NIS2

KIBERBIZTONSÁGI INTÉZKEDÉSEK

BUDAI LÁSZLÓ
IT Biztonságtechnikai üzletágvezető, CDPSE
budai.laszlo@nador.hu

SIPOS GYŐZŐ
IT BIZTONSÁGI TANÁCSADÓ, CISA, CDPSE, ISO27001 AUDITOR
sipos.gyozo@nador.hu

Nádor RENDSZERHÁZ 30 éves

2022/2555 (EU) IRÁNYELV – NIS2

KIBERBIZTONSÁGI TANÚSÍTÁS

Tanúsító hatóságok

SZTFH

Általános

Ibtv. III/A. fejezet

KNBSZ

Hadiipari kutatás, fejlesztés, gyártás és kereskedelem

718/2021. (XII. 20.) Korm. Rendelet

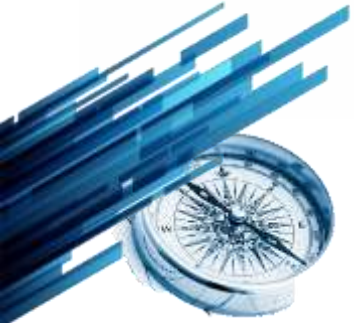
Értékelés típusai

Gyártó ← **Megfelelőségi önértékelés**

Akkreditált és nyilvántartásba vett szervezet ← **Megfelelőségértékelés**

EURÓPAI KIBERBIZTONSÁGI TANÚSÍTÁS

EURÓPAI TANÚSÍTÁSI RENDSZEREK	MEGBÍZHATÓSÁGI SZINTEK
érintett termékek és szolgáltatások kategóriái	Alap
kiberbiztonsági követelmények (szabványok vagy műszaki előírások)	Jelentős
az értékelés típusa	Magas
garantált szint	



MINDEN EU TAGÁLLAMBAN AUTOMATIKUSAN EL KELL FOGADNI!

2022/2555 (EU) IRÁNYELV – NIS2

KIKET ÉRINT? - KIEMELTEN KOCKÁZATOS 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

* Magyar jogszabályba belekerült a Tömegközlekedés is a szállítás alá.

KIKET ÉRINT? - KOCKÁZATOS ÁGAZATOK

POSTAI- ÉS FUTÁRSZOLGÁLATOK

ELEKTRONIKAI GYÁRTÁS

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

JÁRMŰGYÁRTÁS

járművek, pótkocsik

KUTATÓHELYEK

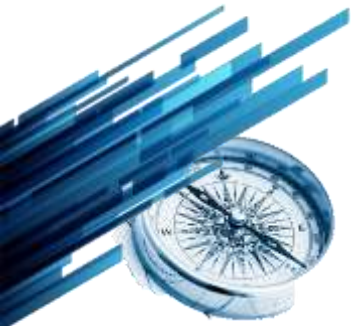
HULLADÉKGAZDÁLKODÁS

ÉLELMISZER ELŐÁLLÍTÁS ÉS FORGALMAZÁS

DIGITÁLIS SZOLGÁLTATÁSOK

online piactér, online keresőmotor, közösségimédia-szolgáltatási platform

VEGYIPARI GYÁRTÁS ÉS FORGALMAZÁS



* Magyar jogszabályba belekerült a Cement-, mész-, gipszgyártás is.

KIKET ÉRINT? - MÉRETKORLÁT

Kritériumok

10 és 2M €

50 és 10M €

250 és 50M €

„amelyek a 2003/361/EK ajánlás mellékletének 2. cikke szerint középvállalkozásoknak minősülnek vagy meghaladják az említett cikkben a középvállalkozásokra vonatkozóan előírt küszöbértékeket"

NIS 2

Több, mint

50

vagy

10M €

KIKET ÉRINT? - MÉRETKORLÁT ALÓLI KIVÉTELEK

Meghatározott szolgáltatók
nyilvános elektronikus hírközlés, bizalmi szolgáltatók, TLD-nyilvántartók, DNS-szolgáltatók, domainnév-nyilvántartók

Kritikus szervezetek
CER (2022/2557 EU) irányelv alapján azonosított

Köz-szempont
szolgáltatás zavara jelentős hatású lehet a közvédelemre, közegészségre, közbiztonságra

