Útmutató a légiközlekedési védelmi terv kibervédelmi intézkedések végrehajtásához

Szakhatósági állásfoglalás

Verzió 1.1.

1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

Fortes fortuna adiuvat

NEMZETI KIBERBIZTONSÁGI INTÉZET

2026

Tartalomjegyzék

FOGALOMMAGYARÁZAT

adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől feltéve, hogy a technikai feladatot az adatokon végzik;

adatkezelés*:* az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése;

bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

elektronikus információs rendszer:[*]

a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy

c) az *a)* és *b)* pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

észlelés: a biztonsági esemény bekövetkezésének felismerése;

felhasználó: egy adott elektronikus információs rendszert igénybe vevők köre;

fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;

kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a

kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhezés működtetéséhez;

kibervédelem: a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;

kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

rendelkezésre állás*:* annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

sérülékenység: az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

sérülékenységvizsgálat: az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;*

szervezet: az adatkezelést végző, illetve az adatfeldolgozást végző vagy végeztető jogi személy vagy egyéni vállalkozó, valamint az üzemeltető;

üzletmenet-folytonosság: a szervezet azon képessége, hogy előre meghatározott, elfogadható szinten folytassa a tevékenységét vagy a szolgáltatását egy kárt okozó eseményt követően;

üzemeltető: az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer, vagy annak részei működtetését végzi és a működésért felelős;

védelmi feladatok: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;

ÚTMUTATÓ ALKALMAZÁSA

Jelen dokumentum két fő részből áll, a 0-0 fejeztek útmutató jelleggel írják le, hogy a polgári légiközlekedés védelmének szabályairól és a Légiközlekedés Védelmi Bizottság jogköréről, feladatairól és működésének rendjéről 169/2010. (V.11.) kormányrendelet (a továbbiakban: Rendelet) által elvárt feladatokat hogyan célszerű megvalósítania az érintett szervezeteknek. A dokumentum 0 fejezete pedig egy mintát tartalmaz azon kibervédelmi intézkedések megfogalmazására, amelyek ahhoz szükségesek, hogy a szervezet meg tudjon felelni a Rendelet elvárásainak.

A kibervédelmi intézkedések esetében nem kötelező a szervezetnek a megadott sablont használnia, de akkor a megadott mintához hasonló szerkezetben szükséges összefoglalnia az alkalmazott kibervédelmi intézkedéseit, hogy így igazolja az elvárt intézkedések teljesítését.

Amennyiben a szervezet a kibervédelmi intézkedéseit a megadott sablon használatával fogalmazza meg, akkor azt testre kell szabnia és az ott szereplő általános értékeket a saját maga által alkalmazott értékekkel kell feltöltenie. Ahol a sablon testre szabása, és valamilyen szervezetre specifikus információ megadása szükséges ott sárga kiemeléssel is megjelölésre került a szöveg. *(Például.: felsorolások esetében, ahol a segítségképpen megadott értékeket felül kell vizsgálni, a szükségteleneket törölni kell, az esetleg hiányzókkal pedig bővíteni kell a listát)*

Amennyiben a szervezet nem azonosít olyan elektronikus információs rendszert, amely a Rendelet 40/A. § hatálya alá tartozik, akkor erről nyilatkozatot kell készíteni, melyet a Légiközlekedési Védelmi Tervben egyértelműen szerepeltetni szükséges.

Amennyiben egy adott kontroll alkalmazása a szervezet esetében nem releváns, azt nem kell szerepeltetni a dokumentumban, az arra vonatozó részt törölni kell a sablonból, de dokumentálni szükséges, hogy azok miért nem relevánsak. Például, ha nem lehet mobil eszközökről hozzáférni a szervezet érintett rendszereihez, akkor a mobil eszközzel való hozzáférésre vonatkozó kontrollok törölhetőek.

FELKÉSZÜLÉSI TEVÉKENYSÉGEK

MIT ÉS HOGYAN?

Az alábbi fejezetek tartalmazzák azt, hogy mit és hogyan kell elvégezni a szervezetnek ahhoz, hogy a kibervédelmi intézkedései megfeleljenek a vonatkozó jogszabályi elvárásoknak.

KRITIKUS ELEKTRONIKUS INFORMÁCIÓK VAGY RENDSZEREK AZONOSÍTÁSA

A Rendelet 40/A. §-a szerint az alábbi elektronikus információk vagy rendszerek minősülnek kritikusnak:

- a meghatalmazott ügynökök, ismert szállítók, meghatalmazott beszállítók adatbázisa;
- az utasoktól különböző személyek által használt beléptető rendszerek beleértve az elektronikus kapukat és egyéb ajtókat, valamint a riasztó rendszerek;
- a kártyaleolvasók;
- az E-útlevél leolvasók;
- a kamerás megfigyelőrendszer;
- az utas és poggyász összeegyeztető rendszer;
- a védelmi átvizsgálásra használt rendszerek és robbanóanyag felderítő rendszerek;
- a repülőtéri azonosító kártya adatbázis, ideértve a foglalkoztatásra és a védelmi háttérellenőrzésre vonatkozó adatokat is;
- a személyek védelmi képzésére vonatkozó adatbázis.

A szervezetnek a Rendelet szerint meg kell vizsgálnia a fenti lista alapján, hogy milyen kritikusnak minősülő elektronikus információkat, illetve rendszereket használ.

A szervezetnek a Rendelet szerint el kell készítenie az általa kezelt kritikusnak minősülő elektronikus információk, illetve rendszerek nyilvántartását.

Amennyiben a szervezet a fent említett vizsgálat során nem azonosít olyan elektronikus információs rendszert, amelyre a 169/2010. (V.11.) kormányrendelet 40/A.§ vonatkozik, akkor erről nyilatkozatot kell készíteni, amelyet a Légiközlekedési Védelmi Tervben egyértelműen szerepeltetni szükséges.

KOCKÁZATOK, SEBEZHETŐSÉGEK FELTÁRÁSA

A szervezetnek fel kell mérnie a szervezetet érintő kiberfenyegetéseket és meg kell határozni azt, hogy azok mekkora kockázatot jelentenek a szervezet számára.
Az alábbi példák segítséget nyújtanak a szervezet számára, hogy azonosítani tudja azokat a sebezhetőségeket, amelyek veszélyeztethetik a szervezet, illetve az általa használt IT rendszerek működési biztonságát.

Gyengeségek az üzleti szempontból kritikus alkalmazásokban

Az alkalmazás gyengesége lehet, ha rossz minőségű a szoftver és/vagy ha azt nem a kellő szigorúsággal fejlesztették és tesztelték. Az információk és a rendszer elérhetőségével és integritásával kapcsolatos problémák gyakran megoldhatóak a légiforgalmi irányítás rendszerekre vonatkozó megfelelő biztonsági követelmények alkalmazásával. Az alkalmazások biztonságának gyengesége nem csak magát az alkalmazást érinti, hanem az alá- vagy fölérendelt rendszerek biztonságát is. Az alkalmazások sebezhetőségeit gyakran nem csak egy adott alkalmazáshoz való hozzáférés megtagadására lehet felhasználni, hanem a szélesebb értelemben vett rendszerhez vagy hálózathoz való hozzáféréshez is.

Gyengeségek az operációs és az üzleti szempontból kritikus rendszerekben

Az operációs rendszer létrehozásának költsége miatt a gyakorlatban korlátozottak a választható operációs rendszerek. A modern operációs rendszerek korlátozott számban jelennek meg, pl. Linux, Windows, Unix, OSX és Android. Az operációs rendszerek kulcsfontosságú szerepet töltenek be a vállalati működésben, ami megköveteli, hogy többféle képességgel is rendelkezzenek. Ez az összetettség nemcsak képességspecifikus kihasználható sebezhetőségeket eredményez, hanem nem szándékos tervezési hibákat vagy ütközéseket más rendszerekkel vagy alkalmazásokkal. Ez utóbbi jól látható a kiadott javítások számából és azok rendszerességéből.

Nem támogatott vagy nem karbantartott szoftverek

A kereskedelmi forgalomban kapható szoftverek gyengeségeit és sebezhetőségeit folyamatosan értékelik a szoftvergyártók, a felhasználók és a rosszszándékú szereplők is. Ha nem biztosítják, hogy a standard kereskedelmi forgalomban kapható (dobozos) szoftverekre támogatási

megállapodás és/vagy szigorú javítási eljárás vonatkozzon, akkor az az ismert sebezhetőségek kihasználásához vezethet. Ez különösen igaz az internetről elérhető régebbi rendszerekre.

Gyenge hozzáférés kontroll

A megfelelő hozzáférés-ellenőrzés hiánya növelheti annak valószínűségét, hogy illetéktelenek olyan erőforrásokhoz férnek hozzá, amelyeknek tiltottnak kellene lennie számukra. Ha egy szervezet nem korlátozza megfelelően, hogy ki férhet hozzá az információihoz és a tárgyi eszközeihez, akkor növeli mind a belső, mind a külső fenyegetéseknek való kitettségét. A bizalmas vagy üzleti szempontból kritikus elektronikus információk ellopása és jogosulatlan nyilvánosságra hozatala a nem megfelelő hozzáférés-ellenőrzés következtében károsíthatja a cég hírnevét, és pénzügyi kihatásokkal is járhat. A hozzáférés-ellenőrzés lehet fizikai és logikai is, azaz az épülethez való hozzáféréshez proximity kártyát igénylő beléptető pontok fizikai kontrollok, míg a vállalati címtáron (pl. Microsoft Active Directory-n) keresztül kezelt felhasználói fiókhoz kapcsolódó digitális hozzáférési jogok, logikai kontrollok. A szigorú hozzáférés-ellenőrzést a megfelelő jogosultságkezeléssel is kombinálni kell – hiába van hozzáférés-ellenőrzés, ha a felhasználó hozzáférést kérhet a rendszerhez, és megfelelő jóváhagyás nélkül kap hozzáférést, vagy ha a hozzáférést a jóváhagyás megerősítése előtt adják meg.

Gyenge változáskezelés

Ha nincs szervezeti folyamat a változáskezelésre, akkor az ellenőrizetlen változtatások működési zavarokat idézhetnek elő, illetve kitehetik a szervezetet a rendszer sérülékenységeinek.

Gyenge hálózati kontrollok

A legtöbb hálózati eszköz alapértelmezés szerint lehetővé teszi az adatokhoz való hozzáférést bármely felhasználó vagy rendszer számára, aki hozzá akar férni. Hatékony kontrollokat kell alkalmazni annak biztosítására, hogy csak azok a rendszerek/személyek hozzáférése legyen engedélyezve, akiknek jogos a hálózathoz való hozzáférési igénye. A gyenge hálózati kontrollok lehetnek belsők vagy külsők, ettől függetlenül a szervezetnek minden esetben gondoskodnia kell arról, hogy a határvédelmi kontrollok hatékonyak legyenek, és ne engedjenek illetéktelen hozzáférést a hálózathoz illetékteleneknek.

Gyenge felhőszolgáltatás és virtuális gép megvalósítás, illetve üzemeltetés

A felhőalapú számítástechnika és a virtuális gépek viszonylag új technológiai platformok a légiforgalmi irányítási környezetben. Ezen új technológiák használata növelheti a szervezet kitettségét a felmerülő kockázatoknak és fenyegetéseknek. A felhőalapú számítástechnika különösen növelheti a cég kitettségét, mivel harmadik féltől származó szolgáltatásra támaszkodik. Egy szervezet sebezhetővé válhat, ha például a felhőszolgáltatóját szolgáltatásmegtagadási (DOS) támadás éri.

