Kórházak témaellenőrzése 2022

Selyem Zsuzsanna, Hegyi Károly
NKI Hatósági Főosztály
hatosag@nki.gov.hu

Miért épp a mentések?!

Az ellenőrzési folyamat lépései

NKI	KÓRHÁZ
megkeresés	
online konzultációk	lemaradások pótlása (IBF, IBSZ, biztonsági osztályba, -szintbe sorolások)
adatbekérő végzés	lemaradások pótlása (ld. fent)
vizsgálatindító végzés	kért dokumentumok beküldése, bizonyítékok előkészítése
dokumentumellenőrzés, interjúk	interjún történő részvétel
ellenőrzési feljegyzés	észrevételek közlése
ellenőrzést lezáró határozat	végrehajtás és beszámolás

Határidős feladatok

- elektronikus információs rendszer biztonságáért felelős személy (IBF) regisztrálása → **60 nap**
- informatikai biztonsági szabályzat (IBSZ) beküldése → 90 nap
- rendszerek biztonsági osztályba sorolása → 1 év
- szervezet biztonsági szintbe sorolása → 1 év

A határidőket a létfontosságú rendszerelemmé kijelölő határozat véglegessé válásától kell számítani!

IBF kijelölés

- lehet külsős vagy saját alkalmazott
- követelmények: büntetlen előélet, felsőfokú végzettség, megfelelő szakképzettség/5 év szakmai gyakorlat
  - NKE EIV képzés
  - az Information Systems Audit and Controll Association (ISACA) által kiadott:
    - Certified Information System Auditor (CISA),
    - Certified Information Security Manager (CISM),
    - Certified in Risk and Information Systems Control (CRISC)
  - az International Information Systems Security Certification Consortium Inc. által kiadott Certified Information Systems Security Professional (CISSP) **érvényes** oklevél
- a szakképzési követelményeket a kijelölő határozat véglegessé válásától számított 5 éven belül kell teljesíteni
- bejelentés az NBSZ-IBF űrlapon, a kórház hivatali kapujáról, IBF-től nem jó

IBSZ beküldése

- hatályos, a kórház vezetője által kiadott dokumentum
- a szabályzat szövegét kereshető formátumban
- az aláírt előlapot pdf vagy kép formátumban
- beküldés az NBSZ-IBD űrlaphoz becsatolva (szükség szerint tömörítve)
- a későbbiekben a felülvizsgált, frissített verziókat is ugyanilyen módon kell benyújtani

Előzmény: rendszerek felmérése

- a kijelölt rendszerelemeknek **a létfontosságú tevékenységben közreműködő** elektronikus információs rendszerei
- elektronikus információs rendszerek nyilvántartása (rendszer alapfeladatai, szolgáltatásai, licensz szám, a rendszer felett felügyeletet gyakorló személy, valamint a szállító/ fejlesztő/ karbantartó adatai és elérhetőségei)
- A besoroláshoz szükséges információk még: a rendszer szerepe, súlya, helyettesíthetősége a létfontosságú tevékenységében, a benne kezelt adatok típusa és mennyisége

Biztonsági osztályba sorolás

- kockázatelemzés saját módszertan vagy a NEIH-OVI űrlap „Osztályba sorolás” lapja szerint ➔ elvárt biztonsági osztály
- a követelményeknek történő aktuális megfelelés vizsgálata ➔ teljesített biztonsági osztály
- lehetőség a biztonsági intézkedések fokozatos kivitelezésére ➔ az első besoroláskor megállapított biztonsági osztályhoz képest minden egyes következő osztály teljesítésére 2 év áll rendelkezésre

Biztonsági szintbe sorolás

- az általános szervezet besorolása kötelező, a fejlesztést vagy üzemeltetését végző, az üzemeltetéséért vagy az információ-biztonságáért felelős szervezeti egységeké opcionális
- NBSZ-SZVI űrlapon a „Szintbe sorolás” fülön ➔ elvárt biztonsági szint
- „Követelmények” lapon az aktuális megfelelés vizsgálata ➔ teljesített szint
- biztonsági szint fokozatos elérése ➔ minden egyes biztonsági szint elérésére 2 év, ha vizsgálat időpontjában nem érik el az 1. szintet, akkor az ahhoz tartozó intézkedések teljesítésére 10 év

Cselekvési terv

- ha a biztonsági osztály vagy –szint teljesítésénél hiányosságot állapítanak meg, akkor **90 napon belül** cselekvési tervet kell készíteni a megvalósítandó intézkedések ütemezésére
- konkrét tennivalók felsorolása, határidőkkel és felelősökkel
- a fokozatos kivitelezés alkalmazásánál a határidőszámítás során nem vehető figyelembe a besorolások csúszása, az óra elkezd ketyegni a létfontosságú kijelöléstől, így a teljesítés végső időpontjánál ezt kell alapul venni.

