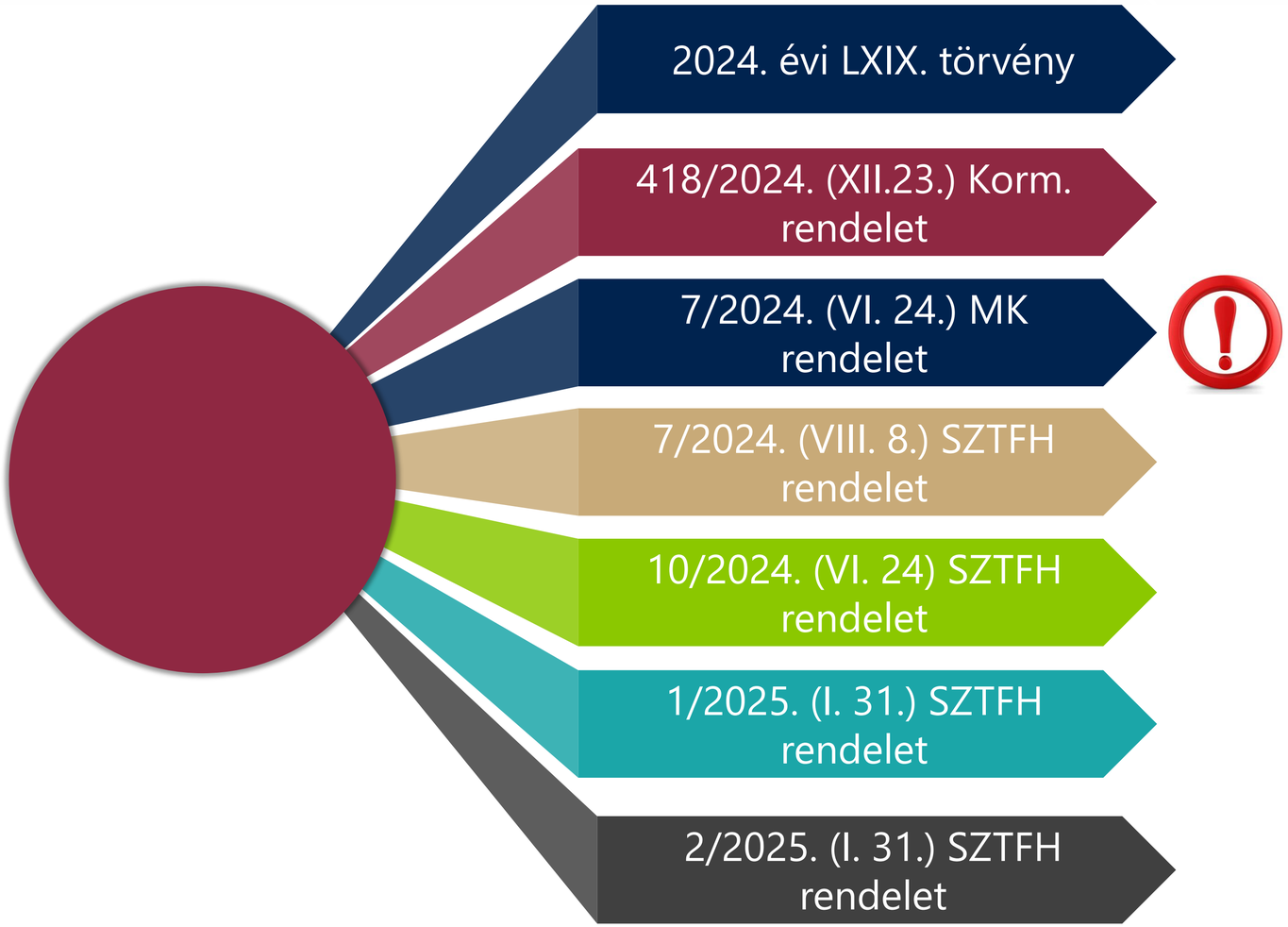
2019/881 EU rendelet

ENISA (Európai Uniós Kiberbiztonsági Ügynökség) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról

2022/2555 EU irányelv

NIS2 - az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről

Hazai jogszabályi környezet



Magyarország kiberbiztonságáról

Magyarország kiberbiztonságáról szóló törvény végrehajtásáról (a továbbiakban: Kiberbiztonsági törvény)