Gyenge eszközkezelés

Az üzletmenethez szükséges eszközök lehetnek tárgyi eszközök (fizikai eszközök, például laptopok, szerverek stb.) és immateriális javak (digitálisan tárolt információk). Ha nem vezetnek leltárt az eszközökről, akkor a szervezet számára nehéz lesz nyomon követni eszközeit, és késedelmet szenvedhet abban, hogy a szervezet észreveszi, hogy elvesztette vagyonát, legyen szó fizikai vagy információs eszközökről. Továbbá, ha egy eszköznek az értékét, amit a szervezet számára képvisel, nem értékelik és rögzítik megfelelően, akkor az eszköz és közvetlen környezete védelmét szolgáló arányos kontrollok nem vezethetőek be.

Avulás

A meglévő hardver- és szoftvereszközök frissítése gyakran túl drágának tekinthető, mivel nem jár azonnali haszonnal a vállalkozás számára. Az elavult rendszerekre való támaszkodás azonban számos kockázatnak teheti ki a szervezetet, ami kiszolgáltatottá teheti az ezeket kihasználni óhajtó szereplőkkel szemben. Az elavult rendszerek nem rendelkeznek ugyanolyan szintű szolgáltatói támogatással, mint a napra kész rendszerek, ezért nem valószínű, hogy megtalálják és javítják a más szoftverekkel vagy hardverekkel való ütközésből adódó sebezhetőségeket.

Gyenge szoftverkontrollok

Az alapműködéshez kapcsolódó rendszer teljesítményét erősen befolyásolhatja, ha nem megfelelő szoftverek kerülnek telepítésre a szervezet adott környezetébe. Ha nincsenek olyan szabályok, amelyek korlátoznák a szoftverek alapműködéshez kapcsolódó rendszerek működési környezetébe történő telepítését, akkor bármely felhasználó bármit telepíthet az adott környezetbe. Ennek eredményeként rosszindulatú programok kerülhetnek a hálózatba, vagy

ronthatják az alapműködéshez kapcsolódó rendszer teljesítményét. Noha a sérülékenységek kezelése során az alapműködéshez kapcsolódó kulcsfontosságú rendszerekre kell helyezni a hangsúlyt, fontos annak biztosítása is, hogy a standard vállalati (pl. pénzügyi, HR, stb.) rendszerek se maradjanak sérülékenyek, mivel ezen rendszerek gyakran egy zónában működnek vannak a szervezet többi rendszerével, ha a hálózati szabályok nem elég szigorúak, pl. ha a hálózati tartományok nincsenek elválasztva, illetve elkülönítve egymástól.

Vészhelyzetben az alapműködéshez kapcsolódó szoftverre és az utolsó biztonsági mentésre van szükség ahhoz, hogy az alapműködéshez kapcsolódó szolgáltatásokat visszaállítsák a megszokott módon. A normál üzemi szolgáltatáshoz szükséges szoftverek biztonsági másolatait másik helyszínen kell tárolni, mert a normál működési helyszínen történt tűz vagy más előre nem látható esemény azok károsodását vagy elvesztését okozhatja.

A hatékony felügyelet *hiánya*

Ha nincs behatolásészlelő vagy fenyegetésfigyelő rendszer a hálózatban, akkor nem valószínű, hogy egy szervezet tudni fogja, hogy megtámadták, csak jóval az után, hogy ez megtörtént; és azt sem, hogy ez egy külső fenyegetés, amely kívülről próbál betörni a hálózatba, vagy egy bennfentes, aki olyan rendszerekhez próbál hozzáférni, amelyek használatára nem jogosult. Egy szervezet nem hagyatkozhat pusztán a hálózati felügyeletre, mivel nem azonosítható minden tevékenység vagy cselekvés, különösen egy motivált külső fenyegetés. Más védelmi felügyeleti kontrollokat kell alkalmazni, amelyek magukban foglalhatnak egy hatékony behatolásérzékelő rendszert.

A hatékony naplózás hiánya

Ha egy szervezet nem naplózza az összes rendszertevékenységet, akkor ez korlátozza a képességét arra vonatkozóan, hogy a műveletek és tevékenységek visszavezethetőek legyenek a rendszer felhasználóira egy biztonsági esemény esetén. A hatékony naplózási képesség olyan akár bűnügyi felderítési képességeket biztosít a szervezetnek, amelyek kritikus annak meghatározásához, hogy ki mit és mikor csinált, és elősegíti a hatékony válaszadást a biztonsági eseményekre. E képességek nélkül lényegesen nehezebb vagy akár lehetetlen egy-egy biztonsági események felfedezése.

A reagálási képesség hiánya

Ha egy szervezet nem rendelkezik valamilyen reagálási képességgel a (potenciális) biztonsági események kapcsán, akkor a beépített naplózási vagy felügyeleti kontrolloktól függetlenül sem tud a szükséges gyorsasággal és hatékonyan cselekedni.

A standard működésen túli képesség hiánya (mentések és üzletmenet-folytonosság)

A rendszer állandó rendelkezésre állása nem garantálható – egyetlen szervezet sem mentes a krízis- vagy katasztrófahelyzetektől. Ha egy szervezet nem rendelkezik alternatív működési képességekkel vagy üzletmenet-folytonossági tervekkel, legyen szó az alapműködéshez kapcsolódó rendszerekről, az emberekről vagy a létesítmény áramellátásáról, akkor magas szintű kockázatnak teszi ki magát. Az a szervezet, amely nem tud hatékonyan működni egy krízis- vagy katasztrófahelyzet, illetve egy biztonsági esemény során az alternatív működési képességek hiánya miatt, akkor jelentős anyagi, illetve a jó hírnevét érintő károkat szenvedhet.

A kiberbiztonsági képzés és tudatosság hiánya

Ha egy szervezet nem fektet be a munkatársak kiberbiztonsági képzésébe, akkor valószínűleg számos, a biztonsággal kapcsolatos problémától fog szenvedni. A gyenge kiberbiztonsági tudatosság következtében fellépő sebezhetőségek közé tartozik többek között a következő:

- a személyes biztonság hiánya az interneten (például a közösségi médiában), beleértve a szervezet biztonságát veszélyeztető adatok nyilvánosságra hozatalát is;
- az érzékeny információk nem megfelelő felhasználása;
- a kulcskártyák őrizetlenül hagyása;
- a laptopok/számítógépek lezárásának elmulasztása, ha azok felügyelet nélkül vannak;
- illetéktelen belépés figyelmen kívül hagyása, vagyis az, hogy valaki megfelelő engedély nélkül követ valakit („tailgating”) az épületbe.
- rosszindulatú szoftverek telepítése a szervezet rendszereire.

A megfelelő tudatossági képzés hiánya a munkavállalók kihasználásához vezethet a „social engineering” (pszichológiai manipuláció) révén, amely egy olyan technika, amelyet gyakran használnak arra, hogy számos médiumon keresztül információkat gyűjtsenek az emberekről és munkájukról. Ha az alkalmazottak ugyanazt a jelszót használják otthon, mint a munkahelyükön,

és nem tesznek megfelelő intézkedéseket személyes jelszavuk védelmére, akkor azonnal kiszolgáltatottá teszik a szervezetet is egy potenciális betöréssel szemben.

Biztonsági kontrollok a szállítói kapcsolatokban

Egy szolgáltató nagy valószínűséggel nem tekinti kiemelt fontosságúnak a légi szektorban érintett partnere biztonságát, hacsak nem kötelezi erre például egy szerződéses megállapodás. Sok esetben, ha egy szervezet nem fogalmazza meg kifejezetten a biztonsági követelményeit, előfordulhat, hogy a beszállítói diktálják vagy nagy mértékben befolyásolják az alkalmazott műszaki-biztonsági megvalósításokat. Gyakran előfordul, hogy egy szervezet több beszállítóval vagy harmadik féllel is kapcsolatban áll. Ennek eredményeképpen az információcsere-megoldások széles skálája lehet használatban, az átviteli mechanizmusok, a protokollok és az alkalmazott titkosítási szabványok széles skálájával. A szervezet felelőssége annak biztosítása, hogy beszállítói megfelelő biztonsági szinten legyenek; hogy következetes biztonsági kontrollokat alkalmazzanak; és végső soron, hogy ne legyen kiszolgáltatott a biztonság harmadik fél általi megsértésének.

Az üzleti szempontból kritikus adatok átvilágításának hiánya

Az adatok ki vannak téve a „minőségi romlásnak”, így fontos, hogy egy szervezet biztosítsa adatai és információi sértetlenségét. A szervezet adatait ellenőrizni kell a sértetlenség szempontjából, amikor azok bekerülnek valamelyik rendszerébe, illetve elhagyják azt. A „manipulált” adatok többféleképpen is hatással lehetnek egy szervezet működésére. Károsíthatja a szervezet hírnevét, és befolyásolhatja az ügyfélkör és a szolgáltatást igénybe vevők bizalmát; vagy károsíthatja a szervezet rendszereit, illetve valamilyen módon akadályozhatja/korlátozhatja a működését. A légiforgalmi szolgáltatással összefüggésben pl. egy sérült repülési terv "felfüggesztheti" a repülési adatfeldolgozó rendszert, ha azt nem vizsgálják át a feldolgozás előtt a sértetlenség szempontjából. Ez az úgynevezett "puffer túlcsordulás", ami egy olyan rendellenesség, amikor egy program, miközben adatokat ír egy memóriapufferbe, túllépi a puffer határát, és felülírja a szomszédos memóriaterületet is, ami a program hibás viselkedéséhez vagy akár a rendszer összeomlásához vezethet. A puffer túlcsordulás számos szoftveres sebezhetőség alapja, és rosszindulatúan kihasználható.

A rendszerórák nincsenek szinkronizálva egy referenciaidőhöz

Számos légügyi irányítási rendszer valós idejű környezetben működik, és a pontos időre támaszkodik. A létesítmények vagy rendszerek közötti szinkronizálás hiánya a következőket okozhatja: a szolgáltatások megszakadása, sérült információk és adatvesztés.

Környezeti és fizikai infrastruktúra fenyegetései

A rendszereket és létesítményeket úgy kell megtervezni, hogy hatékonyan működjenek abban a környezetben, amelyben üzembe helyezik őket. A telephely építése/elhelyezése során figyelembe kell venni az olyan állandó környezeti kockázatokat, mint a szél és az eső, de figyelembe kell venni az olyan kevésbé valószínű eseményeket is, mint az árvíz, a szélsőségesen magas hőmérséklet, valamint azt, hogy ez milyen hatással lehet a szolgáltatás működése szempontjából kritikus támogató szolgáltatásokra, például az áramellátásra és a telephelyhez való hozzáférésre.

Információs eszközök elvesztése

Az információs eszközök elvesztése vagy ellopása egyaránt összefügg a nem megfelelő hozzáférés-ellenőrzéssel és a kiberbiztonsági tudatosság hiányával. Ide tartoznak az ellopható, értékes adatokat tartalmazó eszközök, például egy őrizetlenül hagyott laptop. Olyan tárgyakat is ellophatnak, amelyek hatással lehetnek az operatív teljesítményre, például a kábelezés ellopása. Nem a fizikai veszteségről van szó, hanem a fizikai „hordozóhoz” eszközköz kapcsolódó információs eszköz elvesztéséről, illetve a működési teljesítményre és a szolgáltatásnyújtásra gyakorolt hatásról.

Berendezések selejtezése

A felesleges információs eszközök, mint például a régi merevlemezek, nyomtatók, útválasztók (router-ek) értékes szellemi tulajdont és más érzékeny információkat tartalmazhatnak, ha nincsenek biztonságosan megtisztítva. Az ilyen elemeket biztonságosan meg kell semmisíteni a fennmaradó adatok bizalmas kezelésének biztosítása érdekében.

Rádióalapú technológiák

Az interferencia ronthatja a rádióalapú technológiák, például a Wi-Fi hálózat, a radar, a rádió vagy a navigációs eszközök teljesítményét. Az ezen a technológián keresztül továbbított

információ is érzékeny lehet a lehallgatásra, ha a hálózat vagy az adat nincs megfelelően biztosítva, pl. titkosított Wi-Fi.