Hivatalos elektronikus kommunikáció

- IBF regisztráció az NBSZ-IBF űrlapon, kizárólag az ügyfél szervezet hivatali kapujáról
- IBSZ benyújtás, biztonsági osztályba és –szintbe sorolások, egyéb dokumentumok NBSZ-IBD űrlaphoz (több file esetén tömörítve) becsatolva, vagy az ügyfél szervezet hivatali kapujáról, vagy az IBF személyes ügyfélkapujáról
- az NBSZ hivatali kapujára: NBSZ (KRID: 427386978)
- Űrlapok: https://nki.gov.hu/hatosag/tartalom/urlapok/

Jogszabályi előírások

- A mentéseket a 41/2015 BM rendelet 3.1.4.8 és 3.1.4.9 pontjai és ezek alpontjai alapján **az EIR-ek biztonsági osztályához** tartozó előírásoknak megfelelően kell végezni.
- **2-es vagy magasabb** biztonsági osztályba sorolt EIR esetében rendszeresen mentést kell végezni az EIR-ekben kezelt ill. tárolt
  - adatokról, felhasználó-szintű információkról, (3.1.4.8.1.1)
  - rendszerszintű információkról, (3.1.4.8.1.2)
  - dokumentációról. (3.1.4.8.1.3)
- Gondoskodni kell a mentett adatok és információk védelméről. (bizalmasság, sértetlenség, rendelkezésre állás) (3.1.4.8.1.4)
- Gondoskodni kell az EIR helyreállításáról és újraindításáról egy havaria helyzetet követően. (3.1.4.9)

Jogszabályi előírások (folytatás)

- **4-es vagy 5-ös** biztonsági osztályba sorolt EIR esetében
  - rendszeresen tesztelni kell a mentett információkat, (3.1.4.8.2)
  - tranzakció alapú EIR esetén úgy kell a mentést megvalósítani, hogy tranzakció helyreállításra is legyen lehetőség. (3.1.4.9.2)
- **5-ös** biztonsági osztályba sorolt EIR esetében
  - úgy kell a mentést megvalósítani, hogy annak teszteléskor képesnek kell lenni egyes funkciók önálló visszaállítására is, (3.1.4.8.3)
  - a kritikus információkat el kell különíteni és biztonságosan kell tárolni, (3.1.4.8.4)
  - Az elektronikus információs rendszer biztonsági másolat információit biztonsági tárolási helyszínen kell tárolni, amely az azonos veszélyektől való érzékenység csökkentése érdekében elkülönül az elsődleges helyszíntől. (3.1.4.8.5)

Az ellenőrzésre kért dokumentumok

- IBSZ
- Mentési eljárásrend
- A mentés részletes dokumentációja
  - (mentési terv, mentési napló)
- EIR-ek biztonsági osztályba sorolásának dokumentációja (OVI űrlapok) Erről további információk a hatóság honlapján: https://nki.gov.hu/hatosag/tartalom/ugyfajtak/biztonsagi-osztalyba-sorolas-megfelelosegenek-ellenorzese/

Az IBSZ és a mentési eljárásrend

- Az IBSZ-ben *vagy annak mellékletében* szerepeltetni kell az EIR-ek felsorolását és azok biztonsági osztályát.
- Az IBSZ-ben *vagy a mentési eljárásrendben* meg kell határozni az adatok mentésének és archiválásának rendjét:
  - A mentéssel kapcsolatos **tevékenységek** felsorolása és azok **felelősei**, szerepkör alapon megnevezve.
  - A mentés folyamata, a mentés folyamatának ellenőrzése, a mentés eredményének ellenőrzése, adathordozók rendelkezésre állásának biztosítsa, adathordozók kezelése, tárolása, szállítása, törlése, újra felhasználása, és selejtezése során alkalmazandó **szabályok**.
  - A mentéssel kapcsolatos **elvárások**. (lásd a következő diát)

Ki mondja meg, hogy mik az elvárások?