A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

A kiberbiztonsági audit végrehajtására jogosult auditorok nyilvántartásáról és az auditorral szemben támasztott követelményekről

Az IoT-eszközök nemzeti kiberbiztonsági tanúsítási rendszeréről

A kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról

A kiberbiztonsági felügyeleti díjról

Kiberbiztonsági felügyelet – érintett szervezetek

A hatósági nyilvántartásba vétel, együttműködés

- **A nyilvántartásba vétel az SZTFH honlapján található, az *SZTFH – 420 Érintett szervezet nyilvántartásba vételére irányuló kérelem* elektronikus űrlapon keresztül kezdeményezhető.**
- **A nyilvántartásba vétel a kérelemben szereplő adatok alapján történik.**
- **Amennyiben az érintett szervezet esetében változás következett be, azt az *SZTFH – 421 Érintett szervezet nyilvántartásba vételére irányuló kérelem* elektronikus űrlap segítségével lehet Hatóságunk felé jelezni.**
- **A Hatósággal folytatott együttműködés keretében a szervezet vezetője gondoskodik az adatoknak, dokumentumoknak, valamint ezek változásainak, a változást követő tizenöt napon belül a kiberbiztonsági hatóság részére – nyilvántartásba vétel céljából – történő megküldéséről.**

Audit – és felügyeleti díj fizetési kötelezettség

A Kiberbiztonsági törvény alapján:

Azon szervezetek, melyek a Kiberbiztonsági törvény 1. § (1) bekezdés b) pontja szerinti azon szervezetek, amelyek egyúttal a 2. és 3. melléklet szerinti szervezetek is, valamint az 1. § (1) bekezdés d) pontja és – a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény szerinti mikrovállalkozás kivételével – az 1. § (1) bekezdés e) pontja szerinti szervezetek,
kötelesek a kétévenkénti kiberbiztonsági audit lefolytatására, valamint a felügyeleti díj megfizetésére, abban az esetben is, ha esetükben a hatósági felügyeletet nem az SZTFH látja el.

Vagyis:

- **a mikrovállalkozások mentesülnek az auditkötelezettség alól, de a felügyeleti díj fizetési kötelezettségük továbbra is fennáll, valamint**
- **azon szervezetek, melyek többségi állami tulajdonban vannak, de az SZTFH nyilvántartásában is szerepelniük kell, kiberbiztonsági felügyeleti díj fizetésére és a rendelkezésükben álló EIR-ek tekintetében auditra kötelezettek.**

Hatósági ellenőrzések

A kiberbiztonsági felügyelet és feladatellátás és a hatósági ellenőrzés lefolytatásának részletes szabályairól, valamint az információbiztonsági felügyelőről szóló 3/2025 (IV.17.) SZTFH rendelet alapján:

A Kiberbiztonsági törvény 1. § (1) bekezdés d) pontja és e) pontja – a Kiberbiztonsági tv. 23. § (1) bekezdés a) pontja hatálya alá nem tartozó – szerinti szervezetek tekintetében hatósági ellenőrzéseket végezhet.

Vagyis:

- **Az auditkötelezettség alóli mentesülés ≠ a védelmi intézkedések teljesítése alóli mentesüléssel.**

Ezen felül a Kiberbiztonsági törvény 1. § (1) bekezdés d) és e) pontja szerinti szervezetek esetében a hatósági ellenőrzésekben minden, a hatósági nyilvántartásban szereplő szervezet érintett lehet.

Az audit lefolytatására vonatkozó határidő

A Magyar Kereskedelmi és Iparkamara és az SZTFH közösen kezdeményezte a Kiberbiztonsági törvény módosítását annak érdekében, hogy:

- **az audit lefolytatásának végső határideje 2026. június 30. legyen, ugyanakkor**
- **2025. augusztus 31-ig szerződést kell kötni a kötelezetteknek az általuk választott auditorral, a kiberbiztonsági audit lefolytatására vonatkozóan.**

A módosító javaslat a 2025. évi XXXII. törvény kihirdetésével elfogadásra került.

