Informatikai biztonsági stratégia

Informatikai biztonsági stratégia

Tartalom

1. Bevezetés

Még a legkifinomultabb biztonsági intézkedések sem zárhatják teljesen ki a szervezet IT szolgáltatásainak véletlenszerű vagy esetleg szándékosan okozott kiesését. Habár a teljes kiesés kockázata kicsi, de létezik, és utólag nem mentség, hogy a katasztrófa bekövetkezésének az esélye egy volt a millióhoz.

Egy ilyen esemény bekövetkezte utáni helyreállítás részletes és körültekintő tervezést igényel, és egyáltalában nem kicsi feladat. Egy eredményes helyreállítási terv igényli a különböző területek, részlegek, szolgáltatások és szolgáltatók együttműködését. A tervezés során figyelmen kívül hagyott elemek alááshatják az egész terv használhatóságát.

Ahogy az IT használatától való függőség egyre nő, egyre fontosabb, hogy a szolgáltatásokat egy előre megállapodott minőségben nyújtsák. Minden estben, amikor a szolgáltatás színvonala csökken, vagy éppenséggel nem áll rendelkezés, a felhasználók nem tudják elvégezni mindennapi munkájukat. Az IT-től való függőség trendje várhatóan marad, és egyre növekvő mértékben fogja befolyásolni a felhasználókat, a vezetést és az alapelvek alakítóit.

Ennélfogva fontos, hogy az IT rendszerek kiesésének hatásait értékeljük. A következmények változni fognak a költségek és az okozott kényelmetlenség tekintetében, attól függően hogy mekkora időre esik ki, illetve mennyire kritikus a szolgáltatás.

A katasztrófa elhárítási terv tartalmazza mindazokat az információkat, melyek szükségesek az IT szolgáltatások helyre állításához egy esetleges katasztrófa bekövetkezte után. A terv arra is világos útmutatást fog adni, hogy hogyan, és mikor kell használni.

2. A katasztrófák megelőzése

A katasztrófáknál a megelőzés szempontjából az elsődleges lépés, a veszélyforrások azonosítása és csoportosítása. Az esetlegesen bekövetkező károkra vonatkozóan kárértéki szinteket kell felállítani, amik általában a következő csoportokat foglalják magukba:

- jelentéktelen kár,
- csekély kár,
- közepes kár,
- nagy kár,
- kiemelkedően nagy kár

A katasztrófa-menedzsmentben veszélyforráson a biztonság ellen ható események bekövetkezésének lehetőségét értjük.

A veszélyforrások a következők lehetnek:

- természeti csapás
- szándékosság
- szoftver, hardver vagy rendszerhibák

A katasztrófa védelem két szinten jelenik meg egy szervezetben, egyrészt az **információvédelem,** másrészt a **működés megbízhatóság**ának területén. Ennek alapján 8 kiemelt terület van, amelyek a katasztrófák megelőzése szempontjából:

- Infrastrukturális védelem,
- Hardvervédelem,
- Szoftvervédelem,
- Adathordozók védelme,
- Adatok védelme,
- Dokumentumok védelme,
- Kommunikáció biztonságának biztosítása,
- Személyek biztonsága

3. Az infrastrukturális védelem

Az infrastrukturális védelem kiterjed a légkondicionálás, tűzvédelem, villám-, és sugárzásvédelem, valamint az elektromos áram okozta problémák kivédésére. Az IT infrastruktúra menedzsment tárgykörében **a hardver, szoftver, és az adathordozók védelme.**

Az információfeldolgozás biztonsága egy jó és tesztelt hardver és egy megbízható szoftver együttműködésén alapszik. A hardver részét alkotják a számítógép-hálózatok, a kábelezés, a számítógépek, az operációs rendszerek, az adatbázis-kezelő rendszerek, az irodaautomatizálás, és az alkalmazási csomagok.

4. Áramellátás

A Cég szerverszobájának és más irodahelyiségének (pl. könyvelés) zavartalan áramellátása kiemelten fontos a folyamatos üzemeltetés biztosítása érdekében. Ez a következő védelmi megoldások együttműködésével biztosított:

- szünetmentes energiaellátás,
- zárlati leoldásra szelektív áramkörök,
- villamos zavar, villám és túlfeszültség védelem.

A szünetmentes energiaellátást biztosító rendszer a Cég szerverszobájában Cover Energy NH S 20 UPS típusú akkumulátoros szünetmentes tápegység. Az üzemi táp kimaradása vagy csökkenése esetén a rendszer átkapcsol a szünetmentes tápra, amennyiben az üzemi táp ismét használható, akkor a rendszer visszatér rá.

A Cég minden munkaállomásain, munkaállomásonként egy-egy akkumulátoros szünetmentes áramforrás biztosítja a védelmet.

5. Légkondicionálás

Biztosított a szerverszoba épülettől független légkondicionálása. A védett szerverszoba üzemi hűtésigényének kiszolgálását klímaberendezés és szellőztető rendszer biztosítja.