- Az informatikus? Az IBF ? A hatóság ?
- **Minden esetben az alkalmazásgazda határozza meg a mentés/visszatöltés követelményeit, amelyek a következők**
  - **Mentendő adatok köre,**
  - **mentési gyakoriság,** hatással van az RPO-ra,
  - **mentési technológia és módszer**: hatással van az RTO-ra,
  - **megőrzési idő.** (hosszú távú és rövid távú)
- A mentés követelményeinek meghatározásakor az IT üzemeltetés közreműködése nélkülözhetetlen!
  - Figyelembe kell venni a költségeket is! Minél nagyobbak a követelmények, annál költségesebb a megvalósítás.
  - A mentési technológiák és módszerek részletekbe menő ismerete nem várható el az alkalmazásgazdától.

A mentés részletes dokumentációja 1

- **Mentési terv**
  - Mentés-job ok részletes leírása: a mentésre kerülő állományok / könyvtárak felsorolása **EIR-enként,**
  - a mentés típusa (pl. hetente full, naponta inkrementális),
  - a mentő eszköz(ök) és szoftverek pontos típusát/verziószámát,
  - a mentés-job-ok futásának tervezett ütemezése és a mentési időablak,
  - az adathozdozók rövid távú, gyors elérésű tárolásának módszere,
  - az adathordozók rotációjának menete, *
  - az adathordozók hosszú távú megőrzésének módszere,

A mentés részletes dokumentációja 2

- **Mentési napló**
- Az elvégzett mentés-job-okról naplót kell vezetni! A napló lehet elektronikus, vagy papíros, készülhet automatikusan, vagy kézi beavatkozással.
- **Legfontosabb tartalmi elemei**:
  - A mentés-job mentési terv szerinti azonosító száma,
  - Visszatöltés esetén a visszatöltés oka (pl: teszt, vagy kérés alapján)
  - Kezdete és vége tényleges időpontja,
  - Sikeresség jelzése, hibaüzenetek,
  - Mentési adathozdozó azonosítója,

Az ellenőrzés sarkalatos pontjai

- **A szabályozási környezet legyen összhangban az alkalmazott gyakorlattal!**
- A mentésekkel szemben támasztott elvárásokat az alkalmazás-felelősök **dokumentáltan** kell hogy jóváhagyják. (**RTO, RPO, megőrzési idők**)
- A mentés részletes dokumentációjából (mentési terv és mentési napló) legyen kiolvasható, hogy a mentés gyakorlati megvalósítása teljes mértékben megfelel az alkalmazásfelelősök elvárásainak.
- Az alkalmazott mentési technológia képes legyen biztosítani a hosszútávú adattárolási igényeket is. (archiválás)
  - Egy szemléletes példa arra, amikor ez nem látszik biztosítottnak: Az elvárás az, hogy 10 évig kerüljenek megőrzésre és a mentéseket **LTO 5** technológiára épülő mentő eszközzel írják szalagra.

    Indoklás: Az LTO 5-ös 2010-es technológia. A jelenleg még működő (10+ éves!!) LTO 5 meghajtó folyamatos használatban tartása esetén a meghibásodás esélye az eszköz öregedésével arányosan nő. Új LTO 5 eszköz vásárlásának lehetősége egyre kisebb.

A mentés és a Ransomware-ek

- A Ransomware támadás valós veszély!
  - Az egészségügyi intézmények kitettsége nagy,
  - súlyos következményekkel jár.
- **Kizárólag az offline – elkülönítetten – tárolt, teljes körű biztonsági mentés megléte nyújthat segítséget egy Ransomware támadás okozta károk enyhítésére.**
- A mentési terv készítése során az adathordozók rotációjának megtervezésekor arra is figyelemmel kell lenni, hogy a Ransomware fertőzés és annak észlelése közt több nap/hét is eltelhet! Nem biztos, hogy az észlelést megelőző napi mentés lesz az, amiből az adatok teljes köre visszanyerhető!

Kérdés 1: Az ellenőrzések ütemezése

Válasz: Az ellenőrzések hivatalos részét vizsgálatindító végzéssel kezdjük várhatóan nyár elejétől. A sorrendnél figyelembe vesszük a kórházak felkészültségét, azokkal kezdjük, akiknél a legkevésbé van szükség a fő feladatoknál pótlásra.

A biztonsági besorolásoknál háromévenkénti felülvizsgálati kötelezettség van, akinél ez az idő eltelt az első besorolástól, kérjük ezt figyelembe venni.

Az ellenőrzéseket idén be szeretnénk fejezni, ezért az utolsó végzéseket szeptemberben küldjük ki. Akinek méltányolható indoka van, kérjük, előre jelezze, ha valamelyik időszak alkalmatlan az ellenőrzésre.