Az auditorok

AUDITOR	BIZTONSÁGI OSZTÁLY	STÁTUSZ	MŰVELET
Alverad Technology Focus Korlátolt Felelősségű Társaság	Alap	Aktív	Részletek
Andrews IT Engineering Mérnöki, Információtechnikai és Szolgáltató Korlátolt Felelősségű Társaság	Alap	Aktív	Részletek
Certop Informatikai Tanúsítási Szolgáltatások Korlátolt Felelősségű Társaság	Jelentős, Alap	Aktív	Részletek
Ernst & Young Tanácsadó Korlátolt Felelősségű Társaság	Alap	Aktív	Részletek
HUNGUARD Számítástechnikai-, informatikai kutató - fejlesztő és általános szolgáltató Korlátolt Felelősségű Társaság	Magas, Jelentős, Alap	Aktív	Részletek
KÜRT Információbiztonsági és Adatmentő Zrt.	Jelentős, Alap	Aktív	Részletek
Mikroháló Távközlési, Szolgáltató Korlátolt Felelősségű Társaság	Alap	Aktív	Részletek
NETI Informatikai Tanácsadó Kft.	Alap	Aktív	Részletek
VALILAB IT Biztonsági Vizsgálólaboratórium Korlátolt Felelősségű Társaság	Alap	Aktív	Részletek
VERITAN Hírközlési és Informatikai Tanúsító Kft.	Alap	Aktív	Részletek

Fontos, hogy

- **az „alap” biztonsági osztályba sorolt EIR vizsgálatára feljogosított auditor:**
  - **„alap”**
- **a „jelentős” biztonsági osztályba sorolt EIR vizsgálatára feljogosított auditor:**
  - **„alap”**
  - **„jelentős”**
- **a „magas” biztonsági osztályba sorolt EIR vizsgálatára feljogosított auditor**
  - **„alap”**
  - **„jelentős”**
  - **„magas”**

biztonsági osztályba sorolt EIR-ek vizsgálatára jogosult.

Az audit díja - 1/2025. (I.31.) SZTFH Rendelet

Előző üzleti évi nettó árbevétel

Szorzószám az árbevétel függvénye:

0,9-4

EIR darabszáma

Darabszám függvénye a szorzószám

- 1-5 EIR: 1
- 6-15 EIR: 2,5
- 16 vagy több: 4

EIR biztonsági osztálya

Szorzószám biztonsági osztályonként:

