



NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA

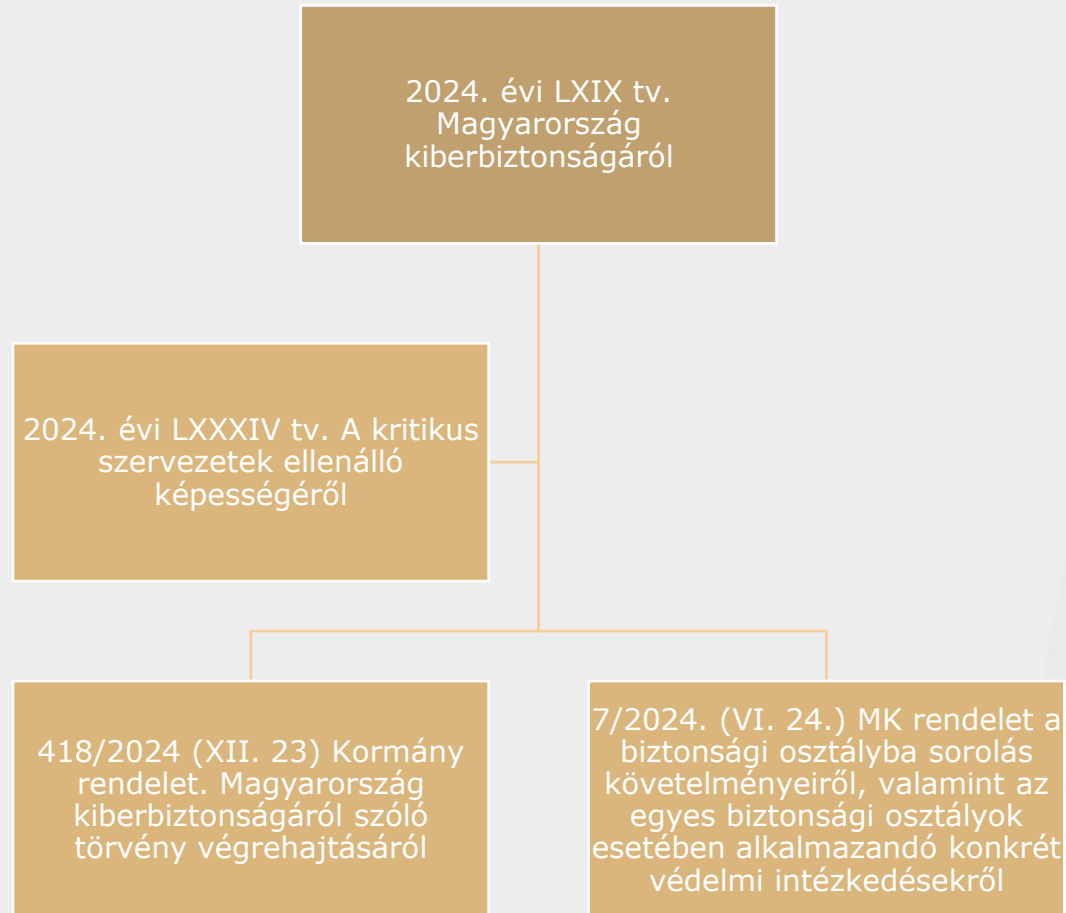
Magyarország új kiberbiztonsági stratégiája – és érdekességei

Dr. Krasznay Csaba

egyetemi docens

NKE ÁNTK Kiberbiztonsági tanszék

Kiberbiztonsági jogszabályok 2025-től



- 578/2023. (XII. 19.) Korm. rendelet a honvédelmi célú elektronikus információs rendszerek korai figyelmeztető rendszeréről
- 15/2023. (VII. 31.) SZTFH rendelet a Szabályozott Tevékenységek Felügyeleti Hatósága kiberbiztonsági feladataival összefüggő eljárásainak igazgatási szolgáltatási díjairól
- 7/2024. (VI. 24.) SZTFH rendelet a kiberbiztonsági audit végrehajtására jogosult auditorok nyilvántartásáról és az auditorral szemben támasztott követelményekről
- 23/2023. (XII. 19.) SZTFH rendelet az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásáról
- 10/2023. (V. 15.) SZTFH rendelet az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról
- 341/2024. (XI. 14.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltatásokról
- 608/2023. (XII. 22.) Korm. rendelet a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsításról
- 214/2020. (V. 18.) Korm. rendelet az elektronikus információbiztonsági korai figyelmeztető rendszerről
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról
- 2/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági felügyeleti díjról
- 2/2025. (II. 6.) MK utasítás kiberbiztonságért felelős biztos kinevezéséről

Ami még hiányzik

- A kiberbiztonsági szolgáltatások nyújtására jogosult szerv kijelölése
- A kiberbiztonsági szolgáltatások részletes szabályainak meghatározása
- **A szervezet vezetőjének, az IBF-nek és az információbiztonsági felügyelőnek a képzési követelményei**
- A kötelezően alkalmazandó nemzeti vagy európai kiberbiztonsági tanúsítási rendszer alapján tanúsított IKT-termékeket, IKT-szolgáltatásokat vagy IKT-folyamatokat felhasználó szervezetek kijelölése
- A poszt-kvantumtitkosítással kapcsolatos szabályok
- A sérülékenységvizsgálat lefolytatására és a kiberbiztonsági incidensek kezelésére jogosult gazdálkodó szervezetekre vonatkozó szabályok

Magyarország kiberbiztonsági stratégiája

**Nemzeti
Jogszabálytár**

Magyar Közlöny  Cégközlöny 

Belépés

A-

A+

Hu





Szókereső

Paragrafus



ELI





1089/2025. (III. 31.) Korm. határozat

Magyarország Kiberbiztonsági Stratégiájáról

✓ Hatályos: 2025. 04. 01. – 

A Kormány

1. elfogadja Magyarország Kiberbiztonsági Stratégiáját az [1. melléklet](#)ben foglaltak szerint, és felhívja a Miniszterelnöki Kabinetirodát vezető minisztert, hogy gondoskodjon a stratégia kormányzati honlapon történő közzétételéről;

Felelős: Miniszterelnöki Kabinetirodát vezető miniszter
Határidő: azonnal

2. felhívja a kiberbiztonságért felelős biztost, hogy – a feladat- és hatáskörükben érintett miniszterek bevonásával – intézkedjen az [1. melléklet](#)ben foglalt Magyarország Kiberbiztonsági Stratégiája végrehajtását szolgáló Nemzeti Kiberbiztonsági Akcióterv (2025–2030) elkészítése érdekében;

Felelős: kiberbiztonságért felelős biztosérintett miniszterek
Határidő: a Nemzeti Kiberbiztonsági Munkacsoport megalakulását követő 90 nap

3. felhívja a kiberbiztonságért felelős biztost, hogy – a feladat- és hatáskörükben érintett miniszterek bevonásával – intézkedjen Magyarország Kiberbiztonsági Stratégiájának felülvizsgálata és szükség szerinti aktualizálása érdekében;

Felelős: kiberbiztonságért felelős biztosérintett miniszterek
Határidő: 2030. december 31.

Érdekességek 1: A legnagyobb kihívások



Érdekességek 2: A kiemelt operatív szereplők

kiberbiztonsági incidenskezelő központok (CSIRT)

- a nemzeti kiberbiztonsági incidenskezelő központ,
- honvédelmi kiberbiztonsági incidenskezelő központ,
- ágazaton belüli kiberbiztonsági incidenskezelő központ,

a kiberbiztonsági hatóságok,

az egyedüli kapcsolattartó pont (SPOC),

az (EU) 2021/887 európai parlamenti és tanácsi rendelet szerinti, a kiberbiztonsági kompetenciaközösséggel való kapcsolattartásra kijelölt nemzeti koordinációs központ,

a Magyar Honvédség kibervédelmi erői,

a Rendőrség információs rendszerekkel összefüggő bűncselekmények megelőzésére, felderítésére hivatott szervezetei,