A Cég összes irodahelyisége légkondicionáltak.

6. A belépés ellenőrzése

A cég összes irodái kulccsal zárhatók, így megakadályozva az illetéktelen behatolást.
A Cég munkaidőn kívül az illetéktelen behatolást jelző (riasztó) berendezéssel van ellátva.
A szerverszoba nappal is be van riasztózva, minden belépésnél használni kell a riasztó kioldását, kilépésnél kötelező ismét beriasztózni.

7. Hardvervédelem

7.1 A külső adathordozók beviteli/kiviteli felügyelete

A Cég felhasználói szigorúan csak a munkavégzéshez szükséges adathordozókat használhatják tárolási, adattovábbítási célra. Ezeket az adathordozókat a Cég informatikusának engedélyével használhatják. Amennyiben az adathordozó használata során vírusriasztást, hibás működést, a normál működéstől eltérő viselkedést tapasztalnak, azonnal értesíteni kötelesek a Cég informatikusát, távollét esetén közvetlen felettesét.

7.2 Folyamatos nyilvántartás a rendszerben található munkaállomásokról (hardver, softwer leltár)

A Cég informatikai rendszeréről naprakész leltárt vezet a szerver leltározó modulja. A leltárban megtalálható az egyes eszközök megnevezése, egyéb műszaki paraméterei. A leltár ismeretében az esetlegesen bekövetkezett katasztrófa esetén visszakereshetők az érintett informatikai eszközök.

7.3 Rendszeres megelőző karbantartás, pótalkatrészek készletezése

A Cég informatikai eszközein legalább félévente, átfogó megelőző karbantartást kell végezni.
A karbantartás során:

- az eszközök tisztítását, szükség esetén kompresszorral,
- a háttértárak karbantartását, telítettségének ellenőrzését,
- a cserére szoruló alkatrészek utánpótlását,
- az elavult hardverelemek cseréjét

kell végezni.

7.4 Alternatív cselekvési forgatókönyvek összeállítása a hardver kiesésekre vonatkozóan

A Cég informatikai rendszer működéséhez legnélkülözhetetlenebb elemeinek pótlásáról minél előbbi pótlásáról gondoskodni kell.

Ide tartozó eszközök:

- szerver számítógép,
- adatkommunikációs eszközök (router, switch)
- munkaállomások

A pótalkatrészek beszerzése a Cég informatikusának a feladata. Beszerzések előtt a Cég vezetőjének engedélyét is kérnie kell.

8. Szoftvervédelem, adathordozók védelme

A szoftverek és az adathordozók védelmében elsősorban a megelőzésre kell koncentrálni, cél a vírusfertőzések, külső behatolások megelőzése, az adathordozók esetében pedig a fizikai sérülések elkerülése.

A vírusfertőzések érdekében a Cég valamennyi számítógépét frissített vírusellenőrző rendszerrel kell ellátni.

9. Jelszóvédelem

9.1 Központi szerver gép

A központi szerver géphez, annak adataihoz közvetlenül csak az informatikus férhet hozzá. A szerveren tárolt adatokhoz a Felhasználók jogosultságuknak megfelelően férhetnek csak hozzá.

9.2 Munkaállomások

A felhasználók csak az irodájukban található saját munkájukhoz szükséges munkaállomásokat használhatják. Minden munkaállomás jelszavas védelem alatt áll. Minden Felhasználó csak a saját jelszavával férhet hozzá a rendszer erőforrásihoz.

9.3 Felhasználói programok

Minden felhasználói program használatához jelszavas védelem tartozik. A jelszavakat a Cég informatikusa adja, bármikor megváltoztathatja, törölheti, új felhasználót adhat az adott rendszerhez.

10. Biztonsági mentések

10.1 A rendszer mentési folyamatai

A szerver biztonsági okokból tükrözött winchesterekkel működik, ezen kívül az adatok mentése másodlagosan a BIX szerverközpont szerverére történik. A winchesterek a szerveren tárolt összes adatot mentik, beleértve a levelezési és felhasználási jogosultsági adatokat is. Az archiválásokat az egyes ügyintézők végzik. Az archiválás – az archiválni kívánt adatok fontossága alapján – naponta,

hetente, havonta történik. A napi, heti, havi és hosszú távú mentéseket külső adathordozókra írja.

- Havonta a napi, heti és havi mentéseket CD-re írja és a pénzügyi csoport páncélszekrényében egy elkülönített helyen tárolja zárt borítékban.
- A hosszú távú mentéseket (negyedéves, év végi zárások) szintén CD-re írja és a pénzügyi csoport páncélszekrényében egy elkülönített helyen tárolja, az egyes évek anyagait CD-re írja.

