Milyen oktatásokat kell elvégezni a NIS2 megfeleléshez és hogyan kell azokat végrehajtani?

VFP2 KiberVéd - NIS2 Audit felkészítés szakmai iránymutatás
A Szabályozott Tevékenységek Felügyeleti Hatósága által jóváhagyott szöveg

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.02.12	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. ÖSSZEFOGLALÁS

Jelen iránymutatás célja annak részletes bemutatása, hogy a NIS2 megfeleléshez kapcsolódó kiberbiztonsági képzési és tudatosítási kötelezettségek milyen típusú oktatási tevékenységeket igényelnek, kiket érintenek, valamint hogyan kell azt a gyakorlatban végrehajtani úgy, hogy a szervezet védelmi intézkedései valóban működőképesek legyenek.

Az iránymutatás abból az alapelvből indul ki, hogy a NIS2 szerinti megfelelés nem kizárólag szabályzatok és eljárásrendek létrehozásával valósul meg, hanem olyan képességek és kompetenciák kialakításával és fenntartásával, amelyek biztosítják a szabályozási elvárások napi szintű alkalmazását.

A védelmi intézkedések végrehajtása minden esetben az érintett szereplők – vezetők, rendszergazdák, általános felhasználók, stb. – tudásán, felkészültségén és döntésein alapul, ezért a képzés nem önálló, elkülönült megfelelési elemként, hanem a teljes védelmi rendszer működésének alapfeltételeként értelmezendő.

Az informatikai biztonsághoz kapcsolódó oktatások elsődleges célja nem a szabályzatok részletes ismertetése, hanem annak biztosítása, hogy a szervezet különböző szerepköreiben eljáró személyek tisztában legyenek a rájuk vonatkozó elvárásokkal, felelősségekkel és beavatkozási pontokkal. A biztonsági képzés a szervezet kezében az az eszköz, amely a jogszabályi és belső szabályozási követelményeket a napi működés során meghozott döntésekhez és végrehajtási tevékenységekhez kapcsolja.

Jelen iránymutatás ezen alapelvek mentén ismerteti a szükséges oktatási elemeket, a célcsoportokat, valamint a végrehajtás irányelveit.

2. PROBLÉMAFELVETÉS

A modern információbiztonsági gyakorlatban közismert, hogy a technológiai intézkedések és a kialakított folyamatok hatékonyságát döntően az azokat alkalmazó humán erőforrás határozza meg. Az érintett munkavállalók és szereplők a védelmi rendszer elválaszthatatlan részei, ugyanakkor megfelelő felkészítés hiányában a biztonsági lánc leginkább sérülékeny elemévé válhatnak.

Általánosan elfogadott tapasztalat, hogy a biztonsági események jelentős része nem a technikai védelmi intézkedések hiányára, hanem emberi hibára, figyelmetlenségre vagy nem megfelelő döntésre vezethető vissza. Ennek következtében a védelmi intézkedések önmagukban nem biztosítanak megfelelő védelmet. Az oktatások révén válik egyértelművé, hogy az egyes védelmi intézkedések milyen konkrét elvárásokat támasztanak a vezetők, a szakmai területek, az üzemeltetés, a fejlesztés vagy a beszerzés szereplői felé.

A megfelelően kialakított oktatási rendszer hiányában a védelmi intézkedések alkalmazása esetleges és személyfüggő maradhat. Ezzel szemben a célzott, rendszeres és dokumentált oktatások biztosítják, hogy a NIS2 szerinti követelmények a szervezeti működés szerves részévé váljanak, és ne kizárólag dokumentációs megfelelési célt szolgáljanak.

3. IRÁNYMUTATÁS

3.1 Milyen oktatásokat kell elvégezni a NIS2 megfeleléshez?

A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (továbbiakban: Kiberbiztonsági tv.), valamint a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (továbbiakban: MK rendelet) nem határoz meg tételes, előre rögzített képzési vagy tanfolyamlistát a szervezetek számára. A jogalkotó ehelyett a kiberbiztonsági védelmi intézkedésekhez rendelten ír elő képzési és tudatosságnövelési kötelezettségeket, amelyek teljesítésének módját és tartalmát a szervezet saját kockázati környezetéhez, működéséhez és szerepköreihez igazodva kell kialakítani.

