Tájékoztató az információbiztonsági képzésre vonatkozó jogszabályi kötelezettségekről

Dátum: 2026. 06. 18.

A kiberbiztonság mára kiemelt vállalatirányítási és üzleti kockázattá vált, amely közvetlen hatással van a szervezet működésére, pénzügyi stabilitására és reputációjára. A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény előírja, hogy az érintett szervezet köteles gondoskodni a szervezet munkatársainak rendszeres információbiztonsági képzéséről. Így a dolgozók oktatása nemcsak a szervezet jól felfogott érdeke, hanem egyúttal jogszabályi kötelezettsége is.

Jogszabályi háttér

Magyarország az elmúlt években jelentősen megújította és szigorította a kiberbiztonságra vonatkozó jogszabályi keretrendszerét, elsősorban az uniós **NIS2 irányelv** hazai átültetése révén. A jelenleg hatályos fő jogforrás a **Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény** (a továbbiakban: Kiberbiztonsági tv.), amely 2025. január 1-jén lépett hatályba, és ezzel egyidejűleg hatályon kívül helyezte két elődjét: a 2023. évi XXIII. törvényt (Kibertan tv.) és a 2013. évi L. törvényt (Ibtv.).

A hazai Kiberbiztonsági tv. a NIS2 irányelvnek való megfelelést szolgálja, és hatálya a korábbi NIS2-es érintetti körnél szélesebb: kiterjed az állami szervekre, valamint az állam szempontjából kritikus tevékenységet ellátó szervezetekre is.

A pénzügyi szervezetek esetében a digitális működési reziliencia tekintetében az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (ún. **DORA-rendelet**) előírásait szükséges figyelembe venni.

A kiberbiztonsági képzések tekintetében a szervezet vezetőjére és információbiztonsági felelősére vonatkozóan további fontos részletszabályozást tartalmaz a **17/2025. (VII. 24.) EM rendelet**, valamint az elvárt védelmi intézkedések esetében a **7/2024. (VI. 24.) MK rendelet**.

Magyarországon a versenyszféra kiberbiztonsági felügyeleti hatósága a Kiberbiztonsági tv. 23. § (1) bekezdés b) pontja alapján a **Szabályozott Tevékenységek Felügyeleti Hatósága** (SZTFH), amely 2023-tól látja el ezt a feladatot. Az SZTFH hatáskörébe tartozik az érintett szervezetek nyilvántartásba vétele, az auditok elrendelése, a bejelentett események kezelése és a szankcionálás.

A pénzügyi szektorban a **Magyar Nemzeti Bank** (MNB) is rendelkezik kiberbiztonsági felügyeleti jogkörrel, különösen a DORA-rendelet vonatkozásában. Jogszabályban meghatározott körben szintén ellát hatósági

feladatokat a **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézete** (NBSZ NKI), valamint a **Katonai Nemzetbiztonsági Szolgálat** (KNBSZ).

Jogszabályok és 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 (NIS 2 irányelv). URL: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022L2555
- Az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2554 RENDELETE (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról (DORA-rendelet). URL: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022R2554
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról. URL: https://njt.jog.gov.hu/jogszabaly/2024-69-00-00
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről. URL: https://njt.jog.gov.hu/jogszabaly/2024-7-20-7G
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról. URL: https://njt.jog.gov.hu/jogszabaly/2024-418-20-22
- 17/2025. (VII. 24.) EM rendelet a Magyarország kiberbiztonságáról szóló törvény szerinti végzettségekre, szakképzettségekre, valamint képzésekre és továbbképzésekre vonatkozó követelményekről. URL: https://njt.jog.gov.hu/jogszabaly/2025-17-20-8Y
- Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) weboldala: https://sztfh.hu/
- Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NKI) weboldala: https://nki.gov.hu/
- Felnőttképzési Adatszolgáltatási Rendszer weboldala: https://far.nive.hu/
- Nemzeti Koordinációs Központ (NCC-HU) weboldala: https://ncc.gov.hu/

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

Információbiztonsági képzés, mint törvényi kötelezettség

A Kiberbiztonsági törvény 6. szakasz 5. a) pontjában egyértelműen rögzíti, hogy a szervezet vezetője az elektronikus információs rendszer védelmének biztosítása érdekében gondoskodik az elektronikus információs rendszerek védelmi feladatainak és az azokhoz kapcsolódó felelősségi köröknek az oktatásáról, saját maga és a szervezet munkatársainak kiberbiztonsági képzéséről, továbbképzéséről.

