Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Tudatosság és képzés

Verzió 1.2.

NEMZETI KIBERBIZTONSÁGI INTÉZET

2026

Tartalomjegyzék

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.

MAGYARÁZAT

A biztonságtudatossági képzésre vonatkozó szabályzatnak és a kapcsolódó eljárásrend(ek)nek illeszkednie kell az érintett szervezet kockázatkezelési stratégiájához. A megfelelő minőségben és megfelelő szempontok mentén elkészített szabályzatok és eljárásrendek nagy mértékben járulnak hozzá a szervezet biztonságának megőrzéséhez. Az elkészült szabályzatoknak és eljárásrendeknek összhangban kell lenniük egymással és a szervezet információbiztonsági környezetével. A szervezeti szintű biztonsági szabályzatok és eljárásrendek használata általában előnyösebb, hiszen szükségtelenné teheti a különböző szervezeti célok vagy rendszerek szintjén kialakítandó szabályzatokat és eljárásrendeket. A szervezet azonban dönthet úgy (amennyiben a szervezet felépítése ezt indokolja), hogy a szabályzati szinten megjelenő követelményeket egy általános biztonsági szabályzatban [pl.: Információbiztonsági Szabályzat (IBSZ)], vagy

több szabályzatban implementálja, míg az eljárásrendek szintjén megjelenő követelményeket (melyek a szabályzatban foglalt követelményeket részletezik rendszer- és szerepköri szinten) beépítheti a rendszerbiztonsági tervébe, vagy több különböző dokumentumban jeleníti meg azokat. A szervezetnek kiemelt figyelmet kell fordítania mind a szabályzat, mind az eljárásrendek megfelelő frissítésére. A frissítéseket kiváltó események lehetnek értékelésből vagy (felül)vizsgálatból eredő megállapítások, biztonsági események vagy változások a hatályos jogszabályokban, irányelvekben, szabályozásokban, szabványokban és ajánlásokban. A szervezetnek szem előtt kell tartania, hogy az elvárt védelmi intézkedések egyszerű újraközlése nem minősülhet szervezeti szabályzatnak vagy eljárásrendnek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek gondoskodnia kell a biztonságtudatossági képzésre vonatkozó szabályzat és eljárásrendek kidolgozásával, dokumentálásával, jóváhagyásával, kiadásával és megismertetésével kapcsolatos feladatok ellátásáról.
2. A szervezetnek meg kell bizonyosodnia arról, hogy a biztonságtudatossági képzésre vonatkozó szabályzatban foglaltak megfelelnek a szervezetre vonatkozó hatályos jogszabályoknak, irányelveknek, szabályozásoknak, szabványoknak és ajánlásoknak.
3. A szervezetnek - a megfelelő szereplők bevonásával, dokumentált módon - ki kell dolgoznia a vonatkozó szabályzatot és a kapcsolódó eljárásrendeket, és gondoskodnia kell a szabályzat és az eljárásrendek megfelelő kihirdetéséről, valamint az érintett felekkel történő megismertetéséről.
4. A szabályzat és a kapcsolódó eljárásrendek kidolgozásánál a szervezetnek figyelembe kell vennie a rá vonatkozó sajátosságokat. Az elvárt védelmi intézkedések szó szerinti átvétele nem minősül szervezeti szabályzatnak vagy eljárásrendnek.
5. A szervezetnek a gyakorlatban is alkalmaznia kell a biztonságtudatossági képzésre vonatkozó szabályzatban és az ahhoz kapcsolódó eljárásrendekben megfogalmazott elvárásokat, ezáltal biztosítva azok tényleges megvalósulását.
6. A szervezetnek felül kell vizsgálnia és szükség esetén frissítenie kell az aktuális biztonságtudatossági képzésre vonatkozó szabályzatot/szabályokat, illetve a kapcsolódó eljárásrendeket a szervezet által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően.

Kapcsolódó intézkedések

1.10. Kockázatkezelési stratégia

14.12. Fegyelmi intézkedések

18.67. Információ kezelése és megőrzése

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

MSZ ISO/IEC 27001:2023 referencia

5.2; 5.3; 7.5.1; 7.5.2; 7.5.3; A.5.1; A.5.2; A.5.4; A.5.31; A.5.36; A.5.37

NIST SP 800-53 rev.5 referencia

AT-1

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

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.

