41/2015. (VII. 15.) BM rendelet

az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24. § (2) bekezdés *a)* pontjában kapott felhatalmazás alapján, a Kormány tagjainak feladat- és hatásköréről szóló 152/2014. (VI. 6.) Korm. rendelet 21. § 5. és 20. pontjában meghatározott feladatkörömben eljárva - a Kormány tagjainak feladat- és hatásköréről szóló 152/2014. (VI. 6.) Korm. rendelet 109. § 11. pontjában meghatározott feladatkörében eljáró nemzeti fejlesztési miniszterrel egyetértésben - a következőket rendelem el:

1. § Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) hatálya alá tartozó elektronikus információs rendszerrel rendelkező szervezet az elektronikus információs rendszereit az 1. mellékletben felsorolt szempontok szerint sorolja biztonsági osztályba.

2. § Az elektronikus információs rendszerrel rendelkező szervezet vagy e szervezetnek az Ibtv. 9. § (2) bekezdése szerinti szervezeti egysége (a továbbiakban: szervezeti egység) a biztonsági szintbe sorolást a 2. melléklet szerinti biztonsági szintek alapján végzi el.

3. § (1) Az 1. § és a 2. § szerint elvégzett besorolás alapján az elektronikus információs rendszerrel rendelkező szervezet a 3. mellékletben meghatározott, az elektronikus információs rendszerére érvényes biztonsági osztályhoz rendelt követelményeket a 4. mellékletben meghatározott módon teljesíti.

(2) Ha az elektronikus információs rendszerrel rendelkező szervezetre vagy a szervezeti egységre e rendelet előírásai szerint kidolgozott szabályzatokban meghatározott adminisztratív és fizikai védelmi intézkedésektől egy elektronikus információs rendszer esetében a magasabb védelmi igény miatt el kell térni, az eltéréseket az érintett elektronikus információs rendszer e rendelet előírásai szerint kidolgozott szabályzatában kell rögzíteni.

(3) Ha a szervezeti egységre vonatkozóan - a magasabb védelmi igény miatt a szervezetre megállapított biztonsági szinttől - eltérő biztonsági szint megállapítása indokolt, a szervezeti egységet önállóan kell szintbe sorolni a 2. mellékletben meghatározott szempontok alapján.

(4) Ha az elektronikus információs rendszerrel rendelkező szervezet az elektronikus információs rendszernek csak egyes elemeit vagy funkcióit üzemelteti vagy használja - részben vagy teljesen -, a 4. mellékletben meghatározott követelményeket ezen elemek és funkciók tekintetében kell teljesíteni.

(5) Ha az elektronikus információs rendszert több szervezet használja, az elektronikus információs rendszer üzemeltetője az üzemeltetés elektronikus információbiztonságához szükséges követelményeket az elektronikus információs rendszeren tevékenységet végző minden, elektronikus információs rendszerrel rendelkező szervezet tekintetében érvényesíti.

(6) Az elektronikus információs rendszer üzemeltetője az üzemeltetés elektronikus információbiztonságához szükséges követelményeket úgy érvényesíti az elektronikus információs rendszeren tevékenységet végző elektronikus információs rendszerrel rendelkező szervezetek tekintetében, hogy a követelményeknek való megfelelés az elektronikus információs rendszerrel rendelkező szervezet elektronikus információbiztonsággal kapcsolatos eljárási rendjébe beépüljön. Az elektronikus információs rendszer üzemeltetője és az elektronikus információs rendszerrel rendelkező szervezetek az üzemeltetés elektronikus információbiztonságához szükséges követelményeket az elektronikus információs rendszer üzemeltetésére kötött szerződésben rögzítik.

4. § Ez a rendelet 2015. július 16-án lép hatályba.

5. §[1]

6. § (1) Ha az elektronikus információs rendszerrel rendelkező szervezet az Ibtv. 26. §-ában meghatározott határidőig az elektronikus információs rendszereinek biztonsági osztályba sorolását elvégezte és az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről szóló BM rendelet 5. § (1) bekezdés *b)* és *c)* pontja szerinti bejelentési kötelezettségének eleget tett, az elektronikus információs rendszerek e rendelet szerinti osztályba sorolását az Ibtv. 8. § (1) bekezdésében foglalt esetekben kell elvégezni.

(2) Ha az elektronikus információs rendszerrel rendelkező szervezet az Ibtv. 26. §-ában meghatározott határidőig a szervezet biztonsági szintbe sorolását elvégezte és a biztonsági szint - az e rendelet 2. mellékletében foglaltak alkalmazásával - nem változik, továbbá az Ibtv. 9. § (2) bekezdése szerinti szervezeti egység nem kerül kijelölésre, valamint az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről szóló BM rendelet 5. § (1) bekezdés *a)* pontja szerinti bejelentési kötelezettségének eleget tett, a szervezet e rendelet szerinti osztályba sorolását az Ibtv. 10. § (5) bekezdésében foglalt esetekben kell elvégezni.

(3) Ha az elektronikus információs rendszer fejlesztése e rendelet hatálybalépésekor az R. előírásai szerint már folyik, az elektronikus információs rendszer e fejlesztésére az e rendeletben foglaltakat 2015. október 1. napjától kell alkalmazni.

7. §[2] Ez a rendelet a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-ai (EU) 2016/1148 európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.

1. melléklet a 41/2015. (VII. 15.) BM rendelethez

Az elektronikus információs rendszerek biztonsági osztályba sorolása

1 *Hatályon kívül helyezve: 2010. évi CXXX. törvény 12. § alapján. Hatálytalan: 2015. VII. 17-től.*
2 *Beiktatta: 40/2017. (XII. 29.) BM rendelet 14. §. Hatályos: 2018. V. 10-től.*

1. Általános irányelvek

1.1. Az érintett szervezet az elektronikus információs rendszere biztonsági osztályba sorolásakor az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit a rendszer funkcióira tekintettel, és azokhoz igazodó súllyal érvényesíti;
1.1.1. a nemzeti adatvagyont kezelő rendszerek esetében a sértetlenség követelményét emeli ki;
1.1.2. a létfontosságú információs rendszerelemek esetében a rendelkezésre állást követeli meg elsődlegesen;
1.1.3. a különleges személyes adatokkal kapcsolatban alapvető igényként fogalmazza meg a bizalmasság fenntartását.

1.2. Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet az érintett szervezet vezetője hagy jóvá, kockázatelemzés alapján kell elvégezni. A Nemzeti Elektronikus Információbiztonsági Hatóság ajánlásként kockázatelemzési módszertanokat adhat ki. Ha a szervezet saját kockázatelemzési módszertannal nem rendelkezik, az így kiadott ajánlást köteles használni.

2. Biztonsági osztályok

2.1. A jogszabályban meghatározott biztonsági osztályba sorolás elvégzése a következő elvek figyelembevételével az érintett szervezet felelőssége. A 2.2.-2.6. pontok a döntéshez csak iránymutatást képeznek:

2.2. Az 1. biztonsági osztály esetében csak jelentéktelen káresemény következhet be, mivel
2.2.1. az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot;
2.2.2. nincs bizalomvesztés, a probléma az érintett szervezeten belül marad, és azon belül meg is oldható;
2.2.3. a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez képest jelentéktelen;

2.3. A 2. biztonsági osztály esetében csekély káresemény következhet be, mivel
2.3.1. személyes adat sérülhet;
2.3.2. az érintett szervezet üzlet-, vagy ügymenete szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet;
2.3.3. a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;
2.3.4. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át.

2.4. A 3. biztonsági osztály esetében közepes káresemény következhet be, mivel
2.4.1. különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek;

2.4.2. az érintett szervezet üzlet-, vagy ügymenete szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet;
2.4.3. a lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek;
2.4.4. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%-át.

2.5. A 4. biztonsági osztály esetében nagy káresemény következhet be, mivel
2.5.1. különleges személyes adat nagy mennyiségben sérülhet;
2.5.2. személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);
2.5.3. az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;
2.5.4. a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyi felelősségre vonást kell alkalmazni;
2.5.5. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át.

2.6. Az 5. biztonsági osztály esetében kiemelkedően nagy káresemény következhet be, mivel
2.6.1. különleges személyes adat kiemelten nagy mennyiségben sérülhet;
2.6.2. emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;
2.6.3. a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;
2.6.4. az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;
2.6.5. a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
2.6.6. az érintett szervezet üzlet- vagy ügymenete szempontjából nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet;
2.6.7. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.

2. melléklet a 41/2015. (VII. 15.) BM rendelethez

Az elektronikus információs rendszerrel rendelkező szervezetek vagy szervezeti egységek biztonsági szintbe sorolása

1. Az érintett szervezet biztonsági szintje 1., ha a szervezet nem üzemeltet és nem fejleszt elektronikus információs rendszert, és saját hatáskörben erre más szervezetet vagy szolgáltatót (ide nem értve a telekommunikációs szolgáltatót) sem vesz igénybe. Az adatfeldolgozás módját nem maga határozza meg, az adatkezelés tekintetében technikai vagy információtechnológiai döntést nem hoz, a használt elektronikus információs infrastruktúra kialakítása tekintetében döntési jogköre - ide nem értve a szervezet munkavégzését érintő informatikai rendszerelemek elhelyezését - nincs, egyedi adatokat és információkat kezel vagy dolgoz fel, és kritikus adatot nem kezel. A szervezet információbiztonsági tevékenysége elsődlegesen az elektronikus információs rendszerrel kapcsolatba kerülő személyek információbiztonsággal kapcsolatos kötelezettségeinek szabályozására, számonkérésére terjed ki, addig a mértékig, ameddig a szervezet vagy az egyes személyek tevékenysége az elektronikus információs rendszerre hatást tud gyakorolni.

1.1. Az 1. biztonsági szervezeti szint követelményei:

1.1.1. az érintett szervezet az érintett személyi kör részére biztosítja az 1.1.3. pont szerinti szervezeti vagy feladathoz rendelt működési terület hatályos információbiztonságot érintő munkautasítását, belső rendelkezését, szabályozását vagy más erre célra szolgáló dokumentumot (a továbbiakban együtt: szabályzat);

1.1.2. az informatikai biztonsági szabályzat része a folyamatos kockázatelemzési eljárás, amely tartalmazza a beépített ellenőrzési pontokat;

1.1.3. az informatikai biztonsági szabályzat vonatkozhat egész szervezetre és működési területére, vagy meghatározott vagyonelemre vagy szervezeti egységre;

1.1.4. a informatikai biztonsági szabályzatot a szervezetre érvényes rendelkezések szerint az erre jogosult vezetőnek kell jóváhagynia;

1.1.5. a informatikai biztonsági szabályzat tartalmazza az információbiztonság felügyeleti rendszerét, az információbiztonsággal kapcsolatos kötelezettségeket és felelősségeket;

1.1.6. az informatikai biztonsági szabályzat be nem tartása jogkövetkezményt von maga után.

2. Az érintett szervezet biztonsági szintje 2., ha a szervezet vagy szervezeti egység az 1. szinthez rendelt jellemzőkön túl olyan elektronikus információs rendszert használ, amely személyes adatokat kezel, és a szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe.

2.1. A 2. biztonsági szervezeti szint követelményei az 1. szinthez rendelt követelményeken túl:

2.1.1. az érintett szervezet biztonsági kontrollfolyamatai eljárásrendben szabályozottak;

2.1.2. a 2.1.1. pont szerinti eljárásrend tartalmazza a kontrollfolyamatok végrehajtásának menetét, módját, időpontját, végrehajtóját, tárgyát, eszközét;

2.1.3. az egyes folyamatok egyértelműen meghatározzák az információbiztonsági felelősségeket és a biztonságtudatos viselkedést az elektronikus információs rendszerrel kapcsolatba kerülő személyek, valamint az információbiztonságért felelős személyek és szervezeti egységek tekintetében;

2.1.4. az egyes folyamatokat szervezeti egységek vagy személyek felügyelete alá kell rendelni, akik az adott folyamat végrehajtása érdekében közvetlen kapcsolatban állnak a folyamatban érintett más személyekkel vagy szervezeti egységekkel;

2.1.5. a folyamatokat és végrehajtásukat úgy kell dokumentálni, hogy abból az elvégzett kontroll tevékenység - ideértve annak egyes jellemzőit, így különösen mélységét, érintett személyi és tárgyi körét - megállapítható legyen.

3. Az érintett szervezet biztonsági szintje 3., ha a szervezet vagy szervezeti egység a 2. szinthez rendelt jellemzőkön túl szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt. A szervezet kritikus adatot, nem minősített, de nem közérdekű, vagy közérdekből nyilvános adatot kezel, központi üzemeltetésű, és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek vagy zárt célú elektronikus információs rendszer felhasználója, illetve feladatai támogatására más külső szolgáltatót vesz igénybe.

3.1. A 3. biztonsági szervezeti szint követelményei a 2. szinthez rendelt követelményeken túl:

3.1.1. az érintett szervezet a biztonsági kontroll folyamataiba bevonja, és feladataikról, a velük szemben támasztott elvárásokról tájékoztatja a folyamatokban résztvevő személyeket;

3.1.2. a 3.1.1. pont szerinti folyamatokat az érintett szervezet vagy szervezeti egység tekintetében szabályozottan és ellenőrizhető módon kell bevezetni, az érintett személyek számára oktatás tárgyává tenni;

3.1.3. a 3.1.1. pont szerinti folyamatok nem alkalmazandók egyéni vagy eseti eljárásokra;

3.1.4. a 3.1.1. pont szerinti folyamatokat a szervezetre érvényes rendelkezések szerint erre jogosult vezetőnek kell jóváhagynia;

3.1.5. a 3.1.1. pont szerinti folyamatok előzetes tesztelésével biztosítani kell a folyamatok előre meghatározott követelmények szerinti működését;

3.1.6. a szervezetnek rendelkeznie kell információbiztonsági költség- és haszonelemzési módszertannal.

4. Az érintett szervezet biztonsági szintje 4., ha a szervezet vagy szervezeti egység a 3. szinthez rendelt jellemzőkön túl elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet vagy fejleszt.

4.1. A 4. biztonsági szervezeti szint követelményei a 3. szinthez rendelt követelményeken túl:

4.1.1. az üzemeltetési vagy fejlesztési tevékenységbe épített rendszeres, előre meghatározott tesztekkel biztosítani kell az üzemeltetés vagy fejlesztés információbiztonsági intézkedéseinek hatékonyságát és megfelelőségét;

4.1.2. tesztelési eljárásban rögzítetten biztosítani kell minden szabályozási folyamat és kontroll működését az elvárt és előre meghatározott információbiztonsági követelmények szerint;

4.1.3. azonnali és eredményes, előre meghatározott biztonsági intézkedéseket kell bevezetni a feltárt vagy bekövetkezett biztonsági események kezelésére, beleértve az eseménykezelő központok, a beszállítók vagy egyéb megbízható forrás jelzése alapján lehetséges vagy bekövetkezett biztonsági esemény kezelését is;

4.1.4. folyamatba épített rendszeres belső értékelés alá kell vonni az egyes információ, rendszer vagy alkalmazás biztonsága érdekében bevezetett intézkedések megfelelőségét és hatékonyságát, mely belső értékelések részben, vagy egészben történhetnek alvállalkozók vagy más, erre feljogosított, vagy a szerv felett felügyelet gyakorló szerv bevonásával;

4.1.5. a szervezet folyamatba épített belső értékelései nem helyettesíthetőek;

4.1.6. a 4.1.3. pont szerinti forrásból származó, potenciális vagy a valódi biztonsági eseményekkel és biztonsággal kapcsolatos információk, vagy riasztások alapján tesztelési eljárást vagy biztonsági ellenőrzést kell végezni;

4.1.7. a tesztelés értékelése alapján megállapított követelményeket, - beleértve a tesztelés típusával és gyakoriságával kapcsolatos követelményeket is - dokumentálni kell, az arra jogosulttal jóvá kell hagyatni és be kell vezetni;

4.1.8. az egyedi kontroll eljárások tesztelésének gyakoriságát és mélységét ahhoz kell igazítani, hogy milyen biztonsági kockázattal jár a kontrollok nem megfelelő működése.

5. Az érintett szervezet biztonsági szintje 5., ha a szervezet vagy szervezeti egység a 4. szinthez rendelt jellemzőkön túl európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek üzemeltetője, fejlesztője, illetve az információbiztonsági ellenőrzések, tesztelések végrehajtására jogosult szervezet vagy szervezeti egység.

5.1. A 5. biztonsági szervezeti szint követelményei a 4. szinthez rendelt követelményeken túl:

5.1.1. biztosítani kell az információbiztonsági kontrollfolyamatoknak a szervezet alapfeladataiba történő beépítését;

5.1.2. biztosítani kell a szabályzatok, tesztelési eljárások, biztonsági folyamatok folyamatos felülvizsgálatát és továbbfejlesztését;

5.1.3. a szervezetnek rendelkeznie kell átfogó információbiztonsági programmal, amely szerves része a szervezet feladatellátásnak és biztosítja a személyi állomány biztonságtudatosságának növelését;

5.1.4. a szervezet személyi állományának rendelkeznie kell információbiztonsági operatív képességgel és a feladat elvégzéséhez szükséges szaktudással;

5.1.5. a biztonsági sérülékenységek felismerésének és kezelésének képességét a szervezet egésze tekintetében meg kell valósítani;

5.1.6. a fenyegetettségek folyamatos újraértékelésével, a kontrollfolyamatok felülvizsgálatával nyomon kell követni információbiztonsági környezet változását;

5.1.7. az információbiztonságot érintő külső vagy belső környezeti változásokra figyelemmel további információbiztonsági alternatívákat kell meghatározni;

5.1.8. a szervezetnek ki kell alakítania az információbiztonsági képesség- és állapotmérési és értékelési módszertanát, meg kell határozni annak mutatóit és 5.1.7. pont szerinti esetben aktualizálnia kell azt.

3. melléklet a 41/2015. (VII. 15.) BM rendelethez

1. Besorolási útmutató

1.1. Általános rendelkezések

1.2. A megvalósítandó biztonsági intézkedéseket és azok megvalósításának sorrendjét a kívánt biztonsági osztály (biztonsági szint) elérésére megalkotott intézkedési tervben kell meghatározni.

1.3. A sorszám rovatban a 4. melléklet *„3. Védelmi intézkedés katalógus”*-ának az adott számhoz rendelt intézkedésének a száma került feltüntetésre.

1.4. Az adminisztratív és fizikai védelmi intézkedések tekintetében az érintett szervezet elektronikus információs rendszerének biztonsági osztályát az 1-5. számozású oszlopok jelzik.

1.5. A logikai védelmi intézkedések követelményrendszerének kialakítása során az 1. melléklet 2. pontjára figyelemmel kell eljárni, és az elektronikus információs rendszert az információbiztonsági alapelveknek (bizalmasság, sértetlenség, rendelkezésre állás) megfelelően 2-5. osztályokba besorolni. Mivel a logikai védelmi intézkedések terén az 1. biztonsági osztály nem értelmezhető, az a táblázatban nem szerepel.

1.6. Bármely oszlopban

1.6.1. „0” jelzi, hogy a vízszintes sorban szereplő védelmi intézkedés ebben a biztonsági osztályban nem kötelező;

1.6.2. „X” jelzi, hogy a vízszintes sorban szereplő védelmi intézkedés ebben a biztonsági osztályban kötelező.

2. A 4. melléklet „3. Védelmi intézkedés katalógus” alcímben meghatározott védelmi intézkedések besorolásának táblázatai:

A) 3.1. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

	A	B
1.	**Sorszám**	**Intézkedés típusa**
2.		
3.	**3.1.1.**	**Szervezeti szintű alapfeladatok**
4.	3.1.1.1.	Informatikai biztonsági szabályzat
5.	3.1.1.2.	Az elektronikus információs rendszerek biztonságáért felelő személy
6.	3.1.1.3.	Az intézkedési terv és mérföldkövei
7.	3.1.1.4.	Az elektronikus információs rendszerek nyilvántartása
8.	3.1.1.5.	Az elektronikus információbiztonsággal kapcsolato engedélyezési eljárás
9.	**3.1.2.**	**Kockázatelemzés**
10.	3.1.2.1.	Kockázatelemzési és kockázatkezelési eljárásrend
11.	3.1.2.2.	Biztonsági osztályba sorolás
12.	3.1.2.3.	Kockázatelemzés
13.	**3.1.3.**	**Rendszer és szolgáltatás beszerzés**
14.	3.1.3.1.	Beszerzési eljárásrend
15.	3.1.3.2.	Erőforrás igény felmérés
16.	3.1.3.3.	Beszerzések
17.	3.1.3.3.2.	A védelem szempontjainak érvényesítése a beszerzés során
18.	3.1.3.3.3.	A védelmi intézkedések terv-, és megvalósítási dokumentációi
19.	3.1.3.3.4.	Funkciók - protokollok - szolgáltatások
20.	3.1.3.4.	Az elektronikus információs rendszerre vonatkozó dokumentáció

21.	3.1.3.5.	Biztonságtervezési elvek
22.	3.1.3.6.	Külső elektronikus információs rendszerek szolgáltatásai
23.	3.1.3.7.	Független értékelők
24.	3.1.3.8.	Folyamatos ellenőrzés
25.	3.1.3.8.2.	Független értékelés
26.	**3.1.4.**	**Üzletmenet (ügymenet) folytonosság tervezése**
27.	3.1.4.1.	Üzletmenet folytonosságra vonatkozó eljárásrend
28.	3.1.4.2.	Üzletmenet folytonossági terv informatikai erőforrás kiesésekre
29.	3.1.4.2.2.	Egyeztetés
30.	3.1.4.2.3.	Alapfunkciók újraindítása
31.	3.1.4.2.4.	Kritikus rendszerelemek meghatározása
32.	3.1.4.2.5.	Kapacitástervezés
33.	3.1.4.2.6.	Összes funkció újraindítása
34.	3.1.4.2.7.	Alapfeladatok és funkciók folyamatossága
35.	3.1.4.3.	A folyamatos működésre felkészítő képzés
36.	3.1.4.3.2.	Szimuláció
37.	3.1.4.4.	Az üzletmenet folytonossági terv tesztelése
38.	3.1.4.4.2.	Koordináció
39.	3.1.4.4.3.	Tesztelés a tartalék feldolgozási helyszínen
40.	3.1.4.5.	Biztonsági tárolási helyszín
41.	3.1.4.5.2.	A tartalék feldolgozási helyszín elkülönítése
42.	3.1.4.5.3.	Üzletmenet folytonosság elérhetőség
43.	3.1.4.5.4.	Üzletmenet folytonosság helyreállítás
44.	3.1.4.6.	Tartalék feldolgozási helyszín
45.	3.1.4.6.2.	Elkülönítés
46.	3.1.4.6.3.	Elérhetőség
47.	3.1.4.6.4.	Szolgáltatások priorálása a tartalék feldolgozási helyszínen
48.	3.1.4.6.5.	Előkészület a működés megindítására
49.	3.1.4.7.	Infokommunikációs szolgáltatások
50.	3.1.4.7.2.	Szolgáltatás-prioritási rendelkezések
51.	3.1.4.7.3.	Közös hibalehetőségek kizárása
52.	3.1.4.8.	Az elektronikus információs rendszer mentései
53.	3.1.4.8.2.	Megbízhatósági és sértetlenségi teszt
54.	3.1.4.8.3.	Helyreállítási teszt
55.	3.1.4.8.4.	Kritikus információk elkülönítése
56.	3.1.4.8.5.	Alternatív tárolási helyszín
57.	3.1.4.9.	Az elektronikus információs rendszer helyreállítása é újraindítása
58.	3.1.4.9.2.	Tranzakciók helyreállítása
59.	3.1.4.9.3.	Helyreállítási idő
60.	**3.1.5.**	**A biztonsági események kezelése**
61.	3.1.5.1.	Biztonsági eseménykezelési eljárásrend
62.	3.1.5. 2.	Automatikus eseménykezelés
63.	3.1.5. 3.	Információ korreláció
64.	3.1.5.4.	A biztonsági események figyelése
65.	3.1.5.5.	Automatikus nyomonkövetés, adatgyűjtés és vizsgálat
66.	3.1.5.6.	A biztonsági események jelentése
67.	3.1.5.6.2	Automatizált jelentés
68.	3.1.5.7.	Segítségnyújtás a biztonsági események kezeléséhez
69.	3.1.5.7.2.	Automatizált támogatás
70.	3.1.5.8.	Biztonsági eseménykezelési terv
71.	3.1.5.9.	Képzés a biztonsági események kezelésére
72.	3.1.5.9.2.	Szimuláció
73.	3.1.5.9.3.	Automatizált képzési környezet
74.	3.1.5.9.4	A biztonsági események kezelésének tesztelése
75.	3.1.5.9.4.2.	Egyeztetés

