Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Programmenedzsment

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

1.1. INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

1.1. A szervezet:

1.1.1. kidolgozza és kihirdeti az információbiztonsági szabályzatot, amely:

1.1.1.1. - átfogó képet nyújt a biztonsági követelményekről, valamint a követelményeknek való megfelelés érdekében a szervezet által működtetett, vagy bevezetni kívánt védelmi intézkedésekről.

1.1.1.2. - meghatározza a célkitűzéseket, a ható- és szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat.

1.1.1.3. - leírja az információbiztonságért felelős szervezeti egységek közötti együttműködést.

1.1.1.4. - a szervezet vezetője által kerül jóváhagyásra, aki felelősséget vállal és elszámoltatható a szervezeti műveletek (beleértve a célkitűzéseket, funkciókat, imázst és hírnevet), a szervezeti eszközök, személyek, más szervezetek szempontjából számottevőnek tartott kockázatokért.

1.1.2. Felülvizsgálja és frissíti az információbiztonsági szabályzatot a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

1.1.3. Gondoskodik arról, hogy az információbiztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.

MAGYARÁZAT

Az információbiztonsági szabályzat egy szervezeti szintű dokumentum, amely átfogó képet nyújt az érintett szervezet információbiztonsági követelményeiről. Leírja az egész szervezetre érvényes biztonsági szabályokat és követelményeket, amelyek az egész szervezeten belül kötelező érvényűek. Az információbiztonsági szabályzat lehet egyetlen dokumentum vagy dokumentumok gyűjteménye is. A szabályzat elegendő információt nyújt a biztonsági követelményekről, hogy lehetővé tegye a szabályzat szándékával egyértelműen összhangban lévő megvalósítást. Az információbiztonsági szabályzat frissítései során az érintett szervezet reagál a szervezetben bekövetkezett változásokra, valamint a szabályzatban foglaltak végrehajtása és a (felül)vizsgálatok során azonosított problémákra. A meghatározott biztonsági követelményeket végre kell hajtani szervezeti szinten, valamint az üzleti folyamatok szintjén, továbbá elengedhetetlenek a szervezet információbiztonsági céljainak kezeléséhez és eléréséhez. Az egyes EIR-ekhez tartozó rendszerbiztonsági tervek és az érintett szervezet

információbiztonsági szabályzatnak együtt teljes képet kell nyújtaniuk a szervezetben alkalmazott biztonsági követelményekről és megvalósított védelmi intézkedésekről. Amennyiben ez szükséges, az információbiztonsági szabályzat hivatkozik a különálló rendszerbiztonsági tervekre vagy eljárásrendekre, amelyek tartalmazzák az alacsonyabb szintű rendelkezéseket. Az információbiztonsági szabályzat frissítését kiváltó események lehetnek értékelésből vagy (felül)vizsgálatból eredő megállapítások, biztonsági események vagy változások a hatályos jogszabályokban, irányelvekben, szabályozásokban, szabványokban és ajánlásokban. Az elvárt védelmi intézkedések egyszerű újraközlése nem minősülhet szervezeti szabályzatnak vagy eljárásrendnek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek - a megfelelő szereplők bevonásával, dokumentált módon - ki kell dolgoznia egy információbiztonsági szabályzatot, amely átfogó képet nyújt a szervezet biztonsági követelményeiről és ezek alapján bevezetett vagy bevezetni kívánt védelmi intézkedésekről. Ez a szabályzat meghatározza a szervezet biztonsági célkitűzéseit, a hatályát, szerep- és felelősségi köröket, a vezetői elkötelezettséget, a szervezeten belüli és kívüli együttműködés kereteit, valamint a megfelelőségi kritériumokat.
2. A szervezetnek meg kell bizonyosodnia arról, hogy az információbiztonsági szabályzatban foglaltak megfelelnek a szervezetre vonatkozó hatályos jogszabályoknak, irányelveknek, szabályozásoknak, szabványoknak és ajánlásoknak. Az elvárt védelmi intézkedések egyszerű újraközlése nem minősülhet elfogadható információbiztonsági szabályzatnak.
3. A szervezet vezetőjének jóvá kell hagynia a szabályzatot, és felelősséget kell vállalnia a szervezeti tevékenységekért, a szervezeti eszközökért, a szervezethez köthető személyekért, a más szervezetek szempontjából számottevőnek tartott kockázatokért.
4. A szervezetnek gondoskodnia kell az információbiztonsági szabályzat megfelelő kihirdetéséről, valamint az érintett felekkel történő megismertetéséről.
5. A szervezetnek a gyakorlatban is alkalmaznia kell az információbiztonsági szabályzatban megfogalmazott elvárásokat, ezáltal biztosítva azok tényleges megvalósulását.
6. A szervezetnek gondoskodnia kell arról, hogy az informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető. Az információbiztonsági szabályzat

módosítására csupán az erre jogosultsággal rendelkező személyeknek, dokumentált módon van lehetősége.

7. A szervezetnek felül kell vizsgálnia és szükség esetén frissítenie kell az aktuális információbiztonsági szabályzatot a szervezet által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.1.1.1. Informatikai biztonsági szabályzat

ISO/IEC 27001:2023 REFERENCIA

4.1; 4.2; 4.3; 4.4; 5.2; 5.3; 6.1.1; 6.2; 7.4; 7.5.1; 7.5.2; 7.5.3; 8.1; 9.3.1; 10.1; A.5.1; A.5.2; A.5.4; A.5.31; A.5.36

NIST SP 800-53 REV.5 REFERENCIA

PM-1

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

1.2. ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGÁÉRT FELELŐS SZEMÉLY

1.2. A szervezet vezetője a jogszabályi követelményeknek megfelelő, az elektronikus információs rendszerek biztonságáért felelős személyt nevez ki a szervezeti szintű információbiztonsági szabályzatnak való megfelelés koordinálására, fejlesztésére, bevezetésére és fenntartására és biztosítja számára a célok eléréséhez szükséges erőforrásokat.

MAGYARÁZAT

Az érintett szervezet vezetője a jogszabályi követelményeknek megfelelően nevezi ki az EIR biztonságáért felelős személyt. Ez a személy felelős az érintett szervezet szintű információbiztonsági szabályzatnak való megfelelés koordinálásáért, fejlesztéséért, bevezetéséért és fenntartásáért. Az érintett szervezet vezetője biztosítja számára a célok eléréséhez szükséges erőforrásokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet vezetője kijelöl egy személyt, aki felelős lesz az elektronikus információs rendszerek biztonságáért. Ennek a személynek függetlennek kell lennie (pl. nem lehet egy személyben az informatikai vagy más vezető).
2. A szervezet vezetője biztosítja, hogy a kijelölt személy rendelkezzen a célok eléréséhez szükséges erőforrásokkal. Ez magában foglalhatja a megfelelő képzést, eszközöket, technológiát és támogató személyzetet.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.1.1.2. Az elektronikus információs rendszerek biztonságáért felelős személy

ISO/IEC 27001:2023 REFERENCIA

5.1; 5.3; A.5.2

NIST SP 800-53 REV.5 REFERENCIA

PM-2

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

1.3. INFORMÁCIÓBIZTONSÁGOT ÉRINTŐ ERŐFORRÁSOK

1.3. A szervezet:

1.3.1. Beépíti az információbiztonsági célok végrehajtásához és fejlesztéséhez szükséges erőforrásokat az éves költségvetés tervezésébe és beruházási kérelmeibe, valamint dokumentál minden olyan esetet, amelyek e követelmény alól kivételt képeznek.

1.3.2. Gondoskodik arról, hogy a szükséges dokumentáció összhangban legyen a hatályos törvényekkel, végrehajtási rendeletekkel, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.

1.3.3. Biztosítja az információbiztonsági célok végrehajtásához és fejlesztéséhez tervezett forrásokat.

MAGYARÁZAT

A szervezetek fontolóra vehetik egy információbiztonságért felelős szakértői csoport létrehozását, amelybe a szükséges erőforrások bevonásának részeként speciális szakértelemmel rendelkező személyeket vonnak be. A szervezetek kijelölhetnek és felhatalmazhatnak egy beruházási felülvizsgálati bizottságot vagy hasonló csoportot, hogy irányítsa és felügyelje a beruházástervezési és -ellenőrzési folyamat információbiztonsági szempontjait.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell fontolnia, hogy olyan speciális szakértelemmel és szakmai elhivatottsággal rendelkező felelős(ök)et [ún. "security champion"] nevez ki az információbiztonság területére, és a szükséges erőforrások bevonásának részeként biztosítja számára/számukra a szükséges jogköröket és erőforrásokat.

2. A szervezet kijelölhet és felhatalmazhat egy, a beruházások felülvizsgálatáért felelős csoportot, hogy kezelje és felügyelje az információbiztonsági szempontokat a költségvetés tervezési és ellenőrzési folyamatában.

3. A szervezet gondoskodik arról, hogy a szükséges dokumentáció összhangban legyen a hatályos törvényekkel, végrehajtási rendeletekkel, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. Ez magában foglalja az EIR biztonsági szabályzatainak, eljárásrendjeinek, eljárásainak dokumentálását, valamint a kivételek dokumentálását és naplózását.