MAGYARÁZAT

Az érintett szervezet alap- és haladó szintű biztonságtudatossági képzést biztosít a felhasználók számára, mely magában foglalja a felhasználók tudásszintjének mérését is. A szervezet a biztonságtudatossági képzés tartalmát a szervezeti követelmények, a felhasználók által elérhető rendszerek, és a munkakörnyezet alapján (pl.: távmunka) határozzák meg. A képzés tartalma magában foglalja a biztonság szükségességének megértését, a felhasználók által a biztonság fenntartása érdekében megteendő intézkedéseket, valamint a biztonsági eseményekre történő reagálást. A képzés hangsúlyozza a biztonságos működés fontosságát. A biztonságtudatosság erősítésére használt eszközök közé sorolhatjuk a plakátok kihelyezését, a biztonsági emlékeztetőkkel ellátott tárgyak biztosítását, a bejelentkezési képernyőn üzenetek elhelyezését, a szervezet vezetőitől kapott e-mailes figyelmeztetéseket vagy tanácsokat, valamint tudatosító események lebonyolítását.

A kezdeti képzést követően a biztonságtudatossági képzést a szervezetre vonatkozó hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások alapján meghatározott minimális gyakorisággal kell lefolytatni. A későbbi biztonságtudatossági képzés egy vagy több rövid ad hoc képzéssel is teljesíthető és tartalmazhat aktuális információkat a legutóbbi

támadási sémákról, a szervezeti biztonsági irányelvek változásairól, a felülvizsgált biztonsági elvárásokról vagy a kezdeti képzés témaköreinek egyes részeiből. A biztonságtudatossági képzés és a figyelemfelhívó anyagok rendszeres frissítése segít abban, hogy a tartalom releváns maradjon. A biztonságtudatossági képzés tartalmi frissítését kiváltó események többek között lehetnek értékelésből vagy felülvizsgálatból eredő megállapítások, biztonsági események vagy változások a hatályos jogszabályokban, irányelvekben, szabályozásokban, szabványokban és ajánlásokban.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia egy alap- és haladó szintű biztonságtudatossági képzést és azokat meg kell tartania a felhasználók számára, mely magában foglalja a felhasználók tudásszintjének mérését is. A felhasználók alatt a vezetők, felsővezetők és a szervezet szerződéses partnerei is értendők.
2. A szervezetnek a biztonságtudatossági képzés tartalmát a szervezeti követelmények, a felhasználók által elérhető rendszerek, és a munkakörnyezet alapján (pl.: távmunka) kell meghatároznia.
3. A szervezetnek úgy kell kidolgoznia a biztonságtudatossági képzést, hogy az képes legyen megértetni a felhasználókkal a biztonság fontosságát és szükségességét. Emellett tartalmaznia kell, hogy a felhasználóknak milyen intézkedéseket kell megtenniük, hogy elősegítsék a biztonság fenntartását. A képzésnek arra is ki kell térnie, hogy egy felhasználónak hogyan kell reagálnia egy biztonsági eseményre pl.: hová kell bejelentenie a felhasználónak egy általa biztonsági eseménynek vélt történést.
3. A szervezetnek meg kell határoznia, hogy milyen biztonságtudatosságot elősegítő eszközöket fog használni és a gyakorlatban is alkalmaznia kell azokat pl.: plakátok kihelyezése, biztonsági emlékeztetőkkel ellátott tárgyak biztosítása, a bejelentkezési képernyőn üzenetek elhelyezését, a szervezet vezetőitől kapott e-mailes figyelmeztetések vagy tanácsok, valamint biztonságtudatosságot erősítő események lebonyolítása. A biztonságtudatosságot erősítő események közé sorolható egy adathalász kampány szimulálása.
4. A kezdeti képzést követően a szervezetnek a vonatkozó hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások alapján meghatározott minimális gyakorisággal kell lefolytatnia a biztonságtudatossági képzéseket.

5. A kezdeti képzést követő biztonságtudatossági képzés egy vagy több rövid ad hoc képzéssel is teljesíthető és tartalmazhat aktuális információkat a legutóbbi támadási sémákról, a szervezeti biztonsági irányelvek változásairól, a felülvizsgált biztonsági elvárásokról vagy a kezdeti képzés témaköreinek egyes részeiből.

6. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a biztonságtudatossági képzést és a figyelemfelhívó anyagokat annak érdekében, hogy azok tartalma releváns maradjon.

