XV. FIATAL MŰSZAKIAK TUDOMÁNYOS ÜLÉSSZAKA

Kolozsvár, 2010. március 25-26.

INFORMÁCIÓBIZTONSÁGI ÉS IT KOCKÁZATOK

TÓTH Georgina Nóra

Abstract

The information security has growing role in the everyday work of companies because of evolution of information equipments. The information security is a very complicated area and it can be analysed difficultly. The IT security one of the most important part of the information security. There are lot of risks in a company's information system not only the external effects for stole secure data but internal effects like data deletion by user or technical problems. The risk management and analysis is suitable for companies in order to decrease the effects of personal and technical problems.

Key words:

information security, IT security, risk analysis

Összefoglalás

Az információbiztonsági kérdések a számítástechnikai eszközök rohamos fejlődésével egyre nagyobb hangsúlyt kapnak a vállalatok életében, legyen az kicsi, közepes vagy nagy. Az információbiztonság rendkívül összetett terület és sok esetben nehezen elemezhető. Az egyik leglényegesebb része az IT biztonság. Amellett, hogy az egyes vállalatok informatikai eszközein tárolt adatokat védeni kell a külső, rosszindulatú támadások ellen, több olyan helyzetre is fel kell készülni, amely a belső munkatársak véletlen vagy akaratlagos károkozásából valamint egyéb szolgáltatások kimaradásából, meghibásodásából adódhat. Az egyes vállalatok számára létszükséglet megfelelő részletességű, megalapozott kockázatelemzés elvégzése és a különböző veszély helyzetekre való felkészüléshez intézkedési tervek készítése.

Kulcsszavak:

információbiztonság, IT biztonság, Kockázatelemzés

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. További problémát jelent, hogy megjelent egy új lehetőség a költségek csökkentése érdekében, a számítási felhők, 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 költségsökkentési 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], [3]

2. Információbiztonság és az IT biztonság kapcsolata

Az információbiztonság területe igen összetett, és sokrétű. 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.

1. ábra Az információbiztonság és az IT biztonság kapcsolata

Az információkkal kapcsolatban több követelménynek kell teljesülnie, legyen az elektronikus vagy papír alapú. Alapkövetelményként jelenik meg az információkkal kapcsolatban az 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. Az adatok integritása a naprakész, helyes információk elérését teszi lehetővé. A bizalmasság a jogosultságok kezelésével kapcsolatos követelményeket foglalja magába. Ennek megfelelően biztosítani szükséges, hogy bizonyos adatokhoz, csak azok férjenek, hozzá, akiknek feltétlenül szükséges, és folyamatos loggolást a műveletekkel kapcsolatban. [4]

Több előírás született az informatikai eszközök védelmével kapcsolatban. Eleinte 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.

Az információbiztonságra vonatkozó ajánlások szabványok a legtöbb esetben bár hangsúlyozzák a kockázatelemzés fontosságát, azonban a módszer megválasztását a rendszer kialakítójára bízzák. [1], [5]

3. 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.[5],[6],[7]

4. 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. Hatékony információbiztonsági rendszer kialakítása érdeké-

ben 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.

Irodalom

- [1] Dr. Haig Zsolt, *Az információbiztonság szabályozói és szervezeti keretei* Robothadviselés 7 Tudományos Szakmai Konferencia 2007. november 27.
(http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles7/haig_rw7.pdf)
- [2] *Az adatvédelmet a Cloud Computing korszakhoz kell igazítani* (2010. január 29.)
(http://www.sg.hu/cikkek/72178/az_adatvedelmet_a_cloud_computing_korszakhoz_kell_igazitani)
- [3] Molnár József, *Felhő törvényért lobbizik a Microsoft* (2010. január 21.)
(<http://nonstopuzlet.hu/felho-torvenyert-lobbizik-a-microsoft-20100121.html>)
- [4] Munk Sándor, *Információbiztonság vs. Informatikai*, Robothadviselés 7 Tudományos Szakmai Konferencia 2007. november 27.
(http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.html) (2010. február 13.)
- [5] MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények.
- [6] Symantec Corporation, *IT Risk Management Report 2007*,
(http://www.symantec.com/enterprise/theme.jsp?themeid=itrisk_report), 2010.02.13.
- [7] 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)

Tóth Georgina Nóra, tanársegéd, doktorandus

Munkahely: Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Anyag és Gyártástechnológiai Intézet

Cím: 1081, Magyarország, Budapest, Népszínház utca, 8.

Telefon / Fax: +36-1-6665339

E-mail: toth.georgina@bgk.uni-obuda.hu