Póserné Oláh Valéria
Budapesti Műszaki Főiskola NIK
poserne.valeria@nik.bmf.hu

A SZERVEZETI INFORMATIKAI BIZTONSÁG MEGTEREMTÉSÉNEK, FENNTARTÁSÁNAK ALAPVETŐ FELTÉTELEI

Absztrakt

A szervezetek hatékony működtetéséhez elengedhetetlen információs technológiák magas fokú alkalmazása, azonban e technológiák bevonása a szervezet működésébe fokozott veszélyforrást is jelent. A „biztonságos" működés érdekében fokozott körültekintést igényel a megfelelő szervezeti struktúra kialakítása, esetleg módosítása, a felelősségi körök pontos meghatározása. A cikk célja a rendelkezésre álló dokumentumok, ajánlások, szabályzók figyelembevételével ismertetni, rendszerezni a „biztonságos" informatikai rendszer kialakítása, működtetése érdekét szolgáló informatikai biztonsági célkitűzés, és stratégia kialakítását, valamint a megfontolandó legfontosabb felelősség- és szerepköröket.

For the effective motion of the organizations the high-level usage of the information systems, but the implementation into the motion of the organization of these technologies can cause an increased risk opportunity as well. For the 'secure' system motion the developments of the organizational structure, the exact definition of responsibilities must circumspect on a high-level. With the consideration of the available documents, references and regulations the aim of the article is to review and systematize the formation of the most important responsibilities and roles and the strategy and the aims of the secure information that is interested in the build up and motion of the 'secure' information system.

Kulcsszavak: *informatikai biztonságpolitika, informatikai biztonsági célkitűzés, informatikai biztonsági stratégia, informatikai biztonsági felelősségkörök, szervezeti informatikai biztonság.*

BEVEZETÉS

A szervezetek hatékony vezetéséhez, rendeltetésének megfelelő működtetéséhez szükség van információkra, azok feldolgozására, tárolására, esetlegesen továbbításra. Tudvalevő azonban, hogy egy információs rendszer előbb említett funkciói számtalan veszélyforrást rejtenek (az információ sérülhet, elveszhet, illetéktelen kezekbe juthat, stb.), melyek jelentős anyagi és erkölcsi károkat okozhatnak, ezért a rendszer kialakítása, működtetése során a megfelelő biztonság érdekében igen körültekintően kell eljárni. Az információ azonos szintű védelméről kell gondoskodni, legyen szó akár elektronikus, akár ismeret, vagy papír alapú megjelenítési formájáról.

Az elektronikus információ-kezelő rendszerekben a megfelelő védelem érdekében szükség van **személyi, fizikai, dokumentumbiztonsági és elektronikus információvédelmi intézkedések meghatározására, alkalmazására**, amelyekkel elérhető az elektronikus információ bizalmasságának, az információ és az azt kezelő rendszer sértetlenségének rendelkezésre állásának biztosítása. Mindezek hatékony megvalósítása érdekében

informatikai biztonsági célok (egy bizonyos idő alatt milyen biztonsági szintre kívánják eljuttatni az informatikai rendszert) és a megvalósításuk módjának meghatározása, a végrehajtandó feladatok megfogalmazása, a végrehajtás nyomon követése és ellenőrzése szükséges. A célkitűzések elérését elősegítendő, **informatikai biztonsági stratégiát** kell kidolgozni.

Az információbiztonság alapját az **információ minősítése** és az érvényes **szabályozók** képezik, de a biztonság megteremtéséhez szükséges a **megfelelő szervezeti struktúra kialakítása, esetleg módosítása, a felelősségi körök pontos meghatározása** is.

Jelen dokumentum célja a rendelkezésre álló dokumentumok, ajánlások, szabályzók figyelembevételével ismertetni, rendszerezni a „biztonságos" informatikai rendszer kialakítása, működtetése érdekét szolgáló informatikai biztonsági célkitűzés, és stratégia kialakítását, valamint a megfontolandó legfontosabb felelősség- és szerepköröket.

1. A SZERVEZET INFORMATIKAI BIZTONSÁGPOLITIKÁJA

A szervezet hatékony működésének, racionális irányításának elengedhetetlen követelménye az informatikai biztonság egységes értelmezése, informatikai biztonsági célok és a megvalósításukhoz vezető út, a szükséges feladatok meghatározása, és végrehajtásuk figyelemmel kísérése, az esetleges változások figyelembe vétele érdekében évente egyszeri felülvizsgálata.