A fenti jogszabályok mellett a jogalkotó egyéb, kifejezetten nevesített képzési kötelezettségeket is előírhat, amelyek nem közvetlenül a védelmi intézkedésekhez, hanem meghatározott funkciókhoz vagy tisztségekhez kapcsolódnak. Ilyenek például az információbiztonsági felelős[1], valamint a szervezet vezetője[2] részére előírt kötelező képzések és továbbképzések. A fentieken túl a szervezet a szerződéses partnereivel szemben is megkövetelhet, illetve – az MK rendelet alapján bizonyos esetekben[3] – megkövetel olyan képzés igazolását, mely valamely védelmi intézkedéshez kapcsolódóan a kockázatok kezeléséhez hozzájárulhat. Ez utóbbi két képzési kategória esetében a képzések megszervezése és lebonyolítása nem a szervezet feladata, ugyanakkor a képzésen, illetve továbbképzésen való részvétel igazolásának beszerzése és nyilvántartása a szervezet felelősségi körébe tartozik.

Mindezek alapján a képzési kötelezettségek áttekinthető és következetes kezelése érdekében indokolt a képzési portfóliót az alábbi fő csoportokba rendezni:

– *általános biztonságtudatossági képzések*, amelyek a szervezet valamennyi szerepkörben foglalkoztatott felhasználójára kiterjednek,

– *speciális, szerepkörhöz rendelt képzések*, amelyek meghatározott feladatkörökhöz vagy felelősségekhez kapcsolódnak, valamint az

– *egyéb, nem a szervezetnél teljesítendő kötelező képzések és továbbképzések*, különös tekintettel a vezetői és információbiztonsági felelősi képzésekre, valamint a szerződéses partnerektől elvárt képzésekre.

3.2 Hogyan kell az oktatásokat végrehajtani?

Az MK rendelet alapján a szervezetet alapvető védelmi intézkedési kötelezettségként terheli a kiberbiztonsági képzések szabályozott keretek közötti megvalósítása.[4] Ennek részeként mindhárom biztonsági osztályba sorolt szervezetnek tudatossági és képzési szabályzatot (*3.1.1.1.*

[1] a Magyarország kiberbiztonságáról szóló törvény szerinti végzettségekre, szakképzettségekre, valamint képzésekre és továbbképzésekre vonatkozó követelményekről szóló 17/2025. (VII. 24.) EM rendelet 3. alcím

[2] 17/2025. (VII. 24.) EM rendelet 4. alcím

[3] lásd az iránymutatás 4.1.3.1. alcímében

[4] MK rendelet 2. melléklet 3. követelmény: „Tudatosság és képzés”

követelmény) és a végrehajtást részletező tudatossági és képzési eljárásrendet (*3.1.1.2. követelmény*) kell kialakítania és fenntartania.

E dokumentumok feladata, hogy a jogszabályi elvárásokkal összhangban, egységes rendszerben határozzák meg a szervezet képzési gyakorlatát, különös tekintettel a képzések céljára, hatókörére, érintett szerepkörökre, gyakoriságára, valamint az elszámoltathatóság és nyomon követhetőség biztosítására. A képzési szabályzatnak és eljárásrendnek egyértelműen le kell fednie mind az általános tudatossági képzéseket, mind a speciális, szerepkörhöz kötött képzéseket, továbbá az egyéb jogszabály alapján kötelező képzéseket és továbbképzéseket.

Az MK rendelet nem ír elő egységes, minden szervezetre azonos módon alkalmazandó oktatási formát, hanem azt az elvet érvényesíti, hogy a képzési és tudatossági védelmi intézkedéseket a szervezet biztonsági osztályával és kockázati kitettségével arányosan kell megvalósítani.

