IT biztonság és szerepe az információbiztonság területén

Tóth Georgina Nóra

Óbudai Egyetem
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Anyag és Gyártástechnológiai Intézet
1081 Budapest, Népszínház utca 8.
E-mail: toth.georgina@bgk.uni-obuda.hu

***Összefoglalás**: Manapság egy szervezet életében a legnagyobb érték az információ. Az információ tárolása, továbbítása egyre inkább informatikai eszközök segítségével történik. Az IT biztonság az információbiztonság egyik legdinamikusabban fejlődő területe. A különböző nemzetközi előírások, szabványok, próbálnak lépést tartani az újabb és újabb kihívásokkal. Az IT biztonság egy vállalat életében alapvető jelentőségű lehet, annak profiljától függően. Egy rosszindulatú támadás, károkozás akár a szervezet működének végét is jelentheti. Hasonlóan súlyos következményekkel járhat a véletlen károkozás is.*

***Kulcsszavak**: IT biztonság, információbiztonság. IT szabványok*

1. Bevezetés

A vállalatok életében egyre nagyobb szerepet töltenek be az információk, illetve az ezek tárolására, továbbítására, alkalmazására használt eszközök. Az üzleti életben az információk a vállalat sikerességének vagy bukásának a kulcsa. Ennek megfelelően egyre nagyobb hangsúlyt fektetnek a piaci szereplők információik védelmére. Ugyanakkor ma már az információkkal kapcsolatos veszélyforrások nem csupán fizikai jellegűek lehetnek, már nem elegendő korszerű vagyon-, objektum- és személyvédelmi eszközök bevetése. Újabb szintér jelent meg az információk védelmével kapcsolatban, a virtuális világ, számítógépes hálózatok. Egyre elterjedtebb a költségek csökkentése érdekében, a számítási felhők használata, amelyek esetén csak a felhasznált erőforrások mértékétől, a kihasználtság idejétől függ a bérleti díj. A havidíjas szolgáltatások csábítóak lehetnek, mivel a kisebb cégek beruházás nélkül juthatnak azokhoz a szoftverekhez, amelyek eddig csak a nagyvállalatok számára voltak elérhetőek. Utóbbiak pedig költségcsökkentési okokból térnek át egyre gyakrabban a számítási felhők használatára, hiszen így megtakaríthatják a saját szerver

fenntartási és az üzemeltetéshez szükséges munkaerő költségét. Információbiztonság szempontjából azonban nem elhanyagolható kérdés, hogy a vállalat számára fontos információk hol tárolódnak. Amennyiben egy másik országban, akkor ott milyen információbiztonsági előírások vonatkoznak rá.

Egyre több számítástechnikával, szoftverfejlesztéssel foglalkozó cég kezdett számítógép „farmok", számítási felhők létrehozásába. Az informatika világa abba az irányba halad a fejlett számítógépes hálózatoknak és az Internetnek köszönhetően, hogy minél inkább felhő technológiák szolgáltatásait használják mind a vállalatok, mind az egyéni felhasználók. Az információbiztonsággal kapcsolatos szabályozás, azonban az említett technológia esetében nem egységes és egyre sürgetőbb probléma. [1], [2], [10]

2. Információbiztonság és az IT biztonság kapcsolata

Az információbiztonság területe igen összetett, több tényező által befolyásolt. Egy jelentős és napjainkban egyre inkább előtérben lévő része az IT biztonság, amely speciálisan az informatikai eszközöké és az azokon tárolt, vagy általuk továbbított információk védelmét foglalja magába.

Az információk biztonságával kapcsolatban több szempontot is figyelembe kell venni illetve értékelni, legyen az elektronikus vagy papír alapú. Alapkövetelményként jelenik meg az információkkal kapcsolatban a rendelkezésre állás, integritás, és a bizalmasság. A vállalatok egy részének tevékenységi körükből adódóan elsődleges követelmény az üzleti folyamataihoz szükséges információk folyamatos elérhetősége. Bizonyos tevékenységek esetén akár egy pár órás kiesés a cég csődjét jelentheti. [4] Alapvetően az információkkal kapcsolatos követelmények teljesülésére helyezi a hangsúlyt. [2] Általánosságban megfogalmazható, hogy az információkkal kapcsolatban három biztonsági követelmény jelenik meg.