4. A szervezet biztosítja az információbiztonsági célok végrehajtásához és fejlesztéséhez tervezett forrásokat. Ez magában foglalja a szükséges anyagi források biztosítását, valamint a szükséges személyi és technikai erőforrások biztosítását. Az érintett szervezetnek biztosítania kell, hogy ezek az erőforrások beépüljenek az éves költségvetés tervezésébe és beruházási kérelmeibe.

Kapcsolódó intézkedések

1.4. Intézkedési terv és mérföldkövei

16.2. Erőforrások rendelkezésre állása

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

5.1; 6.2; 7.1

NIST SP 800-53 rev.5 referencia

PM-3

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

1.4. INTÉZKEDÉSI TERV ÉS MÉRFÖLDKÖVEI

1.4. A szervezet:

1.4.1. Bevezet egy folyamatot, amely biztosítja, hogy az információbiztonság és az ellátási lánc kockázatkezelése, valamint a kapcsolódó szervezeti elektronikus információs rendszerek (a továbbiakban: EIR-ek) intézkedési tervei:

1.4.1.1. - ki legyenek dolgozva és karban legyenek tartva;

1.4.1.2. - dokumentálják a helyreállító információbiztonsági és ellátási lánc kockázatkezelési intézkedéseket, hogy megfelelően reagáljanak a szervezeti műveletek és eszközök, személyek, más szervezetek kockázataira;

1.4.1.3. - a meghatározott jelentési követelmények bemutatásra kerüljenek.

1.4.2. Áttekinti az intézkedési terveket és mérföldköveket, hogy azok összhangban állnak-e a szervezeti kockázatmenedzsment stratégiával és a kockázatkezelési intézkedések szervezeti szintű prioritásaival.

MAGYARÁZAT

Az intézkedési terv és a mérföldkövei kulcsfontosságú szervezeti dokumentum, amelyet a vezetőség felé jelenteni kell. A szervezetek intézkedési terveket és mérföldköveket dolgoznak ki az egész szervezetre kiterjedően, a priorizált kockázatkezelési intézkedésekkel, biztosítva az összhangot a szervezet céljaival és célkitűzéseivel. Az intézkedési terv és a mérföldköveinek frissítése a végrehajtott intézkedések értékelése és a folyamatos monitoring tevékenység alapján történik. Több intézkedési terv is létezhet egyszerre, az EIR-nek, az üzleti folyamatnak és a szervezet összetettségének megfelelően.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell vezetnie egy folyamatot, amely biztosítja, hogy az információbiztonsági és ellátási lánc kockázatkezelési intézkedések, valamint az EIR-ek intézkedési tervei kidolgozásra és karbantartásra kerüljenek.
2. A szervezetnek dokumentálnia kell a helyreállító információbiztonsági és ellátási lánc kockázatkezelési intézkedéseket, hogy megfelelően reagálhasson a szervezet műveleteinek és eszközeinek, személyeknek, más szervezeteknek a kockázataira.

3. A szervezetnek be kell tartania a meghatározott jelentési követelményeket, hogy megfeleljen a szabályozási előírásoknak.
4. A szervezetnek át kell tekintenie az intézkedési terveket és mérföldköveket, hogy biztosítsa, hogy azok összhangban vannak a szervezet kockázatkezelési stratégiájával és a kockázatkezelési intézkedések szervezeti szintű prioritásaival.
5. A szervezetnek dokumentálnia kell az összes lépést és intézkedést, hogy biztosítsa a folyamat átláthatóságát és nyomon követhetőségét.

Kapcsolódó intézkedések

5.9. Az intézkedési terv és mérföldkövei
5.14. Folyamatos felügyelet
1.3. Információbiztonságot érintő erőforrások
15.20. Kockázatokra adott válasz
18.67. Információ kezelése és megőrzése

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

3.1.1.3. Az intézkedési terv és mérföldkövei

ISO/IEC 27001:2023 referencia

6.1.1; 6.2; 7.5.1; 7.5.2; 7.5.3; 8.3; 9.3.2; 10.2

NIST SP 800-53 rev.5 referencia

PM-4

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

1.5. Elektronikus információs rendszerek nyilvántartása

1.5. A szervezet létrehozza és a szervezet EIR-jeiben bekövetkezett változások (pl.: új rendszer bevezetése, meglévő rendszer kivezetése) esetén frissíti, valamint a szervezet által meghatározott gyakorisággal felülvizsgálja az EIR-ek nyilvántartását.

Magyarázat

Az érintett szervezetnek létre kell hoznia egy listát vagy adatbázist, amelyben nyomon követi az összes elektronikus információs rendszerének (EIR) rendszerelemeit és összetevőit. Ez magában foglalja a szoftvereket, hardvereket, hálózati infrastruktúrát és egyéb technológiai eszközöket.

Az EIR-ek nyilvántartása rendkívül fontos a szervezet számára, mivel segít azonosítani, hogy mely rendszerek fontosak az üzletmenet szempontjából, lehetővé teszi, hogy a szervezet nyomon követhesse a rendszerek jelenlegi állapotát, beleértve a frissítéseket, konfigurációkat és egyéb változásokat, segít a szervezetnek felmérni a rendszerek kockázatát, mivel a régi vagy elavult rendszerek gyakran nagyobb kockázatot jelentenek, lehetővé teszi az IT csapat számára, hogy hatékonyabban tervezzen és végrehajtson karbantartási és frissítési feladatokat és elősegíti a szükséges dokumentáció és a hitelesítési követelmények teljesítését.

A követelmény alkalmazásának lépései

1. A szervezetnek először létre kell hoznia egy EIR nyilvántartást. Ez magában foglalja az összes EIR azonosítását és kategorizálását a szervezeten belül.
2. A szervezetnek meg kell határoznia a nyilvántartás frissítésének gyakoriságát. Ez lehet hetente, havi vagy negyedéves rendszerességgel, attól függően, hogy milyen gyakran változnak az EIR-ek vagy azok rendszerelemei, összetevői.
3. A szervezetnek rendszeresen ellenőriznie kell az EIR-eket, hogy biztosítsa azok megfelelőségét és naprakészségét. Ez magában foglalja az EIR-ek ellenőrzését a nyilvántartásban rögzített változások alapján.
4. A szervezetnek dokumentálnia kell az EIR-ek változásait, beleértve az új rendszerelemek hozzáadását, a meglévők módosítását vagy törlését.

5. A szervezetnek biztosítania kell, hogy az EIR-ek nyilvántartása naprakész és pontosan egyezik a valósággal. Ez magában foglalja a nyilvántartás rendszeres felülvizsgálatát és frissítését.
6. A szervezetnek biztosítania kell, hogy a nyilvántartásban szereplő összes EIR megfelel az aktuális kiberbiztonsági követelményeknek. Ez magában foglalja a naplóban rögzített biztonsági események ellenőrzését és a szükséges intézkedések megtételét a biztonsági problémák kezelésére.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

PM-5

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

1.6. BIZTONSÁGI TELJESÍTMÉNY MÉRÉSE

1.6. A szervezet kifejleszti az EIR-ei biztonsági mérésének rendszerét, folyamatosan felügyeli a teljesítménymutatókat, és rendszeres jelentéseket készít ezekről.

MAGYARÁZAT

Az érintett szervezet - az információbiztonsági szervezési intézkedéseire, valamint azok ellenőrzésére vonatkozó hatékonyság növelése érdekében - kifejleszti az EIR-ek biztonsági mérésének rendszerét. A mérési rendszer akkor eredményes, ha az az érintett szervezet kockázatkezelési stratégiájával, továbbá működési és menedzsment céljaival szoros kapcsolatban áll. Egy szofisztikáltan megalkotott, biztonsági teljesítmény mérésére szolgáló program olyan teljesítménymutatókat használ, melyek valós és reprezentatív képet adnak a menedzsment számára az EIR biztonságáról, illetőleg az érintett szervezet által alkalmazott biztonsági irányítási rendszer állapotáról. A biztonsági teljesítménymutatók irányulhatnak például a rendszer állapotára (rendszerfrissítések és azok hatékonysága - rendszerek naprakészsége), irányulhatnak az érintett szervezet kiberbiztonsági rezilienciájára (vírusvédelem hatékonysága, dolgozók biztonságtudatossága - például egy phishing kampánnyal szembeni ellenállása, egy adott képzést követő vizsga eredményei, vagy a felhasználók jelszókezelési szokásai), irányulhatnak többek között a szervezet reakcióidejére (pl. átlagos biztonsági esemény reagálási idő, sérülékenységek felfedése utáni frissítési és hibakezelési eljárási idő), de a rendelkezésre állás monitoring kapcsán is számos teljesítménymutató meghatározható. Gyakori teljesítménymutató továbbá az üzletmenet-folytonosság vonatkozásában az üzletmenet-folytonossági és katasztrófa utáni helyreállítási tesztelés végrehajtási ideje és annak hatékonysága. Az érintett szervezetek függetlenül attól, hogy tanúsítottak-e az ISO/IEC 27001 szabványra, a teljesítménymutatók megfelelő kiválasztása érdekében segítségül hívhatják az ISO/IEC 27004 nemzetközi szabványt.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell fejlesztenie az EIR-re vonatkozó biztonsági mérésének rendszerét.
2. A szervezetnek folyamatosan monitoroznia kell az általa meghatározott teljesítménymutatókat. Rendszeresen ellenőrizni kell a meghatározott mérőszámokat, és figyelemmel kell kísérni a változásokat. Ez lehetővé teszi a szervezet számára, hogy időben

észlelje a potenciális biztonsági problémákat, és megtegye a szükséges lépéseket a kockázatok csökkentése érdekében.