Ennek megfelelően a képzések többféle formában is megvalósulhatnak: személyes jelenléttel tartott oktatásként, online vagy e-learning formában, gyakorlati példákkal alátámasztott tudatosságnövelő képzésként, illetve — különösen magasabb kockázatú szerepkörök esetében — konkrét gyakorlatok vagy szimulációk keretében. Az alkalmazott módszertan megválasztását minden esetben befolyásolja az adott képzés tematikája, a célzott szerepkör, a szervezet biztonsági osztályba sorolása, valamint a kezelt kockázatok jellege és mértéke.

A képzések végrehajtása során alapvető követelmény az információbiztonsági képzési tevékenységek dokumentálása és folyamatos nyomon követése, összhangban az MK rendelet 2. mellékletében meghatározott[5] elvárásokkal. Ennek keretében a szervezetnek igazolható módon kell rögzítenie mind az általános információbiztonsági tudatossági képzéseket, mind a speciális, szerepkörhöz kötött információbiztonsági képzéseket.

A dokumentációnak alkalmasnak kell lennie arra, hogy bemutassa a képzések megvalósulását, így különösen azok időpontját, tematikáját, az érintett résztvevői kört, valamint a teljesítés tényét. A képzésekhez kapcsolódó dokumentumokat a szervezet a belső szabályozásában meghatározott ideig köteles megőrizni, biztosítva ezzel a megfelelés igazolhatóságát.

4. INDOKOLÁS

4.1 Milyen oktatásokat kell elvégezni a NIS2 megfeleléshez?

A biztonsági képzések a belső szabályozási rendszer gyakorlati kiegészítéseként értelmezhetők. Míg az Információbiztonsági szabályzat (IBSZ) és az egyes eljárásrendek rögzítik az elvárt magatartási és működési szabályokat, a képzések ezek értelmezését és alkalmazását támogatják, amelynek keretében az általános biztonságtudatossági képzések elsősorban az IBSZ valamennyi felhasználót érintő rendelkezéseire, míg a szerepköralapú képzések az IBSZ kapcsolódó szabályaira és a speciális eljárásrendekre épülnek.

[5] MK rendelet 2. melléklet 3.13. követelmény: „A biztonsági képzésre vonatkozó dokumentációk”

4.1.1 Általános biztonságtudatossági képzések

Az általános biztonságtudatossági képzések célja, hogy a szervezet valamennyi felhasználója számára átadásra kerüljenek az informatikai biztonsághoz kapcsolódó alapvető ismeretek. A képzés egyfajta „alapműveltség” kialakítását szolgálja, amely a szervezetre irányadó legfontosabb, minden felhasználóra – szerepkörtől függetlenül – vonatkozó védelmi intézkedések, valamint az általánosan felismerhető és kezelhető fenyegetések és kockázatok bemutatásán keresztül biztosítja a szervezet vezetése által – a kockázatokkal arányosan – elvárt minimális ellenállóképességet.

4.1.1.1 A képzés tematikája

Az általános biztonságtudatossági képzés tematikájával kapcsolatban a jogalkotó az MK rendelet alábbi követelményei révén fogalmaz meg elvárást, illetve ajánlást:

Védelmi intézkedés szerinti tematika	**Védelmi intézkedés leírása**	**Követelmény száma**	**Biztonsági osztály**
Általános információbiztonsági tudatossági képzés biztosítása	*A szervezet:* *3.2.1 Biztonságtudatossági képzést biztosít a rendszer felhasználói számára (beleértve a vezetőket, felsővezetőket és a szerződéses partnereket is)* *3.2.4 Integrálja a belső és külső biztonsági eseményekből levont tanulságokat a képzési anyagokba, valamint az alkalmazott biztonságtudatossági eszközrendszerébe.*	3.2	Alap (A); Jelentős (J); Magas (M)
Gyakorlati feladatok	*A szervezet a felkészítő képzést olyan gyakorlati feladatokkal egészíti ki, amelyek szimulálják a biztonsági eseményeket.*	3.3	-
Belső fenyegetések felismerésére	*A szervezet felkészítő képzést nyújt a belső fenyegetések potenciális jeleinek felismerésére és jelentésére.*	3.4	A;J;M
Pszichológiai befolyásolás és információszerzés (social engineering) felimerése és jelentése	*A szervezet felkészítő képzést nyújt a pszichológiai manipuláció és adatgyűjtés lehetséges és valós jeleinek*	3.5	J;M

