Kibertan törvény + NIS2

Tájékoztató az információbiztonsági képzésre vonatkozó jogszabályi kötelezettségekről

Dátum: 2024. 07. 17.

A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (Kibertan.tv.) előírja, hogy az érintett szervezet köteles gondoskodni a szervezet munkatársainak rendszeres információbiztonsági képzéséről és ismereteinek szinten tartásáról. Így a dolgozók oktatása nemcsak a szervezet jól felfogott érdeke, hanem egyúttal jogszabályi kötelezettsége is. A tudatosság és képzés területén a KnowBe4 integrált oktatási és szimulált támadási rendszere kulcsrakész megoldást biztosít a szükséges védelmi intézkedések gyors megtételéhez.

Háttér

A 2016-ban életbe lépett **Network and Information Systems (NIS) Directive** a kritikus nemzeti infrastruktúrákba tartozó szervezetek számára írt elő biztonsági és jelentési kötelezettségeket az Európai Unión belül. Az állami intézményekre és a vállalatokra leselkedő kiberkockázatok növekedése miatt az Európai Unió 2022-ben elfogadta a direktíva második változatát (**NIS 2**), amelynek célja a kiberbiztonsági képességek egységesítése és az unióban működő szervezetek védelmének megerősítése.

A **Kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény** (Kibertan.tv.) a NIS 2 irányelvnek történő hazai megfelelést szolgálja. A Kibertan.tv. kiberbiztonsági követelményrendszert állít fel a szereplők számára, továbbá meghatározza a betartásukhoz szükséges felügyeleti intézkedéseket és bevezeti a hatósági felügyeleti rendszert. Ennek értelmében a **Szabályozott Tevékenységek Felügyeleti Hatósága** (SZTFH) lett a felelős a kiberbiztonsági követelmények betartásának ellenőrzéséért. A kijelölt hatóság többek között meghatározza az ellenőrzés, a nyilvántartás és a szankcionálás módját is.

Jelen tájékoztatóban a jogszabály részletes ismertetése helyett elsősorban azokat a pontokat emeljük ki, amelyek fontosak lehetnek a kötelező biztonságtudatossági képzés tekintetében.

Kikre vonatkozik?

A Kibertantv. minden olyan közép és nagyvállalatra vonatkozik, amely legalább 50 főt foglalkoztat, vagy 10 millió eurónál nagyobb az éves árbevétele, ÉS tevékenysége benne van a törvény által meghatározott ágazati listában. A kiemelten kockázatos ágazatokat a Kibertantv. 1. számú, a kockázatos ágazatokat a törvény 2. számú melléklete részletezi.

Viszont vannak kivételek a minimum középvállalati besorolás alól. Ugyanis ha az érintett szervezet elektronikus hírközlési szolgáltató, bizalmi szolgáltató, DNS-szolgáltatást nyújtó szolgáltató, legfelső szintű domainnév-nyilvántartó vagy domainnév-regisztrációt végző szolgáltató, akkor rá mérettől függetlenül (mikró- vagy kisvállalkozásként is) vonatkozik a törvény.

Határidők

A Kibertantv. alkalmazása tekintetében az alábbi határidők irányadók az érintett szervezetek részére:

Dátum	Feladat
2024. január 1.	Önazonosítás, információbiztonsági felelős kinevezése
2024. június 30.	Nyilvántartásba vételre bejelentkezés (Szabályozott Tevékenységek Felügyeleti Hatósága)
2024. október 18.	Védelmi intézkedések alkalmazása, felügyeleti díj megfizetése
2024. december 31.	Szerződéskötés az auditor szervezettel (a hatóság által közzétett listáról)
2025. december 31.	Első kiberbiztonsági audit lefolytatása

Szabályozott Tevékenységek Felügyeleti Hatósága

A fenti menetrend szerint a jelen tájékoztató kiadásának időpontjában az érintett szervezeteknek már be kellett regisztrálniuk magukat a Szabályozott Tevékenységek Felügyeleti Hatóságánál.

Amennyiben ez esetleg még nem történt meg, akkor az **Érintett szervezet nyilvántartásba vételére irányuló kérelem** megnevezésű SZTFH 420 űrlap a következő linken érhető el:
https://sztfh.hu/ugyintezes/nyomtatvanyok-es-urlapok/sztfh420/

Az űrlap kitöltésére az érintett szervezet cégkapujához meghatalmazással rendelkező természetes személy (cégvezető) jogosult.