Kérdés 2: IBF összeférhetetlenség, végzettség

Válasz: Összeférhetetlenségi előírások nem szerepelnek a vonatkozó jogszabályokban, azonban a szakmai ajánlások alapján javasolt az IT üzemeltetési és a biztonsági feladatkörök személyi elkülönítése.

Nem kizárt, hogy a biztonsági összekötő lássa el az IBF feladatokat is, amennyiben a törvényi feltételeknek megfelel.

Az IBF szervezetben elfoglalt helyének vonatkozásában törvényi elvárás, hogy az IBF a szervezet vezetőjének közvetlenül adhasson tájékoztatást.

A végzettségre vonatkozó korlátozások: Felsőfokú végzettség szükséges, de nem feltétel az informatikai szakirány. Ezen felül az IBF-ként kijelölésre kerülő személynek rendelkeznie kell a 26/2013. KIM rendelet szerinti megfelelő szakképzettséggel vagy 5 év szakmai gyakorlattal.

Kérdés 3: létfontosságú kijelölések

Válasz: A Nemzeti Kibervédelmi Intézetnek nincs befolyása a létfontosságú kijelölésekre. A létfontosságú rendszerek és üzemeltetőik adatait a kijelölést követően a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóságtól mint nyilvántartó hatóságtól kapja meg a hatóság.

Az Ibtv. hatálya alá a létfontosságú kijelölés véglegessé válásával kerülnek a kijelölt létesítmények/ rendszerek azon elektronikus információs rendszerei, amelyek közreműködnek a létfontosságú tevékenységben (ebben az esetben: aktív fekvőbeteg-ellátás és a működtetéséhez szükséges szolgáltatások).

Kérdés 4: hivatalos értesítés

Válasz: A teljes ellenőrzési eljárás lefolytatására összesen 120 nap áll rendelkezésre a vizsgálatindító végzés és a záró határozat kiküldése között. Jelen tájékoztatás célja, hogy a hatóság lehetőséget biztosítson a hiányok ledolgozására még a hatósági eljárás megindítását megelőzően.

Ebből következően, ahol a három fő feladat teljesítésében hiányosságot tapasztal a hatóság, ott adatbekérő végzést küld a tavaszi hónapokban, majd a későbbiekben vizsgálatindító végzéssel veszi kezdetét a konkrét hatósági ellenőrzési eljárás. Ettől eltérő, egyéb hivatalos értesítés kiküldése nem áll módunkban.

Kérdés 5: A 4-es biztonsági osztály további információbiztonsági követelményei

Válasz: A jelenleg meghirdetett ellenőrzés **részellenőrzés**. Célja a mentésekre vonatkozó követelmények teljesülésének ellenőrzése. A további követelményeknek történő megfelelést jelen ellenőrzés nem érinti, de a vizsgálat megkezdéséhez szükséges minimum feltételeket minden szervezetnek szükséges teljesítenie :

- IBF kijelölés,
- IBSZ beküldés,
- EIR-ek azonosítása és osztályba sorolása,
- A szervezet biztonsági szintbe sorolása.

Részletesen lásd az 5-9 es diákon.

A további követelmények a 41/2015. BM rendelet 3-4. mellékletében találhatók, illetve jobban használható formában az OVI űrlapok 3.1.1-3.3.13. munkalapjain.

Kérdés 6: EIR-ek azonosítása

Válasz: Minden olyan EIR-t azonosítani kell, amely **közreműködik a létfontosságú tevékenységben**.

Az **ecoSTAT** gazdasági rendszer –a konzultáción vázoltak szerint,– leginkább az anyagellátás biztosításában betöltött szerepe alapján kimeríti ezt a kritériumot, ezért a hatóság álláspontja szerint be kell sorolni. Ezen álláspontunk egy vázlatos megismerésen alapul, tehát részletes indoklással vitatható.

A **központi rendszereket** annak a szervezetnek kell besorolnia, aki a rendszer **adatkezelő**je. Az adatkezelést végző szervezetnek akkor is be kell sorolnia a rendszert, ha annak üzemeltetését nem ő végzi. A biztonsági osztályhoz tartozó követelményeket az adatkezelő az üzemeltető és a felhasználók felé szerződéses úton érvényesíti.

A képalkotó- és labordiagnosztikai rendszerek több esetben nem a kórház üzemeltetésében/tulajdonában vannak, a besorolásnál ezeket sem szabad figyelmen kívül hagyni. Ha ezek külső üzemeltetésben vannak, akkor is a kórház feladata biztosítani a biztonsági osztályához tartozó követelmények teljesülését (szerződés!).