A DORA-rendelet 13. cikk 6. bekezdése rögzíti, hogy a pénzügyi szervezeteknek a személyzetük képzési rendszerének részét képező kötelező modulokként IKT-biztonsági tudatosságot elősegítő programokat és a digitális működési rezilienciával kapcsolatos képzéseket kell kidolgozniuk.

A fenti hivatkozások alapján egyértelműen látszik, hogy a dolgozók biztonságtudatossági oktatása nemcsak a szervezetek jól felfogott érdeke, hanem egyúttal jogszabályi kötelezettsége is.

7/2024. (VI. 24.) MK rendelet:
Elvárt védelmi intézkedések a képzés területén

A 7/2024. (VI. 24.) MK rendelet meghatározza, hogy az adott szervezet a Kiberbiztonsági törvény hatálya alá tartozó elektronikus információs rendszerét (EIR) mely szempontok szerint sorolja biztonsági osztályba. Továbbá ezen besorolás alapján a rendelet 2. számú melléklete, a „Védelmi intézkedések katalógusa" részletezi az elvárt védelmi intézkedéseket az egyes területeken.

A melléklet 3. fejezete foglalkozik a „Tudatosság és képzés" témakörével, és a biztonsági osztályba sorolás (Alap, Jelentős, Magas) szerint meghatározza az elvárt intézkedéseket. A könnyebb átláthatóság érdekében az egyes tudatosság és képzési 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 részletes táblázatot lásd a Mellékletben.)

Figyelembe kell venni, hogy a DORA hatálya alá tartozó szervezetekre nem vonatkozik ez a rendelet, mivel ez a jogszabály a NIS2/Kiberbiztonsági törvény hatálya alá tartozó szervezetekre érvényes.

Ugyanakkor a DORA 13. cikk (6) bekezdése szerint a pénzügyi szervezeteknek a személyzetük képzési rendszerének részét képező kötelező modulokként IKT-biztonsági tudatosságot elősegítő programokat és a digitális működési rezilienciával kapcsolatos képzéseket kell kidolgozniuk. Az említett programok és képzések valamennyi munkavállalóra és a felső vezetés valamennyi tagjára alkalmazandók, és azok összetettségi szintjét a munkavállalók feladatköreihez kell igazítani.

17/2025. (VII. 24.) EM rendelet:
Képzésekre és végzettségekre vonatkozó követelmények

A 17/2025. (VII. 24.) EM rendelet szabályozza a képzési- és vizsgakövetelményeket a szervezet vezetője, valamint az elektronikus információs rendszer (EIR) biztonsági felelős számára.

MUNKATÁRSAK KÉPZÉSE

A szervezet munkatársainak kibertudatosságát növelő szervezeten belüli képzéseket nem ez a rendelet, hanem a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet szabályozza (lásd a korábbi fejezetben).

A SZERVEZET VEZETŐJÉNEK KÉPZÉSE

A 17/2025. (VII. 24.) EM rendelet kiemeli annak a jelentőségét, miszerint az érintett szervezetek kiberbiztonságának kulcsszereplője, a szervezet vezetője vegyen részt a kiberbiztonság jelentőségét tudatosító képzésen, illetve továbbképzésen.

Hatály

Fontos megvizsgálni, hogy az adott szervezetre vonatkozik-e egyáltalán a rendeletnek ezen előírása?

A NIS2/Kiberbiztonsági törvény tekintetében nagy valószínűséggel igen, mert a rendeletnek a szervezet vezetőjére vonatkozó rendelkezéseit a Kiberbiztonsági tv. 1. § (1) és (2a) bekezdése szerinti szervezetek vonatkozásában alkalmazni szükséges.

- Például vonatkozik a rendelet azon cégek vezetőire, amelyek létszáma minimum 50 fő, és a törvény 2. és 3. számú mellékleteiben felsorolt ágazatokban (energetika; közlekedés; egészségügy; élelmiszer előállítása, feldolgozása, forgalmazása; gyártás; digitális szolgáltatók; stb.) működnek. Ez a pont önmagában több ezer céget érint Magyarországon.
- De a vezetők képzése tekintetében ugyanígy a rendelet hatálya alá tartoznak méretüktől függetlenül az elektronikus hírközlési szolgáltatók.
- Továbbá ide tartoznak többek között a közigazgatási ágazathoz tartozó szervezetek, a minimum 50 fős többségi állami befolyás alatt álló gazdálkodó szervezetek, a kiberbiztonsági hatóság által alapvető vagy fontos szervezetként azonosított szervezetek, a jogszabály alapján kijelölt kritikus szervezetek.

