ECSÉD

Ecsédi Polgármesteri Hivatal

biztonságelemzési eljárásrendje

Tartalomjegyzék

I. BEVEZETÉS

Az Ecsédi Polgármesteri Hivatal az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.), valamint annak végrehajtására kiadott rendeletekben foglalt elektronikus információbiztonsági feladatok elvégzésére irányuló felkészülést, illetve azok végrehajtását megkezdte.

Az Ibtv. 11. §-ának (1) bekezdés e) pontja és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet 3.3.4.1. pontjában meghatározottak szerint az Biztonságelemzési eljárásrendben a Hivatal mint érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a biztonságértékelési eljárásrendet, amely a biztonságértékelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő; a biztonságértékelési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a biztonságértékelési eljárásrendet.

Jelen dokumentum célja, hogy ismertesse a Hivatal biztonságelemzési eljárásrendjét.

II. BIZTONSÁGELEMZÉSI ELJÁRÁSREND

2.1A rendszerek biztonsági követelményei

2.1.1 A biztonsági követelmények elemzése és meghatározása

Az alkalmazások fejlesztése során kialakított rendszerek, rendszerelemek dokumentáltsága olyan részletezettségű kell, hogy legyen, hogy a hivatal azt a fejlesztő nélkül is képes legyen üzemeltetni, szükség esetén továbbfejleszte(t)ni.
Az informatikai rendszer hardver elemeinek fejlesztése során kialakított dokumentációnak olyan részletezettségűnek kell lennie, hogy a hivatal azt a fejlesztő/szállító nélkül is képes legyen üzemeltetni, egyedi eszköz esetén utángyártatni, pótolni.

Fejlesztés / tervezés

Az operációs, az alap- és az alkalmazás rendszerek biztonsági funkcionalitását a rendszer által kezelt adatok besorolásának megfelelően kell kialakítani.
Az alkalmazások specifikálása során meg kell határozni a rendszerbe beépítendő biztonsági és ellenőrzési kritériumokat, valamint az adatok jóváhagyásának eljárásrendjét. Az alkalmazások adatainak kezeléséhez a felhasználók részére megfelelő felületet kell specifikálni.

Tesztelés

Az alkalmazások éles üzemi környezetbe történő telepítésüket megelőzően az éles üzemi környezettől független tesztkörnyezetben a szállítóktól független, dokumentált tesztelésének kell alávetni.

Tesztelés céljára a mentett, illetve archivált „éles" adatok felhasználását el kell kerülni. Ha ez nem valósítható meg, akkor az adatok titkosságát oly módon kell biztosítani, hogy az feleljen meg a jogszabályokban meghatározott adat- és titokvédelmi követelményeknek.

Forráskód

Az alkalmazások üzembe helyezésével egyidejűleg az üzembe helyezendő rendszer forráskódját, amennyiben az a hivatal tulajdona, biztonságos körülmények között, eltérő földrajzi helyen, 1-1 példányban kell őrizni.

A forráskódok letétbe helyezésére olyan eljárást kell kidolgozni, amely biztosítja, hogy a szállító által letétbe helyezett, illetve a hivatalnak átadott forráskódok megegyezzenek az éles üzemben működő rendszerek forráskódjával.

2.2Alkalmazási rendszerek biztonsága

2.2.1 A bemenő adatok érvényesítése

Az alkalmazások bemenő adatainak hitelességét ellenőrizni kell, hogy gondoskodjunk annak pontosságáról, és helyességéről. Az állandó adatokat (neveket és címeket, ügyfelek azonosító számait), valamint a paramétertáblázatokat (árakat, adókulcsokat) ellenőrizni kell. Felelős az adatgazda.

Lehetőség szerint maga a feldolgozó rendszer is beépítetten ellenőrizze az adatokat.

2.2.2 A feldolgozás ellenőrzése

A helyesen bevitt adatok is sérülhetnek akár a feldolgozás hibái, akár szándékos tevékenységek következményeként. A rendszerekbe az ilyen meghibásodások felismerése érdekében érvényesítő ellenőrzéseket kell beépíteni. Az alkalmazások

tervezésekor kell gondoskodni arról, hogy a korlátozások megvalósítása valóan minimalizálja a sértetlenség elvesztésére vezető feldolgozási hibák kockázatát.

