Abonyi
Polgármesteri Hivatal
Informatikai
Katasztrófa-elhárítási Terve

Érvényes: 2008. július 2-től
Aktualizálva: 2013. december 3.

Tartalom

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 bekövetkeztének 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 esetben, amikor a szolgáltatás színvonala csökken, vagy éppenséggel nem áll rendelkezésre, 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 a alapelvek alakítóit.

Ennél fogva 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.

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
- személy által kifejtett rombolás, vagy eltulajdonítás
- **rendszer szoftver, hardver, áram, vagy egyéb környezeti kiesés**

A katasztrófa védelem két szinten jelenik meg egy szervezetben, egyrészt az **információvédelem**, másrészt a **működés megbízhatóságának** 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

Az infrastrukturális védelem

Az infrastrukturális védelem kiterjed a légkondicionálás, tűzvédelem, villám-, víz-, 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, a szoftverekét pedig az ezeken futtatott operációs rendszerek, az adatbázis-kezelő rendszerek, és felhasználói célszoftverek.

Áramellátás

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

- szünetmentes energiaellátás,
- villamos zavar, villám és túlfeszültség védelem.

A szünetmentes energiaellátást biztosító rendszer a Hivatal szerverszobájában APC típusú lokális akkumulátoros szünetmentes tápegység, redundáns tápválasztó. Az üzemi táp kimaradása vagy csökkenése esetén a rendszer átkapcsol a tartalék tápra,vagy annak üzemidő kapacitásának végstádiumában automatikus leállást kezdeményez a központi egységek irányában. amennyiben üzemi táp ismét használható, akkor a rendszer automatikus visszakapcsol, vagy túl hosszú áramkimaradás esetén létrejött rendszerleállás esetében manuális úton van mód az újraindításra.

A Hivatal fontosabb munkaállomásain egyedi akkumulátoros szünetmentes áramforrás biztosítja a védelmet.

Légkondicionálás

A Hivatal irodahelységei közül csak az a Díszterem légkondicionált. A többi iroda a fekvéseik és az épület adottságai (vastag, homogén falak) miatt hűtést nem igényelnek, ezért nem légkondicionáltak.

Tűzmegelőzés és tűzvédelem

Tűz érzékelése esetén azonnal meg kell kezdeni a rendelkezésre álló poroltókkal az oltást és haladéktalanul értesíteni kell a tűzoltóságot.

A belépés ellenőrzése

Hivatali munkaidőben portaszolgálat működik, valamint az egyes irodák kulccsal zárhatók, így megakadályozva az illetéktelen behatolást.
A Hivatalon belül munkaidőn kívül az illetéktelen behatolást jelző (riasztó) berendezéssel van ellátva.

Hardvervédelem

A külső adathordozók beviteli/kiviteli felügyelete

A Hivatal felhasználói szigorúan csak a munkavégzéshez szükséges adathordozókat használhatják tárolási, adattovábbítási célra. Amennyiben az adathordozó használata során vírusriasztást, hibás működést, a normál működéstől eltérő viselkedést tapasztalnak, azonnal értesíteni kötelesek a LEADER Kft. informatikusát.

Folyamatos nyilvántartás a rendszer minden készülékéről, azok műszaki változásairól

A Hivatal informatikai rendszeréről (számítógépek, perifériák, hálózati elemek) naprakész leltárt kell vezetni. A leltárban megtalálható az egyes eszközök megnevezése, gyári száma, egyéb műszaki paraméterei. A leltár ismeretében az esetlegesen bekövetkezett katasztrófa esetén visszakereshetők az érintett informatikai eszközök.

Rendszeres megelőző karbantartás, pótalkatrészek készletezése

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

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

kell elvégezni.

Alternatív cselekvési forgatókönyvek összeállítása a hardver kiesésekre vonatkozóan

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

Ide tartozó eszközök:

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

A pótalkatrészek beszerzése a LEADER Kft. informatikusának a feladata. Beszerzések előtt a Hivatal vezetőjének engedélyét kell kérnie.

Szoftvervédelem, adathordozók védelme

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

Jelszóvédelem

Központi szerver gép

A központi szerver géphez, annak adataihoz közvetlenül csak a LEADER Kft. informatikusa férhet hozzá. A szerveren tárolt adatokhoz a Felhasználók jogosultságuknak megfelelően férhetnek csak hozzá. A Felhasználói jogosultságok nyilvántartása és karbantartása a kijelölt hivatali munkatárs feladata.