76.	**3.1.6.**	**Emberi tényezőket figyelembe vevő - személy - biztonság**
77.	3.1.6.1.	Személybiztonsági eljárásrend
78.	3.1.6.2.	Munkakörök, feladatok biztonsági szempontú besorolása
79.	3.1.6.3.	A személyek ellenőrzése
80.	3.1.6.4.	Eljárás a jogviszony megszűnésekor
81.	3.1.6.5.	Az áthelyezések, átirányítások és kirendelések kezelése
82.	3.1.6.6.	Az érintett szervezettel szerződéses jogviszonyban álló (külső szervezetre vonatkozó követelmények
83.	3.1.6.7.	Fegyelmi intézkedések
84.	3.1.6.8	Belső egyeztetés
85.	3.1.6.9.	Viselkedési szabályok az interneten
86.	**3.1.7.**	**Tudatosság és képzés**
87.	3.1.7.1.	Kapcsolattartás az elektronikus információbiztonsá jogszabályban meghatározott szervezetrendszerével, és az e cé szolgáló ágazati szervezetekkel
88.	3.1.7.2.	Képzési eljárásrend
89.	3.1.7.3.	Biztonság tudatosság képzés
90.	3.1.7.4.	Belső fenyegetés
91.	3.1.7.5.	Szerepkör, vagy feladat alapú biztonsági képzés
92.	3.1.7.6.	A biztonsági képzésre vonatkozó dokumentációk

B) 3.2. FIZIKAI VÉDELMI INTÉZKEDÉSEK

	A	B
1.	**Sorszám**	**Intézkedés típusa**
2.		
3.	3.2.1.2.	Fizikai védelmi eljárásrend
4.	3.2.1.3.	Fizikai belépési engedélyek
5.	3.2.1.4.	A fizikai belépés ellenőrzése
6.	3.2.1.4.2.	Hozzáférés az információs rendszerhez
7.	3.2.1.5.	Hozzáférés az adatátviteli eszközökhöz és csatornákhoz
8.	3.2.1.6.	A kimeneti eszközök hozzáférés ellenőrzése
9.	3.2.1.7.	A fizikai hozzáférések felügyelete
10.	3.2.1.7.2.	Behatolás riasztás, felügyeleti berendezések
11.	3.2.1.7.3.	Az elektronikus információs rendszerekhez való hozzáféré felügyelete
12.	3.2.1.8.	A látogatók ellenőrzése
13.	3.2.1.8.2.	Automatizált látogatói információkezelés
14.	3.2.1.9.	Áramellátó berendezések és kábelezés
15.	3.2.1.9.1.	Tartalék áramellátás
16.	3.2.1.9.2.	Hosszú távú tartalék áramellátás a minimálisan elvárt működé képességhez
17.	3.2.1.10.	Vészkikapcsolás
18.	3.2.1.11.	Vészvilágítás
19.	3.2.1.12.	Tűzvédelem
20.	3.2.1.12.2.	Automatikus tűzelfojtás
21.	3.2.1.12.3.	Észlelő berendezések, rendszerek
22.	3.2.1.12.4.	Tűzelfojtó berendezések, rendszerek
23.	3.2.1.13.	Hőmérséklet és páratartalom ellenőrzés
24.	3.2.1.14.	Víz-, és más, csővezetéken szállított anyag okozta kár ellen védelem
25.	3.2.1.14.2.	Automatizált védelem
26.	3.2.1.15.	Be- és kiszállítás
27.	3.2.1.16.	Az elektronikus információs rendszer elemeinek elhelyezése
28.	3.2.1.17.	Ellenőrzés
29.	3.2.1.18.	Szállítási felügyelet
30.	3.2.1.19.	Karbantartók

31.	3.2.1.19.2.	Karbantartás fokozott biztonsági intézkedésekkel
32.	3.2.1.19.3.	Időben történő javítás

C) 3.3. LOGIKAI VÉDELMI INTÉZKEDÉSEK

	A	B	C	D	E	F	G	H	I
1.	**Sorszám**	**Intézkedés típusa**							**Alapelv**
2.			**Bizalmasság**				**Sértetler**		
3.									**Biztonsági o**
4.			**2**	**3**	**4**	**5**	**2**	**3**	4
5.	**3.3.1.**	**Általános védelmi intézkedések**							
6.	3.3.1.3.	Az elektronikus információs rendszer kapcsolódásai	0	X	X	X	0	X	X
7.	3.3.1.3.2.	Belső rendszer kapcsolatok	0	X	X	X	0	X	X
8.	3.3.1.3.3.	Külső kapcsolódásokra vonatkozó korlátozások	0	X	X	X	0	X	X
9.	3.3.1.4.	Személybiztonság	X	X	X	X	X	X	X
10.	**3.3.2.**	**Tervezés**							
11.	3.3.2.1.	Biztonságtervezési szabályzat	0	0	X	X	0	0	X
12.	3.3.2.2.	Rendszerbiztonsági terv	X	X	X	X	X	X	X
13.	3.3.2.3.	Cselekvési terv	X	X	X	X	X	X	X
14.	3.3.2.4.	Személyi biztonság	X	X	X	X	0	0	0
15.	3.3.2.5.	Információbiztonsági architektúra leírás	0	0	X	X	0	0	0
16.	**3.3.3.**	**Rendszer és szolgáltatás beszerzés**							
17.	3.3.3.2.	A rendszer fejlesztési életciklusa	X	X	X	X	0	0	0
18.	3.3.3.3.	Funkciók, portok, protokollok, szolgáltatások	0	X	X	X	0	X	X
19.	3.3.3.4.	Fejlesztői változáskövetés	0	0	X	X	0	0	X
20.	3.3.3.5.	Fejlesztői biztonsági tesztelés	0	0	X	X	0	0	X
21.	3.3.3.6	Fejlesztési folyamat, szabványok és eszközök	0	0	0	X	0	0	0
22.	3.3.3.7.	Fejlesztői oktatás	0	0	0	X	0	0	0
23.	3.3.3.8.	Fejlesztői biztonsági architektúra és tervezés	0	0	0	X	0	0	0
24.	**3.3.4.**	**Biztonsági elemzés**							
25.	3.3.4.1.	Biztonságelemzési eljárásrend	0	X	X	X	0	X	X
26.	3.3.4.2.	Biztonsági értékelések	0	X	X	X	0	X	X
27.	3.3.4.3.	Speciális értékelés	0	0	X	X	0	0	X
28.	3.3.4.4.	A biztonsági teljesítmény mérése	0	X	X	X	0	X	X
29.	**3.3.5.**	**Tesztelés, képzés és felügyelet**							
30.	3.3.5.1.1.	Tesztelési, képzési és felügyeleti eljárások	0	X	X	X	0	X	X
31.	3.3.5.2.	A biztonsági teljesítmény mérése	0	X	X	X	0	X	X
32.	3.3.5.3.	Sérülékenység teszt	0	X	X	X	0	X	X
33.	3.3.5.3.2.	Frissítési képesség	0	X	X	X	0	0	0
34.	3.3.5.3.3.	Frissítés időközönként, új vizsgálat előtt vagy új sérülékenység feltárását követően	0	X	X	X	0	0	0
35.	3.3.5.3.4.	Privilegizált hozzáférés	0	X	X	X	0	X	X
36.	3.3.5.3.5.	Felfedhető információk	0	X	X	X	0	X	X
37.	**3.3.6.**	**Konfigurációkezelés**							
38.	3.3.6.1.	Konfigurációkezelési eljárásrend	X	X	X	X	X	X	X
39.	3.3.6.2.	Alap konfiguráció	X	X	X	X	X	X	X
40.	3.3.6.2.2.	Áttekintések és frissítések	0	0	X	X	0	0	X

41.	3.3.6.2.3.	Korábbi konfigurációk megőrzése	0	0	X	X	0	0	X
42.	3.3.6.2.4.	Magas kockázatú területek konfigurálása	0	0	X	X	0	0	X
43.	3.3.6.2.5.	Automatikus támogatás	0	0	0	X	0	0	0
44.	3.3.6.3.	A konfigurációváltozások felügyelete (változáskezelés)	0	X	X	X	0	X	X
45.	3.3.6.3.2.	Előzetes tesztelés és megerősítés	0	0	X	X	0	0	X
46.	3.3.6.3.3.	Automatikus támogatás	0	0	0	X	0	0	0
47.	3.3.6.4.	Biztonsági hatásvizsgálat	0	X	X	X	0	X	X
48.	3.3.6.4.2.	Elkülönített teszt környezet	0	0	0	X	0	0	0
49.	3.3.6.5.	A változtatásokra vonatkozó hozzáférés korlátozások	0	0	0	0	0	0	X
50.	3.3.6.5.2.	Automatikus támogatás	0	0	0	0	0	0	0
51.	3.3.6.5.3.	Felülvizsgálat	0	0	0	0	0	0	0
52.	3.3.6.5.4.	Aláírt elemek	0	0	0	0	0	0	0
53.	3.3.6.6.	Konfigurációs beállítások	0	X	X	X	0	X	X
54.	3.3.6.6.2.	Automatikus támogatás	0	0	0	X	0	0	0
55.	3.3.6.6.3.	Reagálás jogosulatlan változásokra	0	0	0	X	0	0	0
56.	3.3.6.7.	Legszűkebb funkcionalitás	0	X	X	X	0	X	X
57.	3.3.6.7.2.	Rendszeres felülvizsgálat	0	0	X	X	0	0	X
58.	3.3.6.7.3.	Nem futtatható szoftverek	0	0	X	X	0	0	X
59.	3.3.6.7.4.	Futtatható szoftverek	0	0	0	X	0	0	0
60.	3.3.6.8.	Elektronikus információs rendszerelem leltár	X	X	X	X	X	X	X
61.	3.3.6.8.2.	Frissítés	0	0	X	X	0	0	X
62.	3.3.6.8.3.	Jogosulatlan elemek automatikus észlelése	0	0	0	X	0	0	0
63.	3.3.6.8.4.	Duplikálás elleni védelem	0	0	0	X	0	0	0
64.	3.3.6.8.5.	Automatikus támogatás	0	0	0	X	0	0	0
65.	3.3.6.8.6.	Naplózás	0	0	0	X	0	0	0
66.	3.3.6.9.	Konfigurációkezelési terv	0	0	X	X	0	0	X
67.	3.3.6.10.	A szoftver használat korlátozásai	X	X	X	X	X	X	X
68.	3.3.6.11.	A felhasználó által telepített szoftverek	X	X	X	X	X	X	X
69.	**3.3.7.**	**Karbantartás**							
70.	3.3.7.1.	Rendszer karbantartási eljárásrend	0	0	0	0	X	X	X
71.	3.3.7.2.	Rendszeres karbantartás	0	0	0	0	X	X	X
72.	3.3.7.2.2.	Automatikus támogatás	0	0	0	0	0	0	0
73.	3.3.7.3.	Karbantartási eszközök	0	0	0	0	0	0	X
74.	3.3.7.3.2.	Adathordozó ellenőrzés	0	0	0	0	0	0	X
75.	3.3.7.4.	Távoli karbantartás	0	0	X	X	0	0	X
76.	3.3.7.4.2.	Dokumentálás	0	0	0	X	0	0	0
77.	3.3.7.4.3.	Összehasonlítható biztonság	0	0	0	X	0	0	0
78.	**3.3.8.**	**Adathordozók védelme**							
79.	3.3.8.1.	Adathordozók védelmére vonatkozó eljárásrend	X	X	X	X	X	X	X
80.	3.3.8.2.	Hozzáférés az adathordozókhoz	X	X	X	X	X	X	X
81.	3.3.8.3.	Adathordozók címkézése	0	0	X	X	0	0	0
82.	3.3.8.4.	Adathordozók tárolása	0	0	X	X	0	0	0
83.	3.3.8.5.	Adathordozók szállítása	0	0	X	X	0	0	X
84.	3.3.8.5.2.	Kriptográfiai védelem	0	0	X	X	0	0	X
85.	3.3.8.6.	Adathordozók törlése	X	X	X	X	0	0	0
86.	3.3.8.6.2.	Ellenőrzés	0	0	0	X	0	0	0
87.	3.3.8.6.3.	Tesztelés	0	0	0	X	0	0	0

88.	3.3.8.6.4.	Törlés megsemmisítés nélkül	0	0	0	X	0	0	0
89.	3.3.8.7.	Adathordozók használata	X	X	X	X	X	X	X
90.	3.3.8.7.2.	Ismeretlen tulajdonos	0	0	X	X	0	0	X
91.	**3.3.9.**	**Azonosítás és hitelesítés**							
92.	3.3.9.1.	Azonosítási és hitelesítési eljárásrend	X	X	X	X	X	X	X
93.	3.3.9.2.	Azonosítás és hitelesítés	X	X	X	X	X	X	X
94.	3.3.9.2.2.	Hálózati hozzáférés privilegizált fiókokhoz	0	X	X	X	0	0	X
95.	3.3.9.2.3.	Hálózati hozzáférés nem privilegizált fiókokhoz	0	0	X	X	0	0	X
96.	3.3.9.2.4.	Helyi hozzáférés privilegizált fiókokhoz	0	0	X	X	0	0	X
97.	3.3.9.2.5.	Visszajátszás-védelem	0	0	X	X	0	0	X
98.	3.3.9.2.6.	Távoli hozzáférés - külön eszköz	0	0	X	X	0	0	X
99.	3.3.9.2.7.	Helyi hozzáférés nem privilegizált fiókokhoz	0	0	0	X	0	0	0
100.	3.3.9.2.8.	Visszajátszás ellen védett hálózati hozzáférés nem privilegizált fiókokhoz	0	0	0	X	0	0	0
101.	3.3.9.3.	Eszközök azonosítása és hitelesítése	0	0	X	X	0	0	X
102.	3.3.9.4.	Azonosító kezelés	X	X	X	X	X	X	X
103.	3.3.9.5.	A hitelesítésre szolgáló eszközök kezelése	X	X	X	X	X	X	X
104.	3.3.9.5.2.	Jelszó (tudás) alapú hitelesítés	0	0	X	X	0	0	X
105.	3.3.9.5.3.	Birtoklás alapú hitelesítés	0	0	X	X	0	0	X
106.	3.3.9.5.4.	Tulajdonság alapú hitelesítés	0	0	X	X	0	0	X
107.	3.3.9.5.5.	Személyes vagy megbízható harmadik fél általi regisztráció	0	0	X	X	0	0	X
108.	3.3.9.6.	A hitelesítésre szolgáló eszköz visszacsatolása	X	X	X	X	X	X	X
109.	3.3.9.7.	Hitelesítés kriptográfiai modul esetén	0	X	X	X	0	X	X
110.	3.3.9.8.	Azonosítás és hitelesítés (szervezeten kívüli felhasználók)	X	X	X	X	X	X	X
111.	3.3.9.8.2.	Hitelesítés szolgáltatók tanúsítványának elfogadása	0	X	X	X	X	X	X
112.	**3.3.10.**	**Hozzáférés ellenőrzése**							
113.	3.3.10.1.	Hozzáférés ellenőrzési eljárásrend	X	X	X	X	X	X	X
114.	3.3.10.2.	Felhasználói fiókok kezelése	X	X	X	X	X	X	X
115.	3.3.10.2.2.	Automatikus kezelés	0	0	X	X	0	0	X
116.	3.3.10.2.3.	Ideiglenes fiókok eltávolítása	0	0	X	X	0	0	X
117.	3.3.10.2.4.	Inaktív fiókok letiltása	0	0	X	X	0	0	X
118.	3.3.10.2.5.	Automatikus naplózás	0	0	X	X	0	0	0
119.	3.3.10.2.6.	Kiléptetés	0	0	0	X	0	0	0
120.	3.3.10.2.7.	Szokatlan használat	0	0	0	X	0	0	0
121.	3.3.10.2.8.	Letiltás	0	0	0	X	0	0	0
122.	3.3.10.3.	Hozzáférés ellenőrzés érvényesítése	X	X	X	X	X	X	X
123.	3.3.10.4.	Információáramlás ellenőrzés érvényesítése	0	0	X	X	0	0	X
124.	3.3.10.5.	A felelősségek szétválasztása	0	0	X	X	0	0	X
125.	3.3.10.6.	Legkisebb jogosultság elve	0	0	X	X	0	0	X
126.	3.3.10.6.2.	Jogosult hozzáférés a biztonsági funkciókhoz	0	0	X	X	0	0	X

127.	3.3.10.6.3.	Nem privilegizált hozzáférés a biztonsági funkciókhoz	0	0	X	X	0	0	X
128.	3.3.10.6.4.	Privilegizált fiókok	0	0	X	X	0	0	X
129.	3.3.10.6.5.	Privilegizált funkciók használatának naplózása	0	0	X	X	0	0	X
130.	3.3.10.6.6.	Privilegizált funkciók tiltása nem privilegizált felhasználóknak	0	0	X	X	0	0	X
131.	3.3.10.6.7.	Hálózati hozzáférés a privilegizált parancsokhoz	0	0	0	X	0	0	0
132.	3.3.10.7.	Sikertelen bejelentkezési kísérletek	0	X	X	X	0	X	X
133.	3.3.10.8.	A rendszerhasználat jelzése	0	X	X	X	0	X	X
134.	3.3.10.9.	Egyidejű munkaszakasz kezelés	0	0	0	X	0	0	0
135.	3.3.10.10.	A munkaszakasz zárolása	0	0	X	X	0	0	X
136.	3.3.10.10.2.	Képernyőtakarás	0	0	X	X	0	0	X
137.	3.3.10.11.	A munkaszakasz lezárása	0	0	X	X	0	0	X
138.	3.3.10.12.	Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek	X	X	X	X	X	X	X
139.	3.3.10.13.	Távoli hozzáférés	0	X	X	X	0	X	X
140.	3.3.10.13.2.	Ellenőrzés	0	0	X	X	0	0	X
141.	3.3.10.13.3.	Titkosítás	0	0	X	X	0	0	X
142.	3.3.10.13.4.	Hozzáférés ellenőrzési pontok	0	0	X	X	0	0	X
143.	3.3.10.13.5.	Privilegizált parancsok elérése	0	0	X	X	0	0	X
144.	3.3.10.14.	Vezeték nélküli hozzáférés	0	X	X	X	0	X	X
145.	3.3.10.14.2.	Hitelesítés és titkosítás	0	0	0	X	0	0	0
146.	3.3.10.14.3.	Felhasználó konfigurálás tiltása	0	0	0	X	0	0	0
147.	3.3.10.14.4.	Antennák	0	0	0	X	0	0	0
148.	3.3.10.15.	Mobil eszközök hozzáférés ellenőrzése	0	X	X	X	0	X	X
149.	3.3.10.15.2.	Titkosítás	0	0	X	X	0	0	X
150.	3.3.10.16.	Külső elektronikus információs rendszerek használata	X	X	X	X	X	X	X
151.	3.3.10.16.2.	Korlátozott használat	0	0	X	X	0	0	X
152.	3.3.10.16.3.	Hordozható adattároló eszközök	0	0	X	X	0	0	X
153.	3.3.10.17.	Információ megosztás	0	0	X	X	0	0	0
154.	3.3.10.18.	Nyilvánosan elérhető tartalom	X	X	X	X	X	X	X
155.	**3.3.11.**	**Rendszer és információ sértetlenség**							
156.	3.3.11.2.	Rendszer és információ sértetlenségre vonatkozó eljárásrend	0	0	0	0	X	X	X
157.	3.3.11.3.	Hibajavítás	0	0	0	0	X	X	X
158.	3.3.11.3.2.	Automatizált hibajavítási állapot	0	0	0	0	0	0	X
159.	3.3.11.3.3.	Központi kezelés	0	0	0	0	0	0	0
160.	3.3.11.4.	Kártékony kódok elleni védelem	X	X	X	X	X	X	X
161.	3.3.11.4.2.	Központi kezelés	0	0	X	X	0	0	X
162.	3.3.11.4.3.	Automatikus frissítés	0	0	X	X	0	0	X
163.	3.3.11.5.	Az elektronikus információs rendszer felügyelete	X	X	X	X	X	X	X
164.	3.3.11.5.2.	Automatizálás	0	0	X	X	0	0	X
165.	3.3.11.5.3.	Felügyelet	0	0	X	X	0	0	X
166.	3.3.11.5.4.	Riasztás	0	0	X	X	0	0	X
167.	3.3.11.6.	Biztonsági riasztások és tájékoztatások	0	X	X	X	0	X	X
168.	3.3.11.6.2.	Automatikus riasztások	0	0	0	X	0	0	0
169.	3.3.11.7.	A biztonsági funkcionalitás ellenőrzése	0	0	0	X	0	0	0

