KISKÖRE VÁROS POLGÁRMESTERI HIVATAL

Információbiztonsági Szabályzat

2.0 Verzió

Előírások, szabályok és eljárásrendek gyűjteménye

Verziótörténet

Verzió	Dátum	Készítette / módosította	Módosítás
v2.0	2025.12.12	IT SCHecurity Kft.	Első kiadás alap biztonsági osztály szerint

TARTALOMJEGYZÉK

INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

1.BEVEZETÉS ÉS KÖVETELMÉNYEK

1.1. A SZABÁLYZAT CÉLJA

Az Információbiztonsági Szabályzat (továbbiakban: IBSZ) alapvető célja, hogy szabályozza a Kisköre Város Polgármesteri Hivatala (továbbiakban: Szervezet), valamint annak Elektronikus Információs Rendszerét (Továbbiakban EIR) használók, a vele informatikai rendszerüzemeltetési szerződéses kapcsolatban lévő egyéb szervezetek EIR-ében kezelt adatok bizalmasságát, sértetlenségét és rendelkezésre állását, illetve a rendszerek funkcionalitását fenyegető veszélyforrások elleni védelmi intézkedéseket, ezáltal biztosítsa a Szervezet célkitűzéseinek és feladatainak teljesítését.

Az IBSZ további célja, hogy biztosítsa a hatályos jogszabályoknak való megfelelőséget, különös tekintettel azokra az előírásokra, amelyek alapján az informatikai rendszerek biztonsági besorolása szerint kell gondoskodni.

Az IBSZ célja továbbá, hogy a Szervezet informatikai üzemeltetője (továbbiakban: Informatika csoport) valamint a felhasználók – és az informatikai rendszerüzemeltetési szolgáltatás esetleges ügyfelei – számára meghatározza az EIR üzemeltetésére, illetve használatára vonatkozó szabályokat, eljárásokat.

A dokumentumnak az alábbi részletes céljai vannak:

a) Határozza meg az IT biztonság szervezeti kereteit, az IT biztonsági feladatokat ellátó szerepköröket, azoknak a feladatát, felelősségét és hatáskörét,
b) Határozza meg az IT biztonsági intézkedések működtetésével összefüggő feladatokat, amelyeket a mindennapi működés során végre kell hajtani, alkalmazni kell,
c) Határozza meg az IT biztonsági intézkedés végrehajtásának felelősét, akin számonkérhető a biztonsági intézkedések működtetése, alkalmazása.
d) Határozza meg az IT biztonsági intézkedés végrehajtásában, alkalmazásában közreműködő egyéb szereplőket, érintettjeit és azok feladatait.

Az IBSZ-ben meghatározott biztonsági intézkedések részletes végrehajtási utasításait, eljárásait kapcsolódó dokumentumok, mint például üzemeltetési kézikönyvek, felhasználói kézikönyvek tartalmazzák.

1.2. HATÁLYA

A szabályzat hatálya a következőkre terjed ki:

1.2.1. SZERVEZETI-SZEMÉLYI HATÁLY

A szabályzat szervezeti hatálya a Szervezet valamennyi olyan szervezeti egységére kiterjed, amely a Szervezet EIR-eit használja, üzemelteti, fejleszti, továbbá ilyen tevékenységeket irányít és ellenőriz.

A szabályzat személyi hatálya kiterjed a Szervezettel munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre, tehát azokra, akik kapcsolatba kerülnek a Szervezet EIR-eivel (azt használják, üzemeltetik, fejlesztik, telepítik, javítják stb.), így

a) a munkaviszony alapján foglalkoztatott alkalmazottakra;
b) a Szervezettel szerződéses kapcsolatban álló természetes és jogi személyekre;
c) más szervezetek képviseletében a Szervezet munkahelyein vagy ezek környezetében tartózkodó személyekre;
d) a rendszer bármely részén karbantartást végző támogató személyzetre.

1.2.2. TÁRGYI HATÁLY

A szabályzat tárgyi hatálya kiterjed az Szervezet EIR-eire, így az EIR-t alkotó

a) környezeti infrastruktúra elemeire;
b) hardver eszközökre, készülékekre, berendezésekre;
c) szoftverekre;
d) adathordozókra;
e) dokumentációkra.

A tárgyi hatály kiterjed továbbá az EIR-ben rögzített, tárolt, feldolgozott vagy továbbított adatokra.

1.2.3. TERÜLETI HATÁLY

A szabályzat területi hatálya kiterjed a Szervezet 3384 Kisköre, Széchenyi út 24. alatti központi telephelyére továbbá mindazon területekre, ahol a Szervezet informatika használatával a tevékenységét kifejti, függetlenül annak geográfiai elhelyezkedésétől.

A szabályzat területi hatálya nem terjed ki a Szervezet tulajdonában lévő, de bérlőnek tartós használatra átadott fizikai területre abban az esetben, ha a bérlő semmilyen módon nem csatlakozik a Szervezet informatikai infrastruktúrájához.

1.2.4. IDŐBELI HATÁLY

Az IBSZ, úgyis mint információbiztonsági szabályzatok gyűjteménye, a kiadásának napján lép hatályba. Jelen szabályzat kiadásával a korábban érvényben lévő informatikai szabályzatok, kézikönyvek, házirendek hatályukat veszítik.

1.3. A SZABÁLYZAT FELÜLVIZSGÁLATA

Az IBSZ eseti módosítására van szükség, ha a benne szereplő adatok megváltoztak, illetve az EIR működésében, vagy az EIR működését meghatározó jogszabályi környezetben, szabványokban jelentős változások következnek be.

A szabályzatot és a benne foglalt eljárásrendeket legalább évente egy alkalommal felül kell vizsgálni.

A szabályzat eseti módosításának, felülvizsgálatának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az informatikai rendszerek biztonságáért felelős személy (továbbiakban: EIBF) feladata. A módosítások engedélyezése és az újabb változat jóváhagyása a Szervezet vezetőjének hatásköre.

Felelős: EIBF
Felülvizsgálat: évente, vagy nagyobb változások esetén.

1.4. HATÁSKÖRI ÉS ILLETÉKESSÉGI SZABÁLYOK

Az IBSZ belső használatú dokumentum, amelynek kivonatolt változatát (Informatikai Biztonsági Házirend) az EIR felhasználói, illetve egyéb érintettek (a Szervezettel szerződéses kapcsolatban álló természetes és jogi személyek, más szervezetek képviseletében a Szervezet munkahelyein tartózkodó személyek) megismerhetik és birtokolhatják, de illetéktelenek nem adhatják tovább.

A Szervezet informatikáért felelős vezetőjének (továbbiakban: IT vezető) feladata gondoskodni arról, hogy a szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.

1.5. KAPCSOLÓDÓ DOKUMENTUMOK

Az IBSZ-hez a következő dokumentumok kapcsolódnak:

1.5.1. JOGSZABÁLYOK

- 2012. évi I. törvény a munka törvénykönyvéről;
- 2012. évi C. törvény a Büntető Törvénykönyvről;
- 2013. évi V. törvény a Polgári Törvénykönyvről;
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Infotv.);
- 1999. évi LXXVI. törvény a szerzői jogról (továbbiakban: Szjt.);
- Az Európai Parlament és Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (továbbiakban: GDPR);
- 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól;
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról;
- 418/2024. (XII.23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról (a továbbiakban: Korm. rendelet);
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről.

1.5.2. SZABVÁNYOK, AJÁNLÁSOK, EGYÉB KÖVETELMÉNYEK

- Az EP és ET 2022. december 14-i (EU) 2022/2555 irányelve (továbbiakban EU NIS2);
- MSZ ISO/IEC 27001:2023 Informatika. Biztonságtechnika. Az információbiztonság-irányítási rendszerek. Követelmények;
- NIST 800-53 Rev5. Security and Privacy Controls for Information Systems and Organizations

1.6. SZEREP- ÉS FELELŐSSÉGI KÖRÖK AZ INFORMÁCIÓBIZTONSÁGBAN

A munkavállalók információbiztonsági szerepkörének a munkavállalók munkaköri leírásában is meg kell jelennie. Erről a munkahelyi vezetők kötelesek gondoskodni.

Az informatikai biztonsági szereplők jelen pontban nem említett további feladatait, felelősségét a munkaköri leírásuk tartalmazza.

1.6.1. ÁLTALÁNOS SZEREPKÖRÖK

Ezek a szerepkörök alapvetők a Szervezet életében.

1.6.1.1. JEGYZŐ

A Szervezet első számú vezetője.

Feladatai:

- Meghatározza és rendszeresen felülvizsgálja a Szervezet informatikai biztonsági politikáját és a biztonsági stratégiáját.
- Kinevezi, illetve megbízza az EIBF-t (ld. Elektronikus információs rendszerek biztonságáért felelős személy (EIBF)pont).
- Meghatározza az EIR védelmének felelőseire, feladataira, az ehhez szükséges hatáskörökre és a felhasználókra vonatkozó szabályokat, illetve kiadja az Informatikai Biztonsági Szabályzatot (továbbiakban: IBSZ).
- Biztosítja a Szervezet minden felhasználója számára a munkavégzéshez szükséges informatikai eszközöket és szoftvereket.
- Felelős a Szervezet EIR kialakításáért, a fejlesztési feladatok meghatározásáért, valamint a rendszerek információbiztonságáért.
- Az EIBF-fel rendszeresen ellenőrizteti, hogy a Szervezetnél megfelelően alkalmazzák-e az IBSZ előírásait.
- Egyszemélyi felelősségének megtartása mellett az egyes funkciók irányítását átadhatja más szervezeteknek és személyeknek.

Elkötelezett az információbiztonsági intézkedések végrehajtása iránt, amelynek keretében biztosítja a megvalósításhoz szükséges erőforrásokat, valamint támogatja a biztonsági célok teljesülését és a szabályzatban foglaltak következetes betartását.

1.6.1.2. IT VEZETŐ

A Szervezet informatikai üzemeltetés felügyeletével megbízott személye. A Szervezetnél ezt a szerepkört a Jegyző látja el.

Feladatai:

- Gondoskodik az informatikai biztonságra vonatkozó jogszabályok, a biztonságpolitika, a biztonsági stratégia és az IBSZ végrehajtásáról és betartásáról.
- Felelős a Szervezetnél előforduló valamennyi, az EIR védelméhez kapcsolódó feladat ellátásáért.
- Engedélyezi az információbiztonsággal kapcsolatos eljárási és védelmi követelményszinteket és folyamatokat.
- Felelős az EIR biztonságának folyamatos felülvizsgálatáért. Ennek keretében az EIBF-fel elvégezteti az EIR kockázatelemzését.
- Felelős az EIR üzemeltetéséhez szükséges erőforrások biztosításáért és a rendszerek folyamatos működéséért.
- Gondoskodik a folyamatos munkát biztosító koordinációról és a zökkenőmentes végrehajtást akadályozó tényezők megszüntetéséről.
- Meghatározza az informatikai feladatok prioritását, végrehajtási sorrendjét.

- Felügyeli az alap informatikai szolgáltatásokat megvalósító alaprendszerek (pl. központi címtár, fájl szerver szolgáltatások, levelező rendszer stb.) és rendszerszoftverek (pl.: operációs rendszerek, adatbáziskezelő szoftverek, tűzfal szoftverek stb.), a szerver és felhasználói oldali informatikai eszközök, illetve hálózati eszközök üzemeltetését.
- Irányítja a belső fejlesztésű EIR fejlesztését és a webes fejlesztési tevékenységeket, biztosítja az ehhez a szükséges feltételeket.
- Irányítja az új alkalmazói szoftverek vagy rendszerek bevezetését és a meglévő rendszerek továbbfejlesztését.
- Törekszik arra, hogy a Szervezet célkitűzéseket támogató és a folyamatok hatékony működését biztosító, korszerű EIR kerüljenek kialakításra.
- Fokozott figyelmet fordít az EIR bevezetése és továbbfejlesztése során az IBSZ-ben rögzített információbiztonsági előírások teljesülésére. Ennek során együttműködik az EIBF-fel.
- A kulcsfelhasználókkal együttműködve elkészíti és rendszeresen felülvizsgálja a Szervezet Készenléti tervét.
- Felügyeli az alap informatikai szolgáltatásokat megvalósító alaprendszerek (pl. központi címtár, fájl szerver szolgáltatások, levelező rendszer stb.) és rendszerszoftverek (pl.: operációs rendszerek, adatbáziskezelő szoftverek, tűzfal szoftverek stb.), a szerver és felhasználói oldali informatikai eszközök, illetve hálózati eszközök üzemeltetését.
- Biztosítja a Szervezet informatikai eszközeinek minél kisebb kieséssel történő üzemeltetését.
- Felügyeli az informatikai eszközök műszaki karbantartását, javítását a leggazdaságosabb megoldásokat helyezve előtérbe.
- Irányítja az új rendszerszoftverek, alaprendszerek bevezetését.
- Törekszik arra, hogy a Szervezet célkitűzéseket támogató és a folyamatok hatékony működését biztosító, korszerű EIR kerüljenek kialakítása.
- Fokozott figyelmet fordít az EIR bevezetése és továbbfejlesztése során az IBSZ-ben rögzített információbiztonsági előírások teljesülésére. Ennek során együttműködik az EIBF-fel.

Ezen szerepkör összeférhetetlen az EIBF-fel: az IT vezető főként a Szervezet üzleti igényeit és technológiai fejlesztéseit helyezi előtérbe, míg az EIBF elsősorban a biztonsági szempontokra koncentrál, emiatt ellentétes érdekeket képviselnek.

1.6.1.3. ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGÁÉRT FELELŐS SZEMÉLY (EIBF)

A Szervezetnél az elektronikus információs rendszerek biztonságáért felelős személy (továbbiakban: EIBF) a Szervezet informatikai biztonsági vezetője. Ezt a munkakört a szolgáltató megbízási szerződése rögzíti.

Feladatai:

- Felelős a Szervezetnél előforduló valamennyi, az EIR védelméhez kapcsolódó feladat felügyeletéért.
- Gondoskodik a Szervezet EIR biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról. Irányítja ezen tevékenységek tervezését, szervezését, koordinálását és ellenőrzését.
- Előkészíti és rendszeresen felülvizsgálja a Szervezet Informatikai Biztonsági Szabályzatát.

- Információbiztonsági szempontból véleményezi a Szervezet szabályzatait és szerződéseit, biztosítja a biztonsági követelmények érvényre juttatását.
- Összeállítja az információbiztonsági ismeretek és előírások oktatási anyagát, megszervezi az információbiztonsági képzések lebonyolítását.
- Részt vesz az EIR bevezetése és továbbfejlesztése során a biztonsági rendszer tervezésében, kialakításában, a védelmi eszközök alkalmazására vonatkozó döntés előkészítésben, a biztonságot növelő intézkedések kialakításában.
- Kockázatelemzés végzésével követi az EIR-t fenyegető veszélyforrások változásait, és kezdeményezi a szükséges védelmi intézkedéseket. Javaslatot tesz új védelmi eszközök és technológiák beszerzésére, illetve bevezetésére.
- Bejelentés alapján kivizsgálja a biztonsági eseményeket, és javaslatot tesz további intézkedésekre.
- Kapcsolatot tart a hatósággal és a kijelölt nemzeti kiberbiztonsági incidenskezelő központtal, amelynek feladatait a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézetének egy biztonsági eseményekkel foglalkozó akciócsoportja látja el (a továbbiakban: Kiberbiztonsági incidenskezelő központ).
- Írásban jelent a Szervezet vezetőjének minden olyan vitás kérdést, melyet az érintett területekkel együttműködve nem tud rendezni, illetve a biztonsági előírások teljesülésének veszélyeztetését észleli és közvetlen intézkedése eredménytelen maradt.
- Az IBSZ súlyos megszegését jelenti a Szervezet vezetőjének, aki az előírások ellen vétőkkel szemben fegyelmi felelősségre vonási eljárást kezdeményezhet.

Jogai:

- Jogosult az IBSZ előírásainak betartását bármely érintett szervezeti egységnél ellenőrizni.
- Ellenőrzési tevékenysége során betekintést nyerhet az EIR működésébe és a kapcsolatos dokumentumokba.
- Közvetlenül jogosult bármely érintett szervezeti egység vezetőjének, beosztott munkatársának olyan utasítást adni, mely az IBSZ-ben foglaltak betartását, annak végrehajtását célozza.
- Feladata ellátása során a Szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.

Ezen szerepkör összeférhetetlen az IT vezetővel (érdekek ütközése), illetve a Rendszergazdával (felügyeleti ellenőrzés), azaz el kell kerülni, hogy ugyanazon személy legyen a végrehajtási, illetve az ellenőrzési oldalon.

Az ellenőrzés hatékonysága lecsökken, valamint rendkívül kockázatossá válik, ha ugyanaz a személy, vagy csoport felügyeli és ellenőrzi saját tevékenységét (önellenőrzés).

1.6.1.4. ADATVÉDELMI FELELŐS (DPO)

Az Infotv. előírásainak és a Szervezet hatályos adatvédelmi szabályzatának szervezeten belüli betartásáért felelős személy.

Felelőssége nemcsak az EIR-ben kezelt adatokra vonatkozik, hanem minden adatkezelésre, függetlenül annak megjelenési formájától (pl.: papír alapú nyilvántartásokra, szerződésekre, dokumentumokra stb.).

Feladatai:

- Szorosan együttműködik az Informatika csoporttal, segíti annak munkáját és iránymutatást nyújt adatkezeléssel összefüggő kérdésekben.
- Ellenőrzi az adatvédelmi előírások betartását.
- Egyéb adatvédelmi feladatait az Adatvédelmi és Adatbiztonsági elvárás(ok) határozza meg.

1.6.1.5. FIZIKAI BIZTONSÁGI FELELŐS (BIZTONSÁGI VEZETŐ)

A Szervezet vezetője által a fizikai belépések felügyeletével megbízott munkatárs (aki általában az őrző- és portaszolgálatot vezeti, illetve koordinálja). A Szervezetnél ezt a szerepkört a Jegyző látja el.

Feladatai:

- Összeállítja és folyamatosan karbantartja a Szervezet informatikai eszközökkel ellátott helységeibe belépésre jogosultak listáját, kiadja és visszavonja a belépési engedélyeket, illetve az engedélyek igazolására szolgáló belépőkártyákat (ld. Fizikai belépési engedélyek pont).
- Felügyelet alatt tartja a fizikai belépések folyamatát, kezeli az ezzel kapcsolatos rendellenességeket.

1.6.1.6. RENDSZERGAZDA

Az EIR felett az Informatika csoport részéről felügyeletet gyakorló személy.

Feladatai:

- Felelős a rábízott EIR üzemszerű, folyamatos működéséért. Rendszeresen ellenőrzi a rendszer és elemeinek helyes működését.
- Felügyeli az EIR (és környezetének) biztonsági állapotát. Folyamatosan ellenőrzi az EIR védelmi eszközeinek megfelelő működését.
- Felelős a biztonsági kockázatok minimalizálásáért, az üzemeltetési feladatokat veszélyeztető és akadályozó tényezők felismeréséért és jelentéséért.
- Felelős az EIR biztonsági mentéseinek készítéséért, ellenőrzéséért, tárolásáért és a kapcsolódó nyilvántartások vezetéséért.
- Átvizsgálja az EIR és kapcsolódó környezetük (alkalmazói szoftverek, szerverek, hálózati eszközök, határvédelmi eszközök és egyéb biztonsági eszközök) eseménynaplóit.
- Elkészíti, rendszeresen felülvizsgálja és teszteli a Szervezet Készenléti tervét (korábban Üzletmenet folytonossági terv és Katasztrófa elhárítási terv). Gondoskodik az EIR katasztrófahelyzetben történő újraindíthatóságáról, illetve az ehhez szükséges beállítások, paraméterek rendelkezésre állásáról.
- Az EIR-re vonatkozóan feltölti és naprakészen tartja az EIR nyilvántartását (EIR nyilvántartás), a rendszer Alapkonfigurációját és az Rendszerelem leltárat.
- Elvégzi az EIR hibáinak felderítését, az ebből adódó szoftvertelepítési, frissítési feladatokat, valamint koordinálja a külső partnerek által végzett javításokat.
- Az EIR kialakítása és üzemeltetése során biztosítja az információbiztonsági és adatvédelmi előírások feltételeit, és figyelemmel kíséri az előírások betartását. Mindezek tekintetében együttműködik az EIBF-fel és az Adatvédelmi felelőssel.
- Indokolt esetben az IT vezető tájékoztatásával és jóváhagyásával dokumentáltan engedélyezi az előírt üzemeltetéstől eltérő eljárások, konfigurációk alkalmazását.
- Nyomon követi az EIR változásait, és ennek megfelelően módosítási javaslatokat dolgoz ki.

- Véleményezi az esetleges fejlesztési igények megvalósíthatóságát, az új védelmi megoldások beépíthetőségét a működő rendszerbe.
- Fokozott figyelmet fordít arra, hogy a szervereket/egyéb eszközöket kiemelt jogosultsággal bejelentkezett állapotban ne hagyja felügyelet nélkül magára, a feladata elvégzése után kijelentkezik a rendszerből.
- Biztosítja a felhasználó oldali informatikai eszközök (számítógépek és tartozékok) működőképességét, fenntartja a folyamatos munkavégzéshez szükséges állapotot.
- Elvégzi az új eszközök IBSZ-ben rögzített információbiztonsági előírásoknak megfelelő biztonsági beállítását, és folyamatosan biztosítja a biztonsági beállítások helyességét és sértetlenségét.
- Az elhasználódott eszközök, adathordozók selejtezése, illetve újra felhasználásra kiadása esetén biztosítja a szükséges adatok mentését és az adathordozók biztonságos törlését, illetve megsemmisítését.
- Fogadja a hibajelentő rendszeren és sürgős esetben telefonon érkező felhasználói bejelentéseket és az egységes kezelés érdekében utólagosan rögzíti a HelpDesk rendszerben.
- Koordinálja a megoldandó HelpDesk hibajegyek kiosztását az EIR-hez kijelölt, felelős munkatársak számára, figyelembe véve a terheltségüket és a szabadság, betegség stb. miatti helyettesítésüket.
- A szolgáltatási szintek biztosítása érdekében figyelemmel kíséri a kiosztott hibajegyek gyors, prioritásuknak megfelelő megoldását, és szükség esetén módosítja a hibajegyek kiosztását.
- A HelpDesken bejelentett biztonsági eseményekről az esemény kivizsgálása céljából értesíti az EIBF-t.

Ezen szerepkör összeférhetetlen az EIBF-fel, mert a Rendszergazdák hozzáférést és ellenőrzést gyakorolhatnak az információbiztonsági rendszerek felett, ami a biztonságos működés és az ellenőrzés hiányát eredményezheti.

1.6.1.7. ADATGAZDA

Annak a szervezeti egységnek (adatgazdai területnek) a vezetője, amelyik szervezeti egységhez az EIR-ben tárolt adatok kezelése rendelhető, illetve ahol az adat keletkezik.

Feladatai:

- Meghatározza az adatok kezelésének célját, és meghozza az adatkezelésre vonatkozó döntéseket (beleértve a felhasznált eszközök megválasztását).
- Új EIR-t integrálása esetén meg kell vizsgálnia, hogy továbbra is fennállnak-e, illetve értelmezhetők a Szervezet által előírt biztonsági követelmények.
- A biztonsági követelmények teljesülése esetén elfogadja és engedélyezi a rendszer működését.

1.6.1.8. KULCSFELHASZNÁLÓ (ADMIN)

Az EIR-hez az adatgazdai terület vezetője által kijelölt, a rendszerben tárolt adatok védelméért, a rendszer funkcionális működéséért felelős Felhasználó.

Feladatai:

- Folyamatosan figyelemmel kíséri a felügyelete alá rendelt EIR megfelelő működését. Ha hibás működést tapasztal, erről a HelpDesk-en értesíti az Informatika Csoportot.
- Közreműködik a Szervezet Készenléti tervének elkészítésében, elvégzi a terv rendszeres tesztelését.

- Az EIR hibás működése esetén - ha úgy ítéli meg, - Készenléti terv alapján eljárva kezdeményezi a rendszer használatának felfüggesztését, és írásban rögzíti a felfüggesztés okát, a tapasztalt jelenséget. Ezzel egyidejűleg erről értesíti az Informatika csoportot és szükség szerint az intézkedésre jogosult vezetőt. Továbbá intézkedik arról, hogy a munkafolyamatok rögzítése a rendszer helyreállításáig papír alapú bizonylatokon történjen.
- Engedélyezi a külső és belső felhasználók különböző szintű hozzáférését az EIR-hez.
- Felügyeli, karbantartja az EIR kódrendszerét. Más rendszerekkel közös, kiemelt kódok esetén egyeztet a kapcsolódó rendszerek kulcsfelhasználóival.
- Gondoskodik a felügyelete alá tartozó EIR-rel dolgozó felhasználók betanításáról, a kezelési és információbiztonsági szabályok megismertetéséről. Ehhez szükség szerint segítséget kérhet az Informatika csoporttól és az EIBF-től.
- Gondoskodik az információbiztonsági és adatvédelmi előírások maradéktalan betartatásáról az adatfeldolgozás során, ebben együttműködik az EIBF-fel és az Adatvédelmi felelőssel.
- Összefogja és koordinálja az EIR-rel kapcsolatban felmerülő fejlesztési, módosítási, javítási igényeket, ezeket képviseli az informatika csoport felé, illetve a rendszer külső fejlesztői felé. Kapcsolatot tart az Informatika csoporttal.
- Vezeti az új vagy módosított EIR tesztelését. Felelős azért, hogy a tesztelés úgy történjen, hogy abból legyen tapasztalat minden üzemszerű működtetési körülményre, és lehetőség szerint nem üzemszerű működtetésre is.

1.6.1.9. ALKALMAZÁSFEJLESZTŐ

Az Informatika csoport szoftverfejlesztéssel megbízott munkatársa.

Feladatai:

- A belső fejlesztésű EIR és weboldalak fejlesztési tevékenysége során fokozott figyelmet fordít az IBSZ-ben rögzített információbiztonsági előírások teljesülésére.

1.6.1.10. MUNKAHELYI VEZETŐ

A Szervezet szakterületi vezetői és a további vezetők.

Feladatai:

- Felelős a saját területén a jelen eljárás betartásáért és betartatásáért.
- Köteles az IBSZ-ben foglaltakat megismerni és azt a munkaterületük beosztott munkatársaival megértetni, a rájuk bízott feladatokat határidőre elvégeztetni, és a végrehajtást folyamatosan ellenőrizni.

1.6.1.11. FELHASZNÁLÓ

Az EIR-rel kapcsolatba kerülő, azt használó munkatársak.

Feladatai:

- Minden Felhasználó köteles megismerni és betartani az IBSZ-ben leírtakat.

- Jelenti a jogszabályokban, szabályzatokban megfogalmazott előírások bárki által történő megszegését a munkahelyi vezetőjének, továbbá az IBSZ megszegését az EIBF-nek.
- Köteles jelenteni, ha biztonsági problémát okozó jelenséget tapasztal (biztonsági eseményt).
- Figyelemmel kíséri az EIR működését. Ha hibás működést tapasztal, erről azonnal értesíti a rendszer kulcsfelhasználóját és sürgős esetben a HelpDesken keresztül közvetlenül az Informatika csoportot. Rendellenes működés esetén az adatfeldolgozást felfüggeszti.
- Együttműködik az információbiztonságért és informatikai üzemeltetésért felelős személyekkel.
- Nem hagyja bejelentkezett állapotban felügyelet nélkül a számítógépét. Ha távozik a számítógéptől vagy befejezi a munkát, kilép az alkalmazói rendszerekből és zárolja, illetve kikapcsolja számítógépet. Ha utolsóként távozik a helyiségből, akkor a Szervezet előírásainak megfelelően zárja a helyisége.
- Karbantartás előtt szükség esetén segítséget nyújt az üzemeltető munkatársnak a számítógépen tárolt adatok mentéséhez. A karbantartásokat, javításokat helyben végző külső partnerek szakembereit még átmeneti időre sem hagyhatja felügyelet nélkül.
- Köteles meghatározott időközönként információbiztonsági képzésen részt venni. Csak a képzés eredményes megtörténtét követően dolgozhat az EIR-ben.
- Szakszerűen kezeli a munkavégzéséhez biztosított informatikai eszközöket (a számítógépet és a hozzá kapcsolt tartozékokat).
- Gondoskodik az informatikai eszközök állagmegóvásáról, a rárakódott szennyeződések eltávolításáról. Óvja nedvességtől, víztől, mágneses és elektromos erőtértől, mechanikai behatásoktól. Szintén óvja a hálózat elemeit.
- Az informatikai eszközök sérülését azonnal jelenti a HelpDesken az Informatika csoportnak.
- Gondoskodik a nevére szólóan kiosztott belépőkártya, és egyéb belépést biztosító eszköz megfelelő kezeléséről és őrzéséről.
- Köteles az EIR-hez hozzáférést biztosító jelszavait titokban tartani. A Felhasználó viseli a felelősséget minden olyan műveletért, amely neki felróható mulasztás miatt az adott felhasználóhoz tartozó azonosítóval kerül.

Jogai:

- A felhasználók jogosultak a rájuk vonatkozó jogszabályok, szabályzatok és a munkájukhoz szükséges információbiztonsági előírások megismeréséhez.
- Jogosultak az EIR-ek technikai problémáiról, tervezett karbantartásokról vagy rendkívüli eseményekről tájékoztatást kapni.
- Jogosultak megtagadni a számítógépes munkát, ha az súlyos törvénysértéshez, vagy bűncselekményhez vezetne.
- Jogosultak a számítógépes munkavégzéssel kapcsolatos sérelmeik jogorvoslati kezelésére. Jogorvoslati kérdésekben az IT vezető, magasabb szinten a Szervezet vezetője áll rendelkezésre.
- Jogosultak a számítógépes tevékenységük során felmerült problémák, akadályok elhárításához támogatást kapni az Informatika csoporttól. A segítségnyújtáshoz az igényt a HelpDesken kell bejelenteni.

1.6.2. KOCKÁZATI SZEREPKÖRÖK

A fellépő kockázatok - legyen az informatikai, technológiai, vagy ellátási lánc kockázata – azonosításával, értékelésével és kezelésével foglalkozó munkatársak.

- A kockázatkezelési hatáskörök és felelősségek szükség szerint a munkaköri leírásokban, esetleg egyéb szabályozásokban rögzítendők.

1.6.2.1. KOCKÁZATKEZELÉSI VEZETŐ (KOCKÁZATMENEDZSER)

A kockázatkezelési stratégiákért, politikákért, folyamatokért felelős személy. A Szervezetnél ezt a szerepkört a Jegyző látja el.

Feladatai:

- Felelős az olyan kockázatkezelési politikák és folyamatok kialakításáért és végrehajtásáért, amelyek segítik a Szervezetet a kockázatok hatékony kezelésében és csökkentésében.
- Azonosítania és értékelnie kell a jelentkező külső, vagy belső kockázatokat, melyek kezelésére javaslatokat kell előkészítenie.
- Együtt kell működnie és kommunikálnia kell a kockázatkezelésben érintett felekkel.
- Kockázatértékelési jelentést kell készítenie a kockázatokról, a kockázatkezelési tevékenységekről a Szervezet vezetőjének (illetve más érintett fél számára).

1.6.2.2. KOCKÁZATFELELŐS:

A kockázatkezelési intézkedések végrehajtásáért és a nyomon követésért felelős.

Feladatai:

- Felelős a kockázatkezelési intézkedések végrehajtásáért és felügyeletéért. Ez magában foglalja a megelőző intézkedések, ellenőrzések és eljárások bevezetését, valamint a kockázatokat elfogadható szintre csökkentő intézkedések végrehajtását.
- Tájékoztatja a vezetőséget és az érintett feleket a kockázatok állapotáról, a kockázatkezelési intézkedésekről és az esetleges kockázatokkal kapcsolatos fejleményekről.
- Folyamatosan monitorozza a kockázatok állapotát, a kockázatkezelés hatékonyságát, valamint az elfogadható kockázati szinteket a szervezetben. Figyelemmel kíséri a teljesítménymutatókat és rendszeresen felülvizsgálja és javítja a kockázatkezelési folyamatoka.

1.6.2.3. KOCKÁZATKEZELÉSI TANÁCSADÓ

Külső- vagy belső tanácsadó, aki szakértelmet és tanácsadást nyújt a kockázatkezelési stratégiák, folyamatok és eszközök kialakításához és végrehajtásához.

Feladatai:

- Támogatja a Kockázatkezelési vezetőt abban, hogy azonosítsa és értékelje a különböző kockázatokat, amelyek befolyásolhatják a Szervezet tevékenységeit.
- Segít a Szervezetnek stratégiákat kidolgozni a kockázatok kezelésére és csökkentésére. (pl: új technológiák alkalmazása, diverzifikáció vagy egyéb stratégiai lépések).

1.6.3. VÉSZHELYZETI SZEREPKÖRÖK

Vészhelyzet esetén az elhárításban, illetve helyreállításban érintettek.

1.6.3.1. VÉSZHELYZETI VEZETŐ

Felelős a vészhelyzet alatt az irányításáért és koordinálásáért. A Szervezetnél ezt a szerepkört a Jegyző látja el.

Feladatai:

- Ki kell értékelnie a helyzetet. Ennek során figyelembe veszi a kialakult vészhelyzet természetét, kiterjedését és hatásait.
- Megfelelő döntéseket kell hoznia a kár csökkentése, vagy a vészhelyzet elhárítása érdekében. Ezek a döntések magukban foglalhatják a biztonsági intézkedések aktiválását, a szükséges erőforrások mozgósítását és a kommunikációs lépéseket.
- Koordinálnia kell az összes vészhelyzetben érintett személyt, vagy csoportot. Jelentenie kell az elvégzett feladatokat és a helyzet alakulását a Szervezet vezetőjének.
- Előkészíti és beépíti a megelőző intézkedéseket a Készenléti tervbe annak érdekében, hogy minimalizálja a vészhelyzet kialakulásának vagy hatásainak kockázatát a jövőben.

1.6.3.2. VÉSZHELYZETI CSOPORT(INCIDENSKEZELŐ CSOPORT)

A rendszer, infrastruktúra vagy üzleti folyamatok helyreállításáért és újraindításáért felelősek csoportja

Feladata:

- A Vészhelyzeti vezető irányításával végrehajtják a Készenléti tervezet.
- Felelősök a kritikus rendszerek és adatok visszaállításában.
- Tesztelniük kell és ki kell értékelniük a helyreállított rendszerek működőképességét.
- Együtt kell működniük más érintett felekkel (pl. szolgáltatók, beszállítók).
- Az elvégzett feladatokról folyamatosan tájékoztatniuk kell a Vészhelyzeti vezetőt.
- Dokumentálniuk kell a végrehajtott lépéseket, úgymint a helyreállítási folyamatokat és elért eredményeket.

1.7. ALAPVETŐ INFORMÁCIÓBIZTONSÁGI FELADATOK

1.7.1. JOGSZABÁLYKÖVETÉS

Az informatikai biztonságot érintő jogszabályok változásának követése az EIBF feladata. A jogszabályok megváltozása esetén az EIBF feladata, hogy szükség esetén javaslatot tegyen intézkedésekre, folyamatok, eljárások módosítására. Amennyiben szerződés keretében keletkezik új, informatikai biztonságra vonatkozó követelmény, a projektvezető feladata a követelmény jelzése az EIBF-nek, illetve az IT vezetőnek.