2.2.3 Üzenethitelesítés

Üzenethitelesítés az a technika, amelyet arra használnak, hogy észleljék a továbbított elektronikus üzenet tartalmában beállt bármely illetéktelen beavatkozást, változtatást vagy rongálást. Az üzenethitelesítés olyan alkalmazások esetében szükséges, ahol biztonsági követelmény az üzenettartalom sértetlenségének a védelme. A hivatalban rendszerszintű üzenethitelesítésére nincs szükség. Meghatározott külső szervezetek rendszereinél szükséges lehet az üzenethitelesítés, ott digitális aláírással rendelkező személy hitelesíti azt.

2.2.4 A kimenő adatok érvényesítése

Az alkalmazási rendszerek kimeneti adatainak hitelességét ellenőrizni kell annak érdekében, hogy gondoskodjunk arról, hogy a tárolt adatok feldolgozása helyes és a követelményeknek megfelelő.

Az informatikai rendszerben előállított vagy tárolt bizalmas adatok szállítónak, támogatónak, vagy külső munkatársnak történő átadása esetén titoktartási nyilatkozat cégszerű aláírása szükséges. Felelős: a bizalmas adatokat átadó, az ellenőrzésért az Információbiztonsági felelős.

2.3 Kriptográfiai óvintézkedések

Az informatikai rendszer által kezelt adatokat – különös tekintettel a jogszabályokban meghatározott minősítésükre, az alkalmazott informatikai technológiára – az általuk megjelenített kockázatokkal arányos kódolási eljárásokkal kell védeni.

Az informatikai rendszer által tárolt felhasználóleveleket, jelszavakat és hozzáférési listákat biztonsági besorolásuknak megfelelően, kriptográfiai eljárással kell védeni az illetéktelen felfedéstől.

2.3.1 A kriptográfiai óvintézkedések használatának szabályzata

A kriptográfiai megoldások alkalmasságára vonatkozó döntéshozatal egy szélesebb folyamat része kell, hogy legyen, amelyben felmérik a kockázatokat és meghatározzák a szükséges óvintézkedéseket.

Az alkalmazandó kriptográfiai megoldásról, használatról az Információbiztonsági felelős dönt a rendszergazda egyetértésével.

2.3.2 Kulcsgondozás

A hivatal csak más szervezet által kiadott kulcsot használ, melynek gondozását a kiadó szervezet végzi.

A kriptográfiai megoldások külső szolgáltatóival, például egy tanúsító szervezettel kötött szolgáltatási megállapodások, vagy szerződések tartalma fedje le az olyan részleteket, mint a felelősség, a szolgáltatás megbízhatósága, valamint a szolgáltatás rendelkezésére bocsátásának ideje a megrendelés időpontjához képest.

2.4 A rendszerállományok/-fájlok biztonsága

Az informatikai eszközökre csak és kizárólag jogtiszta szoftvereket szabad telepíteni és üzemeltetni. A telepített szoftverekről és licenceikről nyilvántartást kell vezetni. A telepítéshez szükséges minden adathordozót, dokumentációt, eszközt lehetőség szerint két példányban kell megőrizni, eltérő helyen.

Licencnyilvántartás

Minden az informatikai rendszerre és munkaállomásra telepített rendszerszoftver és alapszoftver jogtisztaságát igazoló licencről pontos és naprakész nyilvántartást kell vezetni. Felelős: jegyző

Ajánlott a rendszerszoftver és alapszoftver elemek pontos és naprakész leltárba vételét automatikus eljárással végezni.

2.4.1 Az éles szoftver ellenőrzése

Informatikai rendszerben történő minden szoftver telepítését ellenőrzött módon kell végrehajtani. Az üzemeltető, éles rendszeren a szoftverek biztonságát biztosítani és ellenőrizni kell.