3. A szervezetnek rendszeresen jelentéseket kell készítenie az EIR biztonsági mérési rendszerének eredményeiről. Ezek a jelentések részletes információkat tartalmaznak a mérőszámok aktuális állapotáról, a változásokról és a potenciális kockázatokról. A jelentések segítenek a szervezetnek a kiberbiztonsági stratégia finomításában, és lehetővé teszik a vezetőség számára, hogy megalapozott döntéseket hozzanak a biztonsági kérdésekben.

4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az EIR biztonsági mérési rendszerét, hogy biztosítsa annak relevanciáját és hatékonyságát a változó kiberbiztonsági környezetben.

Kapcsolódó intézkedések

5.14. Folyamatos felügyelet

1.10. Kockázatkezelési stratégia

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

3.3.5.2. A biztonsági teljesítmény mérése: Az érintett szervezet kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.

ISO/IEC 27001:2023 referencia

5.3; 6.1.1; 6.2; 9.1

NIST SP 800-53 rev.5 referencia

PM-6

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

1.7. SZERVEZETI ARCHITEKTÚRA

1.7. A szervezet kifejleszti és fenntartja a szervezeti szervezetrendszert, amely tekintettel van mindazon kockázatokra, amelyek hatással lehetnek a szervezeti működésre, az eszközökre, az egyénekre és más szervezetekre.

MAGYARÁZAT

A biztonsági követelmények és védelmi intézedések integrálása a vállalati architektúrába segít annak biztosításában, hogy a biztonsági megfontolások a rendszerfejlesztési életciklus során mindvégig érvényesüljenek, és kifejezetten kapcsolódjanak a szervezet működési céljaihoz és üzleti folyamataihoz. A biztonsági követelmények integrálásának folyamata a vállalati architektúrába és a szervezet biztonsági architektúráiba is beágyazódik, összhangban a szervezeti kockázatkezelési stratégiával. Jelen követelmény esetében a az összes szervezeti rendszerre vonatkozó biztonsági követelményt alakítják ki. A Tervezés követelménycsoport részét képező Biztonsági Architektúra követelmény esetében a biztonsági architektúrát az egyedi rendszerek szintjén alakítják ki. A rendszerszintű architektúra összhangban van a szervezet számára meghatározott biztonsági architektúrával. A biztonsági követelmények és a védelmi intézkedések integrációja a leghatékonyabban a kockázatkezelési keretrendszer és a támogató biztonsági szabványok és iránymutatások következetes alkalmazásával valósítható meg.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fejlesztenie kell egy vállalati architektúrát, amely integráltan kezeli az összes szervezeti biztonsági követelményt.
2. A szervezetnek a biztonsági követelmények integrációs folyamata során össze kell hangolnia a vállalati architektúrát és az érintett szervezet biztonsági architektúráit, valamint a szervezet kockázatkezelési stratégiáját. A "Információbiztonsági architektúra leírás (Tervezés)" követelmény esetében a biztonsági és adatvédelmi architektúrákat egyetlen EIR szintjén kell kifejleszteni. Az egyes EIR szintű architektúráknak összhangban kell állniuk a szervezet számára meghatározott biztonsági architektúrákkal. A biztonsági követelmények integrációját a legjobban a Kockázatkezelési Keretrendszer szigorú alkalmazásával, valamint a különböző biztonsági szabványok és irányelvek segítségével lehet elérni.

3. A szervezetnek dokumentálnia kell az egész folyamatot, hogy nyomon követhesse a fejlődést és az felmerülő problémákat.

Kapcsolódó intézkedések

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

13.2. Rendszerbiztonsági terv

13.6. Információbiztonsági architektúra leírás

1.12. Szervezeti működés és üzleti folyamatok meghatározása

15.2. Biztonsági osztályba sorolás

16.3.1. A rendszer fejlesztési életciklusa

16.16. Biztonságtervezési elvek

16.87. Fejlesztői biztonsági architektúra és tervezés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

PM-7

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

1.8. SZERVEZETI ARCHITEKTÚRA – TEHERMENTESÍTÉS

1.8. A szervezet más rendszerekbe, rendszerelemekbe szervezi át vagy külső szolgáltatóhoz szervezi ki a szervezet által meghatározott és a szervezet működése szempontjából nem kritikus funkciókat vagy szolgáltatásokat.

MAGYARÁZAT

Nem minden funkció vagy szolgáltatás, amelyet egy rendszer nyújt, alapvető fontosságú a szervezet működési céljai vagy az üzleti funkciói szempontjából. A nyomtatás vagy másolás egy példa lehet a szervezet számára nem alapvető, de támogató szolgáltatásra. Amennyiben lehetséges, az ilyen támogató, de nem alapvető funkciókat vagy szolgáltatásokat nem helyezik egy helyre az alapvető működési célokat vagy üzleti funkciókat támogató funkciókkal vagy szolgáltatásokkal. Az ilyen funkciók ugyanazon a rendszeren vagy rendszerösszetevőn való fenntartása növeli a szervezet működési céljai szempontjából alapvető fontosságú funkcióinak vagy szolgáltatásainak a támadási felületét. A támogató, de nem létfontosságú funkciók nem kritikus rendszerbe, rendszerelembe vagy külső szolgáltatóhoz történő áthelyezése szintén növelheti a hatékonyságot azáltal, hogy ezeket a funkciókat vagy szolgáltatásokat olyan személyek vagy szolgáltatók irányítása alá helyezi, akik a funkciók vagy szolgáltatások szakértői.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, mely funkciók és szolgáltatások nem kritikusak a szervezet működése szempontjából.
2. A szervezetnek át kell helyeznie a támogató, de nem alapvető fontosságú funkciókat és szolgáltatásokat azoktól az EIR-ekből vagy rendszerelemekből, amelyek az alapvető alapfeladatokat vagy üzleti funkciókat támogatják.
3. A szervezetnek át kell helyeznie a támogató, de nem létfontosságú funkciókat egy nem kritikus EIR-re, rendszerelemre vagy külső szolgáltatóhoz.
4. A szervezetnek dokumentálnia kell a nem kritikus funkciók és szolgáltatások áthelyezését, hogy nyomon követhető legyen a folyamat és biztosítható legyen a biztonsági követelményeknek való megfelelés.

Kapcsolódó intézkedések

16.16. Biztonságtervezési elvek

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

PM-7(1)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a nem alapvető funkciók vagy szolgáltatások meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

1.9. A SZERVEZET MŰKÖDÉSE SZEMPONTJÁBÓL KRITIKUS INFRASTRUKTÚRA BIZTONSÁGI TERVE

1.9. A szervezet a szervezet működése szempontjából kritikus infrastruktúra és kulcsfontosságú erőforrások biztonsági tervének kidolgozása, dokumentálása és frissítése során kezeli az információbiztonsági kérdéseket.

MAGYARÁZAT

A védelmi stratégiák a kritikus eszközök és erőforrások rangsorolásán alapulnak. A szervezet működése szempontjából kritikus infrastruktúra és a kulcsfontosságú erőforrások meghatározására és a kapcsolódó infrastruktúra védelmi tervének elkészítésére vonatkozó követelményeket és útmutatást a vonatkozó jogszabályok, végrehajtási rendeletek, irányelvek, szabályok, rendeletek, szabványok és iránymutatások tartalmazzák.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, melyek a szervezet működése szempontjából kritikus infrastruktúrák és kulcsfontosságú erőforrások.
2. A szervezetnek ki kell dolgoznia az ezen infrastruktúrák biztonsági tervét. Ez a terv tartalmazza az információbiztonsági kérdéseket, beleértve az EIR védelmét és a kiberbiztonsági fenyegetések kezelését.
3. A szervezetnek dokumentálnia kell a biztonsági tervet, beleértve az EIR-re vonatkozó információbiztonsági intézkedéseket. Ez magában foglalja a biztonsági eljárásokat, a kiberbiztonsági fenyegetések kezelésének módszereit, és a szervezet működése szempontjából kritikus infrastruktúrák és erőforrások védelmének stratégiáit.
4. A szervezetnek rendszeresen frissítenie kell a szervezet működése szempontjából kritikus infrastruktúrák biztonsági tervet, hogy az naprakész legyen és megfeleljen a változó kiberbiztonsági környezetnek. Ez magában foglalja az EIR-re vonatkozó információbiztonsági intézkedések felülvizsgálatát és módosítását, valamint a infrastruktúrák és erőforrások védelmének stratégiáinak aktualizálását.
5. A szervezetnek dokumentálnia kell a biztonsági terv kidolgozásának, módosításának és frissítésének folyamatát.

Kapcsolódó intézkedések

7.2. Üzletmenet-folytonossági terv

7.13. Üzletmenet-folytonossági terv tesztelése

12.44. Az információs rendszer elemeinek elhelyezése

13.2. Rendszerbiztonsági terv

1.10. Kockázatkezelési stratégia

1.12. Szervezeti működés és üzleti folyamatok meghatározása

15.4. Kockázatértékelés

18.67. Információ kezelése és megőrzése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

PM-8

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

1.10. KOCKÁZATMENEDZSMENT STRATÉGIA

1.10. A szervezet:

1.10.1. Kidolgoz egy átfogó stratégiát, amely kezeli:

1.10.1.1. - az EIR-ek működésével és használatával összefüggő, a szervezet működéséhez, vagyonelemeihez, a szervezethez köthető személyekhez, és más szervezetekhez kapcsolódó biztonsági kockázatokat.

1.10.1.2. - a személyes adatok kezeléséből fakadó kockázatokat.

1.10.2. Az egész szervezeten belül egységesen alkalmazza a kockázatmenedzsment stratégiát.

1.10.3. A szervezet által meghatározott gyakorisággal és esetekben felülvizsgálja és frissíti a kockázatmenedzsment stratégiát, hogy meg tudjon felelni a szervezeti változásoknak.

MAGYARÁZAT

Az egész szervezetre kiterjedő kockázatkezelési stratégia magában foglalja a szervezet kockázattűrésének meghatározását, a kockázatcsökkentési stratégiákat, az elfogadható kockázatértékelési módszereket, a szervezet egészére kiterjedő kockázatértékelésének folyamatát, valamint a kockázat időbeli nyomon követésére szolgáló megközelítéseket. A kockázatkezelésért felelős vezető (a szervezet vezetője vagy kijelölt képviselője) összehangolja az információbiztonság irányítási folyamatait a stratégiai, operatív és költségvetési tervezési folyamatokkal. A kockázatkezelésért felelős vezető által vezetett kockázatkezelési irányítási funkció elősegítheti a kockázatkezelési stratégia következetes alkalmazását az egész szervezetre kiterjedően. A kockázatkezelési stratégiát a szervezeten belüli és kívüli, más forrásokból származó, a kockázatokkal kapcsolatos információkkal lehet alátámasztani annak biztosítása érdekében, hogy a stratégia kellően széles körű és átfogó legyen. Az ellátási lánc kockázatkezelési stratégiája szintén hasznos információkat szolgáltathat a szervezet egészére kiterjedő kockázatkezelési stratégiához.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia egy átfogó kockázatkezelési stratégiát, amely tartalmazza a szervezet kockázattűrését, a kockázatok csökkentésének stratégiáit, az elfogadható kockázatértékelési módszertanokat, egy folyamatot a biztonsági kockázatok értékelésére az

egész szervezeten belül, valamint a szervezet kockázattűrésével összhangban, és a megközelítéseket a kockázatok időbeli nyomon követésére.

2. A kockázatkezelésért felelős személy összehangolja az információbiztonsági irányítási folyamatokat a stratégiai, operatív és költségvetési tervezési folyamatokkal.

3. Az EIR-ekkel kapcsolatos ellátási lánc kockázatkezelési stratégia, hasznos bemeneteket is nyújthat az érintett szervezet széles körű kockázatkezelési stratégiájához.

4. Az érintett szervezet által meghatározott gyakorisággal és esetekben felülvizsgálja és frissíti a kockázatkezelési stratégiát, hogy meg tudjon felelni a szervezeti változásoknak. Ezt a folyamatot naplózni kell, hogy biztosítsa a folyamat átláthatóságát és nyomon követhetőségét.

Kapcsolódó intézkedések

2.1. Szabályzat és eljárásrendek

4.1. Szabályzat és eljárásrendek

3.1. Szabályzat és eljárásrendek

5.1. Szabályzat és eljárásrendek

5.2. Biztonsági értékelések

5.9. Az intézkedési terv és mérföldkövei

5.11. Engedélyezés

5.14. Folyamatos felügyelet

6.1. Szabályzat és eljárásrendek

7.1. Szabályzat és eljárásrendek

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

4.3; 4.4; 6.1.1; 6.1.2; 6.2; 7.5.1; 7.5.2; 7.5.3; 10.1

NIST SP 800-53 rev.5 referencia

PM-9

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

1.11. ENGEDÉLYEZÉSI FOLYAMATOK MEGHATÁROZÁSA

1.11. A szervezet:

1.11.1. Engedélyezési folyamatokon keresztül kezeli az EIR-ek és azok környezetének biztonsági állapotát.

1.11.2. Kijelöli a szervezet kockázatmenedzsment folyamatának felelőseit (névvel és felelősségi körrel ellátva).

1.11.3. Beilleszti az engedélyezési folyamatokat a szervezet egészét átfogó kockázatmenedzsment keretrendszerbe.

MAGYARÁZAT

A szervezeti rendszerek és működési környezetük engedélyezési folyamatai megkövetelik az egész szervezetre kiterjedő kockázatkezelési eljárás kialakítását, amelyhez a szervezet segítségül hívhatja meglévő kockázatkezelési keretrendszerek iránymutatásait, valamint a kapcsolódó biztonsági szabványokat, amelyek alapján implementálhat és végrehajthat az egész szervezetre kiterjedően. Ezen eljárás kialakításában kulcsfontosságú szerepet tölt be egy kockázatkezelésért felelős vezető és minden egyes szervezeti rendszer esetében egy kijelölt engedélyező. A szervezet engedélyezési folyamatait a folyamatos ellenőrzési folyamatokkal integrálják, hogy megkönnyítsék a szervezeti működésre, a szervezeti eszközökre, személyekre, és más szervezetekre vonatkozó biztonsági kockázatok folyamatos megértését és elfogadását.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek engedélyezési folyamatokat kell létrehoznia az EIR-ek és azok működési környezetének biztonsági állapotának kezelésére. A kockázatkezelési folyamatokért felelős személyt és az egyes EIR-ekért felelős engedélyezőket kell kijelölni.

3. A szervezetnek be kell illesztenie az engedélyezési folyamatokat a szervezet egészét átfogó kockázatkezelési keretrendszerbe.

4. A szervezet engedélyezési folyamatait össze kell hangolni a folyamatos felügyeleti folyamatokkal, hogy elősegítsék a biztonsági kockázatok folyamatos megértését és elfogadását az érintett szervezet működésére, eszközeire, személyekre, más szervezetekre.

5. A szervezetnek dokumentálnia kell az engedélyezési folyamatokat, hogy nyomon követhesse és ellenőrizhesse a folyamatokat és az esetleges biztonsági eseményeket.

Kapcsolódó intézkedések

5.11. Engedélyezés

5.14. Folyamatos felügyelet

13.2. Rendszerbiztonsági terv

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.2

NIST SP 800-53 rev.5 referencia

PM-10

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

1.12. SZERVEZETI MŰKÖDÉS ÉS ÜZLETI FOLYAMATOK MEGHATÁROZÁSA

1.12. A szervezet:

1.12.1. Meghatározza a szervezeti célokat és az üzleti folyamatokat, figyelembe véve az információbiztonságot, valamint a szervezeti működésre, eszközökre, személyekre, más szervezetekre gyakorolt kockázatokat.

1.12.2. Meghatározza a szervezeti célokból és üzleti folyamatokból adódó információvédelmi igényeket.

1.12.3. Meghatározott gyakorisággal felülvizsgálja és módosítja a szervezeti célokat és az üzleti folyamatokat.

MAGYARÁZAT

A szervezeti célokkal és az alapfunkciókkal összhangban megalkotott információvédelmi igények határozzák meg a szervezet és az EIR-ek számára szükséges biztonsági követelményeket. A biztonsági követelmények meghatározásához hozzátartozik annak a káros hatásnak a megértése, amelyet az információk veszélyeztetése vagy sérülése eredményezhet. A működési célokat és az alapfunkciókat, valamint a kapcsolódó védelmi követelményeket a szervezeti irányelvekkel és eljárásokkal összhangban dokumentálni szükséges.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a szervezeti célokat és az alapfunkciókat, figyelembe véve az információbiztonságot és a szervezeti működésre, EIR-re, személyekre, más szervezetekre gyakorolt kockázatokat.

2. A szervezetnek meg kell határoznia a szervezeti célokból és alapfunkciókból adódó információvédelmi igényeket.

3. A szervezetnek dokumentálnia kell az alapfeladatok és az alapfunkciók meghatározásait, valamint a hozzájuk kapcsolódó védelmi követelményeket az érintett szervezet szabályzatai és eljárásrendjei szerint.

4. A szervezetnek meghatározott gyakorisággal felül kell vizsgálnia és módosítania a szervezeti célokat és az alapfunkciókat, hogy biztosítsa azok relevanciáját és hatékonyságát a változó környezeti és üzleti körülmények között.

Kapcsolódó intézkedések

7.2. Üzletmenet-folytonossági terv

13.2. Rendszerbiztonsági terv

1.7. Vállalati architektúra

1.9. A szervezet működése szempontjából kritikus infrastruktúra biztonsági terve

15.2. Biztonsági osztályba sorolás

15.4. Kockázatértékelés

15.21. Rendszerelemek kritikusságának elemzése

16.2. Erőforrások rendelkezésre állása

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

4.1

NIST SP 800-53 rev.5 referencia

PM-11

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

1.13. Belső fenyegetés elleni program

1.13. A szervezet bevezet egy belső fenyegetések elleni programot, amely magában foglalja egy több szakterületet átfogó, belső fenyegetéssel kapcsolatos biztonsági események kezelését végző csoport működtetését.

Magyarázat

A belső fenyegetések elleni progamok olyan védelmi intézkedéseket tartalmaznak, amelyek a rosszindulatú bennfentes tevékenységet a technikai és nem technikai információk integrálásával és elemzésével fedezik fel és akadályozzák meg. A központosított integrálási és elemzési képességen túlmenően a belső fenyegetés elleni programok megkövetelik a szervezetektől, hogy készítsenek belső fenyegetésre vonatkozó szabályzatokat és biztosítsanak ezzel kapcsolatos tudatossági képzést a munkavállalók számára, szerezzenek be külső forrásból olyan információkat, amelyek a fenyegetettség elemzéséhez szükségesek, és végezzenek önértékelést a szervezet belső fenyegetettségi helyzetéről. Különösen hasznos lehet a humánerőforrás szervezeti egység bevonása, mivel bizonyítékokat lehet szerezni arra, hogy bizonyos típusú belső szabálysértéseket gyakran megelőzik a munkahelyi elégedetlen viselkedési minták és a konfliktusok a közvetlen munkatársakkal és más kollégákkal. Továbbá ajánlott a jogi szervezeti egység bevonása, beleértve az adatvédelemért felelős tisztviselővel való konzultációt, aki biztosítja, hogy a felügyeleti tevékenységek összhangban legyenek az alkalmazandó törvényekkel, végrehajtási rendeletekkel, irányelvekkel, belső szabályokkal, szabványokkal és útmutatókkal.

A követelmény alkalmazásának lépései

1. A szervezet vezetője nevezzen ki egy megfelelően magas rangú vezetőt, aki felelős lesz a belső fenyegetések elleni program megvalósításáért és felügyeletéért.
2. A szervezetnek szabályzatba kell foglalnia a belső fenyegetések elleni meghatározottakat és egy ehhez tartozó eljárásrendet is dokumentálni szükséges.
3. A szervezetnek host-alapú felhasználói monitorozást kell megvalósítania a szervezet tulajdonában álló EIR(ek)-en.
4. A szervezetnek belső fenyegetésekkel kapcsolatos tudatossági képzést kell biztosítania a munkavállalók számára.

5. A szervezetnek saját magán belül lehetőség szerint minél több információforrásból (például minden szervezeti egységtől) hozzájárulást és hozzáférést kell szereznie az általuk kezelt információkhoz a belső fenyegetések elemzéséhez.
6. A szervezetnek önértékelést kell végeznie saját, belső fenyegetésekkel szembeni állapotáról.
7. A szervezetnek javasolt kihasználnia a már meglévő, például az eseménykezelő csapatokat.
10. A szervezetnek folyamatosan naplóznia és elemeznie kell a belső fenyegetésekkel kapcsolatos eseményeket, hogy időben észlelhessék és megelőzhessék a potenciális belső fenyegetéseket.

Kapcsolódó intézkedések

2.60. Legkisebb jogosultság elve
3.2. Biztonságtudatossági képzés
4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel
4.22. Naplóbejegyzések csökkentése és jelentéskészítés
4.33. Letagadhatatlanság
4.40. Naplóbejegyzések létrehozása
4.44. Információk kiszivárgásának figyelemmel kísérése
5.14. Folyamatos felügyelet
8.14. Azonosító kezelés
9.9.1. Biztonsági események kezelése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

PM-12

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

1.14. BIZTONSÁGI SZEMÉLYZET KÉPZÉSE

1.14. A szervezet létrehozza a biztonsági személyzet képzését és fejlesztését elősegítő programot.

MAGYARÁZAT

A biztonsági személyzet képzését és fejlesztését elősegítő programok magukban foglalják a biztonsági feladatok és feladatok ellátásához szükséges ismeretek, készségek és képességek meghatározását, a szerepkör alapú képzési programok kidolgozását a biztonsági szerep- és felelősségi körökkel megbízott személyek számára, valamint szabályok és iránymutatások kidolgozását a biztonsággal kapcsolatos pozíciókat betöltő személyek és a pályázók egyéni képzettségének mérésére és fejlesztésére. A képzési programok mérhetővé teszik az egyéni teljesítményt, valamint karrierutat biztosítanak a biztonsági szerepköröket betöltők számára, ezzel is ösztönözve a szakembereket a területen való előrelépésre és a nagyobb felelősséggel járó pozíciók betöltésére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azt a tudást, készségeket és képességeket, amelyekre szükség van a biztonsággal kapcsolatos feladatok elvégzéséhez.
2. A szervezetnek szerepkör-alapú képzési programokat kell kifejlesztenie azok számára, akik biztonsági szerep- és felelősségi köröket látnak el.
3. A szervezetnek meglévő szabványokat és irányelveket kell alkalmaznia az egyéni képesítések méréséhez és fejlesztéséhez a biztonsági pozíciókban dolgozók és jelentkezők számára.
4. A szervezetnek biztonsági karrierutakat be kell kidolgoznia a programban, hogy ösztönözze a biztonsági szakembereket a területen való előrelépésre és a nagyobb felelősségfel járó pozíciók betöltésére.
5. A szervezetnek a programokat úgy kell kialakítania, hogy ösztönözzék a képesítéssel rendelkező személyeket a biztonsági pozíciók betöltésére.
6. A szervezetnek a biztonsági munkaerő-fejlesztési programokat össze kell hangolnia a szervezeti biztonsági tudatosság és képzési programokkal, és összpontosítania kell a személyzet alapvető biztonsági képességeinek fejlesztésére és intézményesítésére, hogy ilyen módon is védje a szervezet működését, eszközeit és a személyeket.

7. A szervezetnek dokumentálnia kell a programban részt vevők előrehaladásáról és fejlődéséről, hogy biztosítsa a program hatékonyságát és folyamatos fejlesztését.

Kapcsolódó intézkedések

3.2. Biztonságtudatossági képzés

3.9. Szerepkör alapú biztonsági képzés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

7.2; A.6.3

NIST SP 800-53 rev.5 referencia

PM-13

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

1.15. TESZTELÉS, KÉPZÉS ÉS FELÜGYELET

1.15. A szervezet:

1.15.1. Bevezet egy folyamatot, amely biztosítja, hogy a szervezeti EIR-ekhez kapcsolódó biztonsági tesztelések, képzések és felügyeleti tevékenységek elvégzésére vonatkozó szervezeti tervek megfelelő fejlesztés és karbantartás mellett folyamatosan végrehajtásra kerüljenek.

1.15.2. Felülvizsgálja és összehangolja a terveit a szervezeti kockázatmenedzsment stratégiával és a kockázatkezelési intézkedésekre vonatkozó, az egész szervezetre kiterjedő prioritásokkal.

MAGYARÁZAT

Az egész szervezetre kiterjedő biztonsági tesztelési, képzési és felügyeleti folyamat segít biztosítani, hogy a szervezet mindig tisztán lássa a tesztelési, képzési és felügyeleti tevékenységek aktuális állapotát, és lehetősége nyílik arra, hogy ezeket a tevékenységeket összehangoltan kezelje. A folyamatos felügyeleti folyamatok növekvő fontosságával, az információbiztonsági védelmi intézkedések megvalósításával a kockázatelemzések alapján, valamint az egész szervezetre kiterjedő biztonsági követelmények széles körű használatával a szervezet összehangolja és konszolidálja a különböző biztonsági követelmények megvalósulását támogató folyamatos értékelések részeként rutinszerűen végzett tesztelési és felügyeleti tevékenységeket. A biztonsági képzési tevékenységek, bár az egyes rendszerekre és konkrét szerepkörökre összpontosítanak, az összes szervezeti elemre kiterjedő koordinációt igényelnek. A tesztelési, képzési és felügyeleti terveket és tevékenységeket az aktuális fenyegetés- és sérülékenységi vizsgálatok eredményei alapján határozzák meg.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell vezetnie egy folyamatot, amely biztosítja, hogy az EIR-ekhez kapcsolódó biztonsági tesztelések, képzések és felügyeleti tevékenységek folyamatosan végrehajtásra kerüljenek. Ez magában foglalja a tesztelési, képzési és felügyeleti tervek fejlesztését és karbantartását.

2. A szervezetnek gondoskodnia kell arról, hogy ezek a tevékenységek összehangoltak legyenek.

3. A szervezetnek biztosítania kell, hogy a tesztelési, képzési és felügyeleti tervek és tevékenységek a jelenlegi fenyegetés- és sérülékenységi vizsgálati eredmények alapján készülnek.
4. A szervezetnek felül kell vizsgálnia és össze kell hangolnia a terveit a szervezeti kockázatkezelési stratégiával és a kockázatkezelési intézkedésekre vonatkozó, az egész szervezetre kiterjedő prioritásokkal.
5. A szervezetnek dokumentálnia kell a tesztelési, képzési és felügyeleti tevékenységeket, hogy biztosítsa a folyamatok átláthatóságát és a felelősséget.

KAPCSOLÓDÓ INTÉZKEDÉSEK

3.2. Biztonságtudatossági képzés
3.9. Szerepkör alapú biztonsági képzés
5.14. Folyamatos felügyelet
7.13. Üzletmenet-folytonossági terv tesztelése
9.5. Biztonsági események kezelésének tesztelése
1.13. Belső fenyegetés elleni program
18.13. Az EIR monitorozása

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

3.3.5.1. Az érintett szervezet:

ISO/IEC 27001:2023 REFERENCIA

6.2

NIST SP 800-53 REV.5 REFERENCIA

PM-14

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

1.16. SZAKMAI CSOPORTOKKAL ÉS KÖZÖSSÉGEKKEL VALÓ KAPCSOLATTARTÁS

1.16. A szervezet:

1.16.1. Felveszi és kialakítja a kapcsolatot a kiválasztott szakmai csoportokkal és közösségekkel annak érdekében, hogy

1.16.1.1. - elősegítse a szervezethez köthető személyek folyamatos biztonsági oktatását és képzését;

1.16.1.2. - naprakész információkkal rendelkezzen az ajánlott biztonsági gyakorlatok, technikák és technológiák terén;

1.16.1.3. - megossza az aktuális biztonsággal kapcsolatos információkat, beleértve a fenyegetéseket, sérülékenységeket és biztonsági eseményeket.

MAGYARÁZAT

A szakmai csoportokkal és közösségekkel való folyamatos kapcsolattartás fontos a gyorsan változó technológiák és fenyegetések közepette. A szakmai csoportok és közösségek közé tartoznak a speciális érdekcsoportok, szakmai szövetségek, fórumok, hírcsoportok, felhasználói csoportok és a hasonló szervezetekben dolgozó biztonsági szakemberek csoportjai. A szervezetek a működési célok és az üzleti funkciók alapján választják ki a biztonsági csoportokat és egyesületeket. A szervezetek megosztják egymással a fenyegetésekkel, sebezhetőségekkel és biztonsági eseményekkel kapcsolatos információkat (megfelelő feltételek mentén), valamint a kontextuális tudást igénylő ismereteket és a vonatkozó törvényeknek, végrehajtási rendeleteknek, irányelveknek, szabályzatoknak, előírásoknak, szabványoknak és iránymutatásoknak való megfelelési technikákat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell választania azokat a szakmai csoportokat és közösségeket, amelyekkel kapcsolatot kíván létrehozni.

2. Miután kiválasztotta a megfelelő csoportokat, a szervezetnek kapcsolatot kell létesítenie ezekkel a csoportokkal, és aktívan részt kell vennie a közösségek és csoportok tevékenységeiben. Ez magában foglalhatja a rendszeres kommunikációt, a szakmai- vagy

érdekcsoportok által szervezett eseményeken való részvételt, és a közzétett információk követését.

3. A szervezetnek folyamatosan biztosítania kell a szervezethez köthető személyek biztonsági oktatását és képzését. Ez magában foglalhatja a biztonsági gyakorlatok, technikák és technológiák oktatását, valamint a fenyegetések, sérülékenységek és biztonsági események ismertetését.

4. A szervezetnek naprakész információkkal kell rendelkeznie az ajánlott biztonsági gyakorlatokról, technikákról és technológiákról. Ez magában foglalhatja a csoportoktól és közösségektől származó információk követését, valamint saját kutatások és elemzések végzését.

5. A szervezetnek meg kell osztania az aktuális biztonsággal kapcsolatos információkat, beleértve a fenyegetéseket, sérülékenységeket és biztonsági eseményeket. Ez magában foglalhatja az információk megosztását a csoportokkal és közösségekkel.

6. A szervezetnek dokumentálnia kell a biztonsági eseményeket, és rendszeresen felül kell vizsgálnia a naplót, hogy azonosítsa a potenciális problémákat és javítási lehetőségeket.

Kapcsolódó intézkedések

16.66. Fejlesztői biztonsági tesztelés

18.37. Biztonsági riasztások és tájékoztatások

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

7.4; A.5.6

NIST SP 800-53 rev.5 referencia

PM-15

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

1.17. FENYEGETETTSÉG TUDATOSÍTÓ PROGRAM

1.17. A szervezet a fenyegetésekkel kapcsolatos információk megosztására fenyegetettség tudatosító programot vezet be, amely magában foglalja a fenyegetések felismerését szolgáló szervezeten belüli és szervezetek közötti információmegosztási képességet.

MAGYARÁZAT

A folyamatosan változó és egyre kifinomultabb fenyegetések, különösen a fejlett, tartós fenyegetések (APT csoportok) miatt egyre valószínűbb, hogy a támadók sikeresen behatolnak a szervezeti EIR-ekbe, rendszerelemekbe vagy veszélyeztetik azokat. Az egyik legjobb technika ennek kezelésére az, ha a szervezetek megosztják egymással a fenyegetésekkel kapcsolatos információikat, beleértve a szervezetek által tapasztalt fenyegetési eseményeket (azaz azokat a taktikákat, technikákat és eljárásokat), szervezetek által bizonyos típusú fenyegetésekkel szemben hatásosnak talált kockázatcsökkentő intézkedéseket, valamint a fenyegetési információkat (azaz a fenyegetésekre vonatkozó jelzéseket és figyelmeztetéseket). A fenyegetésekre vonatkozó információk megosztása lehet kétoldalú vagy többoldalú. A többoldalú fenyegetésmegosztás keretében a szereplők fenyegetési információkat megosztó csoportot hoznak létre. A fenyegetésekkel kapcsolatos információk különleges megállapodásokat és védelmet igényelhetnek, vagy szabadon megoszthatók.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először létre kell hoznia egy fenyegetettség tudatosító programot. Ez a program magában foglalja a fenyegetések felderítését és azokról szóló információk megosztását a szervezeten belül és más szervezetekkel.
2. A szervezetnek ki kell dolgoznia egy stratégiát a fenyegetések felderítésére. Ez magában foglalhatja a fenyegetések azonosítását, értékelését és prioritizálását az EIR-en belül.
3. A szervezetnek létre kell hoznia egy információmegosztási rendszert, amely lehetővé teszi a fenyegetésekkel kapcsolatos információk gyors és hatékony megosztását a szervezeten belül és más szervezetekkel.
4. A szervezetnek meg kell határoznia a fenyegetésekkel kapcsolatos információk megosztásának szabályait és eljárásait. Ez magában foglalhatja a megosztandó információk

típusát, a megosztás módját és időzítését, valamint a megosztásért felelős személyeket vagy csoportokat.

5. A szervezetnek rendszeresen naplót kell vezetnie a fenyegetésekkel kapcsolatos információk megosztásáról, hogy nyomon követhesse a program hatékonyságát és szükség esetén módosíthassa azt.

6. A szervezetnek biztosítania kell, hogy a fenyegetésekkel kapcsolatos információk megosztása megfelelően védett legyen, hogy megakadályozza az információk illetéktelen hozzáférését vagy felhasználását.

7. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a fenyegetettség tudatosító programját, hogy biztosítsa annak relevanciáját és hatékonyságát a folyamatosan változó fenyegetési környezetben.

Kapcsolódó intézkedések

9.9.1. Biztonsági események kezelése

1.13. Belső fenyegetés elleni program

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.7

NIST SP 800-53 rev.5 referencia

PM-16

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

1.18. Fenyegetettség tudatosító program – Fenyegetési információk automatizált megosztása

1.18. A szervezet automatizált mechanizmusokat alkalmaz a fenyegetésekkel kapcsolatos információk megosztási hatékonyságának maximalizálása érdekében.

