JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

Dr. Vikman László

Az informatikai biztonság szabályozása a magyar jogban

Bevezető

Napjainkra szinte minden jelentősebb szervezet - legyen bár állami vagy piaci - működésében fontos szerepet játszik a különböző informatikai eszközök használata, üzemeltetése, akár főtevékenységként, akár működést segítő eszközeként. Ennek ellenére az alkalmazott informatikai eszközökkel, szoftverekkel, szervezeti megoldásokkal szemben támasztott biztonsági kritériumokkal átfogóan aránylag kevés magyar jogszabály foglalkozik. Uniós irányelv, vagy rendelet sem született még ezzel az igénnyel, annak ellenére, hogy az informatikai biztonsággal kapcsolatos felhasználói tudatosság növelését, az ezzel kapcsolatos legjobb gyakorlatok, és know-how terjesztését célul kitűző közösségi intézmény, az ENISA [1]2004 óta működik.

A domináns jogi szabályozás esélyeit az sem erősíti, hogy az informatikai biztonság területén a jogi szabályozás mellett ugyanolyan, ha nem fontosabb szerepet játszanak a nem kötelező érvényű iparági szabványok, szakmai ajánlások. Kevés olyan ipari szegmenst ismerünk, amelynek annyira sajátja lenne az innováció, ezt a jogalkotással foglalkozó szakembereknek is szem előtt kell tartaniuk. Abban mindenestre úgy tűnik egyeznek az álláspontok, hogy a technológia-független megközelítés a szerencsés, amely időtálló, versenysemleges, és nem akadályozza az innovációt.[2]

Részletszabályozást szűkebb területekre azonban már számos norma tartalmaz. Tanulmányunk célja az, hogy erről a meglehetősen töredezett jogterületről adjunk egy rövid áttekintést, ismertessük az informatikai biztonság megteremtését célzó, már létező jogintézményeket.[3]

Az első rész azokat az általános jogszabályi előírásokat foglalja össze, amelyek minden komolyabb (személyes) adatkezeléssel foglalkozó piaci szereplőre vonatkoznak. A lehető legteljesebb kép biztosítása érdekében röviden kitérünk az informatikával kapcsolatos büntetőjogi szabályozásra is. Ezt követően sorra vesszük és röviden elemezzük a gazdasági szférára vonatkozó különös szabályozást. Végül zárásként, a még inkább sokszínű közigazgatási szervezeteket érintő speciális rendelkezéseket foglaljuk össze egy táblázat segítségével.

Általános hatályú jogszabályok

Adatvédelmi törvény

Az egyre fejlődő infokommunikációs iparnak is köszönhetően már csaknem minden üzleti tevékenység velejárója a személyes adatok tömeges kezelése. Főként az utóbbi években elterjedt Customer Relationship Management rendszerek, illetve egyre szofisztikáltabb marketing- és vezetői döntéseket támogató szoftverek miatt szinte minden cég komoly hangsúlyt fektet arra, hogy a lehető legjobban megismerje az ügyfeleit, piacait, célközönségét, hogy ezen információk birtokában csökkenthesse piaci kockázatait egy új termék bevezetésénél, vagy növelhesse az értékesítés hatékonyságát.

Ezen tendenciák miatt az adatbiztonság tárgyalásakor nem hagyható figyelmen kívül az adatvédelmi szabályozás sem. A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló, 1992. évi LXIII. törvény hatálya a Magyar Köztársaság területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira vonatkozik, valamint amely közérdekű adatot vagy közérdekből nyilvános adatot tartalmaz.

Az adatbiztonság szempontjából azonban különösen a törvény 10. §-a tartalmaz fontos rendelkezéseket. Eszerint az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik.

Büntető anyagi jog

Az informatikai biztonság szabályozásának tárgyalásakor szintén megkerülhetetlen téma a terület büntetőjogi vonatkozásainak rövid ismertetése. Az adatvédelmi törvényben rögzített adatkezelői, adatfeldolgozói kötelezettségek megsértését, illetve a személyes adatokkal történő visszaélést bünteti a Btk. 177/A. §-ban foglalt tényállás, mely szerint aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével jogosulatlanul vagy a céltól eltérően személyes adatot kezel, az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget, az adatok biztonságát szolgáló intézkedést elmulasztja, és ezzel más vagy mások érdekeit jelentősen sérti, vétséget követ el. A Btk. súlyosító körülményként értékeli, ha a cselekményt hivatalos személyként, közmegbízatás felhasználásával, vagy jogtalan haszonszerzés végett követik el, vagy ha a személyes adattal visszaélést különleges személyes adatra (egészségügyi állapoti, faji, vallási hovatartozás, büntetett előélet, stb.) követik el.

Röviden említésre érdemes a Btk. 178/A. § által szabályozott magántitok jogosulatlan megismerése, a 300/C. § paragrafus által szabályozott számítástechnikai rendszer és adatok elleni bűncselekmény tényállása és említése méltó még a készpénz-helyettesítő fizetési eszközökkel kapcsolatos tényállási kör (313/B. §, 313/C. §, 313/D. §).

Büntető eljárásjog

Bár a büntetőeljárás szabályainak alkalmazására elsősorban a nyomozó hatóságok, az ügyészség, és a bíróságok kötelesek, mégis a büntetőeljárásról szóló, 1998. évi XIX. törvény (Be.) is tartalmaz néhány olyan speciális szabályt (az eljárás alá vont személyek jogain, illetve a törvényes garanciákon túl), melyet azon szervezeteknek, amelyeknek életében kulcsfontosságú szerepet játszik az információtechnológia fontos ismerniük. Kiemelten fontos egy speciális kényszerintézkedési típus, amelyet a jogalkotó a (jellemzően folyamatosan üzemelő) számítógépes közegben feltalálható bizonyítékok biztosítására alkotott meg. Ez a jogintézmény a számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés, melyet a Be. 158/A. §-a szabályoz.