1.1. Informatikai biztonsági célkitűzések

Jó informatikai biztonsági stratégiát csak egyértelműen meghatározott célokhoz lehet kidolgozni, melyek meghatározzák, hogy milyen irányba fejlesszék tovább az informatikai biztonsági rendszert, figyelembe véve a szervezet felépítésének, működésének és informatikai rendszerének jövőbeli alakulását is.

A célkitűzések lehetnek: [1]

- **hosszú távú** (stratégiai), 3 évnél hosszabb kitekintést nyújtó,
- **középtávú** (taktikai), 1-3 évre szóló és
- **rövidtávú** (operatív), 1 évnél rövidebb időtávra vonatkozó célok.

Jellegük szerint:

- **Állapot jellegű célok** (célállapotok): Az adott intézmény jelenlegi informatikai biztonsági szintjéből kiindulva megadják, hogy az egyes állapotjelző paraméterek a jövőben milyenek legyenek (ilyenek pl. az elérendő biztonsági szint, egy-egy rendszer megengedett maximális kiesési ideje, két kiesés közötti megengedett minimális idő, a rendelkezésre állás, hatékonysági mutatók, stb.).

- **Folyamat jellegű** (vagy akció-) **célok**: A folyamat lefolyásával kapcsolatos célkitűzéseket és paramétereket írják elő (pl. egy-egy új informatikai eszköz beszerzése, új szabályzatok bevezetése, az üzemeltető szervezet átalakítása, a személyzet képzése, stb.).

1.2. A legfontosabb szerepkörök az informatikai biztonsági célkitűzések meghatározása során [1]

- **Az informatikai üzemeltető szervezet felelős informatikusai:** feladatuk a tervezési szakaszban informatív adatgyűjtés a külső és belső informatikai környezetről, azok elemzése, a lehetőségek és a még nem látható fenyegetések felderítése. Az informatív adatgyűjtés ki kell, hogy terjedjen az intézmény jelenlegi és tervezett jövőbeli felépítésére, biztonságának színvonalára, a hazai és a nemzetközi trendekre, irányelvekre, más intézmények informatikai biztonsági fejlesztéseire, stb. Figyelembe kell venni a belső elvárásokat, a hazai és nemzetközi informatikai biztonság jövőbeli helyzetére vonatkozó előrejelzéseket, az intézmény környezetében (pl.: jogi, gazdasági, politikai, üzleti, piaci, természeti, stb.) bekövetkezett változásokat. További feladat az információgyűjtés folyamatának dokumentálása, az összegyűjtött információk rendszerezése, nyilvántartásba vétele, feldolgozásuk és elemzésük koordinálása, az informatikai biztonsági rendszer módosítására és fejlesztésére vonatkozó célkitűzések megfogalmazásához a szükséges háttér-információk biztosítása.

- **Az intézmény felső vezetése és az informatikai vezetők:** feladatuk az informatív adatgyűjtés eredményei alapján informatikai biztonsági célok meghatározása, a kitűzött céloknak megfelelő informatikai biztonsági stratégia kidolgozása, évente egyszeri felülvizsgálata, feladatok meghatározása, végrehajtásuk figyelemmel kísérése, ellenőrzése.

  A célkitűzés során a legfontosabb feladatok:

  - Az informatikai biztonsági rendszer jelenlegi és jövőbeli tervezett működésének, a változások vázlatos határidőinek és mérföldköveinek rögzítése az egész szervezetre vonatkozólag.
  - A célteljesítés mérési módjának, időléptékének meghatározása.
  - Az informatikai biztonsági rendszer céljaira vonatkozó fontosság meghatározása.
  - Az informatikai biztonsági rendszer fejlesztésére vonatkozó befektetési elképzelés vázolása.
  - A kidolgozott informatikai biztonsági javaslatok és az adott intézmény szükségleteinek összehangolása.
  - Az alkalmazott informatikai biztonsági megoldások hasznának értékelése.

  Az éves felülvizsgálatok szempontjai:

  - Milyen változások következtek be?
  - Aktuálisak-e az informatikai biztonsági célkitűzések?
  - El tudták-e fogadni és be tudták-e tartani az intézmény vezetői és dolgozói az informatikai biztonsági célkitűzéseket?
  - A vezetők és a dolgozók véleménye és tapasztalata.