Az informatikai rendszeren a megrongálódás kockázatát minimalizálandó a következő védelmi intézkedéseket kell betartani (élesítési rendszabályok):

a) az éles programkönyvtárak frissítését a rendszergazda, vagy megbízottja végzik;

b) ha lehetséges, az éles informatikai rendszer csak futtatható kódot tartalmazzon;

c) a végrehajtható kódot az éles üzemi rendszeren addig nem szabad élesíteni, amíg nem áll rendelkezésre a sikeres teszt jegyzőkönyv és a felhasználói átvétel dokumentuma, valamint a megfelelő program-könyvtárakat nem hozták naprakész állapotba;

d) A szoftver korábbi változatait a kritikusság, valamint a régebbi adatok olvashatósága biztosításának mértéke szerint kell megtartani. A gyenge biztonsági pontok eltávolítása, vagy számuk csökkentésére a rendelkezésre álló patch-eket megfelelő, sikeres tesztelése után telepíteni kell;

e) Az éles rendszer nem tartalmazhat félkész, befejezetlen forráskódokat.

A folyamatért a rendszergazda, az ellenőrzésért az információbiztonsági felelős felel.

2.4.2 Rendszervizsgálati adatok védelme

A teszt adatokat védeni és ellenőrizni kell. Mind a rendszervizsgálatok, mind az átvételi vizsgálatok többnyire jelentős mennyiségű olyan adatot igényelnek, amelyek eléggé közel állnak az éles adatokhoz. Az éles adatbázis használatát kerülni kell. Ha mégis ilyen információ kerül használatra, akkor az adatokat meg kell fosztani személyes jellegüktől, illetve megfelelő módosításokat kell végrehajtani ahhoz, hogy eltérjenek az éles adatokról.

Fentiekét a rendszergazda, valamint a tesztelést végző szervezeti egység vezetője a felelős.

2.4.3 A forrásprogram könyvtár hozzáférés-ellenőrzése

A számítógépes programok veszélyeztetésének csökkentése érdekében szigorúan ellenőrizni kell a forráskódokhoz való hozzáférést a következők szerint.

a) Ahol az lehetséges, a forráskódokat nem szabad éles rendszerekbe tartani.
b) Fejlesztés vagy karbantartás alatt álló programokat nem szabad forrásprogramok könyvtáraiba tartani.
c) Forráskódokat korábbi változatait archiválni kell, pontosan megjelölve annak időpontját, amikor azok éles üzemben voltak.
d) A forrásprogramok könyvtárainak karbantartását és másolatát szigorú változásellenőrző eljárásnak kell alávetni.

A forráskódok nyilvántartásáét a rendszergazda felel.

2.5 A fejlesztő és támogató folyamatok biztonsága

Az alkalmazások fejlesztése egy új termék kifejlesztését, vagy egy piacon meglevő termék testre szabását, vagy egy informatikai rendszerben már működő alkalmazás módosítását – verzióváltását – jelentheti.

2.5.1 A változásellenőrző eljárások

Az informatikai rendszerek fejlesztése – mind infrastruktúrafejlesztés, mind alkalmazásfejlesztés esetén – és üzemeltetése során bekövetkező változásokat követni kell. Részletesen a folyamatot a Változáskezelési szabályzat tartalmazza.

A változáskezelési eljárásrendet úgy kell kialakítani, hogy az informatikai rendszer szervezet, illetve végrehajtott változásait az információ biztonságáért felelős munkatárs nyomon követhesse, azt ellenőrzései során felhasználhassa.

A szállítóktól meg kell követelni a vonatkozó informatikai biztonsági szabályok betartását.

Az informatikai rendszer felépítéséről, biztonsági beállításairól naprakész dokumentációval kell rendelkezni.

2.5.2 Az operációs rendszer változ(tat)ásainak műszaki felülvizsgálata

Időről időre szükség lehet arra, hogy az operációs rendszert lecseréljük, hogy egy újonnan leszállított szoftverváltozatot vagy egy javítást telepítsünk.