7. A szervezetnek a biztonságtudatossági képzés tartalmát frissítenie kell a meghatározott események bekövetkezését követően pl.: értékelésből vagy felülvizsgálatból eredő megállapítások, biztonsági események, vagy változások a hatályos jogszabályokban, irányelvekben, szabályozásokban, szabványokban és ajánlásokban.

8. A szervezetnek be kell építenie a belső és külső biztonsági eseményekből levont tanulságokat a biztonságtudatossági képzési anyagokba, valamint az alkalmazott biztonságtudatossági eszközrendszerébe.

9. A szervezetnek dokumentálnia kell a biztonságtudatossági képzések lebonyolítását – pl.: jelenléti ívek használata, automatikusan generált részvételi igazolás.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

2.100. Távoli hozzáférés

2.124. Nyilvánosan elérhető tartalom

3.9. Szerepkör alapú biztonsági képzés

3.13. A biztonsági képzésre vonatkozó dokumentációk

7.10. A folyamatos működésre felkészítő képzés

8.14. Azonosító kezelés

9.2. Képzés a biztonsági események kezelésére

9.31. Segítségnyújtás a biztonsági események kezeléséhez

9.35. Információszivárgásra adott válaszlépések

41/2015. (VII. 15.) BM rendeleti referencia

3.1.7.3. Biztonság tudatosság képzés

MSZ ISO/IEC 27001:2023 REFERENCIA

7.3; A.6.3; A.8.7

NIST SP 800-53 REV.5 REFERENCIA

AT-2

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

3.3. BIZTONSÁGTUDATOSSÁGI KÉPZÉS – GYAKORLATI FELADATOK

3.3. A szervezet a felkészítő képzést olyan gyakorlati feladatokkal egészíti ki, amelyek szimulálják a biztonsági eseményeket.

MAGYARÁZAT

A gyakorlati feladatok magukban foglalhatják az előzetes bejelentés nélkül végrehajtott pszichológiai manipuláció, amellyel információt, valamint jogosulatlan hozzáférést lehet szerezni. Emellett gyakorlati feladat lehet még a rosszindulatú e-mail mellékletek megnyitásával, valamint a célzott adathalász támadások által célba juttatott rosszindulatú webhivatkozások megnyitásával járó káros hatások szimulációja.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek gyakorlati feladatokkal kell kiegészítenie a biztonságtudatossági képzést pl.: előzetes bejelentés nélkül végrehajtott pszichológiai manipuláció, adathalász kampány szimulálása.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.2. Biztonsági értékelések

5.14. Folyamatos felügyelet

7.13. Üzletmenet-folytonossági terv tesztelése

9.5. Biztonsági események kezelésének tesztelése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

MSZ ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AT-2(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

3.4. BIZTONSÁGTUDATOSSÁGI KÉPZÉS – BELSŐ FENYEGETÉS

3.4. A szervezet felkészítő képzést nyújt a belső fenyegetések potenciális jeleinek felismerésére és jelentésére.

MAGYARÁZAT

A belső fenyegetések potenciális tünete és lehetséges előjele lehet a szélsőséges és hosszú ideig tartó munkahelyi elégedetlenség, a munkavégzéshez nem szükséges információkhoz való hozzáférési kísérlet, a pénzügyi forrásokhoz történő megmagyarázhatatlan hozzáférési kísérlet, a munkatársak zaklatása vagy bántalmazása, a munkahelyi erőszak és a szabályzatok, eljárások, utasítások, szabályok vagy gyakorlatok súlyos megsértése. A biztonságtudatossági képzésnek tartalmaznia kell, hogy a munkavállalók és a vezetőség hogyan kommunikálhatják az észrevételeiket a belső fenyegetések potenciális jeleivel kapcsolatban. A szervezet erre a célra létesíthet - a meghatározott szabályzatokkal és eljárásrendekkel összhangban - egy kommunikációs csatornát.