Praktikus szempont, hogy a regisztrációhoz nem szükséges letölteni az ÁNYK programot. A „Cégkapus ügyintézést” választva egy iForm webes űrlapot kell kitölteni.

A következő fontos határidő **2024. október 18.**, amely dátumig az alábbiakat szükséges megvalósítani:

- elektronikus információs rendszerei biztonsági osztályának megfelelő védelmi intézkedések alkalmazása
- felügyeleti díj fizetési kötelezettség (részletszabályozás folyamatban)

A hatóság honlapján jelenleg összesen kettő megfelelősség-értékelő (auditor) szervezet található, amelyek közül egyedül a Hunguard felel meg a „magas” megbízhatósági szint követelményeinek:

MEGFELELŐSÉGÉRTÉKELŐ SZERVEZET NEVE	MEGBÍZHATÓSÁGI SZINT	STÁTUSZ	NYILVÁNTARTÁSBA VÉTEL DÁTUMA
HUNGUARD Számítástechnikai-, informatikai kutató - fejlesztő és általános szolgáltató Korlátolt Felelősségű Társaság	Magas	Aktív	2023.06.02
VERITAN Hírközlési és Informatikai Tanúsító Korlátolt Felelősségű Társaság	Alap	Aktív	2024.04.11

https://sztfh.hu/nyilvantartasok/megfelelosegertekelo-szervezetek/

Megbízhatósági szintek

A törvény három megbízhatósági szintet határoz meg az alábbiak szerint:

- Alap: a biztonsági eseményekkel és támadásokkal kapcsolatos **alapvető, ismert kockázatok**
- Jelentős: az **ismert kockázatok**, valamint a **korlátozott szakértelemmel és erőforrásokkal** rendelkező elkövetők által végrehajtott biztonsági események és kiberbiztonsági támadások kockázata,
- Magas: a **jelentős szakértelemmel és erőforrásokkal** rendelkező elkövetők által, a **tudomány legutolsó állása szerinti technológiával** végrehajtott kibertámadások kockázata

Ezek a megbízhatósági szintek határozzák meg, hogy egy adott szervezetnek milyen védelmi intézkedéseket szükséges kötelezően meghoznia. Később részletezzük majd, hogy a biztonságtudatossági képzés területén melyek a kötelező, illetve a kiegészítő intézkedések.

Információbiztonsági képzés, mint törvényi kötelezettség

A törvény 19. szakasz 6. c. pontjában egyértelműen rögzíti, hogy **az érintett szervezet vezetője köteles gondoskodni a cég dolgozóinak rendszeres információbiztonsági képzéséről** és ismereteinek szinten tartásáról. Így a dolgozók biztonságtudatossági oktatása nemcsak a vállalat jól felfogott érdeke, hanem egyúttal jogszabályi kötelezettsége is.

Beszállítói lánc vizsgálata

Fontos megjegyezni, hogy a NIS2 hatálya nem korlátozódik csak az adott vállalatra, hanem kiterjed az egész beszállítói láncra és az együttműködő alvállalkozókra is. Ez azt jelenti, hogy az érintett vállalatoknak biztosítaniuk kell, hogy minden olyan szereplő, akivel kapcsolatban állnak az üzletmenetben, megfeleljen a NIS2 előírásoknak. Pontosabban fogalmazva: a vállalat beszállítója vagy alvállalkozója ne áshassa alá a kötelezett szervezet jogszabályi megfelelését.

Elvárt védelmi intézkedések a képzés területén

A Kibertan törvényhez kapcsolódóan 2024. június 24-én megjelent a részletes követelményeket tartalmazó kormányrendelet. A jogszabály teljes neve: „**7/2024. (VI. 24.) MK rendelet A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről**”.