Védelmi intézkedés szerinti tematika	Védelmi intézkedés leírása	Követelmény száma	Biztonsági osztály
	felismerésére, valamint azok jelentésére.		
Gyanús rendszerkommunikáció, szokatlan rendszerviselkedés felismerése	*A szervezet felkészítő képzést nyújt a szervezet rendszereiben felmerülő gyanús kommunikáció és rendellenes viselkedés felismerésére.*	3.6	-
Tartós fejlett fenyegetések (APT) felismerése	*A szervezet felkészítő képzést nyújt a tartós fejlett fenyegetések (APT) felismerésére és kezelésére vonatkozóan.*	3.7	-
Kiberfenyegetési környezetre vonatkozó ismeretek	*3.8.1. A szervezet felkészítő képzést nyújt a kiberfenyegetési környezetről*	3.8.1.	-

A jogalkotó fenti elvárásai, ajánlásai mellett az IBSZ szabályozási körébe utalt azon ismereteket indokolt minimálisan átadni a felhasználók számára, melyek a szervezet mindennapi működéséhez kapcsolódnak, és amelyek a minden felhasználó számára befogadható és velük szemben elvárható követelményeket foglalják össze. Ilyenek különösen:

- Humánpolitikai eseményekhez kapcsolódó informatikai biztonsági ismeretek (Jogviszony létesítéséhez, módosulásához, megszűnéséhez rendelt intézkedések. Pl. jogosultságkezelés, informatikai eszközök igénylése és visszaszolgáltatása, elszámolási kötelezettségek).
- Elvárt magatartás (pl.: munkahelyi és magáncélú internethasználat szabályai; mobileszközök használata; közösségi médiumok munkaidőben történő használata; munkaállomás- és képernyővédelem; idegen és nem engedélyezett szoftverek használata és telepítése). Külön kiemelendő:
    - a magántulajdonú eszközök munkahelyi használatára (BYOD) vonatkozó alapelvek,
    - a generatív mesterséges intelligencia munkavégzési célú használatának szabályai.
- Jelszókezelés és hitelesítés alapelvei, ideértve a biztonságos jelszóhasználatot és az azonosítók védelmét.
- Vírusvédelemmel és rosszindulatú kódokkal kapcsolatos alapvető ismeretek (különös tekintettel a kéretlen elektronikus levelek kezelésére, a külső adathordozók csatlakoztatására vonatkozó szabályokra).

- Social engineering (Bár az MK rendelet a kifejezetten erre irányuló kötelező képzést a jelentős biztonsági osztálytól írja elő, a folyamatosan változó fenyegetési környezetre, valamint a mesterséges intelligencia térnyerésére tekintettel indokolt az alapszintű figyelemfelhívás, különösen a megszemélyesítés jelenségére és tipikus megvalósulási formáira.).
- Biztonsági események észlelésére és jelentésére vonatkozó alapvető információk, ideértve a felhasználók szerepét, a jelentési csatornákat és a bejelentés fontosságát.
- Adatvédelmi alapismeretek.

4.1.2 Szerepkör alapú biztonsági képzések

Az MK rendelet 2. melléklete több, az alábbiakban bemutatott védelmi intézkedés esetében kifejezetten nevesíti a meghatározott szerepkörökhöz rendelt oktatási és felkészítési kötelezettségeket. Ezek a követelmények egyértelművé teszik, hogy az információbiztonság hatékony működése nem kizárólag általános tudatossági szinten értelmezendő, hanem számos esetben célzott, feladatkör- és felelősségalapú felkészítést igényel.