Az operációs rendszer változtatása esetén az alábbi szempontokat kell figyelembe venni:

a) Az alkalmazási rendszereket át kell tekinteni, és tesztelni kell annak érdekében, hogy szavatolni lehessen, hogy a változ(tat)ás az üzemeltetésre és a biztonságra nincsen negatív hatással.

b) Az ügymenet folyamatosságára vonatkozó tervekben amennyiben szükséges, a megfelelő változtatásokat át kell vezetni.

c) Amennyiben a változtatás (javítócsomag) nem befolyásolja hátrányosan az alkalmazások működését, a tesztelt javítócsomagot a legrövidebb időn belül telepíteni kell.

d) Az operációs rendszert úgy kell a rendszergazdának beállítani, hogy automatikusan ne kínálja fel a rendszer javítócsomagjának letöltését és/vagy telepítését. A javítócsomagot a felhasználók semmiképpen nem telepíthetik a munkaállomásokon.

Felelős a rendszergazda.

2.5.3 A szoftvercsomagok változtatási korlátozása

A szoftvercsomagok nem frissítésként vagy verzióváltásként végrehajtott módosítását lehetőség szerint el kell kerülni. Amennyire csak lehetséges és a gyakorlatban az kivitelezhető, a szállító által adott szoftvercsomag módosítás nélkül kell használni.

Felelős a rendszergazda.

2.5.4 Információ kiszivárogtatás

Az információ kiszivárgását minden lehető eszközzel meg kell előzni. A megelőző érdekében az alábbi szempontokat kell alkalmazni:

a) programokat csak tiszta forrásból szabad beszerezni;

b) csak bevizsgált, tesztelt terméket szabad használni;

c) minden forráskódot át kell vizsgálni üzemi (éle) használatba vétel előtt;

d) kulcsfontosságú rendszereken csak megbízható munkatársak dolgozzanak;

e) a munkatársak tevékenységének biztonsági ellenőrzésére a hivatal fenntartja a jogot.

A teszt rendszerben is történjen vírusellenőrzés. Felelős a rendszergazda.

2.5.5 Kihelyezett szoftverfejlesztés

Amikor szoftverfejlesztési feladatra a hivatal szerződést köt, azaz a fejlesztési tevékenységet kihelyezik, a következő szempontokat kell figyelembe venni és a szerződésbe foglalni:

a) licencszerződéseket, a szoftver tulajdonjogát és a szellemi tulajdonjogokat;
b) a végzett munka minőségének és pontosságának tanúsítását;
c) a harmadik fél hibája esetére vonatkozó lépéseket;
d) az elvégzett munka minőségének és pontosságának átvilágító auditálásához szükséges hozzáférési jogokat;
e) a szoftverminőség szerződéses követelményeit;
f) a szoftverfejlesztés projekttervére vonatkozó követelményeket;
g) a telepítés előtt elvégzendő vizsgálatokat.

Amennyiben az informatikai rendszer elemein a hivatal fejlesztését végezhet, akkor a fejlesztés során kialakított dokumentáció olyan részletes legyen, hogy a hivatal a fejlesztett elemet a fejlesztő nélkül is képes legyen biztonságosan üzemeltetni, egyedi eszköz esetén után gyártani, pótolni.

A fenti szempontok alkalmazásáért a fejlesztési szerződést kezdeményező vezető a felelős.

2.6 Technikai sérülékenység menedzsment

2.6.1 A technikai sérülékenységek ellenőrzése

A használt információ feldolgozó rendszerek sebezhetőségére vonatkozó időszerű információkat, rendszeresen be kell szerezni. A sérülékenységek elleni védelem eszközeként az előzetesen megvizsgált frissítések minél előbb történő telepítését el kell végezni. (Patch-menedzsment). A frissítéseket ahol lehetséges központilag kell letölteni és telepíteni. A frissítések kezeléséért a rendszergazda felel.