A törvény szerint a megőrzésre kötelezés a bűncselekmény felderítése és a bizonyítás érdekében a számítástechnikai rendszer útján rögzített adat birtokosának, feldolgozójának, illetőleg kezelőjének a számítástechnikai rendszer útján rögzített meghatározott adat feletti rendelkezési jogának ideiglenes korlátozása. A bíróság, az ügyész, illetőleg a nyomozó hatóság elrendeli annak a számítástechnikai rendszer útján rögzített adatnak a megőrzését, amely bizonyítási eszköz, vagy bizonyítási eszköz felderítéséhez, a gyanúsított kilétének, tartózkodási helyének a megállapításához szükséges.

A számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés esetében az adatrögzítő eszköz a tulajdonosnál marad, nem kerül lefoglalás alá. Amennyiben azonban a büntetőeljárás sikere szempontjából szükséges, akkor lefoglalásra kerülhet sor, ami tehát szintén egy kényszerintézkedési forma, és szintén a büntetőeljárás során előkerült tárgyi bizonyítékok biztosítását teszi lehetővé. Mivel a lefoglalt dolog minősége, mennyisége, természete szerint meglehetősen sokféle lehet a büntetőeljárásokban, ezért néhány kiemelt bizonyítéktípus lefoglalására vonatkozóan a jogalkotó speciális szabályokat alkotott. Ezeket a szabályokat tartalmazza a lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának,

előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról szóló, 11/2003. (V. 8.) IM-BM-PM együttes rendelet.

A rendelet 67. §-a tartalmazza az elektronikus adattal kapcsolatos rendelkezéseket. Eszerint az elektronikus úton rögzített adatot a hatóság adathordozóra történő rögzítés (átmásolás) útján foglalja le, vagy a helyszínen lefoglalt adathordozóról az adatokat szakértő bevonásával menti le. A lefoglaláskor az átmásolás utólag meg nem változtatható adathordozóra történhet. Az átmásolást megelőzően a lefoglalás helyszínén ellenőrizni kell, hogy a hatóság által az átmásoláshoz biztosított adathordozó adatokat nem tartalmaz. A hatóságnak a jegyzőkönyvben a rögzítésre használt adathordozó típusát, gyártási számát, illetőleg a rajta tárolt adat jellegét és tartalmát fel kell tüntetnie.

Szabályozás a gazdasági szférában

Az általános érvényű szabályok áttekintését követően sorra vesszük azokat a már létező jogintézményeket, amelyeket a jogalkotó a – hangsúlyosan pénzügyi - piaci szereplők által üzemeltetett informatikai rendszerek biztonságát hivatottak megteremteni. Megfigyelhető ezek szabályozásában is egyfajta konvergencia, olyannyira, hogy a következő jogszabályok rendelkezései nagyrészt megegyeznek:

- 1993. évi XCVI. törvény, az Önkéntes Kölcsönös Biztosító Pénztárakról (40/C. §)
- 1996. évi CXII. törvény, a hitelintézetekről és a pénzügyi vállalkozásokról (Hpt. 13/B. §)
- 1997. évi LXXXII. törvény, a magánnyugdíjról és a magánnyugdíjpénztárakról (77/A. §)
- 2007. évi CXVII. törvény, a foglalkoztatói nyugdíjról és intézményeiről (18. §)
- 2007. évi CXXXVIII. törvény, a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól (12. §)

A jól azonosítható szabályozási tárgykörök ismertetését Hpt. vonatkozó szabályai segítségével végezzük el.[4]

Személyi és tárgyi feltételek

A pénzügyi szolgáltatási tevékenység csak a pénzügyi szolgáltatás nyújtásához szükséges, külön jogszabályban meghatározott személyi feltételek, a tevékenység végzésére alkalmas technikai, informatikai, műszaki, biztonsági felszereltség, helyiség, a működési kockázatok csökkentését szolgáló információs és ellenőrzési rendszer, valamint a rendkívüli helyzetek kezelésére vonatkozó terv, áttekinthető szervezeti felépítés megléte esetén kezdhető meg, illetve folytatható. [5]

A pénzügyi intézménynek belső szabályzatában meg kell határoznia az egyes munkakörök betöltéséhez szükséges informatikai ismeretet.[6]

A gyakorlatban a felhasználók képzése sajnos nem megoldás minden problémára, nyilván megvannak a korlátai. Egy átlagos felhasználót az informatika csupán mint a munkavégzés eszköze érdekli, ezt az attitűdöt figyelmen kívül hagyni komoly hiba lenne. Ezért a rendszer felépítésekor fontos olyan technikai környezetbe „helyezni", ahol bár alapvető biztonsági óvintézkedések megtételét elvárhatjuk tőle, mégis egy bizonyos technikai szint fölött már levesszük válláról ezt a terhet, és vagy megfelelő minőségű szoftver-hardver eszközök alkalmazásával, vagy folyamatos és magas szintű szakmai felügyelet biztosításával (ideális esetben e kettő kombinációjával) garantáljuk egy szervezet informatikai biztonságát.

Személyes adat feldolgozás kiszervezésének feltételei

A hitelintézet pénzügyi-, illetőleg kiegészítő pénzügyi szolgáltatási tevékenységéhez kapcsolódó, illetve jogszabály által végezni rendelt olyan tevékenységét, amelynek során adatkezelés, adatfeldolgozás vagy adattárolás valósul meg, az adatvédelmi előírások betartása mellett kiszervezheti. A kiszervezett tevékenységet végzőnek - a kockázattal arányos mértékben -

rendelkeznie kell mindazon személyi, tárgyi és biztonsági feltételekkel, melyeket jogszabály a kiszervezett tevékenységet illetően a hitelintézetre vonatkozóan előír.