A szerepkör alapú képzések kapcsán a jogalkotó az MK rendelet alábbi követelményei révén fogalmaz meg elvárást, illetve ajánlást:

Védelmi intézkedés szerinti tematika	**Védelmi intézkedés leírása**	**Követelmény száma**	**Biztonsági osztály**
Biztonsági személyzet képzése	*A szervezet létrehozza a biztonsági személyzet képzését és fejlesztését elősegítő programot.*	1.14.	A;J;M
Nyilvánosan elérhető tartalom közzététele	*A szervezet képzést biztosít a jogosult személyek számára, hogy biztosítsa, hogy a nyilvánosan hozzáférhető információk nem tartalmaznak nem nyilvános információkat.*	2.124.2.	A;J;M
Szerepkör alapú biztonsági képzés	*A szervezet:* *3.9.1. Szerepkör alapú biztonsági képzést nyújt a felhasználóknak* *3.9.3. Beépíti a belső vagy külső biztonsági eseményekből levont tanulságokat a szerepköralapú biztonsági képzésekbe.*	3.9	A;J;M

Védelmi intézkedés szerinti tematika	Védelmi intézkedés leírása	Követelmény száma	Biztonsági osztály
	A szervezet olyan biztonsági gyakorlati feladatokkal egészíti ki a felkészítő képzést, amelyek megerősítik a képzési célokat.	3.12	-
Környezeti védelmi intézkedések	*A szervezet kezdeti és időszakos képzést biztosít a szervezet által meghatározott személyek vagy szerepkörök számára a környezethez kapcsolódó biztonsági követelmények alkalmazásáról és működtetéséről.*	3.10	-
Fizikai védelmi intézkedések	*A szervezet kezdeti és időszakos képzést biztosít a szervezet által meghatározott személyeknek vagy szerepköröknek a fizikai biztonsági követelményekből fakadó védelmi intézkedések alkalmazásáról és működtetéséről.*	3.11	-
A folyamatos működésre felkészítő képzés (Szimulált események; A képzési környezetben használt mechanizmusok)	*A szervezet az EIR felhasználói számára szerepkörüknek vagy felelősségi körüknek megfelelő folyamatos működésre felkészítő képzést tart.*	7.10.1	A;J;M
	A szervezet a folyamatos működésre felkészítő képzésben szimulált eseményeket alkalmaz, hogy elősegítse a személyzet hatékony reagálását a szervezet működése szempontjából kritikus helyzetekben.	7.11.	M

Védelmi intézkedés szerinti tematika	Védelmi intézkedés leírása	Követelmény száma	Biztonsági osztály
	A szervezet valós működési mechanizmusokat alkalmaz, hogy ezáltal alaposabb és valósághűbb vészhelyzeti képzési környezetet biztosítson.	7.12.	-
Biztonsági események kezelése (Szimulált események; Automatizált képzési környezet; Információszivárgásra adott válaszlépések)	*A szervezet biztonsági eseménykezelési képzést biztosít a felhasználóknak a rájuk bízott szerepek és felelősségek szerint.*	9.2.1.	A;J;M
	A szervezet szimulált eseményeket épít be a biztonsági események kezelésére vonatkozó képzésbe, hogy elősegítse a személyzet számára a válsághelyzetekben szükséges reagálást.	9.3.	M
	A szervezet automatizált mechanizmusokat alkalmaz, hogy a biztonsági eseménykezelési képzéséhez valósághű környezetet biztosítson.	9.4.	M
	A szervezet meghatározott gyakorisággal megtartja az információszivárgási események kezelésére vonatkozó képzést.	9.36.	-
Rendszerelem hitelessége – Hamisítás elleni képzés	*A szervezet a meghatározott személyeknek vagy szerepköröknek képzést biztosít a hamisított rendszerelemek (beleértve a hardvert, szoftvert és firmware-t) felismerésére.*	19.24.	A;J;M

Az MK rendelet a szerepkörökhöz kapcsolódó felkészítési kötelezettségeket általános elvként rögzíti a 3.9.1. számú követelményében. Ezt az alapelvet a jogalkotó – a fentebb bemutatott – egyes védelmi intézkedések esetében konkrét, nevesített képzési elvárásokkal, ajánlásokkal egészíti ki.