- Ha nem sikerült megvalósítani a célkitűzéseket, ki vagy mi a felelős?
- Ha sikerült, akkor milyen eredménnyel, és mik a tapasztalatok?
- Az informatikai beruházások és fejlesztések összhangban voltak-e a célkitűzésekkel?
- A célkitűzéseken milyen módosításokra van szükség?

1.3. Informatikai biztonsági stratégia

„Az üzleti életben stratégiaalkotáson egy már elfogadott politikához vagy célhoz vezető alternatív utak meghatározását és értékelését, valamint a követendő alternatíva kiválasztását, részletes kidolgozását értjük." [1]

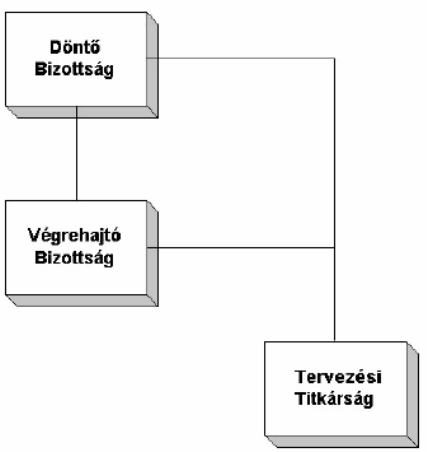
Stratégia tervezése szükséges, ha a megoldandó kérdések az intézmény egészére vagy nagy részére kihatnak, időben hosszú lefutásúak, jelentős erőforrásokat igényelnek, nagyobb változásokhoz vezethetnek a szervezetben.

Az informatikai biztonsági stratégia kialakítása során meghatározó szerepe van a szervezet felépítésének és információszükségletének.

Követelmények az informatikai biztonsági stratégiával szemben:

- A felső vezetés elkötelezett legyen az informatikai biztonsági rendszer szervezetükben betöltendő szerepére vonatkozóan.
- Tartalmazza az információs rendszerek fejlesztésére, üzemeltetésére vonatkozó szabályozási és műszaki terveket.
- Az informatikai rendszer biztonságosabbá tételéhez szükséges finanszírozással kapcsolatos döntéseknek alapját képezze.
- Meg kell adnia a szükséges változtatások azonosításához, tervezéséhez és ellenőrzéséhez szükséges mechanizmusokat.
- Különböző szervezeti (rész)stratégiákra bontható legyen, ha az intézmény különböző szervezeti egységekből tevődik össze. Ekkor szükség van átfogó, az egész intézményre vonatkozó ún. vezérstratégiára is.
- Be kell illeszkednie az intézmény működési kereteit meghatározó éves tervezési ciklusokba.

Az informatikai biztonsági stratégiatervezés szervezeti összetételét az 1. ábra szemlélteti.



1. ábra – Az informatikai stratégiakészítés szervezeti háttere [1]

Döntő bizottság (DB)

Egy intézmény, illetve annak egy nagyobb szervezeti-működési egységében az informatikai biztonsági stratégiatervezés legfelsőbb testülete.

Feladatköre: az informatikai biztonsági rendszer irányítása, az informatikai biztonsági felvetések értékelése és azok alapján döntéshozás az informatikai biztonsági rendszerrel kapcsolatos szervezeti-működési és stratégiai kérdéskörben. Munkamegbízás kiadása minden informatikai biztonsági fejlesztésre. Elnöke célszerűen az intézmény informatikai vezetői közül kerül kiválasztásra, tagjai elsősorban az informatikai üzemeltető szervezet kulcsfontosságú funkcióinak felelősei.

Végrehajtó bizottság (VB)

A Döntő Bizottság nevében jár el és jelentések formájában számol be az informatikai biztonsági stratégia megvalósításához kapcsolódó projektekkel, illetve technológiai koncepciókkal kapcsolatos feladatok teljesítéséről.

Feladatköre: az informatikai biztonsági stratégiából származó összetevők irányítása, felügyelete, vezetése. Az egyes informatikai biztonsági projektek belső ellenőrzése azonban az adott projekt vezetőjének felelősségi körébe tartozik. Nagyobb, összetett intézmény esetén több VB felállítására is sor kerülhet, de ebben az esetben is egyetlen Döntő Bizottságnak számolnak be a feladatok teljesítéséről, kiemelve a döntéseket igénylő területeket. Elnöke az informatikai üzemeltető szervezet vezetője, tagjai pedig az intézmény informatikai biztonságért felelős valamennyi munkatársa, esetlegesen kiegészítve külső tanácsadó cég(ek) képviselőivel, amennyiben a megfelelő szakértelem a cégen belül nem áll rendelkezésre.