Magyarázat

A monitorozás hatékonyságának maximalizálása érdekében fontos tudni, hogy az érzékelőknek milyen fenyegetéseket és mutatókat kell keresniük. A jól bevált keretrendszerek, szolgáltatások és automatizált eszközök használatával a szervezetek javítják azon képességüket, hogy gyorsan megosszák egymással és beírják a megfelelő fenyegetésekkel kapcsolatos információkat (szignatúrákat) a megfigyelő eszközökbe.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, milyen fenyegetést indikáló jeleket kell keresnie az EIR-ben.
2. A szervezetnek jól megalapozott keretrendszereket és szolgáltatásokat kell alkalmaznia, amelyek segítenek a fenyegetések azonosításában és kezelésében.
3. A szervezetnek automatizált eszközöket kell használnia a fenyegetésekkel kapcsolatos információk gyors megosztásához és a releváns fenyegetés-észlelési szignatúrák EIR-be történő beírásához. Ez magában foglalja az automatizált fenyegetés-észlelési és reagáló rendszerek, valamint a fenyegetés-intelligencia platformok használatát.
4. A szervezetnek folyamatosan frissítenie kell a fenyegetés-észlelési szignatúrákat és dokumentálnia kell az EIR-be történő beírásukat, hogy naprakész legyen a legújabb fenyegetésekkel és kockázatokkal kapcsolatban.
5. A szervezetnek rendszeresen ellenőriznie kell az EIR működését és a fenyegetés-észlelési szignatúrák hatékonyságát, hogy biztosítsa a kiberbiztonsági követelményeknek való megfelelést. Ez magában foglalja a naplók elemzését és a fenyegetés-észlelési szignatúrák hatékonyságának értékelését.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.5.7

NIST SP 800-53 REV.5 REFERENCIA

PM-16(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

1.19. KOCKÁZATMENEDZSMENT KERETRENDSZER

1.19. A szervezet:

1.19.1. Azonosítja és dokumentálja:

1.19.1.1. - a kockázatelemzést, kockázatkezelést és a kockázatok felügyeletét érintő feltételezéseit;

1.19.1.2. - a kockázatelemzést, kockázatkezelést és a kockázatok felügyeletét érintő megkötéseit;

1.19.1.3. - a kockázatmenedzsment során figyelembe vett prioritásokat és kompromisszumokat; továbbá

1.19.1.4. - a szervezet kockázattűrő képességét.

1.19.2. Megosztja a kockázatmenedzsment tevékenység eredményeit a szervezet által meghatározott személyekkel.

1.19.3. A szervezet által meghatározott gyakorisággal elvégzi a kockázatmenedzsment keretrendszer szempontrendszerének felülvizsgálatát és frissítését.

MAGYARÁZAT

A kockázatkezelési keretrendszer kialakítása akkor a leghatékonyabb, ha a szervezet szintjén és az érdekelt felekkel - beleértve a működési célok, az üzleti funkciók és a rendszer tulajdonosait - konzultálva történik. A kockázatkezelési folyamat részeként azonosított feltételezések, korlátozások, kockázattűrő képesség, prioritások és kompromisszumok alapul szolgálnak a kockázatkezelési stratégiához, amely viszont a kockázatértékelés, a kockázati válaszadás és a kockázatfigyelési tevékenységek elvégzéséhez szükséges információkkal szolgál. A kockázatkezelés eredményeit megosztják az érintett szervezethez köthető személyekkel, beleértve a működési célok és az üzleti funkciók tulajdonosait, az információk tulajdonosait vagy kezelőit, a rendszer tulajdonosait, az engedélyezésre jogosult vezetőket, a szervezet információbiztonsági vezetőjét és a kockázatkezelésért felelős személyt.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania és dokumentálnia kell a kockázatelemzést, kockázatkezelést és a kockázatok felügyeletét érintő feltételezéseit. Ez magában foglalja a kockázatkezelés során figyelembe vett prioritásokat és kompromisszumokat, valamint az érintett szervezet

kockázattűrő képességét, továbbá azonosítania és dokumentálnia kell a kockázatelemzést, kockázatkezelést és a kockázatok felügyeletét érintő megkötéseit.

2. A szervezetnek meg kell osztania a kockázatkezelési tevékenység eredményeit a szervezet által meghatározott személyekkel.

4. A szervezet által meghatározott gyakorisággal el kell végeznie a kockázatkezelési keretrendszer szempontrendszerének felülvizsgálatát és frissítését. Ez magában foglalja a kockázatkezelési stratégia, a kockázatelemzés, a kockázatválasz és a kockázatfelügyeleti tevékenységek felülvizsgálatát és frissítését.

5. A naplózás során az érintett szervezetnek figyelemmel kell kísérnie és dokumentálnia kell a kockázatkezelési tevékenységeket, beleértve a kockázatok azonosítását, értékelését, kezelését és felügyeletét.

Kapcsolódó intézkedések

5.14. Folyamatos felügyelet

1.10. Kockázatkezelési stratégia

15.4. Kockázatértékelés

15.20. Kockázatokra adott válasz

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

4.3; 6.1.2; 6.2; 7.4; 7.5.1; 7.5.2; 7.5.3

NIST SP 800-53 rev.5 referencia

PM-28

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

1.20. KOCKÁZATKEZELÉSÉRT FELELŐS SZEREPKÖRÖK

1.20. A szervezet kijelöl:

1.20.1. Egy kockázatkezelésért felelős személyt, aki összehangolja a szervezeti információbiztonsági irányítási folyamatokat a stratégiai, működési és költségvetés-tervezési folyamatokkal.

1.20.2. Egy kockázati vezető szerepkört betöltő személyt, aki biztosítja a kockázatok szervezeti szintű áttekintését és elemzését, valamint a kockázatmenedzsment szervezeten belüli egységes működését.

MAGYARÁZAT

A kockázatkezelésért felelős személy kinevezése elősegíti, hogy a szervezeti információbiztonsági irányítási folyamatok illeszkedjenek a szervezet stratégiai, működési és költségvetés-tervezési folyamataiba, ill. összhangban legyenek azokkal. A kockázati vezető a szervezet egészére kiterjedő kockázatkezelési tevékenységek vezetésért felelős. A kockázati vezető szerepkört betöltő személy kinevezése elősegíti, hogy a kockázatok a szervezet egészére kiterjedő szemszögből kerüljenek áttekintésre és elemzésre, valamint azt, hogy a kockázatkezelés az egész szervezeten belül következetes legyen.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell jelölnie egy kockázatkezelésért felelős személyt.
2. A szervezetnek ki kell jelölnie egy kockázati vezetőt.
3. A kockázatkezelésért felelős személynek és a kockázati vezetőnek együtt kell működniük, hogy biztosítsák a szervezeti kockázatkezelési folyamatok integrálását a szervezet összes releváns folyamatába.
4. A kockázatkezelésért felelős személynek és a kockázati vezetőnek rendszeresen dokumentálniuk kell a kockázatkezelési tevékenységeket, beleértve a kockázatok azonosítását, értékelését, kezelését és monitorozását.
5. A szervezetnek biztosítania kell, hogy a kockázatkezelésért felelős személy és a kockázati vezető rendelkezzen a szükséges képesítéssel, erőforrásokkal és támogatással a feladataik eredményes végrehajtásához.

6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kockázatkezelési folyamatokat, hogy biztosítsa azok hatékonyságát és relevanciáját a változó kockázati környezetben.

Kapcsolódó intézkedések

1.2. Elektronikus információs rendszerek biztonságáért felelős személy

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

5.1; 5.2; 5.3; 9.3.1; A.5.2

NIST SP 800-53 rev.5 referencia

PM-29

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

1.21. ELLÁTÁSI LÁNC KOCKÁZATMENEDZSMENT STRATÉGIÁJA

1.21. A szervezet:

1.21.1. Kidolgoz egy a szervezet egészére kiterjedő, az ellátási lánc kockázatainak kezelésére vonatkozó stratégiát az EIR-ek, rendszerelemek és rendszerszolgáltatások fejlesztésével, beszerzésével, karbantartásával, üzemeltetésével és selejtezésével kapcsolatosan.

1.21.2. Következetesen alkalmazza az ellátási lánc kockázatmenedzsment stratégiáját minden szervezeti egységében.

1.21.3. A változások lekövetésére az általa meghatározott gyakorisággal rendszeresen felülvizsgálja és frissíti az ellátási lánc kockázatmenedzsment stratégiáját.

MAGYARÁZAT

Az egész szervezetre kiterjedő ellátási lánc kockázatainak kezelésére vonatkozó stratégia tartalmazza a szervezet ellátási láncra vonatkozó kockázattűrésének egyértelmű kifejezését, az elfogadható ellátási lánc kockázatcsökkentési stratégiákat vagy védelmi intézkedéseket, az ellátási láncból fakadó kockázatok következetes értékelésére és nyomon követésére szolgáló folyamatot, az ellátási lánc kockázatkezelési stratégia végrehajtására és kommunikációjára vonatkozó megközelítéseket, valamint a kapcsolódó szerep- és felelősségi köröket. Az ellátási láncra vonatkozó kockázatkezelés magában foglalja az EIR-ek, rendszerelemek és rendszerszolgáltatások fejlesztésével, beszerzésével, karbantartásával és selejtezésével kapcsolatos biztonsági kockázatok figyelembevételét. Az ellátási lánc kockázatkezelési stratégiája beépíthető a szervezet átfogó kockázatkezelési stratégiájába, iránymutató és tájékoztató jellegű lehet az ellátási láncra vonatkozó irányelvek és a rendszerszintű ellátási lánc kockázatkezelési tervek tekintetében. Ezen túlmenően ezen kockázatkezelési funkció alkalmazása elősegítheti az ellátási lánc kockázatkezelési stratégiájának következetes, az egész szervezetre kiterjedő alkalmazását. Az ellátási láncra vonatkozó kockázatkezelési stratégiát szervezeti, valamint üzleti funkciók szintjén hajtják végre, míg az ellátási lánc kockázatkezelési tervek rendszerszinten kerülnek végrehajtásra.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet kidolgoz egy, az egész szervezetre kiterjedő ellátási láncra vonatkozó kockázatkezelési stratégiát.
2. A szervezetnek meg kell fontolnia, hogy az ellátási láncra vonatkozó kockázatkezelési stratégiát beépíti a szervezeti kockázatkezelési stratégiájába.
3. A szervezetnek meg kell különböztetnie az ellátási lánc kockázatkezelési stratégiát, amelyet a szervezeti és üzleti folyamatok szintjén kell végrehajtania, valamint az ellátási lánc kockázatkezelési terveit, amelyeket az EIR-ek szintjén.
4. A szervezet rendszeresen felülvizsgálja és frissíti az ellátási lánc kockázatkezelési stratégiáját a változások nyomon követése érdekében az általa meghatározott gyakorisággal.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.47. A szoftverhasználat korlátozásai