A hitelintézet köteles a Felügyeletnek a kiszervezésről szóló szerződés aláírását követően két napon belül bejelenteni a kiszervezés tényét, a kiszervezett tevékenységet végző nevét, székhelyét vagy állandó lakcímét, a kiszervezés időtartamát. A kiszervezésre vonatkozó szerződésnek tartalmaznia kell az adatvédelemre vonatkozó előírások érvényesülésének bemutatását.[7]

Belső szabályozási rendszer

A pénzügyi intézménynek ki kell alakítania a pénzügyi, kiegészítő pénzügyi szolgáltatási tevékenységének ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét és gondoskodnia kell az informatikai rendszer kockázatokkal arányos védelméről. A szabályozási rendszerben ki kell térni az információtechnológiával szemben támasztott követelményekre, a használatából adódó biztonsági kockázatok felmérésére és kezelésére a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területén.[8]

Az informatika alkalmazásából fakadó biztonsági kockázatok figyelembevételével meg kell határozni a szervezeti és működési rendeket, a felelősségi, nyilvántartási és tájékoztatási szabályokat, a folyamatba épített ellenőrzési követelményeket és szabályokat.[9]

Biztonsági kockázatelemzés[10]

A pénzügyi intézmény köteles az informatikai rendszer biztonsági kockázatelemzését szükség szerint, de legalább kétévente felülvizsgálni és aktualizálni.[11]

Ennek a meglehetősen szűkszavú előírásnak a betartása nyilvánvalóan önmagában nem elégséges a gyakorlatban, de így bőségesen marad tér az adott szervezetre szabott megoldások kidolgozására. Általánosságban a szakirodalom a következő fontos lépéseket különíti el:

1. A védendő adatvagyon azonosítása
2. Rendszeres kockázatelemzések elvégzése a várható veszélyek, sebezhetőségek azonosítására
3. Ellenőrző rendszerek kifejlesztése és bevezetése, amelyek lehetővé teszik a kockázatok feletti ellenőrzést
4. A biztonsági rendszer folyamatos monitorozása, tesztelése
5. A tapasztalatoknak és változásoknak megfelelően a biztonsági rendszer folyamatos hozzáigazítása az új biztonsági kritériumokhoz
6. Külső szolgáltatók biztonsági szempontból releváns intézkedéseinek felügyelete[12]

Rendszerkövetelmények

A pénzügyi intézménynek ki kell dolgoznia az informatikai rendszerének biztonságos működtetését felügyelő informatikai ellenőrző rendszert és azt folyamatosan működtetnie kell.[13]

A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:

a) a rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosításáról,

b) az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról,

c) a rendszer szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációjáról (hozzáférési szintek, egyedi jogosultságok, engedélyezésük, felelősségi körök, hozzáférés naplózás, rendkívüli események),

d) olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza és alkalmas e naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, illetve lehetőséget nyújt a nem rendszeres események kezelésére,

e) a távadatátvitel bizalmasságáról, sértetlenségéről és hitelességéről,

f) az adathordozók szabályozott és biztonságos kezeléséről,

g) a rendszer biztonsági kockázattal arányos vírusvédelméről.[14]

A pénzügyi intézménynek tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez meg kell valósítania a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket és rendelkeznie kell legalább a következőkkel:

a) informatikai rendszerének működtetésére vonatkozó utasításokkal és előírásokkal, valamint a fejlesztésre vonatkozó tervekkel,

b) minden olyan dokumentációval, amely az üzleti tevékenységet közvetlenül vagy közvetve támogató informatikai rendszerek folyamatos és biztonságos működését - még a szállító, illetőleg a rendszerfejlesztő tevékenységének megszűnése után is – biztosítja,

c) a szolgáltatások ellátásához szükséges informatikai rendszerrel, valamint a szolgáltatások folytonosságát biztosító tartalék berendezésekkel, illetve e berendezések hiányában az ezeket helyettesítő egyéb - a tevékenységek, illetve szolgáltatások folytonosságát biztosító – megoldásokkal,

d) olyan informatikai rendszerrel, amely lehetővé teszi az alkalmazási környezet biztonságos elkülönítését a fejlesztési és tesztelési környezettől, valamint a megfelelő változáskövetés és változáskezelés fenntartását,

e) az informatikai rendszer szoftver elemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan biztonsági mentésekkel és mentési renddel (mentések típusa, módja, visszatöltési és helyreállítási tesztek, eljárási rend), amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik. Ezen mentéseket kockázati szempontból elkülönítetten és tűzbiztos módon kell tárolni, valamint gondoskodni kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről,

f) jogszabályban meghatározott nyilvántartás ismételt előhívására alkalmas adattároló rendszerrel, amely biztosítja, hogy az archivált anyagokat a jogszabályokban meghatározott ideig, de legalább öt évig, bármikor visszakereshetően, helyreállíthatóan megőrizzék,
g) a szolgáltatásai folyamatosságát akadályozó rendkívüli események kezelésére szolgáló tervvel.[15]

A pénzügyi intézménynél mindenkor rendelkezésre kell állnia:

a) az általa fejlesztett, megrendelésére készített informatikai rendszer felépítésének és működtetésének az ellenőrzéséhez szükséges rendszerleírásoknak és modelleknek,

b) az általa fejlesztett, megrendelésére készített informatikai rendszernél az adatok szintaktikai szabályainak, az adatok tárolási szerkezetének,

c) az informatikai rendszer elemeinek a pénzügyi intézmény által meghatározott biztonsági osztályokba sorolási rendszerének,

d) az adatokhoz történő hozzáférési rend meghatározásának,

e) az adatgazda és a rendszergazda kijelölését tartalmazó okiratnak,

f) az alkalmazott szoftver eszközök jogtisztaságát bizonyító szerződéseknek,

g) az informatikai rendszert alkotó ügyviteli, üzleti szoftvereszközök teljes körű és naprakész nyilvántartásának.[16]

A szoftvereknek együttesen alkalmasnak kell lenni legalább:

a) a működéshez szükséges és jogszabályban előírt adatok nyilvántartására,

b) a pénz és az értékpapírok biztonságos nyilvántartására,

c) a pénzügyi intézmény tevékenységével összefüggő országos informatikai rendszerekhez történő közvetlen vagy közvetett csatlakozásra,

d) a tárolt adatok ellenőrzéséhez való felhasználására,

e) a biztonsági kockázattal arányos logikai védelemre és a sérthetetlenség védelmére.[17]