170.	3.3.11.8.	Szoftver és információ sértetlenség	0	0	X	X	0	0	X
171.	3.3.11.8.2.	Sértetlenség ellenőrzés	0	0	0	X	0	0	0
172.	3.3.11.8.3.	Észlelés és reagálás	0	0	0	X	0	0	0
173.	3.3.11.8.4.	Automatikus értesítés	0	0	0	X	0	0	0
174.	3.3.11.8.5.	Automatikus reagálás	0	0	0	X	0	0	0
175.	3.3.11.8.6.	Végrehajtható kód	0	0	0	X	0	0	0
176.	3.3.11.9.	Kéretlen üzenetek elleni védelem	0	0	0	0	0	0	X
177.	3.3.11.9.2.	Központi kezelés	0	0	0	0	0	0	X
178.	3.3.11.9.3.	Frissítés	0	0	0	0	0	0	X
179.	3.3.11.10.	Bemeneti információ ellenőrzés	0	0	0	0	0	0	X
180.	3.3.11.11.	Hibakezelés	0	0	0	0	0	0	X
181.	3.3.11.12.	A kimeneti információ kezelése és megőrzése	X	X	X	X	X	X	X
182.	3.3.11.13.	Memória védelem	0	0	X	X	0	0	X
183.	**3.3.12.**	**Naplózás és elszámoltathatóság**							
184.	3.3.12.1.	Naplózási eljárásrend	X	X	X	X	X	X	X
185.	3.3.12.2.	Naplózható események	X	X	X	X	X	X	X
186.	3.3.12.2.2.	Felülvizsgálat	0	0	0	X	0	0	0
187.	3.3.12.3.	Naplóbejegyzések tartalma	X	X	X	X	X	X	X
188.	3.3.12.3.2.	Kiegészítő információk	0	0	X	X	0	0	X
189.	3.3.12.3.3.	Központi kezelés	0	0	0	X	0	0	0
190.	3.3.12.4.	Napló tárkapacitás	0	X	X	X	0	X	X
191.	3.3.12.5.	Naplózási hiba kezelése	0	X	X	X	0	X	X
192.	3.3.12.5.2.	Naplózási tárhely ellenőrzés	0	0	0	X	0	0	0
193.	3.3.12.5.3.	Valósidejű riasztás	0	0	0	X	0	0	0
194.	3.3.12.6.	Naplóvizsgálat és jelentéskészítés	0	X	X	X	0	X	X
195.	3.3.12.6.2.	Folyamatba illesztés	0	0	0	X	0	0	0
196.	3.3.12.6.3.	Összegzés	0	0	0	X	0	0	0
197.	3.3.12.6.4.	Felügyeleti képességek integrálása	0	0	0	X	0	0	0
198.	3.3.12.6.5.	Összekapcsolás a fizikai hozzáférési információkkal	0	0	0	X	0	0	0
199.	3.3.12.7.	Naplócsökkentés és jelentéskészítés	0	0	X	X	0	0	X
200.	3.3.12.7.2.	Automatikus feldolgozás	0	0	X	X	0	0	X
201.	3.3.12.8.	Időbélyegek	X	X	X	X	X	X	X
202.	3.3.12.8.2.	Szinkronizálás	0	0	X	X	0	0	X
203.	3.3.12.9.	A naplóinformációk védelme	X	X	X	X	X	X	X
204.	3.3.12.9.2.	Hozzáférés korlátozás	0	0	0	0	0	0	0
205.	3.3.12.9.3.	Fizikailag elkülönített mentés	0	0	0	0	0	0	0
206.	3.3.12.9.4.	Kriptográfiai védelem	0	0	0	0	0	0	0
207.	3.3.12.10.	Letagadhatatlanság	0	0	0	X	0	0	0
208.	3.3.12.11.	A naplóbejegyzések megőrzése	X	X	X	X	X	X	X
209.	3.3.12.12.	Naplógenerálás	X	X	X	X	X	X	X
210.	3.3.12.12.2.	Rendszerszintű időalap napló	0	0	0	X	0	0	0
211.	3.3.12.12.3.	Változtatások	0	0	0	X	0	0	0
212.	**3.3.13.**	**Rendszer- és kommunikáció védelem**							
213.	3.3.13.1.	Rendszer- és kommunikáció védelmi eljárásrend	X	X	X	X	X	X	X
214.	3.3.13.2.	Alkalmazás szétválasztás	0	0	X	X	0	0	X
215.	3.3.13.3.	Biztonsági funkciók elkülönítése	0	0	0	X	0	0	0
216.	3.3.13.4.	Információmaradványok	0	0	X	X	0	0	0
217.	3.3.13.5.	Túlterhelés - szolgáltatás megtagadás alapú támadás - elleni védelem	0	0	0	0	0	0	0

218.	3.3.13.6.	A határok védelme	X	X	X	X	X	X	X
219.	3.3.13.6.2.	Hozzáférési pontok	0	0	0	X	0	0	0
220.	3.3.13.6.3.	Külső kommunikációs szolgáltatások	0	0	0	X	0	0	0
221.	3.3.13.6.4.	Alapeseti visszautasítás	0	0	0	X	0	0	0
222.	3.3.13.6.5.	Távoli készülékek megosztott csatornahasználatának tiltása	0	0	0	X	0	0	0
223.	3.3.13.6.6.	Hitelesített proxy kiszolgálók	0	0	0	X	0	0	0
224.	3.3.13.6.7.	Biztonsági hibaállapot	0	0	0	X	0	0	0
225.	3.3.13.6.8.	Rendszerelemek elkülönítése	0	0	0	X	0	0	0
226.	3.3.13.7.	Az adatátvitel bizalmassága	0	0	X	X	0	0	0
227.	3.3.13.7.2.	Kriptográfiai vagy egyéb védelem	0	0	X	X	0	0	0
228.	3.3.13.8.	Az adatátvitel sértetlensége	0	0	0	0	0	0	X
229.	3.3.13.8.2.	Kriptográfiai vagy egyéb védelem	0	0	0	0	0	0	X
230.	3.3.13.9.	A hálózati kapcsolat megszakítása	0	0	0	0	0	0	0
231.	3.3.13.10.	Kriptográfiai kulcs előállítása és kezelése	X	X	X	X	X	X	X
232.	3.3.13.10.2.	Rendelkezésre állás	0	0	0	X	0	0	0
233.	3.3.13.11.	Kriptográfiai védelem	X	X	X	X	X	X	X
234.	3.3.13.12.	Együttműködésen alapuló számítástechnikai eszközök	X	X	X	X	0	0	0
235.	3.3.13.13.	Nyilvános kulcsú infrastruktúra tanúsítványok	0	0	X	X	0	0	X
236.	3.3.13.14.	Mobilkód korlátozása	0	0	X	X	0	0	X
237.	3.3.13.15.	Elektronikus Információs rendszeren keresztüli hangátvitel (úgynevezett VoIP)	0	0	X	X	0	0	0
238.	3.3.13.16.	Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás)	0	0	0	0	0	X	X
239.	3.3.13.17.	Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív vagy gyorsító tárat használó feloldás)	0	0	0	0	0	X	X
240.	3.3.13.18.	Architektúra és tartalékok név/cím feloldási szolgáltatás esetén	0	0	0	0	0	X	X
241.	3.3.13.19.	Munkaszakasz hitelessége	0	0	0	0	0	0	X
242.	3.3.13.20.	Hibát követő ismert állapot	0	0	0	X	0	0	0
243.	3.3.13.21.	A maradvány információ védelme	0	0	X	X	0	0	X
244.	3.3.13.22.	A folyamatok elkülönítése	X	X	X	X	X	X	X

4. melléklet a 41/2015. (VII. 15.) BM rendelethez

AZ ADMINISZTRATÍV, FIZIKAI ÉS LOGIKAI BIZTONSÁGI KÖVETELMÉNYEK

1. ELTÉRÉSEK

1.1. Általános követelmények

Az érintett szervezetnek az alábbi lehetséges eltérésekkel és helyettesítő intézkedésekkel lehet teljesítenie a 3. pont szerinti védelmi intézkedés katalógusban meghatározott minimális követelményeket, a rendszerre meghatározott biztonsági kockázati szintnek megfelelő intézkedések kiválasztásával, amellett, hogy az érintett szervezetre érvényes minden kötelezettséget figyelembe kell venni.

1.2. Egyedi eltérések

1.2.1. Működtetéssel, környezettel kapcsolatos eltérések:

1.2.1.1. A működtetési környezet jellegétől függő biztonsági intézkedések csak akkor alkalmazandók, ha az elektronikus információs rendszert az intézkedéseket szükségessé tevő környezetben használják.

1.2.2. A fizikai infrastruktúrával kapcsolatos eltérések:

1.2.2.1. A szervezeti létesítményekkel kapcsolatos biztonsági intézkedések (zárak, őrök, környezeti paraméterek: hőmérséklet, páratartalom stb.) csak a létesítmény azon részeire alkalmazandók, amelyek közvetlenül nyújtanak védelmet vagy biztonsági támogatást az elektronikus információs rendszernek, vagy kapcsolatosak azzal (ideértve a rendszerelemeket is, mint például e-mail, web szerverek, szerver farmok, adatközpontok, hálózati csomópontok, határvédelmi eszközök és kommunikációs berendezések).

1.2.3. A nyilvános hozzáféréssel kapcsolatos eltérések:

1.2.3.1. A nyilvánosan hozzáférhető információkra vonatkozó biztonsági intézkedéseket körültekintően kell számba venni, és végrehajtani, mivel a vonatkozó védelmi intézkedés katalógus rész egyes biztonsági intézkedései (például azonosítás és hitelesítés, személyi biztonsági intézkedések) nem alkalmazhatók az elektronikus információs rendszerhez engedélyezett nyilvános kapcsolaton keresztül hozzáférő felhasználókra.

1.2.4. Technológiai eltérések:

1.2.4.1. A specifikus technológiára [például vezeték nélküli kommunikáció, kriptográfia, nyilvános kulcsú infrastruktúrán (PKI) alapuló hitelesítési eljárás] vonatkozó biztonsági intézkedések csak akkor alkalmazandók, ha ezeket a technológiákat használják az elektronikus információs rendszerben, vagy előírják ezek használatát.

1.2.4.2. A biztonsági intézkedések az elektronikus információs rendszer csak azon komponenseire vonatkoznak, amelyek az intézkedés által megcélzott biztonsági képességet biztosítják vagy támogatják, és az intézkedés által csökkenteni kívánt lehetséges kockázatok forrásai.

1.2.5. Biztonsági szabályozással kapcsolatos eltérések:

1.2.5.1. A tervezett, vagy már működtetett elektronikus információs rendszerekre alkalmazott biztonsági intézkedések kialakítása során figyelembe kell venni a rendszer célját meghatározó jogszabályi hátteret, funkciót is.

1.2.6. A biztonsági intézkedések bevezetésének fokozatosságával kapcsolatos eltérések:

1.2.6.1. A biztonsági intézkedések fokozatosan vezethetők be. A fokozatosságot a védendő elektronikus információs rendszerek biztonsági kategorizálása alapján lehet felállítani.

1.2.7. A biztonsági célokhoz kapcsolódó eltérések:

1.2.7.1. Azok a biztonsági intézkedések, amelyek kizárólagosan támogatják a bizalmasságot, a sértetlenséget és a rendelkezésre állást, visszasorolhatók (vagy módosíthatók, kivehetők, ha alacsonyabb követelményszinten nincsenek meghatározva) alacsonyabb követelményszintre, ha ez az alacsonyabb szintű besorolás:

1.2.7.1.1. összhangban van a vonatkozó bizalmasságra, sértetlenségre vagy rendelkezésre állásra vonatkozóan az úgynevezett „high water mark” elv alkalmazása előtt megállapított biztonsági követelményszinttel, amely elv az információbiztonság szempontjából azt jelenti, hogy a legmagasabb biztonsági célhoz kell hangolni minden elemet;

1.2.7.1.2. a „high water mark” elv alkalmazásával az eredeti bizalmassági, sértetlenségi és rendelkezésre állási biztonsági célokat meghaladó, magasabb biztonsági intézkedés szint meghatározás történt, de ez a magasabb biztonsági intézkedési szint nem szükséges a költséghatékony, kockázatarányos biztonsági intézkedések szempontjából;

1.2.7.1.3. az érintett szervezetre végrehajtott kockázatelemzés szerint indokolható;

1.2.7.1.4. nem befolyásolja a biztonsági szempontból fontos információkat az elektronikus információs rendszeren belül.

1.2.7.2.[1] Az elektronikus információs rendszer dokumentáltan elkülönített, informatikai biztonsági szempontból önállóan értékelhető elemei tekintetében a biztonsági intézkedések a szervezet által elfogadott kockázatelemzési és kockázatkezelési eljárásrendben rögzített vizsgálatot követően, külön-külön egyedi eltérésekkel is alkalmazhatóak, ha az elkülönített elemek közötti határvédelemről gondoskodtak. A határvédelem megfelelőségét, valamint az egyedi eltérések okát és mértékét dokumentálni és meghatározott gyakorisággal felülvizsgálni szükséges.

2. HELYETTESÍTŐ BIZTONSÁGI INTÉZKEDÉSEK

2.1. A helyettesítő biztonsági intézkedés olyan eljárás, amelyet az érintett szervezet az adott biztonsági osztályhoz tartozó biztonsági intézkedés helyett alkalmazni kíván, és egyenértékű vagy összemérhető védelmet nyújt az adott elektronikus információs rendszerre valós fenyegetést jelentő veszélyforrások ellen, és a helyettesített intézkedéssel egyenértékű módon biztosít minden külső vagy belső követelménynek (például törvényeknek vagy szervezeti szintű szabályzóknak) való megfelelést.

2.2. Egy elektronikus információs rendszer esetén az érintett szervezet az alábbi feltételek teljesülése esetén alkalmazhat helyettesítő intézkedést:

2.2.1. ha az elektronikus információs rendszerek biztonságára vonatkozó szabványokban vagy hazai ajánlásokban fellelhető helyettesítő intézkedést választja, vagy ha ezekben nincs megfelelő helyettesítő intézkedés, akkor az érintett szervezet kivételesen alkalmazhat egy, az adott helyzetben megfelelő helyettesítő intézkedést;

2.2.2. a helyettesítő intézkedések kiválasztásánál az érintett szervezetnek törekednie kell arra, hogy a védelmi intézkedés katalógusból válasszon intézkedést; az érintett szervezet által meghatározott helyettesítő intézkedéseket csak végső esetben szabad használni, ha a biztonsági intézkedések katalógusa nem tartalmaz az adott viszonyok között alkalmazható intézkedést;

---

1 Beiktatta: 58/2016. (XII. 22.) BM rendelet 52. §, 4. melléklet 1. Hatályos: 2017. I. 1-től.

2.2.3. a vonatkozó szabályozásában be kell mutatnia, hogy a helyettesítő intézkedések hogyan biztosítják az elektronikus információs rendszer egyenértékű biztonsági képességeit, védelmi követelményszintjét, és azt, hogy miért nem használhatók a vonatkozó alapkészlet biztonsági intézkedései;

2.2.4. a 2.2.3. pont szerinti indoklás részletezettségének és szigorúságának az elektronikus információs rendszerre megállapított biztonsági követelményszintnek megfelelőnek kell lennie;

2.2.5. ha felméri, és a kockázatkezelési eljárási rendnek megfelelően elfogadja a helyettesítő intézkedés alkalmazásával kapcsolatos kockázatot;

2.2.6. a helyettesítő biztonsági intézkedések alkalmazását dokumentálja, és az eljárási rendnek megfelelően az érintett személlyel vagy szerepkörrel jóváhagyatja.

3. VÉDELMI INTÉZKEDÉS KATALÓGUS

3.1. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

3.1.1. SZERVEZETI SZINTŰ ALAPFELADATOK

3.1.1.1. Informatikai biztonsági szabályzat

3.1.1.1.1. Az érintett szervezet:

3.1.1.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonsági szabályzatot;

3.1.1.1.1.2. más belső szabályozásában, vagy magában az informatikai biztonsági szabályzatban meghatározza az informatikai biztonsági szabályzat felülvizsgálatának és frissítésének gyakoriságát;

3.1.1.1.1.3. gondoskodik arról, hogy az informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.

3.1.1.1.2. Az informatikai biztonsági szabályzatban meg kell határozni:

3.1.1.1.2.1. a célokat, a szabályzat tárgyi és személyi (a szervezet jellegétől függően területi) hatályát;

3.1.1.1.2.2. az elektronikus információbiztonsággal kapcsolatos szerepköröket;

3.1.1.1.2.3. a szerepkörhöz rendelt tevékenységet;

3.1.1.1.2.4. a tevékenységhez kapcsolódó felelősséget;

3.1.1.1.2.5. az információbiztonság szervezetrendszerének belső együttműködését.

3.1.1.1.3. Az informatikai biztonsági szabályzat elsősorban a következő elektronikus információs rendszerbiztonsággal kapcsolatos területeket szabályozza:

3.1.1.1.3.1. kockázatelemzés (amely szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz);

3.1.1.1.3.2. biztonsági helyzet-, és eseményértékelés eljárási rendje;

3.1.1.1.3.3. az elektronikus információs rendszer (ideértve ezek elemeit is) és információtechnológiai szolgáltatás beszerzés (ha az érintett szervezet ilyet végez, vagy végezhet);

3.1.1.1.3.4. biztonsággal kapcsolatos tervezés (például: beszerzés, fejlesztés, eljárásrendek kialakítását);

3.1.1.1.3.5. fizikai és környezeti védelem szabályai, jellemzői;

3.1.1.1.3.6. az emberi erőforrásokban rejlő veszélyek megakadályozása (pl.: személyzeti felvételi- és kilépési eljárás során követendő szabályok, munkavégzésre irányuló szerződésben a személyes kötelmek rögzítése, a felelősség érvényesítése, stb.);

3.1.1.1.3.7. az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében;

3.1.1.1.3.8. az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatok, elvárások, jogok (ha az érintett szervezetnél ez értelmezhető);

3.1.1.1.3.9. üzlet-, ügy- vagy üzemmenet folytonosság tervezése (így különösen a rendszerleállás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása, stb.);

3.1.1.1.3.10. az elektronikus információs rendszerek karbantartásának rendje;

3.1.1.1.3.11. az adathordozók fizikai és logikai védelmének szabályozása;

3.1.1.1.3.12. az elektronikus információs rendszerhez való hozzáférés során követendő azonosítási és hitelesítési eljárás, és a hozzáférési szabályok betartásának ellenőrzése;

3.1.1.1.3.13. ha az érintett szervezetnek erre lehetősége van, a rendszerek használatáról szóló rendszerbejegyzések értékelése, az értékelés eredményétől függő eljárások meghatározása;

3.1.1.1.3.14. az adatok mentésének, archiválásának rendje;

3.1.1.1.3.15. a biztonsági események - ideértve az adatok sérülését is - bekövetkeztekor követendő eljárás, ideértve a helyreállítást;

3.1.1.1.3.16. az elektronikus információs rendszerhez jogosultsággal (vagy jogosultság nélkül fizikailag) hozzáférő, nem az érintett szervezet tagjainak tevékenységét szabályozó (karbantartók, magán-, vagy polgári jogi szerződés alapján az érintett szervezet számára feladatokat végrehajtók), az elektronikus információbiztonságot érintő, szerződéskötés során érvényesítendő követelmények.

3.1.1.1.4. Az informatikai biztonsági szabályzat tartalmazza az érintett szervezet elvárt biztonsági szintjét, valamint az érintett szervezet egyes elektronikus információs rendszereinek elvárt biztonsági osztályát.

3.1.1.2. Az elektronikus információs rendszerek biztonságáért felelős személy

3.1.1.2.1. Az érintett szervezet vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg, aki ellátja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 13. §-ában meghatározott feladatokat.

3.1.1.3. Az intézkedési terv és mérföldkövei

3.1.1.3.1. Az érintett szervezet:

3.1.1.3.1.1. intézkedési tervet készít, ebben mérföldköveket határoz meg;

3.1.1.3.1.2. meghatározott időnként felülvizsgálja és karbantartja az intézkedési tervet:

3.1.1.3.1.2.1. a kockázatkezelési stratégia és a kockázatokra adott válasz tevékenységek prioritása alapján;

3.1.1.3.1.2.2. ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, a hiányosság megszüntetése érdekében;

3.1.1.3.1.2.3. ha a meghatározott biztonsági szint alacsonyabb, mint az érintett szervezetre érvényes szint, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, az előírt biztonsági szint elérése érdekében.
3.1.1.3.1.3. folyamatosan aktualizálja a nyilvántartást.
3.1.1.4. Az elektronikus információs rendszerek nyilvántartása
3.1.1.4.1. Az érintett szervezet:
3.1.1.4.1.1. elektronikus információs rendszereiről nyilvántartást vezet;
3.1.1.4.1.2. folyamatosan aktualizálja a nyilvántartást.
3.1.1.4.2. A nyilvántartás minden rendszerre nézve tartalmazza:
3.1.1.4.2.1. annak alapfeladatait;
3.1.1.4.2.2. a rendszerek által biztosítandó szolgáltatásokat;
3.1.1.4.2.3. az érintett rendszerekhez tartozó licenc számot (ha azok az érintett szervezet kezelésében vannak);
3.1.1.4.2.4. a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;
3.1.1.4.2.5. a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.
3.1.1.5. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás
3.1.1.5.1. Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, az érintett szervezet hatókörébe tartozó:
3.1.1.5.1.1. emberi, fizikai és logikai erőforrásra;
3.1.1.5.1.2. eljárási és védelmi követelményszintre és folyamatra.

3.1.2. KOCKÁZATELEMZÉS

3.1.2.1. Kockázatelemzési és kockázatkezelési eljárásrend
3.1.2.1.1. Az érintett szervezet:
3.1.2.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a kockázatelemzési és kockázatkezelési eljárásrendet, mely a kockázatelemzési és kockázatkezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
3.1.2.1.1.2. belső szabályozásában, vagy magában a kockázatelemzési és kockázatkezelési eljárásrendről szóló dokumentumban meghatározza a kockázatelemzési és kockázatkezelési eljárásrend felülvizsgálatának és frissítésének gyakoriságát.
3.1.2.1.2. Az eljárásrend kiterjed:
3.1.2.1.2.1. a lehetséges kockázatok felmérésére;
3.1.2.1.2.2. a kockázatok kezelésének felelősségére;
3.1.2.1.2.3. a kockázatok kezelésének elvárt minőségére.
3.1.2.2. Biztonsági osztályba sorolás
3.1.2.2.1. Az érintett szervezet:
3.1.2.2.1.1. jogszabályban meghatározott szempontok alapján megvizsgálja elektronikus információs rendszereit, és a 3.1.1.4. pont szerinti nyilvántartás alapján meghatározza, hogy azok melyik biztonsági osztályba sorolandók;
3.1.2.2.1.2. vezetője jóváhagyja a biztonsági osztályba sorolást;
3.1.2.2.1.3. rögzíti a biztonsági osztályba sorolás eredményét a szervezet informatikai biztonsági szabályzatában.
3.1.2.2.2. Elvárás:

3.1.2.2.2.1. a biztonsági osztályba sorolást az elektronikus információs rendszereket érintő változások után ismételten el kell végezni;
3.1.2.2.2.2. kapcsolódást kell biztosítani a 3.1.1.3. pontban foglalt intézkedési tervhez és mérföldköveihez.
3.1.2.3. Kockázatelemzés
3.1.2.3.1. Az érintett szervezet:
3.1.2.3.1.1. végrehajtja a biztonsági kockázatelemzéseket;
3.1.2.3.1.2. rögzíti a kockázatelemzések eredményét az informatikai biztonsági szabályzatban, kockázatelemzési jelentésben, vagy a kockázatelemzési eljárásrendben előírt dokumentumban;
3.1.2.3.1.3. a kockázatelemzési eljárásrendnek megfelelően felülvizsgálja a kockázatelemzések eredményét;
3.1.2.3.1.4. a kockázatelemzési eljárásrendnek megfelelően, vagy a 3.1.1.1. pont szerinti informatikai biztonsági szabályzata keretében megismerteti a kockázatelemzés eredményét az érintettekkel;
3.1.2.3.1.5. amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát, ismételt kockázatelemzést hajt végre;
3.1.2.3.1.6. gondoskodik arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek megismerhetők.

