Kiberbiztonsági szabályozás

Kibertantv.

dr. Bencsik Balázs

Kiberbiztonsági Tanúsítási Igazgatóság

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

- Szerencsejáték Felügyelet,
- Nemzeti Dohánykereskedelmi Nonprofit Zrt.,
- Felszámolók Névjegyzékét Vezető Hatóság,
- IM Bírósági végrehajtói felügyelet
- Magyar Bányászati és Földtani Szolgálat

- Kiberbiztonsági tanúsítás és felügyelet

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 járulékbevétel származik.

Kiemelkedő jelenősség és felelősség, hatékony hatósági mozgástérrel párosítva.

Kiberbiztonság - Európai Uniós jogszabályi környezet

2016/1148 (EU) irányelv

NIS - hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

- piaci szereplők elfogadták
- nem egyértelmű értelmezés
- heterogén megvalósítás

2019/881 EU rendelet

Kiberbiztonsági törvény

- **IKT-termék**: hálózati vagy információs rendszerelem vagy azok csoportja
- **IKT-szolgáltatás**: szolgáltatás, amely teljes mértékben vagy legnagyobb részben információ … továbbításából, tárolásából, lekérdezéséből vagy kezeléséből áll
- **IKT-folyamat**: IKT-termék vagy IKT-szolgáltatás tervezése, fejlesztése, rendelkezésre bocsátása illetve nyújtása vagy karbantartása céljából végzett tevékenység

Európai Uniós jogszabályi környezet

2016/1148 (EU) irányelv

NIS

Kiberbiztonsági törvény

2019/881 EU rendelet

2022/2555 (EU) irányelv

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

Kibertan.tv – 2023. évi XXIII. törvény

a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló törvény

ÉRTELMEZŐ RENDELKEZÉSEK

KIBERBIZTONSÁGI TANÚSÍTÁS

2019/881 (EU) rendelet

Nemzeti tanúsítási keretrendszer

KIBERBIZTONSÁGI FELÜGYELET

2022/2555 (EU) irányelv – NIS2

Kiberbiztonsági felügyelet – érintett szervezetek

Kiemelten kockázatos ágazatok

- Energia
- Közlekedés
- Egészségügy
- Víz
- Gyógyszeripar
- Digitális infrastruktúrák
- Kihelyezett szolgáltatók
- Világűr

Kockázatos ágazatok

- Posta, futárszolgálatok
- Hulladékgazdálkodás
- Elektronikai gyártás
- Járműgyártás
- Élelmiszer előállítás és forgalmazás
- Digitális szolgáltatások
- Vegyipar
- Kutatóhelyek

Kiket érint? – kiemelten kritikus ágazatok

ENERGIA
villamosenergia, olaj, földgáz, távhő, **hidrogén**

BANKI ÉS PÉNZÜGYI SZOLGÁLTATÁSOK

VÍZ
ivóvíz, szennyvíz

DIGITÁLIS INFRASTRUKTÚRÁK
hírközlés, IXP-k, **bizalmi szolgáltatók**, felhő- és **adatközpont szolgáltatók**, TLD-nyilvántartók, DNS-szolgáltatók

VILÁGŰR
földi támogató infrastruktúrák

SZÁLLÍTÁS
légi, vasúti, vízi, közúti

EGÉSZSÉGÜGY
egészségügyi szolgáltatók, **referencialaboratóriumok**

KÖZIGAZGATÁS

GYÓGYSZERIPAR
K+F, gyógyszeralapanyag és gyógyszerkészítmény gyártás, kritikus orvostechnikai eszközök

KIHELYEZETT (BIZTONSÁGI) SZOLGÁLTATÓK

Kiket érint? – kritikus ágazatok

POSTAI- ÉS FUTÁRSZOLGÁLATOK

ELEKTRONIKAI GYÁRTÁS

orvostechnikai eszközök, elektronikai- és optikai termékek, villamos berendezések, egyéb gépek

JÁRMŰGYÁRTÁS

járművek, pótkocsik

KUTATÓHELYEK

HULLADÉKGAZDÁLKODÁS

ÉLELMISZER ELŐÁLLÍTÁS ÉS FORGALMAZÁS

DIGITÁLIS SZOLGÁLTATÁSOK

online piactér, online keresőmotor, **közösségimédia-szolgáltatási platform**

VEGYIPARI GYÁRTÁS ÉS FORGALMAZÁS

Kiberbiztonsági felügyelet – érintett szervezetek

Kategória	Főtevékenység	Teljes tevékenységi kör
Kiemelten kockázatos ágazatok	432	528
Kockázatos ágazatok	1247	339
Összesen	1679	867
	2546	