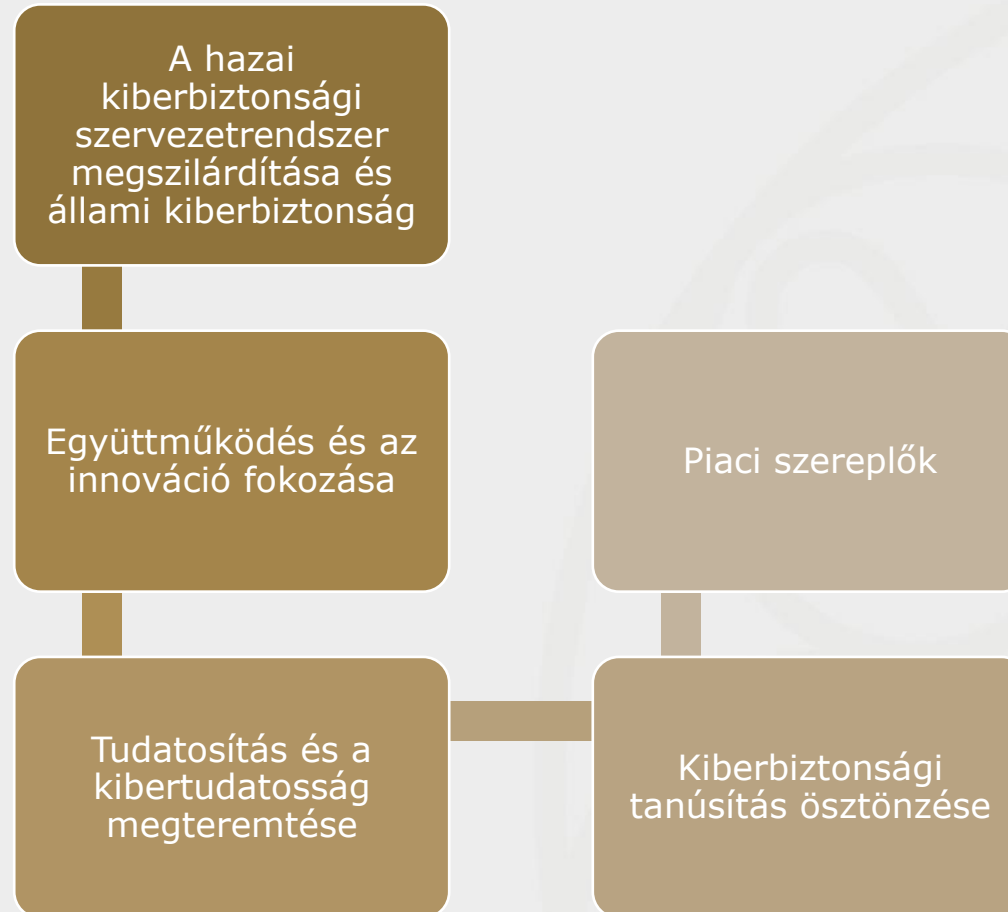
az operatív kiberbiztonsági központok (SOC),

az információmegosztó és elemző szervezetek (ISAC),

a szakágazati egyetemek, kutatóintézetek,

az érintett állami és gazdasági szereplők.

Érdekessegek 3: Prioritások



Érdekessegek 4: Kiemelt ágazatok



Érdekességek 5: Az ISAC-ek



Érdekeség 6: A kiberbiztonság, mint gazdasági lehetőség

A kiberbiztonság erősítése nemcsak védelmi feladat, hanem gazdasági lehetőség is. Ennek kiaknázása érdekében a jövőbe mutató kihívásokra úgy érdemes felkészülni, hogy ne csak finanszírozandó területként, hanem gazdasági, társadalmi és pénzügyi forrásként tekintsünk a kiberbiztonságra, mert a kiberbiztonság fejlesztésében nemcsak védelmi szempontok érvényesülése játszik szerepet, hanem egyedülálló gazdasági potenciál is rejlik benne. Magyarország elkötelezett olyan innovatív kiberképességek kutatása, fejlesztése és kiépítése iránt, amelyek önálló szellemi termékként vagy erre épülő magas minőségi szintű szolgáltatásként jelenhetnek meg határainkon túl is. Hazánk célja mindezek mellett a kibertérben rejlő lehetőségek, az abból következő komplex hatások és a biztonsági vonatkozások tekintetében is kutatásokkal és elemzésekkel vizsgálni a társadalmi, kulturális, állami működési kapcsolódásokat, és kiaknázni ezek eredményeit a kiberbiztonság fokozása terén is.

Nemzeti Kiberbiztonsági Akcióterv (2025–2030)

10.2. Végrehajtás

A kiberstratégia hatékony végrehajtásához egy kooperatív elvek mentén megfogalmazott intézkedési terv elkészítése és végrehajtása szükséges, amelynek segítségével a stratégiában megfogalmazott célkitűzések és szakpolitikai intézkedések maradéktalanul és hatékonyan teljesülhetnek, segítve a beazonosított kitettségek és kockázatok minimalizálását, különös tekintettel a szakemberhiányra, az együttműködés elmélyítésére, az ellenálló képesség célrendszerének érvényesülésére, az adatbiztonság növelésére, a kiberbiztonsági oktatásban részt vevők körének kiszélesítésére és a tananyagok folyamatos felülvizsgálatára. A magyar kibertér biztonságáért felelős intézményrendszer folyamatosan figyelemmel kíséri a digitális környezetben jelentkező kihívások dinamikus változását, és szükség szerint a stratégia felülvizsgálatával reagál az új feladatokra².

Összefoglalás





KÖSZÖNÖM A FIGYELMET!

uni-nke.hu