3.1.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

3.1.3.0. Jelen címben meghatározott eljárásokat abban az esetben nem kell bevezetni az érintett szervezetnél, ha saját hatókörében informatikai szolgáltatást, vagy eszközöket nem szerez be, és nem végez, vagy végeztet rendszerfejlesztési tevékenységet (ide nem értve a jellemzően kis értékű, kereskedelmi forgalomban kapható általában irodai alkalmazásokat, szoftvereket, vagy azokat a hardver beszerzéseket, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzéseket). Jelen fejezet alkalmazása szempontjából nem minősül fejlesztésnek a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése.
3.1.3.1. Beszerzési eljárásrend
3.1.3.1.1. Az érintett szervezet:
3.1.3.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a beszerzési eljárásrendet, mely az érintett szervezet elektronikus információs rendszerére, az ezekhez kapcsolódó szolgáltatások és információs rendszer biztonsági eszközök beszerzésére vonatkozó szabályait fogalmazza meg (akár az általános beszerzési szabályzat részeként), és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
3.1.3.1.1.2. a beszerzési eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a beszerzési eljárásrendet.
3.1.3.2. Erőforrás igény felmérés
3.1.3.2.1. Az érintett szervezet:

3.1.3.2.1.1. az elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében meghatározza, és dokumentálja, valamint biztosítja az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházás tervezés részeként;

3.1.3.2.1.2. elkülönítetten kezeli az elektronikus információs rendszerek biztonságát beruházás tervezési dokumentumaiban.

3.1.3.3. Beszerzések

3.1.3.3.1. Az érintett szervezet az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként meghatározza:

3.1.3.3.1.1. a funkcionális biztonsági követelményeket;

3.1.3.3.1.2. a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);

3.1.3.3.1.3. a biztonsággal kapcsolatos dokumentációs követelményeket;

3.1.3.3.1.4. a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;

3.1.3.3.1.5. az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

3.1.3.3.2. A védelem szempontjainak érvényesítése a beszerzés során

Az érintett szervezet védi az elektronikus információs rendszert, rendszerelemet vagy rendszerszolgáltatást a beszerzés, vagy a beszerzett eszköz beillesztéséből adódó kockázatok ellen.

Az érintett szervezet szerződéses követelményként meghatározza a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.

3.1.3.3.3. A védelmi intézkedések terv-, és megvalósítási dokumentációi

Az érintett szervezet szerződéses követelményként meghatározza a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációit, köztük a biztonsággal kapcsolatos külső rendszer interfészek leírását, a magas és alacsony szintű biztonsági tervet, - ha azzal a szállító rendelkezik - a forráskódot és futtatókörnyezetet.

3.1.3.3.4. Funkciók - protokollok - szolgáltatások

Az érintett szervezet szerződéses rendelkezésként megköveteli a fejlesztőtől, szállítótól, hogy már a fejlesztési életciklus korai szakaszában meghatározza a használatra tervezett funkciókat, protokollokat és szolgáltatásokat.

3.1.3.4. Az elektronikus információs rendszerre vonatkozó dokumentáció

3.1.3.4.1. Az érintett szervezet:

3.1.3.4.1.1. ha hatókörébe tartozik, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza:

3.1.3.4.1.1.1. a rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,

3.1.3.4.1.1.2. a biztonsági funkciók hatékony alkalmazását és fenntartását,

3.1.3.4.1.1.3. a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket;

3.1.3.4.1.2. megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza:

3.1.3.4.1.2.1. a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját,

3.1.3.4.1.2.2. a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit,

3.1.3.4.1.2.3. a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához;

3.1.3.4.1.3. gondoskodik arról, hogy az információs rendszerre vonatkozó - különösen az adminisztrátori és fejlesztői - dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható;

3.1.3.4.1.4. gondoskodik a dokumentációknak az érintett szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.

3.1.3.5. Biztonságtervezési elvek

Az érintett szervezet biztonságtervezési elveket dolgoz ki és alkalmaz az elektronikus információs rendszer specifikációjának meghatározása, tervezése, fejlesztése, kivitelezése és módosítása során.

3.1.3.6. Külső elektronikus információs rendszerek szolgáltatásai

3.1.3.6.1. Az érintett szervezet:

3.1.3.6.1.1. szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az érintett szervezet elektronikus információbiztonsági követelményeinek;

3.1.3.6.1.2. meghatározza és dokumentálja az érintett szervezet felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban;

3.1.3.6.1.3. külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

3.1.3.7. Független értékelők

Az érintett szervezet független értékelőket vagy értékelő csoportokat alkalmaz a védelmi intézkedések értékelésére.

3.1.3.8. Folyamatos ellenőrzés

3.1.3.8.1. Az érintett szervezet folyamatba épített ellenőrzést vagy ellenőrzési tervet hajt végre, amely tartalmazza:

3.1.3.8.1.1. az ellenőrizendő területeket;

3.1.3.8.1.2. az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakoriságát;

3.1.3.8.1.3. az érintett szervezet ellenőrzési stratégiájához illeszkedő folyamatos biztonsági értékeléseket;

3.1.3.8.1.4. a mérőszámok megfelelőségét;

3.1.3.8.1.5. az értékelések és az ellenőrzések által generált biztonsággal kapcsolatos adatok összehasonlító elemzését;

3.1.3.8.1.6. az érintett szervezet reagálását a biztonsággal kapcsolatos adatok elemzésének eredményére;

3.1.3.8.1.7. az érintett szervezet döntését arról, hogy milyen gyakorisággal kell az elemzési adatokat általa meghatározott személyi- és szerepkörökkel megismertetni (ideértve azok változásait is).

3.1.3.8.2. Független értékelés

Az érintett szervezet független értékelőket vagy értékelő csoportokat alkalmazhat az elektronikus információs rendszer védelmi intézkedéseinek folyamatos ellenőrzésére.

3.1.4. ÜZLETMENET-(ÜGYMENET-)FOLYTONOSSÁG TERVEZÉSE

3.1.4.1. Üzletmenet-folytonosságra vonatkozó eljárásrend

3.1.4.1.1. Az érintett szervezet:

3.1.4.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül az érintett személyi kör részére kihirdeti az elektronikus információs rendszerre vonatkozó eljárásrendet, mely az üzletmenet-folytonosságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.1.4.1.1.2. az üzletmenet-folytonossági tervben, vagy más szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti az üzletmenet-folytonosságra vonatkozó eljárásrendet.

3.1.4.2. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

3.1.4.2.1. Az érintett szervezet:

3.1.4.2.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az elektronikus információs rendszerekre vonatkozó üzletmenet-folytonossági tervet;

3.1.4.2.1.2. összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;

3.1.4.2.1.3. meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet;

3.1.4.2.1.4. az elektronikus információs rendszer vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja az üzletmenet-folytonossági tervet;

3.1.4.2.1.5. tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket;

3.1.4.2.1.6. gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható;

3.1.4.2.1.7. meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;

3.1.4.2.1.8. rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;

3.1.4.2.1.9. jelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket;

3.1.4.2.1.10. fenntartja a szervezet által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is;

3.1.4.2.1.11. kidolgozza a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

3.1.4.2.2. Egyeztetés

Az üzletmenet-folytonossági tervet egyeztetni kell a kapcsolódó, hasonló tervekért felelős szervezeti egységekkel.

3.1.4.2.3. Alapfunkciók újraindítása

Meg kell határozni az alapfunkciók újrakezdésének időpontját az üzletmenet-folytonossági terv aktiválását követőn.

3.1.4.2.4. Kritikus rendszerelemek meghatározása

Meg kell határozni az elektronikus információs rendszer alapfunkcióit támogató kritikus rendszerelemeket.

3.1.4.2.5. Kapacitástervezés

Meg kell tervezni a folyamatos működéshez szükséges információ-feldolgozó, infokommunikációs és környezeti képességek biztosításához szükséges kapacitást.

3.1.4.2.6. Összes funkció újraindítása

Meg kell határozni az összes funkció újrakezdésének időpontját az üzletmenet-folytonossági terv aktiválását követően.

3.1.4.2.7. Alapfeladatok és alapfunkciók folyamatossága

Az alapfeladatok és alapfunkciók folyamatosságát úgy kell megtervezni, hogy azok üzemelési folyamatosságában semmilyen, vagy csak csekély veszteség álljon elő, fenntartható legyen a folyamatosság az elektronikus információs rendszer elsődleges feldolgozó vagy tárolási helyszínén történő teljes helyreállításáig.

3.1.4.3. A folyamatos működésre felkészítő képzés

3.1.4.3.1. Az érintett szervezet az elektronikus információs rendszer folyamatos működésére felkészítő képzést tart a felhasználóknak, szerepkörüknek és felelősségüknek megfelelően:

3.1.4.3.1.1. szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül;

3.1.4.3.1.2. meghatározott gyakorisággal, vagy amikor az elektronikus információs rendszer változásai ezt szükségessé teszik.

3.1.4.3.2. Szimuláció

A folyamatos működésre felkészítő képzésben szimulált eseményeket kell alkalmazni, hogy elősegítse a személyzet hatékony reagálását a kritikus helyzetekben.

3.1.4.4. Az üzletmenet-folytonossági terv tesztelése

3.1.4.4.1. Az érintett szervezet:

3.1.4.4.1.1. meghatározott gyakorisággal és meghatározott teszteken keresztül vizsgálja az elektronikus információs rendszerre vonatkozó üzletmenet-folytonossági tervet a terv hatékonyságának és az érintett szervezet felkészültségének a felmérése céljából;

3.1.4.4.1.2. értékeli az üzletmenet-folytonossági terv tesztelési eredményeit;

3.1.4.4.1.3. az értékelés alapján szükség esetén javítja a tervet, a javításokkal kapcsolatban az üzletmenet-folytonossági tervre vonatkozó általános eljárási szabályok szerint jár el.

3.1.4.4.2. Koordináció

Az üzletmenet-folytonossági terv tesztelését a kapcsolódó tervekért felelős szervezeti egységekkel egyeztetni kell.

3.1.4.4.3. Tesztelés a tartalék feldolgozási helyszínen

Az üzletmenet folytonossági tervet a tartalék feldolgozási helyszínen is tesztelni kell, hogy az érintett szervezet megismerje az adottságokat és az elérhető erőforrásokat, valamint értékelje a tartalék feldolgozási helyszín képességeit a folyamatos működés támogatására.

3.1.4.5. Biztonsági tárolási helyszín

3.1.4.5.1. Az érintett szervezet kijelöl egy biztonsági tárolási helyszínt, ahol az elektronikus információs rendszer mentéseinek másodlatát az elsődleges helyszínnel azonos módon, és biztonsági feltételek mellett tárolja.

3.1.4.5.2. A tartalék feldolgozási helyszín elkülönítése

A biztonsági tárolási helyszínnek el kell különülni az elsődleges tárolás helyszínétől, az azonos veszélyektől való érzékenység csökkentése érdekében.

3.1.4.5.3. Üzletmenet-folytonosság elérhetőség

A biztonsági tárolási helyszínhez történő hozzáférés érdekében - meghatározott körzetre kiterjedő rombolás vagy katasztrófa esetére - vészhelyzeti eljárásokat kell kidolgozni.

3.1.4.5.4. Üzletmenet folytonosság helyreállítás

A biztonsági tárolási helyszínt úgy kell kialakítani, hogy az elősegítse a helyreállítási tevékenységeket, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

3.1.4.6. Tartalék feldolgozási helyszín

3.1.4.6.1. Az érintett szervezet:

3.1.4.6.1.1. kijelöl egy tartalék feldolgozási helyszínt azért, hogy ha az elsődleges feldolgozási képesség nem áll rendelkezésére, elektronikus információs rendszere előre meghatározott műveleteit, előre meghatározott időn belül - összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal - a tartalék helyszínen újra kezdhesse, vagy folytathassa;

3.1.4.6.1.2. biztosítja, hogy a működés újrakezdéséhez, vagy folytatásához szükséges eszközök és feltételek a tartalék feldolgozási helyszínen, vagy meghatározott időn belül rendelkezésre álljanak;

3.1.4.6.1.3. biztosítja, hogy a tartalék feldolgozási helyszín informatikai biztonsági intézkedései egyenértékűek legyenek az elsődleges helyszínen alkalmazottakkal.

3.1.4.6.2. Elkülönítés

Olyan tartalék feldolgozási helyszínt kell kijelölni, amely elkülönül az elsődleges feldolgozás helyszínétől, az azonos veszélyektől való érzékenység csökkentése érdekében.

3.1.4.6.3. Elérhetőség

A tartalék feldolgozási helyszínhez történő hozzáférés érdekében - meghatározott körzetre kiterjedő rombolás vagy katasztrófa esetére - vészhelyzeti eljárásokat kell kidolgozni.

3.1.4.6.4. Szolgáltatások priorálása a tartalék feldolgozási helyszínen

A tartalék feldolgozási helyszínre vonatkozóan olyan megállapodásokat kell kötni, intézkedéseket kell bevezetni, amelyek a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban álló szolgáltatás-prioritási rendelkezéseket tartalmaznak.

3.1.4.6.5. Előkészület a működés megindítására

Az érintett szervezet úgy készíti fel a tartalék feldolgozási helyszínt, hogy az meghatározott időn belül készen álljon az alapfunkciók működésének támogatására.

3.1.4.7. Infokommunikációs szolgáltatások

3.1.4.7.1. Az érintett szervezet - a Nemzeti Távközlési Gerinchálózatra csatlakozó elektronikus információs rendszerek kivételével - tartalék infokommunikációs szolgáltatásokat létesít, erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az elektronikus információs rendszer alapfunkciói, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újrakezdését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.

3.1.4.7.2. Szolgáltatás-prioritási rendelkezések

Ha az elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, az tartalmazza a szolgáltatás-prioritási rendelkezéseket, a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban.

3.1.4.7.3. Közös hibalehetőségek kizárása

Olyan tartalék infokommunikációs szolgáltatásokat kell igénybe venni, melyek csökkentik az elsődleges infokommunikációs szolgáltatásokkal közös hibalehetőségek valószínűségét (pl. alternatív technológiára épülnek).

3.1.4.8. Az elektronikus információs rendszer mentései

3.1.4.8.1. Az érintett szervezet:

3.1.4.8.1.1. meghatározott gyakorisággal mentést végez az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

3.1.4.8.1.2. meghatározott gyakorisággal elmenti az elektronikus információs rendszerben tárolt rendszerszintű információkat, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

3.1.4.8.1.3. meghatározott gyakorisággal elmenti az elektronikus információs rendszer dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

3.1.4.8.1.4. megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen.

3.1.4.8.2. Megbízhatósági és sértetlenségi teszt

Meghatározott gyakorisággal tesztelni kell a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének a garantálása érdekében.

3.1.4.8.3. Helyreállítási teszt

Egy kiválasztott mintát kell használni a biztonsági másolat információkból az elektronikus információs rendszer kiválasztott funkcióinak helyreállításánál.

3.1.4.8.4. Kritikus információk elkülönítése

Az érintett szervezet által meghatározott, az elektronikus információs rendszer kritikus szoftvereinek és egyéb biztonsággal kapcsolatos információinak biztonsági másolatait egy elkülönített berendezésen vagy egy minősítéssel rendelkező tűzbiztos tárolóban kell tárolni.

3.1.4.8.5. Alternatív tárolási helyszín

Az elektronikus információs rendszer biztonsági másolat információit a 3.1.4.5. pontban meghatározottak szerinti biztonsági tárolási helyszínen kell tárolni.

3.1.4.9. Az elektronikus információs rendszer helyreállítása és újraindítása

3.1.4.9.1. Az érintett szervezet gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

3.1.4.9.2. Tranzakciók helyreállítása

Az érintett szervezet tranzakció alapú elektronikus információs rendszerek esetén tranzakció helyreállítást hajt végre.

3.1.4.9.3. Helyreállítási idő

Az érintett szervezet biztosítja azt a lehetőséget, hogy az elektronikus információs rendszerelemeket előre definiált helyreállítási idő alatt helyre lehessen állítani egy olyan konfigurációellenőrzött és sértetlenség védett információból, ami az elem ismert működési állapotát reprezentálja.

3.1.5. A BIZTONSÁGI ESEMÉNYEK KEZELÉSE

3.1.5.1. Az érintett szervezet:

3.1.5.1.1. eseménykezelési eljárást dolgoz ki a biztonsági eseményekre, amelyek magukban foglalják az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást;

3.1.5.1.2. egyezteti az eseménykezelési eljárásokat az üzletmenet-folytonossági tervéhez tartozó tevékenységekkel;

3.1.5.1.3. az eseménykezelési tevékenységekből levont tanulságokat beépíti az eseménykezelési eljárásokba, a fejlesztési és üzemeltetési eljárásokba, elvárásokba, továbbképzésekbe és tesztelésbe.

3.1.5.2. Automatikus eseménykezelés

Az érintett szervezet automatizált mechanizmusokat alkalmaz az eseménykezelési eljárások támogatására.

3.1.5.3. Információ korreláció

Az érintett szervezet összekapcsolja a biztonsági eseményekre vonatkozó információkat és az egyedi eseményekre való reagálásokat, hogy szervezetszintű rálátást nyerjen a biztonsági eseményekkel kapcsolatos tudatosságra és reagálásokra.

3.1.5.4. A biztonsági események figyelése

3.1.5.4.1. Az érintett szervezet nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit.

3.1.5.5. Automatikus nyomonkövetés, adatgyűjtés és vizsgálat

Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy segítse a biztonsági események nyomon követését és a biztonsági eseményekre vonatkozó információk gyűjtését és vizsgálatát.

3.1.5.6. A biztonsági események jelentése

3.1.5.6.1. Az érintett szervezet:

3.1.5.6.1.1. mindenkitől, aki az elektronikus információs rendszerrel, vagy azok elhelyezésére szolgáló objektummal kapcsolatban áll megköveteli, hogy jelentsék a biztonsági esemény bekövetkeztét, vagy ha erre utaló jelet, vagy veszélyhelyzetet észlelnek;

3.1.5.6.1.2. jogszabályban meghatározottak szerint jelenti a biztonsági eseményekre vonatkozó információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek.

3.1.5.6.2. Automatizált jelentés

Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy segítse a biztonsági események jelentését.

3.1.5.7. Segítségnyújtás a biztonsági események kezeléséhez

3.1.5.7.1. Az érintett szervezet tanácsadást és támogatást nyújt az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez.

3.1.5.7.2. Automatizált támogatás

Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy növelje a biztonsági események kezelésével kapcsolatos információk és a támogatás rendelkezésre állását.

3.1.5.8. Biztonsági eseménykezelési terv

3.1.5.8.1. Az érintett szervezet:

3.1.5.8.1.1. kidolgozza a biztonsági eseménykezelési tervet, amely:

3.1.5.8.1.1.1. az érintett szervezet számára iránymutatást ad a biztonsági esemény kezelési módjaira,

3.1.5.8.1.1.2. ismerteti a biztonsági eseménykezelési lehetőségek struktúráját és szervezetét,

3.1.5.8.1.1.3. átfogó megközelítést nyújt arról, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek az általános szervezetbe,

3.1.5.8.1.1.4. kielégíti az érintett szervezet feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeit,

3.1.5.8.1.1.5. meghatározza a bejelentésköteles biztonsági eseményeket,

3.1.5.8.1.1.6. meghatározza és folyamatosan pontosítja a biztonsági események kiértékelésének, kategorizálásának (súlyosság, stb.) kritériumrendszerét,

3.1.5.8.1.1.7. támogatást ad a biztonsági eseménykezelési lehetőségek belső mérésére,

3.1.5.8.1.1.8. meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására;

3.1.5.8.1.2. kihirdeti és tudomásul veteti a biztonsági eseménykezelési tervet a biztonsági eseményeket kezelő (névvel és/vagy szerepkörrel azonosított) személyeknek és szervezeti egységeknek;

3.1.5.8.1.3. meghatározott gyakorisággal felülvizsgálja a biztonsági eseménykezelési tervet;

3.1.5.8.1.4. frissíti a biztonsági eseménykezelési tervet, figyelembe véve az elektronikus információs rendszer és a szervezet változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat;

3.1.5.8.1.5. a biztonsági eseménykezelési terv változásait a 3.1.5.8.1.2. pont szerint ismerteti;

3.1.5.8.1.6. gondoskodik arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.

3.1.5.9. Képzés a biztonsági események kezelésére

3.1.5.9.1. Az érintett szervezet:

3.1.5.9.1.1. biztonsági eseménykezelési képzést biztosít az elektronikus információs rendszer felhasználóinak a számukra kijelölt szerepkörökkel és felelősségekkel összhangban;

3.1.5.9.1.2. a képzést a biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követő, meghatározott időtartamon belül, vagy amikor ezt az elektronikus információs rendszer változásai megkívánják, vagy meghatározott gyakorisággal tartja.

3.1.5.9.2. Szimuláció

Az érintett szervezet a biztonsági esemény kezelési képzésébe szimulált eseményeket foglal, hogy elősegítse a személyzet hatékony reagálását kritikus helyzetekben.

3.1.5.9.3. Automatizált képzési környezet

Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy biztonsági esemény kezelési képzéséhez mélyrehatóbb és valószerűbb környezetet biztosítson.

3.1.5.9.4 A biztonsági események kezelésének tesztelése

3.1.5.9.4.1. Az érintett szervezet meghatározott gyakorisággal teszteli az elektronikus információs rendszerre vonatkozó biztonsági eseménykezelési képességeket előre kidolgozott tesztek felhasználásával, annak érdekében, hogy meghatározza a biztonsági eseménykezelés hatékonyságát, és dokumentálja az eredményeket.

3.1.5.9.4.2. Egyeztetés

Az érintett szervezet egyezteti a biztonsági eseménykezelés tesztelését a kapcsolódó tervekért (pl. üzletmenet-folytonossági terv és katasztrófaelhárítási terv) felelős szervezeti egységekkel.

3.1.5.9.5 A biztonsági esemény kivizsgálásában részt vevő személynek a megbízása előtt részt kell vennie a biztonságiesemény-kezelő eljárásról szóló, a kormányzati eseménykezelő központ által tartott tájékoztató előadáson.

3.1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG

3.1.6.1. Személybiztonsági eljárásrend

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed az érintett szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki az érintett szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges vagy feltételezhető kapcsolatba kerülő személy nem az érintett szervezet tagja, a jelen fejezet szerinti elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

3.1.6.2. Munkakörök, feladatok biztonsági szempontú besorolása

3.1.6.2.1. Az érintett szervezet:

3.1.6.2.1.1. minden érintett szervezeti munkakört, vagy érintett szervezethez kapcsolódó feladatot biztonsági szempontból besorol;

3.1.6.2.1.2. felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat;

3.1.6.2.1.3. rendszeresen felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.

3.1.6.3 A személyek ellenőrzése

3.1.6.3.1. Az érintett szervezet:

3.1.6.3.1.1. az elektronikus információs rendszerhez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy a 3.1.6.2.1.1. és 3.1.6.2.1.2. pontok szerinti besorolásnak megfelelő feltételekkel rendelkezik-e;

3.1.6.3.1.2. a 3.1.6.2.1.2. szerinti munkaköröket betöltő vagy feladatokat ellátó személyek tekintetében kezdeményezi a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott nemzetbiztonsági ellenőrzést;

3.1.6.3.1.3. folyamatosan ellenőrzi a 3.1.6.3.1. pont szerinti feltételek fennállását.

3.1.6.4 Eljárás a jogviszony megszűnésekor

3.1.6.4.1. Az érintett szervezet:

3.1.6.4.1.1. belső szabályozásban meghatározott időpontban megszünteti a hozzáférési jogosultságot az elektronikus információs rendszerhez;

3.1.6.4.1.2. megszünteti vagy visszaveszi a személy egyéni hitelesítő eszközeit;

3.1.6.4.1.3. tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről;

3.1.6.4.1.4. visszaveszi az érintett szervezet elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;

3.1.6.4.1.5. megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz;

3.1.6.4.1.6. az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket;

3.1.6.4.1.7. a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik;

3.1.6.4.1.8. a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzi.