1. Bizalmasság
2. Sértetlenség
3. Rendelkezésre állás

A bizalmasság elve szerint csak azok férhetnek hozzá az információkhoz, akik jogosultak rá. A jogosultsági szintek meghatározása specifikusan történik. A sértetlenség elve azt jelenti, hogy az információnak naprakésznek, és konzisztensnek kell lennie. A fizikai sértetlenség mellett a logikai helyesség is követelmény. A rendelkezésre állás elve alapján az információnak minden időpillanatban rendelkezésre kell állnia, amikor arra szükség van. [3], [10]

3. IT szabványok, előírások

Több előírás született az informatikai eszközök védelmével kapcsolatban. Korábban az információbiztonság területén az előírások tekintetében nem volt egységes szabályozás. Születtek előírások, szabályozó dokumentumok különböző nemzetek esetében, amelyek különböző részletességűek, felépítések voltak. Azonban mindenki számára világossá vált, hogy szükséges egy egységes, nemzetközi szabályozásra. Ennek érdekében készítették el az „ISO/IEC 27001:2005 (MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények.) című szabványt, amely egységes nemzetközi szintű követelményeket tartalmaz információbiztonsági irányítási rendszerre vonatkozóan.

Néhány, az információ és IT biztonság területén alkalmazandó általános szabványok, előírások a következő felsorolásban láthatók:

- ISO 27000-es szabványcsalád (ISO 27001, ISO 27002)
- ITIL (BS 15000:2000)
- COBIT 4.0
- Common Criteria 2.1 (ISO/IEC 15408:1999)

[4],[5]

3.1. ISO 27000-es szabványcsalád (ISO 27001, ISO 27002)

Az ISO/IEC 27000-es szabványcsalád elkészítéséhez egy korábbi britt szabványt vettek alapul (BS 7799), amelynek frissebb, átdolgozott változatát készítették el. A szabványcsaládnak összesen hét tagja van, amelyek lefedik az információbiztonság irányítási rendszerrel kapcsolatos követelményeket, annak bevezetését, mérését, ellenőrzését valamint tanúsításával kapcsolatos információkat is. A szabványcsalád elemei a következők:

- ISO/IEC 27001:2005 - Az információbiztonsági irányítási rendszerre (ISMS) vonatkozó követelményekeket tartalmazó szabvány.
- ISO/IEC 27002:2007 - az ISO 17799:2005 gyakorlati útmutató az információbiztonság irányítási rendszer gyakorlati előírásainak, az ellenőrzési céloknak és a megvalósításra vonatkozó legjobb gyakorlati megoldásoknak (best practice), a szervezési, szabályozási szempontrendszerét tartalmazza.
- ISO/IEC 27003:2010 – Az ISO/IEC 27000 szabvány implementálásához szükséges tanácsokat és útmutatókat tartalmazza.

- ISO/IEC 27004:2009 – A szabvány az információbiztonság irányítási rendszere hatékonyságának mérési módszereit, az ellenőrzés lépéseit tartalmazza.
- ISO/IEC 27005:2008 – A szabvány tartalmazza az információbiztonsággal kapcsolatos kockázatkezelési eljárásokat.
- ISO/IEC 27006:2007 - Útmutató, amely az ISO/IEC 27001 szabványnak való megfelelést vizsgáló szervezetek számára tartalmazza mindazokat a követelményeket amelyeknek az auditáló szervezeteknek meg kell felelniük.
- ISO/IEC 27007 – Útmutató az információbiztonság irányítási rendszer auditáláshoz.
- ISO/IEC 27011:2008 - Útmutató a telekommunikáció információbiztonsági irányítási rendszeréhez.

[4], [5]

3.2. ITIL 2. (BS 15000:2000)

Az ITIL kifejlesztésének célja a jó minőségű IT szolgáltatások támogatása. Az informatikai szolgáltatások menedzselésére vonatkozóan tartalmazz a legjobb gyakorlatok átfogó gyűjteményét, lefedve a megvalósítás teljes életciklusát. Átfogó következetes dokumentáció.[4], [5]

3.3. COBIT 5

A COBIT (Control Objectives for Information and Related Technology) olyan nemzetközi szabvány, amelynek alapján az informatikai rendszerek fejlesztését lehet megvalósítani valamint biztonságossá tenni. A COBIT informatikai szabályozási célokat tartalmaz, amelyek általánosan alkalmazhatóak az információ biztonsági kérdéseivel kapcsolatban. Kialakításakor figyelembe vették a felsővezetés, a felhasználók, és a rendszer ellenőreinek szempontrendszerét egyaránt. [4],[5]

3.3. Common Criteria

A Common Criteria egységes követelményrendszert határoz meg, amelyekkel kapcsolatban a megvalósítás módját nem határozza meg. Az informatikai rendszerekre vonatkozóan megfogalmaz egy egységes módszertant. Több szinten definiálja az IT rendszerekkel kapcsolatos biztonsági követelményeket, amelyek alkalmazhatóak szoftverek és hardverek esetében is. Védelmi profilok definiálásával terméktől függetlenül kategorizálhatók a Common Criteria-ban definiált hét biztonsági szint szerint. [4], [5]

Az információbiztonságra vonatkozó ajánlások szabványok a legtöbb esetben bár hangsúlyozzák a kockázatelemzés fontosságát, azonban a módszer megválasztását a rendszer kialakítójára bízzák. [1], [7]

4. IT kockázatok

Nagyon leegyszerűsítve egy értelmezés szerint a kockázat valamely nemkívánatos esemény bekövetkezésének a valószínűsége. Valójában a kockázatelemzés, a kockázatértékelés e nem kívánatos esemény lehetséges bekövetkezésének vizsgálata. A vizsgálat történhet a viszonylag nagy számban bekövetkezett események, vagy a működés körülményeinek elemzésével vagy statisztikai módszerek, matematikai logika segítségével.