Az archiválás a következő adatokat érintik gyakoriságuk szerint:

Gyakoriság	Mentett adatok megnevezése
Napi	Pénzügyi osztály megosztott mappája, Könyvelés, számlázás
Heti	Számlázás Munkaügyi rendszer (IMI)
Hosszú távú	Év végi zárások, negyedéves beszámolók és a legutolsó napi-heti-havi mentés Ingatlanvagyon-leltár

A mentések adathordozóin fel kell tüntetni, hogy miről, mikor készült a mentés.

11. A rendszer védelme és hozzáférési szabályok

A Cég az archivált adatállományokat védi a módosítástól illetve biztosítja azt, hogy az adatállomány tartalmához jogosulatlan személyek ne férhessenek hozzá. Az archivált adatokhoz csak a Cég vezetője és informatikusa férhetnek hozzá.

12. Az informatikai katasztrófa elhárítás menete

12.1 A katasztrófa elhárításáért felelős személyek meghatározása

Cég vezetője (ügyvezető):
A Cég vezetője a katasztrófa elhárítás első számú vezetője.
Feladata:

- katasztrófa-állapot megállapítása,
- koordinálja a szükséges intézkedések menetét,
- betartja és betartatja a vonatkozó jogszabályokat,
- kapcsolatba lép a társszervekkel,
- személyi riasztások,
- a szolgáltató tevékenységek korlátozása, ideiglenes szüneteltetése

Informatikus:
Az informatikai rendszer mielőbbi visszaállításáért felelős személy, aki közvetlen kapcsolatban van a Cég vezetőjével.
Felel:

- az informatikai rendszer mielőbbi újratelepítéséért, újrakonfigurálásáért,
- a mentések helyreállításáért,
- javaslatot tesz a kieső eszközök pótlására.

A Cég vezetője által kijelölt szükséges résztvevők:
A Cég jogállású alkalmazottai, akiket a Cég vezetője jelöl ki a katasztrófa-elhárításban való részvételre. Számuk és feladatuk a katasztrófa ismeretében valósul meg.
Feladatuk:

- szállítás,
- koordinálás,
- információgyűjtés,
- tájékoztatás,
- üzemeltetési feltételek biztosítása,
- kárelhárítás,
- veszteségek számbavétele,
- extra szükséglétesítmények létrehozása.

13. Ideiglenes telephely kiválasztása, tartalékrendszerek kiépítése

Amennyiben a Cég informatikai infrastruktúrája olyan mértékben használhatatlanná válik, hogy a folyamatos és üzembiztos működés ne biztosított, a Cég vezetője jelöli ki az ideiglenes telephelyet. Amennyiben ez nem áll fenn, úgy a kieső rendszereket mielőbb pótolni kell.

A telephely kiválasztása után amennyiben marad az informatikai rendszerből felhasználható eszköz azt az informatikus irányításával azonnal az ideiglenes telephelyre kell szállítani, a szállításokért felelős személyek részvételével.

A tartalék telephelyre vonatkozó üzemeltetési feltételeket (villamos energia, telefon, …) a Cég vezetőjének irányításával a műszaki osztály munkatársai végzik.

Amennyiben az üzemeltetési feltételek fennállnak, az informatikai rendszer kiépítése történik meg. A felhasználható eszközök üzembeállítása után a cég munkavégzés legfontosabb munkafolyamatait kell először helyreállítani, (pl.: ügyféladatok, fejállomás vezérlés, számlázás) majd ezek után a kevésbé fontosakat. A helyreállítás során a biztonsági mentéseket kell felhasználni.

A nem felhasználható eszközökről leltárt kell készíteni és intézkedni pótlásukról. A beszerzést az informatikus a Cég vezetőjének engedélyével végzi.

A helyreállítás célja a tartalék telephelyen való legjobb szolgáltatási szint elérése. El kell kezdeni az elveszett vagy késleltetett tranzakciók ismételt bevitelét. A vezető, az irodavezetők, az informatikus, az alkalmazók és a végfelhasználók együtt munkálkodnak azon, hogy helyreállítsák a normál

feldolgozási rendet.
A biztonsági intézkedések szintje a végzett munka jellegétől függ. A felelős vezető feladata annak biztosítása, hogy a szükséges szintű biztonságot elérjék.

14. Visszatérés az eredeti telephelyre

A normál telephelyre történő visszatérés tervezése, a visszatérésig szükséges idő nagyban függ a károk mértékétől, a berendezések, a helyszínek és telekommunikációs vonalaknak az eredeti telephelyen történő helyreállításának időigényétől.

A normál állapot elérésének alappillérei:

- hardverrekonstrukció,
- szoftverrekonstrukció,
- adatrekonstrukció.

A normál állapothoz történő visszatérést engedélyező döntés része kell, legyen az eredeti gyakorlat felülvizsgálata, hogy az eredeti katasztrófa ismételt bekövetkeztét el lehessen kerülni. Megtörténik a tapasztalatok értékelése, hasonló esetek elkerülésére teendő intézkedések definiálása.