Hűtés, szellőzés és légkondicionálás

Az informatikai hardver tápellátási, páratartalomi és hőmérsékleti határértékekkel rendelkezik, és e határértékek megsértése hatással lesz a működési teljesítményére. A környezeti feltételeket biztosító rendszerek nem megfelelő karbantartása vagy egy szándékos támadás működésképtelenné teheti a hardvert, és ez megzavarhatja vagy leállíthatja a kapcsolódó szoftverrendszereket is, pl. a légkondicionálás kikapcsolása a szerverteremben a rack szekrények túlmelegedéséhez és a működő rendszer megzavarásához vezethet.

KOCKÁZATOK ELEMZÉSE

A szervezetnek meg kell fogalmaznia a kockázatok elemzésére, illetve a kockázatok kezelésére vonatkozó gyakorlatát, erre azért van szükség, hogy a szervezet felmérje az elektronikus információs rendszerét fenyegető kiberbiztonsági kockázatokat, és a kiberbiztonsági rendszerét a szervezetet érintő kockázatokkal arányosan alakíthassa ki.

A kockázatelemzés lefolytatására javasolt a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (a továbbiakban: NBSZ NKI) által rendelkezésre bocsátott kockázatelemzési módszertan használata, de a szervezet alkalmazhat másik módszertant is, amely alkalmas az elvárt eredmény biztosítására, vagyis a szervezetet fenyegető kiberbiztonsági kockázatok felmérésére. Az NBSZ NKI által rendelkezésre bocsátott módszertan a Civil Air Navigation Services Organisation (CANSO) Cyber Security and Risk Assessment Guide-jának adaptált változata.

A kockázatelemzés elvégzésére és kockázatkezelési tevékenység koordinálására javasolt a szervezetnek egy kockázatkezelési felelőst kijelölnie.

A kockázatkezelésért felelős személynek a választott módszertan alapján kell elvégeznie a kockázatelemzést, és az elemzés végrehajtását követően javaslatot kell tennie az egyes kockázatok felvállalására vagy kockázatcsökkentő lépések végrehajtására a menedzsment számára.

Az illetékes vezetők dönthetnek úgy, hogy nem fogadják el a kockázatkezelési javaslatot.(pl. a csökkenteni javasolt, de felvállalható kockázatok között lehet olyan, amelynél a kockázatcsökkentés költségei, ill. az egyéb erőforrások (pl. humán) meghaladják a szervezet adott tevékenységre racionálisan felhasználható erőforrásait.) Ebben az esetben a vezetőnek a fennmaradó kockázat felvállalásáról nyilatkoznia kell.

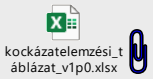
Amennyiben a menedzsment elfogadta a kockázatkezelési javaslatokat, akkor a kockázatkezelési felelős koordinálásával, egyéb személyek vagy szakterületek bevonásával akciótervet készít a szükséges intézkedések végrehajtására. Az akcióterv elkészítése, illetve a feladatok végrehajtása a kockázatkezelési felelős feladata. A kockázatkezelési felelősnek rendszeresen (legalább 3 havonta) tájékoztatnia kell az illetékes vezetőket a kockázatcsökkentő tevékenységek előre haladásáról és az esetleges fennakadásokról.

A kockázatelemzést rendszeresen felül kell vizsgálni, illetve ismételten le kell folytatni. Az iparági jó gyakorlat szerint legalább 2 évente, illetve amikor a szervezet elektronikus információs rendszerében jelentős változások történtek, felül kell vizsgálni azt.

A kockázatelemzés eredménye, illetve a kockázatcsökkentő intézkedések, továbbá a kapcsolódó akciótervek nem nyilvános dokumentumok, ahhoz csak az arra illetékesek férhetnek hozzá.

Módszertani segédlet a kockázatelemzéshez.

Az NBSZ NKI által rendelkezésre bocsátott módszertant az alábbi Excel táblázat tartalmazza:



A mellékelt Excel munkafüzet 3 munkalapot (Kockázatelemzés, Kockázatok számítása és Kockázatcsökkentő intézkedések) tartalmaz. Az első munkalap szolgál a kockázatelemzés elvégzésére, a második munkalap módszertani segédlet a kockázatok meghatározásához, a harmadik munkalap pedig a feltárt és kezelendő kockázatok, áttekintését hivatott segíteni.
Az első munkalap az alábbi módon épül fel:

- Az „A” oszlopa egy referencia érték, ami az egyes kockázatokra való hivatkozást teszi könnyebbé, egyszerűbbé.

- A „B” és „C” oszlopok a felmérendő kockázatok funkciónkénti (Azonosítás, Védekezés, Észlelés, Reagálás, Helyreállítás) és azon belül kategóriánkénti besorolását tartalmazzák.
- A „D” oszlop tartalmazza az értékelendő kockázat szöveges leírását.
- Az „E” oszlopba kell leírni azt, hogy a szervezet jelenleg milyen kontrollal rendelkezik az adott kockázat vonatkozásában.
- Az „F”, G” és „H” oszlopok szolgálnak az aktuális kockázati szint meghatározására, amelyhez a segítséget a 2. munkalap tartalmazza.
- Az „I” oszlopban kell rögzíteni a szervezet döntését a „H” oszlopban meghatározott kockázat kapcsán: felvállalja vagy kockázatcsökkentésre van szükség?
- Amennyiben a szervezet a kockázat csökkentését tartja szükségesnek, a kockázatcsökkentéshez szükséges új kontrollt a „J” oszlopban szükséges rögzíteni.
- Az új kontrollhoz kapcsolódóan el kell végezni a maradványkockázat számítását, amire a „K”, „L” és „M” oszlopok szolgálnak.

A második munkalap tartalmazza a kockázat meghatározásához használatos segédletet:

- A kockázat bekövetkezési valószínűségének meghatározására egy hatelemű skála szolgál, ahol az adott esemény potenciális bekövetkezési ideje (gyakorisága) alapján kell meghatározni az adott kockázathoz tartozó valószínűségi értéket.
- A kockázat bekövetkezéséhez tartozó következmény súlyosságának meghatározására egy ötfokozatú skála szolgál. A következmények számszerűsítésénél azt kell figyelembe venni, hogy az adott esemény bekövetkezése milyen súlyos hatást gyakorolhat a szervezet működésére, reputációjára, illetve pénzügyi helyzetére.
- A besorolási tábla szolgál a kockázat mértékének a meghatározásra a bekövetkezési valószínűség és a következmény súlyosságának függvényében.

A harmadik munkalapon lehet összegyűjteni a kezelendő (csökkentendő) kockázatok esetében a javasolt intézkedéseket, és itt lehet követni azok aktuális állapotát.

Üzletmenet-folytonosság tervezése

A szervezetnek meg kell határozni az üzletmenet folytonossága szempontjából releváns szolgáltatásokat és azokra ki kell dolgoznia az üzletmenet-folytonossági akcióterveket, amelyek segítségével biztosítani lehet az adott szolgáltatás esetében a minimálisan elvárt

szolgáltatást (alapfeladatok és alapfunkciók) a standard szolgáltatást biztosító rendszerelem(ek) kiesése esetén is.

Az adott szolgáltatás tekintetében meg kell határozni, hogy az adott szolgáltatás milyen időtartamú kiesése tolerálható a szervezet részéről és a vészhelyzeti működést, illetve a helyreállítási tevékenységet is ez alapján kell megtervezni.

A szervezetnek ki kell dolgoznia a lényeges szolgáltatásokra a standard működésre vonatkozó helyreállítási akcióterveket is. (Hogyan, milyen lépéseken keresztül (hibás eszköz javítása vagy cseréje, mentésből valóhelyreállítás, hiányzó adatok ismételt rögzítése, stb.) kerül helyreállításra a standard szolgáltatási szint, normál üzemi működés?)

A szervezetnek ki kell dolgoznia az üzletmenet-folytonosságra vonatkozó szervezeti működés szabályait. Meg kell határozni a vészhelyzeti működéshez szükséges szerepköröket és döntési kompetenciákat. (Ki vagy milyen testület dönthet a vészhelyzeti működésre történő átállásról, ill. a normál üzemi működésre történő visszatérésről? Az érintett szervezeti egységeknél ki kell nevezni a vészhelyzeti felelősöket, akik helyi szinten koordinálják a vészhelyzeti feladatokat.)

A szervezetnek ki kell jelölni azt a szervezeti egységet vagy felelős személyt, amely/aki elvégzi a folyamatos működést szolgáló információfeldolgozó, infokommunikációs és környezeti képességek biztosításához szükséges kapacitások megtervezését. (Pl. milyen tartalék eszközökre, redundáns kialakításra, szolgáltatási szerződésekre van szükség a folyamatos működés biztosításához.)

A szervezetnek ki kell dolgoznia a vészhelyzeti értesítési rendet, amely tartalmazza az érintettek összes szükséges/lehetséges elérhetőségét. (Pl. a hálózat kiesése esetén nagy valószínűséggel sem a levelező, sem a (z IP) telefon szolgáltatás nem lesz elérhető.)

A szervezetnek ki kell dolgoznia a vészhelyzeti működésre vonatkozó dokumentumok tárolási gyakorlatát is, és azt meg kell ismertetni minden érintettel. (Pl. a vonatkozó anyagok elsődleges tárolása hálózati meghajtón is történhet, ahol megfelelő jogosultságkontrollt alkalmaznak. Ezáltal a szakterületi anyagokat a szakterületi felelős tudja szerkeszteni, a szakterületi munkatársak csak olvasási hozzáféréssel rendelkeznek.)

A vészhelyzeti működéshez kapcsolódó anyagok esetében gondoskodni kell azok papír alapú elérhetőségéről is. A vonatkozó dokumentumokat célszerű a mentésekhez hasonlóan külső helyszínen is tárolni, hogy azok a telephely megsemmisülése esetén is rendelkezésre álljanak.

BIZTONSÁGI ESEMÉNYEK KEZELÉSE

A szervezetnek meg kell határoznia azt, hogy milyen potenciális forrásokból gyűjti a kiberbiztonsági eseményeket. (Pl. felügyeleti rendszer riasztásai, felhasználói bejelentések, az üzemeltetők által tapasztalt rendellenességek.)

A szervezetnek gondoskodnia kell arról, hogy minél hamarabb megtörténjen a kiberbiztonsági események észlelése, így meg lehessen kezdeni az események kivizsgálását, illetve a szükséges intézkedések megtételét. A felügyeleti rendszer riasztásainak kezelési rendjét ki kell alakítani. (pl. munkaidőn kívül is van ügyeletes, aki be tud avatkozni.)

A szervezetnek meg kell határozni, hogy milyen kiberbiztonsági események jelentését várja el a felhasználóktól.

Célszerű, ha a felhasználóknak minden a normál üzemi működéstől vagy a megszokott gyakorlattól eltérő eseményt jelenteniük kell az arra biztosított csatornák valamelyikén.

Potenciális bejelentési csatornák: e-mail, telefon, valamilyen ügykezelő (ticketing) rendszer.

A hatékony, kockázatarányos működés miatt a szervezetnek ki kell alakítania a biztonsági események minősítési rendszerét és az ehhez igazodó reagálási időket.

Az alábbi minta egy általános iránymutatás, hogy a szervezet a sajátosságaihoz igazodóan kialakíthassa a saját rendszerét, működését.

Az illetékes szakterületnek az esemény súlyosságának (bejelentésben vagy riasztásban szereplő minősítés) függvényében kell a vizsgálatok megkezdéséről vagy annak későbbi időpontra halasztásáról döntenie.