Tervezési titkárság (TT)

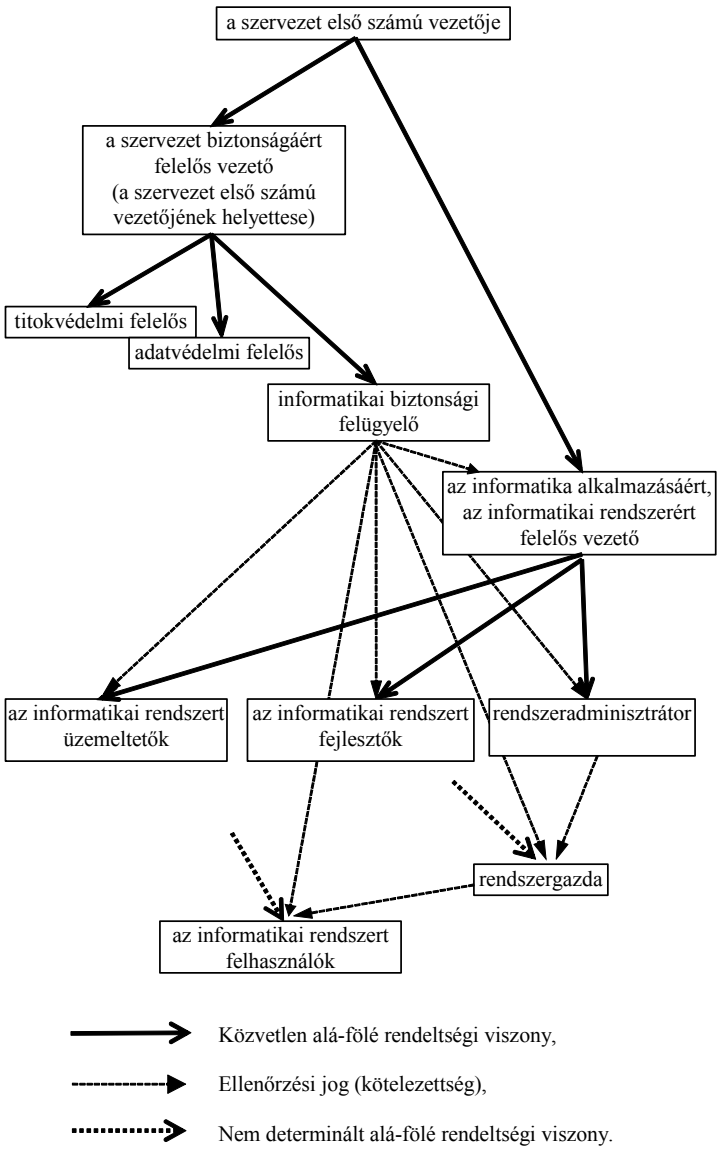
Munkájával a Döntő Bizottságot támogatja, megtervezi a feladatok végrehajtásának menetét, felügyeli és ellenőrzi azt. Így ötleteket dolgoz ki, az ésszerű és gazdaságos végrehajtás érdekében a hasonló problémákat összevonja, biztosítja az informatikai biztonsági célkitűzések és a megvalósítandó tervek összhangját.

Feladatköre: az informatikai biztonsági stratégiákkal és tervekkel kapcsolatban felmerülő végrehajtási, irányítási és műszaki jellegű problémák beazonosítása, kivizsgálása, és a

megfelelő szintre való eljuttatása, az egyes területeken belül illetve azok összességében a teljesítés ellenőrzése.

2. A SZERVEZET INFORMATIKAI BIZTONSÁGI FELADAT- ÉS FELELŐSSÉGI KÖREI

A Szervezeti és Működési Szabályzatok illetve az Informatikai Biztonsági Szabályzat elkészítésekor a szervezeten belül a feladatköröket, a felelősség és kompetencia kérdését az egyes szervezeti egységek, illetve személyek között jól elkülönülten rögzíteni kell és az informatikai biztonság területén is érvényesíteni kell. Az informatikai rendszer biztonsága kapcsán jelentkező feladatokhoz tartozó fontosabb szerepköröket a 2. ábra szemlélteti.