1.10. Kockázatkezelési stratégia

19.1. Szabályzat és eljárásrendek

19.2. Ellátási láncra vonatkozó kockázatkezelési szabályzat

19.4. Ellátási láncra vonatkozó követelmények és folyamatok

19.8. Rendszerelemek és kapcsolódó adatok eredetisége

19.13. Beszerzési stratégiák, eszközök és módszerek

19.16. Beszállítók értékelése és felülvizsgálata

19.18. Ellátási lánc működésbiztonsága (OPSEC)

19.19. Értesítési megállapodások

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

4.4; 6.2; 7.5.1; 7.5.2; 7.5.3

NIST SP 800-53 REV.5 REFERENCIA

PM-30

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

1.22. ELLÁTÁSI LÁNC KOCKÁZATMENEDZSMENT STRATÉGIA – ÜZLETMENET (ÜGYMENET) SZEMPONTJÁBÓL KRITIKUS TERMÉKEK BESZÁLLÍTÓI

1.22. A szervezet azonosítja, rangsorolja és értékeli azokat a beszállítókat, amelyek a szervezet működése szempontjából kritikus technológiákat, termékeket és szolgáltatásokat szállítanak a szervezet alapvető feladatainak ellátásához.

MAGYARÁZAT

Az egész szervezetre kiterjedő ellátási lánc kockázatainak kezelésére vonatkozó stratégia tartalmazza a szervezet ellátási láncra vonatkozó kockázattűrésének egyértelmű kifejezését, az elfogadható ellátási lánc kockázatcsökkentési stratégiákat vagy védelmi intézkedéseket, az ellátási láncból fakadó kockázatok következetes értékelésére és nyomon követésére szolgáló folyamatot, az ellátási lánc kockázatkezelési stratégia végrehajtására és kommunikációjára vonatkozó megközelítéseket, valamint a kapcsolódó szerep- és felelősségi köröket. Az ellátási láncra vonatkozó kockázatkezelés magában foglalja az EIR-ek, rendszerelemek és rendszerszolgáltatások fejlesztésével, beszerzésével, karbantartásával és selejtezésével kapcsolatos biztonsági kockázatok figyelembevételét. Az ellátási lánc kockázatkezelési stratégiája beépíthető a szervezet átfogó kockázatkezelési stratégiájába, iránymutató és tájékoztató jellegű lehet az ellátási láncra vonatkozó irányelvek és a rendszerszintű ellátási lánc kockázatkezelési tervek tekintetében. Ezen túlmenően ezen kockázatkezelési funkció alkalmazása elősegítheti az ellátási lánc kockázatkezelési stratégiájának következetes, az egész szervezetre kiterjedő alkalmazását. Az ellátási láncra vonatkozó kockázatkezelési stratégiát szervezeti, valamint üzleti funkciók szintjén hajtják végre, míg az ellátási lánc kockázatkezelési tervek rendszerszinten kerülnek végrehajtásra.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először azonosítania kell azokat a beszállítókat, akik a szervezet működése szempontjából kritikus technológiákat, termékeket és szolgáltatásokat szállítanak.

2. A szervezetnek rangsorolnia kell ezeket a beszállítókat a szervezet működésének szempontjából. Ez azt jelenti, hogy meg kell határozniuk, mely beszállítók termékei és/vagy szolgáltatásai nélkülözhetetlenek a szervezet alapvető feladatainak ellátásához.
3. A szervezetnek rendszeresen értékelnie kell a beszállítókat a beszállítói felülvizsgálatok segítségével.
4. A szervezetnek elemzést kell végeznie az ellátási lánc kockázatáról, hogy azonosítsa azokat az EIR-eket vagy rendszerelemeket, amelyeknél további ellátási lánc kockázatcsökkentő intézkedésekre van szükség.
5. A szervezetnek dokumentálnia kell a beszállítói felülvizsgálatokat és az ellátási lánc kockázatelemzési folyamatokat, hogy nyomon követhessék a kockázatok változásait és a kockázatcsökkentő intézkedések hatékonyságát.

Kapcsolódó intézkedések

15.4. Kockázatértékelés
19.16. Beszállítók értékelése és felülvizsgálata

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

PM-30(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

1.23. FOLYAMATOS FELÜGYELETI STRATÉGIA

1.23. A szervezet folyamatos felügyeleti stratégiát fejleszt ki és folyamatos felügyeleti programot működtet, amely magában foglalja:

1.23.1. Az egész szervezet számára teljesítménymutatók meghatározását.

1.23.2. A felügyelet és a hatékonyság-értékelés gyakoriságának meghatározását.

1.23.3. A teljesítménymutatók folyamatos, a felügyeleti stratégia szerint történő figyelemmel kísérését.

1.23.4. A felügyelet és az elvégzett értékelések adatai közötti összefüggések és információk elemzését.

1.23.5. A védelmi intézkedések értékelések és felügyeleti információk eredményéből származtatott válaszlépések megtételét.

1.23.6. Az EIR biztonsági állapotáról rendszeres időközönként, a kijelölt személyeknek történő jelentést.

MAGYARÁZAT

A szervezeti szinten történő folyamatos felügyelet elősegíti, hogy a szervezetnek folyamatos és valós képe legyen a szervezet biztonsági állapotáról, ezzel támogatva a szervezet kockázatkezelési döntéseit. A folyamatos kifejezés azt jelenti, hogy a szervezetek a kockázatalapú döntések támogatásához megfelelő gyakorisággal értékelik és monitorozzák a védelmi intézkedéseket és a kapcsolódó kockázatokat. A különböző típusú védelmi intézkedések eltérő felügyeleti gyakoriságot igényelhetnek. A folyamatos felügyelet eredményei iránymutatást adnak és támogatják a szervezetek kockázatkezelési válaszait (intézkedéseit). A folyamatos felügyeleti programok lehetővé teszik a szervezetek számára, hogy a védelmi intézkedéseket a változó működési célokkal és üzleti igényekkel, fenyegetésekkel, sérülékenységekkel és technológiákkal jellemezhető, rendkívül dinamikus működési környezetekben is fenntartsák. A biztonsággal kapcsolatos információkhoz való folyamatos hozzáférés a jelentéseken keresztül biztosítja a szervezet vezetői számára a hatékony, gyors és megalapozott kockázatkezelési döntések meghozatalának képességét, beleértve a folyamatos jóváhagyási döntéseket is. A kockázatok kezelésének további megkönnyítése érdekében a szervezet fontolóra veszi a szervezet által meghatározott

felügyeleti mérőszámok összehangolását a kockázatkezelési stratégiában meghatározott kockázattűréssel.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia egy stratégiát, amely meghatározza a felügyeleti tevékenységek gyakoriságát és módszereit, valamint a mérőszámokat, amelyek alapján a felügyeleti tevékenységek hatékonyságát értékelik.
2. A szervezetnek fen kell tartania kell egy programot, amely a felügyeleti stratégia szerint folyamatosan figyelemmel kíséri a mérőszámokat.
3. A szervezetnek elemeznie kell a felügyeleti és vizsgálati adatok közötti összefüggéseket, hogy meghatározza a védelmi intézkedések hatékonyságát.
4. A szervezetnek válaszlépéseket kell tennie a védelmi intézkedések értékelése és a felügyeleti információk eredményei alapján.
5. A szervezetnek rendszeres időközönként jelentést kell készítenie az EIR biztonsági állapotáról a kijelölt személyek számára.
6.A szervezetnek dokumentálnia kell a folyamatos felügyeleti tevékenységeket, hogy nyomon követhető legyen a felügyeleti tevékenységek hatékonysága és a védelmi intézkedések hatékonysága.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés
2.60. Legkisebb jogosultság elve
2.100. Távoli hozzáférés
3.13. A biztonsági képzésre vonatkozó dokumentációk
4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel
4.44. Információk kiszivárgásának figyelemmel kísérése
5.2. Biztonsági értékelések
5.9. Az intézkedési terv és mérföldkövei
5.11. Engedélyezés
5.14. Folyamatos felügyelet

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

4.4; 6.2; 7.4; 7.5.1; 7.5.2; 7.5.3; 9.1; 9.2.2; 10.1; 10.2

NIST SP 800-53 REV.5 REFERENCIA

PM-31

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024