Minősítés	**Definíció**	**Reagálási idő**
Kiemelt	Kritikus IT erőforrások kiesése vagy súlyos működési zavara. A felhasználók legalább 10 százaléka vagy kiemelt jogosultsággal rendelkező felhasználó érintett.	Azonnal
Standard	Kritikus IT erőforrás nem súlyos működési zavara. Nem kritikus IT erőforrás kiesése vagy súlyos működési zavara. Kevesebb mint a felhasználók 10 százaléka érintett, és nincs köztük kiemelt jogosultsággal rendelkező felhasználó.	4 órán belül

Elhanyagolható / nem hiba	Az elektronikus információs rendszert vagy a rendszer elemeit érintő kisebb működési zavar. Kevesebb mint a felhasználók 5 százaléka érintett, és nincs köztük kiemelt jogosultsággal rendelkező felhasználó.	30 napon belül

A vizsgálat eredménye alapján születik döntés a további lépésekről:

- további vizsgálatra van szükség;
- a hiba a szervezeten belül javítható;
- a hiba eszkalációjára van szükség (támogató vagy gyártó);
- az üzletment-folytonossági vagy a katasztrófa utáni helyreállítási tervek aktiválása válik szükségessé.

Az illetékes szakterületnek gondoskodnia kell a hibajavításról vagy egy olyan megoldás (pl. kockázatos szolgáltatás leállítása, egyéb biztonsági paraméterek beállítása, stb.) implementálásáról, ami az adott szolgáltatás vagy rendszer esetében az eredetihez képest közel azonos biztonsági szintet biztosít.

Az elsődleges intézkedés után az illetékes szakterületnek meg kell vizsgálnia, hogy a szolgáltatás biztosításához alkalmazott megoldás végleges megoldásnak tekinthető-e, vagy további javítási tevékenységre van szükség az eredeti szolgáltatási szint, illetve működési mód helyreállításához. Amennyiben további javítási tevékenységre van szükség, akkor az illetékes szakterület feladata annak végrehajtása vagy külső szolgáltató bevonása erre vonatkozóan.

Az illetékes szakterületnek ki kell értékelnie az esemény okát és a javítás folyamatát, hogy annak tapasztalatai beépítésre kerüljenek az érintett folyamatokba. Amennyiben az elemzésben az kerül megállapításra, hogy a jelenlegi üzletmenet-folytonossági tervek nem alkalmasak az adott biztonsági eseményt követően az elvárt működési szint biztosítására, akkor az üzletmenet-folytonossági terveket aktualizálnia kell a felelős szakterületnek.

A szervezetnek minden biztonsági eseményt rögzítenie kell az arra rendszeresített rendszerben/regiszterben. (Nincs kötelezően előírt forma, lehet papír alapon, lehet valamilyen elektronikus formon, vagy akár erre rendszeresített ticketing rendszerben is. Javasolt a ticketing rendszer használata a könnyebb visszakereshetőség, illetve az elemzések és a visszamérés támogatása miatt.)

A szervezetnek meg kell határoznia a biztonsági események kapcsán minimálisan összegyűjtendő információkat.

Javasolt minimálisan az alábbi információkat összegyűjteni:

- a biztonsági esemény bekövetkezésének ideje;
- a biztonsági esemény megnevezése, leírása;
- a biztonsági esemény súlyossága (kategória);
- a biztonsági esemény bekövetkezésének helye (pontos fizikai vagy logikai hely);
- amennyiben lehetséges, akkor a biztonsági esemény okozójának azonosítása (név, felhasználói név, IP cím stb.).

A szervezetnek ki kell alakítani a mérés, illetve hatékonyságnövelés gyakorlatát is. A szükséges elemzést célszerű legalább 2 havonta elvégezni. Amennyiben az elemzésből az derül ki, hogy további kiberbiztonsági fejlesztésekre van szükség, akkor fejlesztési tervet javasolt készíteni és azt el kell juttatni az illetékes vezető(k)nek.

Alább pár példa a funkciót támogató mutatókra:

- Hány esemény került rögzítésre a tárgyidőszakban?
- Az események megoldásának átlagos átfutási ideje;
- Az események megoszlása (új igény, hiba, stb.)
- A hibák megoszlása súlyosság szerint.

MUNKAERŐVEL KAPCSOLATOS IT ELVÁRÁSOK MEGHATÁROZÁSA

A szervezetnek meg kell határoznia, hogy az egyes (a kritikus elektronikus információk vagy rendszerek kezelésében érintett) felhasználói csoportokkal szemben milyen IT kompetenciákra van szükség a munkaköri feladatok megfelelő szintű ellátásához.

A szükséges kompetenciákat az alábbi csoportok szerint célszerű meghatározni:

A standard felhasználókkal szembeni elvárások:

- általános felhasználói szintű ismeretek (fájlkezelés, internetes keresés, böngésző használata, levelezés, stb.);
- kliens oldali operációs rendszer (Windows X vagy valamilyen Linux disztribúció használata)
- MS Office vagy hasonló irodai programcsomag használat (dokumentum szerkesztés, táblázatkészítés, prezentáció készítés, stb.)

A kulcsfelhasználókkal (pl. adatgazdák) szembeni elvárások:

- a standard felhasználókkal szembeni elvárások;
- adatbázis kezelési ismeretek (pl. MS Access, különféle SQL disztribúciók (MS SQL, PostgreSQL), stb. ismerete).

IT üzemeltetőkkel szembeni elvárások:

- hálózati üzemeltetési ismeretek/tapasztalat;
- szerver- és kliensoldali operációs rendszerek (Microsft X verziók, adott Linux/UNIX disztribúciók) üzemeltetési tapasztalata;
- kibervédelmi eszközök üzemeltetési ismerete/tapasztalata (tűzfal, tartalomszűrő, IDS/IPS, vírusvédelmi rendszer);
- adatbázis üzemeltetési tapasztalat (pl. MS SQL, PostgreSQL, stb.);
- levelező rendszer (szerver és kliens) üzemeltetési tapasztalat.

A FELHASZNÁLÓK KIBERVÉDELMI TUDATOSSÁGI KÉPZÉSÉNEK TERVEZÉSE

A szervezet minden érintett szereplőjének (alkalmazott, kölcsönzött munkaerő vagy szerződéses partner), aki a kritikus elektronikus információk vagy rendszerek kezelésében részt vesz rendszeresen kibervédelmi tudatossági képzésben kell részesülnie.

A képzések ütemezése:

- A képzést legalább évente meg kell ismételni.
- Az új belépők estében a képzést a munkába állást követően 15 napon belül célszerű megtartani.
- Speciális, a munkakör betöltéséhez szükséges képzés esetében a képzést a kinevezéstől számított 5 munkanapon belül javasolt megtartani.
- Ha a helyzet (pl. új típusú kiberfenyegetések megjelenése) indokolja, akkor ad-hoc képzés megtartása is szükséges.

A képzés során az érintetteket arra kell felkészíteni, hogy milyen módon kell használni az érintett IT rendszereket, hogy a használat során ne növeljék egy esetleges kiberfenyegetés kockázatát, illetve védjék a szervezet adatvagyonának bizalmasságát és sértetlenségét.

Javasolt témák (az alábbi lista egy minta és nem tekinthető teljeskörűnek):

- a felhasználó azonosításával kapcsolatos eszközök (jelszavak, tokenek, belépő kártyák, stb.) használata;
- eszközök biztonságos használatának, ill. szállításának szabályai;
- hordozható adattárolók használata;
- kibertámadás gyanújának felismerése kezelése;
- üzletmenet-folytonossági esemény esetén szükséges teendők;
- személyes adatok kezelése;
- távmunka, ill. home office esetén követendő szabályok.

A szervezetnek fel kell mérnie, hogy kik a kibervédelmi tudatossági képzés érintettjei, (Személyek, adott szervezeti egységek munkavállalói, szerződéses munkavállalók stb.) és a létszám függvényében kell oktatási időpontokat szervezni. (minimum 2 alkalom javasolt)

A szervezetnek meg kell határoznia a képzés, illetve az esetleges számonkérés formáit. Jelenléti oktatás, valamilyen online kollaborációs platform, e-learning, videó. A képzés után célszerű valamilyen egyszerű számonkérést tartani, ahol egy rövid kérdőívet kell kitölteni. (pl. 10 feleletválasztós kérdés, ahol minimum 6 vagy 7 helyes válasz kell a megfelelt szinthez.)

A képzésről jelenléti nyilvántartást kell vezetni. Amennyiben számonkérés is történt, akkor az arról készült feljegyzéseket az adott képzéshez tartozó jelenléti nyilvántartással célszerű megőrizni.

Az új belépők képzését célszerű csoportosan megszervezni, de a képzés megtervezésekor figyelembe kell venni a képzés megtartására vonatkozó határidőt (belépéstől számított időtartam).

Az adott évi képzési tervet a szervezet illetékes vezetőjével kell jóváhagyatni. A terv végrehajtásáról, a képzés eredményeiről tájékoztatót kell készíteni és meg kell küldeni az illetékes vezetőnek.

JOGTISZTASÁGI ELVÁRÁSOK AZONOSÍTÁSA

A szervezet a tevékenysége során csak jogtiszta szoftvereket használhat, az engedélyezett licencszám mértékéig. Az esetleges túltelepítéseket meg kell előzni, illetve rendszeresen ellenőrizni kell annak teljesülését.

A szervezet csak olyan adatokat használhat fel a tevékenysége során, amelyek felhasználására megfelelő jogosultsággal rendelkezik.

A szervezetnek a kibervédelmi intézkedések között deklarálnia szükséges a jogtisztasági követelményt. Ahol lehetséges, ott preventív kontrollokat szükséges alkalmazni a követelmény teljesítéséhez, pl. szoftvertelepítést csak a szervezet arra felhatalmazott munkavállalói végezhetnek, és nem minden munkavállaló.

A jogtisztasági ellenőrzés keretében nem csak a szoftverek jogtisztaságát kell ellenőrizni, hanem azt is, hogy a szervezet által használt, illetve a szervezet eszközein tárolt adatok között nem lelhetőek-e fel olyan licenchez kötött állományok, amelyek használatához szükséges jogosultsággal nem rendelkezik a szervezet. (Pl. médiafájlok (audió és videó), e-könyvek, stb.)

A jogtisztasági ellenőrzés eredményeit jegyzőkönyvben kell rögzíteni, és azt a szervezet vezetőjének kell megküldeni.

Szabályozási rendszerrel kapcsolatos javaslatok

A jogszabályi elvárások értelmében az érintett szervezetnek ki kell alakítania a tevékenysége ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét és ezt a védelmi programban kell rögzítenie. Jelen fejezet a szabályozási struktúra kialakításához nyújt segítséget.

Szabályozási rendszer felépítése

Az alábbiakban egy olyan szabályozási struktúra került felvázolásra, amely képes kielégíteni a jogszabály által minimálisan elvárt követelményszintet, amellyel kialakítható a legfontosabb információbiztonsági folyamatok elvárt kontrollja.

Elvárt dokumentumok:

- A kibervédelmi intézkedések megfogalmazása (egy vagy több dokumentum);
- Információs vagyonelemek és az információfeldolgozó eszközök nyilvántartása;
- Kockázatelemzési és kockázatkezelési eljárásrend létrehozása;
- Az egyes munkakörök betöltéséhez szükséges informatikai ismeretek meghatározása;
- Képzési eljárásrend;
- Üzletmenet-folytonossági terv;
- Kiberbiztonsági eseménykezelési eljárás;

Abban az esetben, ha az alkalmazott szabályzati struktúra a fentiektől eltér, akkor javasolt annak a fenti struktúraelemekkel történő összerendelése.

A szervezet megteheti, hogy a kibervédelmi intézkedéseket egy komplex dokumentumban határozza meg, ill. az is lehetséges, hogy a kibervédelmi intézkedéseket egy dokumentumcsomagban (fő témakörönként külön-külön dokumentumban) definiálja. Ez utóbbi esetben a védelmi programban elégséges lehet az egyes dokumentumok pontos meghivatkozása, ill. azok tartalmának rövid, lényegre törő és ellentmondásoktól mentes bemutatása.

