# Komplexen az informatikai központok biztonságáról

***Cikkünkben az informatikai- és távközlési szolgáltatók, illetve a jelentős informatikai infrastruktúrával rendelkező szervezetek komplex biztonsági kihívásait elemezzük. Ez a komplexitás a technikai- és élőerős vagyonvédelem, az információvédelem és a biztonságszervezés területeit foglalja magába.***

A biztonság megvalósítása minden esetben a kockázatok és az üzleti igények alapján történik, az arányos védelemre törekedve. A cikkben egy nagyvállalat informatikai központjának védelmi intézkedéseit tekintjük át, amelyet a kisebb szervezetek saját igényeknek megfelelően tudnak átszabni. A konkrét megvalósításra vonatkozó javaslatot minden esetben gondos mérlegelés után a kockázatelemzés figyelembevételével szakértő terjeszti elő és a menedzsment hagyja jóvá azt.

Az épületek tervezésénél nagy figyelmet kell fordítani az építészeti biztonság kialakítására, úgy, hogy a számítógépterem egy belső épületben lehetőleg földszint alatt helyezkedjen el. Az épület tervezésekor biztonsági szempontból a lehetséges fizikai behatolási pontokat, a természetes illetve mesterséges vizek elleni védekezést, a kinti forgalom által keltett rezgést, valamint az elektromágneses sugárzás elleni árnyékolást kell számításba venni. Egyes esetekben robbanóanyagok, vegyi anyagok elleni védelemről is intézkedni kell.

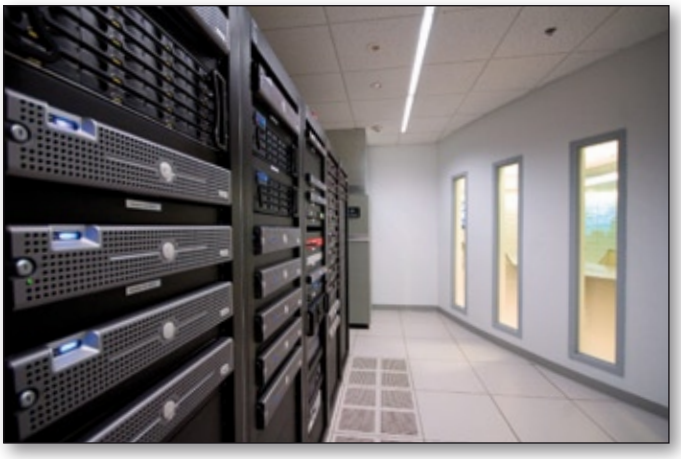
A cél, hogy maga az objektum körkörösen védhető legyen. Ekkor a megfelelő héjvédelemről és kültéri védelemről gondoskodni kell. Az elektromágneses sugárzás elleni védelem felszíni épületrészek esetén Faraday kalitkával történhet. A földszint alatti épületrészek esetében a vasbeton szerkezet önmagában elégségesnek tekinthető.

A gépterem egyik legfontosabb erőforrása a villamos energia, amelynek megfelelő ellátásáról, illetve a szükségellátásról több szinten kell gondoskodni. Az épület betáplálása lehetőleg két, egymástól független alállomásról történjen, megfelelő védelemmel ellátva. Az energiaellátás folyamatos biztosítása érdekében szünetmentes áramforrásokat kell alkalmazni, amelyek a rövidtávú kimaradásokat áthidalják. Hosszabb távra emellett dízelgenerátorok telepíthetők.

A környezeti jellemzők megfelelő szinten tartásának jelentősége nem lebecsülendő ezen a területen. A levegő hőmérséklete és páratartalma légkondicionáló berendezésekkel tartható megfelelő szinten, amelyek kialakításakor a redundanciát és a helyettesíthetőséget is szem előtt kell tartani. A légkondicionáló gépek lehetőleg párosával kerüljenek elhelyezésre, valamint előnyös, ha az egyes egységek kiesése esetén a szomszédos berendezés is el tudja látni a kiesett egység feladatát. A hosszú távú adattárolásnak és a levegő nedvességtartalmának a szoros kapcsolata nemcsak az online, hanem az offline (adathordozóra történő) mentések esetén is bizonyítható.