A szerepkör alapú képzési kötelezettség azonban nem kizárólag a fent kifejezetten megjelölt képzési tárgykörökre és szerepkörökre értelmezendő. Az információbiztonsági követelmények gyakorlati alkalmazása során a szervezet által az MK rendelet alapján kialakított belső szabályozók – különösen az információbiztonsági szabályzat és az ahhoz kapcsolódó eljárásrendek – további szereplőket és felelősségi köröket határoznak meg, amelyek az egyes védelmi intézkedések végrehajtásához közvetlenül kapcsolódnak. E szereplők minőségi feladatellátása szintén csak a megfelelő ismeretek birtokában biztosítható.

A szervezet feladata ezért nem merül ki a szerepkör alapú képzések puszta lebonyolításában. Szükséges valamennyi, a belső szabályozásban meghatározott szerepkör azonosítása, az adott feladatkörökhöz kapcsolódó speciális ismeretek meghatározása, valamint ezen ismeretekhez illeszkedő képzési tartalmak kialakítása. A felkészítés ebben az összefüggésben nem tematikus alapon, hanem szerepkörökhöz rendelten értelmezendő.

A képzések átlátható tervezése és nyomon követhetősége érdekében indokolt, hogy a beazonosított szerepkörök és az azokhoz kapcsolódó képzési tartalmak a szervezet képzési tervében jelenjenek meg, lehetővé téve a szerepkörök későbbi személyi megfeleltetését, valamint azt, hogy a több feladatkörben érintett személyek esetében a szükséges ismeretek összehangolt módon kerüljenek átadásra.

4.1.3 Egyéb – nem a szervezet által lebonyolítandó – kötelező biztonsági képzések

A Kiberbiztonsági tv., illetve az azok végrehajtására kiadott jogszabályok alapján léteznek olyan az informatikai biztonságot szolgáló egyéb képzések, melyek megszervezése nem az érintett szervezet feladata, azonban az azok teljesítését igazoló dokumentumokat evidenciába köteles csatolni. Két releváns rendeletet kell ezzel kapcsolatban ismernie a szervezetnek: egyrészt a már hivatkozott MK rendelet, másrészt pedig a Magyarország kiberbiztonságáról szóló törvény szerinti végzettségekre, szakképzettségekre, valamint képzésekre és továbbképzésekre vonatkozó követelményekről szóló 17/2025. (VII. 24.) EM rendelet (továbbiakban: EM rendelet) alább bemutatott releváns rendelkezéseit.

4.1.3.1 Az MK rendelet szerint egyéb képzés

Az MK rendelet az alábbi védelmi intézkedések esetén elvárja, hogy a magas biztonsági osztályba sorolt szervezet a vele szerződéses kapcsolatban álló egyéb szervezetekkel (beszállító, szolgáltató) szemben követelje meg a nevesített képzés megtartását.

Védelmi intézkedés szerinti tematika	Védelmi intézkedés leírása	Követelmény száma	Biztonsági osztály
Szoftverfejlesztők oktatása (Rendszer- és szolgáltatásbeszerzés)	*A szervezet kötelezi a rendszerfejlesztőt, hogy biztosítson képzést a szoftverfejlesztőknek a megvalósított biztonsági funkciók, szabályozások és mechanizmusok helyes használatáról és működéséről.*	16.86	M
Telekommunikációs szolgáltatások – Szolgáltatói üzletmenet-folytonossági terv (Készenléti Tervezés)	*A szervezet meghatározott gyakorisággal bekéri a szolgáltatóktól a folyamatos működéssel kapcsolatos képzések és tesztelések dokumentációját.*	7.33.3	M

4.1.3.2 Az elektronikus információs rendszer biztonságáért felelős személy továbbképzése

A Kiberbiztonsági tv. 11. § (1) bekezdése alapján a szervezet vezetője köteles az elektronikus információs rendszer biztonságáért felelős személyt (továbbiakban: IBF) alkalmazni, aki feladatait a szervezet munkavállalójaként vagy szerződéses partnerként (szervezeten kívüli személyként) látja el.

A Kiberbiztonsági tv. 11. § (8) bekezdése szerint az IBF a számára előírt továbbképzésen köteles részt venni. A szervezet az IBF kötelező továbbképzésen való részvételét (esetleges munkából való kiesését, munkahelytől való távolmaradását) köteles biztosítani, amennyiben az saját munkavállalója.[6] Függetlenül attól, hogy saját vagy szerződéses IBF-ről van szó, a továbbképzési kötelezettség teljesítésének igazolása a szervezet felelőssége.

