HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Inkovics Ferenc
ferenc.inkovics@gmail.com

A KÜLÜGYMINISZTÉRIUM ÉS AZ INFORMATIKAI BIZTONSÁG

Absztrakt

Informatikai rendszerekkel szinte minden nap találkozunk. Az elmúlt évtizedekben életünk része lett számos informatikai rendszer. A biztonság fogalma alatt ma már nem érthetjük csak a fizikai biztonságunkat. Most már az információs tárdalom tagjai vagyunk. Tudnunk kell, mit jelent az informatikai biztonság. Jelen publikáció röviden ismerteti az informatikai biztonsággal kapcsolatos alapfogalmakat és néhány főbb informatikai biztonságot fenyegető tényezőt. Bemutatja a témához kapcsolódó főbb jogszabályokat, szabványokat és ajánlásokat. És legvégül számba veszi a Külügyminisztériumban használt nemzeti informatikai rendszereket és az Európai Unió informatikai rendszerei közül azokat, melyeket a Külügyminisztérium kollégái használnak.

We meet information systems nearly every day. During the past decades numerous information systems have become the part of our lives. Today we can't already mean only our physical security on the concept of security. Now we are a member of the information society. We have to know what the information security means. This publication reports about the basic concepts of information security and some main factors which threaten the information security. It presents the laws, standards and recommendations connecting to this topic. And finally it enumerates national information systems used in the Ministry for Foreign Affairs (MFA) and those information systems of the EU that are used by the colleagues of the MFA.

Kulcsszavak: *Informatikai Biztonság, Információ biztonság, Külügyminisztérium ~ Information Security, Ministry of Foreign Affaires*

Bevezetés

Az információ megszerzése és védelme egészen az ősközösségig visszanyúlik. E tevékenységek, melyek szinte egyidősek az emberi társadalommal folyamatosan fejlődtek és fejlődnek ma is. A számítógép megjelenése és a számítógépes hálózatok kialakítása robbanásszerű fejlődést idézett elő az információtechnikában. Rengeteget változott mind a védendő információ, mind az információ védelem módja is. Régebben az elég volt az, hogy az információt csak kevés megbízható személlyel osztották meg és védett helyre zárták. Ma azonban már nem elegendő a hagyományos módszerekkel való védelem. Az információ gyűjtését, feldolgozását, kezelését és tárolását új alapokra kellett helyezni. A technika új vívmányait már eleve úgy kell kialakítani, hogy azok képesek legyenek megfelelő védelmet nyújtani az információnak. [1]

Tisztázandó fogalmak

Az információ szerves része lett életünknek, ezért nap, mint nap találkozunk, olyan folyamatokkal, melyek az információkat védik meg a nem engedélyezett hozzáféréstől, a használattól, a kiszivárogtatástól, a megsemmisítéstől, a módosítástól és a megzavarástól. Ezen folyamatok összessége az *információ védelem*. Nem szabad összekeverni az informatikai védelemmel, ami ennek csak egy részhalmaza [2].

A félreértések elkerülése érdekében szükséges tisztázni mit is jelent ez a részhalmaz pontosan. Az *informatikai védelem* [3] az humán, technikai (környezeti, fizikai, logikai) és jogi védelmi intézkedések összessége, az informatikai biztonság (mint megkívánt állapot) megteremtésére és fenntartására. Ezen intézkedéseket az olyan tényezők ellen hozzák, amik fenyegetik:

- az informatikai rendszerben tárolt, kezelt, rendszerezett és továbbított adatot (információt),
- az informatikai szolgáltatásokat,
- és a mindezeket biztosító informatikai rendszereket.

Látható, hogy az előző 2 fogalom mindegyike 1-1 állapot elérésére irányuló tevékenységek összessége. Az információ védelem az információbiztonságra, az informatikai védelem pedig az informatikai biztonságra törekszik. Mindezek mellett szükséges tisztázni ezt a két fogalmat is melyek nem tevékenységet, hanem állapotokat tükröznek. Míg az *Információ biztonság* az információvédelem az általános védelmi rendszabályok és eljárások alkalmazása, az információ megsemmisülésének vagy kompromittálódásának megelőzése, felfedése ellen és helyreállítása céljából [2], addig az *informatikai biztonság* a védelmi rendszer olyan, a védő számára kielégítő mértékű állapota, amely az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos [4].