Az épületnél egyébként szokásos tűzvédelmi berendezések mellett a szervertermekre szigorúbb előírások vonatkoznak a minél gyorsabb oltás és a legkisebb anyagi kár elérésére. Az érzékelés szempontjából ma már bevált technika az aspirációs füstérzékelők telepítése, amely gyorsabban és nagyobb biztonsággal érzékeli a keletkező tüzet. Ez a szerverterembe telepített több szívócsonkból, központi légbeszívásból és egy analizáló berendezésből áll. Mivel ez a megoldás rendkívül költséges, ezért a pontszerű optikai füstérzékelés továbbra is elterjedtebb technika. Az oltásnál ma már alapvető követelmény az automatikus oltórendszer alkalmazása. Az oltás általában valamely inert gáz alkalmazásával történik, de voltak próbálkozások vízköddel oltó berendezés használatára is, amely viszont nem bizonyult megfelelőnek és komoly anyagi károkat okozott. A probléma oka az volt, hogy bár a tiszta víz nem villamos vezető, a szerverterem nem megfelelő tisztasága esetén a szálló por a vízködöt vezetővé változtatta.

A szervertermek őrzése a hagyományos objektumvédelmi feladatokhoz hasonló, viszont nagyobb a jelentősége a védett körletek kialakításának és a belépési jogosultságok szerepkörök alapján történő differenciálásának. Alapvető követelmény a központi jogosultságkezelés kétfaktoros azonosítással, például proximity kártyás és PIN kódos azonosítással. A jogok kiosztása célszerűen egy központi rendszerben történik, az adott munkatárs közvetlen felettesének, az üzleti folyamat felelősének, és a szerver üzemeltetési vagy biztonsági vezetőjének együttes jóváhagyásával. Az így kiosztott jogosultságok felülvizsgálata legalább évente esedékes a kiosztott jogosultságok és az engedélyek automatikus vagy manuális összehasonlításával együtt. Az eltérések okát minden esetben ki kell vizsgálni. Az objektumba történő belépések naplózására a hatályos adatvédelmi szabályozások szerint három napig van lehetőség, ezért szükséges az esetleges illegális behatolások, vagy jogosultság-túllépések felderítése ezen időszakon belül. A bizonyítékként felhasználható adatok tovább tárolhatóak a rendőrségi feljelentés vagy a fegyelmi eljárás lefolytatásáig. A biztonsági körletek kialakításakor érdemes a karbantartók és a logisztika által használt területeket fizikailag elválasztani az informatikai részektől. Célszerű továbbá, ha a szerverpark is több teremben kerül elhelyezésre funkcionális illetve biztonsági szempontok alapján. Szükséges a védett



körletek kamerás megfigyelése, kiemelten az átjárók és a munkavégzés során használt területek. Az itt készült felvételek megőrzésére szintén a három napos megőrzési határidő vonatkozik. A szervertermek lehetőleg ne rendelkezzenek ablakokkal illetve nem védett térbe nyíló ajtókkal. Ha mégis, ezek védelmére kitüntetett figyelmet kell fordítani, biztonsági rácsok, üvegtörésérzékelő és a védett oldalra telepített passzív infravörös érzékelők alkalmazásával.

Magában a védett térben szintén szükséges a passzív infravörös érzékelők használata. Az ajtók biztonsági okokból legyenek zsilip rendszerűek, életvédelmi okból viszont a szerverterem felőli ajtó kilinccsel nyitható legyen, vagy vésznyitó kulcs legyen elhelyezve az ajtó mellett. Ennek célja az oltógázzal történő elárasztás esetén az azonnali menekülés biztosítása. Életvédelmi okból szintén szükséges az oltógáz indítását blokkoló nyomógomb elhelyezése a védett helyiségen belül.