3.1.6.5 Az áthelyezések, átirányítások és kirendelések kezelése

3.1.6.5.1. Az érintett szervezet:

3.1.6.5.1.1. szükség esetén elvégzi a 3.1.6.3. pontban foglalt, a személyek ellenőrzésére vonatkozó eljárást;

3.1.6.5.1.2. logikai és fizikai hozzáférést engedélyez az újonnan használni kívánt elektronikus információs rendszerhez;

3.1.6.5.1.3. szükség esetén elvégzi az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését;

3.1.6.5.1.4. az általa meghatározott módon a jogviszony változásáról értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.

3.1.6.6. Az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

3.1.6.6.1. Az érintett szervezet:

3.1.6.6.1.1. a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy a külső szervezet határozza meg az érintett szervezettel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is;

3.1.6.6.1.2. szerződéses kötelezettségként megköveteli, hogy a szerződő fél feleljen meg az érintett szervezet által meghatározott személybiztonsági követelményeknek;

3.1.6.6.1.3. a szerződő féltől megköveteli, hogy dokumentálja a személybiztonsági követelményeket;

3.1.6.6.1.4. előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az érintett szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az érintett szervezetnek;

3.1.6.6.1.5. folyamatosan ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését.

3.1.6.7. Fegyelmi intézkedések

3.1.6.7.1. Az érintett szervezet:

3.1.6.7.1.1. belső eljárási rendje szerint fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben;

3.1.6.7.1.2. ha az elektronikus információbiztonsági szabályokat nem az érintett szervezet személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat.

3.1.6.8. Belső egyeztetés

Az érintett szervezet tervezi és egyezteti az elektronikus információs rendszer biztonságát érintő tevékenységeit, hogy csökkentse annak a nem érintett szervezeti egységeire gyakorolt hatását.

3.1.6.9. Viselkedési szabályok az interneten
3.1.6.9.1. Az érintett szervezet:
3.1.6.9.1.1. tiltja és számon kéri a szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét;
3.1.6.9.1.2. tiltja a belső szabályzatában meghatározott, interneten megvalósuló tevékenységet (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, stb.);
3.1.6.9.1.3. tilthatja a közösségi oldalak használatát, magánpostafiók elérését, és más, a szervezettől idegen tevékenységet.

3.1.7. TUDATOSSÁG ÉS KÉPZÉS

3.1.7.1. Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel
3.1.7.1.1. Az érintett szervezet:
3.1.7.1.1.1. az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek folyamatos oktatásának, képzésének elősegítése;
3.1.7.1.1.2. az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása;
3.1.7.1.1.3. a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása érdekében kapcsolatot alakít ki és tart fenn az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és e célt szolgáló ágazati szervezetekkel.
3.1.7.2. Képzési eljárásrend
3.1.7.2.1. Az érintett szervezet:
3.1.7.2.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a képzési eljárásrendet, mely a képzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
3.1.7.2.1.2. a képzési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a képzési eljárásrendet.
3.1.7.3. Biztonság tudatosság képzés
3.1.7.3.1. Az érintett szervezet annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára:
3.1.7.3.1.1. az új felhasználók kezdeti képzésének részeként;
3.1.7.3.1.2. amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
3.1.7.3.1.3. az érintett szervezet által meghatározott gyakorisággal.
3.1.7.4. Belső fenyegetés
A biztonságtudatossági képzés az érintett személyeket készítse fel a belső fenyegetések felismerésére, és tudatosítsa jelentési kötelezettségüket.
3.1.7.5. Szerepkör, vagy feladat alapú biztonsági képzés
3.1.7.5.1. Az érintett szervezet szerepkör, vagy feladat alapú biztonsági képzést nyújt az egyes szerepkörök szerinti, azért felelős személyeknek:
3.1.7.5.1.1. az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően;
3.1.7.5.1.2. amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
3.1.7.5.1.3. az érintett szervezet által meghatározott rendszerességgel.

3.1.7.6. A biztonsági képzésre vonatkozó dokumentációk
3.1.7.6.1. Az érintett szervezet:
3.1.7.6.1.1. dokumentálja a biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket;
3.1.7.6.1.2. a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és ezt a dokumentumot megőrzi.

3.2. FIZIKAI VÉDELMI INTÉZKEDÉSEK

3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM

3.2.1.1. Jelen fejezet alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre, valamint arra, hogy e fejezet rendelkezései az adott létesítmény bárki által szabadon látogatható, vagy igénybe vehető területeire nem vonatkoznak.
3.2.1.2. Fizikai védelmi eljárásrend
3.2.1.2.1. Az érintett szervezet:
3.2.1.2.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerek szempontjából érintett létesítményekre vagy helyiségekre érvényes fizikai védelmi eljárásrendet, amely az érintett szervezet elektronikus információbiztonsági vagy egyéb szabályzatának részét képező fizikai védelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
3.2.1.2.1.2. a fizikai védelmi eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a fizikai védelmi eljárásrendet.
3.2.1.3. Fizikai belépési engedélyek
3.2.1.3.1. Az érintett szervezet:
3.2.1.3.1.1. összeállítja, jóváhagyja, és kezeli az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultak listáját;
3.2.1.3.1.2. belépési jogosultságot igazoló dokumentumokat (pl. kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépéshez a belépni szándékozó részére;
3.2.1.3.1.3. rendszeresen felülvizsgálja a belépésre jogosult személyek listáját;
3.2.1.3.1.4. eltávolítja a belépésre jogosult személyek listájáról azokat, akik a belépésre már nem jogosultak;
3.2.1.3.1.5. intézkedik a 3.2.1.3.1.2. pont szerinti dokumentum visszavonása, érvénytelenítése, törlése, megsemmisítése iránt.
3.2.1.4. A fizikai belépés ellenőrzése
3.2.1.4.1. Az érintett szervezet:
3.2.1.4.1.1. kizárólag az érintett szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;
3.2.1.4.1.2. naplózza a fizikai belépéseket;
3.2.1.4.1.3. ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;
3.2.1.4.1.4. kíséri a létesítménybe ad-hoc belépésre jogosultakat, és figyelemmel követi a tevékenységüket;

3.2.1.4.1.5. megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközt;

3.2.1.4.1.6. nyilvántartást vezet a fizikai belépést ellenőrző eszközről;

3.2.1.4.1.7. meghatározott rendszerességgel változtatja meg a hozzáférési kódokat és kulcsokat, vagy azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti a belépési jogosultságát;

3.2.1.4.1.8. az egyéni belépési engedélyeket a belépési pontokon ellenőrzi;

3.2.1.4.1.9. a kijelölt pontokon való átjutást felügyeli a szervezet által meghatározott fizikai belépést ellenőrző rendszerrel vagy eszközzel;

3.2.1.4.1.10. felhívja a szervezet tagjainak figyelmét a rendellenességek jelentésére.

3.2.1.4.2. Hozzáférés az információs rendszerhez

Az érintett szervezet a létesítménybe történő fizikai belépés ellenőrzésén túl külön engedélyhez köti a fizikai belépést az elektronikus információs rendszereknek helyt adó helyiségekbe is.

3.2.1.5. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz

Az érintett szervezet az általa meghatározott biztonsági védelemmel ellenőrzi az elektronikus információs rendszer adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést.

3.2.1.6. A kimeneti eszközök hozzáférés ellenőrzése

Az érintett szervezet ellenőrzi az elektronikus információs rendszer kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek azokhoz hozzá.

3.2.1.7. A fizikai hozzáférések felügyelete

3.2.1.7.1. Az érintett szervezet:

3.2.1.7.1.1. ellenőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményt és reagáljon arra;

3.2.1.7.1.2. rendszeresen átvizsgálja a fizikai hozzáférésekről készült naplókat;

3.2.1.7.1.3. azonnal átvizsgálja a fizikai hozzáférésekről készült naplókat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak;

3.2.1.7.1.4. összehangolja a biztonsági események kezelését, valamint a napló átvizsgálások eredményét.

3.2.1.7.2. Behatolás riasztás, felügyeleti berendezések

Az érintett szervezet felügyeli a fizikai behatolás riasztásokat és a felügyeleti berendezéseket.

3.2.1.7.3. Az elektronikus információs rendszerekhez való hozzáférés felügyelete

Az érintett szervezet a létesítménybe való fizikai belépések ellenőrzésén felül külön felügyeli az elektronikus információs rendszer egy vagy több elemét tartalmazó helyiségekbe történő fizikai belépéseket.

3.2.1.8. A látogatók ellenőrzése

3.2.1.8.1. Az érintett szervezet:

3.2.1.8.1.1. meghatározott ideig megőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt látogatói belépésekről szóló információkat;

3.2.1.8.1.2. azonnal átvizsgálja a látogatói belépésekről készített információkat és felvételeket, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak.

3.2.1.8.2. Automatizált látogatói információkezelés

Az érintett szervezet automatizált mechanizmusokat alkalmaz a látogatói belépésekről készített információk és felvételek kezeléséhez, átvizsgálásához.

3.2.1.9. Áramellátó berendezések és kábelezés

Az érintett szervezet védi az elektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben.

3.2.1.9.1. Tartalék áramellátás

Az érintett szervezet az elsődleges áramforrás kiesése esetére, a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást biztosít az elektronikus információs rendszer szabályos leállításához vagy a hosszútávú tartalék áramellátásra történő átkapcsoláshoz.

3.2.1.9.2. Hosszútávú tartalék áramellátás a minimálisan elvárt működési képességhez

Az érintett szervezet az elsődleges áramforrás kiesése esetén biztosítja a hosszútávú tartalék áramellátást az elektronikus információs rendszer minimálisan elvárt működési képességének és előre definiált minimálisan elvárt működési idejének fenntartására.

3.2.1.10. Vészkikapcsolás

3.2.1.10.1. Az érintett szervezet:

3.2.1.10.1.1. lehetőséget biztosít az elektronikus információs rendszer vagy egyedi rendszerelemek áramellátásának kikapcsolására vészhelyzetben;

3.2.1.10.1.2. gondoskodik a vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségéről;

3.2.1.10.1.3. megakadályozza a jogosulatlan vészkikapcsolást.

3.2.1.11. Vészvilágítás

Az érintett szervezet egy automatikus vészvilágítási rendszert alkalmaz és tart karban, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat.

3.2.1.12. Tűzvédelem

3.2.1.12.1. Az érintett szervezet az elektronikus információs rendszerek számára független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban.

3.2.1.12.2. Automatikus tűzelfojtás

Az érintett szervezet a személyzet által folyamatosan nem felügyelt elektronikus információs rendszerek számára automatikus tűzelfojtási képességet biztosít.

3.2.1.12.3. Észlelő berendezések, rendszerek

Az érintett szervezet az elektronikus információs rendszer védelmére olyan tűzjelző berendezést vagy rendszert alkalmaz, amely tűz esetén automatikusan működésbe lép, és értesítést küld az érintett szervezet által kijelölt tűzvédelmi felelősnek.

3.2.1.12.4. Tűzelfojtó berendezések, rendszerek

Az érintett szervezet az elektronikus információs rendszer védelmére olyan tűzelfojtó berendezést vagy rendszert alkalmaz, amelynek aktiválásáról automatikusan jelzést kap az érintett szervezet által kijelölt tűzvédelmi felelős.

3.2.1.13. Hőmérséklet és páratartalom ellenőrzés

3.2.1.13.1. Az érintett szervezet:

3.2.1.13.1.1. az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) az erőforrások biztonságos működéséhez szükséges szinten tartja a hőmérsékletet és páratartalmat;

3.2.1.13.1.2. az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) figyeli a hőmérséklet és páratartalom szintjét.

3.2.1.14. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

3.2.1.14.1. Az érintett szervezet:

3.2.1.14.1.1. védi az elektronikus információs rendszert a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzárószelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek;

3.2.1.14.1.2. az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése (pl. adatközpont, szerver szoba, központi gépterem) során biztosítja, hogy az a víz-, és más hasonló kártól védett legyen, akár csővezetékek kiváltásával, áthelyezésével is.

3.2.1.14.2. Automatizált védelem

Az érintett szervezet automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer közelében megjelenő folyadékszivárgás észlelésére és az érintett szervezet által kijelölt személyek riasztására.

3.2.1.15. Be- és kiszállítás

Az érintett szervezet engedélyezi, vagy tiltja, továbbá figyeli és ellenőrzi a létesítménybe bevitt, onnan kivitt információs rendszerelemeket, és nyilvántartást vezet ezekről.

3.2.1.16. Az elektronikus információs rendszer elemeinek elhelyezése

Az érintett szervezet úgy helyezi el az elektronikus információs rendszer elemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.

3.2.1.17. Ellenőrzés

Az érintett szervezet ellenőrzi a karbantartó személyzet által a létesítménybe hozott karbantartási eszközöket, a nem megfelelő vagy jogosulatlan módosítások megakadályozása érdekében.

3.2.1.18. Szállítási felügyelet

3.2.1.18.1. Az érintett szervezet védi az információt tartalmazó karbantartási eszközt a jogosulatlan elszállítással szemben azzal, hogy:

3.2.1.18.1.1. ellenőrzi, az eszköz nem tartalmaz-e információt;

3.2.1.18.1.2. ha az eszköz tartalmaz információt, azt törli vagy megsemmisíti;

3.2.1.18.1.3. az eszközt a létesítményen belül őrzi;

3.2.1.18.1.4. az ezért felelős személyekkel engedélyezteti az eszköz elszállítását a létesítményből.

3.2.1.19. Karbantartók

3.2.1.19.1. Az érintett szervezet:

3.2.1.19.1.1. kialakít egy folyamatot a karbantartók munkavégzési engedélyének kezelésére, és nyilvántartást vezet a karbantartó szervezetekről vagy személyekről;

3.2.1.19.1.2. megköveteli a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől;

3.2.1.19.1.3. felhatalmazást ad a szervezethez tartozó, a kívánt hozzáférési jogosultságokkal és műszaki szakértelemmel rendelkező személyeknek arra, hogy felügyeljék a kívánt jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

3.2.1.19.2. Karbantartás fokozott biztonsági intézkedésekkel

3.2.1.19.2.1. Az érintett szervezet:
3.2.1.19.2.1.1. a megfelelő biztonsági engedéllyel nem rendelkező karbantartó személyek alkalmazása során:
3.2.1.19.2.1.1.1. az ilyen karbantartó személyeket megfelelő hozzáférési jogosultságú, műszakilag képzett belső személyekkel felügyelete alatt tartja az elektronikus információs rendszeren végzett karbantartási és diagnosztikai tevékenységek során,
3.2.1.19.2.1.1.2. a karbantartási és diagnosztikai tevékenységek megkezdése előtt az elektronikus információs rendszer minden fellelhető információtároló elemét törli, és a nem törölhető adathordozót eltávolítja, vagy fizikailag leválasztja a rendszertől;
3.2.1.19.2.1.2. alternatív biztonsági védelmet alakít ki, ha egy elektronikus információs rendszerelemet nem lehet törölni, eltávolítani vagy a rendszertől leválasztani.
3.2.1.19.3. Időben történő javítás
Az érintett szervezet karbantartási támogatást szerez be a meghatározott elektronikus információs rendszerelemekhez.

3.3. LOGIKAI VÉDELMI INTÉZKEDÉSEK

3.3.1. ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK

3.3.1.1. Az érintett szervezet:
3.3.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat;
3.3.1.1.2. felügyeli az elektronikus információs rendszer és környezet biztonsági állapotát;
3.3.1.1.3. meghatározza az információbiztonsággal összefüggő szerepköröket és felelősségi köröket, kijelöli az ezeket betöltő személyeket;
3.3.1.1.4. integrálja az elektronikus információbiztonsági engedélyezési folyamatokat a szervezeti szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabályzattal.
3.3.1.2. Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, az érintett szervezet hatókörébe tartozó:
3.3.1.2.1. emberi, fizikai és logikai erőforrásra;
3.3.1.2.2. eljárási és védelmi szintre és folyamatra.
3.3.1.3. Az elektronikus információs rendszer kapcsolódásai
3.3.1.3.1. Az érintett szervezet:
3.3.1.3.1.1. szabályozza, és belső engedélyhez kötheti az elektronikus információs rendszerének kapcsolódását más elektronikus információs rendszerekhez;
3.3.1.3.1.2. dokumentálja az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.
3.3.1.3.2. Belső rendszer kapcsolatok
az érintett szervezet belső engedélyhez köti az elektronikus információs rendszereinek összekapcsolását;
3.3.1.3.3. Külső kapcsolódásokra vonatkozó korlátozások

Az érintett szervezet a külső elektronikus információs rendszerekhez való kapcsolódásokhoz az informatikai biztonsági szabályzatában szabályrendszert állít fel, és alkalmaz, amelynek eredménye lehet az összes kapcsolat engedélyezése vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.

3.3.1.4. Személybiztonság

3.3.1.4.1. Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed az érintett szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki az érintett szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem az érintett szervezet tagja, a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

3.3.2. TERVEZÉS

3.3.2.1. Biztonságtervezési szabályzat

3.3.2.1.1. Az érintett szervezet:

3.3.2.1.1.1. megfogalmazza, az érintett szervezetre érvényes követelmények szerint dokumentálja, és a munka- és feladatkörük miatt érintettek számára kihirdeti a biztonságtervezési szabályzatot, amely tartalmazza a biztonságtervezési eljárás folyamatait, valamint biztosítja annak ellenőrzését;

3.3.2.1.1.2. a biztonságtervezési szabályzatban, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a biztonságtervezési szabályzatot.

3.3.2.2. Rendszerbiztonsági terv

3.3.2.2.1. Az érintett szervezet, ha az elektronikus információs rendszer tervezése a hatókörébe tartozik, az elektronikus információs rendszerhez rendszerbiztonsági tervet készít, amely:

3.3.2.2.1.1. összhangban áll szervezeti felépítésével vagy szervezeti szintű architektúrájával;

3.3.2.2.1.2. meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alapfunkcióit;

3.3.2.2.1.3. meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;

3.3.2.2.1.4. meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;

3.3.2.2.1.5. a vonatkozó rendszerdokumentáció keretébe foglalja az elektronikus információs rendszer biztonsági követelményeit;

3.3.2.2.1.6. meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket, végrehajtja a jogszabály szerinti biztonsági feladatokat;

3.3.2.2.1.7. gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);

3.3.2.2.1.8. belső szabályozásában, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszer rendszerbiztonsági tervét;

3.3.2.2.1.9. frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;

3.3.2.2.1.10. elvégzi a szükséges belső egyeztetéseket;

3.3.2.2.1.11. gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

3.3.2.3. Cselekvési terv

3.3.2.3.1. Az érintett szervezet:

3.3.2.3.1.1. cselekvési tervet készít, ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg;

3.3.2.3.1.2. a cselekvési tervben dokumentálja a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeit;

3.3.2.3.1.3. frissíti a meglévő cselekvési tervet az érintett szervezet által meghatározott gyakorisággal a biztonsági értékelések, biztonsági hatáselemzések és a folyamatos felügyelet eredményei alapján.

3.3.2.4. Személyi biztonság

3.3.2.4.1. Az érintett szervezet:

3.3.2.4.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet;

3.3.2.4.1.2. az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja;

3.3.2.4.1.3. meghatározott gyakorisággal felülvizsgálja, és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységet a viselkedési szabályok betartását;

3.3.2.4.1.4. gondoskodik arról, hogy a 3.3.2.4.1.3. pont szerinti változás esetén a hozzáféréssel rendelkezők tekintetében a

3.3.2.4.1.2. pont szerinti eljárás megtörténjen;

3.3.2.4.1.5. meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket.

3.3.2.5. Információbiztonsági architektúra leírás

3.3.2.5.1. Az érintett szervezet (ha a hatókörébe tartozik, és ha más dokumentumban nem kerül meghatározásra, vagy azokból nem következik):

3.3.2.5.1.1. elkészíti az elektronikus információs rendszer információbiztonsági architektúra leírását;

3.3.2.5.1.2. az általános architektúrájában bekövetkezett változtatásokra reagálva felülvizsgálja, és frissíti az információbiztonsági architektúra leírást;

3.3.2.5.1.3. biztosítja, hogy az információbiztonsági architektúra leírásban tervezett változtatás tükröződjön a rendszerbiztonsági tervben és a beszerzésekben.

3.3.2.5.2. Az információbiztonsági architektúra leírás:

3.3.2.5.2.1. összegzi az elektronikus információs rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló filozófiát, követelményeket és megközelítést;

3.3.2.5.2.2. megfogalmazza, hogy az információbiztonsági architektúra miként illeszkedik a szervezet általános architektúrájába, és hogyan támogatja azt;

3.3.2.5.2.3. leírja a külső szolgáltatásokkal kapcsolatos információbiztonsági feltételezéseket és függőségeket.

3.3.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

3.3.3.1. Jelen címben meghatározott eljárásokat abban az esetben nem kell bevezetni az érintett szervezetnél, ha saját hatókörében informatikai szolgáltatást vagy eszközöket nem szerez be, és nem végez, vagy végeztet rendszerfejlesztési tevékenységet (ide nem értve a jellemzően kis értékű, kereskedelmi forgalomban kapható általában irodai alkalmazásokat, szoftvereket, vagy azokat a hardver beszerzéseket, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzéseket). Jelen fejezet alkalmazása szempontjából nem minősül fejlesztésnek a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése.

3.3.3.2. A rendszer fejlesztési életciklusa

3.3.3.2.1. Az érintett szervezet:

3.3.3.2.1.1. elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikai biztonsági helyzetüket;

3.3.3.2.1.2. a fejlesztési életciklus egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és felelősségeket;

3.3.3.2.1.3. meghatározza, és a szervezetre érvényes szabályok szerint kijelöli az információbiztonsági szerepköröket betöltő, felelős személyeket.

3.3.3.2.2. A rendszer életciklus szakaszai a következők:

3.3.3.2.2.1. követelmény meghatározás;

3.3.3.2.2.2. fejlesztés vagy beszerzés;

3.3.3.2.2.3. megvalósítás vagy értékelés;

3.3.3.2.2.4. üzemeltetés és fenntartás;

3.3.3.2.2.5. kivonás (archiválás, megsemmisítés).

3.3.3.3. Funkciók, portok, protokollok, szolgáltatások

Az érintett szervezet megköveteli, hogy a szolgáltató meghatározza a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.

3.3.3.4. Fejlesztői változáskövetés

3.3.3.4.1. Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

3.3.3.4.1.1. vezesse végig a változtatásokat az elektronikus információs rendszer, rendszerelem vagy rendszer szolgáltatás tervezése, fejlesztése, megvalósítása, üzemeltetése során;

3.3.3.4.1.2. dokumentálja, kezelje, és ellenőrizze a változtatásokat, biztosítsa ezek sértetlenségét;

3.3.3.4.1.3. csak a jóváhagyott változtatásokat hajtsa végre az elektronikus információs rendszeren, rendszerelemen vagy rendszerszolgáltatáson;

3.3.3.4.1.4. dokumentálja a jóváhagyott változtatásokat és ezek lehetséges biztonsági hatásait;

3.3.3.4.1.5. kövesse nyomon az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás biztonsági hibáit és azok javításait, továbbá jelentse észrevételeit az érintett szervezet által meghatározott személyeknek.