Ez utóbbival kapcsolatban fontos megjegyezni, hogy a szoftverfejlesztés egyik legkomolyabb elvarratlan szála a szoftverekkel kapcsolatos szavatossági kérdések. Egyelőre jellemző a fejlesztők felelősségének teljes kizárása a szoftverrel kapcsolatban felmerült bármely üzemzavar, vagy káresemény kapcsán, azonban a jövőben – a szoftverfejlesztés menetének minőségbiztosításával, a kész termékek biztonsági szempontú ellenőrzésével – talán ezen a téren is várható előrelépés. Az mindenesetre bizonyos, hogy az üzletmenetüket potenciálisan megbénító, így akár komoly károkat is okozni képes üzemzavarok kapcsán egy helyreállító support tevékenységnél már egyre többet fognak elvárni a fejlesztők ügyfelei.

Egyedi szabályok

Természetesen nem csak közel megegyező tartalmú jogszabályok rendelkeznek az informatikai biztonság szabályozásáról, néhány érdekesebbet mindenképpen érdemes közülük kiemelni.

1. Hitelintézeti elszámolóházak

Az elszámolóházak informatikai biztonságát a jogalkotó részletesen kidolgozta, jó példa arra, hogy milyen lehet egy kiemelten fontos és kényes terület részletes szabályozása. Úgy véljük ilyen szintű, teljesen átfogó igényű feltételrendszerre minden informatikát alkalmazó gazdasági szereplő esetén nincs szükség, azonban néhány szabályozási elem átvétele mindenképpen megfontolandó. Ilyenek az egységes biztonságtechnikai terminológia és ennek értelmezése (pl. a Hpt-ben meghatározott kockázatelemzés pontos definiálása, minimális tartalmának meghatározása nem történt meg), a tűz- és fizikai védelem minimális szintjének rögzítése.

A hitelintézeti elszámolóházakra vonatkozóan két MNB rendelet tartalmaz részletes szabályokat. Elsőként az elszámolásforgalom lebonyolítására vonatkozó tárgyi, technikai, biztonsági és üzletmenet folytonossági követelményekről szóló 23/2005. (XI. 23.) MNB rendelet szabályait vesszük sorra. A Hpt. 3. §-a (2) bekezdésének b) pontja szerinti elszámolásforgalmi ügyletet a Magyar Köztársaság területén végző szervezetre (hitelintézeti elszámolóház) terjed ki, szabályait a Magyar Nemzeti Bankra, mint országos fizetési és elszámolási rendszert működtető szervezetre is megfelelően alkalmazni kell. A rendeletben foglalt követelmények teljesítése az elszámolásforgalmi tevékenység végzésének a feltétele. A rendeletben foglalt követelmények teljesítését az MNB felvigyázási és jegybanki ellenőrzési tevékenysége keretében ellenőrzi.

A rendelet részletesen kidolgozott biztonsági terminológiát alkalmaz:

a) akcióterv: a krízishelyzetre való felkészülési feltételeket, a krízishelyzetre vonatkozó válaszlépéseket, alternatív, illetve visszaállítási és ellenőrző eljárásokat tartalmazó, rendszeresen aktualizálandó terv;

b) biztonság: a hitelintézeti elszámolóház működésének zavartalan állapota, amelyben az elszámolásforgalmi tevékenység folyamatosan, korlátozásoktól mentesen végezhető;

c) biztonsági kockázat: a rendkívüli eseményekből eredő károk veszélye (mértéke a rendkívüli események bekövetkezési valószínűségének és a bekövetkezéskor várhatóan keletkező károk nagyságának függvénye);

d) biztonsági tevékenység: azon tervezési, szervezési, irányítási, végrehajtási és ellenőrzési feltételekről való intézményes gondoskodás, amely a hitelintézeti elszámolóház saját tulajdonú eszközeinek, más fontos értékeinek, érdekeinek, a munkavállalók személyi tulajdonának és személyes biztonságának védelmét, továbbá a hitelintézeti elszámolóház területén a rendkívüli események és krízishelyzetek megelőzését, illetve elhárítását szolgálják;

e) biztonságpolitika: azon elvek, követelmények, elvárások összessége, amelyek érvényesítését a hitelintézeti elszámolóház szükségesnek tartja a biztonság fenntartása érdekében;

f) elektronikai védelem: a biztonsági tevékenység végzését támogató elektronikus vagyonvédelmi rendszerek összessége;

g) elektronikus vagyonvédelmi rendszer: elektronikus jelző- vagy képi megfigyelőrendszer, illetve egyéb, jel és kép továbbítását lehetővé tevő, fény- és/vagy hangjelzést adó, belépési jogok automatizált kezelését biztosító elektronikus berendezések, műszaki megoldások összessége;

h) krízishelyzet: bekövetkezett rendkívüli esemény nyomán kialakult, a szokásos napi tevékenységtől eltérő, azonnali eljárást igénylő helyzet;

i) mechanikai-fizikai védelem: a hitelintézeti elszámolóház elhelyezésére szolgáló épület (épületrész), valamint a védendő helyiségek illetéktelen behatolás elleni fokozott védelmét, a védendő értékek biztonságos tárolásának kialakítását szolgáló építészeti-műszaki követelmények és eszközök;

j) rendkívüli esemény: mindazon emberi magatartások, természeti vagy technikai eredetű események, amelyek a hitelintézeti elszámolóház lényeges erőforrásainak, rendszereinek hibáját, károsodását, működésük megszűnését okozva fenyegetést jelenthetnek vagy jelentenek a hitelintézeti elszámolóház biztonságára, magukban hordozzák személyek életének, testi épségének vagy egészségének veszélyeztetését vagy vagyoni kár keletkezésének a lehetőségét, vagy amelyek következtében az életben, testi épségben vagy egészségben károsodás vagy vagyoni kár következik be;

k) üzletmenet folytonossági terv: a krízishelyzet kezelésére szolgáló akciótervek rendszere;

l) védendő helyiség: a hitelintézeti elszámolóház minden olyan helyisége, ahol az elszámolásforgalom lebonyolítását végző informatikai rendszer üzemel, továbbá minden olyan - a hitelintézeti elszámolóház által a titokvédelem szempontjából fontosnak minősített - helyiség, ahol üzleti vagy banktitkot, illetve személyes adatokat tartalmazó iratokat, adathordozókat tárolnak, vagy üzleti vagy banktitoknak minősülő, illetve személyes adatokat dolgoznak fel vagy kezelnek.