1.7.2. JOGTISZTASÁG

A szoftverek jogtisztaságának betartása érdekében a szoftverek használatához szükséges licencekről nyilvántartást kell vezetni. A licenc nyilvántartás kérdése hozzákapcsolódik más IT eszközök nyilvántartásához. A licencek nyilvántartása az Informatika csoport, a nyilvántartás értékelése az IT vezető feladata. Amennyiben megalapozott licenc-igény következik be, úgy a beszerzést kezdeményezi.

1.7.3. TÖRVÉNYI MEGFELELÉS

Az törvénynek való megfelelés érdekében el kell készíteni és folyamatosan naprakészen kell tartani a törvény által előírt adatvédelmi nyilvántartásokat. A nyilvántartások elkészítése és karbantartása az Adatvédelmi felelős felelőssége. A nyilvántartás elkészítéséhez az Adatgazdáknak információt kell nyújtaniuk számára.

1.7.4. INTÉZKEDÉSI TERV ÉS MÉRFÖLDKÖVEI

A Szervezet az információbiztonság és az ellátási lánc kockázatkezelése terén, valamint az EIR intézkedési terveinek kidolgozása és karbantartása érdekében egy dokumentált folyamatot vezet be, hogy megfelelő választ tudjon adni az eszközök, valamint a személyek és más szervezetek által jelentett kockázatokra. A folyamat részeként biztosítottak az intézkedések rendszeres felülvizsgálata és frissítése, hogy azok hatékonyan reagáljanak a változó környezeti kockázatokra és a szervezeti igényekre.

A kidolgozott intézkedési tervek részletesen külön dokumentumban találhatók:

- Az osztályba sorolás hiányosságaival kapcsolatos intézkedési terv az Intézkedési terv dokumentumban;
- Az egyéb biztonsági és ellátási lánccal kapcsolatos kockázatokkal kapcsolatosan pedig a Kockázatmenedzsment dokumentumban szerepelnek.

1.7.5. EIR NYILVÁNTARTÁSA

Az EIR nyilvántartása külön dokumentumban, az EIR-nyilvántartásban szerepel

1.7.6. BIZTONSÁGI TELJESÍTMÉNY MÉRÉSE

Az információbiztonsági teljesítmény mérésének célja az, hogy az irányítók átfogó képet kapjanak az információbiztonsági helyzetről, és fel tudják mérni az információbiztonsági irányítási rendszer hatékonyságát. A mutatókat össze kell vetni az előző év hasonló mutatóival, így képet lehet kapni arról, hogy milyen mértékben növekedett (vagy csökkent) a biztonsági teljesítmény. Az információbiztonsági teljesítmény mérésére az alábbi mutatókat, eszközöket és módszereket kell használni:

1.7.6.1. KOCKÁZATELEMZÉS

A kockázatelemzés segít azonosítani az információbiztonsági fenyegetéseket, a kockázatokat, valamint a lehetséges hatásokat. A kockázatelemzés alapján a Szervezet képes felmérni az információbiztonsági teljesítményét, illetve mérni a biztonsági rendszer hatékonyságát.

1.7.6.2. TELJESÍTMÉNYMUTATÓK

Az információbiztonsági teljesítménymutatók segítségével mérhetők az információbiztonsági folyamatok hatékonysága. Az ilyen mutatók a hálózati átviteli sebesség, az adatbiztonság szintje, az incidenskezelési idő, a hibajavítási idő vagy a biztonsági ellenőrzések gyakorisága.

1.7.6.3. TELJESÍTMÉNYMÉRÉSI MÓDSZEREK

Az információbiztonsági teljesítmény mérésére használhatóak az oktatás-felmérési kérdőívek, a biztonsági átvilágítások, illetve az auditok.

1.7.6.4. ELLENŐRZÉSEK

Az információbiztonsági ellenőrzések során meg kell vizsgálni, hogy a munkavállalók betartják-e az információbiztonsági szabályokat, a belső irányelveket, valamint az érvényben lévő jogszabályokat. Az ellenőrzések eredményei alapján is mérhető az információbiztonsági rendszer hatékonysága.

1.7.7. SZERVEZETI ARCHITEKTÚRA

A Szervezeti architektúra a Szervezeti és Működési szabályzatban szerepel.

1.7.8. KRITIKUS INFRASTRUKTÚRA BIZTONSÁGI TERVE

A kritikus infrastruktúra biztonsági terve elérhető a Rendszer biztonsági tervekben és a készenléti tervekben.

1.7.9. KOCKÁZATKEZELÉS

A kockázatmenedzsment-stratégia célja, hogy az elektronikus információs rendszerek (EIR-ek) működéséhez és használatához, a szervezeti vagyonhoz, munkavállalókhoz, partnerekhez, valamint a személyes adatok kezeléséhez kapcsolódó biztonsági kockázatokat azonosítsa, értékelje, kezelje és folyamatosan felülvizsgálja.

Ezen stratégia a Szervezet minden szervezeti egységére és munkavállalójára kiterjed.

1.7.9.1. Kockázatok azonosítása

A következő kockázati területek kerülnek feltérképezésre:

1.7.9.1.1. EIR-ekkel kapcsolatos kockázatok

- Az informatikai rendszerek meghibásodása vagy kiesése, amely akadályozhatja a szervezet működését.
- Adatvesztés vagy adatok sérülése.
- Kiberbiztonsági fenyegetések, például vírusok, zsarolóprogramok, illetéktelen hozzáférések.
- A rendszerekhez hozzáférő személyek nem megfelelő jogosultságkezelése.
- Tesztelési hiányosságok, kompatibilitási problémák

1.7.9.1.2. Rendszer- és vagyonelemekhez kapcsolódó kockázatok

- Informatikai eszközök eltulajdonítása vagy megrongálása.
- Szoftverlicenc- és adatvagyon-kezelés hiányosságai.
- Az üzleti folyamatokat támogató rendszerek nem megfelelő működése.

1.7.9.1.3. Személyekhez kapcsolódó kockázatok

- Véletlen, vagy szándékos felhasználói hibák.
- Jogosultságkezelés hiányosságai.

1.7.9.1.4. Más szervezetekhez kapcsolódó kockázatok

- Megbízhatatlan, nem minősített vagy túlzottan centralizált beszállítók.
- Szerződéses kötelezettségek nem teljesítése.
- Harmadik fél által okozott adat- vagy rendszerbiztonsági incidensek.
- Késedelmes vagy hibás szállítás.

1.7.9.1.5. Személyes adatok kezelésével kapcsolatos kockázatok

- Jogszabályoknak (GDPR) való nem megfelelés;

- Személyes adatokhoz való illetéktelen hozzáférés;
- Adatvesztés vagy adatmanipuláció.

1.7.9.2. Kockázatkezelés-és csökkentés módszerei

1.7.9.2.1. Megelőző intézkedések

- Informatikai biztonsági szabályzatok alkalmazása.
- Jogosultságok szabályozása, naplózás bevezetése.
- Biztonságtudatossági képzések, rendszeres oktatás.
- Beszállítói minősítési rendszer alkalmazása.
- Szerződéses biztonsági követelmények érvényesítése.

1.7.9.2.2. Észlelő intézkedések

- Rendszeres audit elvégzése, naplóelemzések.
- Felügyeleti rendszerek, behatolásérzékelők használata

1.7.9.2.3. Reagáló és helyreállító intézkedések

- Incidenskezelési eljárások tervezése, használata.
- Adatmentés és helyreállítás - tervek és folyamatok kidolgozása.
- Incidenskezelési tervek az ellátási láncra is

1.7.9.3. A Stratégia szervezeten belüli alkalmazása

Jelen IT kockázatmenedzsment-stratégia alkalmazása a szervezet minden szintjén kötelező. Ennek érdekében minden szervezeti egységnek azonos elvek szerint kell eljárnia a kockázatok kezelésében. A kockázatok értékelését és dokumentálását egységes módszertan szerint kell végezni. A szervezeten belül kijelölésre kerülnek a kockázatkezelésért felelős személyek (Lásd: IBSZ 1.6 Szerep- és felelősségi körök).

1.7.9.4. Felülvizsgálat és aktualizálás

A stratégiát legalább évente egy alkalommal felül kell vizsgálni, hogy alkalmazkodni tudjon a szervezeti változásokhoz, a technológiai és szabályozási környezet változásaihoz, valamint az újonnan felmerülő kockázatokhoz.

Az eseti módosításának, felülvizsgálatának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az informatikai rendszerek biztonságáért felelős személy (továbbiakban: EIBF) feladata.

1.7.10. ENGEDÉLYEZÉSI FOLYAMATOK MEGHATÁROZÁSA

Új EIR bevezetése, meglévő módosítása vagy kivezetése csak az IT vezető előzetes jóváhagyásával történhet. A cél, hogy minden ilyen döntés előtt átgondolják a lehetséges biztonsági kockázatokat, és azok kezelése biztosított legyen. A kockázatok kezelésével konkrét felelősökét kell meghatározni.

1.7.11. SZERVEZETI MŰKÖDÉS ÉS ÜZLETI FOLYAMATOK MEGHATÁROZÁSA

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

1.7.12. BIZTONSÁGI SZEMÉLYZET KÉPZÉSE

A biztonsági személyzet képzését és fejlesztését az oktatási tematika részévé kell tenni.

1.7.13. TESZTELÉS, KÉPZÉS ÉS FELÜGYELET

Éves szinten, dokumentáltan el kell végezni az EIR-hez kapcsolódó biztonsági teszteléseket, képzéseket és felügyeleti tevékenységeket.

1.7.14. SZAKMAI CSOPORTOKKAL ÉS KÖZÖSSÉGEKKEL VALÓ KAPCSOLATTARTÁS

Az EIBF feladata a Nemzeti Kiberbiztonsági Intézettel (NKI)/Szabályozott Tevékenységek Felügyeleti Hatóságával (SZTFH) történő kapcsolattartás. Amennyiben valamely esemény kapcsán szükséges, úgy a következő szervezetekkel történő kapcsolattartás is szükséges lehet:

1. Nemzeti Média- és Hírközlési Hatóság (NMHH)
   Kapcsolat az elektronikus kommunikáció biztonsága és az adatvédelem terén.
2. Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)
   A DPO mellett az adatvédelmi előírások betartása és az adatvédelmi incidensek kezelése érdekében.
3. Nemzeti Bűnüldözési Ügynökség (NBU)
   A kibertérben elkövetett bűncselekmények elleni küzdelem és az információbiztonsági incidensek nyomozása és kezelése érdekében.

A Szervezet a jogszabályban meghatározottak szerint bejelentette a Nemzeti Kibervédelmi Intézet részére az EIBF azonosító adatait, ezzel megteremtette kapcsolattartás feltételeit az információbiztonság felügyeletével megbízott kormányzati szervekkel is.

Az EIBF-nek folyamatosan figyelemmel kell kísérnie a fenti szervezetek által kiadott riasztásokat és gondoskodnia kell az EIR-re vonatkozó megfelelő ellenintézkedésekről és válaszlépésekről.

Amennyiben a riasztás érinti a Szervezet felhasználóit, akkor az EIBF elektronikus levélben értesíti a felhasználókat a riasztásban foglaltakról, a megtett védelmi intézkedésekről, valamint felhívja a felhasználók figyelmét a felhasználói oldalról követendő magatartásra.

1.7.15. FENYEGETETTSÉG TUDATOSÍTÓ PROGRAM

A Szervezet felismerte a növekvő információbiztonsági fenyegetésekre való tudatosítás fontosságát, ezért bevezeti a Fenyegetettség tudatosító programot a szervezeten belül. A program célja:

a) Fenyegetések Felderítése
   A program a legújabb információbiztonsági fenyegetéseket és támadási módszereket követi, és folyamatosan frissíti a kapcsolódó fenyegetési információkat.
b) Információmegosztás Szervezeten belül
   Az informatikai üzemeltetés és a felhasználók között létrehoz egy hatékony információmegosztási rendszert, amely lehetővé teszi biztonsági szakemberek és a felhasználók számára a legújabb fenyegetésekről szóló információk cseréjét.
c) Tudatosság növelése
   A munkatársak és a vezetőség részére tart tréningeket és tudatosságnövelő programokat, hogy felismerjék a legfrissebb fenyegetéseket, és megfelelően tudjanak rájuk reagálni.
d) Kapcsolat a Szakmai szervezetekkel

Folyamatos kell legyen a kapcsolat a Kibervédelemmel foglalkozó közösséggel, beleértve a szakmai szervezeteket és a kormányzati szerveket, hogy időben meg tudják osztani egymással az információkat az aktuális fenyegetésekről.

Ezen program bevezetése révén a Szervezet aktívan részt vesz az információbiztonság iránti tudatosság növelésében, és hatékonyan reagál a folyamatosan változó információbiztonsági kihívásokra.

1.7.16. KOCKÁZATKEZELÉSI KERETRENDSZER, KOCKÁZATKEZELÉSÉRT FELELŐS SZEREPKÖRÖK

A kockázatkezelési keretrendszer a 15. Kockázatkezelés fejezetben, a kockázatkezelésért felelős szerepkörök pedig az 1.6.2 Kockázati szerepkörök pontban kaptak helyet.

1.7.17. ELLÁTÁSI LÁNC KOCKÁZATKEZELÉSI STRATÉGIÁJA

Rangsorolni és értékelni kell azokat a beszállítókat, amelyek kritikus technológiákat, termékeket és szolgáltatásokat szállítanak a Szervezet alapvető feladatainak ellátásához. Ez a stratégia összhangban van az üzletmenet-folytonossági tervvel (BCP) és a kockázatkezelési eljárásokkal.

Ellátási lánc kockázatkezelési folyamata:

1.7.17.1. AZONOSÍTÁS

A Szervezet azonosítja azokat a külső partnereket, szolgáltatókat és rendszerelemeket, amelyek működés szempontjából kritikus szolgáltatást biztosítanak.

1.7.17.2. ÉRTÉKELÉS

A beszállítók értékelését el kell végezni. Szempontkét figyelembe kell venni a következőket:

- általuk kezelt, vagy elérhető információk
- szolgáltatás elérhetősége
- esetleges korábbi incidensek

1.7.17.3. KEZELÉS

Magas kockázatú partnerek esetében biztonsági követelményeket kell előírni. Különösen a hozzáférés-felügyelet, a naplózás és a titkosítás a prioritás.

Szerződésben kell rögzíteni az incidens-jelentési és együttműködési kötelezettségeket. Ezen partnerek esetében rendszereres beszállítói értékelést kell végezni.

Szükség esetén helyettesítő szolgáltatót kell kijelölni

1.7.17.4. MONITORING

Legalább éves szinten felül kell vizsgálni az ellátási lánccal kapcsolatos kockázatokat. Ezen felülvizsgálat szempontjai között kell, hogy szerepeljenek a következők:

- szolgáltatásokban felmerülő változások

- bekövetkezett incidensek, vagy SLA-sértések
- jogszabályi környezet változásai, vagy szervezeti környezet változása

1.7.17.5. DOKUMENTÁLÁS

A tevékenységek kapcsán dokumentálni, illetve vezetni kell

- a beszállítói nyilvántartást
- értékelési táblázatot
- elfogadott kockázatokat, illetve megtett intézkedéseket

1.7.18. FOLYAMATOS FELÜGYELETI STRATÉGIA

A stratégia célja, hogy a szervezet az információs rendszerek, hálózatok és szolgáltatások működését folyamatosan figyelje, észlelje a biztonsági eseményeket és szabálytalanságokat, valamint időben reagáljon azokra a szervezet információvagyonának védelme érdekében.

A szervezet folyamatos felügyelete kiterjed az alábbi rendszerekre és tevékenységekre:

- Hálózati infrastruktúra (routerek, tűzfalak, switchek, VPN-kapcsolatok)
- Szerverek (Windows)
- Alkalmazások, adatbázisok és NAS rendszerek
- Felhasználói tevékenység, bejelentkezések, jogosultság-használat
- Biztonsági megoldások (AV)

Folyamatos felügyeleti folyamat

1.7.18.1. MEGFIGYELÉS ÉS ADATGYŰJTÉS

A Szervezet manuális napló- és eseménygyűjtési folyamatot működtet, amely során:

- a kritikus eseményeket (sikeres/sikertelen bejelentkezések, hálózati vagy rendszeranomáliák, jogosulatlan hozzáférési kísérletek) a kijelölt felelősök időszakos kézi ellenőrzéssel azonosítják,
- a rendszerek üzemállapotát, elérhetőségét és teljesítményét az üzemeltetés kézi ellenőrzéssel vizsgálja,
- a naplók kézi letöltése és archiválása történik, a megőrzési rendnek megfelelő, időbélyeggel ellátott mappastruktúrában.

1.7.18.2. ÉSZLELÉS ÉS RIASZTÁS

- A rendellenességek felismerése kézi naplóellenőrzéssel, rendszerüzemeltetői vizsgálattal és a felhasználók által jelzett hibák alapján történik.
- A túlterhelések, működési problémák és biztonsági események észlelése nem valós időben, hanem rendszeres manuális vizsgálat vagy bejelentés útján valósul meg.
- A potenciális támadások azonosítása a naplóadatok kézi értelmezése és egyszerű ellenőrző listák alapján történik.
- Riasztást a kijelölt személyek telefonon, e-mailen vagy hibajegyben kezdeményeznek.

1.7.18.3. ÉRTÉKELÉS ÉS REAGÁLÁS

- Az azonosított eseményeket a Biztonsági események kezelése eljárásrend szerint osztályozzák, értékelik és kezelik.

- Súlyos események esetén az EIBF értesítése és a vészhelyzeti csoport aktiválása történik.
- A reagálás eredményeit minden esetben dokumentálni kell.

1.7.18.4. JELENTÉS ÉS FELÜLVIZSGÁLAT

- Rendszeres biztonsági jelentések készülnek a naplózott eseményekről.
- Évente legalább egyszer felülvizsgálatra kerül a felügyeleti rendszer hatékonysága és lefedettsége.

A tapasztalatok alapján a Szervezet módosíthatja a naplózási és monitorozási szabályzatokat.

1.8. EGYÉB ELŐÍRÁSOK

1.8.1. ESZKÖZÖK ÁTADÁSA MUNKAVISZONY LÉTESÍTÉSEKOR

Az eszközök átadásának folyamatát minden esetben dokumentálni kell.

1.8.2. JELSZÓHASZNÁLAT, -BIZTONSÁG

A munkaállomások és hálózati erőforrások használatához jelszó használata kötelező.

A jelszavak minimális hossza 8 karakter, tartalmaznia kell min. 1 kis betűt, 1 nagybetűt, 1 számot és 1 speciális karaktert is. (lásd 8.21. A hitelesítésre szolgáló eszközök kezelése pont)

A jelszavakat legfeljebb 180 naponta kötelező megváltoztatni. (lásd 8.21. A hitelesítésre szolgáló eszközök kezelése pont)

A rendszergazdai jogosultsággal rendelkező felhasználók felhasználó nevüket és jelszavukat zárt borítékban kötelesek elhelyezni a Szervezet páncélszekrényében.

1.8.3. ADATBIZTONSÁG

Az archivált adatokat, és a biztonsági mentéseket, azonos biztonsági szinten kell kezelni, mint a használatban lévő adatokat, nyilvántartásokat.

A mentésekhez használt berendezéseket, eszközöket, informatikai „üresség" vizsgálat nélkül, selejtezni, értékesíteni tilos.

1.8.4. MUNKAÁLLOMÁSOK VÉDELME

A munkaállomásokon egyedi vírusvédelmi szoftvereket kell futtatni. A szoftver beállítása és frissítése egyedileg történik. (lásd: 18.8. Kártékony kódok elleni védelem pont)

A munkaállomásokat jelszóval kell védeni.

A képernyővédőt jelszóval kell védeni. A képernyővédőt automatikusan aktiválni kell 10 perc inaktivitás után.

A munkaállomások merevlemezei csak a rajta található adatok végleges és biztonságos megsemmisítését követően selejtezhetők. Az adatok megsemmisítéséről jegyzőkönyvet kell felvenni. (lásd: 11.8. Adathordozók törlése pont)

1.8.5. HORDOZHATÓ ESZKÖZÖK VÉDELME

A felhasználók számára kiadott hordozható eszközök (notebook, mobiltelefon, hordozható adattároló) biztonságos tárolásáért, lopás és elvesztés elleni védelméért a felhasználó felel.

A hordozható eszközökre érzékeny, személyes, titkos adatot másolni tilos a meghajtó teljes titkosítása nélkül!

Hordozható eszközök csak a rajta található adatok végleges és biztonságos megsemmisítését követően selejtezhetők. Az adatok megsemmisítéséről jegyzőkönyvet kell felvenni. (lásd: 11.8. Adathordozók törlése pont)

2. HOZZÁFÉRÉS-FELÜGYELET

2.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Ezen eljárásrendnek a középpontjában azok a meghatározott célok állnak, amelyeket el kell érni a hozzáférés-felügyelet terén, például az adatbiztonság növelése vagy a jogosultságok megfelelő kezelése. Továbbá szabályozza, hogy a hozzáférés-felügyeleti eljárások mely területekre és rendszerekre vonatkoznak, valamint meghatározza az egyes szereplők, mint például a Felhasználók vagy a Rendszergazdák, felelősségi körét és jogosultságait ezen a területen. Biztosítja, hogy a szabályzat és az eljárásrendek megfeleljenek a vonatkozó jogszabályoknak, irányelveknek és szabályozásoknak.

Felelős: EIBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

2.2. FIÓKKEZELÉS

Az EIR-hez történő hozzáférés szempontjából a következő fióktípusok kerültek megkülönböztetésre:

1. felhasználói fiókok;
2. névre szóló rendszergazdai fiókok;
3. beépített rendszergazdai fiókok;
4. technikai felhasználói fiókok.

A felhasználói fióktípusba tartoznak az EIR-rel dolgozó, „normál" felhasználók fiókjai. Azonosításuk és hitelesítésük egyedileg, névre szólóan kell, hogy történjen. Jogosultságuk korlátozott, kizárólag az üzleti folyamatokhoz kapcsolódó feladataik elvégzéséhez szükséges jogosultságokkal rendelkezhetnek.

A névre szóló rendszergazdai fiókok az EIR felügyeletére, adminisztrálására (pl.: a rendszer paramétereinek karbantartására, hozzáférési jogosultságok kezelésére, a rendszer működésének felügyeletére stb.) szolgálnak, amelyhez kiemelt jogosultságok biztosítása szükséges. A fióktípusba kizárólag az Informatika csoport informatikai rendszer felügyeletével megbízott, Rendszergazda szerepkörben dolgozó munkatársai tartozhatnak, akiket egyedileg, névre szólóan kell azonosítani.

Amennyiben a Rendszergazda felhasználóként is használja a rendszert, úgy a felhasználói tevékenységet külön (nem kiemelt jogosultságú) felhasználói fiók alatt kell végeznie.

A beépített rendszergazdai fiókok alatt a szoftverek és hardver eszközök kiemelt jogosultságú, gyárilag beépített rendszergazdai fiókjait (pl.: admin, administrator, root, superuser, sa, stb.) értjük, amelyek segítségével a rendszerelem felügyelhető, adminisztrálható.

A beépített rendszergazdai fiókok közös használatú fiókoknak számítanak, ezért tilos a használatuk, helyettük a rendszerelemet felügyelő rendszergazdáknak névre szóló rendszergazdai fiókokat kell létrehozni. Ugyanakkor a beépített rendszergazdai fiókokat nem szükséges letiltani vagy törölni, mert biztonsági tartalék céljából szükség lehet rájuk.

Technikai felhasználói fiókokról beszélünk, amikor egy felhasználói fiók nem személyhez kötődik, hanem egy szoftverhez, szolgáltatáshoz vagy hardver eszközhöz, amely belsőleg használja a fiókot valamely más rendszer szolgáltatásának eléréséhez (pl.: egy alkalmazói szoftver használja adatok tárolásához az adatbáziskezelő szerveren, vagy egy multifunkciós nyomtató szkennelt dokumentumok e-mail-ben történő küldéséhez; stb.). Ezek a fiókok nem igényelnek feltétlenül kiemelt, rendszergazdai jogosultságot, csak azt, ami az adott feladat ellátásához szükséges.

A technikai felhasználói fiókok a szoftverek/hardver eszközök belső működésére vannak fenntartva, személyek általi használatuk tilos! Ez alól kivételt képez a technikai felhasználói fiók tesztelése, ami engedélyezett az EIR fejlesztői és üzemeltetői számára.

Ugyancsak tilos névre szóló felhasználói vagy rendszergazdai fiókokat technikai felhasználói fiókként használni, mert ha a fiók tulajdonosának jogosultsága megszüntetésre kerül, úgy leáll az a szolgáltatás, amely az adott fiókra épül.

Valamennyi fióktípust az EIR kijelölt rendszergazdája kezeli (létrehozza, módosítja, megszünteti a fiókokat), viszont a névre szóló és a beépített rendszergazdai fiókok kezeléséhez az IT vezető engedélyezése szükséges.

Az EIR hozzáférési jogosultságainak kezelésénél alapelvként kell érvényesíteni, hogy a szoftverek menüpontjaihoz, funkcióihoz, illetve a fájlrendszer mappáihoz, fájljaihoz kapcsolódó elemi jogosultságokat nem közvetlenül kell egy-egy felhasználóhoz rendelni, hanem ezekből az elemi jogosultságokból jogosultsági csoportokat kell képezni és a csoportok tagjai közé kell a felhasználókat felvenni.

A jogosultsági csoportok alkalmazása áttekinthetőbbé teszi a jogosultságok rendszerét és leegyszerűsíti a hozzáférési jogok igénylését és kiadását (nagyszámú elemi jogosultság helyett, kevesebb jogosultság csoporttal kell foglalkozni).

A jogosultsági csoportok elvét akkor is követni kell, ha a csoportnak jelenleg egy felhasználó lesz a tagja, és fölösleges adminisztrációnak tűnik a csoport létrehozása, mert pl. a fájlrendszer jogosultságok esetén könnyebben lekérdezhetővé válik, hogy egy felhasználónak milyen mappákhoz van jogosultsága, és könnyebben visszavonható lesz a jogosultság vagy kiadható lesz más felhasználónak. Ez alól funkciójuknál fogva kivételt képeznek a felhasználók személyes használatára létrehozott mappái (a felhasználók „home" mappája).

A jogosultsági csoportokat olyan szemlélettel kell kialakítani, hogy megfeleltethető legyen a felhasználók munkaköri feladatellátásának, az EIR-ben betöltött szerepkörüknek (pl.: beszerző, főkönyvelő, pénztáros, pénzügyi előadó stb.). A csoportok kialakítása során biztosítani kell, hogy a csoport csak a szerepkör feladatellátásához szükséges és elégséges jogosultságokat tartalmazza.

A jogosultsági csoportokat egy rövid leírás hozzáfűzésével kell dokumentálni, amely a csoport nevén túl bővebben utal arra, hogy a csoport mire vonatkozik. A jogosultsági csoportok listáját és a csoportok leírását a felhasználók rendelkezésére kell bocsájtani segítségképpen a hozzáférési jogosultságok (jogosultsági csoportok) igényléséhez.

A Szervezet EIR-hez kizárólag olyan személy kaphat hozzáférést, akinek a munkájához szükséges az EIR használata, és aki megismerte és dokumentáltan elfogadta a rendszerre vonatkozó hozzáférési szabályokat, valamint:

a. a Szervezet alkalmazottja (rögzítésre került a Szervezet munkaügyi rendszerében), vagy;

b. informatikai rendszerüzemeltetési szerződéssel rendelkező cég alkalmazottja (ideértve az Informatika csoport külsős munkatársait), vagy;
c. a Szervezettel megbízási vagy vállalkozási szerződéses kapcsolatban álló magánszemély, egyéni vállalkozó vagy cég alkalmazottja, vagy;
d. a Szervezetnél munkát vagy más tevékenységet folytató, érvényes szerződéssel rendelkező hallgató, illetve gyakornok.

Azok a felhasználók, akik nem a Szervezet alkalmazottjai csak az IT vezető tudtával és jóváhagyásával kaphatnak hozzáférést. Csak valós, aktív munka- vagy szerződéses viszonyban álló személyeket lehet regisztrálni a rendszerben.

A jogosultságok kezelésekor alapelvként kell érvényesíteni, hogy csak a felhasználók feladatellátásához szükséges és elégséges mértékű jogosultságok biztosíthatók.

A munkahelyi vezetők feladata, hogy a beosztott munkatársaikra vonatkozóan megkérjék azokat a hozzáférési jogosultságokat, amelyek az EIR használatához kapcsolódóan a munkatársak feladatellátásához szükségesek.

A beosztott munkatársak feladatkörében vagy az EIR-ben bekövetkező változások esetén a munkahelyi vezetőknek felül kell vizsgálniuk a munkatársak hozzáférési jogosultságait és kezdeményezniük kell a szükségtelen jogosultságok visszavonását, illetve új jogosultságok kiadását.

A Szervezettől kilépő alkalmazottak hozzáférési jogosultságának megszüntetését a Munkaügyi ügyintéző kezdeményezi.

Az EIR kulcsfelhasználónak 3 havonta felül kell vizsgálnia a felhasználói fiókokat, és ellenőriznie kell, hogy minden kilépő alkalmazott hozzáférési jogosultsága megszüntetésre került-e.

A felhasználói fiókok felülvizsgálata céljából a Munkaügyi ügyintéző az Informatika csoport kérésére annak rendelkezésére bocsájtja a Szervezetnél aktuálisan dolgozó alkalmazottak listáját, illetve az elmúlt 3 hónapban kilépettek listáját. Az Informatika csoport betekintést enged a kulcsfelhasználók számára a listába, a hozzáférési jogosultságok felülvizsgálatához.

A fiókok használatát a kulcsfelhasználónak kell nyomon követnie.

A munkahelyi vezetők felelőssége, hogy azonnal értesítsék a kulcsfelhasználókat a következő esetekben:

a) ha az adott Felhasználó hozzáférése a rendszerhez a továbbiakban szükségtelen;
b) ha az adott Felhasználó jogviszonya megszűnik;
c) ha a rendszerhasználathoz szükséges ismeretek megváltoznak.

Csak a következő esetekben engedélyezett a rendszer használata:

a) érvényes hozzáférési engedély birtokában;
b) tervezett rendszerhasználat esetén.

A kilépő alkalmazottakról a Munkaügyi ügyintéző írásban értesíti az Informatika csoportot és a kulcsfelhasználókat, akik megszüntetik az alkalmazottak jogosultságait.

A hozzáférési jogosultságok megszüntetésével egyidejűleg az elektronikus belépőkártyák jogosultságát is meg kell szüntetni, függetlenül attól, hogy a belépőkártya visszaadásra került-e, vagy sem.

A jogosultságok megszüntetéséért a Rendszergazda és a kulcsfelhasználó a felelős.

2.15. HOZZÁFÉRÉS-ELLENŐRZÉS ÉRVÉNYESÍTÉSE

A Szervezetnél csak olyan EIR használható, amely képes a kiadott hozzáférési jogosultságokat érvényesíteni, azaz az EIR-ben kezelt adatokhoz, a rendszerelemekhez csak a megfelelő jogosultsággal rendelkezők férhetnek hozzá.

2.71. SIKERTELEN BEJELENTKEZÉSI KÍSÉRLETEK

A felhasználói azonosító ismeretében a támadók gyakran kísérlik meg a jelszót próbálkozással kitalálni (sokszor nyers erő felhasználásával, azaz egy szótár szavainak vagy az összes lehetőség végig próbálásával).

Ennek a támadásnak kell csökkenteni a hatékonyságát azzal, hogy ha túl sok sikertelen bejelentkezési kísérlet történik egy megadott időn belül, akkor a rendszer egy rövid ideig zárolja a felhasználói fiókot, vagyis nem engedi a bejelentkezést.

Az EIR-nek a következő fiókzárolási házirendet kell alkalmaznia sikertelen bejelentkezési kísérletek esetén:

Szabály megnevezése	Beállított érték	Magyarázat
Fiókzárolás alsó értéke	5 sikertelen próbálkozás	A rendszer ennyi hibás jelszó megadása után zárolja a felhasználói fiókot és tagadja meg a rendszerbe történő bejelentkezést.
Fiókzárolás időtartama	fiók feloldásig	Ennyi ideig kerül zárolásra a felhasználói fiók.
Fiókzárolási számláló nullázása	-	Ha ennyi percig nem történt sikertelen bejelentkezési kísérlet, a rendszer nullázza a sikertelen bejelentkezések számát.

2.75. A RENDSZERHASZNÁLAT JELZÉSE

Az EIR elindításakor – még a bejelentkezés előtt – tájékoztatni kell a felhasználókat a következőkről:

a) a Felhasználó a Szervezet EIR-ét használja;
b) a rendszer használatot a Szervezet figyelheti, rögzítheti, naplózhatja;
c) a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár;
d) a rendszer használatával a Felhasználó elfogadja és tudomásul veszi a fentieket.

A figyelmeztető üzenetet mindaddig a képernyőn kell tartani, amíg a Felhasználó közvetlen műveletet nem végez az EIR-be való bejelentkezéshez vagy további rendszer hozzáféréshez.

2.88. AZONOSÍTÁS VAGY HITELESÍTÉS NÉLKÜL ENGEDÉLYEZETT TEVÉKENYSÉGEK

A Szervezet EIR-ében azonosítás és hitelesítés nélkül semmilyen felhasználói tevékenység nem engedélyezett.

A jelszavas (vagy más) hitelesítésnek ki kell terjednie a szerverekre, valamint minden hálózaton üzemelő és hálózattól független, egyedi munkaállomásra.

A fentek alól kivételt képez a Szervezet Internetes honlapja, amelyen bárki számára hitelesítés nélkül elérhető, publikus információkat helyez el.

2.100. TÁVOLI HOZZÁFÉRÉS

Távoli hozzáférésnek minősül minden olyan hozzáférés a Szervezet EIR-hez, amelyben a kommunikáció egy külső, nem a Szervezet által ellenőrzött hálózaton (pl. Interneten) zajlik.

Távoli elérés kialakítását az Informatika csoportvezetőnek kell engedélyeznie.

Az EIR-hez történő távoli hozzáférés alapesetben az alábbi felhasználók számára biztosítható:

- a Szervezet azon alkalmazottai számára, akik a lassú adatkapcsolattal (pl.: Internet, mikrohullámú kapcsolat) rendelkező telephelyen dolgoznak, vagy munkájuk megköveteli, hogy azt sokféle helyszínen, mobil eszközökkel végezzék;
- infrastruktúra szolgáltatás esetén
- A Szervezet által üzemeltetett szoftverek és rendszerek külsős fejlesztői és rendszertámogatást ellátó partnerek számára

Távoli hozzáférés esetében minimálisan elvárt biztonsági követelmény, hogy a hitelesítés során használt jelszó a hálózaton titkosított formában kerüljön továbbításra, és amennyiben lehetséges a teljes adatforgalmat titkosítani kell.

A távoli hozzáférést alapesetben az általános jogosultságigényléshez leírtak szerint kell igényelni.

A felhasználói körre és hozzáférés igénylésére vonatkozóan az alapesettől való eltéréseket az egyes hozzáférés típusok szabályozása tartalmazza.

A Szervezet távoli hozzáférésre az Internetet használja (a telefonos kapcsolatfelvétel nem támogatott) és az alábbi hozzáférés típusokat alkalmazhatja:

Virtuális magánhálózat (VPN)

A virtuális magánhálózat (VPN) egy nyilvános hálózat (pl. Internet) egyes végpontjai között kiépített logikai hálózat, amelyen keresztülmenő adatok nem láthatók az eredeti hálózaton, mivel titkosított adatcsomagokba vannak csomagolva.