50 és 10M €

250 és 50M €

NIS2

Több, mint 50 vagy 10M €

Kiberbiztonsági felügyelet – érintett feladatai

Vezetői feladatok

Biztonságért felelős személy

Szervezeti szabályozások

Tudatosító oktatások és szinten tartás

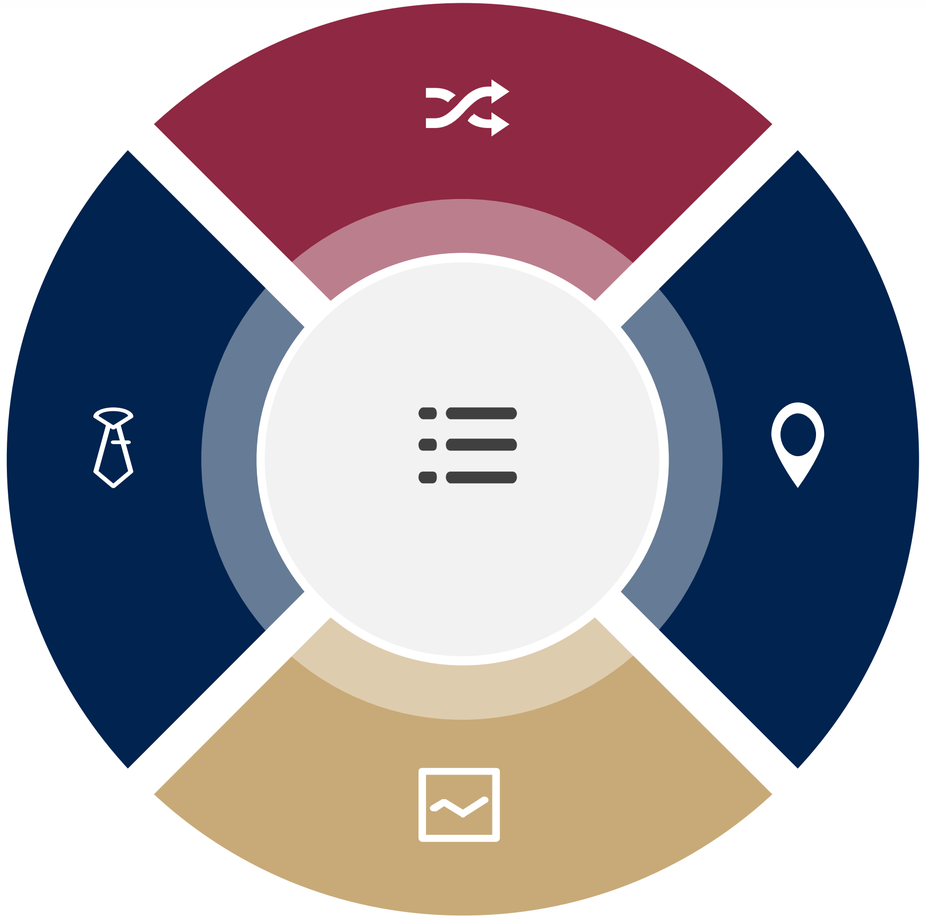
Kiberbiztonsági audit megrendelése

Biztonsági osztályba sorolás

alap

jelentős

magas



Védelem - mit

Hálózati és információs rendszerek + fizikai környezetük

Adatok/információk

Szolgáltatások

Célok

IBIR

Kockázatelemzés

Védelmi intézkedések

Incidensek megelőzése, kezelése, hatásának csökkentése

BC

Életciklus egészében megvalósuló védelem

Kiberbiztonsági felügyelet és ellenőrzés

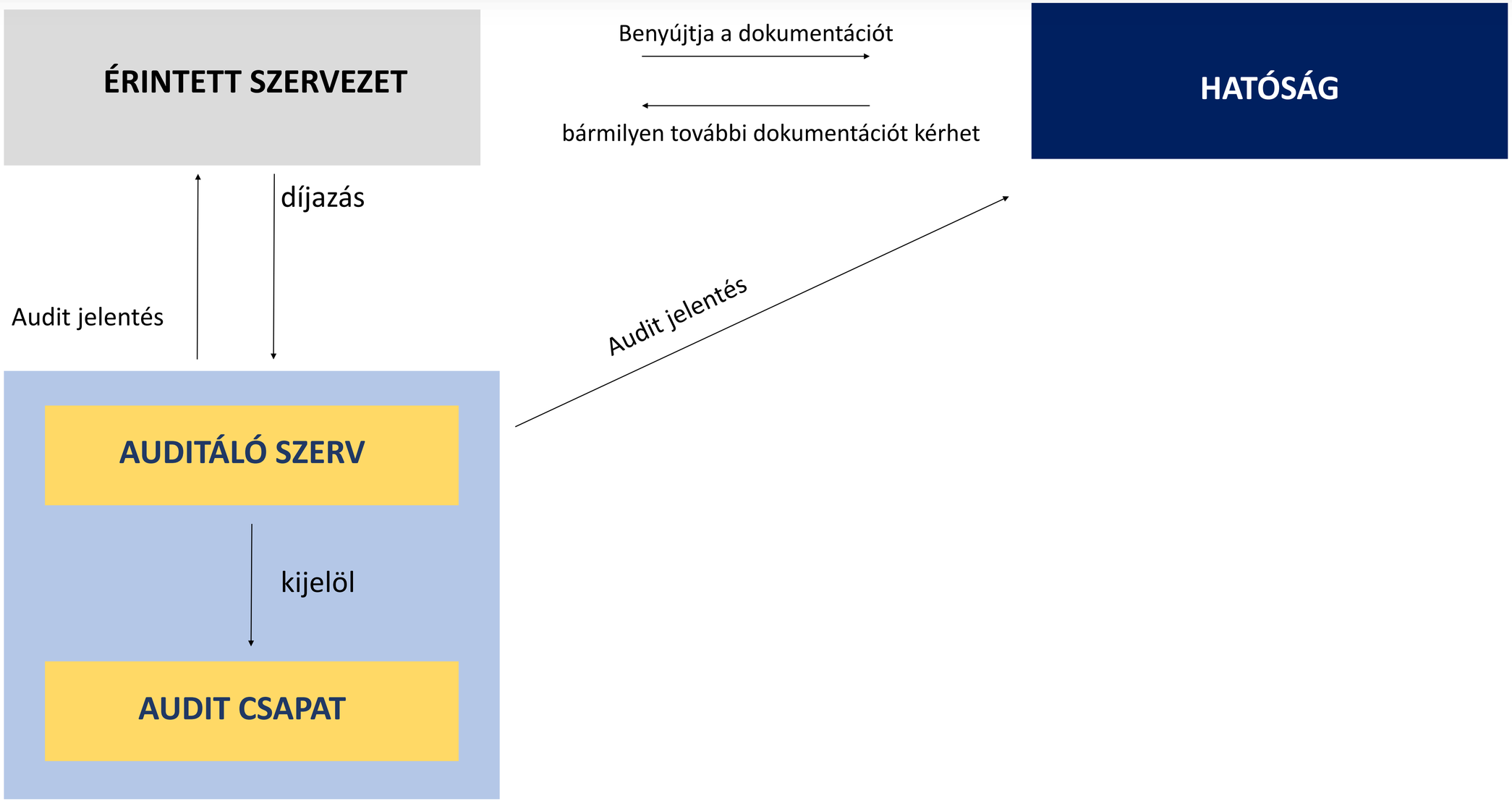
SZTFH

- Hatósági felügyelet – díj:
  - előző évi árbevétel 0,015 %-a, de max. 10M Ft.
- Nyilvántartás
- Hatósági ellenőrzés
- Rendkívüli ellenőrzés elrendelése
- Figyelmeztetés
- Eltiltás (egyéb hatóságokkal együttműködve)
- Bírság
- 10 000 000 EUR, de legfeljebb éves árbevétel 2%-a

Auditorok

- Érintett szervezet felkérésére
- Kiberbiztonsági audit
  - Biztonsági osztályba sorolás
  - Védelmi intézkedések
  - Sérülékenység- és behatolásvizsgálat
  - Kriptográfiai megfelelőség
  - Forráskód-vizsgálat
- Kétévente kötelező
- Eredmény

Feladatok és felelősségek



www.sztfh.hu

Fogalmak

Kiberbiztonsági audit

Az elektronikus információs rendszerek tekintetében a kiberbiztonsági követelmények teljesülésére vonatkozó vizsgálat, ellenőrzés.