3.3.3.5. Fejlesztői biztonsági tesztelés

3.3.3.5.1. Az érintett szervezet megköveteli, hogy az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője:

3.3.3.5.1.1. készítsen biztonságértékelési tervet, és hajtsa végre az abban foglaltakat;

3.3.3.5.1.2. hajtson végre (a fejlesztéshez illeszkedő módon) egység-, integrációs-, rendszer-, vagy regressziós tesztelést, és ezt értékelje ki az érintett szervezet által meghatározott lefedettség és mélység mellett;

3.3.3.5.1.3. dokumentálja, hogy végrehajtotta a biztonságértékelési tervben foglaltakat, és ismertesse a biztonsági tesztelés és értékelés eredményeit;

3.3.3.5.1.4. javítsa ki a biztonsági tesztelés és értékelés során feltárt hiányosságokat.

3.3.3.6. Fejlesztési folyamat, szabványok és eszközök

3.3.3.6.1. Az érintett szervezet:

3.3.3.6.1.1. megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy dokumentált fejlesztési folyamatot kövessen;

3.3.3.6.1.2. előírja, hogy az általa meghatározott biztonsági követelményeknek való megfelelés érdekében általa meghatározott gyakorisággal a fejlesztő tekintse át a fejlesztési folyamatot, szabványokat, eszközöket és eszköz opciókat, konfigurációkat.

3.3.3.6.2. A dokumentált fejlesztési folyamat:

3.3.3.6.2.1. kiemelten kezeli a biztonsági követelményeket;

3.3.3.6.2.2. meghatározza a fejlesztés során alkalmazott szabványokat és eszközöket;

3.3.3.6.2.3. dokumentálja a fejlesztés során alkalmazott speciális eszköz opciókat és konfigurációkat;

3.3.3.6.2.4. nyilvántartja a változtatásokat, és biztosítja ezek engedély nélküli megváltoztatás elleni védelmét.

3.3.3.7. Fejlesztői oktatás

Az érintett szervezet oktatási kötelezettséget ír elő az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára, hogy az érintett szervezet által kijelölt személyek - elsősorban adminisztrátorok - és biztonsági felelősök a megvalósított biztonsági funkciók, intézkedések és mechanizmusok helyes használatát és működését megismerhessék és elsajátíthassák.

3.3.3.8. Fejlesztői biztonsági architektúra és tervezés

3.3.3.8.1. Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan specifikációt és biztonsági architektúrát hozzon létre, amely:

3.3.3.8.1.1. illeszkedik a szervezet biztonsági architektúrájához és támogatja azt;

3.3.3.8.1.2. leírja a szükséges biztonsági funkciókat, valamint a védelmi intézkedések megosztását a fizikai és logikai összetevők között;

3.3.3.8.1.3. bemutatja az egyes biztonsági funkciók, mechanizmusok és szolgáltatások együttműködését az előírt biztonsági követelmények megvalósításában, valamint a védelem egységes megközelítésében.

3.3.4. BIZTONSÁGI ELEMZÉS

3.3.4.1. Biztonságelemzési eljárásrend
3.3.4.1.1. Az érintett szervezet:
3.3.4.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a biztonságértékelési eljárásrendet, amely a biztonságértékelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
3.3.4.1.1.2. a biztonságértékelési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a biztonságértékelési eljárásrendet.
3.3.4.2. Biztonsági értékelések
3.3.4.2.1. Az érintett szervezet:
3.3.4.2.1.1. biztonságértékelési tervet készít;
3.3.4.2.1.2. meghatározott gyakorisággal értékeli az elektronikus információs rendszer és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését;
3.3.4.2.1.3. elkészíti a biztonságértékelés eredményét összefoglaló jelentést;
3.3.4.2.1.4. gondoskodik a biztonságértékelés eredményét összefoglaló jelentésnek az érintett szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismeréséről.
3.3.4.2.2. A biztonsági értékelés tartalmazza:
3.3.4.2.2.1. az értékelendő (adminisztratív, fizikai és logikai) védelmi intézkedéseket;
3.3.4.2.2.2. a biztonsági ellenőrzések eredményességét meghatározó eljárásrendeket;
3.3.4.2.2.3. az értékelési környezetet, az értékelő csoportot, az értékelés célját, az értékelést végzők feladatát.
3.3.4.3. Speciális értékelés
Az érintett szervezet a védelmi intézkedések értékelése keretében bejelentés mellett, vagy bejelentés nélkül sérülékenységvizsgálatot, rosszhiszemű felhasználó tesztet, belső fenyegetettség értékelést, a biztonságkritikus egyedi fejlesztésű szoftverelemek forráskód elemzését, az érintett szervezet által meghatározott egyéb biztonsági értékeléseket végeztet.
3.3.4.4. A biztonsági teljesítmény mérése
Az érintett szervezet kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.

3.3.5. TESZTELÉS, KÉPZÉS ÉS FELÜGYELET

3.3.5.1. Az érintett szervezet:
3.3.5.1.1. ha ez hatókörébe tartozik, megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint kihirdeti az elektronikus információs rendszer tesztelésével, képzésével és felügyeletével kapcsolatos eljárásokat, amelyek támogatják a tesztelési, képzési és felügyeleti tevékenységek:

3.3.5.1.1.1. fejlesztését és fenntartását;
3.3.5.1.1.2. folyamatos időbeni végrehajtását;
3.3.5.1.1.3. felülvizsgálja a tesztelési, képzési és ellenőrzési terveket a kockázatkezelési stratégia és a lehetséges, vagy bekövetkezett biztonsági események súlya alapján.
3.3.5.2. A biztonsági teljesítmény mérése
Az érintett szervezet kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.
3.3.5.3. Sérülékenység teszt
3.3.5.3.1. Az érintett szervezet:
3.3.5.3.1.1. az elektronikus információs rendszerei és alkalmazásai tekintetében sérülékenység tesztet végez, ha azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik;
3.3.5.3.1.2. meghatározott gyakorisággal, vagy véletlenszerűen, valamint olyan esetben, amikor új lehetséges sérülékenység merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban, megismétli a sérülékenység tesztet;
3.3.5.3.1.3. a sérülékenység tesztet sérülékenységvizsgálati eszközök és technikák alkalmazásával, vagy külső szervezet bevonásával azon elektronikus információs rendszerek tekintetében végzi el, amelyek az érintett szervezet felügyelete, irányítása alatt állnak;
3.3.5.3.1.4. kimutatást készít a feltárt hibákról, valamint a nem megfelelő konfigurációs beállításokról;
3.3.5.3.1.5. végrehajtja az ellenőrzési listákat és tesztelési eljárásokat;
3.3.5.3.1.6. felméri a sérülékenység lehetséges hatásait;
3.3.5.3.1.7. elemzi a sérülékenység teszt eredményét;
3.3.5.3.1.8. megosztja a sérülékenység teszt eredményét a szervezet által meghatározott személyekkel és szerepkörökkel.
3.3.5.3.2. Frissítési képesség
Az érintett szervezet olyan sérülékenységi teszteszközt alkalmaz, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel.
3.3.5.3.3. Frissítés időközönként, új vizsgálat előtt vagy új sérülékenység feltárását követően
Az érintett szervezet az elektronikus információs rendszerre vizsgált sérülékenység körét aktualizálja az új tesztet megelőzően, vagy a sérülékenység feltárását követően azonnal.
3.3.5.3.4. Privilegizált hozzáférés
Az elektronikus információs rendszer különleges jogosultsághoz kötött - úgynevezett privilegizált - hozzáférést biztosít az érintett szervezet által kijelölt rendszerelemekhez a sérülékenység teszt végrehajtásához.
3.3.5.3.5. Felfedhető információk
Az érintett szervezet meghatározza, hogy egy támadó milyen információkat képes elérni az elektronikus információs rendszerben, és ennek elhárítására javításokat hajt végre.

3.3.6. KONFIGURÁCIÓKEZELÉS

3.3.6.1. Konfigurációkezelési eljárásrend
3.3.6.1.1. Az érintett szervezet:

3.3.6.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a konfigurációkezelési eljárásrendet, mely a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.6.1.1.2. a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a konfigurációkezelési eljárásrendet.

3.3.6.2. Alapkonfiguráció

3.3.6.2.1. Az érintett szervezet az elektronikus információs rendszereihez egy-egy alapkonfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges elemeit.

3.3.6.2.2. Áttekintések és frissítések

Az alapkonfiguráció frissítését az elektronikus információs rendszerelemek telepítésének és frissítéseinek szerves részeként kell elvégezni.

3.3.6.2.3. Korábbi konfigurációk megőrzése

Változatlan állapotban meg kell őrizni az elektronikus információs rendszer alapkonfigurációját és annak további verzióit, hogy szükség esetén lehetővé váljon az erre való visszatérés.

3.3.6.2.4. Magas kockázatú területek konfigurálása

3.3.6.2.4.1. Biztonsági szempontokból meghatározott módon konfigurált elektronikus információs rendszerelemeket vagy eszközöket kell biztosítani azon személyek számára, akik az elektronikus információs rendszert külső helyszínen használják.

3.3.6.2.4.2. Megfelelő biztonsági eljárásokat kell alkalmazni a 3.3.6.2.4.1. pont szerinti eszköz belső használatba vonásakor.

3.3.6.2.5. Automatikus támogatás

Automatikus mechanizmusokat kell alkalmazni az elektronikus információs rendszer naprakész, teljes, pontos, és állandóan rendelkezésre álló alapkonfigurációjának a karbantartására.

3.3.6.3. A konfigurációváltozások felügyelete (változáskezelés)

3.3.6.3.1. Az érintett szervezet:

3.3.6.3.1.1. meghatározza a változáskezelési felügyelet alá eső változástípusokat;

3.3.6.3.1.2. meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit (csatolt dokumentációk, teszt jegyzőkönyvek, stb.);

3.3.6.3.1.3. megvizsgálja a változáskezelési felügyelet elé terjesztett, javasolt változtatásokat, majd kockázatelemzés alapján jóváhagyja vagy elutasítja azokat;

3.3.6.3.1.4. dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket;

3.3.6.3.1.5. megvalósítja a jóváhagyott változtatásokat az elektronikus információs rendszerben;

3.3.6.3.1.6. visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását;

3.3.6.3.1.7. auditálja és felülvizsgálja a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.

3.3.6.3.2. Előzetes tesztelés és megerősítés

A konfiguráció megváltoztatása előtt az új verziót tesztelni kell, ezután dönteni kell annak megfelelőségéről, továbbá dokumentálni kell az elektronikus információs rendszer változtatásait az éles rendszerben történő megvalósítása előtt.

3.3.6.3.3. Automatikus támogatás
3.3.6.3.3.1. Automatikus mechanizmusokat kell alkalmazni:
3.3.6.3.3.1.1. az elektronikus információs rendszerben javasolt változtatások dokumentálására;
3.3.6.3.3.1.2. a jóváhagyásra jogosultak értesítésére;
3.3.6.3.3.1.3. a késedelmes jóváhagyások kiemelésére;
3.3.6.3.3.1.4. a még nem jóváhagyott változások végrehajtásának a megakadályozására;
3.3.6.3.3.1.5. az elektronikus információs rendszerben végrehajtott változások teljes dokumentálására;
3.3.6.3.3.1.6. a jóváhagyásra jogosultak értesítésére a jóváhagyott változtatások végrehajtásáról.
3.3.6.4. Biztonsági hatásvizsgálat
3.3.6.4.1. Az érintett szervezet megvizsgálja az elektronikus információs rendszerben tervezett változtatásoknak az információbiztonságra való hatását, még a változtatások megvalósítása előtt.
3.3.6.4.2. Elkülönített tesztkörnyezet
Az érintett szervezet a változtatásokat éles rendszerben történő megvalósításuk előtt egy elkülönített tesztkörnyezetben vizsgálja, hibákat, sebezhetőségeket, kompatibilitási problémákat és szándékos károkozásra utaló jeleket keresve.
3.3.6.5. A változtatásokra vonatkozó hozzáférés korlátozások
3.3.6.5.1. Az érintett szervezet az elektronikus információs rendszerre vonatkozóan szabályozásában meghatározza a változtatásokhoz való hozzáférési jogosultságot, dokumentálja a hozzáférési jogosultságokat, jóváhagyja azokat, fizikai és logikai hozzáférés korlátozásokat alkalmaz az elektronikus információs rendszer változtatásaival kapcsolatban.
3.3.6.5.2. Automatikus támogatás
Az érintett szervezet az elektronikus információs rendszerben automatikus mechanizmusokat alkalmaz a hozzáférési korlátozások érdekében, az ezzel kapcsolatos tevékenység naplózására.
3.3.6.5.3. Felülvizsgálat
Az érintett szervezet rendszeresen felülvizsgálja az elektronikus információs rendszer változtatásait annak megállapítására, hogy történt-e jogosulatlan változtatás.
3.3.6.5.4. Aláírt elemek
A szervezet által meghatározott szoftver- és az úgynevezett firmware (vezérlőeszköz) elemek esetében meg kell akadályozni az elemek telepítését, ha azok nincsenek digitálisan aláírva ismert és jóváhagyott tanúsítvány alkalmazásával.
3.3.6.6. Konfigurációs beállítások
3.3.6.6.1. Az érintett szervezet:
3.3.6.6.1.1. meghatározza a működési követelményeknek még megfelelő, de biztonsági szempontból a lehető leginkább korlátozott módon - a „szükséges minimum” elv alapján - az elektronikus információs rendszerben használt információtechnológiai termékekre kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálja;
3.3.6.6.1.2. elvégzi a konfigurációs beállításokat az elektronikus információs rendszer valamennyi elemében;
3.3.6.6.1.3. a meghatározott elemek konfigurációs beállításaiban azonosít, dokumentál és jóváhagy minden eltérést;

3.3.6.6.1.4. figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait, az érintett szervezet belső szabályzataival és eljárásaival összhangban.

3.3.6.6.2. Automatikus támogatás

Az érintett szervezet az elektronikus információs rendszerre vonatkozóan automatikus mechanizmusokat alkalmaz a konfigurációs beállítások központi kezelésére, alkalmazására és ellenőrzésére.

3.3.6.6.3. Reagálás jogosulatlan változásokra

Az érintett szervezet meghatározott intézkedéseket vezet be a meghatározott konfigurációs beállítások jogosulatlan változtatásai esetén.

3.3.6.7. Legszűkebb funkcionalitás

3.3.6.7.1. Az érintett szervezet:

3.3.6.7.1.1. az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa;

3.3.6.7.1.2. meghatározza a tiltott, vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát.

3.3.6.7.2. Rendszeres felülvizsgálat

3.3.6.7.2.1. Az érintett szervezet meghatározott gyakorisággal átvizsgálja az elektronikus információs rendszert, meghatározza és kizárja, vagy letiltja a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat.

3.3.6.7.2.2. Az érintett szervezetnek a szoftver használatra meghatározott szabályzatainak vagy a szoftver használatára vonatkozó feltételeinek és kikötéseinek megfelelően az elektronikus információs rendszer megakadályozza a tiltott programok futtatását.

3.3.6.7.3. Nem futtatható szoftverek

Az érintett szervezet meghatározza, rendszeresen felülvizsgálja és frissíti az elektronikus információs rendszerben nem futtatható (tiltott, úgynevezett feketelistás) szoftverek listáját, és megtiltja ezek futtatását.

3.3.6.7.4. Futtatható szoftverek

Az érintett szervezet meghatározza, rendszeresen felülvizsgálja és frissíti az elektronikus információs rendszerben jogosultan futtatható (engedélyezett, úgynevezett fehérlistás) szoftverek listáját, és engedélyezi ezek futtatását, az ettől eltérő szoftver futtatását egyedi engedélyhez köti.

3.3.6.8. Elektronikus információs rendszerelem leltár

3.3.6.8.1. Az érintett szervezet:

3.3.6.8.1.1. leltárt készít az elektronikus információs rendszer elemeiről;

3.3.6.8.1.2. meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszerelem leltárt;

3.3.6.8.1.3. gondoskodik arról, hogy a leltár:

3.3.6.8.1.3.1. pontosan tükrözze az elektronikus információs rendszer aktuális állapotát;

3.3.6.8.1.3.2. az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza;

3.3.6.8.1.3.3. legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez.

3.3.6.8.2. Frissítés

Az érintett szervezet az elektronikus információs rendszerelem leltárt frissíti az egyes rendszerelemek telepítésének, eltávolításának, frissítésének időpontjában.

3.3.6.8.3. Jogosulatlan elemek automatikus észlelése

3.3.6.8.3.1. Automatizált mechanizmusok biztosítják, hogy a szervezet által meghatározott gyakorisággal a jogosulatlan hardver-, szoftver- és firmware elemek észlelése megtörténjen.

3.3.6.8.3.2. A jogosulatlan elemek észlelése esetén le kell tiltani az ilyen elemek általi hálózati hozzáférést, el kell őket különíteni, és értesíteni kell az illetékes személyeket.

3.3.6.8.4. Duplikálás elleni védelem

Az érintett szervezet ellenőrzi, hogy az elektronikus információs rendszer hatókörén belüli elemek nincsenek-e felvéve más elektronikus információs rendszerek leltárában.

3.3.6.8.5. Automatikus támogatás

Az érintett szervezet automatikus mechanizmusokat alkalmaz az elektronikus információs rendszerelem leltár naprakész, teljes, pontos, és állandóan rendelkezésre álló kezelésének támogatására.

3.3.6.8.6. Naplózás

Az elektronikus információs rendszerelem leltárhoz csatolni kell az egyes elemek adminisztrálásáért felelős személyek nevét, pozícióját vagy szerepkörét.

3.3.6.9. Konfigurációkezelési terv

3.3.6.9.1. Az érintett szervezet:

3.3.6.9.1.1. kialakít, dokumentál és végrehajt egy, az elektronikus információs rendszerre vonatkozó konfigurációkezelési tervet, mely figyelembe veszi a szerepköröket, felelősségeket, konfigurációkezelési folyamatokat és eljárásokat;

3.3.6.9.1.2. bevezet egy folyamatot a konfigurációelemek azonosítására a rendszer-fejlesztési életciklus folyamán és a konfigurációelemek konfigurációjának kezelésére;

3.3.6.9.1.3. meghatározza az elektronikus információs rendszer konfigurációelemeit, és a konfigurációelemeket a konfigurációkezelés alá helyezi;

3.3.6.9.1.4. védi a konfigurációkezelési tervet a jogosulatlan felfedéssel és módosítással szemben.

3.3.6.10. A szoftverhasználat korlátozásai

3.3.6.10.1. Az érintett szervezet:

3.3.6.10.1.1. kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak;

3.3.6.10.1.2. a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;

3.3.6.10.1.3. ellenőrzi és dokumentálja az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

3.3.6.11. A felhasználó által telepített szoftverek

3.3.6.11.1. Az érintett szervezet:

3.3.6.11.1.1. megfogalmazza az elektronikus információs rendszer vonatkozásában, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti azokat a szabályokat, amelyek meghatározzák a szoftverek felhasználó általi telepítési lehetőségét;

3.3.6.11.1.2. érvényesíti a szoftvertelepítésre vonatkozó szabályokat az érintett szervezet által meghatározott módszerek szerint;

3.3.6.11.1.3. meghatározott gyakorisággal ellenőrzi a szabályok betartását.

3.3.7. KARBANTARTÁS

3.3.7.1. Rendszer karbantartási eljárásrend
3.3.7.1.1. Az érintett szervezet:
3.3.7.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a rendszer karbantartási eljárásrendet, mely a rendszer karbantartási kezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
3.3.7.1.1.2. a fizikai védelmi eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer karbantartási eljárásrendet.
3.3.7.2. Rendszeres karbantartás
3.3.7.2.1. Az érintett szervezet:
3.3.7.2.1.1. a karbantartásokat és javításokat ütemezetten hajtja végre, dokumentálja és felülvizsgálja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a szervezeti követelményeknek megfelelően;
3.3.7.2.1.2. jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;
3.3.7.2.1.3. az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a szervezeti létesítményből;
3.3.7.2.1.4. az elszállítás előtt minden adatot és információt - mentést követően - töröl a berendezésről;
3.3.7.2.1.5. ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;
3.3.7.2.1.6. csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz.
3.3.7.2.2. Automatikus támogatás
3.3.7.2.2.1. Az érintett szervezet:
3.3.7.2.2.1.1. automatizált mechanizmusokat alkalmaz a karbantartások és javítások ütemezésére, lefolytatására és dokumentálására;
3.3.7.2.2.1.2. naprakész, pontos és teljes nyilvántartást készít minden igényelt, ütemezett, folyamatban lévő és befejezett karbantartási és javítási akcióról.
3.3.7.3. Karbantartási eszközök
3.3.7.3.1. Az érintett szervezet az elektronikus információs rendszer vonatkozásában jóváhagyja, nyilvántartja, és ellenőrzi az elektronikus információs rendszer karbantartási eszközeit.
3.3.7.3.2. Adathordozó ellenőrzés
Az érintett szervezet ellenőrzi a diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák.
3.3.7.4. Távoli karbantartás
3.3.7.4.1. Az érintett szervezet:
3.3.7.4.1.1. jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket;

3.3.7.4.1.2. akkor engedélyezi a távoli karbantartási és diagnosztikai eszközök használatát, ha az összhangban áll az informatikai biztonsági szabályzattal, és dokumentálva van az elektronikus információs rendszer rendszerbiztonsági tervében;

3.3.7.4.1.3. hitelesítéseket alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásánál;

3.3.7.4.1.4. nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről;

3.3.7.4.1.5. lezárja a munkaszakaszt és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik.

3.3.7.4.2. Dokumentálás

Az érintett szervezet az elektronikus információs rendszer rendszerbiztonsági tervében dokumentálja a távoli karbantartási és diagnosztikai kapcsolatok létrehozására és használatára vonatkozó szabályokat és eljárásokat.

3.3.7.4.3. Összehasonlítható biztonság

3.3.7.4.3.1. Az érintett szervezet megköveteli, hogy a távoli karbantartási és diagnosztikai javítások olyan elektronikus információs rendszerből legyenek végrehajtva, amelyben a biztonsági képességek azonos szintűek a szervizelt rendszer biztonsági képességekkel.

3.3.7.4.3.2. Ha a 3.3.7.4.3.1. pont szerinti eljárás nem biztosított, a szervizelendő elemet el kell távolítani az elektronikus információs rendszerből, és a távoli karbantartási és diagnosztikai szervizelést megelőzően minden információt törölni kell az érintett rendszerelemről.

3.3.7.4.3.3. Ha a 3.3.7.4.3.1. vagy a 3.3.7.4.3.2. pont szerinti eljárást nem lehet lefolytatni, a szervizelés végrehajtását követően át kell vizsgálni az elemet a lehetséges kártékony szoftverek miatt, mielőtt visszakapcsoljak az elektronikus információs rendszerhez.

3.3.8. ADATHORDOZÓK VÉDELME

3.3.8.1. Adathordozók védelmére vonatkozó eljárásrend

3.3.8.1.1. Az érintett szervezet:

3.3.8.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az adathordozók védelmére vonatkozó eljárásrendet, mely az adathordozókra vonatkozó védelmi szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.8.1.1.2. az adathordozók védelmére vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti az adathordozók védelmére vonatkozó eljárásrendet.

3.3.8.2. Hozzáférés az adathordozókhoz

Az érintett szervezet az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát meghatározza.

3.3.8.3. Adathordozók címkézése

Az érintett szervezet megjelöli az elektronikus információs rendszer adathordozóit, jelezve az információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket, ha ezek rendelkezésre állnak.