A szervezet megfontolhatja a belső fenyegetésekkel kapcsolatos tudatosság témáinak személyre szabását az érintettek szerepköre szerint. Például a vezetőknek szóló képzés a beosztottak viselkedésének változásaira összpontosíthat, míg az alkalmazottaknak szóló képzés általánosabb megfigyelésekre összpontosíthat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek tisztában kell lennie azzal, hogy mi a belső fenyegetés és mik lehetnek annak potenciális jelei, illetve mindez milyen veszélyekkel járhat a szervezet egészére nézve.
2. A szervezetnek törekednie kell a belső fenyegetések potenciális jeleinek felismerésére és meg kell tennie a szükséges intézkedéseket, melyekkel igyekszik csökkenteni a fenyegetés mértékét vagy megszüntetni azt.
3. A szervezetnek a biztonságtudatossági képzés keretében foglalkoznia kell a belső fenyegetéssel. A képzésnek tartalmaznia kell, hogy mi számít belső fenyegetésnek, mik lehetnek a belső fenyegetés potenciális jelei. Emellett a képzésben szerepelnie kell annak, hogy a munkavállalók milyen kommunikációs csatornán keresztül jelezhetik, amennyiben belső fenyegetésére utaló történést érzékelnek.

4. A szervezet a belső fenyegetéssel kapcsolatos tudnivalók oktatását megvalósíthatja személyre szabottan is, az érintettek szerepköre szerint. Például a vezetőknek szóló képzés a beosztottak viselkedésének változásaira összpontosíthat, míg az alkalmazottaknak szóló képzés általánosabb megfigyelésekre összpontosíthat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

1.13. Belső fenyegetés elleni program

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.1.7.4. Belső fenyegetés: A biztonságtudatossági képzésaz érintett személyeket készítse fel a belső fenyegetések felismerésére, és tudatosítsa jelentési kötelezettségüket.

MSZ ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AT-2(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

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.

MAGYARÁZAT

A pszichológiai manipuláció egy kísérlet arra, hogy egy személy átverés által információt fedjen fel vagy olyan tevékenységet hajtson végre, ami adatszivárgást, kompromittálódást vagy egyéb negatív hatást gyakorol egy EIR-re. A pszichológiai manipuláció magában foglalja az adathalászatot, a nyílt információ felhasználásával végrehajtott megszemélyesítést (pretexting), a megszemélyesítést, a csalizást (baiting), az ajándékozást bejelentkezési adatokért cserébe (quid pro quo), a témaeltérítést (thread-jacking), a közösségi média oldalakon található információk kártékony célra történő felhasználását (social media exploitation) és a szoros követést (tailgating). Az adatgyűjtés (social mining) egy kísérlet arra, hogy a szervezetről olyan információ kerüljön összegyűjtésre, amit egy jövőbeni lehetséges támadás során fel lehet használni. A biztonságtudatossági képzésnek tartalmaznia kell, hogy a munkavállalók és a vezetőség hogyan kommunikálhatják az észrevételeiket a pszichológiai manipuláció és az adatgyűjtés potenciális jeleivel kapcsolatban. A szervezet erre a célra létesíthet - a meghatározott szabályzatokkal és eljárásrendekkel összhangban - egy kommunikációs csatornát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek tisztában kell lennie azzal, hogy mi a pszichológiai manipuláció és az adatgyűjtés, illetve azzal is, hogy mindez milyen veszélyekkel járhat a szervezet egészére nézve.
2. A szervezetnek törekednie kell a pszichológiai manipuláció potenciális jeleinek felismerésére és meg kell tennie a szükséges intézkedéseket, melyekkel igyekszik csökkenteni a fenyegetés mértékét.
3. A szervezetnek a biztonságtudatossági képzés keretében foglalkoznia kell a pszichológiai manipulációval és az adatgyűjtéssel. A képzésnek tartalmaznia kell, hogy mi számít

pszichológiai manipulációnak és adatgyűjtésnek, mik lehetnek azok potenciális jelei. Illetve a képzésben arra is ki kell térni, hogy hogyan lehet ezen támadási formák ellen védekezni. Emellett a képzésben szerepelnie kell annak, hogy a munkavállalók milyen kommunikációs csatornán keresztül jelezhetik, amennyiben pszichológiai manipulációra vagy adatgyűjtésre utaló történést érzékelnek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

MSZ ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AT-2(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

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.