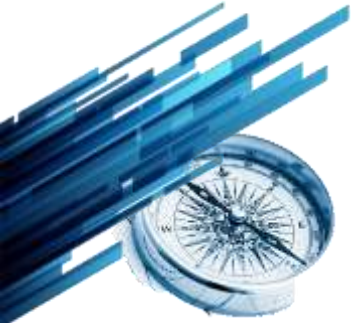
Közigazgatási szerv
nemzeti jog alapján

Különös fontosságú
nemzeti vagy regionális szinten

Egyetlen szolgáltatásnyújtó
szolgáltatása a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához elengedhetetlen

KIKET ÉRINT? - SZÁMOKBAN

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



KIBERTAN TV. – ÉRINTETT SZERVEZETEK FELADATA

Vezetői feladatok

Biztonságért felelős személy

Szervezeti szabályozások

Tudatosító oktatások és szinten tartás

Best practice-ek

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

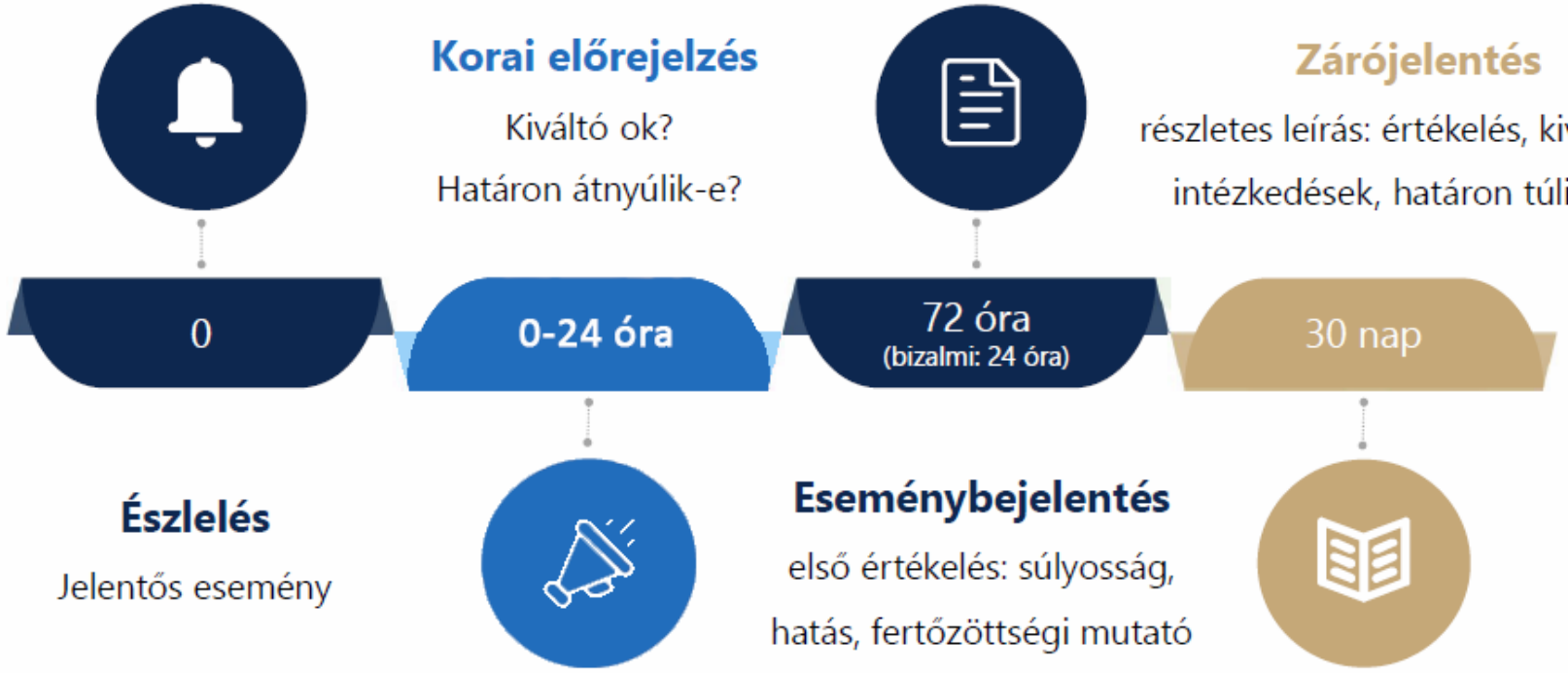
BC

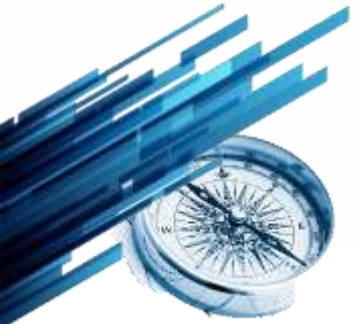
Életciklus egészében

KIBERTAN TV. – JELENTÉSI KÖTELEZETTSÉG

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





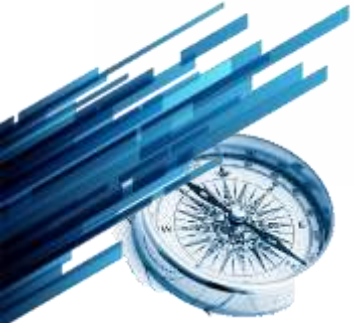
KIBERTAN TV. – ELLENŐRZÉS

SZTFH

- Hatósági felügyelet - díj
- Nyilvántartás
- Hatósági ellenőrzés
- Rendkívüli ellenőrzés elrendelése
- Figyelmeztetés
- Eltiltás (egyéb hatóságokkal együttműködve)