Link: https://net.jogtar.hu/jogszabaly?docid=a2400007.mkf

A rendelet 2. számú melléklete (Védelmi intézkedések katalógusa) részletezi az elvárt védelmi intézkedéseket az egyes kiberbiztonsági területeken. Az említett 2. számú melléklet 3. fejezete foglalkozik a „**Tudatosság és képzés**” témakörével. A könnyebb átláthatóság érdekében az egyes védelmi intézkedéseket két részre bontottuk az alábbi táblázat szerint:

Elvárt (kötelező) védelmi intézkedések*	Nem kötelező, kiegészítő védelmi intézkedések
3.1. Szabályzat és eljárásrendek (tudatossági és képzési szabályzat) (Alap-Jelentős-Magas)	3.3. Biztonságtudatossági képzés – Gyakorlati feladatok (szimulált biztonsági események)
3.2. Biztonságtudatossági képzés (Alap-Jelentős-Magas)	3.6. Biztonságtudatossági képzés – Gyanús kommunikáció és szokatlan rendszerviselkedés
3.4. Biztonságtudatossági képzés – Belső fenyegetések (felismerése és jelentése) (Alap-Jelentős-Magas)	3.7. Biztonságtudatossági képzés – Tartós fejlett fenyegetések
3.5. Biztonságtudatossági képzés – Pszichológiai befolyásolás és információszerzés (Jelentős-Magas)	3.8. Biztonság-tudatossági képzés – Kiberfenyegetési környezet
3.9. Szerepkör alapú biztonsági képzés (Alap-Jelentős-Magas)	3.10. Szerepkör alapú biztonsági képzés – Környezeti védelmi intézkedések
3.13. A biztonsági képzésre vonatkozó dokumentációk (képzési tevékenységek) (Alap-Jelentős-Magas)	3.11. Szerepkör alapú biztonsági képzés – Fizikai védelmi intézkedések
	3.12. Szerepkör alapú biztonsági képzés – Gyakorlati feladatok
	3.14. Képzés eredményeiről való visszajelzés (meghatározott személyeknek)

(*Zárójelben a Biztonsági osztály megnevezése: Alap, Jelentős, Magas)

A szervezeten belüli biztonságtudatossági képzés lebonyolításához jogszabály szerint nem kötelező e-learning rendszert alkalmazni (*Learning Management System - LMS*), ugyanakkor a nagyobb méretű szervezetek esetében mindenképpen sokkal hatékonyabb a képzések megszervezése, ütemezése, illetve az elvégzett tréningek dokumentálása egy ilyen rendszerben. Továbbá a szimulált támadások kivitelezése és a munkavállalói hibázások mérése csak egy erre a célra fejlesztett szoftverrel megvalósítható.

KnowBe4 - Security Awareness Training

Az adatvédelmi incidensek többségét az emberi réteget, a szervezet dolgozóit ért támadások okozzák. Ezt felismerve 2010-ben informatikai és adatbiztonsági szakemberek megalapították a KnowBe4 céget, amely a dolgozók biztonságtudatossági képzésére fókuszál. Azóta a gyors növekedésnek köszönhetően az USA leggyorsabban növekvő magánvállalatait rangsoroló Inc. 500-as listán a KnowBe4 folyamatosan előkelő helyen szerepel.

A KnowBe4 jelenleg a világ legnagyobb integrált biztonságtudatossági képzés és szimulált adathalász platformját kínálja több mint 65 ezer vállalati ügyfelének.

Mint a kiberbiztonsági iparágban működő vállalat, a KnowBe4 mindent elkövet a saját és ügyfelei informatikai biztonsága érdekében. A teljesség igénye nélkül a KnowBe4 az alábbi megfelelősséggel rendelkezik:

- ISO 27001:2013 (information security controls)
- ISO 27701:2019 (privacy information management)
- ISO 27017:2015 (information security controls for cloud computing)
- ISO 27018:2019 (protecting PII in the public cloud for data processors)
- FedRAMP Moderate ATO
- SSAE18 SOC2 Type 2

A részletes megfelelőség tekintetében tekintse meg a https://www.knowbe4.com/security oldalt.

Human Hacking

A Human Hacking a KnowBe4 hivatalos magyarországi forgalmazója, amelyet informatikai és távközlési szakemberekkel közösen alapítottunk. Küldetésünk a dolgozók képzésével megakadályozni a kiberbűnözőket abban, hogy pszichológiai manipulációval áttörjenek a cégek informatikai védelmén. A KnowBe4 licencek hazai értékesítése mellett igény esetén vállaljuk a KnowBe4 rendszer teljes körű menedzselését is.