Kérdés 7: EIR-ek azonosítása (folytatás)

Várhatóan 2022 végére minden kórházban olyan HIS rendszer lesz, amelyet az OKFŐ fejleszttet. Ennek besorolása szükséges-e az egyes kórházak részéről?

Válasz: A megvalósítás részletei az előadás időpontjában még nem ismertek.

- Ha központi rendszerként lesz megvalósítva, amelynek az OKFŐ az adatkezelője, akkor a rendszer biztonsági osztályba sorolását az OKFŐ-nek kell elvégeznie. A kórházaktól elvárt informatikai biztonsági feltételek teljesüléséről az OKFŐ és a felhasználó kórház közötti szerződésben kell gondoskodni.
- Ha egyedileg üzemeltetett rendszerként lesz megvalósítva, azaz a kórházak lesznek az adatkezelők, akkor a rendszer besorolását a felhasználó kórháznak kell elvégeznie és neki kell gondoskodni az elvárt informatikai biztonsági követelmények teljesüléséről is.

Kérdés 8: Követelmények meghatározása

Válasz: A megőrzési idők, továbbá az RPO és RTO értékek meghatározásakor minden esetben figyelembe kell venni a kórházak működését szabályozó jogszabály(ok) előírásait is. A mentési, archiválási rendszereket az adatok mentésére és hosszú távú megőrzésére vonatkozó ágazati szabályokat is szem előtt tartva kell kialakítani.

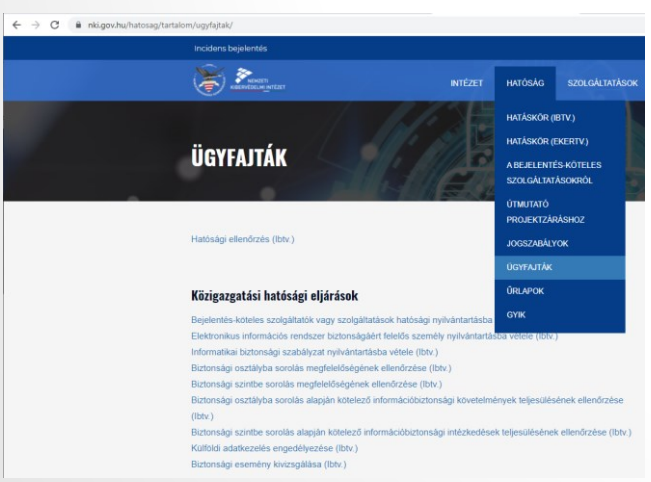
Kérdés 9: A szankciók

Válasz: Az ellenőrzésen feltárt hiányosságok pótlására a hatóság határozatban kötelezi az ügyfelet. Amennyiben ez nem vezet eredményre, a hatóság **nem tiltja meg** az EIR használatát, hanem a rendelkezésére álló szankciós eszközökkel él, melyeket az Ibtv. 16. § (2) és (3) bekezdése sorolja fel:

- felszólítás
- a (kórházakat) felügyelő szerv közreműködésének kérése
- információbiztonsági felügyelő kirendelése
- bírság

Kérdés 10: Kapcsolattartás a Hatósággal

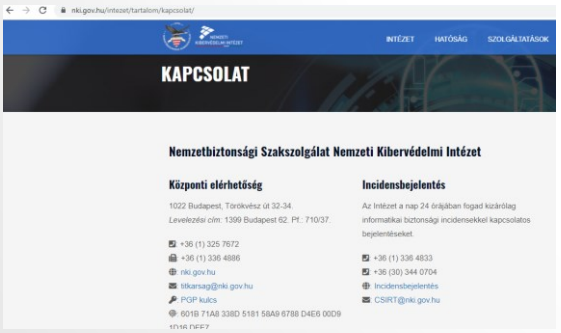
Válasz: Az NKI honlapján a Hatóság / Ügyfajták menüpont alatt részletes útmutatókat tett közzé. **https://nki.gov.hu/hatosag/tartalom/ugyfajtak/**



Incidensbejelentés

Az NKI CSIRT szakterülete a linken látható csatornákon fogadja az incidensbejelentéseket: https://nki.gov.hu/intezet/tartalom/kapcsolat/

Kérjük, haladéktalanul jelentsék be az incidenseket, különös tekintettel az adathalász e-mailekre!



Köszönöm a figyelmet!