A Szervezet VPN hozzáférést biztosít az alapesetben engedélyezett felhasználók mellett:

- az Informatika csoport Rendszergazda szerepkörben dolgozó munkatársai számára távoli asztal hozzáféréssel kombinálva a többtényezős hitelesítés megvalósításához;

- közvetlen (optikai) adatkapcsolattal nem rendelkező telephelyek és a központi telephely Interneten keresztüli összekötésére (site-to-site VPN);
- indokolt esetben – az IT vezető engedélyével – az EIR-hez támogatást nyújtó külső partnerek számára távoli asztal hozzáféréssel kombinálva.

A VPN kapcsolat titkosított, így az adatok bizalmasságára nézve biztonságos, de a Szervezet hálózatához távolról kapcsolódó számítógép részévé válik a hálózatnak, és ezzel fenyegetést jelenthet a hálózatra nézve (pl. vírusfertőzést okozhat). A kockázatok csökkentése érdekében az alábbiakról kell gondoskodni:

- A VPN hozzáférést úgy kell létrehozni, hogy csak a szükséges rendszerelemek legyenek elérhetők a távolról kapcsolódó számítógépekről.
- A távoli hozzáférés esetében is ugyanazokat a munkaállomásokra vonatkozó biztonsági előírásokat kell betartani, mint a belső hálózatban használt számítógépek esetén (pl.: naprakész vírusvédelmi szoftverrel, telepített biztonsági frissítésekkel, bekapcsolt tűzfallal kell a számítógépnek rendelkeznie).

A telephelyek közötti VPN kapcsolatok a telephely minden felhasználójára érvényesek, a hozzáférést nem kell külön igényelni.

A VPN szerver központi felügyeleti rendszerén a Rendszergazda napi szinten megvizsgálja a regisztrált sikeres vagy sikertelen belépéseket, a szokásostól eltérő aktivitásokról tájékoztatja az IT vezetőt, aki megteszi a szükséges intézkedéseket

Távoli asztal (RDP)

A távoli asztal használatakor amennyiben a hozzáférés során a kliens számítógép egy terminál szerverre csatlakozik és a szerver erőforrásait használja az alkalmazói szoftverek futtatására, úgy a kliens számítógép csak a terminál szerver képernyőjét jeleníti meg, és továbbítja a kliensen végzett billentyűzet és egér műveleteket a szervernek. A Felhasználó gyakorlatilag azt érzékeli, mintha közvetlenül a terminál szerver előtt dolgozna.

A Szervezet távoli asztal hozzáférést biztosít az alapesetben engedélyezett felhasználók mellett:

- az Informatika csoport Rendszergazda szerepkörben dolgozó munkatársai számára rendszerüzemeltetés céljából;
- indokolt esetben – az IT vezető engedélyével – az EIR-hez támogatást nyújtó külső partnerek számára.

A hozzáférés titkosított kapcsolaton keresztül kell, hogy megvalósuljon.

Saját számítógép távoli elérése VPN kapcsolattal, távoli asztallal

- indokolt esetben – az IT vezető engedélyével – a felhasználók saját számítógépükbe távolról bejelentkezhetnek.

Távoli hozzáférést (távtámogatást) biztosító szoftver (TeamViewer, AnyDesk, VNC)

Távoli hozzáférést biztosító szoftver lehetővé teszi egy számítógép, vagy eszköz távoli irányítását egy másik eszközről. A gyártó honlapján regisztrálni kell egy fiókot (a Szervezet által biztosított kapcsolattartási adatokkal – e-mail, a Központi felügyelethez. A kliens(ek)re és az irányító eszközre is telepíteni szükséges a Távoli hozzáférést biztosító szoftvert. A Felhasználó gyakorlatilag azt érzékeli, mintha közvetlenül a távvezérelt eszköz előtt dolgozna.

A Szervezet ilyen módon Távoli hozzáférést biztosít:

- az Informatika csoport Rendszergazda szerepkörben dolgozó munkatársai számára rendszerüzemeltetés céljából;
- indokolt esetben az otthoni munkavégzéssel, vagy távmunkával dolgozó, engedélyezett felhasználók számára;
- különösen indokolt esetben – az IT vezető engedélyével – az EIR-hez támogatást nyújtó külső partnerek számára.

A hozzáférés minden esetben titkosított kapcsolaton keresztül valósul meg, ezen kapcsolat létrehozása a Távoli hozzáférést biztosító szoftver feladata.

Elvárás, hogy a távoli bejelentkezésnél biztosított legyen, hogy a Felhasználó tudomással bírjon a távoli hozzáférés megtörténtéről, maga engedélyezze.

2.108. VEZETÉK NÉLKÜLI HOZZÁFÉRÉS

A Szervezet a következőkben leírtak szerint elkülönített vezeték nélküli hozzáférést biztosíthat az alkalmazottai és a vendégek számára a Szervezet telephelyeire vonatkozóan.

Az alkalmazottak és vendégek WiFi hozzáférésére vonatkozó védelmi intézkedések beállítása a Rendszergazda feladata. Amennyiben egy WiFi hozzáférésre a továbbiakban nincs szükség, annak letiltása a Rendszergazda feladata.

Alkalmazottak

Kizárólag az alkalmazottak számára a Szervezet a belső hálózatra történő kapcsolódáshoz legalább IEEE 802.11n szabványnak megfelelő (WiFi) vezeték nélküli hozzáférést biztosít a Szervezet tulajdonában levő mobil eszközökön.

A vezeték nélküli hozzáférésnél az alábbi módon kell gondoskodni az illetéktelen használat megelőzéséről:

- A vezeték nélküli WiFi eszközön (hozzáférési ponton/routeren) WPA2/WPA3 protokollt kell alkalmazni (a sok esetben alapértelmezett, bizonyítottan könnyen feltörhető WEP protokoll használata kifejezetten tilos).
- A vezeték nélküli hozzáféréshez legalább 9 karakter hosszú, a felhasználói jelszó kiválasztására vonatkozó szabályoknak megfelelő, véletlenszerűen generált hozzáférési kulcsot kell beállítani.
- A hozzáférési kulcsokat a rendszergazdának 365 naponta meg kell változtatnia, és ezt dokumentálnia.
- A hozzáférési kulcsokat az informatikai csoport a beépített adminisztrátori jelszavakkal megegyező módon tárolja.
- A kulcsok kezelésére a fenti eltéréssekkel a felhasználói jelszavakra vonatkozó előírások és biztonsági intézkedések vonatkoznak.

- A WiFi eszközön le kell tiltani a WiFi Protected Setup (WPS) használatát, amely a hozzáférési kulcs ismerete nélkül is lehetővé tenné az eszközökhöz való kapcsolódást.
- A WiFi eszköz web-es adminisztrálási felületének eléréséhez tikosított (HTTPS) kapcsolatot kell alkalmazni az alapértelmezett menedzsment-port megváltoztatásával.
- A rendszerbe csak olyan céges eszköz csatlakozhat be, amelynek csatlakozását az IT vezető előzetesen engedélyezte és a hálózaton regisztrálva lett (MAC azonosítóval). A becsatlakozott eszközök felügyelete a Rendszergazda feladata.
- A Wifi hozzáférés AD authentikációval is megvalósítható.

A belső hálózathoz való vezeték nélküli hozzáférés mobil eszközön történő beállítását az Informatika csoporttól a HelpDesken kell igényelni. A beállítás csak az IT vezető írásos jóváhagyásával történhet.

Vendégek

A Szervezet a vendégei számára az Internet elérését legalább IEEE 802.11n szabványnak megfelelő (WiFi) vezeték nélküli hozzáféréssel biztosítja.

A vendégek biztonságos vezeték nélküli kapcsolódása érdekében a következőkről kell gondoskodni:

- Külön a vendégek számára fenntartott, és a kapcsolódó eszközök számára láthatóvá tett (broadcast-olt) WiFi hálózati nevet (SSID) kell létrehozni.
- A WiFi eszköz web-es adminisztrálási felületének eléréséhez tikosított (HTTPS) kapcsolatot kell alkalmazni az alapértelmezett menedzsment-port megváltoztatásával.
- A vendég WiFi forgalmát logikailag (VLAN) vagy fizikailag (másodlagos ISP) el kell különíteni a belső hálózattól.
- Logikailag elkülönített hálózatok esetén:
    - A WiFi eszközön legalább WPA2/WPA protokollt kell alkalmazni (a WEP protokoll használata kifejezetten tilos).
    - A WiFi eszközön le kell tiltani a WiFi Protected Setup (WPS) használatát.
- Fizikailag elkülönített hálózatok esetén:
    - Egyszerű jelszó használata megengedett.

A vendégek Internet eléréséhez szükséges kulcsot az informatika csoport adja ki az IT vezető jóváhagyásával.

2.113. MOBIL ESZKÖZÖK HOZZÁFÉRÉS-ELLENŐRZÉSE

A Szervezet EIR-hez mobil eszközről történő hozzáférésnél a telephelyen belüli vezeték nélküli hozzáférés esetén a Vezeték nélküli hozzáférés pont, az Interneten keresztüli távoli hozzáférés esetén a Távoli hozzáférés pont rendelkezései szerint kell eljárni.

Mobil eszközökkel történő hozzáférés csak a Szervezet tulajdonában lévő mobil eszközökről engedélyezett. Ezeken kötelező a VPN használata.

A mobil eszközök esetén nagyobb valószínűséggel fordulhat elő az eszköz elvesztése vagy eltulajdonítása. A kockázatok csökkentése érdekében az alábbiakról kell gondoskodni:

- A hordozható számítógépeket felhasználói azonosítás nélkül használni tilos;

- A hordozható számítógépek háttértárolóját titkosítani kell (pl. Windows operációs rendszer esetén a beépített BitLocker funkció használatával). A számítógép üzembe helyezési folyamatának részét kell képeznie a titkosítás beállításának.
- A mobiltelefonokhoz, PDA-khoz, táblagépekhez való hozzáférést képernyő mintával vagy PIN kóddal (amely nem azonos a SIM kártya feloldásához alkalmazott PIN kóddal) kell védeni. Ennek beállítása az eszköz használójának a feladata, de HelpDesken bejelentve segítség kérhető az Informatika csoporttól.
- A mobiltelefonok, PDA-k, táblagépek elvesztése vagy eltulajdonítása esetén gondoskodni kell az eszköz tartalmának távolról történő törléséről.
- A mobil eszközök elvesztését vagy eltulajdonítását a Munkahelyi vezetőnek jelenteni kell.

2.115. KÜLSŐ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK HASZNÁLATA

A Szervezet a külső EIR-ek használatát csak akkor engedélyezi, ha azokban is érvényesülnek az IBSZ-ben megfogalmazott biztonsági elvárások, illetve, ha az adatgazda engedélyezte.

A Szervezet felhasználóinak a hozzáférését külső rendszerekhez, a külső EIR adatgazdája engedélyezheti, ha a munkavégzéshez szükséges.

Ha a Szervezet adatfeldolgozói tevékenységet végez külső rendszerekben, annak részleteit és biztonsági követelményeit szerződésben kell rögzíteni (Adatfeldolgozói szerződés)

Minden egyéb külső rendszer használata tilos!

A fentiek előírások alól kivételnek tekinthető olyan külső rendszer használata, amire jogszabály kötelezi a Szervezetet.

2.124. NYILVÁNOSAN ELÉRHETŐ TARTALOM

A Szervezet az Internetes honlapján, illetve a hivatalos, szociális média oldalán bárki számára elérhető, publikus információkat tesz közzé.

Az információk közzétételére csak a Szervezet vezetője által kijelölt személyek jogosultak. Az ő engedélye nélkül semmilyen információ nem tehető közzé.

Az Adatvédelmi felelős áttekinti a közzétenni kívánt tartalmat annak érdekében, hogy ellenőrizze, nem tartalmaznak nem nyilvános információkat.

Az adatvédelmi felelős további feladata, hogy 30 naponta áttekintse a publikált tartalmakat, és amennyiben nem nyilvános információt talál, úgy azt eltávolítja.

A Szervezet hivatalos honlapja: https:/kiskore.hu

3. TUDATOSSÁG ÉS KÉPZÉS

3.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend meghatározza a tudatosság és képzés területén elérni kívánt célokat és feladatokat. Ez magában foglalja az információbiztonsági szabályok betartásának növelését és az adatvédelem iránti tudatosság fejlesztését.

Kiemelten kezeli a vezetők szerepét és elkötelezettségét ezen a területen. Fontos, hogy összhangban legyen a vonatkozó jogszabályokkal és szabványokkal. Emellett rögzíti, hogy milyen szankciók vagy intézkedések léphetnek érvénybe a szabályok megsértése esetén. A szabályzat folyamatos frissítése és könnyű elérhetősége minden alkalmazott számára biztosítja a hatékony és megfelelő tudatosság és képzés fenntartását.

Felelős: EIBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

3.2. BIZTONSÁGTUDATOSSÁGI KÉPZÉS

A képzések célja

Az Információ biztonsági képzések alapvető célja a munkatársak, és a szabályzat hatálya alá tartozók ismereteinek bővítése, frissítése. A képzési és tudatossági tananyagot éves szinten frissíteni szükséges. A belső és külső biztonsági eseményekből levont tanulságot is be kell építeni a képzésekbe.

A képzésekkel szembeni elvárások, képzések fajtái:

a) Betanító képzés:
Célja az új vagy áthelyezett Felhasználó megismertetése a rendszerrel, és az informatikai szabályokkal. A kezdeti képzések keretében kell megtartani egyénileg, vagy csoportosan.
b) Szinten tartó képzés:
Célja az ismeretek felfrissítése, a jogszabályváltozások követése, a technikai változások megismerése, amennyiben a rendszert érintő változások megkövetelik. A képzés anyaga épülhet a Szervezetben tapasztalt események elemzésére is.
c) Fejlesztő képzések:
Az információbiztonság témakörére épített tréning jellegű képzés, az elvárt magatartások begyakorlása, és a várható események kezelése, az oktatási anyag része. A képzés irányulhat a technikai változások beillesztésére való felkészülésre, a logikai változások tanulmányozására.

A képzés témakörei:

A képzésen a következő témaköröket kell minimálisan érinteni:

a) Információbiztonsági alapfogalmak;
b) Támadási formák;
c) számítógépes kártevők fajtái;
d) ember által elkövetett támadások fajtái;

e) Vonatkozó jogszabályok, szabályzatok;
f) Felhasználók feladatai, felelőssége és jogai;
g) Biztonsági események felismerése és jelentése;
h) Az Internet és az elektronikus levelezés biztonsága;
i) Vírusok és egyéb kártevők elleni védelmi intézkedések;
j) A hibák, üzemzavarok bejelentések menete;
k) Jogosultsági rendszer, jogosultság igénylés folyamata;

Az EIR-hez való hozzáférés engedélyezésére, vagy kijelölt feladat végrehajtására csak a képzésen való részvételt követően kerülhet sor.

3.4. BIZTONSÁGTUDATOSSÁGI KÉPZÉS – BELSŐ FENYEGETÉS

A Fejlesztő képzéseknek ki kell térniük a belső fenyegetések potenciális jeleinek felismerésére és jelentésére is.

3.9. SZEREPKÖR ALAPÚ BIZTONSÁGI KÉPZÉS

Kiemelt fontosságú, hogy a speciális szerepkörökben, vagy speciális feladatot végző munkavállalók ne csak általános, hanem szerepkör alapú biztonsági képzést kapjanak.

Ilyen kiemelt szerepkörök:

a) Felsővezetők;
b) Adatgazdák;
c) Rendszergazdák/Rendszerüzemeltetők

Számukra az általános képzésen túl szerepkörre, vagy feladatkörre irányuló képzést szükséges tartani!

Az EIR-hez való hozzáférés engedélyezésére, vagy kijelölt feladat végrehajtására csak a képzésen való részvételt követően kerülhet sor.

A biztonsági személyzetnek az EIR-ben bekövetkezett változások esetén minden esetben haladéktalanul képzésben kell részesülnie.

3.13. A BIZTONSÁGI KÉPZÉSRE VONATKOZÓ DOKUMENTÁCIÓK

A Szervezetnek a többi képzéssel együtt dokumentálnia kell biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket. A dokumentumoknak tartalmazniuk kell:

a) Az oktatás tematikáját
b) Az oktatás anyagait (ppt)
c) Az oktatás helyét és idejét
d) A résztvevők felsorolását és aláírását
e) Az oktató megnevezését, és aláírását.

A Szervezet a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és a dokumentumokat megőrzi legalább 5 évig.

4. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

4.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend feladata a Szervezet belső folyamatainak és tevékenységeinek rögzítése, nyomon követése és ellenőrzése. Ennek révén biztosítja az átláthatóságot, az események követését, valamint az esetleges hibák vagy visszaélések azonosítását és kezelését. Emellett segíti a jogszabályoknak való megfelelést és a biztonságot. A szabályzat további célja, hogy elősegítse az elszámoltathatóságot, azaz az egyének és csoportok felelősségének és számadási képességének biztosítását a tevékenységeikért és döntéseikért.

A naplózás során az EIR automatikusan rögzíti az eseménynaplóban a rendszerben bekövetkező eseményeket, hibákat, felhasználói tevékenységeket és ezek időpontját.

A naplózás lehetővé teszi a változások észlelését, a felhasználók számon kérhetőségét, és elengedhetetlen a biztonsági események kezeléséhez.

Felelős: EIBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

4.2. NAPLÓZHATÓ ESEMÉNYEK

A naplózásnak az EIR kapcsolódó környezetére is ki kell terjednie, vagyis az alkalmazói szoftverek mellett a szerverek, hálózati eszközök, határvédelmi eszközök és egyéb biztonsági eszközök esetén is engedélyezni kell a naplózást.

Biztosítani kell, hogy az EIR és kapcsolódó környezetük naplózni tudják a következő eseményeket:

a) a felhasználók be- és kijelentkezését a rendszerbe (beleértve mind a sikeres, mind a sikertelen belépési kísérleteket);
b) a Rendszergazdák a rendszer bármely rétegébe történő be-és kijelentkezését;
c) a Rendszergazdák tevékenységét a rendszer bármely rétegében;
d) a felhasználói fiókok és jogosultságok módosítását;
e) a konfigurációs beállítások módosítását;
f) az alkalmazói szoftverekben az adatállományok (adatbázisok) módosítását;
g) a rendszer eseményeket (pl. a rendszer leállását és újra indulását);
h) a rendszerben fellépő hibákat.

Amennyiben valamely rendszer nem képes minden előírt eseményt naplózni, annál törekedni kell, hogy a későbbi fejlesztések során alkalmas legyen, illetve a leghatékonyabb megoldást kell megvalósítani. Az EIR naplózásának kialakításakor a rendszer kulcsfelhasználóját is be kell vonni azért, hogy adatgazdai oldalról meghatározásra kerüljenek azok a többletinformációk, amelyek a felhasználói tevékenységek nyomon követéséhez szükségesek.

A naplózási beállításokat az EIBF a rendszer bevezetésekor és évente felülvizsgálja annak érdekében, hogy elegendőek-e a biztonsági események kivizsgálásához.

4.3. NAPLÓBEJEGYZÉSEK TARTALMA

Az EIR naplóbejegyzéseinek a következőket kell tartalmazniuk:

a) az esemény típusát;
b) az esemény időpontját;
c) az esemény helyét (mely lokáció, rendszerelem vagy rendszer);
d) az esemény forrását (miből származott az esemény);
e) az esemény leírását (mi lett a kimenetel);
f) a Felhasználó azonosítóját;

4.5. NAPLÓZÁS TÁRKAPACITÁSA

A naplók tárkapacitását az EIR fejlesztőjének a bevonásával az előzetes kapacitástervezési folyamat során kell kialakítani.

A naplózást és a naplók tárkapacitását úgy kell beállítani, hogy a naplóbejegyzések gyakrabban kerüljenek mentésre, mint ahogyan a naplótárhely betelése miatt a bejegyzések felülírásra kerülnének, ezzel biztosítva, hogy a naplóbejegyzések ne veszhessenek el.

A naplók tárkapacitásának figyelését az EIR felügyeleti tevékenységébe kell beépíteni.

4.7. NAPLÓZÁSI HIBA KEZELÉSE

Az EIR naplóinak a figyelését oly módon kell kialakítani, hogy naplózási hiba esetén a rendszer küldjön riasztást a rendszergazdának.

Amennyiben kivitelezhető, naplóhiba esetén függessze fel a további feldolgozást a hiba elhárításáig.

4.13. NAPLÓBEJEGYZÉSEK FELÜLVIZSGÁLATA, ELEMZÉSE ÉS JELENTÉSTÉTEL

Az EIR és kapcsolódó környezetük (alkalmazói szoftverek, szerverek, hálózati eszközök, határvédelmi eszközök és egyéb biztonsági eszközök) eseménynaplóit az üzemeltetési feladatok részeként a rendszergazdának legalább havonta át kell vizsgálnia.

Nem megfelelő, vagy szokatlan működésre utaló jelek esetén értesíteni kell az IT vezetőt, aki dönt az esetleges további lépésekről. Incidens gyanúja esetén az EIBF is haladéktalanul értesítendő.

Incidens gyanúja esetén az adott naplóbejegyzések szélesebb körű vizsgálata szükséges, a naplóvizsgálatot a Rendszergazda végzi és az EIBF koordinálja.

4.24. IDŐBÉLYEGEK

Az EIR-nek valamennyi naplóbejegyzését időbélyeggel (időbejegyzéssel) kell ellátnia, melyhez a rendszerórát kell alapul venniük. Az EIR elemeinek rendszeróráját hálózati idő protokoll (Network Time Protocol, NTP) segítségével az egyezményes koordinált világidőhöz kell szinkronizálni.

A rendszerekben engedélyezett időeltérés 1 másodperc.

4.25. NAPLÓINFORMÁCIÓK VÉDELME

Gondoskodni kell arról, hogy az EIR naplóinformációi védettek legyenek a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. A naplóinformációk védelmét a Szervezet a hozzáférési jogosultságok megfelelő beállításával éri el.

Jogosulatlan hozzáférés, módosítás vagy a naplóinformáció törlésének észlelésekor a Rendszergazda értesíti az IT vezetőt, illetve az EIBF-t.

4.38. A NAPLÓBEJEGYZÉSEK MEGŐRZÉSE

A naplóinformációk mentését be kell vonni a Társaság mentési rendszerébe. A mentéseket a napló tárkapacitással összhangban úgy kell kialakítani, hogy a naplóbejegyzések ne vesszenek el. A naplóinformációkat biztonsági események utólagos kivizsgálása érdekében:

a) a határvédelmi eszközök és az arra alkalmas hálózati eszközökre vonatkozóan legalább 1 év;
b) a kliens oldali operációs rendszerek naplóira vonatkozóan legalább 6 hónap;
c) a szerver oldali operációs rendszerek naplóira vonatkozóan legalább 1 év;
d) az alkalmazás szoftverek naplóira vonatkozóan 1 évig;
e) konzisztens adatbázisok naplóira vonatkozóan (tranzakció log) 8 év;

A megőrzési idők biztosítása érdekében az alkalmazói szoftverek naplóinak mentését, az archív mentését, az egyéb környezeti naplók mentését a havi mentésekkel együtt kell végezni.

4.40. NAPLÓBEJEGYZÉSEK LÉTREHOZÁSA

A Szervezetnél csak olyan EIR használható, amely megfelel a következő követelményeknek:

a) Tegye lehetővé a Rendszergazdáknak a naplózható események kiválasztását
b) Biztosítsa a naplóbejegyzések előállítási lehetőségét a 4.2 Naplózható események pontban meghatározott naplózható eseményekre.

5. ÉRTÉKELÉS, ENGEDÉLYEZÉS ÉS MONITOROZÁS

5.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend fő feladata a biztonságértékelési folyamatok és eljárások meghatározása, dokumentálása és megvalósítása a szervezetben. Ennek révén biztosítja a szervezet belső biztonsági intézkedéseinek összhangját a vonatkozó jogszabályokkal és irányelvekkel, valamint elősegíti az átláthatóságot és hatékonyságot a biztonsági intézkedések felügyeletében és követésében.

Az eljárásrend célja továbbá, hogy biztosítsa a folyamatos megfelelést és hatékonyságot a biztonsági területen, valamint a rendszeres felülvizsgálatok révén lehetőséget teremtsen a frissítésekre és az esetleges fejlesztésekre.

Felelős: EIBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

5.2. BIZTONSÁGI ÉRTÉKELÉSEK

Biztonságértékelési terv célja

A biztonsági elemzés során a rendszer vagy hálózat biztonsági kockázatait lehet azonosítani, ami lehetővé teszi a problémák orvoslását. A Szervezet továbbá képes lesz arra, hogy előre felismerje a potenciális biztonsági problémákat és meghozza a szükséges intézkedéseket a kockázatok minimalizálása érdekében. Emellett azonosítani tudja a biztonsági eszközök hiányosságait, illetve fel tudja mérni ezen eszközök hatékonyságát. Ezen tevékenységeket évente, vagy a rendszerben történő nagyobb változtatásokkor el kell végezni.

Források azonosítása

a) Napló fájlok
   A rendszer vagy hálózat működéséről készített log fájlok segíthetnek azonosítani a biztonsági problémákat, például a sikertelen bejelentkezéseket vagy a támadásokat. A naplófájlok kezelésének, mentésének és elemzésének részletszabályait az IBSZ Naplózás és elszámoltathatóság fejezete tartalmazza.
b) Sérülékenységi vizsgálatok
   A vizsgálat célja az, hogy teszteljék a rendszer vagy hálózat biztonságát, és felismerjék a biztonsági problémákat. Külső- és belső sérülékenységi vizsgálatokkal mérhető fel a rendszerek jelenlegi biztonsági állapota és javítások eszközölhetők a biztonság fokozása érdekében.
c) Biztonsági értesítések
   A biztonsági értesítések és figyelmeztetések számos forrásból érkezhetnek, például a szoftvergyártóktól, biztonsági szakemberektől, vagy IT biztonsági közösségi fórumokról. Heti szinten több alkalommal (naponta) figyelni kell ezen riasztásokat. https://nki.gov.hu/figyelmeztetesek/riasztas/
d) Felhasználói tevékenységek
   A felhasználói tevékenységek elemzése segíthet azonosítani a biztonsági problémákat, például a rosszindulatú felhasználókat vagy a belső fenyegetéseket.

Adatgyűjtés, adatelemzés

Az adatok gyűjtését a Rendszergazda végzi:

Biztonsági problémák azonosítása

Az információbiztonsági problémák azonosítása kulcsfontosságú a biztonság fenntartása érdekében. Az alábbiakban lépések segítenek az információbiztonsági problémák azonosításában:

a) Kockázatértékelés
A kockázatelemzés során ki kell értékelni a különböző biztonsági kockázatokat, például a hálózati támadásokat, a malware fertőzéseket, a fizikai lopásokat stb. Ezen elemzés és értékelés az IBSZ 15. Kockázatkezelés fejezetében foglaltak szerint történik.

b) Sebezhetőségek azonosítása
Az információbiztonsági sebezhetőségek azonosítók a rendszerek és szoftverek rendszeres ellenőrzése, a sérülékenységfelmérések, a sérülékenységi vizsgálatok és a vulnerability scanner eszközök használatával.

c) Jogosulatlan hozzáférések ellenőrzése
Rendszeresen kell ellenőrizni és kontroll alatt tartani a hozzáféréseket, ez segít megakadályozni a jogosulatlan adathozzáféréseket és az illetéktelen tevékenységeket.

d) Rendszeres ellenőrzések
Az előírások szerint rendszeresen ellenőrizni szükséges az EIR-t és szoftvereket, hogy azonosítani lehessen a lehetséges problémákat és hibákat. Az ellenőrzések magukban kell foglalják a biztonsági naplók ellenőrzését, a rendszerek konfigurációinak ellenőrzését és a biztonsági mentések ellenőrzését.

e) Tanulás a múltbéli incidensekből
A múltbeli biztonsági incidensek felhasználhatók a jövőbeli biztonsági problémák elkerüléséhez. Meg kell vizsgálni a korábbi biztonsági incidenseket, hogy azonosítani lehessen azok okait, és megfelelő intézkedéseket lehessen alkalmazni a hasonló incidensek megelőzésére.

Teljesítménymutatók

Az információbiztonsági teljesítménymutatók segítségével mérhetők az információbiztonsági folyamatok hatékonysága.

a) Incidensek száma időszakonként (kategorizálás súlyosság szerint)
b) Hibák száma időszakonként (hibák átlagos javítási ideje)
c) Jogosultságok felülvizsgálatából fakadó mérőszámok
d) Biztonsági ellenőrzések rendszeressége és eredményei
e) Frissítések időzítése és végrehajtása

Az értékelés alapján összefoglaló jelentést kell készíteni az értékelés eredményéről. A jelentés készítése a megadott paraméterek alapján a Rendszergazda feladata. A jelentést kapja az IT vezető és az EIBF.

5.4. BIZTONSÁGI ÉRTÉKELÉSEK – KIBERBIZTONSÁGI AUDIT

Legalább kétévente kiberbiztonsági auditot kell végrehajtani az EIR-ek biztonsági intézkedéseinek értékelésére. Az auditot külsőszemély, vagy független szervezet végezheti.

5.7. INFORMÁCIÓCSERE

Az IT vezető jóváhagyja és szabályozza az információcserét az EIR és más rendszerek között. A Szervezetnek kapcsolódási pontokra vonatkozó biztonsági megállapodásokat kell kötnie a külső partnerekkel és szolgáltatókkal.

Amikor Szervezet új információcsere-megállapodást köt egy rendszerrel kapcsolatban, akkor dokumentálni kell az egyes rendszerek interfészeinek jellemzőit. A felek rögzítik a biztonsági követelményeket, védelmi intézkedéseket és felelősségi köröket is. Emellett fel kell jegyezni a megosztott információk hatásának szintjét, figyelembe véve a szolgáltatási szintre (SLA), a felhasználókra, a titoktartásra és a szervezet által meghatározott egyéb megállapodásokra vonatkozó előírásokat is.

Ezen megállapodásokat éves szinten felül kell vizsgálni, illetve változás esetén frissíteni.

5.10. AZ INTÉZKEDÉSI TERV ÉS MÉRFÖLDKÖVEI

Az EIR gyengeségeinek vagy hiányosságainak kijavítására a Szervezetnek Intézkedési tervet kell kidolgoznia. Ezen tervben meg kell határozni az intézkedések céljait, a célok eléréséhez szükséges mérföldköveket.

Az intézkedési tervet a szükséges intézkedések végrehajtásáért felelős személyek és a vonatkozó határidők megjelölésével kell elkészíteni vonatkozó eljárási szabályok, felelősök, határidők megjelölésével, figyelembe véve a védelmi intézkedések értékeléseit, a független auditokat és felülvizsgálatokat, valamint a folyamatos felügyeleti tevékenységek eredményeit.

Az Intézkedési tervben rögzíteni kell az alábbiakat:

a) a megvalósítandó intézkedéseket;
b) amennyiben a feladat jellege egy éven túl mutat, akkor részfeladatokat (mérföldköveket), illetve részhatáridőket kell meghatározni, abban az esetben, ahol ez értelmezhető;
c) a feladatok végrehajtásának becsült munkaidő ráfordítását (és az esetleges költségeket);
d) a feladatok mellé rendelt felelőst;
e) a feladatok végrehajtásának határidejét.

A tervet az EIBF javaslatainak figyelembevételével az IT vezető irányításával és a Rendszergazda közreműködésével kell kidolgozni, melyet a szervezet vezetője hagy jóvá.

Az intézkedési terv elkészítéséért, végrehajtásáért, felülvizsgálatáért és a megtett intézkedésekről a szervezet vezetőjének történő beszámolásért az EIBF a felelős.

5.12. ENGEDÉLYEZÉS

A Szervezeti vezető feladata kijelölni az EIR Adatgazdáit.

Abban az esetben, ha a Szervezet új EIR-t integrál más rendszerekkel, az Adatgazdának és az EIBF-nek meg kell vizsgálnia, hogy továbbra is fennállnak-e, illetve értelmezhetők a Szervezet által előírt biztonsági követelmények (pl. jelszókövetelmények, legkisebb jogosultság elve, naplózási követelmények). Amennyiben a követelmények fennállnak, úgy az Adatgazda elfogadja és engedélyezi a rendszer működését.

Emellett rendszeresen egyeztetnie kell a különböző rendszerek üzemeltetőivel, valamint részt kell vennie a biztonsági kérdésekkel kapcsolatos döntéshozatali folyamatokban a szervezet belső irányelvei és szabályzatai alapján.

5.15. FOLYAMATOS FELÜGYELET

A folyamatos felügyeleti stratégia célja az EIR, hálózatok és adatok biztonságának fenntartása, az esetleges kockázatok korai észlelése és kezelése. A rendszer teljesítményének, hatékonyságának követésében a következő metrikák segítenek:

a) Elérhetőség (Availability): A rendszer vagy alkalmazás mennyi időn keresztül volt elérhető a tervezett működési időszakban. Az elérhetőségi metrikák segítenek azonosítani a hálózati hibákat.
b) Teljesítmény (Performance): Átlagos válaszidő, illetve átviteli sebesség.
c) Skálázhatóság (Scalability): A rendszer képessége, hogy rugalmasan növelje a terhelését, és hatékonyan kezelje a megnövekedett terhelést.
d) Rendszerkihasználtság (System Utilization): CPU- és memória kihasználtsága.
e) Biztonság (Security): A rendszerre irányuló támadási kísérletek vagy sikeres támadások száma, illetve a rendszerben talált hibák és sebezhetőségek száma.
f) Jogosultság-kezelés (Access Control): Sikeres és sikertelen bejelentkezések száma.
g) Teljesítményproblémák (Troubleshooting): A rendszerből származó hibaüzenetek és naplóbejegyzések elemzése a hibák és problémák azonosításához.

Az elemzések alapján válaszintézkedésekre lehet szükség, melyet az IT vezető jóváhagyásával a Rendszergazdának kell foganatosítania. A rendszer biztonsági állapotáról rendszeresen jelentést kell kapnia az IT vezetőnek és az EIBF-nek.

5.18. FOLYAMATOS FELÜGYELET – KOCKÁZATMONITOROZÁS

A folyamatos felügyeleti stratégiának része kell legyen:

a) a hatékonyság ellenőrzése;
b) a megfelelés ellenőrzése;
c) a változások nyomon követése;

5.25. BELSŐ RENDSZERKAPCSOLATOK

Az EIR összekapcsolása csak akkor lehetséges a belső rendszerek esetében, ha annak kockázatait a rendszer Rendszergazdája, a Szervezet mindenkori Szervezeti és Működési Szabályzatában meghatározott - legfelsőbb vezetője, illetve az EIBF mérlegeli, majd az IT vezető jóváhagyja.

Jóváhagyás esetén dokumentálni kell az interfész jellemzőit, követelményeit.

A kapcsolatot meg kell szüntetni, ha használat okafogyottá válik. A kapcsolat megszüntetését az IT vezető hagyja jóvá.

A Rendszergazda feladata, hogy évente, vagy nagyobb változtatásokkor felülvizsgálja a kapcsolat további szükségességét.

6. KONFIGURÁCIÓKEZELÉS

6.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

A konfigurációkezelés célja, hogy az EIR elvárt biztonsági osztályának megfelelően biztosítsa azok megbízható működését a rendszerösszetevők telepítésének, konfigurálásának, megváltoztatásának, tesztelésének és nyilvántartásának szabályozott körülmények közötti végrehajtásával. Segíti a változások nyomon követését és dokumentálását, ideértve az új bevezetéseket, módosításokat és törléseket is. Emellett segít az azonosított hibák kezelésében és a rendszerek visszaállításában a hibás konfigurációból a stabil állapotba.