- alap: 1
- jelentős: 3
- magas: 5

1 750 000 forint

alapdíj

Az audit díja

1.575.000 forint

Minimum

EIR száma: 1-5 között

Árbevétel < 1 milliárd

Biztonsági osztály: alap

140.000.000 forint

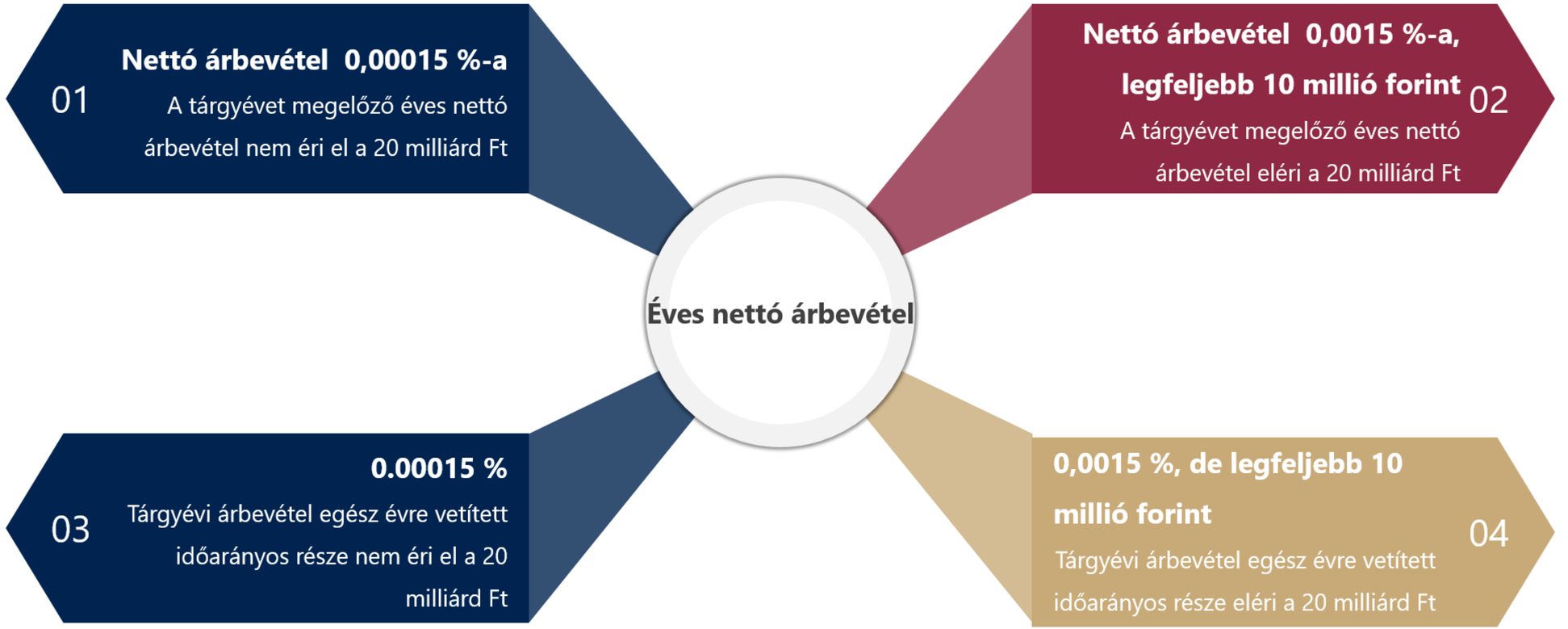
Maximum

EIR száma: 16 vagy több

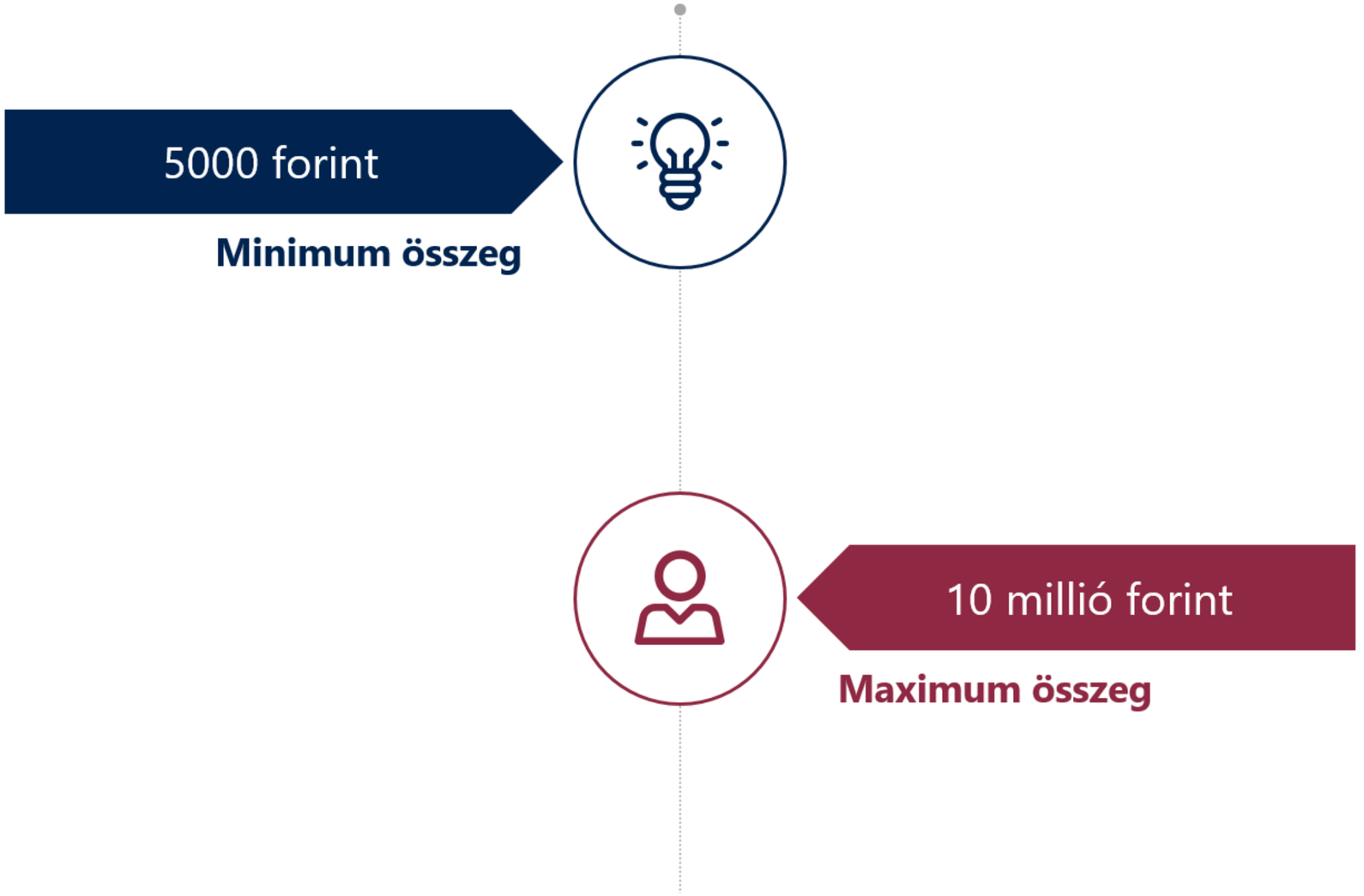
Árbevétel:>40 milliárd

Biztonsági osztály: magas

A kiberbiztonsági felügyeleti díj – 2/2025 (I.31.) SZTFH Rendelet



A kiberbiztonsági felügyeleti díj



A kiberbiztonsági felügyeleti díj - határidők

Digitális szolgáltatók - kiberbiztonsági audit

A DÁP törvény alapján:

a) hulladékgazdálkodási közszolgáltatási résztevékenység körébe tartozó szolgáltatást nyújtó,
b) távhőszolgáltató,
c) a földgáz egyetemes szolgáltatói engedélyes és a földgázelosztói engedélyes,
d) a víziközmű-szolgáltatást nyújtó,
e) a szennyvíz rendszeres begyűjtésére, gyűjtésére, elszállítására és elhelyezésére irányuló szolgáltatást nyújtó,
f) a kéményseprő-ipari szolgáltatást nyújtó,
g) az egyetemes postai szolgáltatást nyújtó,
h) a villamos energia egyetemes szolgáltatói engedélyes és a villamos energia elosztói,
o) az egyéni előfizetői szolgáltatást nyújtó elektronikus hírközlési szolgáltatógazdálkodó szervezet

az elektronikus információs rendszereik tekintetében a kiberbiztonsági követelményeknek való megfelelést a Magyarország kiberbiztonságáról szóló törvényben foglalt kiberbiztonsági követelményeknek való megfelelés biztosításával, valamint kiberbiztonsági audit lefolytatásával teljesítik.