MAGYARÁZAT

A jól képzett munkaerő preventív védelmi funkciót is betölthet, amely a mélységi védelmi stratégia részeként alkalmazva megakadályozhat egy, a szervezetbe e-mailen vagy webes alkalmazásokon keresztül beküldött kártékony kód segítségével végrehajtott támadást. A munkatársak a képzésen elsajátított információk alapján képesek észlelni a potenciálisan gyanús e-mailekre utaló jeleket. A képzés arra is megtanítja a munkatársakat, hogy miképpen reagáljanak a gyanús e-mail üzenetekre, illetve az Internet irányából érkező gyanús kommunikációra. Ahhoz, hogy ez a folyamat hatékonyan működjön, a munkatársak a képzés során megismerik, hogy mi számít gyanús kommunikációnak. A munkatársak képzése a rendszerek rendellenes viselkedésének felismerésére segítheti a szervezetet abban, hogy már korai szakaszban értesülhessen egy rosszindulatú kód jelenlétéről. A rendellenes viselkedés munkatársak általi felismerése elősegítheti a rosszindulatú kódok észlelését, illetve kiegészíti a szervezetek által alkalmazott védelmi eszközöket és rendszereket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek tisztában kell lennie azzal, hogy mi számíthat gyanús kommunikációnak és szokatlan rendszerviselkedésnek, illetve azzal is, hogy mindez milyen veszélyekkel járhat a szervezet egészére nézve.
2. A szervezetnek törekednie kell a gyanús kommunikáció és a szokatlan rendszerviselkedés jeleinek felismerésére - pl.: gyanús e-mail-ek, melyek helyesírási hibával tűzdeltek, nem ismert domain címről érkeztek és sürgetnek egy bizonyos tevékenység végrehajtására - és meg kell tennie a szükséges intézkedéseket, melyekkel igyekszik csökkenteni a fenyegetés mértékét.
3. A szervezetnek a biztonságtudatossági képzés keretében foglalkoznia kell a gyanús kommunikációval és szokatlan rendszerviselkedéssel. A képzésnek tartalmaznia kell, hogy mi számít gyanús kommunikációnak és rendszerviselkedésnek, mik lehetnek azok potenciális jelei.

Illetve a képzésbe arra is ki kell térni, hogy hogyan lehet az említett jelenségek ellen védekezni. Emellett a képzésben szerepelnie kell annak, hogy a munkavállalók milyen kommunikációs csatornán keresztül jelezhetik, amennyiben gyanús kommunikációra és szokatlan rendszerviselkedésre utaló történést érzékelnek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

MSZ ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AT-2(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kártékony kódra utaló jelek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

3.7. BIZTONSÁGTUDATOSSÁGI KÉPZÉS – TARTÓS FEJLETT FENYEGETÉSEK

3.7. A szervezet felkészítő képzést nyújt a tartós fejlett fenyegetések (APT) felismerésére és kezelésére vonatkozóan.

MAGYARÁZAT

A tartós fejlett fenyegetések (APT) észlelésének és a sikeres támadások megelőzésének hatékony módja az egyének számára biztosított, specifikus biztonságtudatossági képzés. A fenyegetésekkel kapcsolatos biztonságtudatossági képzés magában foglalja az egyének oktatását az APT-k szervezetbe való beszivárgásának különböző módjairól (pl. weboldalakon, e-maileken, felugró ablakokon, cikkeken és pszichológiai manipuláción keresztül). A hatékony képzés tartalmazza a gyanús e-mailek felismerésének technikáit, a hordozható eszközök nem biztonságos környezetben történő használatát, valamint az egyének otthoni célba vételének lehetőségét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek tisztában kell lennie azzal, hogy mit jelent a tartós fejlett fenyegetés (APT), illetve azzal is, hogy a fenyegetés milyen veszélyekkel járhat a szervezet egészére nézve.
2. A szervezetnek törekednie kell a tartós fejlett fenyegetés (APT) jeleinek felismerésére és meg kell tennie a szükséges intézkedéseket, melyekkel igyekszik csökkenteni a fenyegetés mértékét.
3. A szervezetnek a biztonságtudatossági képzés keretében foglalkoznia kell a tartós fejlett fenyegetésekkel (APT). A képzésnek tartalmaznia kell, hogy mi számít tartós fejlett fenyegetésnek (APT), mik lehetnek annak potenciális jelei. Illetve a képzésbe arra is ki kell térni, hogy hogyan lehet az említett fenyegetés ellen védekezni. Emellett a képzésben szerepelnie kell annak, hogy a munkavállalók milyen kommunikációs csatornán keresztül jelezhetik, amennyiben tartós fejlett fenyegetésre (APT) utaló történést érzékelnek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

MSZ ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AT-2(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

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.