Az elszámolásforgalom lebonyolításának tárgyi, technikai feltételeiről a 3. § rendelkezik:

A hitelintézeti elszámolóház csak olyan épületben vagy épületrészben működhet,

a) amely a hitelintézeti elszámolóház saját tulajdonában áll, vagy
b) amelyet a hitelintézeti elszámolóház határozatlan időtartamú, a bérbeadót legalább egyéves felmondási idő biztosítására kötelező szerződéssel bérel.

Az elszámolásforgalmat lebonyolító informatikai rendszerek, valamint az elszámolásforgalom zavartalanságát biztosító egyéb eszközök folyamatos áramellátása érdekében a hitelintézeti elszámolóháznak tartalék áramforrással kell rendelkeznie.

Az elszámolásforgalom lebonyolításához szükséges üzenetközvetítés folyamatossága érdekében a hitelintézeti elszámolóháznak biztosítania kell

a) legalább két független távközlési csatorna rendelkezésre állását, ha a hitelintézeti elszámolóház áll szerződéses jogviszonyban a telekommunikációs szolgáltatókkal,
b) legalább két független csatlakozási lehetőséget, ha a távközlési szolgáltatás rendelkezésre állásáról a hitelintézeti elszámolóház ügyfelei gondoskodnak.

Az elszámolásforgalom lebonyolításának személyi biztonsági feltételeit a 4. § rögzíti:

Biztonsági szervezetet kell működtetni vagy biztonságért felelős személyt kell alkalmazni, kivéve, ha a biztonsági tevékenység teljes körének végzésére a vállalkozás keretében végzett személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól, a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamaráról szóló 1998. évi IV. törvény hatálya alá tartozó gazdasági társaságot, illetőleg egyéni vállalkozót bíz meg.

A biztonsági szervezet vezetőjévé az nevezhető ki vagy a biztonságáért felelős személy az lehet, aki

a) a hitelintézeti elszámolóházzal munkaviszonyban áll,
b) rendőrtiszti vagy katonai főiskolai vagy egyetemi végzettséggel, illetve egyéb egyetemi vagy főiskolai és felsőfokú biztonsági szakképesítést nyújtó végzettséggel, és
c) legalább hároméves biztonsági, védelmi területen szerzett vezetői gyakorlattal
rendelkezik.

A biztonsági szervezet vezetője végzi a biztonsági szervezet szakmai irányítását. A biztonsági szervezet vagy a biztonságért felelős személy feladatai a következők:

a) ellátja a biztonsági tevékenység körébe tartozó feladatokat,
b) végzi, illetőleg szervezi és felügyeli a munkavállalók támadás vagy egyéb vészhelyzet esetén követendő magatartására vonatkozó oktatást,
c) elemzéseket végez, és javaslatokat tesz a megfelelő védelmi intézkedésekre és a biztonsággal összefüggő szabályokra,
d) felelős a biztonságpolitika és a biztonsági szabályzat szakmai tartalmáért, aktualizálásáért,
e) ellenőrzi a biztonsági előírások végrehajtását.

A biztonsági szervezet vezetője vagy a biztonságért felelős személy a hitelintézeti elszámolóház első számú vezetőjének közvetlen irányítása alatt végzi tevékenységét.

Az elszámolóháznak a biztonság tárgyi feltételeit a tevékenységéhez kapcsolódó biztonsági kockázatok felmérése alapján, azokkal arányos módon és a vagyonbiztosításhoz szükséges követelmények figyelembevételével kell megteremtenie. A biztonsággal kapcsolatos minden információt, tényt, megoldást és adatot, ideértve a biztonság céljából megteremtett tárgyi, technikai feltételeket és ezek műszaki dokumentumait is, üzleti titokként kell kezelni. A biztonsági szabályzatban foglaltak szerint köteles gondoskodni az elhelyezésére szolgáló épület (épületrész) és védendő helyiségek mechanikai-fizikai védelméről. Az épületnek (épületrésznek), függetlenül attól, hogy az kizárólagos használatában áll-e, a külső határoló felületek tekintetében meg kell felelnie a Magyar Biztosítók Szövetsége (a továbbiakban: MABISZ) által közzétett „Betöréses lopás- és rablásbiztosítás technikai feltételei” című ajánlásban meghatározott részleges mechanikai-fizikai védelem követelményeinek. A védendő helyiségek határoló felületei minőségének meg kell felelnie az ajánlásban meghatározott teljes körű mechanikai-fizikai védelem követelményeinek.

A védendő helyiségeket a mechanikai-fizikai védelmen túlmenően elektronikai védelemmel is el kell látni. Elektronikus vagyonvédelmi rendszereket csak

a) a biztonsági szervezet vezetője, a biztonságért felelős személy, illetve a szervezeti és működési szabályzatban meghatározott személy által jóváhagyott terv alapján lehet telepíteni,
b) a külön jogszabályban előírt szakvizsgával rendelkező személy tervezhet, telepíthet és tarthat karban.