Az informatikai rendszer védelme bár külön szakterület tárgyát képezi, pár szót érdemel cikkünkben is. A hálózatot kívülről el kell választani az internettől, amely általában tűzfallal történik. Minden külső forgalomnak a tűzfalakon keresztül kell zajlania, titkosított protokollok alkalmazásával (pl. HTTPS, SFTP, SSH). A szervertermen belüli forgalom történhet titkosítás nélkül, amennyiben a hálózatból való kiszivárgás, illetve az illetéktelen hozzáférés kizárható. A szerverekre való belépés a szervertermekbe való belépéshez hasonlóan személyre kiosztott, és több szinten engedélyezett hozzáféréssel történhet. A szerverekre való sikertelen és sikeres belépéseket valamint különösen védendő rendszerek esetén minden tevékenységet naplózni kell, mely naplók védelmére szintén kiemelt figyelmet kell fordítani. A naplókat célszerű központi helyre gyűjteni (naplószerver), amelyhez csak a biztonsági osztály munkatársai férhetnek hozzá. A naplózási tevékenység a bizonyítékként való felhasználás és az illegális cselekmények felderítése kapcsán elengedhetetlen. A naplóállományokat a rendszer szokásos mentéséhez hasonlóan célszerű gyakran, például naponta elvégezni, és amennyiben a szervezetnek erre lehetősége van, a mentéseket másik telephelyen tárolni. Amennyiben a telephelyek közti forgalom elektronikusan történik, akkor az titkosítva illetve az átküldött és fogadott tartalmakat összehasonlítva kell elvégezni, valamint ha a szállítás fizikai módon történik, akkor az értékkíséréskor szokásos biztonsági eljárásokat kell követni.

A katasztrófahelyzetek, amelyek a szervezet infrastruktúráját szignifikáns mértékben károsítják, illetve használhatatlanná teszik, fontos rendszerek esetén kiemelt figyelmet és tervezést igényelnek. A tervezés alappillére a katasztrófa helyreállítási terv (Disaster Recovery Plan, DRP), amely a katasztrófahelyzet esetén szükséges szervezési és műszaki feladatokat tartalmazza a helyreállítás részletes leírásával. Ide tartozik a helyreállításra használható rendszerek beszerzésének, konfigurálásának sorrendje, az adatok helyreállításának módszere, illetve a megfelelő üzemeltető személyzet rendelkezésre bocsátása is. A katasztrófahelyzetek esetére lehetséges egy telephelyen kívüli, folyamatosan üzemben tartott és az élő rendszerrel megegyező tartalék rendszer használata, szintén telephelyen kívüli, de csak vészhelyzet esetén üzemelő rendszer használata. De akár a hardver forgalmazóval is lehet olyan szerződést kötni, amelyben a forgalmazó vállalja rövid időn belül a megfelelő hardver biztosítását. Gyakran elhanyagolt feladat a katasztrófatesztek végrehajtása, amely a terv működőképességét és alkalmazhatóságát hivatott ellenőrizni. Ekkor célszerű, de nem feltétlenül szükséges az éles rendszerek kikapcsolása, mivel ez a nem megfelelő tervek és intézkedések esetén szolgáltatáskieséssel járhat. Gyakrabban alkalmazott módszer inkább a terv lépéseinek a munkatársakkal történő begyakorlása a tesztrendszeren. A katasztrófatervezéshez kapcsolódó másik terv az üzletmenet folytonossági terv (Business Continuity Plan, BCP), amely viszont üzleti oldalról közelíti meg a problémát, az üzleti folyamatok működésének biztosítása szempontjából.

A fent leírt eljárások és módszerek iparági legjobb gyakorlatnak tekinthetők, azonban az azokkal szemben elvárt követelmények nagyban függnek az adott területtől. Például pénzügyi intézmények esetén a fent leírtaknál nem kevésbé szigorúan várja el a hatóság a biztonsági követelmények teljesítését, amíg mondjuk egy elektronikus hírközlési szolgáltatónál nem ilyen szigorúak a jogszabályi előírások. Egyéb, kevéssé szabályozott területen, mint például az elektronikus kereskedelemnél, vagy személyes adatok kezelésénél, feldolgozásánál még kevésbé követeli meg a jogalkotó a fenti módszerek alkalmazását. Ettől függetlenül, mint iparági legjobb gyakorlat, elvárható azok betartására való törekvés azért, hogy a szervezetek eleget tegyenek a tőlük elvárható védelem biztosításának. A szerző sok éves audit gyakorlata alapján a nagy üzemeltetők jó úton haladnak a teljes körű megvalósítás felé, amely mind a hatóság, mind az ügyfelek elégedettségével jár, így tényleges üzleti előnyhöz juttatja őket.

***Szádeczky Tamás***