Audit jelentés

Az ellenőrzési eredményeket tartalmazó dokumentum.
Az ellenőrzési jelentést az ellenőrző szerv készíti el, és bemutatja az érintett szervezetnek és a hatóságnak. A hatóság kérheti a felülvizsgálat alapjául szolgáló dokumentáció (pl. informatikai biztonsági koncepciók, folyamatdokumentáció, audit jelentés, üzletmenet-folytonosság-kezelés és kontingenciakoncepciók) benyújtását.

Érintett szervezet kötelezettségei

Az auditnak ki kell terjednie a kritikus infrastruktúra teljes és aktuális hatókörére.

Az ellenőrzés végrehajtásához és a megfelelőség dokumentálásához a következőket kell ismertetni:

- **a rendszer**
- **az érintett szervezet által nyújtott alapvető szolgáltatás részei**
- **az alapvető szolgáltatás külső szolgáltatók által nyújtott részei (pl. kiszervezés, anya-/leányvállalat csoporton keresztül történő ellátás)**
- **a kölcsönhatás más rendszerekkel**
- **az interfészek és függőségek**

Példák azokra a dokumentumokra, amelyeket át kell adni az auditornak:

- az információbiztonsági menedzsment rendszer (ISMS) leírása
- a folytonosság kezelésének leírása
- vagyonkezelési dokumentumok
- fizikai biztonsági folyamatok dokumentálása (pl. helyszíni beléptető vagy tűzvédelmi biztosítékok)
- a személyi és szervezeti biztonság dokumentálása (pl. az alkalmazottak képzési intézkedéseinek nyilvántartása, figyelemfelkeltő kampányok, jogosultságkezelés)
- az incidensek azonosítására és feldolgozására vonatkozó koncepciók és dokumentáció
- belső ellenőrzés és az egyéb elvégzett auditok ellenőrzési jelentései, gyakorlatok, szisztematikus naplóelemzések stb.)
- Irányelvek a beszállítókkal és szolgáltatókkal való kapcsolattartáshoz (pl. szolgáltatási szintű megállapodások és egyéb, a szolgáltatókkal kötött, biztonsággal kapcsolatos megállapodások)

Kockázatkezelés

Kockázat elfogadás

Kockázatokat nem lehet elfogadni, ha *state-of-the-art* biztonsági intézkedések elérhetőek és alkalmazhatók.

A kockázat elfogadása csak a fennmaradó maradék kockázat esetében lehetséges.

Kockázatáthárítás

A kockázatok átadása, például biztosítás útján, nem helyettesíti az előírt biztonsági intézkedéseket.
Biztosítás vagy egyéb kockázatátadás esetén a legkorszerűbb biztonsági intézkedéseket is alkalmazni kell a műszaki állapotnak megfelelően. Azonban az érintett szervezet szabadon választhat további biztosítást is.

A kockázatok és a védelem szükségességének pusztán gazdasági szempontból történő megfontolása általában nem elegendő.

A védelmi intézkedések kiválasztásakor gondoskodni kell az alkalmasságról is, azaz figyelembe kell venni a szolgáltatások meghibásodásának vagy kiesésének lehetséges társadalmi és egyéb következményeit a biztonsági óvintézkedések költségéhez viszonyítva.

Auditáló szerv

Az auditáló szerv összeállít egy megfelelő, képzett és független ellenőrző csapatot, amely előkészíti és végrehajtja az ellenőrzést, majd dokumentálja azt egy jelentésben

Az auditáló szerv felelős az ellenőrzés végrehajtásáért, valamint az ellenőrzési jelentés és a hozzá tartozó dokumentumok helyességéért

Mivel az auditáló szerv és az érintett szervezet felelőssége közös, a felek közti kötelezettségeket világosan rögzíteni szükséges szerződésben

Ellenőrzés

1. lépés	Az ellenőrzés előkészítése és a terjedelem megfelelőségének vizsgálata
2. lépés	Gap analízis készítése
3. lépés	Hivatalos dokumentumok ellenőrzése
4. lépés	Helyszíni ellenőrzés
5. lépés	Helyszíni ellenőrzés nyomon követése
6. lépés	Az ellenőrzési jelentés elkészítése

Minden ellenőrzésnek le kell fednie az alább felsorolt hat ellenőrzési lépést, amelyeket az adott rendszerre és az iparági sajátosságokra kell adaptálni.