- Bírság

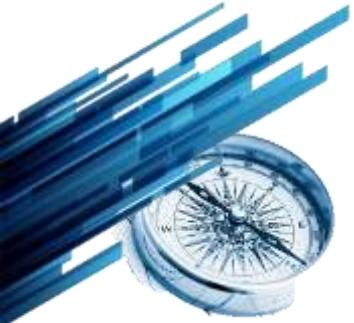
Auditorok

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



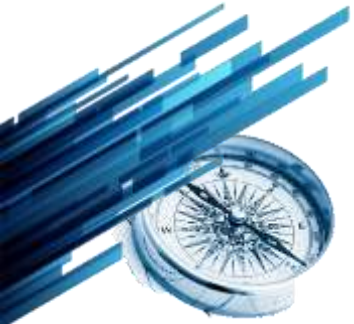
BÍRSÁG

- Alapvető (kiemelten kockázatos) szervezet esetében:
  - 10 000 000 Euro vagy az előző évi teljes világszintű forgalom 2%-a, attól függően melyik a nagyobb
- Fontos (kockázatos szervezetek) esetében:
  - 7 000 000 Euro vagy az előző évi teljes világszintű forgalom 1,4%-a, attól függően melyik a nagyobb



KIBERBIZTONSÁGI FELÜGYELETI DÍJ

- Az SZTFH kiberbiztonsági felügyeleti tevékenységéért – a költségvetési szervek kivételével – az érintett szervezet az SZTFH elnökének rendeletében meghatározott mértékű kiberbiztonsági felügyeleti díj fizetésére köteles, amelynek mértéke a szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének – max 0,015 %-a, de max. 10M Ft.



KIBERBIZTONSÁGI AUDIT DÍJ

SZTFH rendeletben maximalizálásra kerül majd.

KIBERTAN TV. – ÜTEMEZÉS

AKKOR NEM IS KELL SEMMIT TENNÜNK…

…mert nincsenek meg a jogszabályok.