Audit eredménye – VMI

VMI:

$$VMI = 100 - 100 * \frac{2*\sum_{i=1}^{n} b_i + \sum_{j=1}^{m} t_j}{20n+10m}$$

A „Biztosító” típusú követelménycsoportok kétszeres, míg a „Támogató” típusú követelménycsoportok teljesítése egyszeres súlyozással számítódik a képlet alapján és amely alapján az eltérés mértéke az alábbiak szerint alakul:

Eltérés mértéke	Az EIR-nek a védelmi intézkedések katalógusa elvárásainak való megfelelés szempontjából történő értékelése
VMI ≥ 95	megfelel
90 ≤ VMI < 95	alacsony kockázattal megfelel
80 ≤ VMI < 90	jelentős kockázattal megfelel
70 ≤ VMI < 80	magas kockázattal megfelel
VMI < 70	nem felel meg

Audit eredménye – SZEKI

SZEKI: $$szervezet\ ellenálló - képességi\ indexe = \frac{\sum_{i=1}^{n} VMI_i}{n}$$

A VMI értékek számtani átlaga, amely alapján a szervezet minősítése az alábbiak szerint alakul:

A szervezet értékelése	A szervezetnek a védelmi intézkedések katalógusa elvárásainak való megfelelés szempontjából történő minősítése	Értékelés eredménye
SZEKI ≥ 95	elhanyagolható kockázattal megfelel	megfelelt
90 ≤ SZEKI < 95	alacsony kockázattal megfelel	auditált
80 ≤ SZEKI < 90	közepes kockázattal megfelel	
70 ≤ SZEKI < 80	magas kockázattal megfelel	
SZEKI < 70	kritikus kockázattal nem felel meg	nem megfelelt

kiberbiztonsag@sztfh.hu

Köszönöm a figyelmet!