Nevet váltunk, irányt nem

Szabó Lajos
NBSZ NKI Igazgató

10 éves a Cybersec

„Szabályok,
megfelelés,
tudatosság”

Idei témáink

- digitális bűnözés elleni hatósági fellépések
- sérülékenységvizsgálatok és incidenskezelés aktuális gyakorlatai
- információbiztonsági ellenőrzések,
- ipari kibervédelem,
- állami honeypotok működése,
- Az MI és deepfake-technológiák jelentette kihívások,
- a kiberpszichológia és a tudatosság növelése.

A kiberbiztonság
ma **már nem csupán**
informatikai kérdés
– hanem a nemzeti
szuverenitás, a gazdasági
stabilitás és a társadalmi
bizalom kulcseleme.

Új stratégia és szervezetrendszer

Magyarország 2025-ben új kiberbiztonsági korszakba lépett.

- A 1089/2025. (III. 31.) Korm. határozat rögzíti az új **Nemzeti Kiberbiztonsági Stratégiát**, és elindította a **Nemzeti Kiberbiztonsági Akcióterv** (2025–2030) megvalósítását.

Az új szervezetrendszer három pilléren nyugszik:

Nemzeti Kiberbiztonsági Munkacsoport – stratégiai irány, kormányzati koordináció

Nemzeti Kiberbiztonsági Fórum – szakmai közösség, tudásmegosztás, párbeszéd

Kiberbiztonsági Operatív Törzs – gyors és összehangolt válságkezelés

A modell célja: gyors reagálás, hatékony koordináció, közös döntésképesség, illeszkedés az EU-s ökoszisztémába.

Új jogszabályi környezet

- 2025. január 1-jével hatályba lépett a **2024. évi LXIX. törvény Magyarország kiberbiztonságáról**, amely a NIS2 irányelv hazai átültetése.
- A törvény és a **418/2024. (XII. 23.) Korm. rendelet** új, kockázatalapú és egységes követelményrendszert hozott létre.

Új jogszabályi környezet

Kulcselemei:

- „Alapvető” és „fontos” szervezeti kategóriák
- Vezetői felelősség és folyamatos megfelelés
- Kockázatértékelés, hiányfelmérés, ütemterv
- Beszállítói lánc-biztonság és rendszeres gyakorlatok

A jogszabály célja: átláthatóbb, kockázatarányos kiberbiztonsági megfelelés – minden érintett szervezet számára.

Ügyfélstruktúra és szereplők

A NIS2 hatálya kiterjed:

- kritikus infrastruktúrákra,
- közszolgáltatókra,
- digitális szolgáltatókra,
- és közérdekű vállalkozásokra.

A kibervédelmi ökoszisztéma szereplői:

- állami szervek és hatóságok (SZTFH, MNB, HM)
- piaci és technológiai szolgáltatók,
- oktatási és kutatási intézmények,
- valamint a Nemzeti Kiberbiztonsági Intézet mint központi szereplő.

Az NKI a magyar kibertér rezilienciájának motorja – hatóság, elemző központ és tudásmegosztó közösség egyben.

Az NKI a megelőzés – észlelés – reagálás – helyreállítás teljes folyamatát lefedi.

Az NKI feladatai

- **Hatósági feladatok** – felügyelet, ellenőrzés, megfelelés
- **Sérülékenységvizsgálat** – hivatalból és kérelemre, minden szektorban
- **Nemzeti CSIRT** – incidensek fogadása, elemzés, reagálás
- **Biztonsági elemzés** – log-, forensics-, malware-elemzés
- **Fenyegetettség- és tudatosságnövelés** – CTI, Honeypot, EWS, képzések, kiberverseny

Újdonságok

- új sérülékenységvizsgálati rendszer és automatizált elemzés (AI-támogatással)
- Zero Trust és identitás-alapú védelem előmozdítása
- SBOM és beszállítói due diligence módszertan bevezetése
- OT/ICS fókusz, a SECTOR16 tapasztalatain alapulva
- felhő-biztonsági láthatóság és naplózási sztenderdek erősítése
- poszt-kvantum felkészülés és hibrid kriptográfiai gyakorlatok

Köszönöm a figyelmet!