MAGYARÁZAT

Mivel a kiberfenyegetések az idő múlásával folyamatosan változnak, a kiberfenyegetési környezet bemutatásáról szóló szervezeti képzést is frissen kell tartani. Emellett a kiberfenyegetésekkel kapcsolatos ismeretek oktatását nem szabad a szervezeti küldetést és az üzleti funkciókat támogató rendszerműveletektől elszigetelten végezni.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek tisztában kell lennie azzal, hogy milyen kiberfenyegetési környezetben működik, amihez a szervezetnek figyelemmel kell kísérnie az aktuális kiberfenyegetési tendenciákat.
2. A szervezetnek a biztonságtudatossági képzés keretében be kell mutatnia a kiberfenyegetési környezetet a munkavállalók számára.
3. A szervezetnek rendszeresen aktualizálnia kell a biztonságtudatossági képzés tananyagát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

15.4. Kockázatelemzés

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

MSZ ISO/IEC 27001:2023 REFERENCIA

7.3, A.6.3, A.8.7

NIST SP 800-53 REV.5 REFERENCIA

AT-2(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

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.

MAGYARÁZAT

Az érintett szervezet a képzés tartalmát az egyének által betöltött szerepkörök és felelősségek, valamint a szervezet biztonsági követelményei alapján határozza meg, beleértve a személyzetnek az EIR-hez való hozzáférését is, amely speciálisan az adott feladatokra szabott technikai képzést tartalmaz. A szerepköralapú képzést igénylő szerepek közé tartoznak a vezetők vagy a menedzsment tagjai, EIR tulajdonosok; engedélyező tisztviselők; biztonsági tisztviselők; adatvédelmi tisztviselők; beszerzési tisztviselők; rendszer tervezőmérnökök; rendszermérnökök; szoftverfejlesztők; biztonsági mérnökök; rendszer-, hálózati és adatbázis-adminisztrátorok; központi naplózás adminisztrátorai; konfigurációkezelési tevékenységeket végző személyek; ellenőrzési tevékenységeket végző személyek; rendszerszintű szoftverhez hozzáféréssel rendelkező személyek; vészhelyzeti és biztonsági eseménykezelési feladatokat ellátó személyek; adatvédelmi feladatokat ellátó személyek; és személyes adatokhoz hozzáféréssel rendelkező személyek.

A szerepköralapú képzés átfogóan kezeli a menedzsment, az operatív és a technikai szerepeket és felelősségeket, beleértve a fizikai, személyi és technikai ellenőrzéseket. A szerepköralapú képzés magában foglalja a biztonsági szerepekre vonatkozó szabályokat, eljárásokat, eszközöket, módszereket és dokumentumokat. A szervezet a szükséges képzést biztosítja az egyének számára, hogy képesek legyenek ellátni az operatív és ellátási lánc kockázatkezelési feladataikat a szervezet biztonsági elvárásainak megfelelően. A képzés típusai közé tartozik a

web-alapú- és számítógépes képzés, a dedikált helyiségben megtartott képzés és a gyakorlati képzés is. A szerepköralapú képzés rendszeres frissítése segít annak biztosításában, hogy a képzés tartalma továbbra is releváns és hatékony maradjon. A szerepkör alapú biztonságtudatossági képzés tartalmi frissítését kiváltó események többek között lehetnek értékelésből vagy felülvizsgálatból eredő megállapítások, biztonsági események vagy változások a hatályos jogszabályokban, irányelvekben, szabályozásokban, szabványokban és ajánlásokban.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek szerepkör alapú biztonsági képzést kell biztosítania a felhasználóknak. A képzés tartalmát az egyének által betöltött szerepkörök és felelősségek, valamint az érintett szervezet biztonsági követelményei határozzák meg.
2. A kezdeti képzést követően a szervezetnek a vonatkozó hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások alapján meghatározott minimális gyakorisággal kell lefolytatnia a biztonságtudatossági képzéseket.
3. A képzésnek meg kell előznie az EIR-hez vagy az információhoz való hozzáférés biztosítását, vagy a kijelölt feladat végrehajtását. A képzést rendszeresen, az érintett szervezet által meghatározott gyakorisággal meg kell ismételni.
4. A szervezetnek rendszeresen, illetve az érintett szervezet által meghatározott események bekövetkezése után is frissítenie kell a szerepköralapú képzés tartalmát.
5. A szervezetnek be kell építenie a belső vagy külső biztonsági eseményekből levont tanulságokat a szerepköralapú biztonsági képzésekbe.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése
2.100. Távoli hozzáférés
2.124. Nyilvánosan elérhető tartalom
3.2. Biztonságtudatossági képzés
3.13. A biztonsági képzésre vonatkozó dokumentációk
7.10. A folyamatos működésre felkészítő képzés
9.2. Képzés a biztonsági események kezelésére
9.9.1. Biztonsági események kezelése

9.31. Segítségnyújtás a biztonsági események kezeléséhez

9.35. Információszivárgásra adott válaszlépések

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.1.7.5. Szerepkör, vagy feladat alapú biztonsági képzés

MSZ ISO/IEC 27001:2023 REFERENCIA

A.6.3

NIST SP 800-53 REV.5 REFERENCIA

AT-3

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

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.