KIBERVÉDELMI INTÉZKEDÉSEK (JAVASLAT)

Kockázatelemzés és kockázatkezelés

A szervezet az alábbiak szerint fogalmazza meg a kockázatok elemzésére, illetve a kockázatok kezelésre vonatkozó gyakorlatát. *(Amennyiben a szabályok megfogalmazása külön dokumentumban történik, akkor azt elégséges csak hivatkozni, illetve röviden összefoglalni.)*

A szervezet gondoskodik a szervezetet fenyegető kiberbiztonsági kockázatok felméréséről, hogy a kiberbiztonsági rendszerét a szervezetet érintő kockázatokkal arányosan alakíthassa ki.

A kockázatelemzés lefolytatására a szervezet az NBSZ NKI által rendelkezésre bocsátott kockázatelemzési módszertant használja.

(A szervezet alkalmazhat másik módszertant is, de az alkalmazott módszertannak alkalmasnak kell lennie az elvárt eredmény biztosítására, vagyis a szervezetet fenyegető kiberbiztonsági kockázatok felmérésére.)

A kockázatelemzés elvégzését és a kockázatkezelési tevékenység koordinálását végző személyt vagy szerepkört a szervezet illetékes vezetője jelöli ki.

A <**kockázatkezelésért felelős személynek**> a módszertan alapján elvégzi a kockázatelemzést, és az elemzés végrehajtását követően javaslatot tesz az egyes kockázatok felvállalására vagy kockázatcsökkentő lépések végrehajtására.

Amennyiben az illetékes vezetők nem fogadják el a kockázatkezelési javaslatot, akkor az illetékes személynek módosítania kell a kockázatkezelési tervet a vezetői elvárások alapján.

A kockázatkezelési javaslatok elfogadását követően akciótervet kell készíteni a szükséges intézkedések végrehajtására. Az akcióterv elkészítése, illetve a feladatok végrehajtása a <**kockázatkezelésért felelős személy**> feladata. A <**kockázatkezelésért felelős személy**> <**meghatározott időközönként**> tájékoztatja az illetékes vezetőket a kockázatcsökkentő tevékenységek előre haladásáról, esetleges fennakadásokról.

A kockázatelemzés eredménye 2 évente, illetve amikor a szervezet elektronikus információs rendszerében jelentős változások történtek, felülvizsgálatra kerül

A kockázatkezeléssel kapcsolatos dokumentumokat (a kockázatelemzés eredménye, a felvállalt, illetve kezelendő kockázatok, továbbá a kapcsolódó intézkedési terv) a szervezet bizalmasan kezeli, ahhoz csak az illetékesek férhetnek hozzá.

Üzletmenet-folytonosság és helyreállítás

A szervezet az alábbiakban fogalmazza meg az üzletmenet-folytonosságának biztosítására, illetve egy esetleges katasztrófa utáni helyreállításra vonatkozó gyakorlatát. *(Amennyiben a szabályok megfogalmazása külön dokumentumban történik, akkor azt elégséges csak hivatkozni, illetve röviden összefoglalni.)*

A szervezet az alábbi szolgáltatásokat tekinti az üzletmenet folytonossága szempontjából lényeges szolgáltatásoknak

- szállítói nyilvántartás;
- beléptetési kontroll;
- a kártyaleolvasás;
- az E-útlevél leolvasás;
- a kamerás megfigyelés;
- az utas és poggyász összeegyeztetés;
- a védelmi átvizsgálás;
- a repülőtéri azonosító kártya információk;
- a személyek védelmi képzésére vonatkozó adatok.

(A fenti felsorolás csak egy minta, ami a jogszabály által érintett rendszereket/szolgáltatásokat tartalmazza, ebből csak azokat kell itt szerepeltetni, amelyeket a szervezet valójában használ.)

A fenti szolgáltatásokra üzletmenet-folytonossági akciótervek kerültek kidolgozásra. A tervek kidolgozása az arra kijelölt munkatársak *(központi, illetve szakterületi felelősök)* feladata. A központi, illetve szakterületi felelősök kijelölése az *(illetékes vezető(k))* feladata.

Az akciótervekben meghatározásra kerültek az egyes szolgáltatások esetében a szervezet által minimálisan elvárt szolgáltatások a standard szolgáltatást biztosító rendszerelem(ek) kiesése esetére. Az akciótervek kidolgozását megelőzően meghatározásra került, hogy az adott szolgáltatás milyen időtartamú kiesése tolerálható a szervezet részéről és a vészhelyzeti működés, illetve a helyreállítási tevékenység is ez alapján került megtervezésre. A helyreállítási

tevékenységek kapcsán meghatározásra kerültek az egyes tevékenységek helyreállítási prioritásai is és amennyiben egy időszakban több tevékenység helyreállítása szükséges, akkor a helyreállítást a korábban megállapított prioritások szerint kell végrehajtani.

A szervezet a vészhelyzeti működés esetére krízis irányító bizottságot (KIB) állít fel, amelynek tagjai <**itt meghatározandó, pl. központi felelős, ill. az illetékes vezetők**>. Az üzletmenet-folytonossági tervekben megfogalmazott működésre való áttérést, illetve a standard üzemi működésére való visszatérést a KIB rendelheti el. A szakterületi feladatok koordinálását a helyi üzletmenet-folytonossági felelősök végzik.

A vészhelyzeti működéssel kapcsolatosan a szervezet nyilvántartást vezet az érintett személyek elérhetőségéről. A nyilvántartás a többi az üzletmenet-folytonossági tevékenységhez kapcsolódó dokumentummal azonos módon kerül tárolásra / érhető el. A nyilvántartás az alábbi adatokat tartalmazza:

- Érintett neve;
- Szervezeti egysége;
- Szerepköre az üzletmenet-folytonossági tevékenységben;
- Elérhetőségei: telefonszám (vezetékes és mobil) és e-mailcím.

(A fenti felsorolás csak egy minta, ott azokat az adatokat kell felsorolni, amelyeket a szervezet valójában használ.)

A szervezet az a <**fájlszerver vagy intranet pontos helye megadása**> teszi közzé. Az érintett anyagok elérhetőségéről az illetékeseket tájékoztatni kell, a tájékoztatás üzletmenet-folytonossági felelős(ök) (központi, illetve szakterületi) feladata. A szervezet az alábbi jogosultságkontrollt alkalmazza az érintett anyagok kapcsán:

- A központi felelős az összes anyagot tudja szerkeszteni, az illetékes vezetők pedig olvasási joggal érhetik el azokat.
- A szakterületi anyagokat a szakterületi felelős tudja szerkeszteni, és a szakterületi munkatársak csak olvasni tudják.

(A fenti felsorolás csak egy minta, ott a szervezet valós működését kell leírni.)

Az üzletmenet-folytonosság biztosításához kapcsolódó dokumentumok esetében a szervezet gondoskodik azok papír alapú elérhetőségéről is, arra az esetre, ha az elektronikus információs rendszerben nem érhetőek el a dokumentumok. A szervezet a papír alapú dokumentumok elérhetőségét az alábbiak szerint határozza meg:

- A központi felelősnél a teljes dokumentáció elérhető.
- A szakterületi anyagok a szakterületi felelősnél találhatóak meg.

(A fenti felsorolás csak egy minta, ott a szervezet valós működését kell leírni.)

A papír alapú dokumentumok estében is gondoskodni kell azok biztonságos tárolásáról, a biztonságos tárolás (zárt iratszekrény vagy széf) a dokumentumot őrző személy feladata.

A szervezet gondoskodik az érintett dokumentumok külső helyszínen történő tárolásáról is arra az esetre, ha a telephely megsemmisülne. <**Külső tárolási mód leírása**> A szervezet a külső helyszínen való tárolás esetében is gondoskodik a dokumentumok hozzáférés kontrolljáról, azokat csak az illetékesek (központi, ill. szakterületi felelősök) érhetik el.

(Ha nincs másodlagos tárolási helyszín, akkor a fenti rész törlendő.)

(Kiberbiztonsági) eseménykezelés

A szervezet az alábbiakban fogalmazza meg a kiberbiztonsági események kezelésre vonatkozó gyakorlatát. **Amennyiben a szabályok megfogalmazása külön dokumentumban történik, akkor azt elégséges csak hivatkozni, illetve röviden összefoglalni.**

A szervezet az alábbi forrásokból gyűjti a kiberbiztonsági eseményeket:

- felügyeleti rendszer riasztásai,
- felhasználó bejelentések,
- az üzemeltetők által tapasztalt rendellenességek.

(A fenti felsorolás csak egy minta, ott azokat a forrásokat kell alkalmazni, amit a szervezet valójában használ.)

A szervezet célja, hogy minél hamarabb megtörténjen a kiberbiztonsági események észlelése, az események kivizsgálása, illetve a szükséges intézkedések megtétele. A mihamarabbi észlelés miatt a szervezet:

- felügyeleti rendszert alkalmaz;
- elemzi a biztonsági naplókat;
- segélyszolgálatot tart fenn.

(A fenti felsorolás egy minta, ott csak azokat a megoldásokat kell szerepeltetni, amelyeket a szervezet valóban alkalmaz.)

A felügyeleti rendszer riasztásainak kezelésére a szervezet ügyeleti rendszert alkalmaz, hogy munkaidőn kívül is legyen olyan illetékes személy, aki be tud avatkozni.

(A fenti felsorolás egy minta, itt azt a megoldást kell leírni, amelyeket a szervezet valóban alkalmaz. Ha nincs felügyeleti rendszer, akkor a fenti szakasz törlendő.)

A szervezet a felhasználói bejelentések kezelésére segélyszolgálatot (Helpdesk) üzemeltet, amely az alább meghatározott csatornákon és működési időben érhető el:

- Telefonon: <**telefonszám, „nyitvatartás” megadása**>
- E-mail: <**e-mail cím, „válaszadási időszak”, pl. standard munkaidőben megadása**>
- Elektronikus bejelentő felület: <**elérhetőség, „válaszadási időszak”, pl. standard munkaidőben megadása**>

(A fenti felsorolás egy minta, ott csak azokat a csatornákat kell szerepeltetni, amelyeket a szervezet valóban alkalmaz.)

A biztonsági eseményekkel kapcsolatos naplóelemzést a szervezet a standard naplóelemzési gyakorlat szerint végzi.

A szervezet nem különít el jelentésköteles, illetve nem szükségszerűen jelentendő eseményeket, a felhasználóknak minden a normál üzemi működéstől vagy a megszokott gyakorlattól eltérő eseményt jelenteniük kell az arra biztosított csatornák valamelyikén.

A hatékony, kockázatarányos működés miatt a szervezet az alábbi minősítési rendszert, illetve a minősítéshez igazodó reagálási időket alkalmazza az elektronikus információs rendszerében észlelt biztonsági események kapcsán.

(Az alábbi minta egy általános iránymutatás, hogy a szervezet a sajátosságaihoz igazodóan alakíthassa ki a saját rendszerét, működését.)

Minősítés	Definíció	Reagálási idő
Kiemelt	Kritikus IT erőforrások kiesése vagy súlyos működési zavara A felhasználók legalább 10 százaléka vagy kiemelt jogosultsággal rendelkező felhasználó érintett	Azonnal
Standard	Kritikus IT erőforrás nem súlyos működési zavara Nem kritikus IT erőforrás kiesése vagy súlyos működési zavara Kevesebb mint a felhasználók 10 százaléka érintett, és nincs köztük kiemelt jogosultsággal rendelkező felhasználó	4 órán belül
Elhanyagolható / nem hiba	Az elektronikus információs rendszert vagy a rendszer elemeit érintő kisebb működési zavar. Kevesebb mint a felhasználók 5 százaléka érintett, és nincs köztük kiemelt jogosultsággal rendelkező felhasználó	30 napon belül

Az illetékes szakterületnek az esemény súlyosságának (bejelentésben vagy riasztásban szereplő minősítés) függvényében kell a vizsgálatok megkezdéséről vagy annak későbbi időpontra halasztásáról döntenie.

