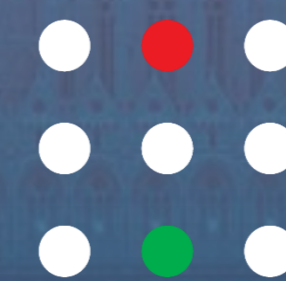


Az SZTFH szerepe a kiberbiztonságban

dr. Bencsik Balázs
igazgató



SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága

Stabil, kiszámítható működési és szabályozási környezet biztosítása a kiemelt ágazatok számára

2021. október 1-től:

- Szerencsejáték Felügyelet,
- Nemzeti Dohánykereskedelmi Nonprofit Zrt.,
- Felszámolóok Névjegyzékét Vezető Hatóság,
- IM Bírósági végrehajtói felügyelet.

2022. január 1-től:

- Magyar Bányászati és Földtani Szolgálat,
- Kiberbiztonsági tanúsítás.



**A Szabályozott
Tevékenységek
Felügyeleti Hatósága**

milliárd forint **2000**

Az iparági szereplők éves szinten több mint 2000 milliárd forintos árbevételt realizálnak.

ezer ember **50**

Az ágazati szereplők mintegy 50 ezer főnek kínálnak munkahelyet.

ezer család **150**

Az ágazatok közvetve és közvetetten 100-150 ezer ember megélhetését biztosítják.

milliárd forint **700**

A felügyelt tevékenységekből évi 700 milliárd forint adó és járulékbévételek származik.

Kiemelkedő jelentőség és felelősség, hatékony hatósági mozgástérrel párosítva.

A Hatóság küldetése a **nemzeti önrendelkezés visszaállítása és megőrzése** a kiemelt ágazatokban.

- **Egység:** centralizált felügyelet
- **Hatékonyság:** gyors reakció
- **Érdekvédelem:** hatékony fogyasztóvédelem
- **Felelősség:** megerősített szuverenitás

Kiberbiztonsági tanúsítás



SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága



- 1. Kiberbiztonsági tanúsítás**
2. Poszt-quantum titkosítás
3. Kommunikáció, awareness

- (EU) 2019/881 európai parlamenti és tanácsi rendelet + lbtv. III. fejezet
- Tanúsító hatóságok:
SZTFH (általános feladatkörben)
KNBSZ (hadiipari kutatás, fejlesztés, gyártás és kereskedelem)
- Két típusú eljárás:
megfelelőségi önértékelés (gyártó)
megfelelőségértékelés (akkreditált és nyilvántartásba vett szervezet)



- 1. Kiberbiztonsági tanúsítás**
2. Poszt-kvantum titkosítás
3. Kommunikáció, awareness

Európai tanúsítási rendszerek

- az érintett termékek és szolgáltatások kategóriáit;
 - a kiberbiztonsági követelményeket (szabványok vagy műszaki előírások);
 - az értékelés típusát (önértékelés vagy harmadik fél általi vizsgálat);
 - a garantált szintet (alap, jelentős, magas).
-
- Tanúsítvány: minden EU tagállamban kötelező elfogadni



- 1. Kiberbiztonsági tanúsítás**
2. Poszt-kvantum titkosítás
3. Kommunikáció, awareness

Európai tanúsítási rendszerek

EUCC

- Common Criteria (ISO/IEC 15408, ISO/IEC 18045)
- EU végrehajtási rendelet-tervezet

EUCCS (European Cybersecurity Certification Scheme for Cloud Services)

- felhőszolgáltatások
- tervezet

5G

IoT





Poszt-quantumtitkosítás:

- a matematikailag igazolható,
- kvantumszámítógép által megvalósított támadás ellen
- a hagyományos kriptográfiai alkalmazáson felüli titkosítás

Alkalmazásra kötelezett szervezet:

- a kormányzati célú hálózatokról szóló kormányrendelet szerinti igénybevételre kötelezett szervezet,
- a hitelintézetekről és a pénzügyi vállalkozásokról szóló törvény szerinti bank
- Közműszolgáltató (villamosenergia, földgáz, távhő, víz, hulladék)

1. Kiberbiztonsági tanúsítás
- 2. Poszt-quantum titkosítás**
3. Kommunikáció, awareness



Poszt-kvantumtitkosítás alkalmazást nyújtó szervezet

- nemzetbiztonsági kockázatot nem jelent
- telephely biztonsági tanúsítvánnyal rendelkezik
- munkavállalója, alvállalkozója személyi biztonsági tanúsítvánnyal rendelkezik,
- az informatikai rendszere zártsági tanúsítással rendelkezik
- Szakvélemény: alkalmazás kriptográfiai alkalmazáson felüli biztonságot nyújtó poszt-kvantumtitkosításra alkalmas
- SZTFH nyilvántartásba vett

1. Kiberbiztonsági tanúsítás
- 2. Poszt-kvantum titkosítás**
3. Kommunikáció, awareness

1. Kiberbiztonsági tanúsítás
2. Poszt-quantum titkosítás
3. **Kommunikáció, awareness**

Az állampolgárok, vállalkozások felé elmagyarázza az Internet biztonság, a kiberbiztonság, valamint a digitalizációból fakadó lehetőségeket és veszélyeket, és támogatást biztosít a biztonság tudatos digitális élethez



1. Kiberbiztonsági tanúsítás
2. Poszt-quantum titkosítás
- 3. Kommunikáció, awareness**

Kiberkoalíció

együttműködési fórum, amelyben az állam részéről az SZTFH, a piac részéről a meghívott vállalatok vesznek részt.

- fontosnak tartják a kiberbiztonsági tudatosság növelését a lakossági és a kis- és középvállalati felhasználók körében
- keresik azokat a lehetőségeket, amelyek által közösen erősíthetik a kiberbiztonsági tudatosságot
- önkéntes alapon - arra vonatkozó egyéb kötelezettség nélkül - információt osztanak meg egymással az aktuális kiberbiztonsági fenyegetésekről, valamint a kiberbiztonságot érintő szabályozási irányokról



1. Kiberbiztonsági tanúsítás
2. Poszt-kvantum titkosítás
- 3. Kommunikáció, awareness**

Toolbox

Szakmai workshopok: tematikus szakmai eszmecsere az SZTFH szervezésében

Podcast (#digitalskills)

Rádió/TV kiber percek: a köznapi életben hasznosítható tippek, ötletek felhasználóknak, állampolgároknak röviden

szemléletformáló szakmai anyagok



Jövőbeli tervek

- 2023 – Nemzeti kiberbiztonsági tanúsítási rendszer megteremtése
- NIS2 alkalmazásához való hozzájárulás
- EU-s intézkedések implementálása (CER, AI, stb.)
-



**Köszönöm a
figyelmet!**



SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága