Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Előkészületek

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

1. A kockázatmenedzsment keretrendszer 3

1.1. Kockázatmenedzsment keretrendszer kialakítása és működtetése 3

2. Felkészülés a kockázatmenedzsment keretrendszer kialakítására 4

2.1. Kiberbiztonsági szerepek, felelősségek és hatáskörök meghatározása 4

2.2. A kockázatmenedzsment stratégia kialakítása 5

2.3. A folyamatos ellenőrzésre vonatkozó biztonságfelügyeleti stratégia 6

2.4. Rendszerszintű előkészítési feladatok 7

2.4.1. A rendszer üzleti céljának, funkciójának, rendszerelemeinek és érintettjeinek dokumentálása 7

2.4.2. Rendszerszintű kockázatértékelés 7

2.4.3. A rendszer szervezeti és technológiai határainak azonosítása 9

2.4.4. A rendszer helyének meghatározása a vállalati architektúrában 10

3. Biztonsági osztályba sorolás 11

3.1. A biztonsági osztályba sorolás menete 12

3.2. Fejlesztendő rendszerek előzetes biztonsági osztályba sorolása 14

3.3. A biztonsági osztály dokumentálása 15

4. Védelmi intézkedések testreszabása, helyettesítő védelmi intézkedések 16

5. A védelmi intézkedések végrehajtása 18

6. Védelmi intézkedések értékelése 20

7. A rendszerhasználat jóváhagyása 23

8. A biztonság folyamatos felügyelete 25

A KOCKÁZATMENEDZSMENT KERETRENDSZER

KOCKÁZATMENEDZSMENT KERETRENDSZER KIALAKÍTÁSA ÉS MŰKÖDTETÉSE

Az elektronikus információs rendszereket érintő fenyegetések megfelelő kezeléséhez a jogszabályi környezet által előírt kiberbiztonsági követelményeknek célszerűen le kell fedniük a rendszerek teljes életciklusát, támogatniuk kell a kiberbiztonsági kockázatkezelés szervezeti kereteinek kialakítását, meg kell határozniuk a védelmi intézkedésekkel kapcsolatos elvárásokat, valamint biztosítaniuk kell azok teljesülésének folyamatos felügyeletét. Ennek szellemében írja elő a vonatkozó jogszabály az érintett szervezetek számára a biztonsági osztályba sorolás és a védelmi intézkedések bevezetésének támogatására kockázatkezelési keretrendszer működtetését. A kockázatkezelési keretrendszer működtetésének a célja, hogy kiberbiztonsági tevékenységek

- átfogó, az egész szervezetre kiterjedő irányítással és a megfelelő erőforrásokkal rendelkezzenek,
- lehetővé tegyék a költséghatékony és következetes kockázatkezelési folyamatok végrehajtását az egész szervezetben,
- az egyes védelmi intézkedések arányosak legyenek a felmerülő kockázatokkal,
- a védelmi intézkedések kiválasztása, megvalósítása, folyamatos felügyelete egy szisztematikus, strukturált és átlátható folyamatként épüljön bele a szervezeti működésbe.

A kockázatkezelési keretrendszer a fenti célokon keresztül szervesen összekapcsolja a kiberbiztonság vezetői szintű irányítási feladatait és a védelmi intézkedések rendszerszintű operatív feladatait. Kialakítása és működtetése ciklikusan egymást követő, szisztematikusan végrehajtott lépéseken keresztül valósítható meg, amely lépéseket az alábbiakban részletezzük.

FELKÉSZÜLÉS A KOCKÁZATMENEDZSMENT KERETRENDSZER KIALAKÍTÁSÁRA

A kockázatkezelési keretrendszer működtetésére való felkészülésnek vannak szervezeti szintű, illetve rendszerszintű feladatai. Ezeknek a feladatoknak a célja végső soron az, hogy biztosítsák a szükséges információkat és erőforrásokat a szervezet céljait érintő, a rendszerek üzemeltetéséből és használatából eredő kiberbiztonsági kockázatok sikeres kezeléséhez. A felkészülési lépések támogatják az erőforrások azonosítását, rangsorolását, a szervezeti kommunikációt, a védelmi intézkedések hatékonyabb kialakítását, és következetes végrehajtásuk csökkentheti a rendszerfejlesztés és a vagyonvédelem költségeit. A kockázatkezelési keretrendszer szervezeti szintű előkészítő feladatai a teljes szervezeti működésre vannak hatással. Ezeket a feladatokat röviden az alábbiakban ismertetjük:

KIBERBIZTONSÁGI SZEREPEK, FELELŐSSÉGEK ÉS HATÁSKÖRÖK MEGHATÁROZÁSA

Az információs rendszerek védelmével kapcsolatos szerepek meghatározása segít kialakítani a szükséges struktúrát és irányítást a biztonsági folyamatok hatékony végrehajtásához. Ezzel a tevékenységgel a szervezet biztosítja, hogy mindenki tisztában legyen a felelősségével és az elvégzendő feladatokkal a biztonsági környezet megfelelő kezelése érdekében. Ennek keretében a szervezet meghatározza, hogy ki a felelős az egyes biztonsági területekért és feladatokért (például, ki felelős a kiberbiztonsági tevékenységek irányításáért, a biztonsági rendszerarchitektúráért, a hálózatbiztonságért, vagy éppen a felhasználói hozzáférés kezeléséért.) A biztonsági szerepkörök meghatározásával a szervezet kijelöli, hogy kik azok a személyek vagy csoportok, akiknek együtt kell működniük a biztonsági feladatok végrehajtásában és elősegíti a hatékony kommunikációt a különböző részlegek és szakterületek között, amelyek részt vesznek a biztonsági folyamatokban, illetve meghatározza, hogy a vezetőség milyen mértékben vesz részt a biztonsági döntéshozatalban és ellenőrzésben. A szerepek és felelősségek adott esetben magukban foglalhatják a szervezeten belüli vagy kívüli érintett személyeket is. Mivel a szervezetek különböző célokkal, funkciókkal és szervezeti struktúrákkal rendelkeznek, különbségek lehetnek a kockázatkezelési szerepkörök elnevezési konvencióiban és az egyes felelősségek szervezeti személyzet közötti elosztásában (pl. több

személy tölt be egy szerepet, vagy egy személy több szerepet tölt be). A szervezetnek biztosítania kell, hogy ne legyen összeférhetetlenség abban az esetben sem, ha ugyanazt a személyt több kockázatkezelési szerepkörhöz rendelik.

A KOCKÁZATMENEDZSMENT STRATÉGIA KIALAKÍTÁSA

A kockázatkezelési stratégia irányítja, befolyásolja a kockázatalapú döntéseket, beleértve a biztonsági kockázatok azonosítását, értékelését, reagálását és nyomon követését. A kockázatmenedzsment stratégia kialakítása olyan terv és irányelv kidolgozását jelenti, amely meghatározza, hogyan fogja az érintett szervezet azonosítani, értékelni, elfogadni vagy csökkenteni az informatikai rendszerek és folyamatok működtetése során észlelt kockázatokat. A kockázatkezelési stratégia kidolgozása segít a szervezetnek proaktívan kezelni a fenyegetéseket és azok hatásait az informatikai rendszerekre.

A kockázatkezelési stratégia állhat egyetlen dokumentumból, vagy különálló kockázatkezelési dokumentumokból. A kockázatkezelési stratégia azonosítja a fenyegetéseket, feltételezéseket, korlátokat, prioritásokat, kompromisszumokat és kockázattűrést. Ez a stratégia tartalmazza azokat a döntéseket és megfontolásokat, hogy a felső vezetők és vezetők hogyan kezeljék a szervezeti működésre, a szervezeti eszközökre, az egyénekre, más szervezetekre vonatkozó biztonsági kockázatokat, beleértve az ellátási lánc kockázatait is.

A kockázatkezelési stratégia magában foglalja

- a szervezeti kockázattűrés meghatározását;
- az elfogadható kockázatértékelési módszereket és kockázatreagálási stratégiákat;
- a biztonsági és adatvédelmi kockázatok szervezeti szintű következetes értékelésének folyamatát;
- valamint a kockázatok időbeli nyomon követését biztosító mechanizmusok meghatározását.

A kockázatkezelési stratégia, szabályzatok, eljárások és folyamatok meghatározásakor és végrehajtásakor fontos, hogy azok tartalmazzák a beszállítói lánccal kapcsolatos kockázatok kezelésére vonatkozó szempontokat is.

A FOLYAMATOS ELLENŐRZÉSRE VONATKOZÓ BIZTONSÁGFELÜGYELETI STRATÉGIA

A folyamatos ellenőrzés végső célja annak meghatározása, hogy a rendszerben lévő biztonsági intézkedések az idő múlásával is hatékonyak maradnak-e a rendszerben és a rendszer működési környezetében bekövetkező elkerülhetetlen változások fényében. A folyamatos nyomon követés hatékony mechanizmust biztosít a rendszerbiztonsági tervek, az értékelő jelentések, valamint a cselekvési tervek frissítéséhez. A folyamatos nyomon követési folyamat magában foglalja

- a szervezeti rendszerek konfigurációkezelési és ellenőrzési folyamatait,
- a rendszerek és működési környezetek tényleges vagy javasolt változtatásainak kockázatértékelését,
- a védelmi intézkedések működésének rendszeres értékelését,
- a szervezet biztonsági helyzetéért felelős szervezeti tisztviselők felé való jelentését.

A folyamatos ellenőrzésre vonatkozó biztonságfelügyeleti stratégiában dokumentálni kell a védelmi intézkedésekhez kapcsolódó tevékenységek ellenőrzésének gyakoriságát, felügyeletének módszereit és eszközeit. A biztonság felügyeleti stratégiák magukban foglalhatják az ellátási lánc kockázati szempontjait is, például a szállító esetleges külföldi tulajdonosának ellenőrzési tevékenységét vagy befolyásának rendszeres felülvizsgálatát, a készlet-előrejelzések nyomon követését vagy a beszállítók folyamatos biztonsági auditálásának megkövetelését.

A folyamatos ellenőrzésre vonatkozó biztonságfelügyeleti stratégia a szervezet, az üzleti folyamat és az információs rendszerek szintjén foglalkozik a felügyeleti követelményekkel és segít a szervezetnek átlátni az információs rendszereinek biztonsági helyzetét. Meghatározza a szervezeten belül kialakított és működtetett védelmi intézkedések minimális ellenőrzési gyakoriságát, és leírja, hogyan kell elvégezni az értékeléseket. Célszerű ezeket a felügyeleti, értékelési feladatokat valamilyen automatizmusokkal támogatni az erőforrások hatékony felhasználása végett.

RENDSZERSZINTŰ ELŐKÉSZÍTÉSI FELADATOK

Mint korábban említettük, a kockázatkezelési keretrendszer előkészítő feladatainak célja a szervezetet és annak céljait érintő, a rendszerek üzemeltetéséből és használatából eredő kiberbiztonsági kockázatok sikeres kezeléséhez szükséges információk és erőforrások biztosítása. Az egyes rendszerek üzleti céljának, érintettjeinek, rendszerelemeinek, határainak, az általa feldolgozott adatok körének meghatározásának és dokumentálásának fontos szerepe van a védelmi intézkedések hatékony tervezésében és megvalósításában.

A rendszer üzleti céljának, funkciójának, rendszerelemeinek és érintettjeinek dokumentálása

A rendszer üzleti céljainak, érdekeltjeinek tisztázása jelentős hatással lehet a vállalati architektúrák kialakítására. Egy rendszer érdekeltjei közé tartoznak azok a személyek, szervezetek, akiknek a rendszer teljes életciklusa során valamilyen érdeke fűződik a rendszer működtetéséhez – a rendszer tervezése, fejlesztése, megvalósítása, szállítása, üzemeltetése és fenntartása érdekében. Az érdekelt felek lehetnek azonos vagy különböző szervezetek tagjai, a szervezethez tartozó ellátási lánc szereplői. Az érdekeltek meghatározása segíti a felek közötti kommunikációt, a rendszerrel kapcsolatos felelősségek és hatáskörök meghatározását. A rendszerrel kapcsolatos vagyonelemek azonosítása elengedhetetlen a hatékony védelmi intézkedések kialakításához, hiszen ennek hiányában a szervezet nem tudja, hogy mit és milyen módon kell védeni.

Rendszerszintű kockázatértékelés

A jogszabály megkövetelheti, hogy a szervezetek a szervezeti szintű kockázatértékelés mellett rendszer szintű biztonsági kockázatértékeléseket végezzenek annak érdekében, hogy minden kockázattípus teljeskörűen értékelve legyen. A biztonsági kockázat értékelése magában foglalja

- a vagyonelemeket érintő fenyegetésforrások és fenyegető események azonosítását,
- annak felmérését, hogy az eszközök sebezhetőek-e a fenyegetésekkel szemben, és ha igen, milyen módon,
- annak valószínűségének meghatározását, hogy egy eszköz sérülékenységét egy fenyegetés milyen módon képes kihasználni,
- valamint a vagyonelemek elvesztésének hatását (vagy következményét).

A kockázatértékelés kulcsfontosságú részeként a vagyonelemeket a fenyegetések káros hatása

vagy a vagyonelemek esetleges elvesztésének következménye alapján rangsorolják. A veszteség mibenlétét minden egyes vagyonelemtípusra vonatkozóan meg kell határozni, hogy lehetővé tegye a következmények (azaz a veszteség káros hatásának) meghatározását. A veszteség következményei lehetnek kézzelfoghatóak (pl. anyagi veszteség, eszközök sérülése) vagy nem kézzelfoghatóak (pl. hírnév romlása), és az eszközhöz viszonyítva a részleges veszteségtől a teljes veszteségig terjedő kontinuumot alkotnak. Az információvesztés értelmezései közé tartozhat például a birtoklás elvesztése, a megsemmisülés, vagy a pontosság elvesztése. A funkció vagy szolgáltatás elvesztése értelmezhető az irányítás elvesztéseként, a hozzáférhetőség elvesztéseként, a normál funkció, teljesítmény vagy viselkedésre való képesség elvesztéseként vagy a képesség korlátozott elvesztéseként, amely a funkció, teljesítmény vagy viselkedés bizonyos szintű romlását eredményezi.

Ipari rendszerek esetén a fenyegetettség fizikai következményei közé tartozhat a termelés nem tervezett leállása, az ipari berendezések károsodása, a helyszínen bekövetkező balesetek, környezeti katasztrófák és a közbiztonság veszélyeztetése. A vagyonelemek rangsorolása azok értéke, a fizikai következmények, a pótlás költségei, a kritikusság, az imázsra vagy a hírnévre gyakorolt hatás stb. alapján történik. Az egyes rendszerek fontossági sorrendjének meghatározása befolyásolja az erőforrások elosztását, a védelmi mechanizmusok erősségét és a megbízhatósági szinteket.

Kockázatértékeléseket annak megállapítására is célszerű végezni, hogy egy külső szolgáltató igénybevétele egy rendszer, rendszerelem vagy szolgáltatás fejlesztésére, bevezetésére, karbantartására, kezelésére, üzemeltetésére vagy megszüntetésére okozhat-e kárt a szervezetnek, és hogy ez milyen hatással járhat. A hatás lehet azonnali (pl. fizikai lopás) vagy folyamatos (pl. a lopás következményeként megszerzett képesség a kritikus eszközök lemásolására). A hatás lehet endemikus (pl. egyetlen rendszerre korlátozódó) vagy rendszerszintű (pl. minden olyan rendszerre kiterjedő), amely egy adott típusú rendszerelemet használ).

Az ellátási lánccal kapcsolatos kockázatértékeléseknek figyelembe kell venniük azokat a sérülékenységeket, amelyek egy rendszer vagy rendszerelem rendelkezésre bocsátásával és külső szolgáltatók igénybevételével kapcsolatban merülhetnek fel. Az ellátási lánc sebezhetőségei közé tartozhat a nyomon követhetőség vagy az elszámoltathatóság hiánya. A

külső szolgáltatók igénybevétele a rendszerek, rendszerelemek és szolgáltatások fejlesztésének, telepítésének és karbantartásának módja feletti átláthatóság és ellenőrzés elvesztését eredményezheti. A fenyegetések, sebezhetőségek és az ellátási láncban történt kedvezőtlen esemény lehetséges hatásainak világos megértése segíthet a szervezeteknek abban, hogy megfelelően egyensúlyba hozzák az ellátási lánc kockázatokat a szervezeti kockázattűréssel.

Az információs rendszer szintű kockázatértékelés rendkívül fontos a kiberbiztonság területén, mivel segít azonosítani, értékelni és kezelni az esetleges veszélyeket és fenyegetéseket, amelyek az információs rendszert érinthetik. A rendszeres kockázatértékelések elengedhetetlenek ahhoz, hogy a szervezet időben felismerje és hatékonyan kezelje az információs rendszerét érő kockázatokat. A folyamatos monitorozás és értékelés lehetővé teszi a rugalmas reagálást a változó kockázati környezetre. A kockázatértékelés eredményeit felhasználják

- a biztonsági követelmények meghatározásához;
- a biztonsági osztályba sorolási döntésekhez;
- a védelmi intézkedések kiválasztásához, testre szabásához, végrehajtásához és értékeléséhez;
- az engedélyezési döntésekhez;
- a cselekvési tervek kialakításához és a védelmi intézkedések prioritásainak meghatározásához;
- valamint a folyamatos biztonságfelügyeleti stratégia kialakításához.

Bár a jogszabály leírja a kockázatértékelési folyamat elvárt főbb lépéseit és a figyelembe veendő fenyegetettségeket, a szervezet jelentős szabadságot élvez a kockázatértékelés formájának meghatározásában (beleértve az ilyen értékelések terjedelmét, szigorúságát és formalitását) és az eredmények jelentésének módját.

A rendszer szervezeti és technológiai határainak azonosítása

A rendszer szervezeti és technológiai határai meghatározzák az információs rendszerek védelmének hatókörét, azaz azt, hogy a szervezetnek mit kell megvédenie az által biztosított menedzsment égisze alatt, illetve felelősségi körén belül. A rendszer szervezeti és technológiai határainak egyértelmű meghatározása fontos az elszámoltathatóság és a biztonsági osztályba sorolás szempontjából, különösen olyan helyzetekben, amikor az alacsonyabb hatású

rendszerek nagyobb hatású rendszerekhez kapcsolódnak, vagy amikor külső szolgáltatók felelősek a rendszer üzemeltetéséért vagy karbantartásáért. A rendszerhatárok tisztázása befolyásolhatja a védelmi intézkedések megvalósítását. A részben vagy egészben külső szolgáltatók által kezelt, karbantartott vagy üzemeltetett rendszerek esetében a rendszerhatárokat egyértelműen leíró megállapodás biztosítja az elszámoltathatóságot. A külső szolgáltatókkal kötött szerződések felhasználhatók annak meghatározására, hogy mi minősül rendszerhatárnak. Az ilyen határok ismerete megkönnyíti az ellátási lánc kockázatának kezelésére szolgáló védelmi intézkedések kiválasztását.

A rendszer helyének meghatározása a vállalati architektúrában

A vállalati architektúra olyan irányítási gyakorlat, amelyet az üzleti folyamatok és az információs erőforrások hatékonyságának maximalizálására, valamint az üzleti célok elérésére használnak. A vállalati architektúra az információs rendszerek tervezése és fejlesztése során alkalmazott információs és működési technológiák jobb megértését biztosíthatja. Előfeltétele annak, hogy a rendszerek ellenálló képességét és túlélőképességét az egyre kifinomultabb fenyegetések környezetében is tartani vagy akár növelni lehessen. A vállalati architektúra lehetőséget nyújt az információs és technológiai eszközök konszolidálására, szabványosítására és optimalizálására is. A hatékonyan megvalósított architektúra olyan rendszereket hoz létre, amelyek átláthatóbbak, és ezért könnyebben érthetők és védhetők. A vállalati architektúra emellett egyértelmű kapcsolatot teremt a beruházások és a mérhető teljesítményjavulás között.

A rendszer elhelyezése a vállalati architektúrában azért fontos, mert nagyobb átláthatóságot és megértést biztosít a rendszerhez kapcsolódó más (belső és külső) rendszerekről, és a rendszer védelmi szintjének fokozása érdekében biztonsági tartományok létrehozására is felhasználható. A biztonsági architektúra a vállalati architektúra biztonsági követelmények végrehajtásához kapcsolódó része. A biztonsági architektúra elsődleges célja annak biztosítása, hogy a vonatkozó biztonsági követelmények következetesen és költséghatékonyan teljesüljenek a szervezet rendszereiben, és összhangban legyenek a kockázatkezelési stratégiával.

BIZTONSÁGI OSZTÁLYBA SOROLÁS

Az információs rendszerek védelmére fordított kiadásoknak arányosnak kell lenniük a felmerülő kockázatokkal, azaz csak a lehetségesen bekövetkező veszteségek és károk nagyságrendjével arányosan indokolt a védelemre költeni. Az információs rendszer védelmének kialakítására és fenntartására fordított költségek mértékét a kezelt adatok, valamint az rendszer elemei bizalmasságának, sértetlenségének vagy rendelkezésre állásának elvesztésével okozott károk meghatározását követően lehet megállapítani. A biztonsági osztályba sorolás tulajdonképpen az információs rendszernek a kockázatok figyelembevételére épülő elvárt védelmi erősségének meghatározása. A kockázatkezelési keretrendszer által meghatározott ciklikus folyamat a biztonsági osztályba sorolással kezdődik, amely befolyásolja a keretrendszer összes többi lépését. A biztonsági osztályba sorolás esetleges hibája a szervezet rendszereihez tartozó túlzó vagy elégtelen védelmi intézkedések alkalmazását eredményezheti. A rendszer biztonságával kapcsolatos minden további kockázatkezelési döntést a biztonsági osztályba sorolás határoz meg. Ez a döntés befolyásolja az alkalmazandó védelmi intézkedések körét, a kapcsolódó dokumentációs elvárásokat, a védelmi intézkedések végrehajtásának részleteit, azok értékelésekre fordítandó erőforrásokat, az engedélyezési döntéseket, a folyamatos nyomon követés gyakoriságát, valamint a folyamatos kockázatértékelést.

A biztonsági osztályba sorolás strukturált eljárást biztosít a rendszer által feldolgozott, tárolt és továbbított adatok kritikusságának meghatározására. Az osztályozás lépéseinek célja, hogy meghatározzák a szervezeti rendszerek és adatok bizalmasságának, sértetlenségének és rendelkezésre állásának elvesztése által a szervezetre gyakorolt káros hatásokat. A folyamatlépések követése a rendszer biztonsági osztályának azonosítását eredményezi, amely a szervezetre gyakorolt potenciális káros hatás mérlegelésén alapul, ha olyan események következnek be, amelyek veszélyeztetik a szervezet üzleti céljainak teljesítéséhez, vagyonelemeinek és személyi állományának védelméhez, jogi kötelezettségeinek teljesítéséhez és mindennapi funkcióinak fenntartásához szükséges információkat és rendszereket. A biztonsági osztályba sorolási döntés meghozatala előtt a rendszer által feldolgozott, tárolt és továbbított adatok típusainak azonosítását kell elvégezni. Hasonlóképpen, az adattípusok azonosítása mellett minden egyes azonosított típus esetében az adat életciklusának minden egyes szakaszát is tudni kell azonosítani. A biztonsági osztályba sorolás elősegíti az

információbiztonsági programok hatékony irányítását és felügyeletét, beleértve az információbiztonsági erőfeszítések hatóság általi koordinálását, valamint az információbiztonsági szabályozások, eljárások és gyakorlatok megfelelőségéről és hatékonyságáról szóló jelentéstételt.

A BIZTONSÁGI OSZTÁLYBA SOROLÁS MENETE

Az adatgazda vagy az érintett rendszer biztonságáért felelős személy azonosítja a rendszer által feldolgozott, tárolt és továbbított adatok típusait. (Az adatgazda annak a szervezeti egységnek a vezetője, ahová a jogszabály vagy közjogi szervezetszabályzó eszköz az adat kezelését rendeli, illetve, ahol az adat keletkezik.) Ezután mind az adatok, mind a rendszer tekintetében vizsgálja a bizalmasság, sértetlenség vagy rendelkezésre állás hatásértékét (alap, jelentős, magas).

Az „alap" biztonsági osztály esetében legfeljebb csekély káresemény következhet be, mivel:

- az elektronikus információs rendszerben jogszabály által nem védett adat vagy legfeljebb kis mennyiségű személyes adat sérülhet,
- a szervezet üzleti vagy ügymenete szempontjából csekély értékű, vagy csak belső (szervezeti) szabályzóval védett adat vagy rendszer sérülhet,
- a lehetséges társadalmi-politikai hatás a szervezeten belül kezelhető,
- a közvetlen és közvetett anyagi kár a szervezet éves költségvetésének vagy nettó árbevételének 1%-át nem haladja meg.

A „jelentős" biztonsági osztály esetében közepes káresemény következhet be, mivel:

- nagy mennyiségű személyes adat, illetve különleges személyes adat sérülhet,
- személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket),
- a szervezet üzleti vagy ügymenete szempontjából érzékeny folyamatokat kezelő rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet,
- a káresemény lehetséges társadalmi-politikai hatásai a szervezettel szemben bizalomvesztést eredményezhetnek, a jogszabályok betartása, vagy végrehajtása elmaradhat, vagy a szervezet vezetésében személyi felelősségre vonást kell alkalmazni,

- a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 1%-át, de nem haladja meg annak 10%-át.

A „magas” biztonsági osztály esetében nagy káresemény következhet be, mivel

- különleges személyes adat nagy mennyiségben sérülhet,
- emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be,
- nemzeti adatvagyon helyreállíthatatlanul megsérülhet,
- az ország, a társadalom működőképességének fenntartását biztosító kritikus infrastruktúra rendelkezésre állása nem biztosított,
- a szervezet üzleti vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet,
- súlyos bizalomvesztés állhat elő a szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok is sérülhetnek,
- a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 10%-át.

A biztonsági osztály (BO) kifejezésére szolgáló általános formátum a következő:

BO = MAX{(bizalmasság, hatás), (sértetlenség, hatás), (rendelkezésre állás, hatás)},

ahol a lehetséges hatás elfogadható értékei *alap*, *jelentős* vagy *magas*. A kapott hatásértékeket a maximum elv alapján összesíteni kell, úgy, hogy az adatok vagy rendszerek bizalmasság, sértetlenség és rendelkezésre állás szerinti hatásértékeit nem átlagolják, hanem azok maximumát veszik. A rendszerek biztonsági osztályát összevonva a bizalmasság, sértetlenség, rendelkezésre állás hármasból a legnagyobb érték adja meg.

Bár a biztonsági osztályba sorolás elsődlegesen az adatgazda felelőssége, abba, az egész szervezetre kiterjedő tevékenységként, be kell vonni a felső vezetést, az információs rendszerek biztonságáért felelős személyt és a szervezet adatvédelmi tisztviselőjét. A biztonsági osztályba sorolás eredményét az érintett szervezet vezetőjének kell jóváhagynia. A szervezet vezetője felel azért, hogy az EIR biztonsági osztályának meghatározása megfeleljen a jogszabályoknak és kockázatoknak, valamint a besorolásban felhasznált adatok teljeskörűek. Felülvizsgálja a

biztonsági osztályba sorolás eredményét és együttműködik a felsővezetőkkel annak biztosítása érdekében, hogy a rendszerre vonatkozó biztonsági osztályba sorolási döntés összhangban legyen a szervezeti kockázatkezelési stratégiával. A felső vezetés részvétele a biztonsági osztályba sorolási folyamatban elengedhetetlen ahhoz, hogy a kockázatkezelési keretrendszer hatékony és következetes módon valósulhasson meg az egész szervezetben.

A biztonsági osztályba sorolás más módszertanon alapuló hatáselemzés alapján is elvégezhető, ebben az esetben az eredményhez mellékelni kell a módszertan részletes leírását is.

Fejlesztendő rendszerek előzetes biztonsági osztályba sorolása

A követelmények meghatározása minden rendszerfejlesztési folyamat kritikus része, és az életciklus nagyon korai szakaszában, jellemzően a kezdeményezési fázisban kezdődik. A biztonsági és adatvédelmi követelmények a rendszerrel szemben támasztott általános funkcionális és nem funkcionális követelmények egy részhalmazát képezik, és a funkcionális és nem funkcionális követelményekkel egyidejűleg épülnek be a rendszerfejlesztési életciklusba. A biztonsági követelmények korai integrálása nélkül a szervezetnek az életciklus későbbi szakaszában jelentős költségei merülhetnek fel olyan biztonsági és adatvédelmi szempontok kezelése miatt, amelyeket már a kezdeti tervezés során is figyelembe lehetett volna venni. Ha a biztonsági követelményeket a többi rendszerkövetelmény szerves részhalmazának tekintik, akkor az így létrejövő rendszer nagy valószínűséggel kevesebb gyenge ponttal, kevesebb kihasználható sebezhetőséggel rendelkezik. Az adatok és az információs rendszer előzetes biztonsági osztályba sorolása a rendszerfejlesztés kezdeti szakaszában történik, az előzetes biztonsági kockázatértékeléssel (hatáselemzéssel) együtt. A kezdeti kockázatértékelés meghatározza azt a fenyegetettségi környezetet, amelyben a rendszer működik, és tartalmazza a rendszer alapvető biztonsági igényeinek leírását. Ezek az igények annak megértésétől függenek, hogy a rendszer valamely összetevője bizalmasságának, sértetlenségének vagy rendelkezésre állásának lehetséges elvesztése hogyan hathat a szervezetre és az ebből ered a rendszer biztonsági osztályba sorolása.

A rendszer használatba vételét követően a szervezet rendszeresen felülvizsgálja a kockázatkezelési keretrendszerben leírt kockázatkezelési tevékenységeket, beleértve a rendszer biztonsági osztályba sorolását is. Ezen túlmenően az üzleti, a szervezeti és technológiai környezetben történt változások szükségessé tehetik a rendszer biztonsági állapotának azonnali

újraértékelését. Biztonsági esemény bekövetkezése szintén indokolhatja a rendszer biztonsági osztályának, és a bevezetett védelmi intézkedéseknek a felülvizsgálatát, , annak érdekében, hogy az érintett rendszer védelme összhangban legyen a szervezeti célokkal. Egy adattípusok biztonsági hatásértékei a rendszer életciklusa során változhatnak. Például az olyan szerződéses információ, amely a szerződés életciklusa alatt „jelentős” bizalmassági hatásértékkel rendelkezik, a szerződés lezárásakor „alap” hatásértékkel rendelkezhet. Ezeket a rendszer éltciklus váltásainál – pl. archív állapotba átvezetés – célszerű figyelembe venni. A jogszabályok egyes adattípusokra további követelményeket is támaszthatnak. Emiatt a biztonsági osztályba sorolást folyamatosan felül kell vizsgálni annak érdekében, hogy az tükrözze az aktuális szervezeti környezetet és prioritásokat.

A BIZTONSÁGI OSZTÁLY DOKUMENTÁLÁSA

Az adatgazda vagy az elektronikus információs rendszer biztonságáért felelős személy a rendszer biztonsági osztályát a rendszerbiztonsági tervben dokumentálja, amelyben a végleges osztályozási döntésen (azaz a rendszer biztonsági hatásszintjén) kívül a biztonsági osztályba sorolást alátámasztó indoklást is szerepeltetni kell.

VÉDELMI INTÉZKEDÉSEK TESTRESZABÁSA, HELYETTESÍTŐ VÉDELMI INTÉZKEDÉSEK

Az elektronikus információs rendszerek biztonsági osztályaihoz a jogszabály meghatározza azokat a védelmi intézkedéseket, amelyeket a szervezetnek be kell építenie a működésébe a rendszerek biztonsági környezetének kialakításához. A szervezet indokolt esetben eltérhet az információs rendszerek biztonsági osztálya alapján megállapított védelmi intézkedésektől. A rendszer biztonságáért felelős személy végzi a védelmi intézkedésektől való eltérések kezelését, a helyettesítő intézkedések meghatározását, és az azokra vonatkozó információk rögzítését a rendszerbiztonsági tervekben. A rendszer biztonságáért felelős személy az adatvédelmi tisztviselővel együtt felelős a rendszerbiztonsági tervek kidolgozásáért, karbantartásáért, valamint biztosítja, hogy a rendszert az elfogadott védelmi intézkedéseknek megfelelően telepítsék és üzemeltessék. Az eltéréseket tartalmazó dokumentumot a szervezet vezetője vagy a kockázatok felvállalására jogosult szerepkört betöltő személy hagyja jóvá.

A szervezet csak akkor alkalmazhat helyettesítő intézkedést, ha a jogszabályban szereplő védelmi intézkedések katalógusa nem tartalmaz az adott viszonyok között eredményesen és kockázatarányosan alkalmazható intézkedést. Erre akkor lehet szükség, ha a rendszer nagyon speciális (pl. fegyverrendszer vagy orvosi eszköz) vagy korlátozott céllal vagy hatókörrel rendelkezik (pl. intelligens fogyasztásmérő). A helyettesítő védelmi intézkedés olyan védelmi intézkedés, amely a helyettesítettel egyenértékű vagy összemérhető szintű védelmet biztosít egy rendszer vagy szervezet számára. Bizonyos esetekben a helyettesítéshez több védelmi intézkedésre lehet szükség. A helyettesítő védelmi intézkedéseket jellemzően azután választják ki, hogy a vonatkozó védelmi intézkedéseket költség-hasznon elemzés vagy kockázatértékelés során elemezték. A szervezet alkalmazhat eltéréseket vagy helyettesítő védelmi intézkedéseket, ha nem képes az megadott védelmi intézkedéseket végrehajtani, vagy ha azok a rendszer vagy a működési környezet sajátosságai miatt nem képesek kockázatok költséghatékony csökkentésére.

Az elvárt biztonsági szint biztosításához szükséges megfelelő védelmi intézkedések végső meghatározása a szervezet kockázatértékelésének, valamint annak függvénye, hogy mi szükséges a kockázatok megfelelő csökkentéséhez. Sok esetben további védelmi

intézkedésekre vagy kiegészítő tevékenységekre lehet szükség a biztonsági igények teljesítéséhez. Az eltéréseket és a helyettesítő védelmi intézkedéseket, valamint a kiválasztási döntések és a rendszerhasználati korlátozások alátámasztó indoklását a rendszerbiztonsági tervekben kell rögzíteni. A jelentős kockázatkezelési döntések rögzítése a rendszerbiztonsági tervekben elengedhetetlen ahhoz, hogy az engedélyezésre jogosult tisztviselők rendelkezzenek a rendszerek engedélyezésével kapcsolatos információkkal a hiteles, kockázatalapú döntések meghozatalához.

A rendszerbiztonsági tervek áttekintést kell, hogy nyújtsanak a rendszerre vonatkozó biztonsági követelményekről, és le kell, hogy írják a biztonsági és adatvédelmi követelmények teljesítése érdekében alkalmazott vagy tervezett intézkedéseket. Kellően részletesnek kell lenniük ahhoz, hogy megállapítható legyen, hogy a védelmi intézkedések megfelelnek-e a követelményeknek. A rendszerre vonatkozó leíró információkat a kockázatkezelési keretrendszer kialakításának felkészülési szakaszában rögzítik (lásd az előző pontokat), amelyek a rendszerbiztonsági tervek fejezeteként vagy mellékleteként szerepelnek, vagy a rendszerfejlesztési folyamat részeként keletkező információk más dokumentumaiban hivatkoznak rájuk. Az információk megkettőzését lehetőség szerint úgy kerüljük el, hogy a rendszerbiztonsági tervekben nem ismételjük meg ugyanazokat az információkat, amelyek más dokumentumokban szerepelnek, hanem hivatkozásokat vagy utalásokat adunk meg az alátámasztó információkra. A rendszerfejlesztési ciklus és a kockázatkezelési keretrendszer feladatainak végrehajtása során el kell végezni a rendelkezésre álló új információk hozzáadását és a meglévő információk módosítását.

A VÉDELMI INTÉZKEDÉSEK VÉGREHAJTÁSA

A védelmi intézkedések végrehajtása magában foglalja új folyamatok, eljárások, termékek és szolgáltatások kialakítását vagy meglévő folyamatok, eljárások, termékek és szolgáltatások felhasználását a biztonsági követelmények teljesítése érdekében. A rendszerbiztonsági tervek útmutatóként szolgálnak a védelmi intézkedések megvalósításához, és azokat szükség esetén az intézkedések végrehajtása során frissíteni kell. A védelmi intézkedések megvalósítása sok esetben a rendszer életciklus fejlesztési vagy beszerzési szakaszában történik. A kiválasztott védelmi intézkedések közül néhány már létezhet a szervezeten belül, például a szervezet által bevezetett, minden rendszerre vonatkozó védelmi intézkedések. A rendszerspecifikus biztonsági intézkedések megvalósítása esetén a rendszer biztonságáért felelős személy határozza meg a védelmi intézkedés implementálásának módját a biztonsági követelmények, a szervezeti kockázattűrés, a rendszer kockázatértékelése és a rendszer biztonsági osztálya alapján. A rendszerspecifikus védelmi intézkedések esetén a rendszer biztonságáért felelős személy, a rendszerbiztonsági mérnök, az adatvédelmi tisztviselő, az adatgazda együttműködve határozza meg a védelmi intézkedések bevezetésének sorrendjét.

A védelmi intézkedések bevezetésekor értékelni kell, hogy azok a rendszer biztonságértékelési terve alapján megfelelnek-e a biztonsági céloknak. Ha egy védelmi intézkedést valamilyen ok miatt módosítanak, akkor annak működési hatékonyságát is újra kell értékelni. A védelmi intézkedések működését és hatékonyságát ezután a rendszer és/vagy a szervezet folyamatos felügyeleti tervének megfelelően értékelik. Megjegyzendő, hogy célszerű a „jelentős” vagy „magas” biztonsági osztályba sorolt rendszereket független harmadik féllel értékeltetni.

Új rendszerek esetében a védelmi intézkedéseket a rendszer életciklusának kezdeti szakaszaiban implementálják, beleértve a fejlesztési/beszerzési és az implementálási/tesztelési szakaszokat. Fejlesztés alatt álló rendszerek esetében egy kezdeti önértékelést kell végezni annak megállapítására, hogy milyen védelmi intézkedések vannak már érvényben, mielőtt újakat vezetnek be. A meglévő rendszereknél a rendszer életciklusának üzemeltetési/karbantartási szakaszában vezethetnek be új intézkedéseket és/vagy frissítik a meglévőket. A bevezetést követően a védelmi intézkedések jó esetben hatékonyan teljesítik a biztonsági követelményeket. Ha valamilyen okból kifolyólag nem ez a helyzet, a rendszer biztonságáért felelős személynek reagálnia kell a felmerült problémára. Ha a védelmi

intézkedés csak részben felel meg a követelményeket, akkor további helyettesítő/kiegészítő védelmi intézkedésre és/vagy a kockázat(ok) elfogadására van szükség.

VÉDELMI INTÉZKEDÉSEK ÉRTÉKELÉSE

A kockázatkezelési keretrendszerben az értékelési lépés célja annak megállapítása, hogy a meghatározott védelmi intézkedéseket helyesen hajtották-e végre, azok rendeltetésszerűen működnek-e, a kívánt eredményt hozzák-e, és megfelelnek-e a szervezeti vagy rendszerszintű biztonsági követelményeknek. Ennek során a szervezet azonosítja a védelmi intézkedésekkel kapcsolatos hiányosságokat és megállapítja a szükséges javítási intézkedéseket. A folyamat során a szervezet kiválasztja a védelmi intézkedések ellenőrzését végző személyeket, elkészíti az értékelési tervet, az értékelési jelentést, valamint a cselekvési tervet. A védelmi intézkedések végrehajtásának hiányosságait aszerint kell rangsorolni, hogy azok milyen potenciális kockázatot jelentenek a rendszerre, az összetevőkre és a szervezetre nézve.

A védelmi intézkedések értékelésének két fő célja van:

- annak biztosítása, hogy a kockázatok kezelését szolgáló védelmi intézkedések működjenek és a kívánt eredményeket hozzák, valamint
- az engedélyező tisztviselő számára az engedélyezési döntés meghozatalához szükséges információk biztosítása.

Minden bevezetett védelmi intézkedést a szervezet által meghatározott gyakorisággal értékelni kell. Az ellenőrzések értékelése a rendszerbiztonsági terveken alapul, és a szervezeti és rendszerszintű folyamatos biztonságfelügyeleti tervek határozzák meg az értékelés gyakoriságát és az értékeléshez szükséges erőfeszítések szintjét is. Új rendszerek esetén az értékeléseket a védelmi intézkedések bevezetésekor szükséges elvégezni, hogy a fejlesztési folyamat korai szakaszában azonosítani lehessen a kontrollokkal kapcsolatos problémákat.

Az értékelőnek meg kell ismernie az értékelendő rendszert, beleértve többek között annak üzleti célját, funkcióit és működési környezetét. Szükség lehet arra, hogy az értékelők speciális készségekkel vagy ismeretekkel rendelkezzenek annak érdekében, hogy az értékelési eredmények tükrözzék a rendszer aktuális biztonsági és adatvédelmi helyzetét (pl., ha a rendszer adatbázis-szolgáltatásokat tartalmaz, az értékelőnek ismernie kell a használt adatbázist). Az alap biztonsági osztályba sorolt rendszerek értékeléséhez nem szükséges független, harmadik fél által biztosított értékelő, de a pártatlanság megőrzése érdekében a közepes és nagy hatású rendszerek értékeléséhez igen. Az értékelőket az általuk értékelt

rendszer vagy komponens típusához kapcsolódó műszaki szakértelmük, valamint a kockázatkezelési keretrendszer valamennyi lépésében - beleértve az értékelési és engedélyezési lépéseket és az azokat támogató feladatokat - szerzett tapasztalatuk alapján célszerű kiválasztani. Az értékelőknek mentesnek kell lenniük azon rendszerekkel, komponensekkel és érintett szervezeti egységekkel kapcsolatban álló tisztviselők bármilyen indokolatlan befolyásától, akiknek a védelmi intézkedéseit értékelik. Az értékelőknek pártatlan döntéseket kell hozniuk a biztonsági értékelések eredményeiről, és elfogulatlan információkkal kell ellátniuk az engedélyező tisztviselőt, hogy a rendszerrel és a szervezettel kapcsolatban megalapozott, kockázatalapú döntéseket lehessen hozni. Az engedélyezésre jogosult tisztviselő határozza meg az értékelő függetlenségének szintjét, amely szükséges a kontrollok elfogulatlan értékelésének elvégzéséhez, hogy a szervezeti tisztviselők számára a kontrollok értékelésére vonatkozó, indokolatlan befolyástól mentes információkat biztosítson. Az értékelő függetlensége nem jelenti azt, hogy az értékelés elvégzéséhez a szervezeten kívüli értékelőkre van szükség. Az értékelés elvégzésére olyan belső értékelők is alkalmazhatók, akik nem állnak az értékelt rendszer tulajdonosának felügyelete és/vagy irányítása alatt.

Ahhoz, hogy az értékelő hatékony és eredményes rendszer-, komponens- vagy szervezeti biztonsági értékelést végezzen, hozzáférésre van szükség az információkhoz és erőforrásokhoz. Ez magában foglalja a rendszerhez, annak működési környezetéhez, a rendszerdokumentációhoz és a kiválasztott személyzethez (pl. a rendszer biztonságáért felelős személy, az adatvédelmi tisztviselő, a biztonsági mérnök, a rendszergazda, a hálózati rendszergazda és az alkalmazásadminisztrátor, valamint a rendszer vagy komponens tervezésével, üzemeltetésével és karbantartásával kapcsolatos felelősséggel rendelkező egyéb személyek) való hozzáférést. Az értékelőknek hozzáférésre lehet szükségük a rendszer kézikönyveihez, rendszergazdai útmutatókhoz, jelentésekhez, kockázati dokumentációhoz (pl. cselekvési terv, kockázatelfogadási dokumentumok), rendszer- és adatáramlási diagramokhoz, korábbi értékelési eredményekhez, valamint egyéb információkhoz is, amelyek elsősorban a rendszer, a küldetés és a működési környezet megértését támogatják.

Az értékelők a rendszerbiztonsági tervek, a szervezet által alkalmazott közös kontrollok és a szervezeti szabályozások (pl. irányelvek, eljárások és egyéb vonatkozó anyagok) áttekintése után értékelési terveket dolgoznak ki. Az értékelési tervek meghatározzák a rendszerrel,

komponensekkel és szervezetekkel kapcsolatos szerepeket és felelősségi köröket, valamint az egyes védelmi intézkedésekre vonatkozó értékelési eljárásokat. Az értékelési tervek meghatározzák az elvégzendő értékelés típusát is, például a fejlesztési tesztelést, a használatba vételi engedélyezést, a további használat engedélyezését vagy a folyamatos ellenőrzést.

Az értékelési terveket az engedélyezésre jogosult tisztviselő vagy az engedélyezésre jogosult tisztviselő kijelölt képviselője vizsgálja felül és hagyja jóvá. A jóváhagyásával az engedélyezésre jogosult tisztviselő vagy az engedélyezésre jogosult tisztviselő által kijelölt képviselő egyetért az erőfeszítések szintjével és a biztonsági és adatvédelmi ellenőrzés értékelésének elvégzéséhez szükséges erőforrásokkal.

Az védelmi intézkedéseket a bevezetésük és/vagy módosításuk során, valamint a rendszer biztonsági terveiben és/vagy a szervezeti és rendszerszintű folyamatos biztonságfelügyeleti tervekben meghatározott gyakorisággal értékelik. A védelmi intézkedések értékelését bármikor el lehet végezni, amíg a rendszer vagy a rendszer alkotóeleme üzemben van. Az értékeléseket például a rendszer vagy komponens módosítása (pl. frissítés) után is célszerű lehet elvégezni annak megállapítására, hogy az új vagy frissített környezet jelent-e kockázatot.

A védelmi intézkedések hatékonyságának értékelése után az ellenőrzést végzők értékelő jelentést készítenek, amely tartalmazza az értékelés megállapításait. Az ellenőrzést végző bemutatja az értékelés eredményeit az engedélyezésre jogosult tisztviselőnek (és/vagy az engedélyezésre jogosult tisztviselő kijelölt képviselőjének), aki a rendszer biztonságáért felelős személlyel együttműködve meghatározza az egyes megállapításokra adandó választ (pl. kockázat csökkentés, elfogadás, elkerülés vagy tovább hárítás). A beavatkozást igénylő megállapításokat cselekvési tervekben rögzítik. A cselekvési tervek részletezik a biztonsági értékelő jelentésekben azonosított elfogadhatatlan kockázatok orvoslására vonatkozó feladatokat, és ez az engedélyezési csomag egyik eleme (lásd később). Az engedélyezésre jogosult tisztviselő a tervet rendszeresen felülvizsgálja, és a kockázatcsökkentés nyomon követésére használja, azáltal, hogy a feladatok elvégzése során visszaköveti az intézkedéseket. A cselekvési tervek az engedélyezési csomag részét képezik, és az engedélyező tisztviselőnek kerülnek bemutatásra. Információt nyújtanak az védelmi intézkedések hiányosságairól, a korrekciós intézkedésekről, a feladatok ütemezéséről és a hiányosságok kijavításáért felelős felekről.

A RENDSZERHASZNÁLAT JÓVÁHAGYÁSA

A kockázatkezelési keretrendszer része az információs rendszerek éles üzemi használatba vételének és használatban tartásának engedélyezése. Az engedélyezési lépés célja a szervezeti elszámoltathatóság biztosítása azáltal, hogy a szervezet vezetője köteles eldönteni, hogy a rendszer működése, a védelmi intézkedések alkalmazása alapján elfogadható-e a szervezeti működésre és eszközökre, egyénekre, más szervezetekre vonatkozó biztonsági kockázat (beleértve az ellátási lánc kockázatát is).

A rendszer működésének engedélyezéséről (vagy engedélyezésének megtagadásáról) szóló döntés a rendszer biztonsági helyzetétől, valamint a rendszer működéséből és használatából eredő kockázattól függ. Ezt a kockázatot az engedélyezési csomagban szereplő információk elemzése, valamint a vezető tisztviselők, a kockázatok elfogadásáért felelős személyek, a védelmi intézkedés értékelők, a rendszerek biztonságáért felelő személy és más érdekelt felek által a szervezet vezetőjének nyújtott szervezeti és rendszerszintű kockázati információk alapján határozzák meg. Szükség esetén további megbeszélésekre kerülhet sor a szervezet vezetője és az információt szolgáltató személyek között annak érdekében, hogy a vezető teljes mértékben megértse a kockázatokat. A kockázatelemzés során a szervezet vezetője figyelembe veszi a szervezeti kockázattűrő képességet, a rendszerek közötti függőségeket, az üzleti célokat és követelményeket, a rendszer üzleti funkcióinak kritikusságát, valamint a szervezet általános kockázatkezelési stratégiáját. A szervezet vezetője az egyetlen személy, aki az értékelő jelentések és az intézkedési tervek vizsgálatát követően elfogadhatja a kockázat(ok)at, és a cselekvési tervet. A rendszer használatára vonatkozó döntést támogató un. engedélyezési csomag információt nyújt a rendszer és a védelmi intézkedések helyzetéről az értékelés elvégzésének időpontjában vagy annak környékén. Az engedélyezési csomag biztonsági terveket, biztonsági értékelési jelentéseket, cselekvési terveket, valamint egy opcionális összefoglalót tartalmaz. A szervezetek automatizált eszközökkel segíthetik az engedélyezési csomag tartalmának naprakészen tartását.

Az engedélyezési döntést az engedélyezési csomag és a rendszerhasználati engedély jóváhagyásán keresztül közlik a rendszer biztonságáért felelős személlyel, illetve szükség esetén más szervezeti tisztviselőkkel. A rendszerhasználat engedélyezéséről szóló végleges döntéshez csatolják az üzemeltetési feltételeket. A feltételek leírják azokat a korlátozásokat

vagy megkötéseket, amelyeket a rendszer biztonságáért felelős személynek vagy a közös védelmi intézkedések megvalósításáért felelős személynek be kell tartania. A feltételek betartását a szervezet folyamatos felügyeleti programjának részeként folyamatosan ellenőrizni szükséges.

A BIZTONSÁG FOLYAMATOS FELÜGYELETE

Ahogy korábban írtuk, a kockázatkezelési rendszer kialakítására való felkészülésként a rendszerek biztonságáért felelős személy stratégiát dolgoz ki z védelmi intézkedések hatékonyságának és a rendszerben vagy működési környezetében tervezett vagy tényleges változtatások folyamatos nyomon követésére. A rendszer folyamatos biztonságfelügyeleti stratégiája meghatározza, hogy milyen védelmi intézkedéseket kell felügyelni, illetve mikor (pl. folyamatosan vagy előre meghatározott gyakorisággal), hogyan kell a rendszer változásait nyomon követni, hogyan kell kockázatértékeléseket végezni, valamint a biztonsági helyzetre vonatkozó jelentéstételi követelményeket, beleértve a jelentések címzettjeit. A rendszerekre vonatkozó folyamatos felügyeleti stratégia a szervezet átfogó folyamatos felügyeleti programjának része.

A kockázati keretrendszerben működő folyamatos felügyeleti program működtetésének célja, hogy

- a biztonság felügyelete beépüljön a szervezeti rendszerek teljes életciklusába,
- támogassa a védelmi intézkedések meghatározását és hatékony működésének kialakítását,
- a folyamatos biztonságfelügyelet beépüljön a meglévő szervezeti változáskezelési, konfigurációkezelési folyamatokba,
- az adatgazdák és a rendszerek biztonságáért felelős személyek képesek legyenek valós helyzetet tükröző jelentések, cselekvési tervek készítésére és értékelésére,
- a szervezeti képes legyen azonosítani a biztonsági gyengeségeket és hiányosságokat, valamint optimalizálni tudja az kezelésükre szolgáló erőforrások elosztását.

Minden megvalósított védelmi intézkedést a szervezet által meghatározott gyakorisággal ellenőrizni kell. Az ellenőrzés gyakoriságának meghatározására vonatkozó kritériumokat a rendszer biztonságáért felelős személy határozza meg más szervezeti tisztviselőkkel együttműködve és a szervezeti szintű folyamatos biztonságfelügyeleti stratégiával összhangban. A kritériumoknak tükrözniük kell a rendszer szervezeti működésben betöltött fontosságát. Azokat a védelmi intézkedéseket, amelyek idővel valószínűleg változnak, vagy kritikusak a szervezet védelmi stratégiájának szempontjából, vagy szerepelnek a cselekvési

tervekben, a funkció kritikusságával és a felügyeleti eszközök képességével összhangban lévő gyakorisággal kell értékelni. A szervezeti kockázatértékelés (akár formális, akár informális) felhasználható a védelmi intézkedés felügyeleti gyakoriságának meghatározásához.

A külső szolgáltatók által kezelt vagy üzemeltetett rendszereket is folyamatosan ellenőrizni kell. A szervezet vezetője felelős azért, hogy megfelelően reagáljon a szervezet működését, eszközeit vagy személyeit érintő azon kockázatokra, amelyek külső rendszerszolgáltatások használatából erednek. A külső szolgáltatókkal kötött szerződéseknek biztonsági követelményeket kell megfogalmazniuk (például előírhatják a szolgáltatók számára, hogy az általuk üzemeltetett és kezelt rendszerekre vezessenek be konfigurációkezelési folyamatot, készítsenek rendszeres biztonsági helyzetjelentéseket, és jelentsék a végrehajtott vagy tervezett változtatásokat). A külső szolgáltató konfigurációkezelési folyamata megkövetelheti az adatgazda vagy a rendszer biztonságáért felelős személy bevonását a folyamatba. Hasonlóképpen, a külső beszállítókat (az ellátási láncban) értékelésekkel és felülvizsgálatokkal ellenőrizni kell.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024