Magyar nyelvű KnowBe4 termékismertető letölthető az alábbi linken:

https://humanhacking.hu/wp-content/uploads/2024/02/Security-Awareness-Training-Productsheet-HU-2024-1.pdf

Hasznos linkek

Az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022L2555

Az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/881 RENDELETE (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály)

https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019R0881

2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

https://njt.hu/jogszabaly/2023-23-00-00

7/2024. (VI. 24.) MK rendelet A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

https://net.jogtar.hu/jogszabaly?docid=a2400007.mkf

https://njt.hu/jogszabaly/2024-7-20-7G

Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) weboldala és tájékoztatók

https://sztfh.hu/tevekenysegek/kiberbiztonsagi-tanusitas/kiberbiztonsagi-felugyelet/

https://sztfh.hu/ugyintezes/nyomtatvanyok-es-urlapok/sztfh420/

https://sztfh.hu/nyilvantartasok/megfelelosegertekelo-szervezetek/

https://sztfh.hu/downloads/kiberbiztonsag/eszkoztar/SZTFH_erintett_tajekoztato.pdf

https://sztfh.hu/downloads/kiberbiztonsag/eszkoztar/SZTFH_nyilv%C3%A1ntartas_tajekoztato.pdf

A Nemzeti Kibervédelmi Intézet tájékoztatója a NIS2 implementációjáról

https://nki.gov.hu/intezet/tartalom/erinti-a-cegemet-a-nis2-szabalyozas/

2004. évi XXXIV. törvény a kis- és középvállalkozásokról, fejlődésük támogatásáról

https://njt.hu/jogszabaly/2004-34-00-00.16

KnowBe4 hivatalos weboldala

https://www.knowbe4.com/

KnowBe4 kiberbiztonsági megfelelésre vonatkozó információk

https://www.knowbe4.com/security

Human Hacking (a KnowBe4 hivatalos magyarországi forgalmazója)

https://humanhacking.hu/

Magyar nyelvű termékismertető

https://humanhacking.hu/wp-content/uploads/2024/02/Security-Awareness-Training-Productsheet-HU-2024-1.pdf

Elvárt védelmi intézkedések a „Tudatosság és képzés” területén

(részletes táblázat az MK rendeletből - 2. számú melléklet 3. fejezete)

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	3.1. Szabályzat és eljárásrendek	3.1. A szervezet: 3.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 3.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó tudatossági és képzési szabályzatot, amely 3.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 3.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 3.1.1.2. a tudatossági és képzési eljárásrendet, amely a tudatossági és képzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 3.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a tudatossági és képzési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 3.1.3. Felülvizsgálja és frissíti az aktuális tudatossági és képzési szabályzatot és a tudatossági és képzési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	3.2. Biztonságtudatossági képzés	3.2. A szervezet: 3.2.1. Biztonságtudatossági képzést biztosít a rendszer felhasználói számára (beleértve a vezetőket, felsővezetőket és a szerződéses partnereket is): 3.2.1.1. Az új felhasználók kezdeti képzése keretében, majd ezt követően a szervezet által meghatározott gyakorisággal. 3.2.1.2. Amennyiben az EIR-ben bekövetkezett változások ezt indokolttá teszik, vagy a szervezet által meghatározott események ezt megkövetelik. 3.2.2. Meghatározza azokat a technikákat, melyeket a rendszerfelhasználók biztonságtudatosságának növelése érdekében alkalmaz. 3.2.3. Frissíti a képzési és tudatossági tananyagot a szervezet által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően. 3.2.4. Integrálja a belső és külső biztonsági eseményekből levont tanulságokat a képzési anyagokba, valamint az alkalmazott biztonságtudatossági eszközrendszerébe.	X	X	X
4.	3.3. Biztonságtudatossági képzés – Gyakorlati feladatok	3.3. A szervezet a felkészítő képzést olyan gyakorlati feladatokkal egészíti ki, amelyek szimulálják a biztonsági eseményeket.	–	–	–
5.	3.4. Biztonságtudatossági képzés – Belső fenyegetés	3.4. A szervezet felkészítő képzést nyújt a belső fenyegetések potenciális jeleinek felismerésére és jelentésére.	X	X	X
6.	3.5. Biztonságtudatossági képzés – Pszichológiai befolyásolás és információszerzés	3.5. A szervezet felkészítő képzést nyújt a pszichológiai manipuláció és adatgyűjtés lehetséges és valós jeleinek felismerésére, valamint azok jelentésére.	–	X	X
7.	3.6. Biztonságtudatossági képzés – Gyanús kommunikáció és szokatlan rendszerviselkedés	3.6. A szervezet felkészítő képzést nyújt a szervezet rendszereiben felmerülő gyanús kommunikáció és rendellenes viselkedés felismerésére.	–	–	–
8.	3.7. Biztonságtudatossági képzés – Tartós fejlett fenyegetések	3.7. A szervezet felkészítő képzést nyújt a tartós fejlett fenyegetések (APT) felismerésére és kezelésére vonatkozóan.	–	–	–
9.	3.8. Biztonság-tudatossági képzés – Kiberfenyegetési környezet	3.8.1. A szervezet felkészítő képzést nyújt a kiberfenyegetési környezetről és 3.8.2. alkalmazza az aktuális kiberbiztonsági fenyegetési információkat a rendszerüzemeltetésben.	–	–	–
10.	3.9. Szerepkör alapú biztonsági képzés	3.9. A szervezet: 3.9.1. Szerepkör alapú biztonsági képzést nyújt a felhasználóknak: 3.9.1.1. Az EIR-hez vagy az információhoz való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően, továbbá azt követően a szervezet által meghatározott rendszerességgel. 3.9.1.2. Amikor az EIR-ben bekövetkezett változás azt szükségessé teszi. 3.9.2. Frissíti a szerepköralapú képzés tartalmát a szervezet által meghatározott rendszerességgel és a szervezet által meghatározott események bekövetkezését követően. 3.9.3. Beépíti a belső vagy külső biztonsági eseményekből levont tanulságokat a szerepköralapú biztonsági képzésekbe.	X	X	X