2. ábra: A fontosabb szerepkörök az informatikai rendszer biztonsága kapcsán jelentkező feladatok alapján. [2]

Az egyes szerepkörök között a következő esetekben lehetnek átfedések:

- *„az első számú vezető kisebb szervezeteknél vagy ahol a biztonság különösen kiemelt, betöltheti a szervezet biztonságáért felelős vezető szerepkörét,*

- *ha a szervezet állam- vagy szolgálati titkot tartalmazó adatokat kezel és a szervezet vezetője nem nevez ki titokvédelmi felelőst, akkor ezt a szerepkört is ő tölti be – ha a szervezet nem kezel állam- vagy szolgálati titkot, akkor a titokvédelmi felelős szerepkörére nincs szükség,*

- *ha a szervezetnél a személyes adatok kezelése kapcsán jogszabály előírja az adatvédelmi felelős kinevezését, ezt a szerepkört a titokvédelmi felelős vagy az informatikai biztonsági felügyelő is betöltheti,*

- *a titokvédelmi felelős egyszemélyben lehet informatikai biztonsági felügyelő is,*

- *az informatika alkalmazásáért, az informatikai rendszerért felelős vezető lehet a rendszeradminisztrátor is,*

- *a rendszeradminisztrátor egyben a rendszer üzemeltetője is lehet,*

- *a rendszergazda feladatát a rendszeradminisztrátor, vagy kijelölt felhasználó is elláthatja."* [2]

A Szervezeti és Működési Szabályzatban továbbá meg kell határozni az összeférhetetlen a szerepköröket is.

„Összeférhetetlen a titokvédelmi felelős, az adatvédelmi felelős és az informatikai biztonsági felügyelő szerepköre az informatika alkalmazásáért, az informatikai rendszerért felelős vezető funkciójával, sőt az informatika alkalmazásáért, az informatikai rendszerért felelős vezető alárendeltségében, tőle függő viszonyban sem lehetnek." [2]

Szerepkörök kapcsolataira vonatkozó általános ajánlások: [2]

A szervezeten belül el kell határolni az informatikai rendszert kezelő, fejlesztő, üzemeltető szerepeket a felhasználói funkcióktól. Az intézmény informatikai szervezeti egysége vezetőjének, a nagyobb és fontos alkalmazási területek vezetőivel egyeztetve a fontos alkalmazásokhoz rendszergazdákat kell kijelölniük, pontosan meghatározva feladataikat és felelősségüket. El kell különíteni a fejlesztői környezetet az alkalmazói környezettől, külön kell szabályozni a fejlesztői, működtetői és adminisztrációs hozzáférési jogköröket.

A szervezet első számú vezetője: felelőssége: a szervezetért vállalt általános felelősségén túl az elektronikus információvédelem gyakorlati megvalósítása, az elektronikus információvédelemre vonatkozó jogszabályok, valamint az előírások betartása, betartatása. Feladatai: célkitűzés, a személyi, szervezeti és pénzügyi keretfeltételek megteremtése és az információk védelméért, az informatikai alkalmazások biztonságáért való felelősség szabályozása, projekt létrehozása az informatikai biztonsági stratégia kidolgoztatására, a szükséges személyi-, anyagi- és időkeretek megszabása, döntések meghozatala valamint felelős a stratégia megvalósításáért. Tájékozottnak kell lennie a helyzetfelmérés eredményeiről és végig részt kell vennie a fontos döntésekben. Rendszeresen kell ellenőriznie a bevezetett intézkedések betartását, hatékonyságát és gazdaságosságát, a biztonsági eseményeket, pedig jegyzőkönyvben rögzíttetni. [3]

A szervezet biztonságáért felelős vezetőnek és az **informatikai szervezeti egység vezetőjének** kell szabályoznia az informatikai biztonság szempontjából kritikus területeken a külső személyek belépési, tartózkodási és kilépési, a felhasználók, az adminisztrátorok, a

rendszergazdák, az üzemeltető és karbantartó személyzet rendszeres informatikai biztonság területét érintő oktatásának, továbbképzésének rendjét, az informatikai biztonság megsértése esetén a személyekre vonatkozó intézkedéseket.