Ugyanakkor a DORA hatálya alá tartozó szervezetek esetében a helyzet eltér a NIS2/Kiberbiztonsági törvény hatálya alá tartozó szervezetekétől. A DORA rendelet maga nem ír elő konkrét óraszámú vagy tanúsítványhoz kötött vezetői kiberbiztonsági képzést. Viszont a DORA rendelet is megköveteli, hogy rendszeres képzések révén a pénzügyi szervezet vezető testülete és a felső vezetés valamennyi tagjának megfelelő tudása legyen az IKT-biztonsági tudatosság és a digitális működési reziliencia területén.

- A DORA 5. cikk (4) bekezdése szerint a pénzügyi szervezet vezető testülete tagjainak aktívan tájékozódniuk kell az aktuális információkról annak érdekében, hogy rendelkezésükre álljanak az

ahhoz szükséges megfelelő ismeretek és készségek, hogy át tudják látni és értékelni tudják az IKT-kockázatot és annak a pénzügyi szervezet működésére gyakorolt hatását, többek között a kezelés alatt álló IKT-kockázattal arányos, célirányos képzés rendszeres végzése révén.

A szervezet vezetője

Felmerül a kérdés, hogy ki az adott szervezet vezetője, akinek részt kell vennie a kötelező kiberbiztonsági képzésen, illetve továbbképzésen?

Fogalomrendszerében sem a 17/2025. (VII. 24.) EM rendelet, sem a Kiberbiztonsági tv. sem határozza meg külön, hogy ki minősül a szervezet vezetőjének. A gyakorlatban a szervezet vezetője az a személy vagy testület, amely a szervezet jogszerű működéséért és irányításáért felelős, és amely a szervezet képviseletére jogosult. A szervezet típusától függően ez jellemzően gazdasági társaságnál az ügyvezető, vezérigazgató vagy igazgatóság; költségvetési szervnél az intézményvezető, hivatalvezető vagy főigazgató.

Zrt. esetében általában az igazgatóság tagjai, illetve vezérigazgatói működés esetén a vezérigazgató tekinthető a szervezet vezetőjének. Van azonban egy gyakorlati bizonytalanság: ha a zrt.-nek többtagú igazgatósága van, a rendelet szövege nem mondja ki egyértelműen, hogy minden igazgatósági tagnak el kell-e végeznie a vezetői képzést, vagy elegendő az igazgatóság elnökének, illetve a vezérigazgatónak.

Képzési kötelezettség

Amennyiben megállapítottuk, hogy a szervezet vezetője tekintetében vonatkozik ránk a rendelet hatálya, és meghatároztuk a szervezet vezetőjét is, akkor menjünk tovább.

A rendelet 4. § (1) szakasza kimondja, hogy a szervezet vezetője köteles részt venni

a) a szervezet vezetőjévé válását követő egy éven belül egy, összesen legalább 8 órás időtartamban szervezett képzésen, valamint ezt követően
b) évente összesen legalább 4 órás időtartamban szervezett továbbképzésen.

A szervezet 2025. december 31-ét megelőzően kinevezett vagy megbízott vezetője a 4. § (1) bekezdés a) pontja szerinti (legalább 8 órás) képzést 2026. december 31-ig köteles elvégezni.