Sajnos összekavarodást okozhat az, hogy az információ védelem és informatikai védelem általános angol megfelelője egyforma: information security; és csak a szövegkörnyezet teszi egyértelművé azt, hogy mit is takar [5].

Az informatikai biztonság szükségessége, létjogosultsága

Az információ, az informatika és kommunikáció a mindennapi életünk aktív szereplője. Az informatikai, információs és kommunikációs rendszereket már nem eszközként, hanem erőforrásként hasznosítják az államok és a vállalatok is. Fontosságuk miatt, ezeknek a rendszereknek a védelme századunk központi kérdése lett [6]. Egyre „többet tudó”, bonyolultabb és nagyobb kiterjedésű informatikai rendszereket alkot az emberiség. A legtöbb

irodai munkakör elengedhetetlen része lett a számítástechnika, mert az intézmények, a vállalatok és vállalkozások tevékenységét egyre nagyobb mértékben támogatják informatikai alkalmazásokkal. Az informatikai rendszerek életünkben betöltött funkciójának növekedésével párhuzamosan az informatikai biztonság szerepe és jelentősége egyre nagyobb jelentőséggel bír.

Az alkalmazott információs és informatikai rendszerek állapota, rendelkezésre állása, működése közvetlenül befolyásolja nagytömegű embercsoportok közvetlen életét, munkáját, társadalmi termelőképességét. Mindezek miatt az információs és informatikai rendszerek ellen mért csapások hatása összemérhető a tömegpusztító fegyverekkel mért csapásokkal. Az elmúlt évtizedekben kialakult és megjelent új fenyegetések, mint pl.: hackerek, crackerek, informatikai hadviselés, adatlopás és kiberterrorizmus miatt egyre nagyobb jelentősége van az informatikai és információ biztonságnak is. Mindezek hátterében az áll, hogy az információ az egyben érték, vagyon és hatalom is.

Kihívások az informatikai biztonság területén

A különböző informatikai rendszereknek számos forrásból eredő fenyegetéssel kell szembe nézniük, melyek bekövetkezésükkor jelentős anyagi és erkölcsi károkat is okozhatnak. Ahhoz, hogy megfelelően fel lehessen készülni a fenyegetések kivédésére, elkerülésére, azok károinak minél hatékonyabb enyhítésére, szükséges, hogy már az informatikai rendszerek tervezésénél figyelembe legyenek ezek véve. Informatikai rendszerek biztonságát az alábbi tényezők fenyegethetik:

a. kiberterrorizmus,
b. információs műveletek (információs hadviselés),
c. gazdasági hírszerzés,
d. ipari kémkedés,
e. számítógépes csalás
f. hackerek, crackerek,
g. rosszindulatú, bosszúálló munkatársak,
h. szabotázs,
i. vandalizmus
j. képzetlen, hanyag, felelőtlen munkatársak,
k. természeti csapások (pl.: tűzkár, árvíz, földrengés, stb.),
l. műszaki hibák,
m. elektronikus dokumentumok bizalmasságának vagy hitelességének sérülése
n. támadás rosszindulatú programokkal
o. szolgáltatás igénybevételének letagadása
p. web lapok tartalmának illegális megváltoztatása
q. adatlopás „védett” szerverekről
r. szolgáltatások megbénítása terheléses támadással (Denial of Service, DoS)
s. stb.

A különböző fenyegetések előfordulási gyakorisága eltérő, de egyes rosszindulatú támadások és szándékos károkozások, mint pl.: elektronikus azonosítók és személyes adatok lopása - adathalászat; vírusok, trójai programok terjesztése; stb. szinte mindennapossá váltak. Az informatikában is mindig a védekezés van hátrányban a fenyegetésekkel szemben. A támadók haladva a korral mindig újabb és újabb fenyegetéseket találnak ki és folyamatosan fejlesztik a módszereiket is. Egyre komplikáltabb megoldásokat és egyre bátrabban alkalmaznak, ezzel is folyamatosan nehezítve az informatikai biztonság fenntartását.