Az illetékes szakterület a vizsgálat eredménye alapján hoz döntés a lehetséges további lépésekről:

- további vizsgálatra van szükség;
- a hiba a szervezeten belül javítható;
- a hiba eszkalációjára van szükség (támogató vagy gyártó);
- az üzletment-folytonossági vagy a katasztrófa utáni helyreállítási tervek aktiválása válik szükségessé.

Az illetékes szakterület gondoskodik a hibajavításról vagy egy olyan megoldás (pl. kockázatos szolgáltatás leállítása, egyéb biztonsági paraméterek beállítása, stb.) implementálásáról, ami az

adott szolgáltatás vagy rendszer esetében az eredetihez képest közel azonos biztonsági szintet biztosít.

Az elsődleges intézkedés után az illetékes szakterület megvizsgálja, hogy a szolgáltatás biztosításához alkalmazott megoldás végleges megoldásnak tekinthető-e, vagy további javítási tevékenységre van szükség az eredeti szolgáltatási szint, illetve működési mód helyreállításához. Amennyiben további javítási tevékenységre van szükség, akkor az illetékes szakterület feladata annak végrehajtása vagy külső szolgáltató bevonása erre vonatkozóan.

Az illetékes szakterületnek kiértékeli az esemény okát és a javítás folyamatát, hogy annak tapasztalatai beépítésre kerüljenek az érintett folyamatokba.

A szervezet elektronikus információs rendszerével kapcsolatosan minden biztonsági eseményt rögzíteni kell <**a meghatározott rendszerben/regiszterben**> A szervezet a biztonsági események kapcsán minimálisan az alábbi információk összegyűjtését várja el:

- a biztonsági esemény bekövetkezésének ideje,
- a biztonsági esemény megnevezése, leírása,
- a biztonsági esemény súlyossága (kategória),
- a biztonsági esemény bekövetkezésének helye (pontos fizikai vagy logikai hely),
- amennyiben lehetséges, akkor a biztonsági esemény okozójának azonosítása (név, felhasználói név, IP cím stb.).)

(Ez egy minta a szervezet rendelkezhet másként is, fent a saját elvárásait kell rögzíteni.)

A szervezet eseménykezelési tevékenységének hatékonyságával kapcsolatosan <**meghatározott időközönként**> el kell végezni a szükséges visszaméréseket, hogy biztosított legyen az eseménykezelés hatékony működése. A visszamérés elvégzése az illetékes vezető által kijelölt személy feladata. A mérés eredményeiről tájékoztatni kell az illetékes vezetőt.

Amennyiben az elemzésből az derül ki, hogy további kiberbiztonsági fejlesztésekre van szükség, akkor arra fejlesztési tervet kell készíteni és azt el kell juttatni az illetékes vezető(k)nek. A fejlesztési terv elkészítése a kibervédelmi tevékenységért felelős személy feladata.

A munkaerővel kapcsolatos IT elvárások

A szervezet az alábbiak szerint fogalmazza meg az elektronikus információs rendszerhez jogosultsággal rendelkező munkavállalóival szemben támasztott IT elvárásokat. Amennyiben a szabályok megfogalmazása külön dokumentumban történik, akkor azt elégséges csak hivatkozni, illetve röviden összefoglalni.

<Itt részletesen meg kell határozni az elvárásokat a 0 fejezetben található minta alapján.>

A munkavállalókkal szembeni IT elvárások teljesítésének ellenőrzését az új munkavállalók esetében a felvételi folyamat során kell megvizsgálni. A meglévő munkavállalók esetében az elvárások megfogalmazását vagy frissítését követően <**meghatározott idő**> végre kell hajtani. Az ellenőrzések végrehajtása a szervezet illetékes vezetője által kijelölt személy feladat. Az ellenőrzés eredményéről jegyzőkönyvet kell készíteni.

A szervezet az esetlegesen hiányzó kompetenciák pótlására megállapodást köt az érintett munkavállalóval. A megállapodásban kell rögzíteni, hogy a munkavállalónak mennyi időn belül kell pótolni az adott kompetenciát, illetve ahhoz a szervezet milyen módon és milyen feltételek mellett nyújt támogatást

A szervezet a munkavállalókkal szemben támasztott IT elvárásait legalább <**megadott időszak**> felülvizsgálja. A felülvizsgálat elvégzésére a szervezet illetékes vezetője felelőst nevez ki. A felelősnek a felülvizsgálat eredményéről jegyzőkönyvet kell készítenie, amelyet megküld az illetékes vezetőnek.

Tudatosság és képzés

A szervezet az alábbiak szerint fogalmazza meg a kibervédelmi tudatosságára és képzésre vonatkozó gyakorlatát. *(A kibervédelmi tudatosságára és képzésre vonatkozó szabályokat lehet jelen, illetve külön dokumentumban is kezelni. Amennyiben a szabályok megfogalmazása külön dokumentumban történik, akkor azt jelen eljárásrendben elégséges csak hivatkozni, illetve röviden összefoglalni.)*

A szervezet minden érintett szereplőjének (alkalmazott, kölcsönzött munkaerő vagy szerződéses partner), aki a kritikus információk vagy rendszerek kezelésében részt vesz rendszeresen kibervédelmi tudatossági képzésben vesz részt.

A kibervédelmi tudatossági képzést legalább évente megismétlésre kerül. Az új belépők estében a képzést a munkába állást követően <meghatározott időtartam> belül meg kell tartani. A speciális, egy adott munkakör betöltéséhez szükséges kiegészítő képzést a kinevezéstől számított <meghatározott időtartam> belül meg kell kapnia az érintettnek. Ha a helyzet (pl. új típusú kiberfenyegetések megjelenése) indokolja, akkor ad-hoc, az éves képzési terven felüli képzést kell tartani az érintetteknek.

A képzés során az érintetteket arra kell felkészíteni, hogy hogyan kell úgy használni a szervezet elektronikus információs rendszerét, hogy a használat során ne növeljék egy esetleges kiberfenyegetés kockázatát, illetve védjék a szervezet adatvagyonának bizalmasságát és sértetlenségét.

A szervezet illetékes vezetője a képzések megtervezésére, ill. lebonyolítására felelőst nevez ki. A felelősnek meg kell határoznia a képzések tematikáját, továbbá a képzés, illetve az esetleges számonkérés módját. A felelősnek a képzések megtartására ütemtervet kell készítenie, amelyet az illetékes vezetőnek jóvá kell hagynia.

A képzésekről jelenléti nyilvántartást kell vezetni, amit legalább <meghatározott ideig> meg kell őrizni. Amennyiben számonkérés is történt, akkor az arról készült feljegyzéseket az adott képzéshez tartozó jelenléti nyilvántartással együtt kell megőrizni.

Információs vagyonelemek és információfeldolgozó eszközök nyilvántartása

A szervezet az alábbiak szerint fogalmazza meg a vagyonelemei és információfeldolgozó eszközei nyilvántartására vonatkozó gyakorlatát.

A nyilvántartásnak tartalmaznia kell minden a szervezet elektronikus információs rendszerének részét képező információs vagyonelemet és információfeldolgozó eszközt. A nyilvántartásnak pontosan tükröznie kell az elektronikus információs rendszer aktuális állapotát, tartalmaznia kell minden az elektronikus információs rendszer hatókörébe eső hardver- és szoftverelemet, továbbá kellően részletesnek kell lennie ahhoz, hogy a vagyonelemek egyértelműen beazonosíthatóak legyek.

A nyilvántartást minden olyan esetben frissíteni szükséges, amikor az elektronikus információs rendszer részét képező információs vagyonelem vagy információfeldolgozó eszköz telepítésére, eltávolítására vagy frissítésére kerül sor.

A nyilvántartást <**meghatározott időnként**> felül kell vizsgálni. A felülvizsgálat az illetékes vezető által kijelölt személy feladata, akinek jelentést kell készítenie az illetékes vezető számára az ellenőrzés eseményéről.

Jogtisztasági elvárások

A szervezet az alábbiak szerint fogalmazhatja meg az elektronikus információs rendszerében használt szoftverekkel és kezelt dokumentációkkal kapcsolatos, jogtisztasági követelmények biztosítására vonatkozó gyakorlatát. *(Amennyiben a szabályok megfogalmazása külön dokumentumban történik, akkor azt elégséges csak hivatkozni, és röviden összefoglalni.)*

A szervezet az elektronikus információs rendszerében csak jogtiszta szoftvereket használ, az engedélyezett licencszám mértékéig.

A szervezet a tevékenysége során csak olyan adatokat és dokumentációkat használ, amelyek felhasználására megfelelő jogosultsággal rendelkezik.

A szervezet lehetőség szerint preventív kontrollt alkalmaz a jogtisztaság biztosításához, szoftvertelepítést csak a szervezet arra felhatalmazott munkavállalói végezhetnek.

A szervezet <**megadott időszakonként**> ellenőrzi a jogtisztasági szabályok betartását. Az ellenőrzés elvégzésére a szervezet illetékes vezetője a <**személy vagy szerepkör**> jelöli ki. A <**megadott időszakonként**> végrehajtott ellenőrzés keretében nem csak a szoftverek jogtisztasága kerül ellenőrzésre, hanem a szervezet által használt, illetve a szervezet eszközein tárolt adatok is. A szervezet tiltja olyan licenchez kötött állományok (pl. médiafájlok vagy e-könyvek) tárolását, illetve megosztását, amelyek használatához a szükséges jogosultságokkal a szervezet nem rendelkezik.

A jogtisztasági ellenőrzés eredményeit a <**kijelölt személynek**> jegyzőkönyvben kell rögzíteni, és azt a szervezet illetékes vezetőjének kell megküldenie.

Azonosítás és hitelesítés

A szervezet az alábbiak szerint fogalmazhatja meg az elektronikus információs rendszeréhez kapcsolódó azonosítási és hitelesítési gyakorlatát. *(Amennyiben a szabályok megfogalmazása külön dokumentumban történik, akkor azt elégséges csak hivatkozni, és röviden összefoglalni.)*

A szervezet egyedileg azonosítja a felhasználókat az elektronikus információs rendszerben. A közös használatú azonosítók használata tilos.

A szervezet az elektronikus információs rendszerhez való hozzáférés tekintetében többtényezős hitelesítést alkalmaz a <**meghatározott, de minimum a privilegizált**> felhasználói fiókok esetében.

A szervezet elektronikus információs rendszereiben <**a szerepkör megadása, pl. IT üzemeltetők**> végezhetik az egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését.

A szervezet nem engedélyezi a felhasználói fiókok ismételt felhasználását, kivéve azt az esetet, ha ugyanaz a fizikai személy tér vissza a szervezethez.

A szervezet meghatározott időtartamú inaktivitás <**időszak megadása**> után letiltja az érintett felhasználói fiókokat. A letiltás az illetékes rendszerüzemeltető feladata, amennyiben a letiltás nem történik meg automatikusan a rendszerben. A letiltott fiókokról tájékoztatót kell készíteni az illetékes vezető(k) számára.

A szervezet elektronikus információs rendszeréhez hozzáférést biztosító hitelesítésre szolgáló eszköz (jelszó vagy egyéb eszköz) átadási folyamata az alábbiak szerint történhet:

? <ide kell leírni a részletes követelményeket
? **Kinek kerül átadásra?** A felhasználó vagy pl. a felettese?
? **Hogyan történik meg az átvevő azonosítása?**
? **Fizikai vagy elektronikus formában történik?**
? **Milyen csatornán?** (Pl. email, SMS, fizikai boríték?)>

A szervezet elektronikus információs rendszeréhez hozzáférést biztosító hitelesítő eszközök kezdeti tartalmának beállítására/megadására az alábbiak szerint kerül sor:

- <a fiók létrehozója **állít be egy generált jelszót**;
- a felhasználó maga tudja beállítani az erre szolgáló felületen.>

A hitelesítésre szolgáló eszköz létrehozásával párhuzamosan az illetékes üzemeltetőnek a megfelelő jogosultságokat is hozzárendeli a hitelesítő eszközhöz.