Titokvédelmi felelős: feladata az elektronikus információvédelemmel kapcsolatos szakfeladatok szervezeten belüli végrehajtása. A rendszer kivitelezése, telepítése és biztonsági jóváhagyása szakaszában információt szolgáltat az elektronikus információ-kezelő rendszert befogadó infrastruktúráról, gondoskodik az objektumokba és az érintett helyiségekbe való bejutásról. Nincs szükség erre a szerepkörre, ha a szervezet nem kezel állam- vagy szolgálati titkot.

Adatvédelmi felelős: ha a szervezetnél a személyes adatok kezelése kapcsán jogszabály előírja az adatvédelmi felelős szerepkört, akkor a titokvédelmi felelős vagy az informatikai biztonsági felügyelő is betöltheti.

Informatikai biztonsági felügyelő: felelős az informatikai biztonságért, csak ő férhet hozzá a biztonsági eseménynapló adataihoz. Feladata a hozzáférési jogok, privilégiumok; jelszavak meghatározása, változtatása, megszüntetése.

Az informatikai rendszert üzemeltetők: az informatikai biztonsági célkitűzések meghatározása során feladatuk a tervezési szakaszban informatív adatgyűjtés a külső és belső informatikai környezetről, azok elemzése, a lehetőségek és a még nem látható fenyegetések felderítése, az információgyűjtés folyamatának dokumentálása, az összegyűjtött információk rendszerezése, nyilvántartásba vétele, feldolgozásuk és elemzésük koordinálása, az informatikai biztonsági rendszer módosítására és fejlesztésére vonatkozó célkitűzések megfogalmazásához a szükséges háttér-információk biztosítása. A biztonsági jóváhagyó szervezet követelményeinek megfelelően, a rendszer tervezéséért, fejlesztéséért felelős szervezettel együttműködve elkészítik a Rendszer Biztonsági Utasítást („Bizalmas” és magasabb feljogosítási szintű elektronikus információ-kezelő rendszer esetében), a rendszerterv biztonsági mellékletét, az Üzemeltetés Biztonsági Szabályzatot. Javaslatot tesznek az elektronikus információ-kezelő rendszer működési életciklusára a rendszer-specifikus biztonsági felelősségeket viselő személyekre, a rendszeradminisztrátorok személyére és a logisztikai támogatásért felelős szervezetre. Felelősek az elektronikus információ-kezelő rendszer biztonsági feladatait ellátó személyekkel együtt a biztonsági dokumentációnak megfelelő működtetésért, az elektronikus információ-kezelő rendszerben kezelt információ archiválásáért. Az üzemeltetésért felelős szervezet vezetője intézkedik a technikai eszközöknek, termékeknek a rendszerből történő kivonására és további sorsára vonatkozóan. [2][4]

Az informatikai rendszert fejlesztők: biztosítják a forráskód szintű hibajavítás feltételeit, részletesen dokumentálják a fejlesztett szoftverek tesztelési eljárásait.

Rendszeradminisztrátor: feladata a rendszernek és elemeinek az elvárt és igényelt üzemelési állapotban való fenntartása, vezetői jóváhagyás után felhasználói neveket, profilokat és jogosultságokat, jelszavakat állít be az elektronikus információ-kezelő rendszeren az engedélyeknek megfelelően az Üzemeltetés Biztonsági Szabályzat előírásainak betartásával. Az Üzemeltetés Biztonsági Szabályzatban megadott rendszerességgel elvégzi a rendszer biztonsági mentéseit, az engedélyezett konfigurációról naprakész hardver és szoftver nyilvántartást vezet, a nyilvántartásában nem szereplő eszközt eltávolítja a rendszerből és jelenti az eseményt a rendszerbiztonsági felelősnek. Végrehajtja az engedélyezett konfiguráció módosításokat, felkészül katasztrófa helyzetre, a rendszeren észlelt informatikai

biztonsági hiányosságot jelenti a rendszerbiztonsági felelősnek. Tanácsokat ad a felhasználóknak rendszer-üzemeltetési kérdésekben, közreműködik a biztonsági dokumentáció szükség szerinti módosításában. [2][4]

Rendszergazda: feladatköre az adatok naprakész és hiteles voltának (adatminőség) biztosítása, a hozzáférések jogosultágának érvényesítése, a felhasználók támogatása az alkalmazások, adatbázisok szintjén.

Felhasználók: ismerniük kell az Üzemeltetés Biztonsági Szabályzat előírásait és a vészhelyzeti tevékenységeket. Részt kell venniük informatikai biztonsági oktatásokon.