Az IBF továbbképzési kötelezettségeinek részleteit a hivatkozott EM rendelet 3. alcíme tartalmazza[7], mely alapján évente összesen legalább 20 órás továbbképzést kell teljesítenie az EM rendelet feltételeinek megfelelő felnőttképző intézmény szervezésében.[8] Az intézmény a továbbképzés elvégzéséről tanúsítványt állít ki.

[6] a Kiberbiztonsági tv. 11. § (5) bekezdés d) pontja

[7] a Kiberbiztonsági tv. 1. § (1) és (2a) bekezdése szerinti szervezetek vonatkozásában kell alkalmazni. – Kiberbiztonsági tv. 1. § (2)

[8] A 2025. december 31-ét megelőzően kinevezett vagy megbízott elektronikus információs rendszer biztonságáért felelős személy a 3. § szerinti továbbképzést első alkalommal 2026. december 31-ig köteles elvégezni. – Kiberbiztonsági tv. 9. § (3)

4.1.3.3 A szervezet vezetőjének képzése és továbbképzése

Az EM rendelet 4. alcíme[9] tárgyalja a szervezet vezetőjével szemben megfogalmazott képzési és továbbképzési kötelezettség részleteit. Az EM rendelet szerint a szervezet vezetője köteles részt venni a szervezet vezetőjévé válását követő egy éven belül egy, összesen legalább 8 órás időtartamban szervezett képzésen[10], valamint ezt követően évente összesen legalább 4 órás időtartamban szervezett továbbképzésen. A képzést lebonyolító felnőttképző intézmény a vezetői képzés, illetve továbbképzés elvégzéséről tanúsítványt állít ki. A vezető EM rendelet szerinti képzési kötelezettségét szintén javasoljuk a szervezet képzési tervébe integrálni.

4.2 Hogyan kell a kiberbiztonsági oktatásokat végrehajtani?

A képzések végrehajtásának részletszabályait a szervezetnél az MK rendelet alapján kialakított tudatossági és képzési szabályzat, illetve a végrehajtását segítő eljárásrend határozza meg. (*3.1.1.1.-3.1.1.2*) Az eljárásrend rögzíti a képzések lebonyolításának kereteit, míg az ütemezés, a célcsoportok és az egyes képzésekhez rendelt érintettek részletes meghatározását célszerű képzési tervbe foglalni, amelyet az eljárásrend mellékleteként javasolt kiadni. E szabályozási felépítés biztosítja, hogy a jogszabályi elvárások a szervezet működésében egységes, nyomon követhető és ellenőrizhető módon jelenjenek meg.

A belső szabályozók kialakításával egyidejűleg a szervezet vezetője kijelöli azt a személyt vagy szervezeti egységet, aki vagy amely a szabályozók karbantartásáért, a képzések megszervezésért, adminisztrálásáért, a képzési terv kezeléséért és megvalósulásának nyomon követéséért felel.

A szervezet által lebonyolítandó általános információbiztonsági tudatossági képzések és a speciális, szerepkör alapú információbiztonsági képzések végrehajtása kapcsán az alábbi közös szabályokat állítja fel a jogalkotó:

- *Dokumentálás és nyomon követés*: a szervezetnek a képzési tevékenységeket igazolható módon dokumentálnia kell, a képzési dokumentumokat pedig meg kell őrizni. (*3.13.1.–3.13.2.*)
- *Kezdeti képzés kötelező életciklus-eseményeknél*:
    - új jogviszony / új felhasználó esetén az általános tudatossági képzést biztosítani kell (*3.2.1.1.*),
    - új feladatkör / hozzáférés engedélyezése előtt, illetve szerepkörbe kerüléskor a szerepkörhöz igazított felkészítést biztosítani kell (*3.9.1.1.*).
- *Rendszeres ismétlőképzés*: mindkét képzéstípusnál elvárás a szervezet által meghatározott rendszerességű ismétlő képzés megtartása, az ismeretek rendszeres felfrissítése, aktualizálása (*3.2.1.1., 3.9.1.1.*).