3.3.8.4. Adathordozók tárolása

3.3.8.4.1. Az érintett szervezet:

3.3.8.4.1.1. fizikailag ellenőrzi és biztonságosan tárolja az adathordozókat, az arra engedélyezett vagy kijelölt helyen;

3.3.8.4.1.2. védi az elektronikus információs rendszer adathordozóit mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy nem törlik.

3.3.8.5. Adathordozók szállítása

3.3.8.5.1. Az érintett szervezet:

3.3.8.5.1.1. meghatározott biztonsági óvintézkedésekkel védi és ellenőrzi az elektronikus információs rendszer adathordozóit az ellenőrzött területeken kívüli szállítás folyamán;

3.3.8.5.1.2. biztosítja az adathordozók elszámoltathatóságát az ellenőrzött területeken kívüli szállítás folyamán;

3.3.8.5.1.3. dokumentálja az adathordozók szállításával kapcsolatos tevékenységeket;

3.3.8.5.1.4. korlátozza az adathordozók szállításával kapcsolatos tevékenységeket az arra jogosult személyekre.

3.3.8.5.2. Kriptográfiai védelem

Kriptográfiai mechanizmusokat kell alkalmazni a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének a védelmére az ellenőrzött területeken kívüli szállítás folyamán.

3.3.8.6. Adathordozók törlése

3.3.8.6.1. Az érintett szervezet:

3.3.8.6.1.1. a helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törli az elektronikus információs rendszer meghatározott adathordozóit a leselejtezés, a szervezeti ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt;

3.3.8.6.1.2. a törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően alkalmazza.

3.3.8.6.2. Ellenőrzés

Az érintett szervezet felülvizsgálja, jóváhagyja, nyomon követi, dokumentálja, és ellenőrzi az adathordozók törlésével és megsemmisítésével kapcsolatos tevékenységeket.

3.3.8.6.3. Tesztelés

A törlésre alkalmazott eszközöket és eljárásokat meghatározott gyakorisággal tesztelni kell.

3.3.8.6.4. Törlés megsemmisítés nélkül

Nem romboló törlési technikák alkalmazhatók a meghatározott hordozható tárolóeszközökre, mielőtt ilyen eszközöket az elektronikus információs rendszerhez csatolnak.

3.3.8.7. Adathordozók használata

3.3.8.7.1. Az érintett szervezet engedélyezi, korlátozza, vagy tiltja egyes, vagy bármely adathordozó típusok használatát a meghatározott elektronikus információs rendszereken vagy rendszerelemeken működő biztonsági intézkedések használatával.

3.3.8.7.2. Ismeretlen tulajdonos

Az érintett szervezet megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható.

3.3.9. AZONOSÍTÁS ÉS HITELESÍTÉS

3.3.9.1. Azonosítási és hitelesítési eljárásrend
3.3.9.1.1. Az érintett szervezet:
3.3.9.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az azonosítási és hitelesítésre vonatkozó eljárásrendet, mely az azonosítási és hitelesítési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
3.3.9.1.1.2. az azonosítási és hitelesítésre vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti az azonosítási és hitelesítésre vonatkozó eljárásrendet.
3.3.9.2. Azonosítás és hitelesítés
3.3.9.2.1. Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a szervezet felhasználóit, a felhasználók által végzett tevékenységet.
3.3.9.2.2. Hálózati hozzáférés privilegizált fiókokhoz
Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a különleges jogosultsághoz kötött - úgynevezett privilegizált - felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.
3.3.9.2.3. Hálózati hozzáférés nem privilegizált fiókokhoz
Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.
3.3.9.2.4. Helyi hozzáférés privilegizált fiókokhoz
Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.
3.3.9.2.5. Visszajátszás-védelem
Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.
3.3.9.2.6. Távoli hozzáférés - külön eszköz
Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a felhasználói fiókokhoz való távoli hozzáféréshez, és az egyik hozzáférést megelőző tényező egy, az elektronikus információs rendszertől elkülönülő olyan eszköz, amelyen a meghatározott biztonsági követelmények teljesülnek.
3.3.9.2.7. Helyi hozzáférés nem privilegizált fiókokhoz
Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.
3.3.9.2.8. Visszajátszás ellen védett hálózati hozzáférés nem privilegizált fiókokhoz
Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.
3.3.9.3. Eszközök azonosítása és hitelesítése
Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a meghatározott eszközöket, vagy eszköz típusokat mielőtt helyi vagy távoli hálózati kapcsolatot létesítene velük.
3.3.9.4. Azonosító kezelés
3.3.9.4.1. Az érintett szervezet:
3.3.9.4.1.1. az egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését a szervezet által meghatározott személyek vagy szerepkörök jogosultságához köti;
3.3.9.4.1.2. hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz;

3.3.9.4.1.3. meghatározott időtartamig megakadályozza az azonosítók ismételt felhasználását;
3.3.9.4.1.4. meghatározott időtartamú inaktivitás esetén letiltja az azonosítót.
3.3.9.5. A hitelesítésre szolgáló eszközök kezelése
3.3.9.5.1. Az érintett szervezet:
3.3.9.5.1.1. ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát;
3.3.9.5.1.2. meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;
3.3.9.5.1.3. biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;
3.3.9.5.1.4. dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;
3.3.9.5.1.5. megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során;
3.3.9.5.1.6. meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;
3.3.9.5.1.7. a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;
3.3.9.5.1.8. megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;
3.3.9.5.1.9. megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;
3.3.9.5.1.10. lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.
3.3.9.5.2. Jelszó (tudás) alapú hitelesítés
3.3.9.5.2.1. Az érintett szervezet:
3.3.9.5.2.1.1. a jelszóra a következő elvárásokat érvényesíti: kis- és nagybetűk megkülönböztetése; a karakterek számának meghatározása; a kisbetűk, nagybetűk, számok és speciális karakterek, és minimális jelszóhosszúság;
3.3.9.5.2.1.2. meghatározott szám karakterváltozást kényszerít ki új jelszó létrehozásakor;
3.3.9.5.2.1.3. a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást), és nem továbbítja;
3.3.9.5.2.1.4. a jelszavakra minimális és maximális élettartam korlátozást juttat érvényre úgy, hogy meghatározott számú új jelszóig megtiltja a jelszavak ismételt felhasználását, és a rendszerbe első lépést lehetővé tevő ideiglenes jelszó lecserélésére kötelez.
3.3.9.5.3. Birtoklás alapú hitelesítés
3.3.9.5.3.1. Az érintett szervezet:
3.3.9.5.3.1.1. az elektronikus információs rendszer hardver token alapú hitelesítése esetén olyan mechanizmusokat alkalmaz, amely megfelel az érintett szervezet által meghatározott minőségi követelményeknek, vagy
3.3.9.5.3.1.2. az elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén:
3.3.9.5.3.1.2.1. ellenőrzi a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is;

3.3.9.5.3.1.2.2. kikényszeríti a megfelelő magánkulcshoz való jogosult hozzáférést;

3.3.9.5.3.1.2.3. összekapcsolja a hitelesített azonosságot az egyéni vagy csoport fiókkal;

3.3.9.5.3.1.2.4. megvalósítja a visszavonási adatok helyi tárolását a tanúsítványlánc felépítésének és ellenőrzésének támogatására arra az esetre, amikor a visszavonási információk a hálózaton keresztül nem elérhetők.

3.3.9.5.4. Tulajdonság alapú hitelesítés

Az érintett szervezet a felhasználó egyedi azonosítást lehetővé tevő tulajdonságai alapján végzi el az azonosítást.

3.3.9.5.5. Személyes vagy megbízható harmadik fél általi regisztráció

Az érintett szervezet meghatározott hitelesítő eszköz átvételéhez megkövetel egy olyan regisztrációs eljárást, melyet meghatározott regisztrációs szervezet folytat le az érintett szervezet által meghatározott személyek vagy szerepkörök jóváhagyása mellett.

3.3.9.6. A hitelesítésre szolgáló eszköz visszacsatolása

Az elektronikus információs rendszer fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

3.3.9.7. Hitelesítés kriptográfiai modul esetén

Az elektronikus információs rendszer egy adott kriptográfiai modulhoz való hitelesítésre olyan mechanizmusokat használ, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának.

3.3.9.8. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

3.3.9.8.1. Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az érintett szervezeten kívüli felhasználókat és tevékenységüket.

3.3.9.8.2. Hitelesítésszolgáltatók tanúsítványának elfogadása

Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el az érintett szervezeten kívüli felhasználók hitelesítéséhez.

3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE

3.3.10.1. Hozzáférés ellenőrzési eljárásrend

3.3.10.1.1. Az érintett szervezet:

3.3.10.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a hozzáférés ellenőrzési eljárásrendet, mely a hozzáférés ellenőrzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.10.1.1.2. a hozzáférés védelmére vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a hozzáférések védelmére vonatkozó eljárásrendet.

3.3.10.2. Felhasználói fiókok kezelése

3.3.10.2.1. Az érintett szervezet:

3.3.10.2.1.1. meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait és ezek típusait;

3.3.10.2.1.2. kijelöli a felhasználói fiókok fiókkezelőit;

3.3.10.2.1.3. kialakítja a csoport- és szerepkör tagsági feltételeket;

3.3.10.2.1.4. meghatározza az elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit;

3.3.10.2.1.5. létrehozza, engedélyezi, módosítja, letiltja, és eltávolítja a felhasználói fiókokat a meghatározott eljárásokkal vagy feltételekkel összhangban;

3.3.10.2.1.6. ellenőrzi a felhasználói fiókok használatát;

3.3.10.2.1.7. értesíti a fiókkezelőket, ha:

3.3.10.2.1.7.1. a felhasználói fiókokra már nincsen szükség,

3.3.10.2.1.7.2. a felhasználók kiléptek vagy áthelyezésre kerültek,

3.3.10.2.1.7.3. az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak;

3.3.10.2.1.8. feljogosít az elektronikus információs rendszerhez való hozzáférésre:

3.3.10.2.1.8.1. az érvényes hozzáférési engedély,

3.3.10.2.1.8.2. a tervezett rendszerhasználat,

3.3.10.2.1.8.3. az alapfeladatok és funkcióik alapján;

3.3.10.2.1.9. meghatározott gyakorisággal felülvizsgálja a felhasználói fiókokat, a fiókkezelési követelményekkel való összhangot;

3.3.10.2.1.10. kialakít egy folyamatot a megosztott vagy csoport felhasználói fiókokhoz tartozó hitelesítő eszközök vagy adatok újra kibocsátására (ha ilyet alkalmaznak), a csoport tagjainak változása esetére.

3.3.10.2.2. Automatikus kezelés

Az elektronikus információs rendszer automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer fiókjainak kezeléséhez.

3.3.10.2.3. Ideiglenes fiókok eltávolítása

Meghatározott időtartam letelte után az elektronikus információs rendszer automatikusan eltávolítja vagy letiltja az ideiglenes vagy kényszerhelyzetben létrehozott felhasználói fiókokat vagy egyes kijelölt felhasználói fiók típusokat.

3.3.10.2.4. Inaktív fiókok letiltása

Az elektronikus információs rendszer automatikusan letiltja az inaktív fiókokat meghatározott időtartam letelte után.

3.3.10.2.5. Automatikus naplózás

Az elektronikus információs rendszer automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket, és értesíti ezekről a meghatározott személyeket vagy szerepköröket.

3.3.10.2.6. Kiléptetés

Meghatározott időtartamú várható inaktivitás vagy egyéb előre meghatározott esetekben ki kell léptetni a felhasználót.

3.3.10.2.7. Szokatlan használat

Figyelni kell az elektronikus információs rendszer fiókjait az érintett szervezet által meghatározott szokatlan használat szempontjából, és meghatározott személyeknek vagy szerepköröknek jelenteni kell azt.

3.3.10.2.8. Letiltás

Azonnal le kell tiltani a kockázatot jelentő felhasználók fiókjait.

3.3.10.3. Hozzáférés ellenőrzés érvényesítése

Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

3.3.10.4. Információáramlás ellenőrzés érvényesítése

Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információáramlás ellenőrzéséhez az érintett szervezet által meghatározott információáramlás ellenőrzési szabályoknak megfelelően.

3.3.10.5. A felelősségek szétválasztása

3.3.10.5.1. Az érintett szervezet:

3.3.10.5.1.1. szétválasztja az egyéni felelősségeket;

3.3.10.5.1.2. dokumentálja az egyéni felelősségek szétválasztását;

3.3.10.5.1.3. meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelősségek szétválasztása érdekében.

3.3.10.6. Legkisebb jogosultság elve

3.3.10.6.1. Az elektronikus információs rendszer a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi.

3.3.10.6.2. Jogosult hozzáférés a biztonsági funkciókhoz

Az érintett szervezet hozzáférési jogosultságokat biztosít a meghatározott biztonsági funkciókhoz és biztonságkritikus információkhoz.

3.3.10.6.3. Nem privilegizált hozzáférés a biztonsági funkciókhoz

Az érintett szervezet kötelezővé teszi, hogy a szervezet meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező felhasználói a nem biztonsági funkciók használatához nem a különleges jogosultsághoz kötött - úgynevezett privilegizált - fiókjukat vagy szerepkörüket használják.

3.3.10.6.4. Privilegizált fiókok

Az érintett szervezet az elektronikus információs rendszer privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.

3.3.10.6.5. Privilegizált funkciók használatának naplózása

Az elektronikus információs rendszer naplózza a privilegizált funkciók végrehajtását.

3.3.10.6.6. Privilegizált funkciók tiltása nem privilegizált felhasználóknak

Az elektronikus információs rendszer megakadályozza, hogy a nem privilegizált felhasználók privilegizált funkciókat hajtsanak végre, ideértve a biztonsági ellenintézkedések kikapcsolását, megkerülését, vagy megváltoztatását.

3.3.10.6.7. Hálózati hozzáférés a privilegizált parancsokhoz

A meghatározott privilegizált parancsok hálózaton keresztüli elérését csak meghatározott üzemeltetési szükséghelyzetben lehet engedélyezni, és az ilyen hozzáférések indoklását dokumentálni kell a rendszerbiztonsági tervben. Privilegizált parancsok csak meghatározott munkaállomásokról, terminálokról, szegmensekről és IP címekről adhatóak ki, mely munkaállomások/terminálok helyiségei fizikai hozzáférés szempontjából normáltól eltérő szintű besorolást kapnak.

3.3.10.7. Sikertelen bejelentkezési kísérletek

3.3.10.7.1. Az elektronikus információs rendszer:

3.3.10.7.1.1. az érintett szervezet által meghatározott esetszám korlátot alkalmaz a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire;

3.3.10.7.1.2. ha a sikertelen bejelentkezési kísérletekre felállított esetszám korlátot a felhasználó túllépi, automatikusan zárolja a felhasználói fiókot, vagy csomópontot meghatározott időtartamig, vagy meghatározott módon késlelteti a következő bejelentkezési kísérletet.

3.3.10.8. A rendszerhasználat jelzése

3.3.10.8.1. Az érintett szervezet az elektronikus információs rendszer felhasználásával:

3.3.10.8.1.1. az érintett szervezet által meghatározott rendszer használatra vonatkozó figyelmeztető üzenetet vagy jelzést küld a felhasználó számára a rendszerhez való hozzáférés engedélyezése előtt, mely jelzi, hogy:

3.3.10.8.1.1.1. a felhasználó az érintett szervezet elektronikus információs rendszerét használja;

3.3.10.8.1.1.2. a rendszer használatot figyelhetik, rögzíthetik, naplózhatják;

3.3.10.8.1.1.3. a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár;

3.3.10.8.1.1.4. a rendszer használata egyben a felhasználó előbbiekbe történő beleegyezését is jelenti.

3.3.10.8.2. Az elektronikus információs rendszer a figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn tartja, amíg a felhasználó közvetlen műveletet nem végez az elektronikus információs rendszerbe való bejelentkezéshez vagy további rendszer hozzáféréshez.

3.3.10.8.3. Az elektronikus információs rendszer a nyilvánosan elérhető rendszerek esetén:

3.3.10.8.3.1. kijelzi a rendszer használat feltételeit, mielőtt további hozzáférést biztosít;

3.3.10.8.3.2. ha felügyelet, adatrögzítés vagy naplózás történik, kijelzi, hogy ezek megfelelnek az adatvédelmi szabályoknak;

3.3.10.8.3.3. leírást biztosít a rendszer engedélyezett felhasználásáról.

3.3.10.9. Egyidejű munkaszakasz kezelés

Az érintett szervezet az elektronikus információs rendszerben meghatározott számra korlátozza az egyidejű munkaszakaszok számát, a meghatározott fiókok vagy fiók típusok számára külön-külön.

3.3.10.10. A munkaszakasz zárolása

3.3.10.10.1. Az érintett szervezet:

3.3.10.10.1.1. meghatározott időtartamú inaktivitás után, vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést;

3.3.10.10.1.2. megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.

3.3.10.10.2. Képernyőtakarás

A munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a záró személy nevét is tartalmazhatja - kell eltakarni.

3.3.10.11. A munkaszakasz lezárása

Az elektronikus információs rendszer automatikusan lezárja a munkaszakaszt az érintett szervezet által meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után.

3.3.10.12. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

3.3.10.12.1. Az érintett szervezet:

3.3.10.12.1.1. kijelöli azokat a felhasználói tevékenységeket, amelyeket az elektronikus információs rendszerben azonosítás vagy hitelesítés nélkül is végre lehet hajtani;

3.3.10.12.1.2. dokumentálja és indokolja a rendszerbiztonsági tervben, vagy más szabályzatban az azonosítás vagy hitelesítés nélkül is végrehajtható felhasználói tevékenységeket.

3.3.10.13. Távoli hozzáférés

3.3.10.13.1. Az érintett szervezet:

3.3.10.13.1.1. kidolgozza és dokumentálja minden engedélyezett távoli hozzáférés típusra a felhasználásra vonatkozó korlátozásokat, a konfigurálási vagy a kapcsolódási követelményeket és a megvalósítási útmutatókat;

3.3.10.13.1.2. engedélyezési eljárást folytat le az elektronikus információs rendszerhez történő távoli hozzáférés feltételeként.

3.3.10.13.2. Ellenőrzés

Az elektronikus információs rendszer figyeli és ellenőrzi a távoli hozzáféréseket.

3.3.10.13.3. Titkosítás

Kriptográfiai mechanizmusokat kell alkalmazni a távoli hozzáférés munkaszakaszok bizalmasságának és sértetlenségének a védelmére.

3.3.10.13.4. Hozzáférés ellenőrzési pontok

Minden távoli hozzáférést felügyelt hozzáférés ellenőrzési ponton keresztül kell irányítani az elektronikus információs rendszerben.

3.3.10.13.5. Privilegizált parancsok elérése

3.3.10.13.5.1. Az érintett szervezet:

3.3.10.13.5.1.1. privilegizált parancsok végrehajtásához és biztonságkritikus információk eléréséhez távoli hozzáférést csak meghatározott és elfogadott igény esetén engedélyez;

3.3.10.13.5.1.2. dokumentálja és indokolja a 3.3.10.13.5.1.1. pont szerinti hozzáféréseket a rendszerbiztonsági tervben.

3.3.10.14. Vezeték nélküli hozzáférés

3.3.10.14.1. Az érintett szervezet:

3.3.10.14.1.1. belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán;

3.3.10.14.1.2. engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

3.3.10.14.2. Hitelesítés és titkosítás

Az érintett szervezet az elektronikus információs rendszerben titkosítással, és a felhasználók, vagy eszközök hitelesítésével védi a vezeték nélküli hozzáférést.

3.3.10.14.3. Felhasználó konfigurálás tiltása

Az érintett szervezet azonosítja a felhasználókat, és csak közvetlen jogosultság birtokában, a védett hálózaton kialakított vezetékes kapcsolaton keresztül teszi lehetővé számukra a vezeték nélküli hálózat független konfigurálását.

3.3.10.14.4. Antennák

Az érintett szervezet olyan karakterisztikájú és teljesítményszintű antennákat és árnyékolási megoldásokat üzemeltet, vagy egyéb technikákat alkalmaz, amelyekkel csökkenti az érintett szervezet fizikai védelmi határain kívül a jelek észlelésének a valószínűségét.

3.3.10.15. Mobil eszközök hozzáférés ellenőrzése

3.3.10.15.1. Az érintett szervezet:

3.3.10.15.1.1. belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre;

3.3.10.15.1.2. engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

3.3.10.15.2. Titkosítás

Az érintett szervezet teljes eszköztitkosítást, tároló alapú titkosítást, vagy más technológiai eljárást alkalmaz az általa meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére, vagy az információk hozzáférhetetlenné tételére.

3.3.10.16. Külső elektronikus információs rendszerek használata

3.3.10.16.1. Az érintett szervezet:

3.3.10.16.1.1. meghatározza, hogy milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni az elektronikus információs rendszerhez;

3.3.10.16.1.2. meghatározza, hogy külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani az érintett szervezet által ellenőrzött információkat.

3.3.10.16.2. Korlátozott használat

3.3.10.16.2.1. Az érintett szervezet csak abban az esetben engedélyezi jogosult felhasználóknak egy külső elektronikus információs rendszer felhasználását az elektronikus információs rendszerhez való hozzáférésre, az által ellenőrzött információk feldolgozására, tárolására vagy továbbítására, ha:

3.3.10.16.2.1.1. előzetesen ellenőrzi a szükséges biztonsági intézkedések meglétét a külső rendszeren saját szabályzóinak megfelelő módon; vagy

3.3.10.16.2.1.2. jóváhagyott kapcsolat van az elektronikus információs rendszerek között, vagy megállapodás született a külső elektronikus információs rendszert befogadó szervezettel.

3.3.10.16.3. Hordozható adattároló eszközök

Az érintett szervezet korlátozza vagy megtiltja az ellenőrzött hordozható tárolóeszközök használatát külső elektronikus információs rendszerben is jogosultsággal rendelkező személyek számára.

3.3.10.17. Információmegosztás

3.3.10.17.1. Az érintett szervezet:

3.3.10.17.1.1. elősegíti az információmegosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információmegosztási körülmények esetén, amikor felhasználói megítélés szóba jöhet;

3.3.10.17.1.2. automatizált mechanizmusokat vagy kézi folyamatokat alkalmaz arra, hogy segítséget nyújtson a felhasználóknak az információmegosztási vagy együttműködési döntések meghozatalában.

3.3.10.18. Nyilvánosan elérhető tartalom

3.3.10.18.1. Az érintett szervezet:

3.3.10.18.1.1. kijelöli azokat a személyeket, akik jogosultak a nyilvánosan hozzáférhető elektronikus információs rendszeren az érintett szervezettel kapcsolatos bármely információ közzétételére;

3.3.10.18.1.2. a 3.3.10.18.1.1. pont szerinti kijelölt személyeket képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat;

3.3.10.18.1.3. közzététel előtt átvizsgálja a javasolt tartalmat;

3.3.10.18.1.4. meghatározott gyakorisággal átvizsgálja a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében, és eltávolítja azokat.

3.3.11. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

3.3.11.1. Ezeket a rendelkezéseket egy adott elektronikus információs rendszer tekintetében abban az esetben kell alkalmazni, ha az adott elektronikus információs rendszert az érintett szervezet üzemelteti. Üzemeltetési szolgáltatási szerződés esetén szerződéses kötelemként kell érvényesíteni a 3.3.11. pontban és alpontjaiban foglaltakat, és azokat a szolgáltatónak kell biztosítania.