11.	3.10. Szerepkör alapú biztonsági képzés – Környezeti védelmi intézkedések	3.10. A szervezet kezdeti és időszakos képzést biztosít a szervezet által meghatározott személyek vagy szerepkörök számára a környezethez kapcsolódó biztonsági követelmények alkalmazásáról és működtetéséről.	–	–	–
12.	3.11. Szerepkör alapú biztonsági képzés – Fizikai védelmi intézkedések	3.11. A szervezet kezdeti és időszakos képzést biztosít a szervezet által meghatározott személyeknek vagy szerepköröknek a fizikai biztonsági követelményekből fakadó védelmi intézkedések alkalmazásáról és működtetéséről.	–	–	–
13.	3.12. Szerepkör alapú biztonsági képzés – Gyakorlati feladatok	3.12. A szervezet olyan biztonsági gyakorlati feladatokkal egészíti ki a felkészítő képzést, amelyek megerősítik a képzési célokat.	–	–	–
14.	3.13. A biztonsági képzésre vonatkozó dokumentációk	3.13. A szervezet: 3.13.1. Dokumentálja és nyomon követi az információbiztonsági képzési tevékenységeket, ideértve az általános információbiztonsági tudatossági képzéseket és a speciális szerepkör alapú információbiztonsági képzéseket. 3.13.2. Meghatározott ideig megőrzi a képzésről készült dokumentumokat.	X	X	X
15.	3.14. Képzés eredményeiről való visszajelzés	3.14. A szervezet rendszeresen visszajelzést ad a meghatározott személyeknek a szervezeti képzések eredményeiről.	–	–	–

A táblázat „C”, „D” és „E” oszlopai jelölik az adott követelmény használhatóságát, az ”Alap”, „Jelentős” és „Magas” biztonsági osztályok esetében. „X” jelöli, ha a védelmi intézkedés használata az adott biztonsági osztálynál elvárt, és „-” jelöli, ha a védelmi intézkedés használata az adott biztonsági osztálynál nem elvárás. Azon védelmi intézkedések, amelyek esetében a „C” „D” és „E” oszlopok egyaránt „-” jelölést tartalmaznak, kiegészítő védelmi intézkedések. Ezen kiegészítő védelmi intézkedéseket egyik biztonsági osztály esetében sem kötelező alkalmazni, a szervezetek azonban felhasználhatják ezeket a rájuk vonatkozó egyéb – különösen rendszerspecifikus sajátosságokból eredő – követelmények teljesítése érdekében.