A fenyegetések ellen lehet és szükséges is védekezni. Az informatikai biztonság eléréséhez az informatikai védelemnek két fajtája terjedt el: a reaktív és a proaktív védekezés. A lényegi

különbség a kettő között az, hogy míg a reaktív védekezés a már bekövetkezett károkat enyhíti, és a proaktív védekezés során pedig megpróbálunk felkészülni a leendő támadások és fenyegetések káros hatásaira is, ezért a bekövetkezett káresemény által okozott költségek és egyéb károk és hatásaik minimalizálódnak. A proaktív védekezés ugyanakkor jóval költségesebb is lehet és akár sokkal több erőforrás bevonását is szükségessé teszi. Azt mindig mérlegelni kell, hogy adott esetben mekkora védelmi erőforrás ráfordítás éri meg. Ezt az alkalmazott biztonságpolitika határozza meg.

Jogszabályok

Az informatikai biztonság témakörét illetően is több csoportba oszthatóak az alkalmazandó jogszabályok, szabályzók. Az alábbi fontosabb jogszabályokat és szabályzókat különítjük el:

- Minősített adat kezelésére,
- Az üzleti titokra,
- Banktitokra és értékpapírokra,
- Adatvédelemre,
- Elektronikus aláírásra és
- E-közigazgatásra vonatkozóak

Az Országgyűlés 2009. december 14-én fogadta el a minősített adat védelméről szóló 2009. évi CLV. törvényt (Mavtv.), amely az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény, valamint a Nemzeti Biztonsági Felügyeletről szóló 1998. évi LXXXV. törvény helyébe lépett. A 2010. április 1-jén hatályba lépett jogszabály alapjaiban kodifikálja újra a minősített adatok védelmének magyarországi struktúráját. Megteremti a minősített adatok védelmének egységes jogszabály- és intézményrendszerét, s egyúttal eleget tesz legfontosabb jogharmonizációs kötelezettségeinknek. Lényegi változás, hogy a törvény mind a nemzeti, mind a külföldi minősített adatok védelmére egységes követelményeket határoz meg.

Egyes információk titokban tartása mögött indokolt állami vagy magánérdek áll, a különböző típusú titkokat ezért szükséges védeni. A magyar jogszabályok meghatározzák a különböző titok fogalmait, és azok kezelési mikéntjét is. A minősített adatok olyan titkok, melyeknél a titoksértést a magyar büntetőjogi törvények szerint büntetni kell. Titkoknak minősülnek az üzleti titkok is, melyet szintén védenek a magyar jogszabályok. A gazdasági társaságok számára létfontosságú, hogy az üzleti információk ne kerüljenek illetéktelen kezekbe. Az a gazdasági társaság, akinek a pénzügyi, gazdasági, termelési információi esetleg jövőbeni tervei idő előtt ismerté válnak a piac többi szereplői előtt, rendkívül kedvezőtlen helyzetbe kerülhet. Ugyanakkor nem szabad megfeledkezni arról, hogy az üzleti titoknak nem minősülő adatokról tájékoztatást kell adni, mert azok viszont közérdekűek. Magyarországon a gazdasági verseny tisztaságát és szabadságát az 1996. évi LVII. törvény szavatolja. Ez a törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szól [7][8].

Az üzleti titok fogalmát a Ptk. 81. § (2) bekezdése tartalmazza. Az üzleti titok azonban nem fed le minden szükséges titok területet. Miként győződhetünk meg arról, hogy a bank kiknek és milyen módon ad tájékoztatást az általa kezelt bizalmas adatainkról, amik üzletileg igen értékesek. De hasonló gondolatok támadhatnak bennünk azon pénzintézetek esetében is, akik az értékpapírjainkat kezelik. Ezt az űrt oldják fel az alábbi törvények:

- 1996. évi CXI. törvény az értékpapírok forgalomba hozataláról, a befektetési szolgáltatásokról és az értékpapír tőzsdéről,
- 1996. évi CXII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról, és a
- 2001. évi CXX. törvény a tőkepiacról.

E három törvényben meghatározásra kerül a banktitok (1996. évi CXI. törvényben) és az értékpapírtitok (2001. évi CXX. törvényben), valamint azoknak a felhasználhatósági köre is,

tehát hogy kinek és milyen módon adható át, valamint mikor és miként használhatóak fel ezek az adatok [1][9].