A szervezet elvárja a hitelesítésre szolgáló eszközökön végzett műveletek (kiosztás, visszavonás, csere, stb.) dokumentálását. A dokumentálás során rögzíti az igénylőt, a jóváhagyót és a végrehajtót is, illetve az egyes műveletek végrehajtásának idejét.

A szervezet elektronikus információs rendszerének vagy rendszerelemeinek telepítése során meg kell változtatni a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékeit. A szervezet szintén megköveteli a hitelesítő eszközök első használatukkor történő megváltoztatását, amennyiben az induló érték nem a fiók tulajdonosa által került beállításra.

A szervezetnek a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit az alábbiak szerint határozza meg:

- A jelszavak esetében a minimális élettartam <**megadott időszak**>.
- A jelszavak esetében a maximális élettartam <**megadott időszak**>.
- Az ismételt felhasználás <**megadott számú**> ciklus után lehetséges.
- A hitelesítésre használt tanúsítványos esetében a maximális használati idő <**megadott időszak**>.

A szervezet megköveteli, hogy a hitelesítésre szolgáló eszköztípusokra <**meghatározott időnként**> megtörténjen a hitelesítésre szolgáló eszközök megváltoztatása vagy frissítése.

A szervezet elektronikus információs rendszerében gondoskodni kell a hitelesítésre szolgáló eszközök tartalmának védelméről a jogosulatlan felfedéssel és módosítással szemben. A jelszavak esetleges továbbítás során sem kerülhetnek felfedésre. A jelszavak továbbítása csak kriptográfiailag védett csatornán keresztül történhet.

A szervezet megköveteli a felhasználóitól, hogy védjék hitelesítésre szolgáló eszközeik bizalmasságát és sértetlenségét. Tilos a jelszavak megosztása másik felhasználóval, illetve azok nem kellően védett formában való tárolása.

A szervezet megköveteli a közös használatú azonosítókhoz tartozó hitelesítő eszköz lecserélését, amennyiben az adott fiókot használó csoport tagságában változás történt (egy vagy több tag távozott).

A szervezet megköveteli, hogy az elektronikus információs rendszer fedett visszacsatolást biztosítson a hitelesítési folyamat során, ezzel megvédve a hitelesítési információt a jogosulatlan személyek számára történő esetleges felfedésétől.

A szervezet megköveteli, hogy az elektronikus információs rendszerben a hitelesítés során csak olyan szabványos kriptográfiai megoldások használhatóak, amelyek megfelelnek a vonatkozó jogszabályi előírásoknak is.

A szervezet az elektronikus információs rendszer szervezeten kívüli felhasználói esetében is megkövetelheti a felhasználók egyedi azonosítását és hitelesítését.

Hozzáférés-ellenőrzés

A szervezet az alábbiak szerint fogalmazza meg az elektronikus információs rendszerhez kapcsolódó hozzáférés-ellenőrzés gyakorlatát. *(Amennyiben a szabályok megfogalmazása külön dokumentumban történik, akkor azt elégséges csak hivatkozni, illetve röviden összefoglalni.)*

A szervezetnek elektronikus információs rendszerében az alábbi fióktípusok vannak használatban:

- standard felhasználói fiókok,
- kulcsfelhasználók,
- adminisztrátorok/rendszergazdák

A szervezet a fiókkezelési tevékenységre, vagyis a felhasználói fiókokhoz kapcsolódó műveletek végzésére a <**a megadott szerepkört**> jelöli ki.

A szervezet elektronikus információs rendszerében kialakított csoportok és szerepkörök tagsági feltételei az alábbiakban kerülnek részletezésre:

<Csoport/szerepkör a rendszerben és a hozzá tartozó tagsági feltétel>

Az adott csoport vagy szerepkör felhasználói az alábbi jogosultságokkal rendelkeznek:

<Csoport/szerepkör és a hozzá tartozó jogosultság (pl. írás, olvasás, végrehajtás, stb.)>

A szervezet elektronikus információs rendszerében a felhasználói fiókok, illetve a hozzá tartozó jogosultságok létrehozása, engedélyezése, módosítása, letiltása és eltávolítása az alábbi folyamaton keresztül történhet:

<**Folyamat leírása**>

A szervezet a felhasználói fiókok használatának ellenőrzését a felhasználói fiókokkal végzett tevékenységek naplózásán és a naplóbejegyzések elemzésén keresztül valósítja meg.

A szervezet előírja, hogy amennyiben egy adott felhasználói fiókra már nincs szükség, mert az adott felhasználó kilépett, más munkakörbe került vagy az adott munkakörhöz tartozó feladatok elvégzéséhez már nincs szükség az adott jogosultságokra, akkor a fiókkezelő kerüljön értesítésre a <**szervezet által meghatározott csatornán keresztül**>. A fiókkezelő értesítése az érintett felhasználó felettesének (munkáltatói jogok gyakorlójának) a feladata.

A szervezet elektronikus információs rendszerében <meghatározott időközönként> felül kell vizsgálnia a felhasználói fiókokat. A szervezet az inaktív, <**megadott ideje nem használt**> fiókokat letiltja. A felhasználói fiókok ellenőrzéséről, illetve az inaktív fiókok letiltásáról jegyzőkönyvet kell készíteni. Az ellenőrzés elvégzése az adott rendszer üzemeltetői, ill. üzleti oldali felelősének a feladata.

A közös használatú (megosztott vagy csoporthoz rendelt) felhasználói fiókok esetében a fiókhoz tartozó jelszót meg kell változtatni, amennyiben az adott fiók felhasználói köre megváltozott.

A szervezet elektronikus információs rendszere a benne tárolt adatokhoz, illetve a rendszer forrásaihoz való logikai hozzáférés során a szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat, és a rendszerhez csak ezen szabályok betartása mellett lehet hozzáférni.

A szervezet az egymást követő <**meghatározott számú**> sikertelen bejelentkezési kísérletet követően az adott fiókot <**letiltja vagy megadott időre felfüggeszti**>

A szervezet az elektronikus információs rendszerében nem engedélyez azonosítás és hitelesítés nélküli tevékenységet.

A szervezet elektronikus információs rendszeréhez való távoli hozzáférés biztosítása során az alábbi szabályokat kell betartani:

- A hozzáférés csak a szervezet által üzemeltetett virtuális magánhálózaton (VPN) keresztül lehetséges.

- A felhasználói hozzáféréshez egyedi, tanúsítványalapú hitelesítését kell alkalmazni.
- A felhasználók számára a VPN hozzáférés csak, akkor biztosítható, ha az illetékesek jóváhagyták az adott felhasználó VPN hozzáférésre vonatkozó igényét.

(Amennyiben nincs távoli hozzáférés, akkor a fentiek helyett azt kell leírni.)

A szervezet elektronikus információs rendszeréhez vezeték nélküli (Wi-Fi) hálózaton keresztül az alábbi szabályok szerint lehet hozzáférni:

- A vezeték nélküli hálózaton keresztüli hozzáféréshez a felhasználók egyedi azonosítását biztosító megoldást kell alkalmazni.
- A Wi-Fi hálózat esetében minimum WPA2 biztonsági protokoll alkalmazása az elvárt.
- Csak a szervezet által engedélyezett eszközökkel lehetséges a hálózathoz való hozzáférés.
- A felhasználók számára a Wi-Fi hozzáférés csak, akkor biztosítható, ha az illetékesek jóváhagyták az adott felhasználó Wi-Fi hozzáférésre vonatkozó igényét.

(Amennyiben nincs vezeték nélküli hozzáférés, akkor a fentiek helyett azt kell leírni.)

A szervezet elektronikus információs rendszeréhez mobil eszközök (mobil telefon vagy tablet) használatával történő hozzáférés szabályai az alábbiak:

- A mobil eszközzel való hozzáférés történhet vezeték nélküli hálózaton keresztül vagy távoli hozzáféréssel (VPN), így a hozzáférés tekintetében a Wi-Fi, ill. a VPN hozzáférés szabályait kell alkalmazni.
- A felhasználók csak megfelelő állapotban lévő (rendszeresen frissített, kártékony kódok elleni védelemmel ellátott és csak megbízható forrásból származó szoftvereket tartalmazó) telefonnal csatlakozzanak a szervezet elektronikus információs rendszeréhez.

(Amennyiben nem engedélyezett a mobil eszközzel való hozzáférés, akkor a fentiek helyett azt kell leírni.)

A szervezet az elektronikus információs rendszeréhez külső elektronikus információs rendszer használatával való hozzáférés szabályait az alábbiak szerint határozza meg:

- Részletesen meg kell határozni, hogy milyen műveletek hajthatóak végre a külső rendszer használatával (adatok olvasása, módosítása, letöltése, stb.)

- A külső elektronikus információs rendszer használatával való hozzáférés csak, akkor biztosítható, ha a külső rendszer tulajdonosával és üzemeltetőjével elfogadtatásra kerültek (szerződés vagy megállapodás) a felhasználás felételei.
- A szervezet illetékes vezetője jóváhagyta a hozzáférési igényt.

(Amennyiben nem engedélyezett a külső rendszer használatával való hozzáférés, akkor a fentiek helyett azt kell leírni.)

Mentés

A szervezet az alábbiak szerint fogalmazza meg az elektronikus információs rendszerhez kapcsolódó mentési rendjét. *(Amennyiben a szabályok megfogalmazása külön dokumentumban történik, akkor azt elégséges csak hivatkozni, illetve röviden összefoglalni.)*

- <**megadandó pontosan, hogy milyen mentés, pl. napi, heti, havi, negyedéves és éves milyen adatok (felhasználói szintű információk, rendszerszintű információk és rendszerdokumentációk) és különbségi vagy teljes, stb.**>

A szervezet a mentési gyakorlatát úgy alakítja ki, hogy az összhangban legyen az üzletmenet-folytonossági, illetve katasztrófa utáni helyreállítási elvárásokkal, vagyis a helyreállítási időkre és a megengedett adatvesztésre vonatkozó elvárásokhoz.

A szervezet elektronikus információs rendszerének a mentéseit úgy tárolja, hogy a mentett információk bizalmassága, sértetlensége és rendelkezésre állása biztosított legyen. A szervezet elsődleges telephelyén a mentéseket <**meghatározott paraméterekkel rendelkező, pl. tűzbiztos**> páncélszekrényben helyezi el, és ahhoz csak az arra jogosult szereplők férhetnek hozzá.

A szervezet a mentések másolatát <**a megadott helyen**> tárolja annak érdekében, hogy egy esetleges az elsődleges telephelyet érintő katasztrófa után is helyre lehessen állítani a szervezet elektronikus információs rendszereit / rendszerelemeit. A másodlagos tárolási helyszínen alkalmazott biztonsági kontrollok nem lehetnek gyengébbek, mint az elsődleges tárolás esetében alkalmazottak, ott is biztosítani szükséges a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását, illetve a mentésekhez való hozzáférés kontrollját. *(Amennyiben nincs másodlagos tárolási helyszín, akkor a fentiek helyett azt kell leírni.)*

A szervezt <**meghatározott időnként**> teszteli a mentések megfelelőségét a mentésekből való helyreállítás elvégzésével. A tesztelés elvégzésére az illetékes vezető felelős személyt jelöl ki. A felelős a tesztelés előtt részletes forgatókönyvet készít, és a tesztelést ez alapján hajtja végre. A forgatókönyvnek tartalmaznia kell az elvégzendő teszt részletes leírását (mely rendszer, mely adatainak, milyen eljárással való helyreállítása), a végrehajtás részleteit, pl. tervezett és tényleges végrehajtási idő, a teszt végrehajtója, a végrehajtás ellenőre, a tesztelés eredménye (sikeres/sikertelen). A felelős a mentési gyakorlatról összefoglalót készít, és tájékoztató jelleggel meg küldi az illetékes vezetőnek. A teszt sikertelensége esetén meg kell vizsgálni az okokat, majd azok kijavítása után <**meghatározott idő**> a tesztelést meg kell ismételni.