3.3.11.2. Rendszer- és információsértetlenségre vonatkozó eljárásrend

3.3.11.2.1. Az érintett szervezet:

3.3.11.2.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a rendszer- és információsértetlenségre vonatkozó eljárásrendet, mely a szervezet informatikai biztonsági szabályzatának részét képező, rendszer- és információsértetlenségre vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.11.2.1.2. a rendszer- és információsértetlenségre vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja, és frissíti a rendszer- és információsértetlenségre vonatkozó eljárásrendet.

3.3.11.3. Hibajavítás

3.3.11.3.1. Az érintett szervezet:

3.3.11.3.1.1. azonosítja, belső eljárásrendje alapján jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit;

3.3.11.3.1.2. telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket az érintett szervezet feladatellátásának hatékonysága, a szóba jöhető következmények szempontjából;

3.3.11.3.1.3. a biztonságkritikus szoftvereket a frissítésük kiadását követő meghatározott időtartamon belül telepíti vagy telepítteti;

3.3.11.3.1.4. beépíti a hibajavítást a konfigurációkezelési folyamatba.

3.3.11.3.2. Automatizált hibajavítási állapot

Az érintett szervezet automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer elemei hibajavítási állapotának meghatározására.

3.3.11.3.3. Központi kezelés

Az érintett szervezet központilag kezeli a hibajavítás folyamatát.

3.3.11.4. Kártékony kódok elleni védelem

3.3.11.4.1. Az érintett szervezet:

3.3.11.4.1.1. az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat;

3.3.11.4.1.2. frissíti a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg;

3.3.11.4.1.3. konfigurálja a kártékony kódok elleni védelmi mechanizmusokat úgy, hogy a védelem eszköze:

3.3.11.4.1.3.1. rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtsa végre a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon, a hálózati belépési vagy kilépési pontokon, a biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják,

3.3.11.4.1.3.2. a kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt, és riassza a rendszeradminisztrátort és az érintett szervezet által meghatározott további személy(eke)t;

3.3.11.4.1.4. ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.

3.3.11.4.2. Központi kezelés

Az elektronikus információs rendszer központilag kezeli a kártékony kódok elleni védelmi mechanizmusokat.

3.3.11.4.3. Automatikus frissítés

Az elektronikus információs rendszer automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat.

3.3.11.5. Az elektronikus információs rendszer felügyelete

3.3.11.5.1. Az érintett szervezet:

3.3.11.5.1.1. felügyeli az elektronikus információs rendszert, hogy észlelje a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;

3.3.11.5.1.2. azonosítja az elektronikus információs rendszer jogosulatlan használatát;

3.3.11.5.1.3. felügyeleti eszközöket alkalmaz a meghatározott alapvető információk gyűjtésére, és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;

3.3.11.5.1.4. védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;

3.3.11.5.1.5. erősíti az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;

3.3.11.5.1.6. meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek.

3.3.11.5.2. Automatizálás

Automatizált eszközöket kell alkalmazni az események közel valós idejű vizsgálatának támogatására.

3.3.11.5.3. Felügyelet

Az elektronikus információs rendszer felügyelje a beérkező és kimenő adatforgalmat a szokatlan vagy jogosulatlan tevékenységekre vagy körülményre tekintettel.

3.3.11.5.4. Riasztás

Az elektronikus információs rendszer riassza az érintett szervezet illetékes személyeit, csoportjait, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli.

3.3.11.6. Biztonsági riasztások és tájékoztatások

3.3.11.6.1. Az érintett szervezet:

3.3.11.6.1.1. folyamatosan figyeli a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;

3.3.11.6.1.2. folyamatosan figyelemmel kíséri a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket;

3.3.11.6.1.3. szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki;

3.3.11.6.1.4. a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez;

3.3.11.6.1.5. kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart az érintett, külön jogszabályban meghatározott szervekkel;

3.3.11.6.1.6. megfelelő ellenintézkedéseket és válaszlépéseket tesz.

3.3.11.6.2. Automatikus riasztások

Mechanizmusokat kell kialakítani a biztonsági riasztások és figyelmeztetések szervezeten belüli elérhetőségének biztosítására.

3.3.11.7. A biztonsági funkcionalitás ellenőrzése

3.3.11.7.1. Az elektronikus információs rendszer:

3.3.11.7.1.1. ellenőrzi a beállított biztonsági funkciókat az ellenőrzésre jogosult felhasználó utasítására, vagy időszakosan;

3.3.11.7.1.2. értesítést küld az érintett szervezet által meghatározott személyeknek vagy szerepköröknek, ha az ellenőrzés hibát tár fel;

3.3.11.7.1.3. rendellenesség észlelése esetén leállítja a rendszert, az érintett szerv által alkalmazott döntése szerint újraindítja a rendszert, vagy egyéb ellenintézkedést valósít meg.

3.3.11.8. Szoftver- és információsértetlenség

3.3.11.8.1. Az érintett szervezet sértetlenség ellenőrző eszközt alkalmaz a szoftverek és információk jogosulatlan módosításának észlelésére.

3.3.11.8.2. Sértetlenség ellenőrzés

Az elektronikus információs rendszer sértetlenség ellenőrzést hajt végre a meghatározott szoftverekre és információkra, a rendszer újraindításakor, vagy biztonsági esemény bekövetkezését követően, vagy meghatározott gyakorisággal.

3.3.11.8.3. Észlelés és reagálás

Az érintett szervezet beépíti az elektronikus információs rendszer jogosulatlan változtatásainak észlelését a biztonsági eseményekre reagáló eljárásaiba.

3.3.11.8.4. Automatikus értesítés

Az érintett szervezet automatizált eszközöket alkalmaz a meghatározott személyek vagy szerepkörök értesítésére, ha a sértetlenség ellenőrzés rendellenességet tár fel.

3.3.11.8.5. Automatikus reagálás

Az elektronikus információs rendszer automatikusan leállítja vagy újraindítja a rendszert, vagy egyéb intézkedést valósít meg, ha a sértetlenség ellenőrzés rendellenességet tár fel.

3.3.11.8.6. Végrehajtható kód

Az elektronikus információs rendszer megtiltja az olyan bináris vagy gépi kód használatát, amely nem ellenőrzött forrásból származik, vagy amelynek forráskódjával nem rendelkezik.

3.3.11.9. Kéretlen üzenetek elleni védelem

3.3.11.9.1. Az érintett szervezet:

3.3.11.9.1.1. kéretlen üzenetek - úgynevezett levélszemét - elleni védelmet valósít meg az elektronikus információs rendszer belépési és kilépési pontjain, a levélszemét észlelése és kiszűrése érdekében;

3.3.11.9.1.2. új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat, összhangban a konfigurációkezelési szabályzattal és eljárásrenddel.

3.3.11.9.2. Központi kezelés

Az érintett szervezet központi beállításokkal irányítja a levélszemét elleni védelmet.

3.3.11.9.3. Frissítés

Az elektronikus információs rendszer automatikusan frissíti a levélszemét elleni védelmi mechanizmusokat azok újabb verzióival.

3.3.11.10. Bemeneti információ ellenőrzés

Az elektronikus információs rendszer ellenőrzi a meghatározott információ belépési pontok érvényességét.

3.3.11.11. Hibakezelés

3.3.11.11.1. Az elektronikus információs rendszer:

3.3.11.11.1.1. hibajelzéseket generál a hibajavításhoz szükséges információkat biztosítva, ugyanakkor nem nyújt semmi olyan információt, amelyet a támadók kihasználhatnak;

3.3.11.11.1.2. a hibajelzéseket kizárólag a meghatározott személyek vagy szerepkörök számára teszi elérhetővé.

3.3.11.12. A kimeneti információ kezelése és megőrzése

Az érintett szervezet az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

3.3.11.13. Memóriavédelem

Az elektronikus információs rendszerben biztonsági beállításokat kell alkalmazni azért, hogy védje a memóriát a jogosulatlan kódok végrehajtásától.

3.3.12. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

3.3.12.1. Naplózási eljárásrend

3.3.12.1.1. Az érintett szervezet:

3.3.12.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül a szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a naplózási eljárásrendet, mely a naplózásra és elszámoltathatóságra vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.12.1.1.2. a naplózásra és elszámoltathatóságra vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja, és frissíti a naplózási eljárásrendet.

3.3.12.2. Naplózható események

3.3.12.2.1. Az érintett szervezet:

3.3.12.2.1.1. meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét;

3.3.12.2.1.2. egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását;

3.3.12.2.1.3. megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

3.3.12.2.2. Felülvizsgálat

Az érintett szervezet meghatározott gyakorisággal felülvizsgálja, és aktualizálja a naplózandó eseményeket.

3.3.12.3. Naplóbejegyzések tartalma

3.3.12.3.1. Az elektronikus információs rendszer a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

3.3.12.3.2. Kiegészítő információk

Az elektronikus információs rendszer a naplóbejegyzésekben további, az érintett szervezet által meghatározott kiegészítő, részletesebb információkat is rögzít.

3.3.12.3.3. Központi kezelés

Az elektronikus információs rendszer biztosítja a meghatározott rendszerelemek által generált naplóbejegyzések tartalmának központi kezelését és konfigurálását.

3.3.12.4. Napló tárkapacitás

Az érintett szervezet a naplózásra elegendő méretű tárkapacitást biztosít, a biztonsági osztályba sorolásból következő naplózási funkciók figyelembevételével.

3.3.12.5. Naplózási hiba kezelése

3.3.12.5.1. Az elektronikus információs rendszer:

3.3.12.5.1.1. naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek;

3.3.12.5.1.2. elvégzi a meghatározott végrehajtandó tevékenységeket, így például a rendszer leállítását, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását.

3.3.12.5.2. Naplózási tárhely ellenőrzés

Az elektronikus információs rendszer figyelmezteti a meghatározott személyeket, szerepköröket és helyszíneket, ha a lefoglalt naplózási tárhely eléri a beállított maximális naplózási tárhely előre meghatározott részét.

3.3.12.5.3. Valósidejű riasztás

Az elektronikus információs rendszer riasztást küld, ha a meghatározott, valós idejű riasztást igénylő hibaesemények listája szerint valamely esemény megtörténik.

3.3.12.6. Naplóvizsgálat és jelentéskészítés

3.3.12.6.1. Az érintett szervezet:

3.3.12.6.1.1. rendszeresen felülvizsgálja és elemzi a naplóbejegyzéseket nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából;

3.3.12.6.1.2. jelenti ezeket a meghatározott személyeknek vagy szerepköröknek.

3.3.12.6.2. Folyamatba illesztés

Az érintett szervezet automatikus mechanizmusokat használ a naplóbejegyzések vizsgálatának, elemzésének és jelentésének átfogó folyamattá integrálására, amely a veszélyes vagy tiltott tevékenységekre és történésekre reagál.

3.3.12.6.3. Összegzés

Az érintett szervezet megvizsgálja és összefüggésbe hozza a különböző adattárakban található naplóbejegyzéseket, a teljes érintett szervezetre kiterjedő helyzetfelmérés érdekében.

3.3.12.6.4. Felügyeleti képességek integrálása

Az érintett szervezet egyesíti a naplóbejegyzések vizsgálatát a sebezhetőség ellenőrzési információkkal, a teljesítmény adatokkal, az elektronikus információs rendszer felügyeletéből származó információkkal, vagy egyéb forrásokból begyűjtött adatokkal vagy információkkal.

3.3.12.6.5. Összekapcsolás a fizikai hozzáférési információkkal

Az érintett szervezet összefüggésbe hozza a naplóbejegyzésekből származó információkat a fizikai hozzáférés felügyeletéből nyert információkkal.

3.3.12.7. Naplócsökkentés és jelentéskészítés

3.3.12.7.1. Az elektronikus információs rendszer:

3.3.12.7.1.1. lehetőséget biztosít naplócsökkentésre és jelentés készítésére, amely támogatja az igény esetén végzendő naplóáttekintési, naplóvizsgálati és jelentéskészítési követelményeket és a biztonsági eseményeket követő tényfeltáró vizsgálatait;

3.3.12.7.1.2. nem változtathatja meg a naplóbejegyzések eredeti tartalmát és időrendjét.

3.3.12.7.2. Automatikus feldolgozás

Az elektronikus információs rendszer biztosítja, hogy a fontos naplóbejegyzéseket automatikusan fel lehessen dolgozni.

3.3.12.8. Időbélyegek

3.3.12.8.1. Az elektronikus információs rendszer:

3.3.12.8.1.1. belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához;

3.3.12.8.1.2. időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz - úgynevezett UTC - vagy a Greenwichi középidőhöz - úgynevezett GMT - rendelhető módon, megfelelve az érintett szervezet által meghatározott időmérési pontosságnak.

3.3.12.8.2. Szinkronizálás

Az elektronikus információs rendszer meghatározott gyakorisággal összehasonlítja a belső rendszerórákat egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórákat a hiteles külső időforrással.

3.3.12.9. A naplóinformációk védelme

3.3.12.9.1. Az elektronikus információs rendszer megvédi a naplóinformációt és a napló kezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

3.3.12.9.2. Hozzáférés korlátozása

A naplófunkciók kezelésére csak az érintett szervezet által meghatározott, privilegizált felhasználók jogosultak.

3.3.12.9.3. Fizikailag elkülönített mentés

Az elektronikus információs rendszer a naplóbejegyzéseket meghatározott gyakorisággal elmenti, egy a keletkezési helyétől fizikailag elkülönülő rendszerre vagy rendszerelemre.

3.3.12.9.4. Kriptográfiai védelem

Kriptográfiai mechanizmusokat kell alkalmazni a naplóinformáció és a napló kezelő eszköz sértetlenségének védelmére.

3.3.12.10. Letagadhatatlanság

Az elektronikus információs rendszer védelmet biztosít az ellen, hogy egy adott személy az általa használt alkalmazás tekintetében letagadhassa, hogy elvégzett-e egy, a letagadhatatlanság követelménye alá sorolt tevékenységet.

3.3.12.11. A naplóbejegyzések megőrzése

Az érintett szervezet a naplóbejegyzéseket meghatározott - a jogszabályi és az érintett szervezeten belüli információ megőrzési követelményeknek megfelelő - időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

3.3.12.12. Naplógenerálás

3.3.12.12.1. Az elektronikus információs rendszer:

3.3.12.12.1.1. biztosítja a naplóbejegyzés generálási lehetőségét a 3.3.12.2. pontban meghatározott naplózható eseményekre;

3.3.12.12.1.2. lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire;

3.3.12.12.1.3. naplóbejegyzéseket állít elő a 3.3.12.2. pont szerinti eseményekre a 3.3.12.3. pontban meghatározott tartalommal.

3.3.12.12.2. Rendszerszintű időalap napló

Az elektronikus információs rendszer a naplóbejegyzéseiből rendszerszintű (logikai vagy fizikai) felülvizsgálati naplót állít össze, amely - a felülvizsgálati napló egyedi bejegyzéseinek időbélyegei közötti kapcsolat tekintetében meghatározott tűréshatáron túli - időviszonyokat is tartalmazza.

3.3.12.12.3. Változtatások

Az elektronikus információs rendszer biztosítja a lehetőséget a meghatározott személyeknek vagy szerepköröknek arra, hogy megváltoztassák az egyes rendszerelemekre végrehajtandó naplózást a kiválasztott esemény kritériumok alapján, meghatározott időtartamon belül.

3.3.13. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

3.3.13.1. Rendszer- és kommunikációvédelmi eljárásrend

3.3.13.1.1. Az érintett szervezet:

3.3.13.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belüli szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a rendszer- és kommunikációvédelmi eljárásrendet, mely a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.13.1.1.2. a rendszer- és kommunikációvédelmi eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja, és frissíti a rendszer- és kommunikációvédelmére vonatkozó eljárásrendet.

3.3.13.2. Alkalmazás szétválasztás

Az elektronikus információs rendszer elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az elektronikus információs rendszer irányítási funkcionalitásától.

3.3.13.3. Biztonsági funkciók elkülönítése

Az elektronikus információs rendszer elkülöníti a biztonsági funkciókat a nem biztonsági funkcióktól.

3.3.13.4. Információmaradványok

Az elektronikus információs rendszer meggátolja a megosztott rendszererőforrások útján történő jogosulatlan vagy véletlen információáramlást.

3.3.13.5. Túlterhelés - szolgáltatás megtagadás alapú támadás - elleni védelem

Az elektronikus információs rendszer véd a túlterheléses (úgynevezett szolgáltatás megtagadás) jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével.

3.3.13.6. A határok védelme

3.3.13.6.1. Az elektronikus információs rendszer:

3.3.13.6.1.1. felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt;

3.3.13.6.1.2. a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól;

3.3.13.6.1.3. csak az érintett szervezet biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

3.3.13.6.2. Hozzáférési pontok

Az érintett szervezet korlátozza az elektronikus információs rendszer külső hálózati kapcsolatainak a számát.

3.3.13.6.3. Külső kommunikációs szolgáltatások

3.3.13.6.3.1. Az érintett szervezet:

3.3.13.6.3.1.1. felügyelt interfészt működtet minden külső infokommunikációs szolgáltatáshoz;

3.3.13.6.3.1.2. minden felügyelt interfészhez forgalomáramlási szabályokat alakít ki;

3.3.13.6.3.1.3. védi az összes interfésznél az átvitelre kerülő információk bizalmasságát és sértetlenségét;

3.3.13.6.3.1.4. dokumentál minden kivételt a forgalomáramlási szabályok alól, a kivételt alátámasztó alapfeladattal és az igényelt kivétel időtartamával együtt;

3.3.13.6.3.1.5. meghatározott gyakorisággal áttekinti a forgalomáramlási szabályok alóli kivételeket, és eltávolítja azokat a kivételeket, amelyeket közvetlen alapfeladat már nem indokol.

3.3.13.6.4. Alapeseti visszautasítás

Az elektronikus információs rendszer a felügyelt kapcsolódási pontjain tilt, és csak kivételként engedélyez hálózati forgalmat.

3.3.13.6.5. Távoli készülékek megosztott csatornahasználatának tiltása

A távoli készülékkel kapcsolatban álló elektronikus információs rendszer meggátolja, hogy a készülék egyidejűleg helyi kapcsolatokat létesítsen a rendszerrel.

3.3.13.6.6. Hitelesített proxy kiszolgálók

Az elektronikus információs rendszer hitelesített proxy - olyan szerver, számítógép vagy szerveralkalmazás, amely a kliensek kéréseit köztes elemként más szerverekhez továbbítja - kiszolgálók segítségével irányítja a belső kommunikációs forgalmat a felügyelt interfészeken a meghatározott külső hálózatokhoz.

3.3.13.6.7. Biztonsági hibaállapot

Az elektronikus információs rendszer hibaállapotba kerül a határvédelmi eszköz működési hibája esetén.

3.3.13.6.8. Rendszerelemek elkülönítése

Az érintett szervezet határvédelmi mechanizmusokat alkalmaz azoknak az elektronikus információs rendszerelemeknek az elkülönítésére, amelyek a meghatározott alapfeladatokat és alapfunkciókat támogatják.

3.3.13.7. Az adatátvitel bizalmassága

3.3.13.7.1. Az elektronikus információs rendszer védje meg a továbbított információk bizalmasságát.

3.3.13.7.2. Kriptográfiai vagy egyéb védelem

Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk jogosulatlan felfedése ellen, kivéve, ha az átvitel más, az érintett szervezet által meghatározott alternatív fizikai ellenintézkedéssel védett.

3.3.13.8. Az adatátvitel sértetlensége

3.3.13.8.1. Az elektronikus információs rendszer megvédi a továbbított információk sértetlenségét.

3.3.13.8.2. Kriptográfiai vagy egyéb védelem

Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk megváltozásának észlelésére, ha az átvitel nincsen más alternatív fizikai intézkedésekkel védve.

3.3.13.9. A hálózati kapcsolat megszakítása

Az elektronikus információs rendszer megszakítja a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, meghatározott időtartamú inaktivitás után.

3.3.13.10. Kriptográfiai kulcs előállítása és kezelése

3.3.13.10.1. Az érintett szervezet előállítja és kezeli az elektronikus információs rendszerben alkalmazott kriptográfiához szükséges kriptográfiai kulcsokat a kulcsok előállítására, szétosztására, tárolására, hozzáférésére és megsemmisítésére vonatkozó belső szabályozásnak megfelelően.

3.3.13.10.2. Rendelkezésre állás

Az érintett szervezet előállítja, biztosítja az információk rendelkezésre állását abban az esetben is, amikor a kriptográfiai kulcsok elérhetetlenné válnak (elvesztés, sérülés, megsemmisülés).

3.3.13.11. Kriptográfiai védelem

Az elektronikus információs rendszer szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg.

3.3.13.12. Együttműködésen alapuló számítástechnikai eszközök

Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett szervezet engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

3.3.13.13. Nyilvános kulcsú infrastruktúra tanúsítványok

Az érintett szervezet nyilvános kulcsú tanúsítványokat állít ki a belső hitelesítési rend szerint, vagy a nyilvános kulcsú tanúsítványokat beszerzi a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatótól.

3.3.13.14. Mobilkód korlátozása

3.3.13.14.1. Az érintett szervezet:

3.3.13.14.1.1. meghatározza az elfogadható és a nem elfogadható mobilkódokat és mobilkód technológiákat;

3.3.13.14.1.2. használati korlátozásokat vezet be vagy megvalósítási útmutatót bocsát ki az elfogadható mobilkódokra és mobilkód technológiákra;

3.3.13.14.1.3. engedélyezi, felügyeli és ellenőrzi a mobilkódok használatát az elektronikus információs rendszeren belül.

3.3.13.15. Elektronikus információs rendszeren keresztüli hangátvitel (úgynevezett VoIP)

3.3.13.15.1. Az érintett szervezet:

3.3.13.15.1.1. használati korlátozásokat vezet be vagy megvalósítási útmutatót ad a VoIP technológiákhoz, felmérve a rosszindulatú használat esetén az elektronikus információs rendszerben okozható károkat;

3.3.13.15.1.2. engedélyezi, felügyeli, és ellenőrzi a VoIP használatát az elektronikus információs rendszeren belül.

3.3.13.16. Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás)

Az elektronikus információs rendszer a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosít, és ha egy elosztott, hierarchikus névtár részeként működik, akkor jelzi utódtartományok biztonsági állapotát is, és (ha azok támogatják a biztonságos feloldási szolgáltatásokat) hitelesíti az utód- és elődtartományok közötti bizalmi láncot.

3.3.13.17. Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív vagy gyorsító tárat használó feloldás)

Az elektronikus információs rendszer eredethitelesítést és adatsértetlenség ellenőrzést kér, és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra.

3.3.13.18. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

Azok az elektronikus információs rendszerek, amelyek együttesen biztosítanak név/cím feloldási szolgáltatást egy szervezet számára, hibatűrők és belső/külső szerepkör szétválasztást valósítanak meg.

3.3.13.19. Munkaszakasz hitelessége

Az elektronikus információs rendszer védje meg a munkaszakaszok hitelességét.

3.3.13.20. Hibát követő ismert állapot

Meghatározott hibatípusokhoz tartozó hibát követően az elektronikus információs rendszer a kijelölt, vagy utolsó ismert állapotba kerül, amely a hiba esetén is megőrzi a rendszerállapot információkat.

3.3.13.21. A maradvány információ védelme

Az elektronikus információs rendszer védi az érintett szervezet által meghatározott maradvány információk (pl.: átmeneti fájlok) bizalmasságát, sértetlenségét.

3.3.13.22. A folyamatok elkülönítése

Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.

TARTALOMJEGYZÉK