Felelős: IT vezető

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

6.2. ALAPKONFIGURÁCIÓ

Az EIR-hez rendszerenként dokumentált formában el kell készíteni egy-egy Alapkonfigurációt és ezt biztonságos helyen kell tárolni.

Az Alapkonfiguráció dokumentációjának célja, hogy új rendszerelemek esetén rögzítse, hogyan kell az elemet telepíteni és konfigurálni, illetve meghibásodás esetén a rendszerelemeket hogyan kell újra telepíteni.

A dokumentáció az egyes eszköztípusokra (pl.: szerver, munkaállomás, tűzfal, router, stb.) vonatkozóan meghatározza az adott feladat ellátásához szükséges hardver és szoftver környezetet.

Az Alapkonfigurációnak minimálisan a következőket kell magában foglalnia:

a) a feladat ellátásához szükséges minimális és ajánlott hardver elemek listáját;
b) a szükséges szoftverek listáját;
c) a szoftverek konfigurációs beállításait, paramétereit;
d) ha a rendszer biztonsági osztálya előírja, a dokumentációnak tartalmaznia kell az engedélyezett szolgáltatások, portok és protokollok listáját a „szükséges minimum" elv alapján

A dokumentáció részeként egy logikai és fizikai hálózati topológia rajzot is készíteni kell, amelyen követhető a rendszerelemek elhelyezkedése a rendszer architektúrájában.

Felelős: Az EIR Alapkonfigurációját a Rendszergazda készíti el, 6 havonta felülvizsgálja, és a módosításokat átvezeti. A dokumentációt az IT vezető felügyeli.

6.7. A KONFIGURÁCIÓVÁLTOZÁSOK FELÜGYELETE (VÁLTOZÁSKEZELÉS)

A Szervezet a következő eljárást követi a változáskezelési folyamat során:

- Azonosítja és rögzíti azokat a rendszerváltozásokat, amelyek a változáskezelési felügyelet szabályozási keretébe tartoznak.
- Elemzi, és biztonsági szempontok figyelembevételével elfogadja vagy elveti a rendszerkonfiguráció jelentős módosításaira irányuló javaslatokat.

- Rögzíti az EIR-ben végrehajtott változásokkal kapcsolatos határozatokat.
- Végrehajtja az elfogadott módosításokat az EIR-en belül.
- Folyamatosan nyilvántartja, és hozzáférhető módon őrzi az EIR-en végrehajtott változtatásokkal kapcsolatos dokumentációt.
- Felülvizsgálja és ellenőrzi azokat a tevékenységeket, amelyek a változások bevezetésével összefüggésben állnak.

A Rendszergazda koordinálja és felügyeli a konfigurációs változtatásokat, - amelyeket adott gyakorisággal, vagy amikor a változások bevezetésének feltételei fennállnak, - alkalmaznak.

Változáskezelés hatálya alá tartozó tevékenységek:

- jelentős változással járó verzióváltások, új fejlesztések;
- rendszerelemek cseréje (hardver/szoftver);
- a rendszer működésének jelentős módosítása, jelentős beavatkozást igénylő hangolások.

A változáskezeléssel kapcsolatosan az alábbi előírásokat kell figyelembe venni:

a) A rendszer bármely funkciójának jelentős megváltoztatásához az Informatikai üzemeltetési vezető és az adatgazdai terület vezetőjének engedélye szükséges.
b) A változtatást az kezdeményezi, akinél az igényként felmerül.
c) A változtatásokra vonatkozó igénybejelentést, véleményezést, döntést, a változtatás kivitelezését dokumentálni kell.
d) A tervezett jelentős változtatást véleményezés céljából az EIBF-nek is meg kell küldeni, aki kockázatelemzéssel megállapítja a változtatás rendszerre gyakorolt hatását.
e) A fejlesztők az éles rendszerben csak az IT vezető, vagy az általa megbízott Rendszergazda felügyelete mellett végezhetnek változtatást.
f) A változtatást az éles üzembe való állítás előtt az erre a célra létrehozott tesztkörnyezetben tesztelni kell.
g) Az éles üzembe állítást csak a változással érintett rendszerek, adatok teljes mentését követően lehet elvégezni.
h) A változtatást munkaidőn kívül kell elvégezni, csak rendkívüli esetben végezhető munkaidőben.
i) Amennyiben a változtatáshoz a rendszer leállítása szükséges, akkor arról az Informatika csoport legalább 1 munkanappal korábban köteles tájékoztatni a felhasználókat.

A változáskezelési folyamatot és a változáskezelési előírások betartását az EIBF az éves ellenőrzési tervében foglaltak szerint ellenőrzi.

6.15. BIZTONSÁGI HATÁSVIZSGÁLATOK

A változtatás megkezdése előtt az EIBF-nek az előzetes kockázatelemzéssel és a biztonsági funkciók tesztelésével kell biztosítania a változtatás éles környezetre ható biztonsági kockázatainak minimalizálását.

6.18. A VÁLTOZTATÁSOKRA VONATKOZÓ HOZZÁFÉRÉS KORLÁTOZÁSOK

A változtatásokat csak az Informatika csoport munkatársai, vagy az aktuális és szükséges jogosultságokkal rendelkező külsős személyek végezhetik el az IT vezető jóváhagyásával. Minden változtatást automatikusan naplózni kell.

6.23. KONFIGURÁCIÓS BEÁLLÍTÁSOK

Az EIR működtetése során csak az Alapkonfigurációjában szereplő, jóváhagyott hardver és szoftver elemek, konfigurációs beállítások használhatók.

A kötelező konfigurációs beállítások érvényesítését az EIBF az éves ellenőrzési tervében foglaltak szerint az 6.2 Alapkonfiguráció pont alapján ellenőrzi.

6.26. LEGSZŰKEBB FUNKCIONALITÁS

Az EIR-t a „szükséges minimum" elv alapján úgy kell konfigurálni, hogy csak azok a szolgáltatások, portok, protokollok legyenek engedélyezve, illetve csak azok a szoftverek legyenek telepítve. amelyek az ügy- és üzletmenet szempontjából létfontosságú szolgáltatások nyújtásához szükségesek.

Az engedélyezett szolgáltatások, portok és protokollok listáját a rendszer Alapkonfigurációjában kell rögzíteni.

Az engedélyezett szolgáltatások, portok és protokollok kizárólagos használatát az EIBF az éves ellenőrzési tervében foglaltak szerint ellenőrzi.

6.36. RENDSZERELEM LELTÁR

A Szervezetnek leltárt kell vezetnie az EIR valamennyi hardver/szoftver eleméről és gondoskodnia kell a leltár teljességéről és naprakészségéről.

A leltárnak tartalmaznia kell:

- a rendszerben használt hardver és szoftverek elemek listáját, az azonosításukhoz szükséges adatokat és a hardver/szoftver elemek összerendelését;
- az egyes elemek használóját, felelősét;
- a szoftver elemekhez rendelt szoftverlicenceket.

A leltár gyakorlati megvalósítása a következő módon történik:

A munkaállomások és szerverek (mind fizikai-, mind virtuális szerverek) leltározásához minden számítógépre telepíteni kell a Szervezetnél *az Automatikus számítógép leltár* készítésére rendszeresített leltározó szoftver kliens programját, amely egy központi adatbázisban naprakészen összegyűjti a leltározott számítógépek részletes hardver jellemzőit, és a számítógépekre telepített szoftvereket.

A szervereket, munkaállomásokat, hálózati eszközöket, a meghatározott nagyobb értékű számítógép tartozékokat (pl.: monitor, nyomtató, szkenner, szünetmentes tápegység, szalagos egység stb.) a Hardver nyilvántartásban kell nyilvántartani. Az egységes kezelés érdekében a virtuális szervereket is tartalmaznia kell a nyilvántartásnak. A kis értékű számítógép tartozékokat (pl.: billentyűzet, egér, hangszóró stb.) és a kábeleket nem kell nyilvántartani, ezeket a Szervezet anyagként kezelni.

A vásárolt, bérelt vagy fejlesztett szoftverek (továbbiakban: licenckötelés szoftverek) licenceit a Szoftver nyilvántartásban kell nyilvántartani.

Az EIR Alapkonfigurációjának részeként hálózati topológia rajzot kell készíteni, amelyeken követhető a Rendszerelem leltárban szereplő rendszerelemek elhelyezkedése a rendszer architektúrájában.

Változások (pl.: új informatikai eszközök/szoftverek üzembe helyezése vagy selejtezése; informatikai eszközök áthelyezése; szoftverek telepítése/eltávolítása; stb.) esetén folyamatosan karban kell tartani a nyilvántartásokat. A változások átvezetése az Informatika csoport azon munkatársának felelőssége, aki a változással kapcsolatos műveletet végrehajtotta.

A Rendszerelem leltárt, valamint a Hardver- és Szoftver nyilvántartások adott rendszerhez kapcsolódó rendszerelemeit a rendszergazdának hathavonta felül kell vizsgálnia, a feltárt eltéréseket javítania kell.

Hardver nyilvántartás

A Hardver nyilvántartásnak az alábbi adatokat kell az informatikai eszközökre vonatkozóan minimálisan tartalmaznia:

- az eszköz csoportját (pl.: fizikai szerver, virtuális szerver, asztali számítógép, laptop, switch, router, monitor, nyomtató, szünetmentes tápegység, külső merevlemez stb.);
- az eszköz informatikai azonosítóját;
- az eszköz rövid megnevezését (szerverek esetén a szerver funkciójának rövid leírását; munkaállomások esetén a Felhasználó nevét);
- az eszköz gyártóját és típusát;
- a fő jellemzőket (számítógépek esetén a processzor típusát, a memória és háttértár méretét, hálózati eszközök esetén a portok számát stb.);
- számítógépek estén az operációs rendszer típusát;
- az eszközért felelős személy nevét (ez munkaállomások esetén a felhasználó, szerver oldali eszközök esetén a Rendszergazda nevét);

- A nyilvántartáshoz kapcsolódóan – az informatikai eszközök üzemeltetésének támogatására – az Informatika csoportnak visszakereshető formában meg kell őriznie az eszköz számlájának szkennelt másolatát, a garancia jegyet, telepítő adathordozót és az egyéb gyártói dokumentációt (pl.: kezelési és karbantartási útmutató, műszaki leírás stb.). A megőrzési idő az eszközök selejtezéséig tart.

Szoftver nyilvántartás

A Szoftver nyilvántartásban az alábbi adatokat kell minimálisan vezetni:

- a szoftver nevét és verziószámát;
- a szoftver funkciójának rövid megnevezését;
- a beszerzett licencek darabszámát;

A nyilvántartáshoz kapcsolódóan – a szoftverlicencek igazolása céljából – az Informatika csoportnak visszakereshető formában meg kell őriznie a szoftverek számlájának szkennelt másolatát és a szoftverlicencet igazoló egyéb dokumentumokat (pl.: licencszerződés, licencengedély, licence kulcs, stb.).

6.47. A SZOFTVERHASZNÁLAT KORLÁTOZÁSAI

A Szervezet minden Felhasználó számára biztosítja a munkavégzéshez szükséges szoftvereket, ezért a Szervezet számítógépein csak legális, a Szervezet által rendelkezésre bocsátott szoftverek használhatók a licencszerződésben foglaltak szerint.

Ebből következően tilos telepíteni a Felhasználó vagy külső partnerek tulajdonában lévő szoftvereket, valamint tilos a szoftvereket a licenc által megengedett darabszámot meghaladó számban használni!

Az előfizetéses licenccel rendelkező szoftverekről (pl. Windows, Office, ESET Antivirus) nyilvántartást kell vezetni. Ezen szoftverek használatát szúrópróba-szerűen ellenőrizni kell. A nyilvántartást évente felül kell vizsgálni. A központi adminisztrációs felülettel rendelkező rendszereknél a felhasználók listáját ill. a felhasználás mennyiségét évente felül kell vizsgálni.

Az egyéb telepítési licencköteles szoftverekről (pl. Total Commander, PicPic, XNView, stb.) nyilvántartást kell vezetni, amelyet telepítés vagy eltávolítás esetén aktualizálni kell.

A Szervezet számos külső partnertől vásárolja meg a szoftverek licencengedélyét. A Szervezet a licencszerződéssel nem válik a szoftverek tulajdonosává, azok telepítő adathordozóit és dokumentációját a szoftver fejlesztőjének külön engedélye nélkül nem áll jogában másolni.

Az IT vezető felelőssége, hogy csak a Szervezet által vásárolt/bérelt, illetve a Szervezet számára belső vagy külső fejlesztéssel készült jogtiszta szoftverek, valamint az engedélyezési eljáráson átesett szabad szoftverek kerüljenek üzembe helyezésre.

A legális szoftverhasználat biztosítása és az EIR biztonsága érdekében az alábbi előírásokat kell betartani:

- Licencköteles szoftvereket csak az Informatika csoport munkatársai, illetve az IT vezető által ezzel megbízott külső partnerek alkalmazottai telepíthetnek.
- A licencköteles szoftverek telepítő adathordozóit és licenckulcsait a másolatok ellenőrzése érdekében a rendszergazdának elzárva kell tárolnia és ellenőriznie kell a hozzáféréseket.
- A rendszergazdának ellenőrzés alatt kell tartania a hálózati megosztások jogosultság beállítását és tartalmát, és gondoskodnia kell arról, hogy a megosztások ne tegyék lehetővé a szerzői jogokkal védett szoftverek illegális használatát, illetve a szoftverek telepítőkészletének vagy licenckulcsának illetéktelen másolását, terjesztését.
- Szoftver telepítőkészleteket kizárólag az Informatika csoport helyezhet el hálózaton megosztott mappákban az általa végzett szoftvertelepítések végrehajtása céljából. A licencköteles szoftverek telepítőkészletéhez csak az Informatika csoport munkatársai rendelkezhetnek hozzáférési jogosultsággal, az engedélyezett szabad szoftverek telepítőkészletéhez a felhasználók is hozzáférhetnek az automatizált telepítési folyamatok működése érdekében.
- A szoftvereket kizárólag a licencszerződés előírásainak megfelelően lehet használni. A hálózati megosztásra, vagy több felhasználó által használt szerverekre (terminál szerverekre) történő szoftvertelepítést megelőzően ellenőrizni kell, hogy a licencszerződés milyen feltételekkel teszi lehetővé az ilyen használatot.
- Amennyiben a Szervezet munkatársainak tudomására jut, hogy szoftvereket illegálisan, érvényes licencengedély nélkül vagy nem a licencszerződésnek megfelelően használnak, akkor ezt kötelesek a munkahelyi vezetőjüknek és az EIBF-nek jelenteni.

- A Szervezet elítéli az illegális szoftverhasználatot, szándékos károkozásnak tekinti az illegális szoftverek telepítését, és az előírás megsértőivel szemben fegyelmi felelősségre vonásra kerülhet sor.
- Azon munkatársak, akik illegális szoftvermásolatot készítenek, szereznek be, telepítenek vagy használnak, a szerzői jogi törvény (továbbiakban: Szjt.) szerint szankcionálhatók és kártérítésre kötelezhetők. Ezért a Szervezet semmilyen felelősséget nem vállal.

6.49. FELHASZNÁLÓ ÁLTAL TELEPÍTETT SZOFTVER

A felhasználók nem telepíthetnek, vagy távolíthatnak el szoftvereket.

A korlátozást az operációs rendszer segítségével kell kikényszeríteni, azaz a felhasználók csak korlátozott felhasználói fiókot használnak, amelynek nincs jogosultsága a telepítésre.

A szabályok betartását az EIBF az éves ellenőrzési tervében foglaltak szerint, személyes megtekintéssel ellenőrzi.

Telepítés nélkül futtatható szoftverek

A telepítés korlátozása a telepítés nélkül futtatható (ún. portable) szoftverek segítségével megkerülhető.

Léteznek olyan telepítés nélkül használható szoftverek, melyeket szerzői jogok védelme alatt álló szoftverek feltörésével, illegális módon hoztak létre. Az ilyen szerzői jogot sértő szoftverek birtoklása és használata illegális szoftverhasználatnak minősül.

A telepítés nélkül futtatható szoftverek nehezen felügyelhetők, használatuk biztonsági és licenc problémákat vet fel, ezért általános esetben a Szervezet számítógépein a telepítés nélkül futtatható szoftverek elindítása vagy a számítógépen történő tárolása tilos!

A telepítés nélkül futtatható szoftverek használatát a Rendszergazda indokolt esetben engedélyezheti. Az ilyen szoftverek engedélyezése során ugyanúgy kell eljárni, mintha a szoftver telepítésre kerülne az adott számítógépre (a licencköteles szoftverekhez érvényes licenccel kell rendelkezni, a szabad szoftvereknek át kellett esniük az engedélyezési eljáráson).

Automatizáltan települő szoftverek

Az engedélyezett szabad szoftverek és az összes munkaállomáshoz licenccel rendelkező szoftverek telepítése vagy a szoftverek verziófrissítése céljából az Informatika csoport alkalmazhat automatizált telepítési módszereket, amelyek pl. a hálózati bejelentkezés folyamán, egy szoftver indításának részeként, vagy a Felhasználó opcionális döntése alapján indulnak el.

Ezeket az automatizált telepítéseket az Informatika csoport által végzett telepítésnek kell tekinteni, akkor is, ha egy felhasználói művelet hatására aktivizálódnak.

Az automatizált telepítésekkel szembeni követelmény, hogy a telepítéseket naplózni kell és a rendszergazdának a naplók vizsgálatával felügyeletet kell gyakorolnia a telepítési folyamat felett.

7. KÉSZENLÉTI TERVEZÉS

7.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

A jelen eljárásrend célja az üzletmenet-folytonosság biztosítása és a Szervezet működésének fenntartása kritikus helyzetekben. Ennek érdekében különféle intézkedéseket és terveket foglal magában.

Készenléti terv létrehozása és fenntartása elsődleges fontosságú a Szervezet számára. Cél a kritikus üzleti funkciók gyors helyreállítása mellett, a személyzet folyamatos működésre való felkészítése, hogy azok képesek legyenek hatékonyan kezelni az esetleges kritikus helyzeteket.

Az EIR mentései és helyreállítása kritikus a Szervezet adatintegritásának megőrzése és a szolgáltatások folytonossága szempontjából. Ez magában foglalja a rendszeres mentéseket, azok megbízhatóságának és sértetlenségének tesztelését, valamint a rendszer helyreállítását és tranzakcióinak visszaállítását kritikus időkben.

A Szervezet az alábbi intézkedéseket hajtja végre az üzletmenet-folytonosság biztosítása érdekében:

- Előkészíti, írásba foglalja, közzéteszi, és ismerteti az érintett személyekkel - szerepkörüknek megfelelően - a Készenléti tervet,
- Meghatározza a szervezeti, folyamatbeli és rendszerszintű követelményeket,
- Meghatározza a célokat, hatáskört, szerepköröket, felelősségeket, a vezetőség elkötelezettségét, a szervezeten belüli együttműködés kereteit, valamint a megfelelőségi kritériumokat,
- Kidolgozza az üzletmenet-folytonossági eljárásokat, és a hozzá kapcsolódó ellenőrzéseknek a végrehajtását.
- Rendszeresen felülvizsgálja és frissíti az üzletmenetfolytonossági eljárásokat a Szervezet által meghatározott időközönként, valamint a Szervezet által meghatározott események bekövetkezte után.
- Az EIR Készenléti tervét világosan megfogalmazza, dokumentálja, és kihirdeti a kulcsfontosságú személyek és szervezeti egységek számára, valamint tájékoztatja a kulcsfontosságú személyeket és szervezeti egységeket a Készenléti terv változásairól.
- Szinkronizálja a folyamatos működés tervezését a biztonsági incidensek kezelésével.
- Rendszeres időközönként felülvizsgálja az EIR Készenléti tervét.
- Az EIR vagy működési környezet változásai, a terv megvalósításának, végrehajtásának vagy tesztelésének során felmerülő problémák alapján frissíti a Készenléti tervet.
- A Készenléti terv teszteléséből, gyakorlatából vagy tényleges alkalmazásából származó tapasztalatokat integrálja a tesztelési és gyakorlati folyamatokba.
- Megvédi a Készenléti tervet a jogosulatlan megismeréstől és módosítástól.
-

Felelős: IT vezető, adatgazda, EIBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, a Rendszergazdával, valamint a Vészhelyzeti szereplőkkel (1.6.3.) minden esetben ismertetni kell.

7.2. ÜZLETMENET-FOLYTONOSSÁGI TERV

A Szervezet az alábbi intézkedésekkel biztosítja az EIR üzletmenet-folytonosságát.

Kialakítja az EIR üzletmenet-folytonossági tervét, amely:

- Meghatározza az alapszolgáltatásokat és -funkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket.
- Meghatározza a helyreállítási célokat, prioritásokat és metrikákat.
- Kijelöli a vészhelyzeti szerepköröket, felelősségeket, kapcsolattartókat és elérhetőségeiket.
- Meghatározza az EIR zavarai esetén is fenntartandó szolgáltatásokat.
- Tartalmazza az EIR teljes körű helyreállításának részletes tervét, amely biztosítja a védelmi intézkedések integritását a helyreállítás után.
- Összhangban áll a Szervezetet érintő érvényes jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.
-
- Tartalmazza az üzletmenet-folytonossági információk megosztásának szabályait.
- Magába foglalja a szervezet meghatározott személyei vagy szerepkörei által történő felülvizsgálatot és jóváhagyást.

7.10. A FOLYAMATOS MŰKÖDÉSRE FELKÉSZÍTŐ KÉPZÉS

A Szervezet az EIR folyamatos működésére felkészítő képzést tart a felhasználóknak, illetve az érintett szerepkörüknek és felelősségüknek megfelelően.

Az üzletmenet-folytonosság megfelelő szinten tartása, valamint a nem várt események esetén alkalmazandó Készenléti terv megfelelő hatékonysággal történő végrehajtása érdekében a tervek végrehajtásában érintett szereplők részére a szerepkörbe kerülésüket vagy a tervek változását követően felkészítő és évente ismétlő képzéseket kell tartani.

A képzéseken a következő területeket kell legalább érinteni:

- az EIR-re ható főbb fenyegetéseket;
- a fenyegetések minimalizálása érdekében megtett kockázatkezelő intézkedéseket;
- a konfigurációkezelési és változáskezelési eljárások megfelelő használatát;
- a mentési eljárásokat;
- a katasztrófa esetén szükséges lépéseket.

A képzés tartalmának összeállítása és a képzés lebonyolítása az EIBF feladata.

A képzéseket a Szervezet évente szervezi, vagy amikor az EIR változásai ezt szükségessé teszik.

Nagyobb változások esetén, vagy ha az EIBF úgy látja, akkor felül kell vizsgálnia és frissíteni kell a képzés anyagát.

7.35. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER MENTÉSEI

A biztonsági mentés módszerei, gyakorisága, illetve a helyreállítás lehetőségei a Mentési Rend dokumentumban kaptak helyet.

7.43. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER HELYREÁLLÍTÁSA ÉS ÚJRAINDÍTÁSA

A biztonsági mentésből történő helyreállítás lehetőségei a Mentési Rend dokumentumban kaptak helyet. A rendszerek karbantartáskor, vagy vészhelyzet esetén történő leállításának sorrendjét az EIR nyilvántartásban szereplő prioritások szerinti ütemezés szerint kell megvalósítani. Az újraindítás ugyanezen analógiára történik.

8. AZONOSÍTÁS ÉS HITELESÍTÉS

8.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend célja a biztonságos és megbízható azonosítás és hitelesítés biztosítása a szervezet tevékenységeihez, a feladatai közé tartozik a szabályok, irányelvek és eljárások kidolgozása, dokumentálása és megismertetése a szervezeten belül.

Emellett a rendszeres felülvizsgálatok és frissítések biztosítják a megfelelőséget és a hatékonyságot az azonosítási és hitelesítési folyamatokban.

Felelős: IT vezető

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

8.2. AZONOSÍTÁS ÉS HITELESÍTÉS

Az EIR-ben egyedileg kell azonosítani és hitelesíteni a Szervezet valamennyi belső felhasználóját, ami lehetővé teszi, hogy egyénileg nyomon lehessen követni a felhasználók által végzett tevékenységeket.

Ennek érdekében a Szervezetnél alkalmazott névkonvenció alapján a felhasználóknak egyedi, névre szóló felhasználói azonosítókat kell képezni. Ez fokozottan vonatkozik a kiemelt jogosultságokkal rendelkező, rendszergazda felhasználók fiókjaira.

8.3. AZONOSÍTÁS ÉS HITELESÍTÉS (FELHASZNÁLÓK) – PRIVILEGIZÁLT FIÓKOK TÖBBTÉNYEZŐS HITELESÍTÉSE

A kiemelt jogosultságokkal rendelkező, ún. privilegizált felhasználók (rendszergazdák) hálózati bejelentkezésére többtényezős hitelesítést kell alkalmazni.

A többtényezős hitelesítés két különböző módszerrel kell, hogy történjen. A hagyományos jelszavas hitelesítés mellett a második tényező lehet pl. egy titkosító kulcs birtoklása (tárolhatja szoftver vagy hardver token); egy biometrikus azonosító (pl.: ujjlenyomat, írisz, érminta); vagy egy mobiltelefonra SMS-ben, vagy Push üzenetben küldött egyszer használatos jelszó.

8.7. AZONOSÍTÁS ÉS HITELESÍTÉS (FELHASZNÁLÓK) – HOZZÁFÉRÉS A FIÓKOKHOZ – VISSZAJÁTSZÁS ELLENI VÉDELEM

Olyan hitelesítési mechanizmusokat kell használni, amelyek biztosítják a visszajátszás elleni védelmet (pl: OTP kódok, időbélyegek, időzítők, jogosultság időkorlát)

8.14. AZONOSÍTÓ KEZELÉS

A felhasználói azonosítókat a Rendszergazda kezeli, kiosztásukat a munkahelyi vezetőnek kell engedélyeznie.

Az azonosítókat úgy kell létrehozni, hogy azok egyértelműen hozzárendelhetők legyenek a kívánt személyhez (vagy szoftverek/hardver eszközök által használt technikai felhasználói fiókok esetén a kívánt rendszerelemhez).

Az azonosítók ismételt felhasználása tilos. Azonos nevű felhasználók esetén a felhasználói azonosítókat sorszám kiegészítéssel kell megkülönböztetni, abban az esetben is, ha az egyik felhasználói fiók már inaktív.

Az EIR-ben, a 3 hónapnyi inaktivitás után a fiókokat felül kell vizsgálni. Ezekről a Rendszergazdának felhasználók munkahelyi vezetőjével egyeztetnie kell, szükség esetén a fiókot fel kell függeszteni.

Az inaktivitás következtében vagy más okból letiltott felhasználói fiókokat csak a munkahelyi vezetőtől az Informatika csoportnak a HelpDesken írt kérelem alapján lehet feloldani a hozzáférési jogosultságok igénylésének folyamata szerint.

8.21. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE

Az illetéktelen hozzáférés megakadályozása érdekében a Felhasználó, vagy Eszköz identitását ellenőrizni kell.

A Rendszergazda első alkalommal egy a jelszókomplexitás követelményeinek megfelelő, véletlenszerű jelszót generál kezdeti jelszónak.

A jelszó minél komplexebb, annál kisebb a valószínűsége, hogy a Felhasználó nevében visszaélést követnek el. Ennek érdekében az alábbi szabályokat kell a jelszó kiválasztásakor betartani:

a) a jelszó legyen legalább 8 karakter hosszú és tartalmazzon kisbetűt, nagybetűt és számot és speciális karaktert is;
b) legyen könnyen megjegyezhető és nehezen kitalálható;
c) ne legyen a felhasználói névre vagy a Szervezet nevére utaló;
d) semmi olyasmi felhasználóhoz kötődő adaton ne alapuljon, amely alapján valaki kitalálhatja (ilyenek a nevek, telefonszámok, születési dátumok, lakcímek stb.);
e) ne tartalmazzon azonos, vagy ismert logika szerint egymást követő karaktereket (pl.: 123456, qwerty, asdfgh, stb.).

Lehetőséget kell teremteni a bonyolult jelszavak automatikus létrehozására (jelszógenerátor).

A kezdeti jelszó létrehozása után biztosítani kell, hogy a kezdeti jelszavak biztonságos körülmények között kerüljenek a felhasználóknak átadásra.

Minden Felhasználó felelőssége, hogy a jelszavak használata során betartsa a következő jelszavak védelmére vonatkozó szabályokat.

A felhasználói azonosító létrehozásakor, fiókvisszaállítás esetén, vagy a jelszó elfelejtése miatt beállított jelszót az első bejelentkezéskor azonnal meg kell változtatni.

A jelszó kiválasztásakor be kell tartani a jelszavak képzésére vonatkozó szabályokat és a jelszavakat meghatározott időnként meg kell változtatni.

A Felhasználó a jelszavát köteles titokban tartani, a jelszót tilos leírni, tilos nyilvános helyen kiírva (pl. monitorra ragasztva) tartani vagy másnak továbbadni.

A jelszót az Informatika csoport munkatársainak sem szabad elárulni. Ha a munkaállomás karbantartásához szükség van a Felhasználó jelszavára, a karbantartást végző munkatárs csak a jelszó Felhasználó általi beírását kérheti.

A Szervezet gondoskodik a felhasználói jelszavak legfeljebb 180 naponta történő cseréjéről.

Ha bármilyen jel mutat arra, hogy a jelszó illetéktelen kézbe jutott vagy feltételezhető a megismerése, azonnal meg kell változtatni a jelszót, és az esetet jelenteni kell a Biztonsági események kezelése pontban leírtak szerint;

A jelszó nem tehető egy automatikus bejelentkezési folyamat részévé (pl. makróra, vagy funkcióbillentyűre).

A Szervezetnél használt jelszavak Szervezeten kívüli rendszerekben nem használhatók.

A jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A Felhasználó felelőssége, ha jelszavának neki felróható mulasztása miatti megismerése révén valaki a nevében visszaélést követ el az EIR-ben.

Csoportos használatú fiók esetén amennyiben a tagok közül valaki eltávolításra kerül, a fiókjelszót azonnal módosítani kell!

8.22. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – JELSZÓ ALAPÚ HITELESÍTÉS

A Rendszergazda feladata, hogy a gyakran használt, könnyen kitalálható, vagy kompromittált jelszavakról nyilvántartást vezessen.

A felhasználók által létrehozni, vagy módosítani kívánt jelszavakat ellenőrizni kell, hogy szerepelnek-e a gyakran használt, vagy kompromittált jelszavak listáján. Amennyiben igen, az adott jelszó nem használható.

A jelszavak továbbítása csak titkosított csatornán keresztül történhet, TÁROLÁSUK PEDIG JÓVÁHAGYOTT, SÓZOTT KULCSSZÁRMAZTATÁSI FUNKCIÓVAL, LEHETŐLEG EGYKULCSOS HASH-T HASZNÁLVA TÖRTÉNHET.

8.36. HITELESÍTÉSI INFORMÁCIÓK VISSZAJELZÉSÉNEK ELREJTÉSE

A Szervezetnél csak olyan EIR használható, amely a hitelesítési folyamat során hibás azonosító vagy jelszó megadása esetén csak olyan hibaüzenetet ad vissza, amelyből nem szerezhető további információ sem az azonosítóra, sem a jelszóra vonatkozóan (pl.: nem derülhet ki az üzenetből, hogy a próbált azonosító érvényes, csak a jelszó hibás; vagy nem tartalmazhatja az üzenet a jelszó hosszára vagy bonyolultságára vonatkozó előírásokat).

8.37. HITELESÍTÉS KRIPTOGRÁFIAI MODUL ESETÉN

Amennyiben a hitelesítés egy kriptográfiai modul (titkosítást végző hardver eszköz) felhasználásával történik (ilyen lehet pl. a rendszergazdai fiókok többtényezős hitelesítése), a modul használata során be kell tartani a hitelesítés szolgáltató által rendelkezésre bocsájtott hitelesítési útmutatóban foglaltakat.

8.38. AZONOSÍTÁS ÉS HITELESÍTÉS (SZERVEZETEN KÍVÜLI FELHASZNÁLÓK)

A szervezeten kívüli felhasználók (külső felhasználók) EIR-hez történő hozzáférése során egyénre szóló, de partnercégre utaló felhasználói azonosítókat kell létrehozni.

Ebben az esetben a felhasználói azonosító létrehozását a külső felhasználó munkáját elrendelő adatgazdai terület vezetője vagy az EIR kulcsfelhasználója kezdeményezheti.

A külső felhasználóknak kiosztott felhasználói azonosítókkal történő tevékenységeket minden esetben naplózni kell, és ezen tevékenységekre a Rendszergazdának kiemelt figyelmet kell fordítania.

Amennyiben a szervezeten kívüli felhasználók hitelesítése nyilvános kulcsú titkosítási eljárással történik, a nyilvános kulcsot tartalmazó tanúsítványok csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványok lehetnek.

8.39. AZONOSÍTÁS ÉS HITELESÍTÉS (SZERVEZETEN KÍVÜLI FELHASZNÁLÓK) – MEGHATÁROZOTT AZONOSÍTÁSI PROFILOK HASZNÁLATA

Külső felhasználók esetén egyedi, számukra létrehozott profilokat kell alkalmazni. Ilyen lehet az Ügyfél profil, Partner profil, vagy Support profil.

8.43. ÚJRAHITELESÍTÉS

Kötelező a felhasználók újrahitelesítése a következő esetekben:

a) lejárt jelszó;
b) hosszabb idejű inaktivitás, vagy hálózati kapcsolat megszakadása;
c) új eszköz használata esetén.

9. BIZTONSÁGI ESEMÉNYEK KEZELÉSE

9.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend fő feladata az informatikai biztonsági események hatékony kezelése és reagálásuk szabályozása a Szervezetben. Célja az események gyors azonosítása, értékelése és megfelelő intézkedések meghozatala az esetleges biztonsági fenyegetések vagy incidensek kezelése érdekében.

Az eljárásrend tartalmazza az események nyomon követésére, dokumentálására és jelentésére vonatkozó irányelveket, valamint meghatározza az eseménykezelésért felelős személyek és csapatok szerepkörét és feladatait. Emellett a rendszeres felülvizsgálatok és frissítések biztosítják az eljárásrend hatékonyságát és megfelelőségét.

Felelős: EIBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, a Rendszergazdával, valamint a Vészhelyzeti szereplőkkel (1.6.3.) minden esetben ismertetni kell.

9.2. KÉPZÉS A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉRE

A felhasználókat képezni kell, hogy felismerjék a biztonsági fenyegetéseket, ismerjék fel a gyanús tevékenységeket, és tudjanak helyesen és azonnal reagálni a lehetséges incidensekre. Ezért a Szervezet éves szinten - vagy ha a körülmények megkívánják gyakrabban – képzést tart a biztonsági események kezelése témában. A képzés anyagának tartalmaznia kell a lehető legtöbb, nagy valószínűséggel elforduló biztonsági eseményt, illetve az ezekhez kapcsolódó teendőket.

9.9. BIZTONSÁGI ESEMÉNYEK KEZELÉSE

A Felhasználó köteles az általa tapasztalt rendellenes eseményeket az Informatika csoporttal azonnal közölni, szóbeli közlés esetén legkésőbb a következő munkanapon HelpDesken is megerősíteni. A Felhasználó a rendellenes eseményről szóló tájékoztatása során köteles az esemény valamennyi körülményének részletes feltárására.

Ha a felhasználónak gyanúja támad arra, hogy a jelszavát más személy is megismerte vagy személyazonosító eszközét más megszerezte vagy lemásolta, úgy köteles azonnal jelezni ezt az Informatika csoport felé, továbbá amennyiben a lehetőségei adottak, köteles a jelszavát azonnal megváltoztatni, személyazonosító eszközét letiltatni a megfelelő szolgáltatónál.

Amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás, vagy vírustámadás okozta, az érintett eszközt le kell választani a hálózatról, illetve szükség esetén ki kell kapcsolni. Ez a Rendszergazda feladata.

Vírustámadás esetén fokozottan figyelni kell a cserélhető adathordozókra is. A fertőzött számítógépben használt adathordozók kizárólag a vírusellenőrzést követően használhatók más számítógépeken.

A Rendszergazda gondoskodik arról, hogy a többféle módon (HelpDesk, e-mailben vagy telefonon) bejelentett biztonsági események a nyilvántartásban minden esetben a „Biztonsági esemény" kategóriába kerüljenek. Rendszergazda ezen kívül telefonon vagy személyesen is jelenti az eseményt az IT vezetőnek és az EIBF-nek.

9.25. A BIZTONSÁGI ESEMÉNYEK NYOMONKÖVETÉSE

A biztonsági események bekövetkeztét az események súlyosságától függően és a Biztonsági eseménykezelési tervnek megfelelően dokumentálni kell.

Az IT vezető feladata a szükséges intézkedések meghozatala, a teljes elhárítási folyamat dokumentálása. Az incidensekről készült feljegyzéseket EIBF rendszeresen áttekinti, szükség esetén további helyesbítő, megelőző intézkedésekre tesz javaslatot.

9.27. A BIZTONSÁGI ESEMÉNYEK JELENTÉSE

Minden munkatárs feladata, hogy az információbiztonsági incidenseket, észlelt gyengeségeket jelentse közvetlen felettesének, eredménytelenség esetén az IT vezetőnek.

Biztonsági eseménynek nevezzük az EIR működésében beállt olyan kedvezőtlen változást, amelynek hatására az EIR vagy a benne kezelt adatok bizalmassága, sértetlensége, rendelkezésre állása sérült vagy sérülhet.

A jellemző biztonsági események a következők:

- szoftver vagy hardver hibás működése;
- nem ellenőrzött rendszerbeli változások;
- a bizalmasság és/vagy sértetlenség sérülése;
- informatikai eszközök elvesztése;
- vírusok és egyéb kártevők általi fertőzés;
- túlterheléses támadások (szolgáltatás megtagadó, DDoS támadások);
- az EIR-rel való visszaélés;
- a szabályzatoknak vagy irányelveknek való nem megfelelés;
- a fizikai biztonsági rendelkezések megsértése;
- a hozzáférési előírások megsértése;
- emberi hibák.

A biztonsági esemény bekövetkeztét fajtájuktól és súlyuktól függően jelenteni kell az illetékes hatóságoknak is:

a) Rendőrség: ha a biztonsági esemény bűncselekmény, adatsértés vagy más jogszabálysértés eredménye. A Szervezet vezetője jelenti.
b) NAIH: ha az esemény kapcsolódik személyes adatok kiszivárgásához vagy illetéktelen hozzáféréshez. A DPO jelenti.
c) Kiberbiztonsági incidenskezelő központ (NBSZ-NKI): minden jelentős biztonsági eseményt.

9.31. SEGÍTSÉGNYÚJTÁS A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉHEZ

Az EIBF feladata, hogy tájékoztatást és segítséget nyújtson az EIR felhasználóinak a biztonsági események észlelése, kezelése és jelentése érdekében.

9.34. BIZTONSÁGI ESEMÉNYKEZELÉSI TERV (IRP)

Ezen terv meghatározza azokat az eljárásokat és intézkedéseket, amelyeket a Szervezet végrehajt a biztonsági incidensek kezelése során. A terv célja, hogy leírja azokat az eljárásokat és lépéseket, amelyeket a Szervezet alkalmaz az incidensek felismerése, kezelése kapcsán. A terv a károk minimalizálására törekszik a biztonsági incidensek során, és lehetővé teszi a gyors és hatékony reakciót azokra.

Felelős: IT vezető, EIBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

KÖTELEZŐ ÉRTESÍTÉSI INTÉZKEDÉSEK

A szervezet minden olyan kiberbiztonsági incidensről értesíti a szolgáltatásait igénybe vevőket, amely hátrányosan érintheti a szolgáltatásnyújtásukat, és amelynek kezelése a szolgáltatásokat igénybe vevők részéről intézkedést igényel.

A szervezet haladéktalanul, vagy amint az információ rendelkezésre áll tájékoztatja a jelentős kiberfenyegetés által potenciálisan érintett szolgáltatásait igénybe vevőket az intézkedésekről, illetve fenyegetést orvosló lehetőségekről, amelyeket a szolgáltatások igénybe vevői maguk megtehetnek vagy amelyekkel élhetnek.

INCIDENS BEJELENTÉSE, ÉSZLELÉSE SZERVEZETEN BELÜL

A bejelentés, illetve észlelés kétféleképpen történhet:

- A 9.27 A biztonsági események jelentése pont szerint rögzített módon.
- Automatizált jelentés a biztonsági eseményben érintett rendszertől (pl: Naplótárhely-elfogyásról jelzés a Rendszergazdának)

A BEJELENTÉS FOLYAMATA A KIBERBIZTONSÁGI INCIDENSKEZELŐ KÖZPONT IRÁNYÁBA

ELSŐ BEJELENTÉS

- A jelentős biztonsági incidens tudomásszerzésétől számított 24 órán belül benyújtandó.
- A bejelentés tartalmát a Korm. rendelet 77. § 1. pontja határozza meg.

ESEMÉNYBEJELENTÉS

- Az első bejelentést követően 72 órán belül benyújtandó.
- Frissített, aktualizált információkat és az incidens első értékelését kell tartalmaznia.

ZÁRÓJELENTÉS

- Legkésőbb az Eseménybejelentést követő egy hónapon belül benyújtandó.
- A jelentés tartalmazza az incidens részletes leírását, a kiváltó fenyegetést vagy okokat, és az alkalmazott, vagy folyamatban lévő mérséklési lépéseket. Amennyiben a benyújtásának időpontjában még folyamatban van a kiberbiztonsági incidens, akkor az addig elért eredményekről szóló jelentést.

ADATSZOLGÁLTATÁS

A fertőzöttségi mutatókat haladéktalanul meg kell adni, amint elérhetővé válnak.

KÖZBENSŐ HELYZETJELENTÉS

A Kiberbiztonsági incidenskezelő központ kérésére közbenső helyzetjelentést kell benyújtani.

AUTOMATIZÁLT ESEMÉNYEK KEZELÉSE

Az automatizmus által kezelhető incidensek bejelentése nem kötelező, kivéve az ismétlődő eseteket.

EGYÜTTMŰKÖDÉSI KÖTELEZETTSÉGEK

Az incidens kezelése és kivizsgálása során a Szervezetnek együtt kell működnie a Kiberbiztonsági incidenskezelő központtal, amelynek során köteles az bejelentéssel kapcsolatos információk és az incidensben érintettek, az incidensért felelősök azonosításához szükséges technikai adatok, valamint a vizsgálat lefolytatásához szükséges adatok átadására, a vonatkozó dokumentumok és eszközök biztosítására, az incidensben érintett infrastruktúra speciális, ágazati sajátosságainak megosztására.

A Szervezetnek biztosítania kell a hozzáférést az incidenssel érintett infrastruktúrához, és tájékoztatnia kell a Kiberbiztonsági incidenskezelő központ szakembereit az incidens kezelése során tett intézkedésekről, illetve az infrastruktúrával kapcsolatos beállításokról.

A Szervezet köteles továbbá előzetes egyeztetést követően telepíteni a Kiberbiztonsági incidenskezelő központ által szükségesnek ítélt korai figyelmeztető vagy csapdarendszereket, szenzorokat, abban az esetben, ha azok telepítése nem akadályozza vagy veszélyezteti a szervezet működését.

INCIDENS AZONOSÍTÁSA, KATEGORIZÁLÁSA:

A biztonsági incidensek fajtájuktól függően lehetnek alacsony, közepes és jelentős szintűek.

ALACSONY

Minden olyan esemény, amely kisebb üzemzavart okozhat, de házon belül gyorsan elhárítható.

Ezek lehetnek kisebb problémák, például, ha egy munkaállomás lassabban működik vagy ha kívülről térképezik fel a hálózatot, ezek általában nem befolyásolják a szolgáltatásokat.

Lehetnek olyan helyzetek is, amikor több felhasználó tapasztal zavarokat, például egy funkció nem működik megfelelően vagy megszűnik egy szolgáltatás tartalékrendszere, ami már fokozottabb figyelmet igényel.

KÖZEPES

Összességében közepesnek minősül minden olyan esemény, amely az Alacsony kategóriánál jóval nagyobb hatással van a Szervezetre, de még nem éri el a bejelentésköteles Jelentős incidens

Komolyabb esetekben a hibák közvetlenül akadályozzák a rendszerek használatát, például, ha ismert sérülékenységet kihasználnak, megszakad a kommunikáció vagy egy fontos rendszer elérhetetlenné válik.

A legsúlyosabb esetekben akár a teljes hálózati infrastruktúra veszélybe kerülhet, hosszabb ideig nem működnek alapvető szolgáltatások, vagy érzékeny adatok kerülnek illetéktelen kezekbe.

JELENTŐS

Jelentős biztonsági eseménynek minősül minden olyan esemény, amely

a) a Szervezet által nyújtott szolgáltatás legalább 5%-os kiesésével jár, vagy fenyeget;
b) a Szervezet éves árbevételének legalább 5%-os kiesésével jár, vagy fenyeget;
c) Súlyos működési zavart okoz vagy képes okozni a szolgáltatásokban, vagy pénzügyi vagy reputációs veszteséget okoz vagy képes okozni a kiberbiztonsági incidens által érintett szervezetnek vagy személynek;
d) Személyi sérüléssel, vagy halállal jár, fenyeget;
e) Visszatérő – ugyanazon esemény 6 hónapon belül többször is előfordul.

AZ INCIDENS ELHÁRÍTÁSA:

A Szervezet haladéktalanul kidolgozza és végrehajtja az incidens felszámolásához szükséges intézkedéseket.

TERVEZÉS ÉS ELŐKÉSZÍTÉS

A biztonsági esemény és incidens kezelés tervezési és előkészítési szakaszának lépései, melynek felelőse a Vészhelyzeti vezető.

a) Vészhelyzeti Csoport (Incidenskezelő Csoport) összehívása, amely biztonsági incidens esetén gyorsan és szakszerűen jár el.
b) Biztonsági esemény és incidens pontos meghatározása (milyen eseményeket tekintünk biztonsági incidensnek) az EIBF bevonásával.
c) Az incidens kategóriájának megállapítása.
d) Az incidens kategóriájától és a biztonsági eseménytől függő együttműködés a következő szervezetekkel:
   - Informatika csoport
   - Üzemeltető, fejlesztő és technológia szállító partnerek.

ÉSZLELÉS ÉS JELENTÉS

A kapcsolódó fő feladatok az alábbiak szerint kerültek meghatározásra:

a) Az automatikus eseményfigyelő és feldolgozó rendszerek riasztásainak figyelése és szükség esetén a védelemi intézkedések megerősítése a fenyegetések függvényében.
b) Külső riasztások monitorozása (pl. EIR felügyeletét ellátó szervek riasztásai és értesítései) és szükség esetén a védelemi intézkedések megerősítése a fenyegetések függvényében.
c) A Szervezet határvédelemi és belső biztonságvédelemi rendszereinek és az információ tartalom folyamatos monitorozása.
d) Biztonsági incidensek detektálása:
   - automatikus valós időben, illetve
   - manuálisan.
e) A biztonsági eseményhez kapcsolódó információ gyűjtése és tárolása.
f) Felhasználói bejelentések rögzítése a gyanús eseményekről.
g) Üzemeltetői bejelentések rögzítése a gyanús eseményekről.

VIZSGÁLAT ÉS DÖNTÉS

A vizsgálati és döntési fázis akkor kezdődik, amikor egy biztonsági esemény megjelenik.

A Vészhelyzeti vezető koordinálásával a Vészhelyzeti Csoport (Incidenskezelő csoport) elvégzi a kezdeti felmérést. Azt kell eldönteni, hogy az esemény valóban biztonsági incidens-e. Ha az esemény valóban biztonsági incidens, akkor meg kell határozni a várható hatását a bizalmasságra, sértetlenségre és rendelkezésre állásra vonatkozóan, valamint az érintett rendszerekre az incidens besorolási szabályok alapján kategorizálni kell a biztonsági eseményt, amennyiben az jelentősnek minősül, vagy visszatérő akkor pedig meg kell tenni az Első bejelentést a Kiberbiztonsági incidenskezelő központ részére. Ebben a fázisban a Vészhelyzeti vezetőnek, vagy az általa kijelölt kompetens személynek (pl.: Rendszergazdának, továbbiakban Incidens menedzser) kell a vizsgálatot elvégeznie és a döntést meghoznia.

A Kiberbiztonsági incidenskezelő központ a bejelentésre haladéktalanul és – ha lehetséges – az Első bejelentés kézhezvételétől számított 24 órán belül választ ad. Ennek keretében visszajelzést küld az incidensről a bejelentő szervezetnek, valamint – a szervezet kérésére – útmutatást vagy operatív tanácsokat nyújt a lehetséges mérséklési intézkedések végrehajtásáról.

A Kiberbiztonsági incidenskezelő központ technikai támogatást nyújt, ha az érintett szervezet ezt kéri.

A 4 lehetséges kimenet:

- nem incidens (pl. hibás értesítés);
- alacsony szintű (házon belül kezelhető), vagy;
- közepes szintű (akár külső erőforrás bevonása is szükséges lehet), vagy;
- jelentős szintű (bejelentésköteles).

Amennyiben a normál működés visszaállítása feltételezhetően meg fogja közelíteni a kiesett erőforrás által támogatott alapfeladatok, folyamatok maximálisan megengedhető kiesési idejét (Maximum Tolerable Downtime - MTD), a Vészhelyzeti vezető az állapotot vészhelyzetként kezeli és értesíti az Szervezet legfelső vezetőjét és az EIBF-t.

Az incidens kategóriájától függően el kell végezni:

a) A hozzárendelt vezetők (személyek vagy szerepkörök) értesítését;
b) Az incidens típushoz hozzárendelt, nem állandó Vészhelyzeti Csoport (Incidenskezelő csoport) értesítését és a vezetők és szakértők bevonását az incidens elhárításába;
c) A megadott kapcsolattartókon keresztül a külső partnerek értesítését és a szükséges információ megosztását;
d) Felelős hozzárendelését;
e) Információgyűjtés, illetve szükség esetén bizonyítékok gyűjtésének megkezdését;
f) Az incidens elhárítását.

ELHÁRÍTÁS

Az incidens elhárításának fázisa akkor kezdődik, amikor az Incidens menedzser elvégezte a biztonsági incidens beazonosítását és kategorizálását. A biztonsági incidensre adott válasznak 3 részfolyamata van:

ELSZIGETELÉS ÉS VIZSGÁLAT

Az első lépésben az incidens kategóriájától függően a Vészhelyzeti vezető, vagy amennyiben szükséges a Vészhelyzeti Csoport (Incidenskezelő csoport) dönt, hogy az incidensben érintett rendszereket, rendszerelemeket el kell-e szigetelni, hogy a támadás vagy fertőzés ne tudjon tovább terjedni. Szokásos megoldás

a rendszer leválasztása a hálózatról, vagy a rendszer leállítása. A leválasztott rendszeren lehetőség nyílik az incidens részletes vizsgálatára, a bizonyítékok összegyűjtésére és a megszüntetés módjának eldöntésére, kidolgozására.

A vizsgálat során:

- meg kell határozni, hogy a biztonsági incidens milyen károkat okozott,
- meg kell határozni az azonnali javító intézkedéseket,
- meg kell határozni a biztonsági esemény elhárításának végső megoldását és határidejét,
- meg kell határozni, hogy milyen átmeneti biztonsági intézkedések mellett lehet újraindítani az incidens által érintett rendszert, illetve szolgáltatást, amelyek megakadályozzák az incidens újbóli előfordulását,
- meg kell határozni a megfelelő, a lehetséges kockázatokkal arányos végleges intézkedést, amely megakadályozza a biztonsági incidens újbóli előfordulását,
- a vizsgálatok eredményét és a döntéseket dokumentálni kell.

MEGSZÜNTETÉS

Az elhárítás következő lépése az incidens következtében korrumpálódott vagy gyanús rendszerkomponensek eltávolítása majd „tiszta" változat újra telepítése, vagy a feltört felhasználói fiók deaktiválása. A megszüntetés előtt minden technikai és jogi bizonyítékot össze kell gyűjteni és el kell menteni módosíthatatlan formában. Gondoskodni kell a bizonyítékok megfelelő tárolásáról.

HELYREÁLLÍTÁS

Az incidens okának és hatásainak megszüntetése után az incidens elhárításának utolsó lépése a normál működés visszaállítása.

A helyreállítás történhet:

- Azonnali átmeneti javító intézkedések után egy meghatározott időtartamra, ameddig a végleges javító intézkedések elvégzésre kerülnek;
- Végleges javító intézkedések mellett;
- A helyreállításnak részét kell, hogy képezze a biztonsági rések és folyamathibák kiküszöbölése, annak érdekében, hogy az incidens újból ne következhessen be. A biztonsági rések javítása esetében is megengedett kockázatarányos átmeneti megoldással történő újraindítás, fokozott védelmi készültség mellett. Ezt a döntést az Informatika csoportnak kell meghoznia.

INCIDENS ELHÁRÍTÁS UTÁNI FELADATOK

- Az incidens részletes dokumentálása;
- A sérülékenységi pontokon a védelmi intézkedések továbbfejlesztése, szükség esetén fejlettebb eszközök alkalmazása;
- Szabályozások, eljárásrendek, munkautasítások aktualizálása és továbbfejlesztése;
- Incidenskezelési eljárások továbbfejlesztése;
- Bizonyítékok mentése;
- Ha szükséges igazságügyi vizsgálat lefolytatása;
- Ha szükséges fegyelmi eljárás indítása.

Jelentős szintű biztonsági esemény esetén a Szervezet tájékoztatja az illetékes hatóságot a feltárt hiányosságok megszüntetésére készített incidenskezelési tervről.

Az incidens felszámolását követően a szervezet felülvizsgálja elektronikus információs rendszereinek kockázatelemzését és kockázatkezelését, és végrehajtja a szükséges módosításokat.

10. KARBANTARTÁS

10.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend fő célja, hogy biztosítsa a Szervezet informatikai eszközei és rendszerei megbízható és hatékony működését. Ennek érdekében számos intézkedést és gyakorlatot foglal magában: a szabályozott karbantartásra összpontosít, amely meghatározza és standardizálja a karbantartási folyamatokat a hatékonyság és az egységesítés érdekében. A távoli karbantartás lehetősége is fontos elem, ami lehetővé teszi a távoli hozzáférést a karbantartási munkákhoz, ami hatékonyabb és gyorsabb reakciót tesz lehetővé a problémákra. Végül meghatározza a karbantartást végző személyek felelősségét és kötelességeit is, biztosítva ezzel a megfelelő szakértelmet és felelősséget a karbantartási tevékenységekhez.

Felelős: IT vezető

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

10.2. SZABÁLYOZOTT KARBANTARTÁS

Rendszeres karbantartás

A folyamatos működés biztosítása érdekében az EIR elemeit megadott rendszeres időközönként karban kell tartani.

A hardver eszközök karbantartásának célja, hogy megelőzze az eszközök véletlenszerűen bekövetkező meghibásodását. Ilyen karbantartás lehet például:

a) az eszközök belső portalanítása;
b) az elhasználódó alkatrészek cseréje;
c) a nyomtatók mozgó és szennyeződő alkatrészeinek tisztítása;
d) a szünetmentes tápegységek akkumulátorának öntesztel történő ellenőrzése.

A szoftver elemek karbantartása során kell elvégezni azokat a szerver oldali rendszeres szoftverfrissítéseket, amelyek EIR vagy alapszolgáltatások leállításával járnak.

A karbantartásokat a gyártói ajánlások és a szoftverfrissítésekre vonatkozó előírások figyelembevételével kell végezni.

Karbantartások ütemezése

A karbantartandó eszközök körét és a karbantartás rendszerességét az IT vezető határozza meg, az eszközök alkalmazási körülményeit is figyelembe véve.

Az adott rendszer rendszergazdájának Éves karbantartási tervet kell készítenie, amelyben meg kell tervezni a karbantartások ütemezését.

A karbantartás csak akkor kezdődhet meg, ha azt az IT vezető jóváhagyja

A Szervezet létesítményeiből a rendszerelemek elszállítása karbantartás vagy csere céljából csak az IT vezető jóváhagyásával lehetséges.

Karbantartások folyamata

A tervezett karbantartásokat (és az eseti javításokat) az IT vezetőnek dokumentált formában engedélyeznie kell.

Amennyiben a karbantartás valamely EIR-nek vagy szolgáltatásának a leállításával jár, akkor az érintett felhasználókat a karbantartás megkezdése előtt legalább 1 munkanappal korábban értesíteni kell.

Eszközök kiszállítása

Amennyiben a karbantartáshoz kapcsolódóan adatot tartalmazó adathordozó kiszállítása válik szükségessé, akkor a 11.8 Adathordozók törlése pontban leírtak szerint kell eljárni. Ez alól jellegénél fogva kivételt képez az eszközök külső IT üzemeltető telephelyére történő kiszállítása.

A kiszállítást az IT vezető engedélyezi.

Karbantartások ellenőrzése

Az elvégzett karbantartás után az eszköz fajtájától függően funkcionális és biztonsági tesztet kell végezni, melynek eredményét a Karbantartási naplóban kell rögzíteni.

Sikertelen teszt esetén az eszköz nem helyezhető újra éles üzembe. Az eseményt jelenteni kell az IT vezetőnek, aki dönt a további intézkedésekről.

Karbantartások dokumentálása

A karbantartás elvégzését a Karbantartási naplóban kell dokumentálni, amely egyben az elvégzett karbantartások nyilvántartására is szolgál.

A Naplóban a következő adatokat kell rögzíteni:

a) az érintett EIR(ek) nevét;
b) a karbantartás tárgyát (az érintett hardver/szoftver rendszerelemeket);
c) a karbantartás rövid megnevezését;
d) a karbantartás dátumát és idejét;
e) a karbantartás végzőjét;
f) a karbantartás engedélyezőjét;
g) az elvégzett karbantartás leírását;
h) a karbantartást követő teszt leírását és eredményét.

A Karbantartási naplókat az Informatika csoportnak visszakereshető formában kell tárolnia. A megőrzési idő 3 év.

10.11. TÁVOLI KARBANTARTÁS

A távoli karbantartási és diagnosztikai tevékenységeket akkor lehet végezni, ha az jóváhagyásra kerül az IT vezető által.

A karbantartási eszközöknek teljes mértékben meg kell felelniük a Szervezet által előírt biztonsági követelményeknek, mint a kriptográfiai követelmények teljesítését, valamint az eszközökön elérhető biztonsági funkciók alkalmazását.

Csak erős hitelesítési eljárás után kezdődhet meg a tevékenység (MFA).

A távoli karbantartás egy kötelezően naplózandó tevékenység!

A távoli karbantartás befejeztével automatikusan le kell zárni a hálózati kapcsolatokat, kapcsolódó szolgáltatásokat, minimalizálva a biztonsági kockázatokat.

10.18. KARBANTARTÓ SZEMÉLYEK

Belső karbantartók

A karbantartásokat és javítási munkákat csak arra felhatalmazott, kompetens személy végezheti:

a) A hardver hibák felderítését és a speciális szakismeretet, szerszámokat és anyagokat nem igénylő hardver karbantartásokat, javításokat az Informatika csoport munkatársai végzik.
b) A speciális szakismeretet, szerszámokat vagy anyagokat igénylő karbantartások és javítások (és a jótállási időn belüli garanciális javítások) elvégzésére az IT vezető megbízhat külső partnereket.

A külső partnerrel történő karbantartások/javíttatások ügyintézését az Informatika csoport adott eszközért felelős munkatársai végzik.

Külső karbantartó partnerek igénybevétele esetén a Külső karbantartók pontban leírtakat kell alkalmazni.

Külső karbantartók

Abban az esetben, ha az EIR karbantartását az Informatika csoport nem tudja elvégezni, vagy egyéb kötelezettségek miatt nem végezheti el, akkor az IT vezető kezdeményezi a külső partner megbízását.

Karbantartási tevékenységet csak olyan külső partner végezhet, aki érvényes szerződéssel rendelkezik, a titoktartási nyilatkozatot aláírta és dokumentált formában megismerte a Szervezetre vonatkozó információbiztonsági előírásokat.

A karbantartást végző hozzáféréssel rendelkező külső partnerekről nyilvántartás kell vezetni (Külső karbantartók nyilvántartása), melynek minimálisan a következőket kell tartalmaznia:

a) a karbantartó szervezet/személy megnevezését, címét;
b) a szerződés/megrendelés tárgyát (mely rendszerelemekre terjed ki);
c) a szerződés/megrendelés időtartamát;

Külső partner munkavégzése esetén az IT vezetőnek ki kell jelölnie azokat a munkatársakat, akiknek folyamatos felügyeletet kell biztosítani a karbantartás során.

A külső partnerrel kötött szerződésbe bele kell foglalni, hogy a karbantartást felügyelő munkatársak jogosultak kérni a karbantartást végzők személyazonosságának igazolását, illetve, hogy a karbantartást végző személynek kötelessége a felszólításra a szükséges iratokat bemutatni.

Ha a karbantartás során a Szervezet EIR-hez logikailag hozzá kell férni, a Rendszergazda kötelessége és felelőssége a hozzáférés során folyamatos felügyelet alatt tartani karbantartást végző személyeket.

11. ADATHORDOZÓK VÉDELME

11.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Ezen eljárásrend célja a szervezeti- folyamat- és rendszer szintű követelményeket tartalmazó analóg és digitális adathordozók biztonságának fokozott és strukturált biztosítása és védelme a Szervezetben.

Felelős: IT vezető, EIBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

11.2. HOZZÁFÉRÉS AZ ADATHORDOZÓKHOZ

Az EIR-ben csak a Szervezet tulajdonában lévő, regisztrált adathordozót lehet használni. Nem a Szervezet tulajdonában lévő adathordozókat csatlakoztatni a Szervezet EIR-hez kizárólag az IT vezető tudtával és engedélyével lehet.

A Szervezeten belül jelenleg engedélyezett adathordozó típusokat, az adathordozókhoz hozzáférő szerepköröket, a hozzáférés módját és célját az alábbi táblázat tartalmazza:

Adathordozó típus	Szerepkör	Hozzáférés / jogosítvány
EIR szerver oldali háttértárai (HDD, SSD)	Rendszergazda	Fizikai, logikai / karbantartás, mentés, visszaállítás
	Felhasználó	Logikai / szerepkörének megfelelően
Szerver oldali, központi mentések adathordozói	Rendszergazda	Fizikai, logikai / tárolás, mentés, visszaállítás
Munkaállomások háttértárai (HDD/SSD, mobiltelefon, fényképezőgép, kártyaolvasó	Rendszergazda	Fizikai, logikai / karbantartás, mentés, visszaállítás
	Felhasználó	Logikai / szerepkörének megfelelően
Munkaállomás mentések adathordozói (pendrive, külső HDD)	Rendszergazda	Fizikai, logikai / karbantartás, mentés, visszaállítás
	Felhasználó	Fizikai, logikai / tárolás, mentés, visszaállítás
Rendszerelemek telepítő adathordozói (pendrive, DVD)	Rendszergazda	Fizikai, logikai /tárolás, telepítés
Készenléti terveket (Készenléti tervet) és vészhelyzeti adatokat tároló adathordozók (DVD, pendrive)	A Készenléti tervekben megadott szereplők	Fizikai, logikai / a Készenléti tervekben leírt műveletek elvégzése és a tervek karbantartása
Analóg adathordozók (iratok, fénymásolatok, jegyzetek, rajzok, térképek, fotók	Felhasználó	Fizikai / munkakörének/szerepkörének megfelelően

ADATHORDOZÓK KÖRNYEZETI HATÁSOKTÓL VALÓ VÉDELME

Az adathordozókat mindig a gyártói előírásoknak (a csomagoláson vagy a kísérő dokumentációban leírtaknak) megfelelően kell kezelni.

Az adathordozókat óvni kell mindenféle:

- mechanikai hatástól (pl.: ütés, hajlítás, karcolás);
- mágneses elvű adathordozók esetén mágneses hatástól;
- egyéb külső hatástól (pl.: hő, maró anyagok, nedvesség);
- szennyeződéstől (pl.: por, korom);

A védelemről a kezelésért, tárolásért felelős munkatársnak kell gondoskodnia.

Az adathordozók nem megfelelő kezelése az adathordozón lévő adatok elvesztéséhez, illetve az adathordozót használó eszköz károsodásához vezethet.

11.8. ADATHORDOZÓK TÖRLÉSE

Az adathordozók vagy adathordozót tartalmazó informatikai eszközök újrahasznosítása, mások rendelkezésre bocsátása vagy selejtezése előtt minden esetben gondoskodni kell arról, hogy az adathordozón tárolt adatok visszaállíthatatlanul eltávolításra kerüljenek.

Ennek érdekében helyreállíthatatlanságot biztosító törlési technikákkal törölni kell az adatokat (olyan szoftvert alkalmazásával, amely többszörösen felülírva törli az adatokat), vagy az adathordozót roncsolással fizikailag kell használhatatlanná tenni, megsemmisíteni.

A törlést vagy megsemmisítést az adathordozón lévő adatok gazdájának előzőleg jóvá kell hagynia.

Garanciális eszközök esetén, ha az eszköz hibája miatt nincs mód az adatok törlésére, az IT vezető dönt az adathordozó cserére történő kiadhatóságáról vagy megsemmisítéséről.

Az adatok eltávolítását a Rendszergazda végzi.

Az adatok eltávolításának tényét és módszerét az eltávolítást végző munkatársnak jegyzőkönyveznie kell.

11.14. ADATHORDOZÓK HASZNÁLATA

Az EIR-hez kapcsolódó munkaállomásokon a felhasználók számára általában tilos a külső adathordozók (pl.: CD, DVD, pendrive, külső merevlemez) használata. Ezeken a munkaállomásokon külső adathordozókat csak az Informatika csoport munkatársai használhatnak a munkaállomás karbantartása (pl.: vírusirtás, telepítés, mentés vagy visszaállítás) céljából.

Egyes felhasználók– amennyiben munkakörükhöz kapcsolódik, vagy az adott munkafolyamat megkívánja – munkahelyi vezetői engedéllyel használhatnak külső adathordozókat. Ezen adathordozókat minden használat előtt a vírusvédelemnek ellenőrizni kell.

Otthoni munkavégzés és bármilyen más célból bármilyen adatot CD-n, DVD-n, pendrive-on, külső merevlemezen, elektronikus levélben, Interneten vagy bármilyen más módon az EIR-ből kijuttatni csak az Adatgazda írásos engedélyével szabad.

Az eszközhasználatot az EIR-hez történő csatlakoztatása után, az érintett szervezet minden előzetes értesítés nélkül figyelheti, ellenőrizheti.

A Szervezet az adathordozók használatát információbiztonsági megfontolásból hardver, illetve szoftver úton korlátozhatja.

Olyan adathordozó használata, amelynek nincs azonosítható tulajdonosa, szigorúan tilos!

12. FIZIKAI ÉS KÖRNYEZETI VÉDELEM

12.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend célja az EIR-t koncentráltan tartalmazó épületek védelme, biztosítva a fizikai belépési engedélyeket, ellenőrizve a belépést, a fizikai hozzáféréseket és felügyelve az adatátviteli eszközök, kimeneti eszközök hozzáférését. Az eljárásrend magában foglalja az áramellátó berendezések biztosítását, vészhelyzeti tápellátást, valamint tűzvédelmi és környezeti védelmi intézkedéseket.

Felelős: IT vezető

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

12.2. A FIZIKAI BELÉPÉSI ENGEDÉLYEK

A Szervezet azon telephelyein, amelyek informatikai eszközöket, illetve infrastruktúrát tartalmaznak, elektronikus beléptető rendszer működik, ennek megfelelően csak beléptető kártyával, illetve előre leadott névjegyzék alapján lehet be- és kilépni.

A Szervezet összeállítja, jóváhagyja, és kezeli az EIR-eknek helyt adó létesítményekbe belépésre jogosultak listáját. A Szervezettel jogviszonyban vagy munkaviszonyban álló valamennyi személynek rendelkeznie kell a beléptető rendszer használatához szükséges kártyával.

A beléptető rendszerben rögzített adatok a munkavégzés, illetve az épületben tartózkodás időtartamának rögzítésére szolgálnak.

A Munkaügyi ügyintéző évente felülvizsgálja a belépésre jogosultak listáját.

Új jogviszony létesítése esetén a Fizikai biztonsági felelős a Munkaügyi ügyintéző tájékoztatása alapján rögzíti az új munkatársat a beléptetőrendszerben. Az új munkatárs beléptető kártyájának kiadásáról szintén ő gondoskodik a beléptető rendszerben történt regisztrálást követő első munkanapon.

A kártya kiadásának alapjául szolgáló jogviszony megszűnése esetén az utolsó munkában töltött napon a kártya birtokosa a kártyát leadja a Fiziki biztonsági felelős részére, aki a kártya érvénytelenítéséről is gondoskodik.

12.6. A FIZIKAI BELÉPÉS ELLENŐRZÉSE

A Szervezet épületeibe csak a hivatalos ki- és belépési pontokon engedélyezett a ki- és belépés. A ki- és beléptetés rendszerét és módját a Tulajdonvédelmi szabályzat tartalmazza

Az informatikai helyiségekbe való belépésre csak abban az esetben adható felhatalmazás, ha az adott személynek arra:

- munkaköri kötelességének, feladatának ellátásához,
- külső személy esetén a Szervezettel szembeni szerződéses kötelezettség teljesítéséhez szüksége van (Ebben az esetben csak a helyiségbe belépésre felhatalmazott munkavállaló kíséretével léphet be ezekre a területekre).

Az informatikai helyiségekbe való belépés – az első bekezdésben foglaltak alkalmazása mellett – állandó jelleggel csak az IT vezető, az Informatika csoport rendszergazdája, valamint az EIBF számára engedélyezhető. Az engedély kiadása, nyilvántartása, felülvizsgálata, valamint a fizikai belépéseket ellenőrző eszközök nyilvántartásának vezetése az IT vezető felelőssége.

A külső partnerek belépését az informatikai helyiségekbe az IT vezető engedélyéhez kell kötni. Külső partnertől igénybe vett IT szolgáltatás esetén azon géptermekbe, ahol a Szervezet szerverei kerülnek elhelyezésre, a szolgáltató vezetője engedélyezheti a belépést.

A Szervezet a kijelölt pontokon való átjutást felügyeli fizikai belépést ellenőrző rendszerrel vagy eszközzel.

A fizikai hozzáférési kódok és kulcsok kompromittálódása esetén a kódok és kulcsok cseréje szükséges. Abban az esetben is cserélni kell a kódokat és kulcsokat, ha az azokkal rendelkező személy elveszíti a belépési jogosultságát.

12.17. A FIZIKAI HOZZÁFÉRÉSEK FELÜGYELETE

A Szervezet ellenőrzi az EIR-nek helyt adó létesítményekbe, és az irodai térben történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményt és reagáljon arra. Az Informatika csoport rendszeresen átvizsgálja a fizikai hozzáférésekről készült naplókat, sértetlenség, bizalmasság és rendelkezésre állás szempontjából.

Ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak, megkezdi az esemény kivizsgálását a belső ellenőrzés, az Adatvédelmi felelős bevonásával. A vizsgálatot megelőzően gondoskodik a naplóállományok zárolásáról.

A belső ellenőrzés összehangolja a biztonsági események kezelését, valamint a napló átvizsgálások eredményét.

12.22. LÁTOGATÓI HOZZÁFÉRÉSI NAPLÓK

A látogatói belépésekről szóló digitális nyilvántartást a szervezet 1 évig megőrzi. A látogatói belépésekről szóló papír alapú nyilvántartást 1 évig megőrzi. A nyilvántartást havonta át kell vizsgálni, és az észlelt rendellenességekről tájékoztatni kell az IT vezetőt, szükség esetén az EIBF-t.

12.28. VÉSZHELYZETI TÁPELLÁTÁS

Az adatközpontot elegendően nagy kapacitású szünetmentes tápegységgel kell ellátni, amely biztosítja a tartalék áramellátásra történő átkapcsolás vagy a rendszerek leállításához szükséges ideig a szünetmentes áramellátást. Hosszabb áramszünetek esetére aggregátoros tartalék áramellátást kell biztosítani.

12.31. VÉSZVILÁGÍTÁS

A Szervezet automatikus vészvilágítási rendszert alkalmaz és tart karban, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat.

12.33. TŰZVÉDELEM

Az épületen belül a tűzrendészeti szabályok betartása egységesen vonatkozik minden az épületben tartózkodó személyre. Az épületen belül a dohányzás nem megengedett. Dohányozni csak a célra kijelölt helyen szabad.

Az épület kijelölt pontjain kötelező tűzoltó eszközöket elhelyezni. Csak az ellenőrzéseken átesett érvényes jegyzőkönyvezett készülékek használhatóak. Az ellenőrzések végrehajtásának módját és dokumentálásának követelményeit a Tűzvédelmi szabályzat tartalmazza.

12.37. KÖRNYEZETI VÉDELMI INTÉZKEDÉSEK

A szerverszoba üzemi hőmérsékletének szabályozásának érdekében az alábbi szempontok figyelembevétele szükséges:

- A szerverszobában klíma-berendezéseket kell üzemeltetni, a megfelelő üzemi hőmérséklet szabályozására.
- A klíma berendezések darabszámát, és teljesítményét úgy kell tervezni, hogy a szerverszobában nem csak a jelenleg elhelyezett eszközök, hanem a jövőbeli, maximális kihasználtság esetén is (az eszközök hődisszipációs mutatóit figyelembe véve), még egy klímaberendezés meghibásodása esetén is biztosítani tudják a megfelelő szabályozást.
- A klíma-berendezések automatikus újra indítását biztosítani kell az esetleges áramszünet megszűnése esetén.

A szerverszoba hőmérsékletét folyamatosan monitorozni kell. Az optimális hőmérséklet +10 Celsius és +25 Celsius fok közötti, illetve a páratartalom nem haladhatja meg a 70%-ot. Amennyiben ezen értékek eltérnek az optimálistól, a rendszernek riasztást kell kiküldeni elsődlegesen az Informatika csoportnak.

12.40. VÍZ-, ÉS MÁS, CSŐVEZETÉKEN SZÁLLÍTOTT ANYAG OKOZTA KÁR ELLENI VÉDELEM

A Szervezet védi az EIR-t a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzáró szelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek.

12.42. BE- ÉS KISZÁLLÍTÁS

A Szervezet vezetője, illetve az IT vezető engedélyezheti, vagy tilthatja, továbbá ellenőrizheti a létesítményeibe bevitt, illetve onnan kivitt információs rendszerelemeket. A behozott és kivitt rendszerelemekről az Informatika csoport nyilvántartást vezet.

13. TERVEZÉS

13.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Az eljárásrend célja az információbiztonság biztosítása, a működés szabályozása és a felhasználói felelősség egyértelmű meghatározása a szervezeten belül.

További célja a rendszerbiztonsági terv kidolgozása és végrehajtása, amely biztosítja a megfelelő védelmet az EIR számára.

Emellett meghatározza és rögzíti a viselkedési szabályokat, ideértve a közösségi média és külső webhelyek, alkalmazások használatára vonatkozó korlátozásokat is.

BIZTONSÁGI TERVEZÉSI ELVEK

Biztonsági tervezésnél a következő elveket kell alkalmazni:

a) Rendszer integritás
A rendszernek ellenállónak kell lennie a rosszindulatú támadásokkal és a belső hibákkal szemben. A rendszerek és szolgáltatások integritását folyamatosan ellenőrizni kell, és biztosítani kell az adatok, rendszerek és hálózatok védelmét az illetéktelen módosítással szemben.

b) Védelem rétegezése
A biztonságot több rétegben kell beépíteni a rendszerbe, hogy a hibák és támadások egy rétegből a másikba való átterjedése ne legyen könnyen kivitelezhető. A rétegezésnek magában kell foglalnia a hálózati, rendszer- és alkalmazási szintű védelmi intézkedéseket.

c) Legkisebb jogosultság elve
A felhasználóknak csak azokat a jogosultságokat kell kapniuk, amelyek feltétlenül szükségesek a munkavégzéshez. A rendszereknek szigorú hozzáférési ellenőrzési mechanizmusokkal kell rendelkezniük, és a jogokat rendszeresen felül kell vizsgálni.

d) Biztonsági teljesítmény mérése
A rendszernek meg kell felelnie az alkalmazandó biztonsági előírásoknak és szabványoknak. A biztonsági intézkedések hatékonyságát rendszeresen ellenőrizni kell, és a szabványokkal való összhangot dokumentálni kell. Lásd 5. Értékelés, engedélyezés, monitorozás.

e) Rendszeres felülvizsgálat
A rendszer biztonsági intézkedéseinek hatékonyságát időről időre ellenőrizni kell, és szükség esetén módosítani kell őket. Az incidensek és sérülékenységek elemzésére rendszeres vizsgálatokat kell végezni, és az eredményeket dokumentálni szükséges. A dokumentálás a felülvizsgálatot végzők feladata.

BIZTONSÁGI KÖVETELMÉNYEK

A biztonság tervezésekor a következő követelményeknek kell megfelelni:

a) Azonosítás és hitelesítés
Biztosítani kell, hogy csak engedélyezett felhasználók férhessenek hozzá a rendszerhez, és azonosításuk és hitelesítésük megfelelő módon történjen. Kötelező az erős jelszavak használata, és lehetőség szerint többtényezős azonosítást kell használni.

b) Adatvédelem
A bizalmas és személyes adatokat megfelelő módon kell kezelni és védeni a jogellenes hozzáférés, megváltoztatás vagy elvesztés ellen. Szabályozni kell az adatok gyűjtését, tárolását, feldolgozását és megosztását, és megfelelő titkosítási és hozzáférési irányelveket kell követni a Szervezet belső irányelvei és szabályzatai alapján.

c) Hálózatbiztonság
A hálózati kommunikáció biztonságának meg kell felelnie a legfrissebb biztonsági szabványoknak és meg kell védenie a külső támadásoktól. Tűzfalakat, hálózati szegmentálást, IDS (intrusion detection) és IPS (intrusion prevention) rendszereket kell bevezetni, valamint szigorú hálózati forgalomellenőrzést szükséges alkalmazni.

d) Rendszerszintű biztonság
A rendszernek megfelelő védelemmel kell rendelkeznie a rosszindulatú szoftverek, a tűzfal áttörési kísérletek, a DDOS és bruteforce támadások, illetve más fenyegetések ellen. A rendszerfrissítéseket és javításokat rendszeresen kell végrehajtani, és telepíteni, és alkalmazni a legfrissebb biztonsági patcheket.

e) Rendszerfigyelés
Rendszeresen ellenőrizni kell a rendszer állapotát, hogy figyelmeztetéseket kaphasson a Szervezet a biztonsági incidensekről vagy rendszerhibákról. A logokat és az incidensek nyomon követését megfelelően dokumentálni szükséges, lehetőleg automatizált eszközöket kell használni a rendszerfigyelésre és a biztonsági incidensek időben történő azonosítására.

f) Vészleállítás
Biztosítani kell, hogy a rendszer vészhelyzet esetén gyorsan helyreállítható, az adatok elvesztése minimális legyen. Rendszer biztonsági tervet kell készíteni, amely tartalmazza a rendszeres adatmentést, a redundáns rendszerarchitektúra leírását és a vészleállítási teszteket.

BIZTONSÁGI TESZTELÉS

Rendszeresen kell biztonsági teszteket végezni a tervezési és fejlesztési folyamat során. Ezek magukban foglalhatják a sebezhetőségvizsgálatokat, sérülékenységi vizsgálatokat és biztonsági elemzéseket.

Évente, vagy gyakrabban kell sérülékenységi vizsgálatot végezni, hogy azonosítsuk a biztonsági sebezhetőségeket és az esetleges gyengeségeket a rendszerben. Ez lehetővé teszi a problémák korai azonosítását és a szükséges javítások végrehajtását a rendszerbiztonság javítása érdekében.

Ha lehetőség van rá, ellenőrizni kell a forráskódot is, hogy kizárjuk a biztonsági hibákat és sebezhetőségeket. A kódellenőrzési folyamat magában foglalhatja a statikus kódvizsgálatot, a manuális kódellenőrzést és az automatizált sebezhetőségi szkennereket.

DOKUMENTÁCIÓ ÉS KÉPZÉS

Rendszeresen dokumentálni kell a biztonsági tervezési és fejlesztési folyamatokat. Ez magában foglalhatja a rendszerterveket, biztonsági irányelveket, incidenskezelési eljárásokat és egyéb kapcsolódó dokumentációkat. Az aktuális dokumentációt mindig elérhetővé kell tenni az érintett felek számára úgy, hogy illetéktelenek viszont ne férhessenek hozzá.

Megfelelő képzést kell biztosítani az alkalmazottaknak a biztonsági politikák és eljárások megismerése érdekében. Az új alkalmazottaknak biztonsági oktatást kell kapniuk, és rendszeresen kell frissítő tréningeket tartani a biztonsági tudatosság növelése érdekében.

Felelős: IT vezető, Fejlesztők

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

13.2. RENDSZERBIZTONSÁGI TERV

Az EIR-ekhez Rendszerbiztonsági tervet kell készíteni, amely tartalmazza az EIR

a) rendszerelemeit,
b) alapfeladatát
c) szolgáltatásait.

A tervnek a továbbiakban meg kell határoznia a kapcsolódó szerep- és felelősségi köröket, illetve az EIR által feldolgozott, tárolt és továbbított információk típusát. Ezek mellett tartalmaznia kell - megfelelően alátámasztott módon – a biztonsági osztályát és az EIR-t érintő fenyegetéseket.

Dokumentálni kell a következőket:

a) vonatkozó biztonsági követelmények (alap-, illetve, ha kell, akkor kiegészítő intézkedések)
b) vonatkozó biztonsági intézkedéseket és azok indoklását
c) biztonsági intézkedések végrehajtásának felelőseit, végrehajtóit.

Gondoskodni kell arról, hogy a tervet a felelősök tekintsék át és hagyják jóvá, valamint ismertessék meg mindazokkal, akik az EIR üzemeltetésében, vagy az esetleges vészhelyzeti koordinációban részt vesznek.

A Rendszerbiztonsági terveket a felelősöknek évente felül kell vizsgálni, és frissíteni, ha az EIR-ben, vagy annak üzemeltetési környezetében, változások történnek.

13.3. VISELKEDÉSI SZABÁLYOK

A Szervezet alkalmazottai munkájukból kifolyólag hozzáférést kapnak a Szervezet belső hálózatához. Az Intranet használatának kizárólagos célja a munkavégzés, a Felhasználó nem jogosult magáncélra használni a belső hálózatot.

A hálózat nem használható az alábbi módon, illetve az alábbi tevékenységekre:

- A hatályos magyar törvényekbe ütköző cselekmények.
- A hálózathoz kapcsolódó más - hazai vagy nemzetközi - hálózatok szabályaiba ütköző tevékenységek.
- A hálózat, illetve erőforrásai normális működését megzavaró, veszélyeztető tevékenység (idegen jelszó kiderítése saját és idegen hálózatban, idegen felhasználói név használata az illető tudomása nélkül).
- A hálózatot, illetve erőforrásait indokolatlanul vagy szándékosan túlzott mértékben, pazarló módon igénybe vevő tevékenység (pl. levélbombák, elektronikus játékok, online rádió).

- A hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, módosítása, törlése.
- A hálózat biztonságát veszélyeztető információk, programok terjesztése.
- Mások személyiségi jogait, vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység (pl. pornográf anyagok közzététele).
- Mások munkájának indokolatlan és túlzott mértékű zavarása vagy akadályozása (pl. kéretlen levelek).
- Tilos az Interneten keresztül belső használatú, bizalmas vagy titkos dokumentumokat, adatokat a Szervezetből engedély nélkül kijuttatni, illetéktelen személyek részére hozzáférhetővé tenni.

A tiltott magatartási formák előkészítése, illetve kísérlete is szankcionálható.

TILTOTT TEVÉKENYSÉGEK

a) Tilos olyan tevékenységet végezni, amely célja mások adatainak jogosulatlan megszerzése, megváltoztatása, letörlése.
b) Tilos más felhasználók nevében tevékenykedni.
c) A Felhasználó nem teheti lehetővé mások számára, hogy a nevében tevékenykedjenek. Ezért – többek között – mindent meg kell tennie a jelszavai titkosságának megőrzése érdekében azért, hogy a személyazonosító eszközeit (például, de nem kizárólag: VPN kulcs, azonosító kártya, mobil telefon) más ne használhassa.
d) A Felhasználó köteles törekedni arra, hogy az általa pillanatnyilag használatba vett rendszerekben más személy az ő nevében ne fejthessen ki aktivitást.
e) Tilos más munkavégzését korlátozó tevékenységet végezni nem munka céljából kifejtett aktivitással.
f) Tilos a rendszer bármely elemének eredeti felhasználási céljától eltérő használata vagy az erre irányuló próbálkozás.
g) Tilos a Felhasználók számára a hálózati forgalom figyelése, erre alkalmas szoftver telepítése.
h) Tilos a Szervezet rendszergazdájától kapott IP címtől eltérő más IP cím jogosulatlan használata.
i) Tilos olyan anyag továbbítása, letöltése vagy közzététele az interneten, amely a Magyar- és az Európai Uniós törvényeket sérti.
j) Tilos a Szervezet belső EIR-én kívüli helyszínről elérni vagy megpróbálni elérni a rendszert, kivéve, ha erre az IT vezető engedélyt ad.
k) Tilos külső személy számára információt adni a rendszer valamely hibájáról, sebezhető pontjáról.
l) Tilos a szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele.

13.4. VISELKEDÉSI SZABÁLYOK – KÖZÖSSÉGI MÉDIA ÉS KÜLSŐ WEBHELYEK, ALKALMAZÁSOK HASZNÁLATÁRA VONATKOZÓ KORLÁTOZÁSOK

A Szervezet alkalmazottai munkájukból kifolyólag hozzáférést kapnak az Internethez. Az Internet használatának kizárólagos célja a munkavégzés. A Felhasználó munkaidőben nem jogosult magáncélra használni a web elérését.

Az Internet nem használható az alábbi módon, az alábbi tevékenységekre:

- A Szervezet által nem jóváhagyott eszközökről és hálózatokról internetelérést igénybe venni. Tilos az engedély nélküli eszközök vagy személyes hálózatok használata.

- A hatályos magyar törvényekbe ütköző cselekmények, ideértve, de nem korlátozva azokra: mások személyiségi jogainak megsértése; tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték); a szerzői jogok megsértése; szoftver szándékos és tudatos illegális terjesztése.
- A hálózathoz kapcsolódó más - hazai vagy nemzetközi - hálózatok szabályaiba ütköző tevékenységek, amennyiben ezek a tevékenységek ezen hálózatokat érintik.
- Profitszerzést célzó direkt üzleti célú tevékenység (pl. bérletöltés), reklámok terjesztése.
- A hálózat biztonságát veszélyeztető információk, programok terjesztése.
- Mások személyiségi jogait, vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység (pl. pornográf anyagok közzététele).
- Tilos az üzleti titoknak minősülő vagy más érzékeny információk interneten történő megosztása. Az ilyen információkat csak a Szervezeti rendszeren belül szabad tárolni és kezelni.

A közösségi hálózatokon való részvétel során kötelező tiszteletteljes és etikus viselkedést tanúsítani. Az online platformokon tilos olyan tartalmak közzététele, amelyek sértik vagy ártanak a Szervezet jó hírnevének. Vigyázzanak arra, hogy az online jelenlétük pozitív és támogató legyen a szervezeti értékeknek és szabványoknak megfelelően.

13.10. BIZTONSÁGI KÖVETELMÉNYEK KIVÁLASZTÁSA

Az EIR alapvető, minden rendszerre érvényes követelményei a következők:

HOZZÁFÉRÉSI ELLENŐRZÉS

Azonosítsa és hitelesítse az egyes felhasználókat vagy rendszerelemeket, és biztosítsa, hogy csak a jogosultak férjenek hozzá az adott erőforrásokhoz vagy funkciókhoz.

ERŐS HITELESÍTÉS

Követelje meg erős jelszavak használatát, és alkalmazzon kétlépcsős azonosítást az arra alkalmas rendszereknél.

TITKOSÍTÁS

Védje az érzékeny adatokat megfelelő titkosítási módszerekkel, hogy megakadályozza az illetéktelen hozzáférést.

RENDSZERFRISSÍTÉSEK

Rendelkeznie kell az alkalmazások, az operációs rendszer és egyéb szoftverek a legújabb biztonsági hibajavításaival és frissítéseivel.

NAPLÓZÁS ÉS NAPLÓVIZSGÁLAT:

Naplóznia kell a rendszereseményeket, beleértve a hozzáférési próbálkozásokat, hogy azonosítsa a potenciális fenyegetéseket vagy jogosulatlan tevékenységeket.

13.11. BIZTONSÁGI KÖVETELMÉNYEK TESTRE SZABÁSA

Ezen követelményeket minden EIR esetén egyedileg kell meghatározni.

14. SZEMÉLYI BIZTONSÁG

14.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed a Szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki a Szervezet EIR-rel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az EIR-rel tényleges vagy feltételezhető kapcsolatba kerülő személy nem a Szervezet alkalmazottja, 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).

A Szervezet minden alkalmazottjának titoktartási nyilatkozatot kell aláírnia, melyben nyilatkozik arról, hogy a munkája, tevékenysége során tudomására jutott, a Szervezet számára értéket jelentő információt sem jogviszonya fennállása idején, sem annak megszűnése után nem hozza harmadik fél tudomására.

A titoktartási nyilatkozat a munkaszerződés részét kell, hogy képezze, amelyről a Munkaügyi ügyintéző vezetőjének kell gondoskodnia.

Felelős: Munkaügyi ügyintéző, EIBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, a Rendszergazdával, valamint a Személyüggyel minden esetben ismertetni kell.

14.2. MUNKAKÖRÖK BIZTONSÁGI SZEMPONTÚ BESOROLÁSA

A Szervezet minden munkakört, kapcsolódó feladatot biztonsági szempontból besorol, a besorolás 4 szintre tagozódik, melyek szorosan kapcsolódnak a szervezeti ábrához.

- Felhasználó (Alacsony biztonsági elvárások)
- Középvezető (Közepes biztonsági elvárások)
- Felső vezető (Magas biztonsági elvárások)
- Rendszergazda, Fejlesztő (Kiemelt biztonsági elvárások)

Az alacsony biztonsági elvárásokkal rendelkező felhasználók kizárólag a munkakörük ellátásához szükséges, minimális jogosultságokkal férhetnek hozzá az EIR-ekhez. Számukra elegendő az egyszerű hitelesítés, azonban érzékenyebb rendszerek esetén ajánlott a többtényezős azonosítás bevezetése. A tudatosság fenntartása érdekében évente kötelező részt venniük információbiztonsági képzésen, és nem rendelkeznek rendszerszintű jogosultságokkal vagy konfigurációs hozzáféréssel.

A közepes biztonsági elvárások szintjén lévő középvezetők számára már bővebb hozzáférés engedélyezett a vezetői döntésekhez és az irányított folyamatokhoz kapcsolódóan, de ez kizárólag a szükséges adatkörökre terjedhet ki. Emellett ők kötelesek betartani és betartatni az információbiztonsági előírásokat a beosztott munkavállalókkal is.

A magas biztonsági elvárások szintjéhez tartozó felső vezetők kiemelt stratégiai pozíciót töltenek be, ezért hozzáférésük általában széles körű, de elsősorban döntéshozatali és jelentésértékelési célokra korlátozódik.

Esetükben a kétlépcsős azonosítás alkalmazása kiemelten javasolt, továbbá elengedhetetlen a rendszerhasználatuk folyamatos felügyelete, valamint a speciálisan számukra kialakított információbiztonsági képzések elvégzése, amelyek a kockázatok kezelésére, a jogszabályi megfelelésre és az irányítási kötelezettségekre fókuszálnak. Amennyiben biztonsági esemény merül fel, a felső vezetők kulcsszerepet kapnak az azonnali döntések meghozatalában és az incidensek megfelelő szintű kezelésében.

A rendszergazdák és fejlesztők munkája különösen érzékeny biztonsági területnek számít, mivel tevékenységük során közvetlen hozzáféréssel rendelkeznek a szervezet rendszereinek mélyebb rétegeihez, beleértve az operációs rendszereket, konfigurációs beállításokat és forráskódokat. Mivel ezek a szerepkörök jelentős kockázatot hordoznak, ezért kiemelten szigorú kontrollokat kell alkalmazni velük szemben. A munkavégzésük megkezdése előtt nélkülözhetetlen az előzetes megbízhatósági vizsgálat lefolytatása, amelynek célja annak ellenőrzése, hogy a személy megbízhatóan láthat-e el ilyen típusú munkakört. Minden rendszerszintű hozzáférésüket részletesen naplózni kell, kizárólag titkosított kommunikációs csatornák használata engedélyezett, és minden hozzáféréshez többtényezős hitelesítés) alkalmazása kötelező annak érdekében, hogy illetéktelen hozzáférés ne történhessen.

A Szervezetnél az egyes pozíciók részletes biztonsági szempontú besorolása és dokumentálása a Munkaügyi ügyintéző feladata.

A Szervezet bármely munkaviszony keletkeztetésekor felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat.

A Szervezet évente felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.

14.3. SZEMÉLYEK HÁTTÉRELLENŐRZÉSE

Előzetes háttérellenőrzés

A munkaerő felvétel részét képezi, hogy a Szervezet a személyi állományba jelentkezőn háttérellenőrzés végez. Ezen ellenőrzésnek a részét képezik a következők:

- Személyazonosság-ellenőrzés
- Végzettség és képesítések ellenőrzése
- Munkatapasztalat-ellenőrzés.
- A megadott referenciák felkeresése és véleményük kikérése a jelölt munkavégzéséről és megbízhatóságáról.
- A jelölt közösségi média profiljainak ellenőrzése a nyilvánosan elérhető információk alapján.

Ellenőrzés hozzáférési jogosultságok megadása előtt

A Szervezet az EIR-hez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy a besorolásnak megfelelő feltételekkel rendelkezik-e. Ezen feltételek ismételt vizsgálata szükséges, amennyiben a személy jogosultsági szintje, munkaköre változik.

A Szervezet tevékenysége, a kezelt adatok és rendszerek jellege alapján nem indokolt az előzetes háttérellenőrzést követően a személyek ismételt háttérellenőrzése.

14.5. SZEMÉLYEK MUNKAVISZONYÁNAK MEGSZŰNÉSE

A jogviszony megszüntetésekor a következő feladatok végrehajtása szükséges.

HOZZÁFÉRÉSEK MEGSZÜNTETÉSE

A jogosultságok megszüntetésének normál folyamata, hogy a kilépő alkalmazottakról a Munkaügyi ügyintéző írásban értesíti az Informatika csoportot, amely megszünteti a kilépő alkalmazottak jogosultságait.

A hozzáférési jogosultságok megszüntetésével egyidejűleg az elektronikus belépőkártyák jogosultságát is meg kell szüntetni, függetlenül attól, hogy a belépőkártya visszaadásra került-e, vagy sem.

A jogosultságok megszüntetéséért a hálózati szinten a Rendszergazda, rendszereken belül a kulcsfelhasználó a felelős.

HOZZÁFÉRÉSI JOGOK VISSZAVONÁSA FELADATKÖR VAGY MUNKAKÖR VÁLTOZÁS ESETÉN:

A munkavállaló feladatkörének vagy munkakörének változás esetén a munkahelyi vezetőnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt. Ez esetben is - az új jogosultság igényléséhez kell folyamodni. A jogosultság igénylésben jelölni kell, hogy mely jogosultságokat kell megszüntetni. A jogosultságok részleges visszavonásának eljárásrendje egyéb tekintetben megegyezik az új jogosultsági igény eljárásendjével.

A munkahelyi vezetőnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt.

HOZZÁFÉRÉSI JOGOK VISSZAVONÁSA RENDES FELMONDÁS ESETÉN:

Ha a Szervezet alkalmazottjának munkaviszonya rendes felmondás keretein belül megszűnik, erről a tényről a közvetlen felettesének, illetve a Munkaügyi ügyintézőnek haladéktalanul tájékoztatást kell nyújtania az IT vezetőnek. Az informatika csoport a jelzett időponttal gondoskodik a Felhasználó összes rendszerhozzáférésének adott időpontban történő megszüntetéséről vagy letiltásáról, illetve ezek kezdeményezéséről. A munkaviszonyt lezáró dokumentumok között szerepeltetni kell a jogosultságok megszűnéséről szóló tájékoztatást, ebben integráltan egy figyelmeztetést a jogosulatlan belépés, vagy annak kísérletének jogi következményeiről.

HOZZÁFÉRÉSI JOGOK VISSZAVONÁSA RENDKÍVÜLI FELMONDÁS ESETÉN:

Amennyiben a munkavállaló munkaviszonya rendkívüli felmondással kerül megszüntetésre, akkor jogosultságainak megszüntetéséről haladéktalanul gondoskodni kell.

Ennek érdekében a felmondást aláíró vezetőnek haladéktalanul tájékoztatnia kell az IT vezetőt. Az IT vezető tájékoztatásáért egyetemlegesen felel a felmondást szignáló személy és a Munkaügyi ügyintéző ügyintézője. Az Informatika csoportnak haladéktalanul gondoskodnia kell az illetéktelen hozzáférés megakadályozásáról. A munkavállalónak azonnal írásos tájékoztatást kell kapnia jogosultságai megszűnéséről, és a belépési kísérletek következményeiről.

HITELESÍTŐ ESZKÖZÖK ÉRVÉNYTELENÍTÉSE

A Szervezet a munkaviszony, vagy a szerződéses jogviszony megszűnésekor érvényteleníti vagy visszaveszi a személy egyéni hitelesítő eszközeit. A visszavétel tényét a munkaviszonyt lezáró dokumentumok között szerepeltetni kell.

TÁJÉKOZTATÁS

A Szervezet tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről (Titoktartás stb.)

ESZKÖZÖK VISSZAVÉTELE

A Szervezet visszaveszi az EIR-rel kapcsolatos, tulajdonát képező összes eszközt. A visszavétel tényét a munkaviszonyt lezáró dokumentumok között szerepeltetni kell.

A vagyontárgyakkal el kell számolni. A munkahelyi vezetőnek HelpDesken kell igényelnie a leadott informatikai eszközök ellenőrzését és az eszközön lévő felhasználói adatok, email fiókok tartalmának mentését.

A bejelentés alapján a Rendszergazdának ellenőriznie kell, hogy az eredeti, rögzített hardver és szoftver specifikációval adják-e vissza az informatikai eszközöket.

FELADATOK ÁTADÁSA

A kilépő alkalmazott munkahelyi vezetőjének feladata, hogy az alkalmazott EIR-rel, vagy azok biztonságával kapcsolatos esetleges feladatainak ellátásáról a munkaviszony megszűnését megelőzően gondoskodjon.

ÉRTESÍTÉS

A Szervezet az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.

TITOKTARTÁS

A Szervezet a jogviszonyt megszüntető személy EIR-rel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik.

Tájékoztatni kell a munkavállalót, hogy a Szervezet EIR-nek használata során a tudomására jutott minden információ bizalmas adatnak minősül, azok illetéktelen, harmadik fél részére történő továbbadása büntetőjogi, illetve polgári jogi következményeket von maga után és a munkavállaló titoktartási kötelezettsége a munkaviszonya megszűnése után is fennáll.

A munkavállaló tájékoztatásáért a Munkaügyi ügyintéző a felelős.

JOGSÉRTÉSEK MEGELŐZÉSE

A Szervezet a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges EIR-t, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását minden eszközzel megelőzi.

14.8. AZ ÁTHELYEZÉSEK, ÁTIRÁNYÍTÁSOK ÉS KIRENDELÉSEK KEZELÉSE

A Szervezet az EIR-hez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy besorolásnak megfelelő feltételekkel rendelkezik-e.

Amennyiben igen, úgy logikai és fizikai hozzáférést engedélyez az újonnan használni kívánt EIR-hez, figyelembe véve a szükségesség elvét. Szükség szerint módosítani kell a hozzáférési jogosultságot, hogy az megfeleljen az áthelyezés vagy átirányítás miatt bekövetkező változásoknak.

Végül a Szervezeti és Működési Szabályzatban meghatározott módon a jogviszony változásáról értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.

14.9. HOZZÁFÉRÉSI MEGÁLLAPODÁSOK

A Szervezet EIR-hez kizárólag olyan munkatárs kaphat hozzáférést, akinek a munkájához szükséges az EIR használata, és aki megismerte és dokumentáltan elfogadta a rendszerre vonatkozó hozzáférési szabályokat, valamint aki eleget tesz a szabályzat 2.2 pont a-d feltételeinek. Azok a felhasználók, akik nem a Szervezet alkalmazottjai csak az IT vezető tudtával és jóváhagyásával kaphatnak hozzáférést. Csak valós, aktív munka- vagy szerződéses viszonyban álló személyeket lehet regisztrálni a rendszerben.

A jogosultságok kezelésekor alapelvként kell érvényesíteni, hogy csak a felhasználók feladatellátásához szükséges és elégséges mértékű jogosultságok biztosíthatók.

A Szervezet nem vizsgálja felül a hozzáférési megállapodásokat, mert az információk, adatok, EIR-ek kritikussága ezt nem teszi szükségessé.

14.11. KÜLSŐ SZEMÉLYEKHEZ KAPCSOLÓDÓ BIZTONSÁGI KÖVETELMÉNYEK

A Szervezet a külső szolgáltatókkal, egyéb szervezetekkel kötött megállapodásban, szerződésben megköveteli, hogy a külső szervezet határozza meg az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is.

Bármely, az EIR-ekhez kapcsolódó szolgáltatást nyújtó szolgáltató, ill. alvállalkozó, valamint más együttműködő partnerrel való együttműködés megkezdése előtt a szerződést előkészítő munkatárs, az EIBF bevonásával, megvizsgálja a felmerülő informatikai biztonsági kockázatokat, hozzáférési igényeket, és a szükséges kontrollokat beépíti a partnerrel kötött szerződésbe, kapcsolódó megállapodásba. Szolgáltató, ill. alvállalkozó bevonása miatt fellépő új kockázat felmerülésekor a kockázatot az EIBF a kockázat-felmérési eljárások során kezeli.

A külső partnerek képviselőivel a mindenkor hatályos IBSZ vonatkozó részeit a feladatnak megfelelő mértékben ismertetni kell. A betekintés mélységének meghatározása a Adatgazda felelőssége. A szerződéskötés és az együttműködés során biztosítani kell, hogy a külső partner (fejlesztő cég) az általa telepített, fejlesztett EIR-t úgy konfigurálja, hogy annak minden eleme és egésze eleget tegyen az IBSZ-ben előírtaknak.

A Szervezet előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a Szervezet EIR-éhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor azonnal küldjön értesítést az IT vezetőnek, aki megteszi a szükséges intézkedéseket (jogosultságok visszavétele).

A Szervezet folyamatosan ellenőrzi a szerződő féltől megköveteli a személybiztonsági követelményeknek való megfelelését.

14.12. FEGYELMI INTÉZKEDÉSEK

Az IBSZ bárki által történő megszegését az észlelő haladéktalanul köteles jelenteni az EIBF-nek.

A Szervezet a felhasználók részéről szándékos károkozásnak tekinti az alábbi tevékenységeket:

- behatolást az EIR környezetébe;
- illetéktelen hozzáférést az adatokhoz, eszközökhöz;
- adatok, eszközök eltulajdonítását, visszaélésszerű felhasználását;
- megtévesztő adatok bevitelét és képzését;
- eszközök, adathordozók megrongálását, működésük, használhatóságuk korlátozását;
- feldolgozások és munkafolyamatok zavarását, késleltetését;
- vírusfertőzött adathordozó szándékos behozatalát, vírusfertőzés előidézését;
- illegális szoftverek telepítését;
- a törvények és szabályok tudatos vagy szándékos megsértését.

A Szervezet gondatlan károkozásnak tekinti az alábbiakat:

- figyelmetlenséget, az ellenőrzés elmulasztását;
- szakmai hozzá nem értést, a kötelezően elvárható gondosság és előrelátás hiányát, elmulasztását;
- megváltozott működési körülményeknek figyelmen kívül hagyását;
- biztonsági követelmények és gyári előírások be nem tartását;
- adathordozók megrongálódását az előírásoktól eltérő tárolás és kezelés miatt;
- karbantartási műveletek elmulasztását;
- biztonsági-, jelző- és riasztóberendezések karbantartásának elhanyagolását;
- eszköz és eljárásbeli biztosítékok EIR-be történő beépítésének elhanyagolását.

Az EIBF a tudomására jutott események súlyosságát mérlegeli, és szándékos, illetve gondatlan károkozás esetén jelenti az IT vezetőnek.

Az információbiztonsági előírások megsértőivel szemben fegyelmi felelősségre vonásra kerülhet sor. Az eljárást a jogszabályok és a Szervezet belső szabályzatai szerint kell lefolytatni.

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

Ha az elektronikus információbiztonsági szabályokat nem a 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.

14.13. MUNKAKÖRI LEÍRÁSOK

A Munkaügyi ügyintéző gondoskodik arról, hogy a biztonsági szerepköröknek és felelősségek bele legyenek foglalva a munkaköri leírásokba.

15. KOCKÁZATKEZELÉS

15.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend célja a biztonsági osztályba sorolás meghatározása majd a kockázatértékelés végrehajtása, beleértve az ellátási lánc kockázatainak elemzését is. Emellett biztosítja a sérülékenységmonitorozást és -szkennelést, beleértve a privilegizált hozzáférés is. Az eljárásrend része a kockázatokra adott válasz kidolgozása és a rendszerelemek kritikusságának elemzése, hogy a Szervezet hatékonyan reagálhasson a felmerülő biztonsági fenyegetésekre.

Felelős: EIBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, a Rendszergazdával, valamint a Kockázati szereplőkkel (1.6.2.) minden esetben ismertetni kell.

15.2. BIZTONSÁGI OSZTÁLYBA SOROLÁS

A Szervezet a jogszabályban meghatározott szempontok alapján megvizsgálja EIR-eit, és a EIR nyilvántartás alapján meghatározza, hogy azok melyik biztonsági osztályba sorolandók.

A szervezet vezetője kizárólagosan hagyja jóvá a biztonsági osztályba sorolást.

Az EIR-ek biztonsági osztályba sorolásának eredményét az EIR nyilvántartó tartalmazza.