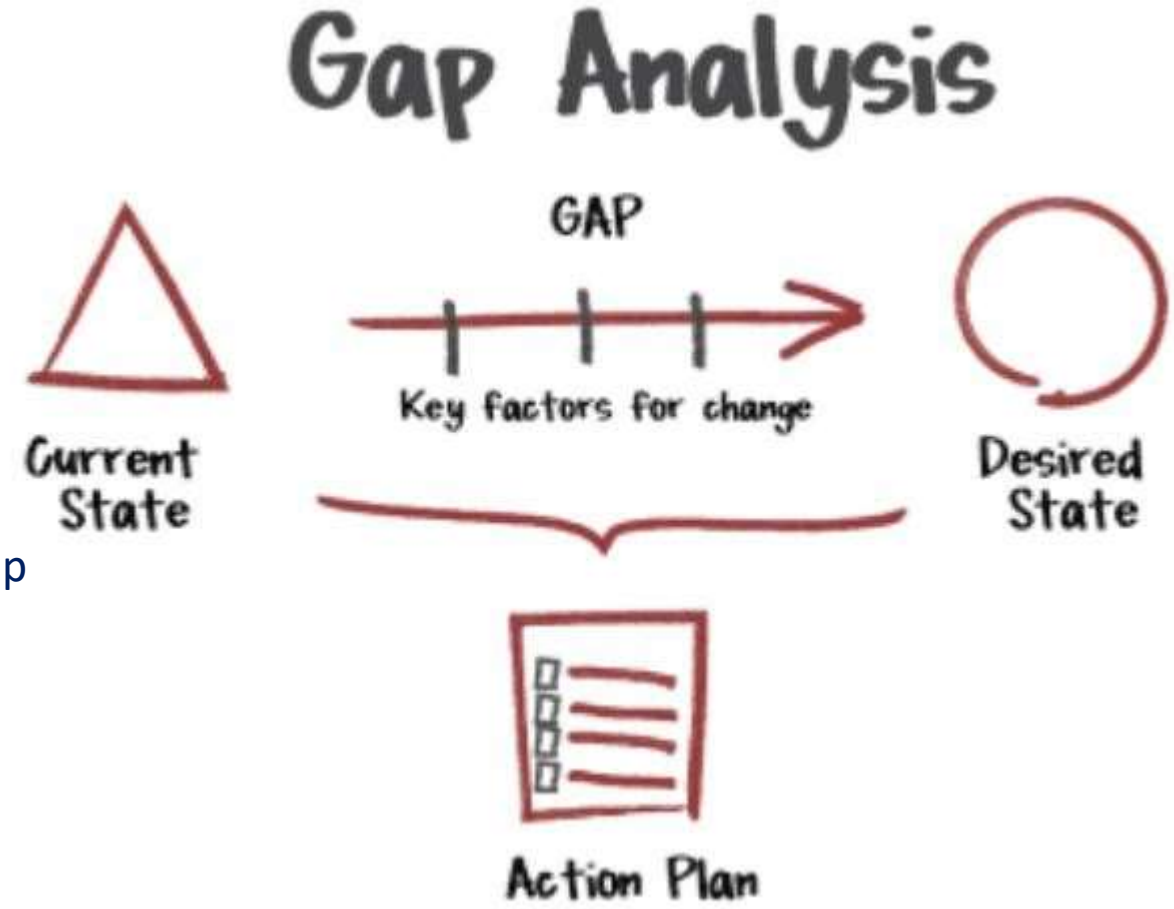
NEM IGAZ! El kell kezdeni a felkészülést, mert sok követelménynek kell megfelelni. Igaz, a részletszabályozások nem állnak rendelkezésre, de irányadó az Ibtv. és a 41/2015 BM rendelet (mely átdolgozás alatt van).

Az információbiztonság irányítási keretrendszerek követelményei is hasonlók, pl.

- Ibtv.
- ISO 27001
- NIST 800-53
- PCI DSS
- COBIT
- stb.

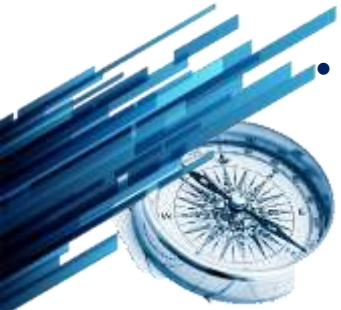
MIBEN SEGÍTHETÜNK? - FELMÉRÉS

- GAP analízis
- Ütemterv
- Költségtervezés
- Szükséges napok: 3-5 tanácsadói nap



MIBEN SEGÍTHETÜNK? – FELKÉSZÍTÉS

- IT Biztonsági szabályzatok elkészítése
- Incidenskezelési eljárások megalkotása, azok kialakításának támogatása (megelőzés, észlelés, reagálás, jelentés)
- BCP / DRP folyamatok kialakításának támogatása, szabályzatok elkészítése, tesztelés
- IBF – biztonsági felelős biztosítása
- Ellátási lánc biztonsága – beszerzési folyamatok átalakítása, eljárások, követelmények megfogalmazása
- Sebezhetőségi vizsgálatok elvégzése – nem auditált
- Kiberbiztonsági kockázatelemzés és információs rendszerekre vonatkozó biztonsági szabályok kialakítása, kockázatkezelési intézkedések és eljárások kialakítása
- Biztonsági osztályba sorolás támogatása
- IT biztonságtudatossági képzések
- Szükséges napok: 25-60 tanácsadói nap



MIVEL? - MEGOLDÁSOK

SOC / SOAR / MDR

Kiberkitettség vizsgálat

Penetration teszt

SIEM

Hálózat monitoring / anomália detektálás /NDR

Felhasználó azonosítás

Web Application Firewall (egyéb tartalomszűrők: AS, IPS URL)

