ECSÉD

Ecsédi Polgármesteri Hivatal

rendszer és kommunikációvédelmi 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 3.3.13.1. pontjában meghatározottak szerint a Rendszer és kommunikációvédelmi eljárásrendben a Hivatal mint érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belüli szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a rendszer- és kommunikációvédelmi eljárásrendet, mely a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő; a rendszer- és kommunikációvédelmi eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja, és frissíti a rendszer- és kommunikációvédelmére vonatkozó eljárásrendet.

Jelen dokumentum célja, hogy ismertesse a Hivatal rendszer és kommunikációvédelmi eljárásrendjét.

II. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

2.1. Rendszer- és kommunikációvédelmi eljárásrend

Az érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belüli szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a rendszer- és kommunikációvédelmi eljárásrendet, mely a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő; a rendszer- és kommunikációvédelmi eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja, és frissíti a rendszer- és kommunikációvédelmére vonatkozó eljárásrendet.

2.2. Túlterhelés - szolgáltatás megtagadás alapú támadás - elleni védelem

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

2.3. A határok védelme

Az elektronikus információs rendszer felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt; a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól; csak az érintett szervezet biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

Jelen fejezetben rögzített szabályok betartása alapvető követelmény, megszegése súlyos biztonsági eseménynek tekintendő.

Alapvető szabályok:

- A különböző zónák (pl. intranet -> internet) közötti kommunikáció tűzfal által kontrollált.
- Ha egy kommunikációs csatorna nincs külön engedélyezve, az tiltott!
- Az egyes hálózati zónák közötti kapcsolat létrehozásakor az alábbiakat kell figyelembe venni:

a kapcsolat legyen megfelelő erősségű titkosítással biztosítva

a kapcsolat legyen megfelelő erősségű azonosítási algoritmussal ellátva

- A kapcsolat megvalósításához ajánlott technológiák (ebben a sorrendben):

VPN kapcsolat kiépítése

SSL/TLS kapcsolat kiépítése

egyedi, titkosított és azonosított kapcsolat kiépítése

Az alkalmazott tűzfal beállításainak meghatározása az informatikai vezető hatáskörébe tartozik, melyet az információbiztonsági felelős véleményezhet. A tűzfal-konfiguráció módosításának igényét, valamint annak jóváhagyását és végrehajtását dokumentálni kell. A módosítás végrehajtása a rendszergazda feladata.

A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban kell elhelyezni, elkülönítve a belső szervezeti hálózattól.

A hálózati határvédelem eszközeinek működését folyamatosan ellenőrizni kell, annak rendszeres frissítéséről kiemelt figyelemmel kell gondoskodni!

2.4. Kriptográfiai kulcs előállítása és kezelése

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

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

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

2.5. Kriptográfiai védelem

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

2.6. Együttműködésen alapuló számítástechnikai eszközök

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

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

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

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

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

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

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

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

Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív vagy gyorsító tárat használó feloldás): Az elektronikus információs rendszer eredethitelesítést és adatsértetlenség ellenőrzést kér és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén: Azok az elektronikus információs rendszerek, amelyek együttesen biztosítanak név/cím feloldási szolgáltatást egy szervezet számára, hibatűrők és belső/külső szerepkör szétválasztást valósítanak meg.

2.9. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

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

2.10. A folyamatok elkülönítése

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

III. 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