III. INFORMATIKAI BIZTONSÁGI INCIDENS KEZELÉS

3.1 Jelentés az informatikai biztonsági eseményekről és gyengeségekről

3.1.1 Jelentés az informatikai biztonsági eseményekről

Az informatikai rendszer felhasználóitól meg kell követelni, hogy jelentsék a rendszerekben vagy a szolgáltatásokban minden felismert vagy feltételezett biztonsági eseményt, a rendellenestől eltérő működését. Ezeket haladéktalanul jelenteni kell vagy saját vezetőiknek, vagy az üzemeltetőnk, vagy az információbiztonsági felelősnek.

A biztonsági esemény kivizsgálása az információbiztonsági felelős feladata. A kivizsgálásba szükség esetén bevonhatja az üzemeltető munkatársait, illetve külső szakértőt.

Az informatikai rendszer minden üzemzavarát, elemeinek minden meghibásodását hibanaplóba kell bejegyezni.

A bejelentést fogadónak legalább a következőket kell feljegyeznie a bejelentett eseményekről: a bejelentés ideje, a bejelentő neve, az esemény rövid leírása, feltételezett oka, az elhárítás résztvevője, az elhárítás kezdete, az elhárításához megtett intézkedés, az elhárítás vége.

Az informatikai rendszer elemeinek meghibásodásairól vezetett bejegyzéseket rendszeresen értékelni szükséges. Felelős a rendszergazda.

3.1.2 Jelentés a biztonsági sérülékenységekről

Az informatikai rendszer felhasználóitól meg kell követelni, hogy jelentsék a rendszerek vagy a szolgáltatások minden felismert vagy feltételezett biztonsági gyengeségét vagy fenyegetettségét. Ezeket haladéktalanul jelenteni kell vagy saját vezetőiknek, vagy az üzemeltetőnek. A felhasználók a feltételezett gyengeséget semmilyen körülmények között se próbálják maguk megszüntetni.

A jelzett informatikai gyengeség kivizsgálása, a szükséges óvintézkedések meghatározása a rendszergazda feladata. A kivizsgálásba szükség esetén bevonhatja az információbiztonsági felelőst.

3.2 A biztonsági eseményekre és incidensekre adott válasz és fejlesztés

3.2.1 Felelősségek és eljárások

A biztonsági események kezelésének felelősségeit és eljárásait úgy kell megállapítani, hogy a biztonsági eseményekre gyorsan, hatékonyan és rendben meg lehessen tennie a válaszlépéseket.

A következő védelmi intézkedéseket kell végrehajtani:

a napló állományokat és hasonló bizonyítékokat össze kell gyűjteni és azokat biztonságosan kell őrizni.

Okulás a biztonsági eseményekből

Az ismétlődő és jelentős hatású biztonsági eseményeket rendszeresen elemezni, értékelni kell és ezek alapján kiegészítő és továbbfejlesztett védelmi intézkedéseket

kell bevezetni vagy a biztonsági szabályzat felülvizsgálati folyamatában, illetve a képzési tervben figyelembe venni a későbbi előfordulások gyakorisága, kára és költségei korlátozására.

Bizonyítékok gyűjtése

Az informatikai biztonsági óvintézkedések kialakításakor törekedni kell arra, hogy az informatikai biztonság esetleges sérülése esetén a hivatal kellő bizonyítékkal rendelkezzen ahhoz, hogy indokolt esetben a bizonyíték támogasson egy intézkedést egy személy vagy más szervezet ellen.

Számítógép-adathordozón rögzített bizonyíték esetében a hordozható adathordozók, valamint a háttértárolón és a központi tárolón talált információ másolatait meg kell őrizni és rendelkezésre állásáról gondoskodni kell. Felelős az információbiztonsági felelős.

A másolási folyamat során valamennyi tevékenységről naplófeljegyzést kell elkészíteni és tanú jelenléte szükséges. A napló és az adathordozó egy-egy példányát biztonságosan meg kell őrizni.

IV.ZÁRÓ RENDELKEZÉSEK

Jelen szabályzat 2017.július 3. napján lép hatályba és visszavonásig érvényes.

Ecséd, 2017. július „3" „.

ECSÉDI POLGÁRMESTERI HIVATAL Jegyző Ecséd

Nagy Lászlóné

jegyző