[9] a Kiberbiztonsági tv. 1. § (1) és (2a) bekezdése szerinti szervezetek vonatkozásában kell alkalmazni. – Kiberbiztonsági tv. 1. § (2)

[10] A szervezet 2025. december 31-ét megelőzően kinevezett vagy megbízott vezetője a 8 órás alapképzést 2026. december 31-ig köteles elvégezni. – Kiberbiztonsági tv. 9. § (4)

- *Eseményvezérelt képzések*: Amikor az EIR változása vagy a szervezet által meghatározott esemény (pl. üzletmenet-folytonossági, eseménykezelési eljárások változása) azt indokolja a szervezet köteles „rendkívüli" képzést szervezni (*3.2.1.2., 3.9.1.2.*).
- *Tanulságok beépítése*: a belső vagy külső biztonsági események tapasztalatait be kell építeni a tananyagokba, és ez jellemzően célzott ismétlő felkészítést is maga után von (*3.2.4., 3.9.3.*).
- *Tartalomkarbantartás*: a tananyagokat meghatározott gyakorisággal és események után a szervezetnek frissíteni kell (3.2.3, 3.9.2).

A fenti közös szabályokon túl az általános információbiztonsági tudatossági és a szerepkör alapú képzések végrehajtása során a szervezetnek lehetősége és egyben felelőssége is, hogy a képzések formáját, módszertanát és mélységét az érintett kockázatok jellegéhez igazítsa.

Az általános tudatossági képzések jellemzően hatékonyan megvalósíthatók online vagy e-learning formában, míg a szerepkör alapú képzések esetében – a konkrét feladat- és felelősségi körökből fakadóan – gyakran az interaktív megközelítés, például műhelymunka, esetfeldolgozás vagy célzott gyakorlati felkészítés járul hozzá hatékonyabban az ismeretek megszerzéséhez.

Mindkét képzéstípus esetében alkalmazható a tudásszint ellenőrzése (pl. teszt, vizsga), azonban a szerepkör alapú képzéseknél jellemzően magasabb elvárás, hogy az érintettek ne csupán az elméleti ismereteket, hanem a szerepkörükhöz kapcsolódó folyamatlépések helyes végrehajtását is igazolni tudják. A gyakorlati és szimulációs elemek alkalmazása ezért az általános tudatossági képzéseknél is megjelenhet – például szimulált biztonsági események formájában (*3.3.*) –, ugyanakkor a szerepkör-alapú képzések esetében különösen indokolt lehet az érintett szereplők együttműködését vizsgáló szimulációk alkalmazása, így például biztonsági eseménykezelési vagy folyamatos működésre felkészítő gyakorlatok keretében[11] (*7.11., 9.3.*).

A képzések végrehajtásával összefüggésben a szervezet felelőssége, hogy a képzési kötelezettségeket a kiváltó eseményekhez – így különösen belépéshez, szerepkörváltozáshoz, szabályozási változásokhoz vagy biztonsági események tapasztalataihoz – rendelje, és a képzések módszertanát, rendszerességét és dokumentálási mélységét a biztonsági osztályhoz, valamint az érintett kockázatok súlyához igazítsa. Ennek megfelelően a képzésekhez kapcsolódó azonos követelmény – például eseményvezérelt ismétlő képzés – alap, jelentős vagy magas biztonsági osztályban eltérő tartalommal, eltérő gyakorlati hangsúllyal és eltérő részletezettségű dokumentálással valósulhat meg

5. FORRÁSOK

- Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény
- A Miniszterelnöki Kabinetirodát vezető miniszter 7/2024. (VI. 24.) MK rendelete a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

[11] magas biztonsági osztálynál kötelező

- a Magyarország kiberbiztonságáról szóló törvény szerinti végzettségekre, szakképzettségekre, valamint képzésekre és továbbképzésekre vonatkozó követelményekről szóló 17/2025. (VII. 24.) EM rendelet