Magyarázat

A környezeti védelmi intézkedések közé tartoznak a tűzoltó és tűzérzékelő berendezések vagy rendszerek, a sprinkler rendszerek, a kézi tűzoltó készülékek, rögzített tűzoltó tömlők, füstérzékelők, a hőmérséklet vagy páratartalom mérők, illetve a fűtés, szellőzés, légkondicionálás és energiaellátás a létesítményen belül.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, hogy mely személyek vagy szerepkörök felelnek a környezethez kapcsolódó biztonsági követelmények alkalmazásáért és működtetéséért.
2. A szervezetnek ki kell dolgoznia egy olyan szerepkör alapú képzést, mely a környezethez kapcsolódó biztonsági követelmények alkalmazását és működtetésével kapcsolatos tudnivalókat foglalja magában.
3. A kezdeti képzést követően a szervezetnek a vonatkozó hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások alapján meghatározott minimális gyakorisággal kell lefolytatnia a környezeti védelmi intézkedésekre vonatkozó szerepkör alapú biztonságtudatossági képzést.

Kapcsolódó intézkedések

12.1. Szabályzat és eljárásrendek
12.28. Vészhelyzeti tápellátás
12.33. Tűzvédelem
12.37. Környezeti védelmi intézkedések
12.40. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

MSZ ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AT-3(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök, illetve a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

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.

MAGYARÁZAT

A fizikai védelmi intézkedések magukban foglalják a fizikai hozzáférés-ellenőrző eszközöket, a fizikai behatolásjelző és behatolásérzékelő riasztókat, a létesítmény biztonsági őreinek működési eljárásrendjeit, valamint a megfigyelő vagy felügyeleti berendezéseket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely személyek vagy szerepkörök felelnek a fizikai biztonsági követelményekből fakadó védelmi intézkedések alkalmazásáért és működtetéséért.
2. A szervezetnek ki kell dolgoznia egy olyan szerepkör alapú képzést, mely a fizikai biztonsági követelmények alkalmazását és működtetésével kapcsolatos tudnivalókat foglalja magában.
3. A kezdeti képzést követően a szervezetnek a vonatkozó hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások alapján meghatározott minimális gyakorisággal kell lefolytatnia a fizikai védelmi intézkedésekre vonatkozó szerepkör alapú biztonságtudatossági képzést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

12.2. A fizikai belépési engedélyek

12.6. A fizikai belépés ellenőrzése

12.14. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

MSZ ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AT-3(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök, illetve a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

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.

Magyarázat

A szerepköralapú biztonságtudatossági képzés gyakorlati feladatai közé tartozik a szoftverfejlesztőknek szóló képzés, amely olyan támadásokat szimulál, melyek során a szoftverek gyakran előforduló sérülékenységeit használják ki. Szintén a gyakorlati feladatok közé sorolható, mikor a vezetőket vagy felsővezetőket veszik célba célzott adathalász szimulációs támadásokkal (spear/whale phishing).

A követelmény alkalmazásának lépései

1. A szervezetnek gyakorlati feladatokkal kell kiegészítenie a biztonságtudatossági képzést pl.: szoftverfejlesztőknek szóló képzés, amely során szoftverek gyakran előforduló sérülékenységeit használják ki, illetve adathalász kampány szimulálása vezetők vagy felsővezetők számára.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

MSZ ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AT-3(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

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.

MAGYARÁZAT

A szervezet dokumentálja és nyomon követi az általános- és a szerepkör alapú biztonságtudatossági képzéseket. A dokumentálás magában foglalhatja magát a képzési anyagot, illetve a képzés lebonyolításával kapcsolatos egyéb dokumentációkat is pl.: jelenléti ívek használata, automatikusan generált részvételi igazolás. A szervezet a vonatkozó hatályos jogszabályokat, irányelveket, szabályozásokat, szabványokat és ajánlásokat figyelembe véve meghatározott ideig megőrzi a képzésről készült dokumentumokat.