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 erőforrásaihoz.

Felhasználói programok

Minden felhasználói program használatához jelszavas védelem tartozik. A jelszavakat a LEADER Kft. informatikusa adja, a Hivatal vezetőjével történt egyeztetésnek megfelelően, bármikor megváltoztathatja, törölheti, új felhasználót adhat az adott rendszerhez.

Az archívum mentési folyamatai

Az archiválásokat az LEADER Kft. informatikusa végzi. Az archiválás - az archiválni kívánt adatok fontossága alapján - naponta, hetente, havonta történik. A napi, heti, havi és hosszú távú mentéseket egy különálló számítógépre, illetve egy külső adathordozóra (Mobil HDD) írja.

- a napi és heti mentéseket az informatikus a szerver szobában található mentésre kijelölt számítógépen tárolja, illetve a szerverteremtől elkülönítve elzártan tárolt Mobil HDD-n.
- a hosszú távú mentések (negyedéves, év végi zárások) szintén az előző pontban említettek szerint duplikáltan kerül mentésre.

Az archiválás a következő adatokat érintik gyakoriságuk szerint:

Gyakoriság	Mentett adatok megnevezése
napi	Pénzügyi osztály megosztott mappája, Könyvelés, felhasználói profilok a szerver gépről, Kimenő számlázás, Szociális igazgatás)
heti	Önkormányzati adók (ONKADO) Munkaügyi rendszer (IMI)
havi	Helyi népesség-nyilvántartás, Munkaidő-nyilvántartás, Ingatlanvagyon-kataszter, Minden felhasználó által hozzáférhető szerver-megosztás (osztályonkénti közös könyvtár, illetve privát könyvtárak)
hosszú távú	Év végi zárások, negyedéves beszámolók és a legutolsó napi-heti-havi mentés

Fizikailag elkülönítetten őrzött mentési példányok

A Mobil HDD-n tárolt mentéseket elkülönítve kell megőrizni olyan helyen ahol vagyon-, tűzbiztonsági követelmények teljesülnek. Ezekhez a mentésekhez csak a Hivatal vezetője és informatikusa férhet hozzá.

Az archívum védelme és hozzáférési szabályok

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

Az informatikai katasztrófa elhárítás menete

A katasztrófa elhárításáért felelős személyek meghatározása

Hivatal vezetője (jegyző):
A Hivatal 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 (LEADER Kft.):
Az informatikai rendszer mielőbbi visszaállításáért felelős személy, aki közvetlen kapcsolatban van a Hivatal vezetőjével.
Felel:

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

A Hivatal vezetője által kijelölt szükséges résztvevők:
A Hivatal közalkalmazotti vagy köztisztviselői jogállású alkalmazottai, akiket a Hivatal 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,

Ideiglenes telephely kiválasztása, tartalékrendszerek kiépítése

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

A telephelyválasztásnál elsődlegesen a helyben található, önkormányzathoz tartozó, működését erősen nem befolyásoló intézmények jöhetnek szóba.
Ilyen például:

- Abonyi Lajos Művelődési Ház, Könyvtár és Múzeumi Kiállítóhely (2740 Abony Báthory u. 2.)

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 Hivatal vezetőjének irányításával a Településfejlesztési Osztály munkatársai végzik.

Amennyiben az üzemeltetési feltételek fennállnak, az informatikai rendszer kiépítése történik meg. A felhasználható eszközök üzembeállítása után a hivatali munkavégzés legfontosabb munkafolyamatait kell először helyreállítani, (pl.: anyakönyvvezetés, lakcímváltozás-bejelentés, iktatás, kommunikáció, ...) majd ezek után a kevésbé fontosakat.

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

A helyreállítás célja a tartalék telephelyen való legjobb szolgáltatási szint elérése. El kell kezdeni az elvesztett vagy késleltetett tranzakciók ismételt bevitelét. A vezető, az osztályvezetők, a 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.

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.

Abony, 2013. december 3.

Jóváhagyta: Dr. Balogh Pál
Jegyző

Abony Város Jegyzője