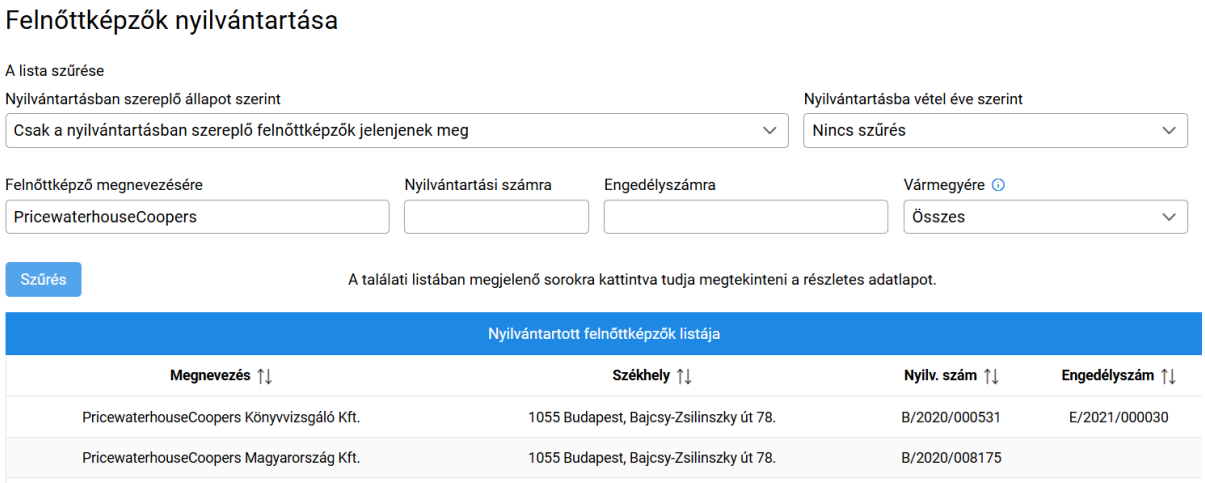
Felnőttképző általi szervezett képzés

A rendelet szintén rögzíti, hogy a szervezet vezetőjének képzése, továbbképzése a felnőttképzésről szóló 2013. évi LXXVII. törvényben (a továbbiakban: Fktv.) meghatározott képzési forma szerint valósítható meg.

Azaz a szervezet vezetője esetében a (munkatársak belső képzésére irányadó) 7/2024. (VI. 24.) MK rendeletben meghatározott képzésen való részvétel nem mentesíti a szervezet vezetőjét az e rendeletben foglaltak szerinti képzés, illetve továbbképzés elvégzésének kötelezettsége alól!

Képzést, továbbképzést olyan, az Fktv. szerint bejelentett felnőttképző szervezhet, amely a kiberbiztonság területén legalább 3 éves oktatási, képzési tapasztalattal rendelkező szakembert tud oktatóként biztosítani. A képzés, illetve továbbképzés tárgyköreit a rendelet meghatározza. A képzés vagy továbbképzés elvégzéséről a felnőttképző az Fktv. 13/B. §-a szerinti tanúsítványt állít ki.

A felnőttképzőnek a képzéshez, továbbképzéshez képzési programot szükséges készítenie, melyet az Fktv. szerinti felnőttképzési adatszolgáltatási rendszerbe fel kell tölteni (https://far.nive.hu/kezdolap).



Példa keresés a felnőttképzési adatszolgáltatási rendszerben:
https://far.nive.hu/publikus-adatok/felnottkepzok-nyilvantartasa

Összefoglalás

Foglaljuk össze a lényeget egy rövid példával:

- A Kiberbiztonsági törvény hatálya alá eső NIS2 kötelezett cég (például egy több mint 50 főt foglalkoztató élelmiszer feldolgozással foglalkozó középvállalat) ügyvezetője köteles részt venni egy regisztrált felnőttképző által szervezett, legalább 8 órás kiberbiztonsági képzésen, majd azt követően évente egy 4 órás továbbképzésen. A képzés vagy továbbképzés elvégzéséről a felnőttképző tanúsítványt állít ki, amelyet a szervezet vezetőjének be kell mutatnia egy esetleges hatósági ellenőrzés alkalmával.

ELEKTRONIKUS INFORMÁCIÓS RENDSZER BIZTONSÁGÁÉRT FELELŐS SZEMÉLY

A 17/2025. (VII. 24.) EM rendelet már a bevezetőjében rögzíti, hogy a szervezet vezetője mellett a szervezet kiberbiztonsági szempontból másik kulcsszereplője, az elektronikus információs rendszer biztonságáért felelős személy megfelelő végzettséggel és szakképzettséggel rendelkezzen, valamint évente részt vegyen a feladatai magas színvonalú ellátásához szükséges, az ismereteit bővítő kiberbiztonsági továbbképzéseken.

Az EIR biztonságáért felelős személy vonatkozásában a rendelet egyes rendelkezéseit nem egyformán kell alkalmazni, azok hatálya nem egységes a szervezetek tekintetében.

Végzettség, szakképzettség (EIR-felelős)

Az elektronikus információs rendszer biztonságáért felelős személy végzettségére, szakképzettségére vonatkozó követelményeket (a rendelet 2. alcíme) a Kiberbiztonsági törvény hatálya alá tartozó alábbi szervezetek esetében szükséges alkalmazni (hatály):

a) a Kiberbiztonsági tv. 1. § (1) bekezdés a)–c) és f) pontja szerinti szervezetnél,
(ide tartoznak többek között a közigazgatási ágazathoz tartozó szervezetek, a minimum 50 fős többségi állami befolyás alatt álló gazdálkodó szervezetek, a kiberbiztonsági hatóság által alapvető

vagy fontos szervezetként azonosított szervezetek, a honvédelmi érdekhez kapcsolódó gazdasági társaságok, DE
nem tartoznak ide a törvény 2. és 3. mellékletében felsorolt ágazatokban működő szervezetek)

b) a Kiberbiztonsági tv. hatálya alá tartozó, a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény alapján kritikus szervezetként kijelölt szervezetnél,
c) a Kiberbiztonsági tv. hatálya alá tartozó, a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény alapján az ország védelme és biztonsága szempontjából jelentős szervezetként kijelölt szervezetnél.