ÖSSZEGZŐ MEGÁLLAPÍTÁSOK

Egy szervezet hatékony működését kiemelten befolyásolja a megfelelő informatikai biztonság kialakítása, mivel ma már elképzelhetetlen a működés az informatikai rendszerek igénybevétele nélkül. Problémákat okoz ma még azonban, hogy hiányzik az összhang az IT menedzserek, igazgatók és döntéshozók szemléletében. Hogy a kockázatkezelési befektetések megtérüljenek, az IT szervezeteknek összhangba kell kerülniük egymással, illetve a vállalat teljes egészével. Az IT kockázatokra vonatkozó eltérő álláspontok az IT irányítás és a vállalati irányítás közötti összhang hiányából erednek, és kockázatot idézhetnek elő a gyenge koordináció miatt. Ez túlzott, vagy nem elégséges befektetéseket eredményez, amely az erőforrások pazarlásához vezet, és nem hatékony IT kockázatkezelési programokat eredményez. A megfelelő szintű informatikai biztonság kialakításának szükséges feltétele egyértelmű, dokumentumban rögzített informatikai biztonsági célok kitűzése, azok alapján egységes informatikai biztonsági stratégia kialakítása.

Az informatikai rendszerek fejlesztése közép- ill. hosszú távú befektetésnek minősül, és ennek megfelelő időtávú tervezést igényel. Egy egységes informatikai biztonsági stratégia kialakítása a legjobb mód az informatikai fejlesztésekre fordított költségek optimalizálására.

Egy informatikai biztonsági stratégiának a felsővezetés kinyilvánításának kell lennie, elkötelezettségét kell élveznie az informatikai biztonsági rendszer szervezetben betöltendő fontos és egyre bővülő szerepére vonatkozóan, az alapját kell, hogy képezze minden olyan finanszírozással kapcsolatos döntésnek, amely az informatikai rendszer biztonságosabbá tételéhez kapcsolódó befektetés kérdéskörben történik.

Az informatikai biztonsági stratégia kialakítása során figyelembe kell venni, hogy az intézmények gyakorta különböző szervezeti egységekből tevődnek össze, tehát részstratégiákra kell tudni bontani, ilyenkor szükség van átfogó ún. vezérstratégiára, amely a rendelkezésre álló erőforrásokkal, az informatikai infrastruktúrával és a felsővezetés információs igényével kapcsolatos központi értékrendet fejezi ki.

Fontos szerepe van a biztonságos működés érdekében az informatikai biztonsági stratégia legalább évenkénti felülvizsgálatának, amikor is figyelembe vehetők a feltételekben, célokban, szerkezetben, teljesítményben bekövetkezett változások és az ebből fakadó esetleges problémák, melyek alapján az informatikai biztonsági célok és stratégia újragondolása szükséges.

A legfontosabb szerepkör az elsőszámú vezető, akinek a döntésén múlik a szervezeti informatikai biztonság megteremtésének sikeressége, minősége. Az ő végső döntésén alapulnak a következők: célok kitűzése, résztvevők kijelölése, motiválása, feltételek

biztosítása, a feladat indítása, ellenőrzése, alternatívák között döntés, jóváhagyás, az intézkedések átvezetése a többi rendszerelemen

A második legfontosabb szerepkör, amin az informatikai biztonság megteremtésének, fenntartásának sikeressége múlhat, az informatikai rendszert üzemeltetők szerepköre, mivel ők végzik az informatív adatgyűjtést és szolgáltatják a megfelelő háttér-információt az egyes döntések meghozatalához.

FELHASZNÁLT IRODALOM

[1] KÜRT Computer Rendszerház Rt.: Informatikai biztonsági rendszerek kialakítása Magyarországon, Budapest, 2002.

[2] Miniszterelnöki Hivatal Informatikai Koordinációs Iroda Informatikai Tárcaközi Bizottság ajánlásai: Informatikai rendszerek biztonsági követelményei, 12. sz. ajánlás, Budapest, 1996.

[3] Dr. Váncsa Julianna: Az informatikai biztonság alapjai, egyetemi jegyzet, Budapest, 2000.

[4] Dr. Váncsa Julianna: Az információtechnológiai fejlődésből adódó kihívások az elektronikus információvédelem területén, Budapest, 2003.