Naplózás

A szervezetnek az alábbiak szerint javasolt megfogalmaznia az elektronikus információs rendszerében, ill. rendszerelemieben alkalmazott naplózási gyakorlatát. *(Amennyiben a szabályok megfogalmazása külön dokumentumban történik, akkor azt elégséges csak hivatkozni, illetve röviden összefoglalni.)*

A szervezet az elektronikus információs rendszerében az alábbi események naplózását várja el:

<**naplózandó események listája, pl. felhasználó ki- és belépése, sikeres vagy sikertelen belépési kísérletek, sikeres vagy sikertelen jelszómódosítás, a felhasználói fiókkal végzett műveletek (létrehozás, módosítás, felfüggesztés, stb.**>

A szervezet elektronikus információs rendszerében a naplózásra kerülő eseményekhez kapcsolódóan annyi információt kell összegyűjteni, amely elégséges ahhoz, hogy egy esetleges biztonsági eseményt követően a történtek rekonstruálásához elégséges információt biztosítsanak.

A szervezet elektronikus információs rendszerében a naplózási tevékenységhez akkora tárkapacitást biztosít, ami a korábbi időszakok tapasztalatai alapján <**a meghatározott időszak**> alatt képződő naplóbejegyzések számára elégséges.

Amennyiben a szervezet elektronikus információs rendszerében naplózási hiba merül fel, akkor az érintett rendszer riasztást küld, és a <**korábbi naplóbejegyzéseket felül kell írni / az érintett rendszert le kell állítani**>.

A szervezet rendszeresen felülvizsgálja a <**megadott rendszerek**> naplóbejegyzéseit, a nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából. A felülvizsgálati tevékenység elvégzésére <**a megadott elemző szoftvert alkalmazzák / felelős személy kerül kijelölésre**>. A naplóvizsgálat eredményeiről jelentést kell készíteni, a jelentés elkészítése az illetékes vezető által kijelölt személy feladata. A jelentést el kell juttatni az illetékes vezető számára.

A szervezet rendszereiben képződő naplóbejegyzésekben szereplő időbejegyzésekhez az adott rendszerelem belső rendszeróráját kell használni. Az egyes rendszerelemek által használt belső rendszerórákat a <**meghatározott**> referenciaidőhöz kerül szinkronizálásra annak érdekében, hogy az egyes rendszerelemek által előállított bejegyzésekben szereplő időbejegyzések esetében biztosított legyen a konzisztencia.

A szervezet elektronikus információs rendszerében tárolt naplóinformációhoz és a naplókezelő eszközökhöz csak a megfelelő jogosultság birtokában lehet hozzáférni, megelőzendő az ott tárolt információk illetéktelen személyek általi módosítását vagy törlését, illetve a naplózási beállítások módosítását.

A szervezet az egyes rendszerek vagy rendszerelemek esetében képződő naplóbejegyzéseket <**x évig**> őrzi meg. A megőrzés lehetséges a forrásrendszerekben, a központi naplózó infrastruktúrában, illetve archivált állományokban is.

A szervezet elektronikus információs rendszerében csak olyan rendszerelemek használhatóak, amelyek képesek a szervezet által meghatározott naplózandó eseményekhez tartozó naplóbejegyzések előállítására. Az elektronikus információs rendszer naplózási funkciója úgy került kialakításra, hogy az lehetővé tegye a megfelelő szerepkörrel rendelkező felhasználók számára annak kiválasztását, hogy az elektronikus információs rendszer egyes elemeiben mely események kerüljenek naplózásra a naplózható eseményekből. Az elektronikus információs rendszernek előállítja a szervezet illetékese(i) által beállított eseményekre a szükséges naplóbejegyzéseket, a szervezet által elvárt tartalommal.

Sebezhetőségek kezelése

A szervezet az alábbiakban határozza meg az elektronikus információs rendszerét veszélyeztető sebezhetőségek kezelésével kapcsolatos szabályait. *(Amennyiben a szabályok megfogalmazása külön dokumentumban történik, akkor azt elégséges csak hivatkozni, illetve azt röviden összefoglalni.)*

A szervezet rendszeresen felméri, hogy az elektronikus információs rendszerei és alkalmazásai tekintetében milyen sérülékenységi tesztek végezhetőek el, mivel a sérülékenység-vizsgálatok nem veszélyeztethetik a szervezet elektronikus információs rendszerének a működési biztonságát, csak olyan tesztek elvégzése lehetséges, amit az elektronikus információs rendszer üzemeltetési és használati körülményei lehetővé tesznek.

A szervezet a <**megadott**> rendszerelemeire legalább <**időszak megadása**> sérülékenység-teszteket végez vagy végeztet. A teszteket minden olyan esetben meg kell ismételni, amikor új, lehetséges sérülékenység merül fel a kötelezően tesztelendő rendszerelemeivel kapcsolatban.

A sérülékenységtesztek végrehajtása során egy előre meghatározott ellenőrzési listát, ill. tesztelési eljárásokat kell végrehajtani, azoktól eltérni csak indokolt esetben lehet. Az ellenőrzési lista összeállításakor meg kell határozni, hogy a teszteléshez milyen jogosultságok szükségesek.

A sérülékenységvizsgálat során olyan sérülékenységtesztelő eszközt kell alkalmazni, amelynek sérülékenység feltáró képessége könnyen bővíthető az új ismertté váló sérülékenységekkel. A tesztek végrehajtása előtt az eszköz sérülékenységi adatbázisát mindig frissíteni kell.

A sérülékenység-teszt eredményeit jegyzőkönyvben kell rögzíteni, ami tartalmazza a feltárt sérülékenységek lehetséges hatásait, illetve a kihasználásának kockázatát, továbbá a javaslatokat sérülékenységek felszámolására, illetve a kockázatok csökkentésére. A jegyzőkönyv elkészítése a teszt elvégzőjének (külső vagy belső szereplő) a feladata. A jegyzőkönyvet tájékoztató jelleggel meg kell küldeni az illetékes vezető(k)nek.

A feltárt sérülékenységek felszámolására, ill. a kockázatok csökkentésére intézkedési tervet kell készíteni, ami részletesen tartalmazza az egyes feladatokat és azok elvégzésének a felelősét, ütemezését (és esetleges mérföldköveit), valamint a szükséges erőforrásokat. Az intézkedési terv elkészítésére, folyamatos karbantartására és az előrehaladás nyomon követésére felelőst kell kijelölni. Az intézkedési tervet az illetékes vezetővel (vezetőkkel) jóvá kell hagyatni. A

felelős személy feladata az illetékesek <**megadott időszakonkénti**> tájékoztatása az előrehaladásról, illetve az esetleges csúszásokról vagy fennakadásokról.

A szervezet a sérülékenységvizsgálatoktól függetlenül is követi az elektronikus információs rendszerével, illetve annak elemeivel kapcsolatos sérülékenységeket. A szervezet illetékes vezetője felelőst jelöl ki erre a feladatra. A felelős az NBSZ NKI weboldalán (https://nki.gov.hu/) követi nyomon az ismert sérülékenységeket, illetve az NBSZ NKI hírlevelére is feliratkozott. A felelős megvizsgálja az NBSZ NKI által publikált vagy levélben küldött sérülékenységeket abból a szempontból, hogy azok bírnak-e a szervezetre vonatkozó relevanciával. Amennyiben az adott sérülékenység releváns a szervezet szempontjából, akkor végrehajtja az abban javasolt intézkedéseket (javítócsomag telepítése vagy konfigurációs beállítások módosítása). Amennyiben az adott sérülékenység nem oldható meg azonnal, mert nincs hozzá javító csomag vagy a kezeléshez valamilyen extra erőforrásra van szükség, akkor az felvételre kerül a szervezet intézkedési tervébe.

Adathordozók kezelése

A szervezet az elektronikus információs rendszerben adathordozók használatával kapcsolatosan az alábbi szabályokat érvényesíti. *(Amennyiben a szabályok megfogalmazása külön dokumentumban történik, akkor azt elégséges csak hivatkozni, illetve röviden összefoglalni.)*

A szervezet az alábbiak szerint határozza meg, hogy mely szerepkörök milyen típusú adathordozók használatára jogosultak az elektronikus információs rendszerben:

- **standard felhasználók**: semmilyen/CD/DVD/USB-s eszköz – saját gép/korlátozás nélkül
- **kulcsfelhasználók**: semmilyen/CD/DVD/USB-s eszköz – saját gép/korlátozás nélkül
- **rendszerüzemeltetők**: semmilyen/CD/DVD/USB-s eszköz – saját gép/korlátozás nélkül

A szervezet az adathordozók újrahasznosítása vagy selejtezése előtt az adathordozón tárolt adatok minősítésének megfelelő törlési mechanizmusokat alkalmaz. A törléshez megfelelő célszoftvert használ, ami az eszközön tárolt adatok minősítésének megfelelő erősségű törlési algoritmussal végzi el az adattároló törlését. Az alábbi metódusok kerülnek alkalmazásra

- **Nyilvános adatok**: egyszerű törlés;

- **Belső felhasználású** (a szervezeten belül szabadon használható) **adatok esetében**: 3x felülírás;
- Az üzleti titkot képező vagy egyéb a szervezeten belül is **csak korlátozottan hozzáférhető adatok** (pl. munkavállalók személyes adatai) esetében: 8x felülírás.) (a lista egy javaslat, melytől el lehet térni)

Az adathordozók selejtezése történhet fizikai megsemmisítéssel vagy roncsolással is, de ebben az esetben az adattároló roncsolásának olyan mértékűnek kell lennie, hogy az adattárolóról már semmilyen adat ne legyen visszaállítható.

Az egyes rendszerelem típusokban az alábbi adathordozók használhatóak:

- **Kritikus rendszerek**: nem használhatóak külső adathordozók, ez alól kivételt csak a rendszerüzemeltetők képezhetnek, amennyiben a külső adathordozó szükséges pl. egy új javítócsomag vagy új szoftververzió telepítéséhez.
- **Egyéb rendszerek**: standard felhasználók is használhatnak külső adathordozót, de csak abban az esetben, ha annak használata engedélyezésre került számukra

A szervezet a rendszereiben csak a szervezet által biztosított adathordozók használhatóak és azokon <**titkosítási mechanizmust neve**> titkosítás alkalmaz. *(Amennyiben nem alkalmaz ilyen mechanizmust, vagy az adathordozókat nem a fentiek szerint használják, akkor a fentiek helyett azt kell leírni.)*

Rosszindulatú programok elleni védelem

A szervezet az elektronikus információs rendszerében a rosszindulatú programok elleni védelmi megoldást alkalmaz. *(Amennyiben a szabályok megfogalmazása külön dokumentumban történik, akkor azt elégséges csak hivatkozni, illetve röviden összefoglalni.)*

A szervezet a rosszindulatú programok elleni védelemi megoldását úgy paraméterezi, hogy az az elektronikus információs rendszer belépési és kilépési pontjain felderíti és megsemmisíti a rosszindulatú programokat.

A rosszindulatú programok elleni védelmi szoftver úgy kerül beállításra, hogy az rendszeresen frissíti a védelmi mechanizmus definíciós adatbázisát. A friss definíciós adatbázis, amint lehetséges letöltésre kerül a gyártótól és a szervezeten belül terítésre kerül az összes érintett

NEMZETI
KIBERBIZTONSÁGI
INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2026