Az elektronikus vagyonvédelmi rendszerek programozásához és a kezelői jogosultság kiadásához szükséges kódoknak a biztonsági szervezet vezetőjénél, a biztonságért felelős személynél vagy az általuk írásban felhatalmazott személynél, illetve a szervezeti és működési szabályzatban meghatározott személynél rendelkezésre kell állnia, a biztonságos őrzés és a

hozzáférési jogosultság szabályozása mellett. Automatikus távjelzés továbbítására alkalmas összeköttetés kiépítéséről és folyamatos működtetéséről kell gondoskodni az elektronikus vagyonvédelmi rendszerek központja és valamely távfelügyeleti szolgáltatást nyújtó vagyonvédelmi társaság fogadó központja között.

A mechanikai-fizikai, illetve elektronikai védelem kialakítására csak az Európai Unióban elfogadott minősítő szervezet, vagy a MABISZ által kiadott biztonságtechnikai megfelelőségi tanúsítvánnyal rendelkező eszközöket lehet alkalmazni. Az elszámolóház kizárólagos használatában lévő épületben, illetve épületrészben üzemelő védendő helyiség mechanikai-fizikai és elektronikai védelmét be kell illeszteni az épület egészének, illetve az épületrésznek a védelmi rendszerébe.

A hitelintézeti elszámolóháznak

a) a működését biztosító, a napi teendők ellátásához már nem szükséges iratokat, adathordozókat (számítógépes programok biztonsági másolata, archivált adatok, biztonsági mentések stb.) zárható és legalább 30 perces tűzállóságú elkülönített helyiségben kell tárolnia,

b) az iratok és adathordozók egy másik példányát zárható és legalább 30 perces tűzállóságú, az a) pontban említettől különböző, elkülönített helyiségben kell őriznie.

Iratkezelési szabályzatban kell meghatározni azoknak az iratoknak és adathordozóknak a körét, amelyek tárolásáról és őrzéséről az (1) bekezdésben foglaltak szerint kell gondoskodnia.

A működés szempontjából stratégiai fontosságúnak minősített épületben, illetve épületrészben 24 órás őrszolgálatot kell biztosítani. Az őrszolgálatot ellátó személy szolgálati helyét a helyi adottságok és a biztonságpolitika alapján kell meghatározni. Gondoskodni kell arról, hogy az őrszolgálatot ellátó személy szükség esetén a tűzoltóságot távjelzéssel vagy távközlési vonalon keresztül, illetve a rendőrséget távközlési vonalon keresztül haladéktalanul értesíthesse. Ha az elszámolóház által stratégiai fontosságúnak minősített épületrész olyan épületben található, amely épület tulajdonosa vagy üzemeltetője az egész épületre vonatkozóan a rendeletben foglaltaknak megfelelően biztosítja az őrszolgálatot, akkor nem szükséges külön őrszolgálatról gondoskodni.

Olyan - a lehetséges, a biztonságot fenyegető rendkívüli eseményekben realizálódó biztonsági kockázatok teljes körének felmérésén és elemzésén alapuló - tesztelt üzletmenet folytonossági tervvel kell rendelkezni, amely az intézkedésre jogosult, felelős személyek megnevezésével részletes akcióterveket tartalmaz a rendkívüli esemény bekövetkeztekor a biztonság lehető leggyorsabb helyreállítására, illetve a folyamatos üzletmenet biztosításával az elszámolásforgalmi tevékenység krízishelyzetben történő folytatására. Az üzletmenet folytonossági tervben meg kell határozni, hogy az elszámolásforgalmi tevékenység krízishelyzetben történő folytatását biztosító erőforrások, rendszerek egészét, illetve egyes elemeit, illetőleg az üzletmenet folytonosságát szolgáló akcióterveket milyen tesztkörnyezetben és milyen gyakorisággal kell tesztelni, valamint hogy hogyan kell gondoskodni az akciótervek rendszeres, szabályozott keretek között folytatott aktualizálásáról.

Az elszámolásforgalmi tevékenység biztonságos végzése érdekében a hitelintézeti elszámolóháznak meg kell határoznia a biztonságpolitikáját és a biztonság feltételeire vonatkozó elveket. A biztonságpolitikája alapján, a biztonsági kockázatokat és azok változásait figyelembe vevő, részletes védelmi intézkedéseket tartalmazó biztonsági szabályzattal kell rendelkeznie. A biztonsági szabályzatnak a következőket kell tartalmaznia:

a) a biztonsági szervezet vagy a biztonságért felelős személy feladatai, hatásköre,
b) a biztonság tárgyi feltételeinek megvalósításához szükséges anyagok, eszközök, berendezések, eljárások, technika, az alkalmazandó műszaki specifikáció (ajánlás, szabvány, illetőleg műszaki engedély) feltüntetésével együtt, és a védelem formái szerinti csoportosításban,
c) a stratégiai fontosságúnak minősített épület (épületrészek) köre,
d) a védendő helyiségek köre,
e) a rendkívüli események kezelésének általános és speciális szabályai,
f) a munkavállalók számára meghatározott, a biztonságért való általános és speciális felelősségi rend,
g) a munkavállalókra vonatkozó személyi védelmi intézkedések, kiemelve a fokozott veszélynek kitett munkakörök (személyek) védelmét,

h) a munkavállalók biztonsági oktatásának rendje.

A hitelintézeti elszámolóházak üzletszabályzatára és szabályzataira vonatkozó követelményekről szóló 11/2006. (VIII. 1.) MNB rendelet hatálya szintén a Hpt. 3. §-a (2) bekezdésének b) pontja szerinti elszámolásforgalmi ügyletet a Magyar Köztársaság területén végző szervezetre terjed ki.

A rendelet alkalmazásában

- működési kockázat: annak a kockázata, hogy nem várt veszteség keletkezik a belső folyamatok, a használt informatikai rendszerek hibás vagy elégtelen volta, emberi magatartás, vagy az igazgatóság vagy a felügyelő bizottság vezetői és tagjai, vagy a vezető állású személyek által elkövetett hiba miatt;
- rendkívüli helyzet: olyan különleges eljárást igénylő helyzet, melynek során az elszámolásforgalom lebonyolításának folyamata az üzletszabályzatban foglaltaktól eltérő;

Az elszámolóház az elszámolásforgalom lebonyolítását szabályozó üzletszabályzatában többek közt meghatározza az elszámolási rendszerben az együttműködő felek által viselt kockázatokat. Az üzletszabályzatban meghatározza az elszámolási rendszerben az együttműködő felek által viselt pénzügyi és működési kockázatokat, és azok kezelésének eljárási rendjét. A rendkívüli helyzetek kezelésére vonatkozó szabályzatában meghatározza a rendkívüli helyzetek fajtáit, kritériumait és a rendkívüli helyzet megállapításának és kihirdetésének szabályait.