15.4. KOCKÁZATÉRTÉKELÉS

KEZDETI HELYZETFELMÉRÉS

Az EIR kockázatelemzésének elvégzéséhez fel kell mérni, meg kell ismerni az EIR-t és a jelenlegi információbiztonsági állapotát.

A rendszer funkciójának és – esetleg szenzitív – adattartalmának megismerésén túl – a következő területeket kell a dokumentációk bekérésével, illetve szakmai interjúk lefolytatásával megismerni:

ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

- a Szervezetre vonatkozó jogszabályok, szabályzatok;
- az EIR-re vonatkozó szabályzatok;
- üzemeltetési eljárások;
- ellátási lánc, szerződések, külső partnerek kezelése;
- biztonsági események kezelése;

FIZIKAI VÉDELMI INTÉZKEDÉSEK

- beléptetés;
- az épületben történő közlekedés;

- a szerverterem kialakítása;
- az irodák kialakítása;
- a tiszta asztal, üres képernyő politika alkalmazása.

LOGIKAI VÉDELMI INTÉZKEDÉSEK

- szoftverfejlesztés, változáskezelés;
- a szervizelés, eszközcsere, selejtezés folyamata;
- mentési megoldások;
- a jogosultsági rendszer, a jogosultságigénylés folyamata;
- vírusok és egyéb kártevők elleni védekezés;
- biztonsági frissítések telepítése;
- naplózás, biztonsági rendszerek;
- a hálózat felépítése;
- kriptográfiai (titkosítási) megoldások.

KOCKÁZATOK AZONOSÍTÁSA

1. GYENGE PONTOK MEGHATÁROZÁSA, KOCKÁZAT MEGNEVEZÉSE

A helyzetfelmérés alapján megszerzett információk birtokában azonosítani kell a kockázat által érintett EIR-t, vagy kontrollt [Kisköre VPH *Kockázat-menedzsment*] elnevezésű táblázat (a továbbiakban: *Táblázat) „B" oszlop*, majd röviden le kell írni az adott kockázatot, vagy gyenge pontot (*Táblázat „C" oszlop*).

A gyenge pontok meghatározásánál figyelembe kell venni

a) a jogosulatlan hozzáférés, használat, közzététel, zavarás, módosítás vagy a rendszer megsemmisítésének valószínűségét és káros hatásait az általa feldolgozott, tárolt vagy továbbított információkra és minden kapcsolódó információra vonatkozóan;

b) a személyes adatok feldolgozásából eredő, egyénekre vetített kedvezőtlen hatások valószínűségét és mértékét;

c) az ellátási lánc zavarával, vagy megszakadásával kapcsolatos kockázatokat az adott rendszer szolgáltatásai és rendszerelemei vonatkozásában;

d) a biztonsági értékelések, ellenőrzések és vizsgálatok megállapításait.

2. FENYEGETŐ TÉNYEZŐK ELEMZÉSE

Meg kell vizsgálni, hogy a fellelt gyenge pontot mely fenyegető tényezők használhatják ki, illetve az adott kockázatot mely fenyegető tényezők okozzák, és azokat a *Táblázat „Fenyegetés" („E") oszlopából* ki kell választani. Ezzel automatikusan kiválasztható az is, hogy az adott Fenyegetés mely információbiztonsági alapelvet érinti (Bizalmasság, Sértetlenség, Rendelkezésre állás, *Táblázat „G" oszlop, Érintett alapelvek*).

3. BEKÖVETKEZÉS VALÓSZÍNŰSÉGÉNEK MEGHATÁROZÁSA

A bekövetkezés valószínűségét több tényező is meghatározhatja, ezeket meg kell becsülni. Minden esetben figyelembe kell venni a fenyegető tényező kategóriáját (Emberi, Üzleti, Informatikai, Környezeti, Fizikai), mert lehetnek az adott geológiai lokáción jellemzőbb fenyegetések (pl.: vízkár egy árterületen), illetve kevésbé jellemző fenyegetések (pl.: adatvesztés egy többszörösen biztosított adatmentési rendszerrel ellátott szervezet esetén, ahol másodlagos feldolgozási helyszín és alternatív tárolási helyszín is van).

A felmérésbe bele kell kalkulálni a következő szempontokat:

a) a motiváció (a lehetséges támadók erőforrásai, az informatikai rendszer vagyontárgyainak a lehetséges támadók által érzékelhető vonzereje, sebezhetősége)

b) az értékelendő földrajzi tényezők (pl. vegyi- és üzemanyag gyárak közelsége, szélsőséges időjárási viszonyok valószínűsége, és olyan tényezők, amelyek befolyással lehetnek az emberi tévedésekre és a berendezések hibás működésére, a véletlenszerű fenyegetési források tekintetében)

c) az emberi tényező, mint az egyik legnagyobb probléma kiváltó ok a fenyegetések bekövetkezésének valószínűségében

Továbbá figyelembe kell venni az évek tapasztalatából az eddigi előfordulásokat is, így a következő kategóriákat lehet használni a bekövetkezés valószínűségének meghatározására:

0. N/A – a Szervezetnél az adott kockázat (már) nem tudja kifejteni a hatását
1. nem valószínű – négy évnél ritkábban, esetileg, kis számban és/vagy esetleges valószínűséggel becsülhető az esemény bekövetkezése
2. ritka – háromévente számottevő gyakorisággal és/vagy valószínűséggel fordul elő az adott esemény
3. közepesen valószínű – kétévente számottevő gyakorisággal és/vagy valószínűséggel fordul elő az adott esemény
4. valószínű – egy éven belül többször és/vagy nagy valószínűséggel becsülhető az esemény bekövetkezése
5. majdnem biztos – félévente, vagy akár havi szinten is problémát jelenthet

KOCKÁZAT ÉRTÉKELÉSE

4. LEHETSÉGES KÖVETKEZMÉNY

Fel kell mérnünk, hogy milyen következményekkel jár az adott kockázat a Szervezetre nézve. Első lépésben leíró módszerrel röviden ki kell fejteni a lehetséges következményt (*Táblázat „H" oszlop*).

5. KÁRÉRTÉK SZINTEK MEGHATÁROZÁSA

A bekövetkezett káresemény súlyosságának, mértékének jellemzésére a következő kárérték szintek kerültek kialakításra:

1. Elenyésző;
2. Kicsi;
3. Közepes;
4. Nagy;
5. Extrém;

A kárérték szintek meghatározása során azt kell figyelembe venni, hogy

a) milyen tényleges vagy erkölcsi kárt jelentene a rendszerben tárolt adatok bizalmasságának sérülése;
b) milyen következményekkel járna a rendszer ideiglenes elérhetetlensége vagy az adatok sérülése, elvesztése;
c) mennyibe kerülne a meghibásodott eszközök javítása, cseréje;
d) mennyi munkaidő ráfordítással járna a helyreállítás.

6. KOCKÁZATOK MEGHATÁROZÁSA

Az információbiztonsági kockázatokat a fenyegetés bekövetkezésének a valószínűsége és az okozott kárt jellemző kárérték szint *szorzata* fogja megadni.

A kockázatok nagyságának, értékének meghatározásához a következő kockázati mátrixot kell használni:

Kárérték	Alacsony	Közép-alacsony	Közepes	Közép-magas	Magas
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

Bekövetkezés valószínűsége

A táblázatban a kockázatok jelentése a következő:

a) 1 – 2 Alacsony;
b) 3 – 5 Közép-alacsony;
c) 6 – 11 Közepes;
d) 12 – 16 Közép-magas;
e) 17 – 25 Magas;

7. NEM TOLERÁLHATÓ KOCKÁZATOK MEGHATÁROZÁSA

A Szervezet azt a döntést hozta, hogy minden Közép-alacsonynál magasabb kockázatot kezelni kíván.

Ennek megfelelően a toleranciamátrix a következő:

Kárérték	Alacsony	Közép-alacsony	Közepes	Közép-magas	Magas
5	T	T	NTH	NT	NT
4	T	T	NTH	NTH	NT
3	T	T	T	NTH	NTH
2	T	T	T	T	T
1	T	T	T	T	T
	1	2	3	4	5

Bekövetkezés valószínűsége

A táblázatban alkalmazott jelölések értelmezése a következő:

a) T – Tolerálható;
b) NTH – Nem tolerálható, hosszú távon kockázatkezelést igényel;
c) NT – Nem tolerálható, azonnali kockázatkezelést igényel.

8. PRIORITÁS MEGHATÁROZÁSA

A Szervezetnek lehetősége van arra, hogy önállóan is meghatározza egy-egy kockázat Szervezetre gyakorolt hatását, így priorizálva a megoldandó kockázatokat. Minél magasabb a prioritás, annál hamarabb szükséges foglalkozni egy adott kockázattal.

A prioritások a következők lehetnek:

a) **Alacsony** - *Nem szükséges azonnal* foglalkozni vele
b) **Közepes** – A *közeljövőben* megoldást kell találni
c) **Magas** - *Azonnali* válaszlépéseket igényel (most kell vele foglalkozni)

15.5. KOCKÁZATÉRTÉKELÉS – ELLÁTÁSI LÁNC

A szervezet rendszeresen felméri az ellátási lánc kockázatait is, különös tekintettel a meghatározott EIR-ekre, rendszerelemekre és rendszerszolgáltatásokra.

A szervezet az ellátási lánc kockázatelemzését felülvizsgálja és frissíti az alábbi esetekben:

- meghatározott időközönként;
- ha jelentős változások következnek be az érintett ellátási láncban;

vagy ha a rendszer, a működési környezet, illetve más körülmények változása indokolttá teheti az ellátási lánc módosítását.

Az ellátási láncban részt vevő szolgáltatók, fejlesztők, beszállítók évente legalább egyszer értékelésre kerülnek. Az értékelés során vizsgálni kell:

- kritikusság a Szervezet szempontjából
- biztonsági tanúsítványokat (pl. ISO 27001, SOC 2),
- szolgáltatási szintet (SLA),
- adatkezelési és hozzáférési feltételeket,
- incidenskezelési képességeket.

A beszállítók kockázati besorolása lehet

- **Kiemelkedő**: tanúsított, megbízható, stabil partner, bizonyított információbiztonsági megfeleléssel.
- **Megfelelő**: stabil, megbízható partner, tanúsítvány nélkül, de elfogadható biztonsági gyakorlatokkal és pozitív együttműködési tapasztalattal.

- **Feltételes:** működése stabil, de biztonsági dokumentáltsága hiányos vagy részben igazolt; további ellenőrzés, kockázatcsökkentő intézkedés szükséges.
- **Kockázatos:** alacsony bizalmi szintű, korlátozott átláthatóságú partner, kritikus rendszerhez vagy adathoz hozzáféréssel, megfelelő szerződéses biztosíték nélkül.
- **Veszélyes:** kritikus rendszerhez vagy adathoz hozzáférő partner, aki nem rendelkezik igazolt információbiztonsági megfeleléssel; együttműködés kizárólag kockázatkezelési terv mellett engedhető.

15.9. SÉRÜLÉKENYSÉGEK ELLENŐRZÉSE

Az Informatika csoportnak rendszeres időközönként, vagy eseti jelleggel amikor ezen sérülékenységekről tudomást szerez, ellenőriznie és javítania kell az EIR-ek sérülékenységeit.

15.18. SÉRÜLÉKENYSÉGMENEDZSMENT – SÉRÜLÉKENYSÉGI INFORMÁCIÓK FOGADÁSA

Ki kell alakítani egy dedikált kommunikációs csatornát (pl: e-mail), amely lehetővé teszi a szervezeti EIR-ekben és rendszerelemekben észlelt sérülékenységekről szóló jelentések fogadását.

15.20. KOCKÁZATOKRA ADOTT VÁLASZ

A Szervezet a kockázatokra többféle válaszlépést adhat. Ezen válaszlépések a következők lehetnek:

Elfogadás

A Szervezet úgy döntött, hogy nem tud azonosítani megfelelő válasz-stratégiát, vagy az aránytalanul költséges lenne. A kockázati fenyegetések esetében nem minden esetben szükséges a csökkentés vagy átruházás, különösen azoknál, amelyeknek alacsony a súlya. A Szervezetnek kell megítélni, hogy szigorúbb (és potenciálisan költségesebb) válaszstratégiát alkalmaz-e.

Megosztás

A Szervezet megosztja a kockázatot részben, vagy akár teljes egészében egy másik féllel, aki azt a legjobban képes kezelni.

Mérséklés

Cél a kockázat valószínűségének és/vagy hatásának csökkentése egy elfogadható küszöb alá. Ennek fajtái lehetnek:

- Megelőző jellegű intézkedések (preventív kontrollok):

A hibák, sérülékenységek, gyenge pontok, illetve ezek kihasználására való lehetőségek kiküszöbölése.

- Korlátozó vagy javító intézkedések (korrektív kontrollok):

A veszélyek hatását csökkentő, enyhítő óvintézkedések, további tevékenységek szükségessége nélkül.

- Észlelő és reagáló intézkedések (detektív kontrollok):

A sérülékenységek, gyenge pontok támadásának észlelése, ártalmas kihatások enyhítésére, illetve válaszreakciók kidolgozása.

Átruházás

A Szervezet átruházza a fenyegetést egy másik félre, aki a legjobban képes minimalizálni a kockázat hatását és/vagy valószínűségét. (pl.: biztosítás kötése, vagy tevékenység kiszervezése, megfelelő beszállítói szerződések megkötése)

Elkerülés

A Szervezt úgy módosítja a jelenlegi tényezőket, hogy megszüntesse a kockázatot vagy megvédje magát annak hatásaitól (pl.: érintett tevékenység megszüntetése)

Szükséges intézkedések leírása

Ha a Szervezet már felmérte a kockázatokat és úgy döntött, hogy kezelni fogja, akkor meg kell határozni, hogy milyen intézkedések szükségesek a kockázatok kezeléséhez. Ezen intézkedéseket szöveges formában fel kell jegyezni a Táblázat „M" oszlopában a „Szükséges intézkedések leírása"-nál.

A kockázatfelelős

Minden azonosított kockázathoz, amellyel a Szervezetnek foglalkozni kell, szükséges egy ún. Kockázatfelelős hozzárendelése. Ő lesz a felelős azért, hogy a hozzárendelt kockázatokat értékelje, felügyelje és kezelje. A Táblázat „O" oszlopába kell kerülnie.

A határidő

A Szervezetnek meg kell határoznia, hogy milyen időintervallumon belül hajtja végre a kockázat kezeléséhez szükséges intézkedéseket. Ehhez az „N" oszlopot, a „Határidő"-t kell igénybe venni.

Készenléti terv

A készenléti terv olyan dokumentum, amely meghatározza, hogy hogyan kell cselekedni váratlan események, vagy válsághelyzetek esetén. Ha a kockázatelemzés részeként elkészítették az esetleges kockázatok és veszélyforrások azonosítását, akkor a készenléti terv ezen felismerésekre építve kínálhat cselekvési tervet az esetleges problémákra. Jelentősen befolyásolhatja egy kockázat mértékét, ha rendelkezünk megfelelő készenléti tervvel.

Figyelés- és felügyelet (kockázat-monitoring)

- *Státusz és frissítés*

Minden kockázathoz tartozik egy státusz, egy állapot, amely azt mutatja, hogy a jelenleg milyen folyamatok történtek (illetve történtek-e) az adott kockázat kezelésével kapcsolatban, vagy azt már lezártnak tekinthetjük.

Jelen módszertan ötféle státuszt különböztet meg, ezek a következők:

1. Aktív (nem indult)

   A Szervezet azonosított és értékelt egy kockázatot, de jelenleg még választerv nincs, illetve válaszlépéseket nem foganatosított. A kockázatot mindemellett aktívan figyelik és ellenőrzik.
2. Aktív (folyamatos)

   A Szervezet az azonosított kockázatot aktívan figyeli és a válaszlépések folyamatban vannak.
3. Aktív (teljesült)

   A Szervezet az azonosított kockázatot aktívan figyeli, a válaszlépések már lezárultak.
4. Alvó (nem indult)

   Az adott kockázat jelenleg nem kiemelt prioritás, de a jövőben aktívvá válhat.

5. Lezárt (teljesült)

   A kockázat a kockázatkezelő intézkedéseknek (vagy egyéb tényezők változásainak) köszönhetően többé nem jelent veszélyt a Szervezetre nézve.

A státuszhoz szervesen kapcsolódik az utolsó frissítés dátuma, amely az időpontot jelöli, amikor utoljára frissítették, vagy felülvizsgálták a kockázatok státuszát a kockázatkezelési rendszerben.

Ennek a dátumnak több szerepe is lehet:

- ***Aktualitás*** - Az utolsó frissítés dátuma azt jelzi, hogy a kockázatokkal kapcsolatos információk naprakészek és aktuálisak-e. Ezzel segít biztosítani, hogy a döntéshozók mindig a legfrissebb adatokkal rendelkezzenek a kockázatok állapotáról.
- ***Nyomon követés*** - A dátum nyomon követése lehetővé teszi a Szervezet számára, hogy lássa, milyen gyakran ellenőrzik és frissítik a kockázatokat. A rendszeres frissítések fontosak a változó kockázati környezet kezelése és a hatékony válaszok biztosítása érdekében.
- ***Döntéshozatali támogatás*** - Az aktuális kockázatstátusz a döntéshozatal alapja lehet. Az utolsó frissítés dátuma segíthet a döntéshozóknak abban, hogy megbecsüljék, milyen régi vagy friss az információ, és hogy szükség lehet-e további vizsgálatokra vagy frissítésekre.

Nyomon követés, kapcsolódó megjegyzések

Az eddig elvégzett kockázattal, illetve kockázatkezeléssel kapcsolatos tevékenységeket kell a Táblázat „S" oszlopába leíró formában feljegyezni. Ez is szervesen kapcsolódik a Státuszhoz, hiszen a Kockázatfelelős itt fejti ki részletesebben a kockázattal kapcsolatos fejleményeket.

Azáltal, hogy rendszeresen rögzítik és nyomon követik a kockázatokkal kapcsolatos megjegyzéseket, a szervezet képes marad reagálni a változó kockázati környezetre és hatékonyabban kezelni a potenciális kockázatokat. Itt dokumentálják a változásokat, melyek megkönnyítik a nyomon követést, illetve döntéstámogatási, döntéselőkészítési szerepük van.

Eredmények értékelése

A kockázatok kezelésének hatékonyságát azok lezárásáig éves szinten, vagy változások esetén (pl: státuszmódosítás) értékelnünk kell. Az értékelésnek szöveges formában a „T" oszlopba kell kerülnie.

Minden esetleges változást, vagy változtatást jelezni kell a Kockázatkezelési vezetőnek.

Kockázatelemzés-jelentés

A jelentés célja, hogy összefoglalja az azonosított kockázatokat, értékelje azokat, és ajánlásokat tegyen a kockázatok kezelésére. A kockázatelemzés-jelentésnek az érintett felek számára könnyen érthetőnek és áttekinthetőnek kell lennie, és az ajánlásoknak konkrétnak és végrehajthatónak kell lenniük.

Évente legalább egy alkalommal összefoglaló jelentést kell készíteni a nem lezárt kockázatokról.

Felelősségek és folyamatok a kockázatkezelés kapcsán (RACI mátrix)

Engedélyezési folyamat	EIBF	Jegyző	Kockázat-menedzser	IT vezető Rendszergazda	Adatgazda munkahelyi vezető	Belső ellenőrzés auditor	Érintett munkatárs
Új kockázat azonosításának jóváhagyása	R	A	C	I	C	I	I
Kockázatértékelés eredményének elfogadása	R	A	C	I	C	I	I
Kockázatkezelő intézkedés végrehajtásának jóváhagyása	R	A	C	C	R	I	I
Maradványkockázat elfogadása	C	A	R	I	C	I	I
Kivételek engedélyezése	R	A	C	I	C	I	I
Kockázatkezelési folyamat módosításának jóváhagyása	R	A	C	I	C	C	I
Kockázatelemzési jelentések	R	A	C	I	C	I	I

EIBF: felelős az információbiztonsági megfelelésért, dokumentációért, és az engedélyezési folyamat koordinálásáért.

Jegyző: végső döntéshozó és felelős a maradvány-kockázatok elfogadásáért.

Kockázatmenedzser: az értékelések és kockázatkezelési tervek szakmai felelőse.

IT vezető / rendszergazda: technikai megvalósításért felelős.

Adatgazda / munkahelyi vezető: a területileg érintett folyamatokért felelős.

Belső ellenőrzés / auditor: felülvizsgálja az engedélyezési folyamatok megfelelőségét.

Érintett munkatárs: informált a döntésekről, végrehajtja az előírásokat.

16. RENDSZER- ÉS SZOLGÁLTATÁSBESZERZÉS

16.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Az eljárásrend célja, hogy meghatározza a beszerzési folyamat lépéseit, ideértve az alkalmazandó védelmi intézkedések funkcionális tulajdonságait és a biztonsági tervezési elveket. Emellett figyelembe veszi a külső szolgáltatóktól érkező információs rendszerek szolgáltatásait és a fejlesztési folyamatot, szabványokat és eszközöket. Ezáltal garantálja a biztonságos és hatékony informatikai infrastruktúra kialakítását és fenntartását a szervezet számára.

Felelős: IT vezető, EIBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

16.2. ERŐFORRÁSOK RENDELKEZÉSRE ÁLLÁSA

Az éves költségvetési tervben, vagy a beruházási tervekben nevesítve szerepeltetni kell az EIR és szolgáltatások védelméhez szükséges erőforrásokat.

16.3. A RENDSZER FEJLESZTÉSI ÉLETCIKLUSA

Figyelemmel kell kísérni az informatikai biztonsági helyzetet az EIR-einek teljes életútján, azok minden életciklusában.

Meg kell határozni és dokumentálni az információbiztonsági szerepköröket és felelősségeket a fejlesztési életciklus egészére. Mindemellett ki kell jelölni az információbiztonsági szerepköröket betöltő felelős személyeket.

A rendszer életciklus szakaszai a következők:

- Követelmények meghatározása
- Fejlesztés vagy beszerzés
- Megvalósítás vagy értékelés
- Üzemeltetés és fenntartás
- Kivonás (archiválás, megsemmisítés).

16.7. BESZERZÉSEK

A BESZERZÉSI KÖVETELMÉNYEK MEGHATÁROZÁSA

A Szervezet az EIR-re, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként meghatározza az alábbiakat:

A beszerzésre kerülő rendszerek az alapvető és más jogszabályokban megkövetelt működési elvárásait teljesítenie kell. Az érintett rendszer esetleges cseréje esetén gondoskodni kell az előzetes felkészülésről, hogy a korábban használt, illetve szükséges folyamatok az új rendszerben hogyan érhetőek el.

A garanciális biztonsági követelmények:

a) A beszerzésre kerülő rendszerek biztonsági funkciói nem gyengülhetnek sem az elvárások, sem a korábbi rendszer paramétereinek tekintetében.
b) Figyelembe kell venni a változó jogszabályi előírásokat
c) A beszerzést megelőzően nem adható ki „valós alapú" tesztadat
d) Vizsgálni kell a termék előállítójának alkalmazott eljárásait, szabványait
e) Az előzetes tesztelés kötelező

Rögzíteni kell az adott rendszer biztonsági osztályát és az ahhoz tartozó követelményeket.

A biztonsággal kapcsolatos dokumentációs követelményeket előzetesen meg kell fogalmazni. A rendszerrel kapcsolatosan alapvető elvárás, hogy a felhasználói, és a biztonsági dokumentáció különállóan jelenjen meg, és önállóan is értelmezhetők legyenek.

A fejlesztésekre vonatkozó szerződéseknek, ill. a szerződésekhez tartozó műszaki specifikációknak, ill. a fejlesztési projektekhez tartozó megállapodásoknak ki kell térniük az IT biztonsági követelményekre és azokra az átadás-átvételi feltételekre, amelyek alapján ezek ellenőrzésre kerülnek.

A fejlesztés tervezése során az IT biztonsági követelményeket a fejlesztésért felelős az IT vezetővel együttműködve azonosítja, és illeszti a specifikációba. meghatározzák, hogy a rendszer működése során milyen bemenő adat ellenőrzési, feldolgozás ellenőrzési, titkosítási, üzenet sértetlenség ellenőrzési, kimenő adat ellenőrzési követelmények fogalmazódnak meg, és a kapcsolódó követelményeket szintén beépítik a specifikációba. A specifikációt elfogadás előtt írásban véleményezi az IT vezető.

Minden egyedi fejlesztés esetén biztosítani kell a forráskód közvetlen, vagy közvetett rendelkezésre állását, valamint feltüntetni a fejlesztői környezetet, melyek hozzáférhetősége, adatai a szerződésben feltüntetésre kell kerüljenek.

A bevezetésre kerülő rendszereket bevezetés előtti tesztelni szükséges. A tesztelésnek ki kell térnie a bevezetés által érintett kapcsolódó rendszerek tesztelésére is. A tesztelések és a bevezetés során a rendszergazdának kell gondoskodnia arról, hogy éles rendszeren csak engedélyezett és felügyelt módosítás történhessen. Ugyancsak a rendszergazdának kell gondoskodnia arról, hogy a megfelelőség ellenőrzéséhez használt teszt adatokhoz, illetve a forráskódokhoz illetéktelen ne férjen hozzá.

Amennyiben külső fejlesztők működnek közre a fejlesztésben, a fejlesztéshez kijelölt projektvezető feladata az információ kiszivárgás kockázatának csökkentése és a fejlesztőkkel együttműködés során a biztonsági követelmények betartása, betartatása. E célból együtt kell működnie az IT vezetővel.

Annak érdekében, hogy az EIR-nek a biztonság szerves részét képezze, a biztonsági követelményeket már az életciklus tervezési, fejlesztési, beszerzési szakaszában figyelembe kell venni. Az üzemeltetés és karbantartás során az információbiztonsági teljesülését biztosítani kell .

16.8. BESZERZÉSEK – ALKALMAZANDÓ VÉDELMI INTÉZKEDÉSEK FUNKCIONÁLIS TULAJDONSÁGAI

Meg kell követelni a fejlesztőtől az adatvédelem, a hálózati biztonság, a hozzáférési ellenőrzés vagy más olyan biztonsági intézkedések leírását, amelyek szükségesek az adott rendszer biztonságának biztosításához.

16.15. AZ EIR-RE VONATKOZÓ DOKUMENTÁCIÓ

ADMINISZTRÁTORI, VAGY ÜZEMELTETÉSI DOKUMENTÁCIÓ

Ha a rendszer üzemeltetése a Szervezet hatókörébe tartozik, akkor megköveteli és birtokába veszi az EIR-re, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori, vagy üzemeltetési dokumentációt, amely tartalmazza az alábbiakat:

a) A rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését leíró adatokat, folyamatokat, specifikációkat.
b) Biztonsági funkciók (hardening)
c) A biztonsági funkciók hatékony alkalmazásának és fenntartásának leiratait.
d) A konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket, gyengeségeket (kockázatelemzés, hatásvizsgálat)

Ezen dokumentációt az Informatika csoport rendelkezésére kell bocsátani.

FELHASZNÁLÓI DOKUMENTÁCIÓ

A Szervezet megköveteli és birtokába veszi az EIR-re, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza:

a) A Felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját, ellenőrzését.
b) A rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit.
c) A Felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához.

Ezen dokumentációt a Felhasználók rendelkezésére kell bocsátani.

Amennyiben valamely dokumentáció nem áll rendelkezésre, akkor az IT vezetőnek dokumentálnia kell a dokumentáció beszerzésére tett kísérleteket.

16.16. BIZTONSÁGTERVEZÉSI ELVEK

A Szervezet az általa használt biztonságtervezési elveket ugyanúgy megköveteli a specifikáció, a tervezés, a fejlesztés, a megvalósítás és módosítás során is.

16.49. KÜLSŐ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK SZOLGÁLTATÁSAI

Külső EIR használata esetén a Szervezet szerződésben megköveteli, hogy az általa igénybe vett rendszerek szolgáltatásai mindenben megfeleljenek a Szervezet információbiztonsági követelményeinek.

Dokumentálni kell a külső rendszer felügyeletét ellátó személyek, illetve a felhasználók feladatait és kötelezettségeit a külső rendszerrel kapcsolatban.

Külső és belső eszközökkel ellenőrizni kell, hogy a külső szolgáltató megfelel-e az elvárt védelmi intézkedéseknek.

16.99. TÁMOGATÁSSAL NEM RENDELKEZŐ RENDSZERELEMEK

Azon rendszerelemeknek (szoftver, hardver) amelyeknek már nem elérhető a fejlesztői, vagy szállítói támogatás,

a) le kell cserélni támogatottra;
b) ki kell vezetni, ha már nincs rá szükség;
c) alternatív támogatást kell biztosítani belső, vagy külső szolgáltatók bevonásával;

17. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

17.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend célja a szervezet EIR-nek és kommunikációs csatornáinak hatékony védelme a külső és belső fenyegetésekkel szemben. Részletesen meghatározza a rendszer és felhasználói funkciók szétválasztásának módját, valamint az osztott használatú rendszererőforrások biztonságos kezelését. Emellett előírja a határvédelmi intézkedéseket, ideértve a hozzáférési pontok és a külső infokommunikációs szolgáltatások védelmét. Kiemelt figyelmet fordít az adatátvitel bizalmasságára és sértetlenségére.

Felelős: IT vezető, EIBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az Informatikai vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

17.12. SZOLGÁLTATÁSMEGTAGADÁSSAL JÁRÓ TÁMADÁSOK ELLENI VÉDELEM

Az EIR-t fel kell készíteni a szolgáltatás megtagadás alapú (Denial of Service) támadásokkal szemben.

A szolgáltatás megtagadó, más néven túlterheléses támadás során a támadó célja, hogy a felhasználók ne tudjanak elérni egy bizonyos szolgáltatást (pl.: a levelezést, bizonyos webhelyeket, online felhasználói fiókokat). Ennek során a támadó felesleges kérésekkel árasztja el és túlterheli a rendszert, amely így nem tudja a felhasználói kéréseket kiszolgálni.

A védelem érdekében biztosítani kell az EIR-t alkotó szoftverek naprakészségét a 10. Karbantartás fejezetben leírtak szerint.

Az informatikai rendszer kártevők elleni védelmét a 18.8. Kártékony kódok elleni védelem pontban leírtak szerint kell megvalósítani.

A határok védelmét a 17.17. A határok védelme fejezet alapján kell kialakítani.

Szegmentált hálózatot kell kialakítani, amelyben a felhasználói tevékenységek céljából külön alhálózatban kell elhelyezni a szervereket és a felhasználói munkaállomásokat, illetve külön menedzsment alhálózatot kell létrehozni az üzemeltetési tevékenységek (pl.: hálózati eszközök, szerverek, tároló rendszerek stb. menedzselése) céljából.

Az EIR-t – a 6.26. Legszűkebb funkcionalitás pont előírásai szerint – úgy kell konfigurálni, hogy csak a minimálisan szükséges szolgáltatások, portok és protokollok legyenek engedélyezve.

17.17. A HATÁROK VÉDELME

Az EIR Internet felőli – és kulcsfontosságú pontokon belső – határvédelmét tűzfalakkal kell biztosítani oly módon, hogy a tűzfalon keresztül csak az engedélyezett szolgáltatások legyenek elérhetők.

A nyilvánosan hozzáférhető rendszerelemeket szeparált hálózaton kötelező elhelyezni, elkülönítve a belső hálózattól. A szeparált (nyilvános) hálózatról a belső (szervezeti) hálózat elérését tűzfalakkal kell biztosítani.

A tűzfalak szabályrendszereinek kialakítása, a beállítások folyamatos karbantartása, a tűzfalak folyamatos felügyelete, az eseménynaplók elemzése, a betörési kísérletek kiszűrése és a szükséges intézkedések megtétele az Informatika csoport kijelölt Rendszergazdájának feladata.

A határvédelmi eszközök üzembiztonságáért, az eszközök karbantartásáért és javításáért, a beállítások mentéséért a Rendszergazda felel.

A rendszer külső határain olyan határvédelmi (tűzfal) megoldást kell alkalmazni, amely:

- alapértelmezett beállításként tilt minden külső kapcsolódást, a külön engedélyezett kapcsolatokon kívül;
- figyeli, naplózza és megakadályozza a kibertámadási kísérleteket;
- képes a túlterhelés alapú támadások felismerésére és hatásainak mérséklésére;
- képes biztonságos VPN kommunikáció biztosítására.

A rendszervédelem további eszközeként:

- blokkolni kell a belső hálózatból a veszélyesként besorolt, vagy kártékony kódot tartalmazó weboldalakhoz történő hozzáférést;
- Az e-mail kommunikációban külső spam szűrő rendszert kell alkalmazni a kéretlen, adathalász és kártékony kódot tartalmazó levelek blokkolására és karanténba helyezésére.

A lehetőségek szerint a Szervezet valamennyi telephelyén törekedni kell a határvédelmi eszközök Alapkonfiguráció szerinti azonos beállítására és a naplózás rendjének betartására.

17.49. KRIPTOGRÁFIAI KULCS ELŐÁLLÍTÁSA ÉS KEZELÉSE

A Szervezet rendelkezik a Nemzeti Média és Hírközlési Hatóság által elfogadott kriptográfiai (titkosító) kulcsokkal, valamint ezen kulcsokból származtatott belső (önaláírt) kripográfiai kulcsokkal is.

A szervezet titkos kulcsát csak az Informatika csoport ismeri. A 2 évnél régebbi kulcsokat a Rendszergazda inaktíválja, vagy eltávolítja.

17.53. KRIPTOGRÁFIAI VÉDELEM

Az EIR-ben csak olyan kriptográfiai (titkosítási) megoldás alkalmazható, mely megfelel az elektronikus aláírásról szóló törvény előírásainak, illetve az elektronikus aláírást felügyelő hatóság ajánlásainak és állásfoglalásainak.

A kommunikáció védelmét szolgáló kriptográfiai kulcsokat külön eszközzel kell előállítani. A kulcsokat elkülönített, biztonságos helyen kell tárolni. A VPN kapcsolatok szerver oldali kulcsai csak a VPN szervereken, a kliens oldali kulcsok csak a VPN klienseken helyezhetők el.

Felhasználási területek:

- Adatátvitel védelme (SSL/TLS)
- E-mail titkosítása (S/MIME)
- Jelszóvédelem (HASH)
- Digitális aláírások (AVDH)

- VPN (AES-256)
- Wifi hálózatok titkosítása (WPA2/WPA3)
- Hardveres titkosítási modulok (HSM):
- Személyazonosság ellenőrzése (biometrikus adatok):
- Hitelesítési tokenek (OTP)

17.54. EGYÜTTMŰKÖDÉSEN ALAPULÓ INFORMATIKAI ESZKÖZÖK

A Szervezet csak olyan együttműködésen alapuló számítástechnikai eszközöket (pl.: a számítógép kameráját és mikrofonját használó kommunikációs szoftvereket; vagy a számítógép képernyőjének, billentyűzetének és egerének távoli elérését biztosító, távsegítség nyújtására szolgáló szoftvereket) alkalmaz, amelyek:

a) vezérlő szoftvere az engedélyezett szoftverek körébe tartozik;
b) működését a munkatársak ismerik;
c) aktiválásához a Felhasználó jóváhagyása szükséges.

Az engedélyezett alkalmazásokat a 2.100 Távoli hozzáférések pontja taglalja.

17.69. BIZTONSÁGOS NÉV/CÍM FELOLDÁSI SZOLGÁLTATÁS (HITELES FORRÁS)

Az EIR névfeloldási szolgáltatását úgy kell kialakítani, hogy a hiteles forrást biztosító DNS szerver (autoritatív DNS) kriptográfiai (titkosítási) megoldással kiegészített, biztonságos tranzakciókat valósítson meg, amely nemcsak hiteles adatokat biztosít a név/cím feloldási kérésekre, hanem az információ eredetét és sértetlenségét is igazolja.