Ellenőrzés témái és technikái

Ebben az összefüggésben azokat az vizsgálandó szempontokat kell megvizsgálnia és értékelnie az auditornak, mint minimum:

- ✓ **az alapvető szolgáltatás funkcionalitását**
- ✓ **alkalmasságot és szükségességet**
- ✓ **teljességet**

Lehetséges audit technikák

Audit technikák alatt egy helyzet felmérésére szolgáló metódust értünk. Egy audit során különböző technikák is alkalmazhatók az alábbiak közül.

Audit technikák

01 **Személyes interjú**

02 **Behatolás- sérülékenység tesztek**

03 **Rendszerek, területek, helyiségek és tárgyak (vizuális) ellenőrzése**

04 **Adatelemzés**
(pl. naplófájlok, tűzfal konfiguráció, adatbázis elemzése stb.)

05 **Dokumentumok elemzése**
(ez magában foglalja az elektronikus adatokat is)

06 **Írásbeni tájékoztatáskérés**

07 **Műszaki helyszíni vizsgálat és/vagy célzott megfigyelés**
(pl. riasztórendszerek működése)

08 **Egyéb megfelelőségértékelési dokumentáció használata**

Audit mélység

Az első alkalommal végzett ellenőrzések mélységének meghatározása magában foglalja például:

- Az érintett szervezet mérete (pl.: a szervezet dolgozóinak száma)
- A nyújtott szolgáltatás kritikussága és az ellátási terület
- Az érintett szervezet bonyolultsága
- Az alapvető szolgáltatás IT függősége
- Szakértői/műszaki tesztek vagy elemzések alapján részletes vizsgálatokat kell-e végezni az ellenőrzés terjedelme keretében

Hiányosság kategóriák

A biztonsági hiányosságokat két dimenzióba kell osztályozni:

1. Az érintett IT-biztonsági probléma
2. A hiányosság súlyossága

1. kategória

Súlyos vagy jelentős eltérés/biztonsági hiányosság

Sürgős cselekvésre van szükség. Az eltérést azonnal vagy amilyen gyorsan csak lehetséges, el kell távolítani, mivel az alapvető szolgáltatás bizalmassága, integritása, hitelessége vagy elérhetősége súlyosan veszélyeztetett, és jelentős károkra lehet számítani.

2. kategória

Kisebb eltérés/biztonsági hiányosság

Egy "kisebb eltérés" fenyegetést és kockázatot jelent. Nincs sürgős cselekvésre szükség. Az alapvető szolgáltatás bizalmasságát, integritását, hitelességét vagy elérhetőségét középtávon kell helyreállítani.

3. kategória

Ajánlás

Az "ajánlás" egy javaslat a fejlesztésre. Az ajánlás végrehajtásával növelhető a biztonság.

4. kategória

Nincs eltérés

Nincs biztonsági hiányosság, ha az összes követelményt teljes egészében betartották, és ha minden védelmi intézkedést teljes mértékben, hatékonyan és megfelelően hajtottak végre.

Biztonsági események jelentése

NIS1 olyan esemény, amely **ténylegesen** kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára

NIS2 olyan esemény, amely **veszélyezteti** a hálózati és információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát

Korai előrejelzés

Kiváltó ok?

Határon átnyúlik-e?

Zárójelentés

részletes leírás: értékelés, kiváltó ok, intézkedések, határon túli hatás

0 | 0-24 óra | 72 óra (bizalmi: 24 óra) | 30 nap

Észlelés

Jelentős esemény

Eseménybejelentés

első értékelés: súlyosság, hatás, fertőzöttségi mutató

Kiberbiztonsági felügyelet - ütemezés

	2024. január 1.	2024. október 18.	2024. december 31.	2025. december 31.
SZTFH	• Érintett szervezetek nyilvántartásba vétele • Auditorok nyilvántartásba vétele	• Felügyeleti tevékenység • Ellenőrzési tevékenység		
Érintett szervezet	• Önazonosítás, nyilvántartásba vételre bejelentkezés 2024. június 30-ig • Biztonsági osztályba sorolás • Elektronikus információs rendszerek biztonságáért felelős személy feladatköre és kijelölése	• Védelmi intézkedések alkalmazása • Felügyeleti díj megfizetése	• Első kiberbiztonsági audit vonatkozásában szerződéskötés az auditorral	• Első kiberbiztonsági audit lefolytatásának határideje

Köszönöm a figyelmet!

dr. Bencsik Balázs

kiberbiztonsag@sztfh.hu

SZTFH

Szabályozott Tevékenységek Felügyeleti Hatósága