A rendkívüli helyzetek kezelésére vonatkozó szabályzatában a hitelintézeti elszámolóház rögzíti a rendkívüli helyzetek esetén

a) alkalmazandó eljárási rendet,
b) alkalmazandó döntési jogosultságokat,
c) az üzletszabályzatban lefektetett szabályoktól való eltérés lehetőségét,
d) a kapcsolattartás módját,
e) a kapcsolattartásra szolgáló központi telefonszámokat, illetve elérhetőségeket.

2. Biztosítók

Érdekes módon a biztosítókra eddig nem rögzítette a jogalkotó a pl. hitelintézeteknél, nyugdíjbiztosítóknál alkalmazott szabályozási rezsimet, sőt az informatikai védelemmel kapcsolatban kifejezetten csak a kiegészítő felügyelet alá tartozó biztosítók esetében rendelkezik. Álláspontunk szerint pedig legalább olyan fontos és védelmet igénylő adatkör a biztosítási titok, mint a banktitok.

A biztosítókról és a biztosítási tevékenységről szóló, 2003. évi LX. törvény szerint kiegészítő felügyelet alá tartozik a pénzügyi konglomerátum élén álló biztosító,

a) amely ellenőrző befolyással vagy részesedési viszonnyal rendelkezik szabályozott vállalkozásban, amelyek közül legalább egy hitelintézet vagy befektetési vállalkozás, vagy
b) amelynek anyavállalata az Európai Unió valamely tagállamában székhellyel rendelkező vegyes pénzügyi holding társaság, vagy
c) amely ellenőrző befolyással rendelkezik egy banki vagy befektetési szolgáltatási ágazatbeli vállalkozásban.

A kiegészítő felügyelet alá tartozó biztosító köteles gondoskodni a pénzügyi konglomerátum szintű belső kontroll rendszer és kockázatkezelés megfelelő működéséről. A kiegészítő felügyelet alá tartozó biztosítónak rendelkeznie kell a kiegészítő felügyelet érdekében szükséges adatok és információk szolgáltatására alkalmas információs rendszerrel, illetőleg azok megbízhatóságát biztosító informatikai és belső kontroll rendszerrel.

3. Elektronikus közbeszerzési szolgáltatások

A közbeszerzési eljárásokban elektronikusan gyakorolható eljárási cselekmények szabályairól, valamint az elektronikus árlejtés alkalmazásáról szóló 257/2007. (X. 4.) Korm. rendelet hatálya kiterjed a közbeszerzési eljárásokban és tervpályázati eljárásokban elektronikus

úton gyakorolt eljárási cselekményekre, az elektronikus árlejtésre, a Kbt. hatálya alá tartozó közbeszerzési eljárásokban részt vevő személyekre, szervezetekre, valamint a közbeszerzési eljárásban elektronikusan gyakorolható egyes eljárási cselekmények lebonyolításához informatikai támogatást nyújtó szolgáltatókra (a továbbiakban: szolgáltató).

Az elektronikus közbeszerzési szolgáltatások a következők:

a) a közbeszerzési eljárásokhoz kapcsolódó eljárási cselekmények valamelyikének vagy valamennyi eljárási cselekmény lebonyolításának informatikai támogatása, ideértve az elektronikus árlejtési szolgáltatást;
b) szállítók áruszállítására és szolgáltatásnyújtására, valamint építési beruházására vonatkozó adatokat és feltételeket tartalmazó elektronikus katalógusok kezeléséhez kapcsolódó szolgáltatás.

A szolgáltatásokat egyenként vagy azok közül bármelyiket együttesen is lehet nyújtani, az ajánlatkérő elektronikus eljárási cselekményt, elektronikus árlejtést szolgáltató igénybevételével a szolgáltató informatikai rendszerén vagy szolgáltató igénybevétele nélkül a saját informatikai rendszerén folytathat le. Amennyiben az ajánlatkérő saját informatikai rendszerén folytat le elektronikus eljárási cselekményt vagy elektronikus árlejtést, a szolgáltatóra vonatkozó rendelkezéseket saját magára nézve is alkalmaznia kell.

Elektronikus közbeszerzési szolgáltatást nyújthat az a természetes személy, jogi személy vagy jogi személyiséggel nem rendelkező gazdasági társaság, amely

a) rendelkezik külső, független rendszervizsgáló által folyamatosan ellenőrzött minőségirányítási és információbiztonsági irányítási rendszerrel;
b) tevékenysége ellátásához hivatalos közbeszerzési tanácsadót vagy közbeszerzési referenst vesz igénybe;
c) a közbeszerzések elektronikus támogatásában felhasznált informatikai rendszer (a továbbiakban: informatikai rendszer) üzemzavarával kapcsolatos telefonhívások fogadását e célra fenntartott hívószámon folyamatosan biztosítja;
d) saját honlapján közzéteszi
da) informatikai biztonsági szabályzatát,
db) az általa biztosított szolgáltatások részletes szabályairól szóló szabályzatát,
dc) általános szerződési feltételeit,
dd) a c) pont szerinti hívószámot.

Véleményünk szerint a fenti szabályozással természetében meglehetősen parallel néhány olyan információs társadalmi szolgáltatás, amely teljesen elterjedt, hétköznapi használatú, azonban az informatikai biztonság szempontjából speciális szabályozást nem alkottak rá. Ilyenek például a különböző aukciós szolgáltatások, online piacterek. Úgy gondoljuk, hogy a fogyasztói bizalom megteremtése, erősítése érdekében akár a piaci szereplők érdeke is lehet egy minimális biztonsági standard jogszabályi rögzítése.