17.71. BIZTONSÁGOS NÉV/CÍM FELOLDÓ SZOLGÁLTATÁS (REKURZÍV VAGY GYORSÍTÓTÁRAT HASZNÁLÓ FELOLDÁS)

Az EIR névfeloldási szolgáltatását megvalósító rekurzív vagy gyorsítótáras DNS szervereknek kriptográfiai (titkosítási) megoldással kiegészített, biztonságos tranzakciókat kell megvalósítaniuk, amely segítségével a hiteles forrásból származó név/cím feloldó válaszokra vonatkozóan ellenőrizniük kell és maguknak is biztosítaniuk kell az információ eredetének és sértetlenségének igazolását.

17.72. ARCHITEKTÚRA ÉS TARTALÉKOK NÉV/CÍM FELOLDÁSI SZOLGÁLTATÁS ESETÉN

Az EIR név/cím feloldási szolgáltatását redundáns, hibatűrő módon kell kialakítani, azaz tartalék DNS szervert kell alkalmazni, amely biztosítja a szolgáltatás magas rendelkezésre állását.

A külső és a belső szerepköröket szét kell választani, vagyis külön DNS szervert kell használni a belső hálózat kiszolgálására, és külön szervernek kell ellátnia az internetes DNS szerverekkel történő kapcsolattartást.

17.108. A FOLYAMATOK ELKÜLÖNÍTÉSE

Az EIR-ben elkülönített végrehajtási tartományt kell fenntartani minden programfolyamat (process) számára, vagyis az egy számítógépen futó, megosztott erőforrásokat használó folyamatok nem szerezhetnek jogosulatlanul információkat más folyamatoktól.

Ennek érdekében a Szervezetnél csak olyan modern operációs rendszerek alkalmazhatóak, amelyek ezt biztosítják.

18. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

18.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend célja az EIR és az információk integritásának és biztonságának védelme. Az eljárásrend meghatározza a hibajavítás folyamatát, valamint előírja a kártékony kódok elleni védelmi intézkedéseket. Emellett előírja az EIR monitorozását, részletesen foglalkozik a szoftver- és információsértetlenség ellenőrzésével, a kéretlen üzenetek elleni védelemmel és a bemeneti információk ellenőrzésével.

Felelős: IT vezető

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, valamint a Rendszergazdával minden esetben ismertetni kell.

18.2. HIBAJAVÍTÁS

Az Informatika csoportnál HelpDesk rendszerű hibabejelentés működik az alábbi feladatok hatékony támogatása céljából:

- a felhasználói oldalon jelentkező, EIR-rel kapcsolatos bejelentések (hibabejelentés, segítségnyújtás kérése, hozzáférési jogosultság igénylés stb.) akár munkaidőn túli fogadására;
- az elvégzett munkák dokumentálására.

A felhasználók a következő formában tehetik meg a bejelentésüket:

- Sürgős esetben – vagy a HelpDesk elérhetetlensége esetén - telefonon a +36 20 4707675 mobilszámon

A bejelentéseknek minden esetben tartalmazniuk kell:

- a bejelentő nevét, e-mail és/vagy telefonos elérhetőségét;
- az EIR megnevezését;
- az igény vagy a hibajelenség pontos leírását;
- hibabejelentés esetén a hiba felmerülésének helyét, az esetleges hibaüzenetet és a hiba észlelésének időpontját.

Az informatikai rendszer kulcsfelhasználója, vagy sürgős esetben közvetlenül a felhasználók a rendszerhibát a Helpdesken bejelentik az Informatika csoportnak.

Az Informatika csoport fogadja a bejelentést, és kiosztja a feladatot az EIR-hez kijelölt, Rendszergazda számára.

Belső üzemeltetésű rendszer esetén:

A kijelölt Rendszergazda megvizsgálja, és szükség szerint pontosítja a hibát, majd gondoskodik a hiba javításáról. Ha a hibát nem tudja a saját hatáskörében megoldani, segítséget kér az IT vezetőtől.

Bizonyos esetekben szükség lehet a hiba kijavításához külső partnerek (pl.: speciális szakismeretet, szerszámokat vagy anyagokat igénylő hardver javítások esetén külső szakszerviz; vagy szoftverhibák esetén a külső szoftverfejlesztő; vagy a rendszer üzemeltetéséhez támogatást nyújtó szerződéses partner) bevonására. Ilyen esetben a Rendszergazda feladata a külső partner által végzett javítás koordinálása, a javított hardver eszközök, illetve szoftverfrissítések éles üzembe állítás előtti tesztelése, a szoftverfrissítések telepítése.

A külső üzemeltetésű rendszerek esetén:

A Rendszergazda a vonatkozó szerződés alapján értesíti a külső üzemeltetőt és koordinálja a hiba kijavítását.

A hibajavítás elvégzéséről az informatikai üzemeltető a HelpDesken értesíti a bejelentőt.

Szoftver- és firmware frissítések

A hibajavításokkal kapcsolatban szükség lehet szoftverfrissítések telepítésére, amely a változáskezelés hatálya alá esik, ezért ennek során a 6.7 A konfiguráció változások felügyelete (változáskezelés) fejezetben leírtak alkalmazandók.

Biztonsági frissítések

A hardvergyártók és szoftverfejlesztők rendszeresen adnak ki biztonsági frissítéseket a termékükben felfedezett biztonsági hibák javítására. Ezen biztonsági frissítések telepítése kiemelt jelentőséggel bír az EIR biztonsága szempontjából, mert az ismert biztonsági hibák kihasználásával könnyen válhat a rendszer támadás célpontjává.

Az EIR és környezetük biztonsági frissítéseinek telepítése a változáskezelés hatálya alá esik, ezért ennek során 6.7 A konfiguráció változások felügyelete (változáskezelés) fejezetben leírtak alkalmazandók.

a) **Microsoft termékek biztonsági frissítéseinek telepítése**
A Microsoft termékek biztonsági frissítéseinek telepítésére lehetőség szerint a Microsoft által biztosított központi menedzsment szervert kell alkalmazni, mely biztosítja a frissítések ütemezését, a munkaállomások újraindításának kikényszerítését, a telepítési műveletek naplózását. A biztonsági frissítések éles környezetben történő telepítését meg kell előznie egy a Szervezet jellemző eszközeiből felépített reprezentatív tesztkörnyezetben való tesztelésnek. A tesztelést a biztonsági frissítés kiadását követő 1 héten belül el kell végezni. Törekedni kell arra, hogy a biztonsági frissítések a kiadást követő 4 héten belül telepítésre kerüljenek valamennyi érintett eszközön.

b) **Nem Microsoft termékek biztonsági frissítéseinek telepítése (Unix, Linux)**
A nem Microsoft termékek frissítését a gyártói ajánlások figyelembevételével kell elvégezni.

c) **Irodai segédprogramok biztonsági frissítéseinek telepítése**
Törekedni kell a kiegészítő irodai segédprogramok (pl.: Java Runtime Environment, Adobe Acrobat Reader stb.) naprakészségének biztosítására. Különös figyelmet kell fordítani az irodai segédprogramok EIR-rel való együttműködésére, ezért a frissítéseket először tesztelni szükséges. Az EIR fejlesztőjével kötött szerződésbe bele kell foglalni, hogy az EIR-t úgy köteles továbbfejleszteni, hogy az mindig kompatibilis legyen a kiegészítő irodai segédprogramokkal.

18.8. KÁRTÉKONY KÓDOK ELLENI VÉDELEM

Vírusvédelem

A vírusok és egyéb kártevők (pl.: férgek, kémprogramok, trójai programok stb.) jelentős veszélyforrást jelentenek az EIR-re és az általunk kezelt adatokra, ezért az ellenük való védekezés elengedhetetlen.

A kártevők általi fertőzés elleni védekezés során a következőkről kell gondoskodni:

A fertőzés elkerülése, illetve megbízható megszüntetése érdekében vírusvédelmi szoftverrel kell ellátni minden szervert és munkaállomást. Vírusvédelmi szoftver nélkül sem hálózati, sem önálló számítógép nem üzemeltethető.

A vírusvédelmi szoftverek vírusdefiníciós adatbázisát a lehető leggyakrabban frissíteni kell, ezért vírusvédelmi szoftvereket úgy kell beállítani, hogy a frissítés letöltése automatizáltan történjen a vírusvédelmi rendszert menedzselő szerverről, amely a vírusvédelmi szoftver és a vírusdefiníciós adatbázis szétosztására szolgál. A frissítések letöltésének időintervalluma nem lehet nagyobb 1 munkanapnál.

A rendszergazdának gondoskodnia kell arról, hogy a vírusvédelmet menedzselő szerveren a vírusvédelmi szoftver lehető legfrissebb program- és vírusadatbázis verziója álljon rendelkezésre.

A vírusvédelmi szoftverhez tartozó szoftverfrissítések telepítése a változáskezelés hatálya alá esik, ezért ennek során a 6.7 A konfiguráció változások felügyelete (változáskezelés) fejezetben leírtak alkalmazása kötelező.

A vírusvédelmi szoftvereket úgy kell telepíteni és beállítani, hogy a háttérben folyamatosan futva (rezidens módban) működjenek, azaz a számítógép indításakor a szoftver aktivizálódjon, és állandó védelmet biztosítson. . A beállítások jelszavas védelmével biztosítani kell, hogy a felhasználók a vírusvédelmi rendszert ne tudják kiiktatni ill. beállításait módosítani.

A vírusvédelmi szoftvereket úgy kell beállítani, hogy legalább hetente automatikusan időzített, a számítógép valamennyi helyi háttértárolójára kiterjedő, teljes körű vírusellenőrzés történjen. Fájl szerverek esetén a vírusellenőrzést úgy kell beállítani, hogy a lezárult vizsgálat után legfeljebb 24 óra múlva újra induljon el.

A cserélhető adathordozókon (pl.: CD, DVD, pendrive, külső merevlemez) a használat előtt minden esetben vírusellenőrzést kell végezni. A vírusvédelmi szoftverek beállításával kell gondoskodni arról, hogy az ellenőrzés automatikusan megtörténjen.

A vírusvédelmi szoftvereket olyan módon kell beállítani, hogy fertőzés esetén a szoftver elsődleges akcióként próbálja megtisztítani, ha az sikertelen, akkor helyezze karanténba vagy törölje a fertőzött fájlokat (a karanténba helyezett fájlok csak a vírusvédelmi szoftver által elérhetők, és később egy újabb vírusdefiniciós adatbázissal a szoftver képes lehet a karanténba helyezett fájlok megtisztítására). Minden ilyen intézkedésről riasztást kell, hogy küldjön a Rendszergazdának.

Amennyiben a Rendszergazda téves riasztást feltételez, azt jeleznie kell az EIBF részére, aki meghatározza az esetleges további teendőket.

18.13. AZ EIR MONITOROZÁSA

A rendszer kiszolgálóira felügyeleti eszközöket kell telepíteni, hogy a Szervezet időben észlelhesse a rendellenességeket.

A felügyeleti eszközök segítségével Rendszergazdáknak folyamatosan monitorozniuk kell a rendszert, hogy

a) felfedezzék a támadásokat, vagy potenciális támadásra utaló jeleket;
b) felfedezzék az engedély nélküli hálózati kapcsolatokat;
c) azonosítsa a rendszer jogosulatlan használatát;
d) haladéktalanul értesüljenek a rendszerelemek működési zavarairól

Az észlelt eseményeket elemezni kell, az események súlyától függően a Rendszergazdának értesítenie kell az IT vezetőt, illetve az EIBF-t.

Amennyiben szükséges, jogi állásfoglalást is kérhet a tevékenységgel kapcsolatban.

18.37. BIZTONSÁGI RIASZTÁSOK ÉS TÁJÉKOZTATÁSOK

Az EIBF az illetékes hatóságok informatikai biztonsági riasztásait, ill. az informatikai szakportálokon megjelenő biztonsági figyelmeztetéseket folyamatosan nyomon követi és a szükséges intézkedéseket megteszi.

Folyamatosan nyomon követi a Kiberbiztonsági incidenskezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket, valamint az informatikai szakportálokon megjelenő biztonsági figyelmeztetéseket.

Szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki, tanácsokat és iránymutatásokat készít.

A biztonsági iránymutatásoknak megfelelően megteszi a megfelelő ellenintézkedéseket és válaszlépéseket.

18.67. INFORMÁCIÓ KEZELÉSE ÉS MEGŐRZÉSE

Az EIR be- és kimeneti információinak (pl.: számlák, adatszolgáltatások) kezelésével kapcsolatban a Szervezet hatályos Iratkezelési Szabályzatával összhangban a következők az előírások:

a) Gondoskodni kell a be- és kimeneti információk tartalmi ellenőrzéséről.
b) Gondoskodni kell arról, hogy a kimeneti információkhoz történő fizikai és logikai hozzáférés csak az arra jogosult személyekre korlátozódjon.
c) Gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat.
d) Biztosítani kell, hogy a megsemmisítési eljárások során a kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.
e) A kimeneti információkat (pl. számlákat) a vonatkozó jogszabályok, szabályzatok szerint kell megőrizni.

A Szervezet az EIR kimeneti információit nyomtatott formában, elzártan vagy hiteles elektronikus formában őrzi meg.

19. ELLÁTÁSI LÁNC KOCKÁZATKEZELÉSE

19.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

Jelen eljárásrend célja a beszállítói lánc kockázatainak kezelése és minimalizálása. Az eljárásrend meghatározza a beszállítói láncra vonatkozó kockázatkezelési szabályokat és követelményeket, emellett előírja az alvállalkozókra vonatkozó ellenőrzéseket és a beszerzési stratégiák kidolgozását. Kiemelt figyelmet fordít a beszállítók értékelésére és felülvizsgálatára, valamint a rendszerek vagy rendszerelemek hitelességének biztosítására.

Felelős: EIBF

Felülvizsgálat: évente, vagy nagyobb változások esetén.

Jelen eljárásrendet az IT vezetővel, a Rendszergazdával, valamint a Kockázati szereplőkkel (1.6.2.) minden esetben ismertetni kell.

19.2. ELLÁTÁSI LÁNCRA VONATKOZÓ KOCKÁZATKEZELÉSI SZABÁLYZAT

Az ellátási láncra vonatkozó kockázatkezelési szabályok megegyeznek az általános informatikai kockázatkezelési szabályokkal.

Ki kell alakítani egy folyamatot annak érdekében, hogy azonosítani és kezelni lehessen a gyengeségeket vagy hiányosságokat a meghatározott EIR-ek ellátási láncának elemeiben és folyamataiban.

Biztosítani kell, hogy az ellátási láncért felelős személyek részt vegyenek a gyengeségek és hiányosságok azonosításában és kezelésében, valamint az erre vonatkozó folyamatok kidolgozásában és végrehajtásában. Ezen személyeket be kell vonni a kockázatkezelésbe.

ELLÁTÁSI LÁNCCAL KAPCSOLATOS KONTROLLOK ALKALMAZÁSA

Alkalmazni kell a meghatározott ellátási lánccal kapcsolatos kontrollokat annak érdekében, hogy védeni lehessen a rendszerelemet vagy rendszer szolgáltatást az ellátási lánccal kapcsolatos kockázatokkal szemben.

Ilyen fenyegető tényezők lehetnek:

- Kutatás-fejlesztés elakadása
- Tervezési hiba
- Gyártási hiba
- Beszerzési probléma
- Szállítás nehézségei
- Üzemeltetés zavara, vagy hibája
- Karbantartás hiányosságai
- Kivezetés/Selejtezés problémái

Csökkenteni lehet az ellátási lánccal kapcsolatos eseményekből eredő károkat és következményeket a meghatározott kontrollok hatékony alkalmazásával.

Abban az esetben, ha a beszállítók megváltoznak, a beszállítói kockázatelemzéseket soron kívül el kell végezni.

Az ellátási lánccal kapcsolatos kockázatok és kezelésük a [Kisköre VPH *Kockázat-menedzsment*] dokumentumban találhatók.

19.4. ELLÁTÁSI LÁNCRA VONATKOZÓ KÖVETELMÉNYEK ÉS FOLYAMATOK

A külső partnerek képviselőivel a mindenkor hatályos IBSZ vonatkozó részeit a feladatnak megfelelő mértékben ismertetni kell. A betekintés mélységének meghatározása Adatgazda felelőssége. A szerződéskötés és az együttműködés során biztosítani kell, hogy a külső partner (fejlesztő cég, szállító) az általa gyártott, telepített, fejlesztett EIR-t és rendszerelemet úgy konfigurálja, hogy annak minden eleme és egésze eleget tegyen az IBSZ-ben előírtaknak.

A már meglévő rendszerek cseréje, megújítása esetén meg kell vizsgálni, és szükség esetén az aktuális kockázatoknak megfelelően módosítani kell a belső besorolást. Új rendszerek bevezetésénél el kell végezni a rendszerek besorolását.

19.7. ELLÁTÁSI LÁNC ELLENŐRZÉSEK ÉS FOLYAMATOK – ALVÁLLALKOZÓK

Bármely informatikához kapcsolódó szolgáltatást nyújtó szolgáltató, ill. alvállalkozó, valamint más együttműködő partnerrel való együttműködés megkezdése előtt a szerződést előkészítő munkatárs az IT vezető bevonásával megvizsgálja a felmerülő informatikai biztonsági kockázatokat, hozzáférési igényeket, és a szükséges kontrollokat beépíti a partnerrel kötött szerződésbe, kapcsolódó megállapodásba. Szolgáltató, ill. alvállalkozó bevonása miatt fellépő új kockázat felmerülésekor a kockázatot az EIBF a kockázat-felmérési eljárások során kezeli.

19.13. BESZERZÉSI STRATÉGIÁK, ESZKÖZÖK ÉS MÓDSZEREK

Vizsgálatnak kell alávetni potenciális beszállítókat, hogy meggyőződjünk arról, hogy megfelelnek a Szervezet által meghatározott biztonsági és minőségi követelményeknek. Ez magában foglalja az üzleti hátterük, referenciáik és minősítéseik ellenőrzését.

Fontos, hogy a szerződésekben szerepeljenek olyan záradékok, amelyek biztosítják a beszállítók felelősségét és kötelezettségét az adatvédelem, az információbiztonság és más kapcsolódó biztonsági kérdések tekintetében.

A kritikus beszállítók kiválasztásánál és felhasználásánál fontos, hogy a Szervezet ne támaszkodjon kizárólag egyetlen beszállítóra. A különböző beszállítók és források felhasználása csökkenti az egyetlen beszállítótól való függőséget és az ezzel járó kockázatot.

Rugalmas szerződési feltételek bevezetése szükséges, amelyek lehetővé teszik a szerződések módosítását vagy felmondását bizonyos kockázati események bekövetkezte esetén, például egy beszállító hanyagsága vagy károkozása esetén.

Rendszeres ellenőrzések és felügyeleti mechanizmusok bevezetése kell az ellátási lánc különböző szakaszaiban annak érdekében, hogy azonosítsák és kezeljék az esetleges kockázatokat és problémákat.

19.19. ÉRTESÍTÉSI MEGÁLLAPODÁSOK

A beszállítói láncban részt vevő szervezetekkel olyan megállapodás szükséges, amely kitér a kommunikációra, információ áramlásra, az ellenőrzésekre a Szervezet és a beszállítók között.

19.22. RENDSZEREK VAGY RENDSZERELEMEK VIZSGÁLATA

A Szervezet a saját üzemeltetésű, de külső szervezet által támogatott rendszerek, vagy rendszerelemek esetén, nagyobb változások kapcsán a következő ellenőrzéseket kell, hogy elvégezze, az esetleges hamisítások felderítése érdekében:

- Kritikus események monitorozása és naplóvizsgálat:
  Az EIR-en kritikus események monitorozása, például bejelentkezések, hozzáférési kísérletek, rendszerműveletek segíthetnek az illetéktelen tevékenységek felismerésében.
- Hálózati forgalom elemzése, IDS/IPS:
  Hálózati switch-ek, vagy hálózati packet analyzer szoftverek használatával monitorozni lehet a kimenő és bejövő adatforgalmat. IDS/IPS rendszer képes észlelni és blokkolni a gyanús, vagy illetéktelen tevékenységeket.

19.23. RENDSZERELEM HITELESSÉGE

A rendszerelemek hamisítás elleni vizsgálata kötelező a rendszerbe illesztés előtt. A különböző rendszerelemeket többféle módszerrel kell vizsgálni:

Hardverkomponensek: fizikai ellenőrzéssel (szemrevételezés) kell vizsgálni. Figyelni kell az idegen címkéket, forrasztásokat vagy változásokat a külső megjelenésben. Ellenőrizni kell az alkatrészek eredetiségét és hitelességét, amelyeket védjegyek vagy tanúsítványok igazolnak.

Szoftverkomponensek: ha lehetőség van rá, akkor forráskód-ellenőrzést kell végezni. Amennyiben nincs. úgy a digitális aláírások hiánya vagy érvénytelensége jelezheti a hamisítást.

Firmware, vagy BIOS: ellenőrizni kell a firmware és BIOS verzióját a gyártó hivatalos weboldalán vagy a rendszer dokumentációjában. Amennyiben van rá lehetőség, akkor a gyártó által rendelkezésre bocsátott speciális firmware vagy BIOS ellenőrző eszközt kell használni. Át kell nézni a BIOS beállítását, amelyben nem jóváhagyott beállításokat kell keresni.

Amennyiben hamisításra utaló nyomokat találunk a rendszerelemekben, úgy azt jelezni kell a rendszerelem szállítójának, illetve az EIBF-nek, aki dönt a további lépésekről.

19.24. RENDSZERELEM HITELESSÉGE – HAMISÍTÁS ELLENI KÉPZÉS

Az Informatika csoportot képezni kell a hamisítások felismerésére. Ezen képzések megszervezése és lebonyolítása az IT vezető feladata.

19.25. RENDSZERELEM HITELESSÉGE – KONFIGURÁCIÓFELÜGYELET

Különös odafigyelést igényelnek a szervizelt, vagy javított rendszerelemek. Az újbóli üzembeállítás előtt a konfigurációs beállításokat össze kell vetni a konfigurációfelügyeletet ellátó rendszer – illetve az automatikus leltár - által dokumentálttal és ellenőrizni kell a nem jóváhagyott változtatásokat.

19.27. RENDSZERELEM SELEJTEZÉSE, MEGSEMMISÍTÉSE

Biztonságosan selejtezni az adatokat, dokumentációkat, eszközöket és rendszerelemeket a következő módszerekkel kell selejtezni (vagy megsemmisíteni):

Adatok és dokumentációk megsemmisítése: A bizalmas adatok és dokumentációk megsemmisítésére biztonságos módszereket kell használni: iratmegsemmisítő gépeket, vagy adathordozó megsemmisítő gépeket.

Adatok és dokumentációk biztonságos törlése: Ha az adatok elektronikus formában vannak, adatmegsemmisítő szoftvereket vagy eszközöket kell alkalmazni, amelyekkel elérhető az adatok és adathordozók visszaállíthatatlan törlése.

Adatok és dokumentációk titkosítása: Ha az adatok és dokumentációk tartalmaznak bizalmas információkat, el lehet végezni azok titkosítását.

Fizikai eszközök selejtezése: A fizikai eszközök (pl. számítógépek, merevlemezek, nyomtatók) selejtezését úgy kell végrehajtani, ha a Rendszergazda előtt meggyőződik arról, hogy a merevlemezeket vagy más adattároló eszközöket visszaállíthatatlan technikával törölték vagy fizikailag megsemmisítették.

Rendszerelemek fizikai megsemmisítése: Ha a rendszerelemeket nem lehet újra hasznosítani vagy újra használni, akkor a hardvert fizikailag meg kell semmisíteni, hogy a Szervezet elkerülje azok visszaállítását vagy visszafejtését.

Dokumentálás és nyilvántartás: a selejtezési folyamatot a Rendszergazdának dokumentálni kell, és a dokumentumon szerepeltetni kell:

a) az összes selejtezett elemet;
b) az elemek selejtezési dátumát;
c) a folyamatot végrehajtó személyt;
d) az eljárás részleteit;

Ez segít megfelelni a jogszabályi előírásoknak és auditoknak.

20. AI ESZKÖZÖK HASZNÁLATA

Az AI, mint eszköz nem tiltott a Szervezetnél, de a következő szigorú szabályozás vonatkozik a használatára:

20.1 FELHASZNÁLÓK - AI-ESZKÖZÖK (CHATGPT, COPILOT)

Szabályok:

- A felhasználó nem adhat meg bizalmas, személyes, üzleti vagy ügyféladatot (pl. neveket, címeket, belső dokumentum-részleteket, jelszavakat, kódokat) semmilyen AI-eszközbe, kivéve, ha a Szervezet írásban engedélyezte az adott platform használatát.
- Az AI-eszközökkel generált tartalmakat (szöveg, kód, elemzés) mindig ellenőrizni kell hitelesség és pontosság szempontjából, mielőtt azokat bármilyen belső vagy külső kommunikációban felhasználják.
- A felhasználó nem hivatkozhat AI-eszközök által generált információra hivatalos szervezeti állásfoglalásként vagy döntéstámogató anyagként.
- Az AI-eszközök használata során mindig be kell tartani a GDPR, szerzői jogi és etikai elveket, különösen, ha az kimenet harmadik félnek továbbításra kerül.
- A felhasználó köteles minden AI-kapcsolódó anomáliát (pl. gyanús adatkérés, hibás működés, adatszivárgás) haladéktalanul jelezni a Rendszergazdának, vagy az IBIR vezetőnek.

20.2 RENDSZERGAZDÁK - AI-INTEGRÁCIÓ ÉS ÜZEMELTETÉS

Szabályok:

- AI-rendszer csak jóváhagyott, dokumentált és tesztelt módon integrálható az informatikai környezetbe.
- Az AI-szolgáltatások eléréséhez használt API-kulcsokat, hitelesítő adatokat, tokeneket kizárólag titkosított jelszó- vagy titokkezelőben szabad tárolni.
- A rendszergazda köteles gondoskodni arról, hogy az AI-eszközök hálózati kapcsolatai TLS-titkosítással és szűrt hozzáférési szabályokkal működjenek.
- Az AI-rendszerekről (beleértve a cloud-alapú AI-szolgáltatásokat is) naplózni kell minden hozzáférést és API-hívást. A naplókat biztonságosan meg kell őrizni és rendszeresen ellenőrizni kell.
- Az AI-eszközök üzemeltetésére és adatáramlására kockázatértékelést kell végezni.
- A rendszergazda köteles felügyelni a külső AI-szolgáltatókat és biztosítani, hogy adatfeldolgozási szerződés érvényben legyen.

21. ZÁRÓ RENDELKEZÉSEK

A Szervezet vezetője gondoskodik arról, hogy az IBSZ-ben foglaltakat valamennyi a Szervezet feladatellátásában részt vevő alkalmazott megismerje.

Új alkalmazott Szervezethez történő felvétele esetén a Munkaügyi ügyintéző gondoskodik arról, hogy az alkalmazott a munkaszerződés aláírása előtt megismerje a szabályzat munkaköréhez kapcsolódó fejezeteit.

A Szervezet alkalmazottai tevékenységük ellátása során kötelesek alkalmazni IBSZ-ben foglalt rendelkezéseket, valamint ennek megfelelően kell kialakítaniuk a munkafolyamataikat.

Kisköre, 2025.12.12.

Kisköre Városi Polgármesteri Hivatal Jegyzője 1.

dr. Tóth János Zoltán
jegyző

22. MELLÉKLETEK

ALKALMAZOTT MEGNEVEZÉSEK, KIFEJEZÉSEK:

A jelen szabályzatban alkalmazott megnevezések és rövidítések a következők:

- **IBSZ:** Információbiztonsági Szabályzat, jelen eljárásgyűjtemény.
- **adatgazdai terület:** az a szervezeti egység, amelyhez az informatikai rendszerben tárolt adatok kezelése rendelhető, illetve ahol az adat keletkezik.
- **alaprendszer**: az alkalmazói szoftverek működéséhez szükséges alap informatikai szolgáltatásokat megvalósító informatikai rendszerek (pl.: központi címtár, fájl szerver szolgáltatások, levelező rendszer, stb.).
- **alkalmazói rendszer**: a Szervezet tevékenységét közvetlenül támogató informatikai rendszer (pl.: Jira, stb.).
- **beépített rendszergazdai fiók:** a szoftverek és hardver eszközök kiemelt jogosultságú, gyárilag beépített rendszergazdai fiókja (pl.: admin, administrator, root, superuser, SA, stb.), amelyek segítségével a rendszerelem felügyelhető, adminisztrálható.
- **belső fejlesztés**: a Szervezet által történő szoftverfejlesztés.
- **elektronikus információs rendszerek biztonságáért felelős személy (EIBF):** a Szervezet elektronikus információs rendszerei biztonságáért felelős személy.
- **hálózati megosztás:** a szerveren elhelyezkedő, programokat vagy dokumentumokat tartalmazó fájl mappa, amelyhez a felhasználók jogosultságokkal szabályozható módon hozzáférhetnek.
- **hálózati nyomtató:** közvetlenül a hálózatra kapcsolódó nyomtató vagy multifunkciós (fénymásolásra és szkennelésre is alkalmas) nyomtató.
- **home mappa:** a felhasználók saját használatú fájljai, dokumentumai, felhasználóhoz kötődő beállításai, lekérdezései tárolására a felhasználók rendelkezésére bocsájtott, mások által nem elérhető mappa.
- **illegális szoftver**: érvényes használati engedély (szoftverlicenc) nélkül, vagy nem a licencszerződésnek megfelelően használt szoftver.
- **informatika csoport:** a belső- és kiszervezett informatikai infrastruktúra- és alkalmazásüzemeltetők, illetve rendszergazdák összessége
- **informatikai azonosító**: az informatikai eszközhöz a Szervezetnél alkalmazott egységes névkonvenció szerint rendelt egyedi azonosító.
- **informatikai erőforrások:** az informatikai rendszer hardver, szoftver, hálózati és környezeti infrastruktúra elemeinek összessége.
- **informatikai eszköz**: számítógép, számítógéphez kapcsolódó periféria (pl.: monitor, billentyűzet, egér, nyomtató, szkenner, pendrive, külső merevlemez, stb.) vagy egyéb olyan hardver eszköz (pl. hálózati eszköz), amely az informatikai rendszer működéséhez szükséges.
- **informatikai rendszer:** azon elektronikus információs rendszer, amely magában foglalja a hardver eszközöket, a szoftvereket, a hálózati és környezeti infrastruktúra elemeit, valamint tágabb értelemben a szoftverekben kezelt adatokat, az adathordozókat, a dokumentációkat, szabályzatokat és a rendszert kezelő személyeket.
- **Infotv.**: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.
- **IT vezető:** az informatikai üzemeltetés, fejlesztés felügyeletével megbízott személye

- **Kiberbiztonsági incidenskezelő központ:** a kijelölt nemzeti kiberbiztonsági incidenskezelő központ, amelynek feladatait a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézetének egy biztonsági eseményekkel foglalkozó akciócsoportja, más néven a nemzeti CSIRT (Computer Security Incident Response Team) látja el.
- **kiemelt kódrendszer**: informatikai rendszerben alkalmazott kiemelt jelentőségű kódrendszer, amelyeket több informatikai rendszer közösen használ és kapcsolódási pontot jelent az egyes informatikai rendszerek között.
- **központi címtár**: a hálózati rendszer felhasználóinak adatait tároló központi adatbázis.
- **kulcsfelhasználó:** az informatikai rendszerhez az adatgazdai terület részéről kijelölt, a rendszerben tárolt adatok védelméért, a rendszer funkcionális működéséért felelős felhasználó.
- **külső fejlesztés**: a Szervezeten kívül egyéb külső fejlesztő cég bevonásával történő szoftverfejlesztés.
- **legális szoftver, jogtiszta szoftver**: érvényes használati engedéllyel (szoftverlicenccel) rendelkező, a licencszerződésnek megfelelően használt szoftver. A vásárolt, bérelt, illetve külső fejlesztésű szoftverek esetében a számla, felhasználói licencszerződés/licencigazolás és az eredeti telepítő adathordozók együttes vagy részbeni meglétével kell hitelt érdemlően bizonyítani a használat jogosságát (számlának minden esetben lennie kell). A belső fejlesztésű szoftverek esetén a szoftverlicenc igazolásához a forrásprogram megléte szükséges.
- **licenceköteles szoftver**: olyan szoftver, amely használata használati engedélyhez (szoftverlicenchez) kötött, és amelyért a szoftver szerzője használati díjat kér. Ide tartoznak a vásárolt, bérelt vagy belsőleg fejlesztett, illetve külső fejlesztő cég bevonásával fejlesztett szoftverek.
- **mobil adathordozó**: informatikai eszköznek minősülő, cserélhető adathordozó (pl.: pendrive, külső merevlemez).
- **mobil eszköz:** hordozható számítógép (laptop, notebook) vagy egyéb informatikai és kommunikációs feladatok ellátására használható, operációs rendszerrel, kommunikációs szolgáltatásokkal rendelkező, hordozható eszköz (pl.: mobiltelefon, PDA, táblagép).
- **munkaállomás**: olyan személyi számítógép (PC), amelyet a felhasználó a napi munkája során használ, és amellyel igénybe veheti a szerverek szolgáltatásait. Lehet asztali számítógép (desktop PC) és hordozható számítógép (laptop, notebook).
- **rendszergazda**: az informatikai rendszer felett felügyeletet gyakorló személy.
- **szabad szoftver**: olyan szoftver, amelynek licencszerződéséből kétséget kizáróan megállapítható, hogy a szerző vagyoni jogairól lemond, a szoftver használatáért díjat nem kér (freeware szoftverek), illetve bizonyos korlátozásokkal engedélyezi a szoftver használatát díj fizetése nélkül (shareware vagy demo szoftverek).
- **Szjt:** 1999. évi LXXVI. törvény a szerzői jogról.
- **távoli hozzáférés:** minden olyan hozzáférés a Szervezet informatikai rendszeréhez (felhasználó vagy másik informatikai rendszer által), amelyben a kommunikáció egy külső, nem a Szervezet által ellenőrzött hálózaton (pl. Interneten) zajlik.
- **technikai felhasználói fiók**: nem személyhez, hanem szoftverhez, szolgáltatáshoz vagy hardver eszközhöz kötődő felhasználói fiók, amelyet belsőleg használnak valamely más rendszer szolgáltatásának eléréséhez (pl.: egy alkalmazói szoftver használja adatok tárolásához az adatbáziskezelő szerveren; vagy egy multifunkciós nyomtató szkennelt dokumentumok e-mail-ben történő küldéséhez; stb.).
- **ticketing és hibabejelentés (HelpDesk)**: a Szervezet által üzemeltetett informatikai rendszer, amely célja a (külső-belső) felhasználói oldalon jelentkező, informatikai rendszerekkel kapcsolatos bejelentések fogadása és a bejelentések kezelése.

- **védett terület**: az informatikai eszközöket koncentráltan tartalmazó helyiségek (pl.: szerverterem, hálózati rendező helyiség), vagy bizalmas iratokat tartalmazó helyiségek (pl. irattár), illetve a nem védett területnek számító helyiségben elhelyezett egyedi hálózati rack szekrények.
- **vírusvédelmi szoftver**: a vírusok és egyéb kártevők (pl.: férgek, kémprogramok, trójai programok) elleni védekezésre szolgáló program, amely képes felismerni, és a legtöbb esetben eltávolítani a fertőzött számítógépről a kártékony programokat.