A fent felsorolt érintett szervezetek esetében a 17/2025. (VII. 24.) EM rendelet 2. § (1) bekezdése szerint az EIR biztonságáért felelős személynek felsőfokú végzettséggel kell rendelkeznie. Ugyanezen szakasz (2) bekezdése szerint az elfogadható szakképzettségek és akkreditált nemzetközi képzettségek listáját a nemzeti koordinációs központ állítja össze, és teszi közzé a honlapján.

2025. január 1-jétől a Nemzetbiztonsági Szakszolgálat került kijelölésre a magyarországi Nemzeti Koordinációs Központ (NCC-HU) feladatainak ellátására. Az elfogadható szakképzettségek listája a következő URL címen található meg: https://ncc.gov.hu/ibf-kepzesek-listaja/

FONTOS! Még egyszer szeretnénk hangsúlyozni, hogy a Kiberbiztonsági törvény 1. § (1) bekezdés d) és e) pontjai szerinti szervezeteknél nem kell alkalmazni az elektronikus információs rendszer biztonságáért felelős személy végzettségére és szakképzettségére vonatkozó rendelkezéseket!

- Azaz a törvény 2. és 3. mellékletében felsorolt ágazatokban működő szervezeteknél nem szükséges, hogy az EIR biztonságáért felelős személy a nemzeti koordinációs központ által elfogadott szakképzettséggel vagy akkreditált nemzetközi képzettséggel rendelkezzen.

Felnőttképző által szervezett továbbképzés (EIR-felelős)

Az elektronikus információs rendszer biztonságáért felelős személy továbbképzésére vonatkozó rendelkezéseket ugyanazon szervezetek esetében szükséges alkalmazni, mint a (korábban részletezett) szervezet vezetője esetében. Azaz a Kiberbiztonsági tv. 1. § (1) és (2a) bekezdése szerinti szervezetek vonatkozásában.

- Tehát vonatkozik a rendelet ezen előírása azon cégek EIR-felelőseire, amelyek létszáma minimum 50 fő, és a törvény 2. és 3. számú mellékleteiben felsorolt ágazatokban működnek. Ugyanígy vonatkozik méretüktől függetlenül egyes a 2. és 3. mellékletben felsorolt, meghatározott szolgáltatókra (elektronikus hírközlési szolgáltatók, DNS-szolgáltatók, stb.).
- Továbbá ide tartoznak többek között a közigazgatási ágazathoz tartozó szervezetek, a minimum 50 fős többségi állami befolyás alatt álló gazdálkodó szervezetek, a kiberbiztonsági hatóság által alapvető vagy fontos szervezetként azonosított szervezetek, a jogszabály alapján kijelölt kritikus szervezetek.

A fenti szervezetek esetében a rendelet 3. § (1) bekezdése szerint az EIR biztonságáért felelős személy köteles a kiberbiztonsági és jogszabályi ismereteit bővítő továbbképzésen részt venni, a rendeletben rögzített tárgykörök közül legalább három tárgykörben, évente összesen legalább 20 órás időtartamban.

A rendelet rögzíti, hogy a szervezet vezetőjének képzéséhez/továbbképzéséhez hasonlóan az EIR biztonságáért felelős személy továbbképzése a felnőttképzésről szóló 2013. évi LXXVII. törvényben (Fktv.)

meghatározott képzési forma szerint valósítható meg. Azaz az EIR biztonságáért felelős személy tekintetében továbbképzést kizárólag az Fktv. szerint bejelentett felnőttképző szervezhet, valamint a továbbképzés elvégzéséről a felnőttképző tanúsítványt állít ki.

Összefoglalás

Foglaljuk össze a lényeget ismét egy rövid példával:

- A Kiberbiztonsági törvény hatálya alá eső NIS2 kötelezett cég (például egy több mint 50 főt foglalkoztató élelmiszer feldolgozással foglalkozó középvállalat) esetében nem szükséges, hogy az EIR biztonságáért felelős személy a nemzeti koordinációs központ (NCC) által elfogadott szakképzettséggel vagy akkreditált nemzetközi képzettséggel rendelkezzen.
- Ugyanakkor ezen társaság EIR-felelőse köteles évente összesen legalább 20 órás időtartamban részt venni egy regisztrált felnőttképző által szervezett kiberbiztonsági továbbképzésen. A továbbképzés elvégzéséről a felnőttképző tanúsítványt állít ki, amelyet be kell mutatni egy esetleges hatósági ellenőrzés alkalmával.

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.