Szabályozás a közigazgatásban

A közigazgatási szféra szabályozása a terület jellegéből adódóan még inkább sokszínűbb, mint a gazdasági szereplők esetében. Ez nyilvánvalóan adódik az egyes közigazgatási szervek eltérő feladatköréből, szervezeti felépítéséből is. Ezek eredményeként nagyon nehéz és tulajdonképpen fölösleges is lenne az uniformizált szabályozás. Mindemellett az e-kormányzás stratégiájának végrehajtása során az állami szervezetrendszerben is született néhány olyan jogszabály, amely a közigazgatás vertikumában is alkalmazandó.

A közigazgatásra vonatkozó informatikai biztonsági szabályozást nem kívántuk részletesebben ismertetni, de egy áttekintést – egy táblázat segítségével - erről is szeretnénk adni:

Témakör	Jogszabály
Elektronikus közigazgatás, elektronikus ügyintézés	195/2005. (IX. 22.) Korm. rendelet, az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról
	84/2007. (IV. 25.) Korm. rendelet, a Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről
	182/2007. (VII. 10.) Korm. rendelet, a központi elektronikus szolgáltató rendszerről
Katasztrófák és rendkívüli helyzetek	1999. évi LXXIV. törvény, a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről (74. §)
	100/2004. (IV. 27.) Korm. rendelet, az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról (3. §)
	131/2003. (VIII. 22.) Korm. rendelet, a nemzetgazdaság védelmi felkészítése és mozgósítása feladatai végrehajtásának szabályozásáról (12., 14. §)
	27/2004. (X. 6.) IHM rendelet, az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségeiről (10. §)
	24/2004. (VIII. 16.) IHM rendelet, a védelmi feladatokban részt vevő elektronikus hírközlési, illetve postai szolgáltatók kijelöléséről és felkészülési feladataik meghatározásáról (2. §, 1. és 2. számú melléklet)
Nemzetbiztonság	1995. évi LXV. törvény, az államtitokról és a szolgálati titokról (1. számú melléklet, Titokköri jegyzék: 16, 27)
	180/2004. (V. 26.) Korm. rendelet, az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről
	86/1996. (VI. 14.) Korm. rendelet, a biztonsági okmányok védelmének rendjéről (5., 6., 12. §)
Közfeladatot ellátó szervek iratkezelése	335/2005. (XII. 29.) Korm. rendelet, a közfeladatot ellátó szervek iratkezelésének általános követelményeiről (1., 5., 18., 25., 67/C. §)
Központosított közbeszerzés	168/2004. (V. 25.) Korm. rendelet, a központosított közbeszerzési rendszerről,

	valamint a központi beszerző szervezet feladat- és hatásköréről (25. §)
Egészségbiztosítási pénztárak	2008. évi I. törvény, az egészségbiztosítási pénztárakról (28. §)
Állami ellenőrzéshez biztosított jogosultságok	1992. évi XXXVIII. törvény, az államháztartásról (121/A. §)
	1989. évi XXXVIII. törvény, az Állami Számvevőszékről (21. §)
EDR, egységes digitális rádió-távközlő rendszer	109/2007. (V. 15.) Korm. rendelet, az egységes digitális rádió-távközlő rendszerről (2. számú melléklet 3.)
Ingatlan-nyilvántartás	207/2006. (X. 16.) Korm. rendelet, a számítógépes ingatlan-nyilvántartási rendszerből történő szolgáltatás feltételeit tartalmazó szolgáltatási szerződés kötelező elemeiről (5. §)
Felsőoktatás	79/2006. (IV. 5.) Korm. rendelet, a felsőoktatásról szóló 2005. évi CXXXIX. törvény egyes rendelkezéseinek végrehajtásáról (6-7. §)

[1] European Network and Information Security Agency - Európai Hálózat- és Információbiztonsági Ügynökség, a 460/2004/EK rendelet hozta létre, http://enisa.europa.eu/
[2] Az informatikai biztonság szabályozásának elméleti hátterének összefoglalásáról, a generális illetve technológia-specifikus szabályozás dilemmájáról lásd: Rátai Balázs: Nature and Future of IT-Security Regulation, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=905856 [2009.01.31.]
[3] Az USA szövetségi informatikai biztonsági szabályozásának összefoglalását, némi nemzetközi kitekintéssel tartalmazza a következő tanulmány: Smedinghoff , Thomas J.: The State of Information Security Law: A Focus on the Key Legal Trends, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1114246 [2009.01.31.]
[4] A Hpt. elemzett rendelkezései 2004. május 6-tól kerültek a törvénybe, de fokozatosan terjesztették ki a hatályát az egyes pénzügyi szolgáltatók típusaira. Az USA-ban 2002-ben megalkotott hasonló tárgyú jogszabály hatásairól, alkalmazásának tapasztalatairól szóló összefoglalót lásd: Gordon, Lawrence A., Loeb , Martin P., Lucyshyn , William, Sohail, Tashfeen: The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=995205 [2009.01.31.]
[5] Hpt. 13. § (1) c) d) f) g) pont
[6] Hpt. 13/B. § (9) bekezdés
[7] Hpt. 13/A. § (1), (2), (3), (4) a) pont
[8] Hpt. 13/B § (1) bekezdés
[9] Hpt. 13/B. § (3) bekezdés
[10] A biztonsági kockázatok közgazdasági megközelítése, elemzése is lehetséges, lásd részletesen: Munteanu, Adrian: Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=917767 [2009.01.31.]
[11] Hpt. 13/B. § (2) bekezdés
[12] Smedinghoff, p. 20.
[13] Hpt. 13/B. § (4) bekezdés
[14] Hpt. 13/B. § (5) bekezdés
[15] Hpt. 13/B. § (6) bekezdés
[16] Hpt. 13/B. § (7) bekezdés
[17] Hpt. 13/B. § (8) bekezdés