Loggyűjtés

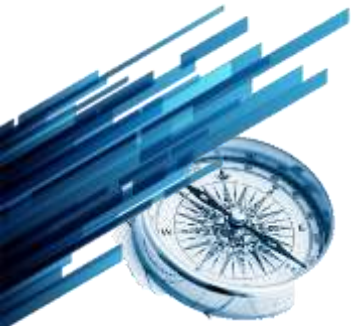
Tűzfal

Vírusvédelem

Mentés

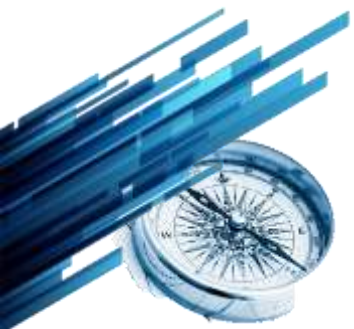
Patch Menedzsment

Sérülékenység Menedzsment



MIBEN SEGÍTHETÜNK? – BIZTONSÁGI MEGOLDÁSOK

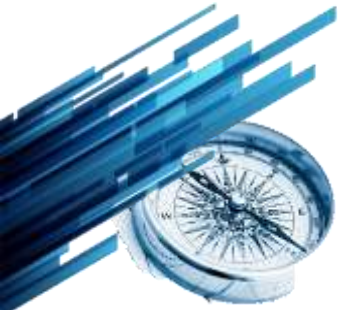
- Sérülékenység vizsgáló megoldások (Tenable Nessus, Cymulate, Rapid7)
- Kiberhírszerzési szolgáltatások (Cyfirma, Rapid7)
- Patch menedzsment (Heimdal)
- Naplózó rendszerek kiegészítve automatikus incidenskezeléssel (Logpoint – SIEM+SOAR)
- Kéttényezős felhasználó azonosítás (Thales FIDO2 eszközök, WatchGuard, Fortinet)
- Hálózati monitorig (Flowmon)
- Hálózati incidens felderítés, észlelés (Sophos MDR szolgáltatás)
- Adatdióda (FOX-IT)
- Mentési rendszerek (Több telephelyen, és offline mentés is javasolt)
- Adatokhoz való hozzáférés szabályozása, adatszivárgás megakadályozása (Safetica, Variato, Terramind)
- Tűzfalak, egyéb szűrők és antivírus megoldások



INFORMÁCIÓK, HATÓSÁGI TÁJÉKOZTATÓK

- A **Szabályozott Tevékenységek Felügyeleti Hatósága** (a továbbiakban: SZTFH) honlapja
  - Felsorolva a Kibertan. tv., a kiadott két SZTFH rendelet a tanúsításról, továbbá megemlítve az Ibtv. és végrehajtási rendelete, a 41/2015. BM rendelet, továbbá az IBF képzésről szóló 26/2013 KIM rendelet. Ez utóbbi kettő még változatlan, nincsenek NIS2-es vonatkozásai;

- **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet** (NBSZ NKI)
  - „A NIS irányelv implementációja által érintett jogszabályok”, 14 elemű felsorolás. Kiemelendő a létfontosságú rendszerelemekre (kritikus infrastruktúra) vonatkozó jogszabályok és az eseménykezelő központra és a sérülékenység vizsgálatokra vonatkozó szabályozások. Ezen jogszabályok módosításra várnak.



JELENLEGI HAZAI JOGSZABÁLYOK

- A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (Kibertan. tv.)

- A nemzeti kiberbiztonsági tanúsító hatóság eljárásával összefüggő kiberbiztonsági tanúsítás keretében fizetendő igazgatási szolgáltatási díjról szóló 30/2022. (II. 14.) SZTFH rendelet

- Információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló 10/2023. (V. 15.) SZTFH rendelet

- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) (Már számos változás történt a NIS2 miatt)

- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet (Ibtv. vhr.)

KÖSZÖNJÜK A FIGYELMET

BUDAI LÁSZLÓ
IT Biztonságtechnikai üzletágvezető, CDPSE
budai.laszlo@nador.hu

SIPOS GYŐZŐ
IT BIZTONSÁGI TANÁCSADÓ, CISA, CDPSE,
ISO27001 AUDITOR
sipos.gyozo@nador.hu

Nádor RENDSZERHÁZ 30