A kockázatelemzés eredményei alapján a vállalat ki tudja alakítani a stratégiáját. A kockázatelemzés elvégzéséhez a következő lépésekre van szükség:

- információs vagyontárgyak felmérése
- lehetséges veszélyforrások meghatározása
- kockázatbecslés (szempontok, skálák kialakítása)
- kockázatcsökkentési lehetőségek vizsgálata
- védelmi intézkedések kidolgozása / kockázatok csökkentése
- maradványkockázatok elfogadása

A kockázatok csökkentése érdekében többféle stratégiát is választhatunk a veszélyforrás megszüntetését, a bekövetkezési valószínűség csökkentését, okozott kár értékének a csökkentését, a kockázatok áthárítását illetve vállalhatunk tudatosan bizonyos kockázatokat (maradványkockázatok). Minden esetben mérlegelni szükséges az esetleges költségvonzatokat. [7], [8], [9], [10]

Következtetések / Összefoglaló

Az információbiztonság összetett, szerteágazó terület, amelynek csak egy igen fontos része az IT biztonság. Mai fejlett digitális világunk egyre több veszélyt rejteget legnagyobb kincsünkre, az információra nézve. A piaci vállalatok jelentős része fejlett informatikai infrastruktúrával rendelkezik, vagy ilyen jellegű szolgáltatásokat vesz igénybe. Az adatok, amelyeket az igénybevett rendszereken tárolódnak a cég fennmaradását jelenthetik. Célszerű egy jól átgondolt információbiztonsági irányítási rendszert létrehozni, amelynek segítségével felkészülhetünk az esetleges veszélyhelyzetekre, támadások, egy esetleges informatikai katasztrófára. Ennek megvalósítása érdekében több nemzetközi szabvány, szabályozó dokumentum is készült, azonban bizonyos területeken még nincs egységes szabályozás (Cloud computing). Abban minden dokumentum

megegyezik, hogy a hatékony információbiztonsági rendszer kialakítása érdekében szükség van egy részletes kockázatelemzés elvégzésére. A kockázatelemzés segítséget nyújt a gyenge pontok, a fenyegetések felismerésében. Önmagában nem oldja meg a problémát, azonban átgondolt védelmi intézkedések alapjául szolgálhat, így biztosítva az információval kapcsolatos követelmények teljesülését. Kockázatelemzés elvégzésére több módszer áll rendelkezésre, azonban ezeket a feladathoz körültekintően kell kiválasztani és alkalmazni. [10]

Irodalom

[1] Dr. Haig Zsolt: Az információbiztonság szabályozói és szervezetei keretei Robothadviselés 7 Tudományos Szakmai Konferencia (http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles7/haig_rw7.pdf) (2007. november 27.)

[2] Az adatvédelmet a Cloud Computing korszakhoz kell igazítani (http://www.sg.hu/cikkek/72178/az_adatvedelmet_a_cloud_computing_korszakhoz_kell_igazitani) (2010. január 29.)

[3] Dr. Muha Lajos: Infokommunikációs biztonsági stratégia hadmérnök IV. Évfolyam 1. szám - 2009. március

[4] Munk Sándor: Információbiztonság vs. informatikai biztonság, robothadviselés 7. tudományos szakmai konferencia 2007. november 27. (http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.html) (2010. február 13.)

[5] Dr. Muha Lajos: Az informatikai biztonság mérése (www.mtakpa.hu/kpa/download/1278547.pdf) (2010. október 9.)

[6] http://www.kurt.hu/szabvanyihatter/ (2010. október 9.)

[7] MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények.

[8] Symantec Corporation: IT Risk Management Report 2007, (http://www.symantec.com/enterprise/theme.jsp?themeid=itrisk_report), (2010.02.13.)

[9] Póserné Oláh Valéria: IT kockázatok, elemzésük, kezelésük, Hadmérnök, II. Évfolyam 3. szám - 2007. szeptember (http://www.zmne.hu/hadmernok/archivum/2007/3/2007_3_poserne.html)

[10] Tóth Georgina Nóra Információbiztonság és IT kockázatok XV. FMTÜ Nemzetközi Tudományos Konferencia, Kolozsvár 2010. március 25-26. ISSN 2067-6 808, pp. 329-332