Az érintett szervezet dokumentálja és nyomon követi az információbiztonsági képzési tevékenységeket. Az érintett szervezet számára fontos, hogy a képzési tevékenységek dokumentálása és nyomon követése segítse a szervezetet abban, hogy biztosítsa a személyzet megfelelő képzését és felkészültségét az információbiztonsági kihívások kezelésére.

A dokumentáció megőrzése lehetővé teszi az érintett szervezet számára, hogy bizonyítékot szolgáltasson a képzési tevékenységekről, és hogy értékelje a képzési programok hatékonyságát.

Az érintett szervezet meghatározott ideig megőrzi a képzésről készült dokumentumokat. A megőrzés időtartama a szervezet belső szabályaitól és a vonatkozó jogszabályi követelményektől függ.

Az érintett szervezet a képzési tevékenységek dokumentálásának és nyomon követésének hatékonyabbá tételére EIR-t vehet igénybe, ami lehetővé teszi a képzési tevékenységek adatainak centralizált tárolását és könnyű hozzáférhetőségét, illetve az anyagokkal kapcsolatos tevékenységek nyomon követését.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek dokumentálnia kell és egyúttal nyomon kell követnie az általános- és a szerepkör alapú biztonságtudatossági képzéseket. A dokumentálás magában foglalhatja magát a képzési anyagot, illetve a képzés lebonyolításával kapcsolatos egyéb dokumentációkat is pl.: jelenléti ívek használata, automatikusan generált részvételi igazolás.
2. A szervezetnek a vonatkozó hatályos jogszabályokat, irányelveket, szabályozásokat, szabványokat és ajánlásokat figyelembe véve meghatározott ideig meg kell őriznie a képzésről készült dokumentumokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

3.2. Biztonságtudatossági képzés

3.9. Szerepkör alapú biztonsági képzés

7.10. A folyamatos működésre felkészítő képzés

9.2. Képzés a biztonsági események kezelésére

1.15. Tesztelés, képzés és felügyelet

18.67. Információ kezelése és megőrzése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.1.7.6. A biztonsági képzésre vonatkozó dokumentációk

MSZ ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AT-4

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

3.14. KÉPZÉS EREDMÉNYEIRŐL VALÓ VISSZAJELZÉS

3.14. A szervezet rendszeresen visszajelzést ad a meghatározott személyeknek a szervezeti képzések eredményeiről.

MAGYARÁZAT

A szervezeti képzések eredményeiről adott visszajelzés magában foglalja a biztonságtudatossági- és szerepkör alapú biztonsági képzések eredményeit. A képzési eredmények potenciálisan súlyos problémát is jelezhetnek, különösen akkor, ha a kritikus szerepkörökben dolgozó munkavállalók sikertelen eredményeket produkálnak. Ezért fontos, hogy a felsővezetők tudomást szerezzenek az ilyen helyzetekről, így megfelelő válaszlépéseket tehetnek. A képzések eredményeiről adott visszajelzés támogatja a szervezeti képzés értékelését és szükség szerinti frissítését. A biztonságtudatossági képzés frissítésével kapcsolatos követelmények a "Biztonságtudatossági képzés" és a "Szerepkör alapú biztonsági képzés" kontrolloknál kerültek bővebben kifejtésre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell vezetnie egy eljárást, amely lehetővé teszi a képzési eredmények rendszeres összegyűjtését és elemzését. Ez magában foglalhatja a képzési tesztek eredményeit, illetve a résztvevők visszajelzéseit.

3. A szervezetnek meg kell határoznia, hogy hogyan és milyen formában kommunikálja a képzés eredményeit a résztvevők felé pl.: a résztvevők számára elérhető összefoglaló a szervezet intranet felületén, online képzési rendszer esetén egy rendszer által készített összefoglalás az eredményről.

4. A szervezetnek meg kell határoznia, hogy milyen lépéseket tehet meg a képzési eredmények függvényében. Ha például a képzési eredmények azt mutatják, hogy a munkavállalók nincsenek tisztában teljes mértékben a biztonsági előírásokkal és nem tudják a gyakorlatban alkalmaznia azokat, akkor a szervezetnek meg kell hoznia a szükséges intézkedéseket pl.: képzési anyagok felülvizsgálata és frissítése.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

MSZ ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AT-6

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság, illetve a személyek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERBIZTONSÁGI
INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2026