Személyes adatainkat[1] nem csak a bankok és pénzintézetek kérhetik el. Bármilyen élethelyzetben szükség lehet arra, hogy használjuk őket (pl.: a boltban való bankkártyás fizetéskor, nemzetközi utazáshoz való jegyváltáshoz, akciós sorsolásokra való jelentkezéskor, regisztrációs űrlapok kitöltésekor stb.). Az Európai Unió Alapjogi Chartája is kimondja, hogy „Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez" [10]. Az államoknak és persze a különböző gazdasági társaságoknak az lenne a célja, hogy az egyes személyek féltett magánéleti adatait is rögzítsék többfajta nyilvántartásban. E tekintetben ütköznek az érdekek az államok, gazdasági társaságok és az egyének között. Mindegyik számára belátható, egyik érdek nem valósítható meg teljes mértékben, ezért kompromisszumos megoldásként születtek meg azok a jogszabályok, melyek meghatározzák, hogy milyen adatok, milyen célból gyűjthetőek és miként lehet őket, tárolni, felhasználni, illetve harmadik félnek átadni. A magyar jogszabályok közül a Magyar KöztársaságAlkotmányának (1949. évi XX. törvény) 59. §-a és az 1992. évi LXIII. törvény foglalkozik e kérdésekkel. Ez utóbbi a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szól és megfelel az Európai Tanács Adatvédelmi Egyezmény valamint a Gazdasági Együttműködési és Fejlesztési Szervezet útmutatásainak is [1].

Életünk során több olyan helyzet is előáll, amikor a személyes adatokon kívül szükség van az aláírásunkra. pl.: egy szolgáltatás megrendelésekor ezzel igazoljuk, hogy az adott megrendelő fél tényleg mi voltunk, magyarán az aláírásunkkal hitelesítjük. Ma az információs társadalomban már arra is van lehetőség, hogy ne csak papíron, hanem elektronikusan is alá tudjunk írni. Mind a papíron, mind az elektronikusan történő aláírásnál is fontos szempont, hogy egyértelműen azonosítható legyen az aláíró fél. A kézzel való aláírásnál a leírt betűk írásmódja az azonosítás alapja, de az elektronikus aláírásnál nem az aláírásunk szkennelt képének az elektronikus dokumentum mellé csatolásáról beszélünk, hanem egy olyan könnyen létrehozható és egyedi azonosítóról, amit csak egyetlen személy, azaz mi tudunk létrehozni. Az elektronikus úton megtett aláírásunk hitelességét törvény is elismeri, a 2001. évi XXXV. törvény az elektronikus aláírásról. Ez a törvény teremtette meg Magyarországon a hiteles elektronikus nyilatkozattétel, illetőleg adattovábbítás jogszabályi feltételeit [11][12].

Az információs társadalom egyre inkább elektronikus útra tereli a különböző szolgáltatásokat. Lehet szó akár adóbevallásról, számlakibocsátásról, szerződések megkötéséről, különböző megrendelésekről, pénzügyi utalásokról és transzferekről; az elektronikus úton történő ügyintézés egyre gyakoribbá válik. Ahogy a társadalom egyre inkább alakul át e-társadalommá, úgy növekszik a közigazgatásban is e-közigazgatási szolgáltatások száma. Magyarországon az alábbi törvények foglalkoznak az e-társadalommal és e-közigazgatással:

- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
- 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól (Ket.)
- 2009. évi LX. törvény az elektronikus közszolgáltatásról
- 2009. évi LXXVI. törvény a szolgáltatási tevékenység megkezdésének és folytatásának általános szabályairól

[1] Személyes adatnak minősül minden olyan információ, amely egy adott személyre vonatkozik, és amely alapján az a személy – közvetlenül vagy közvetetten – azonosítható, pl. a neve, telefonszáma, elektronikus levélcíme, születési helye és ideje stb.

Szabványok és ajánlások [13][14][15][16][17]

A szabványok és ajánlások olyan egységesítő és szabályozó tevékenységnek az eredményei, melyeket a felhasználó és a fogyasztó érdekében hoztak létre azzal a céllal, hogy egységes és következetes megoldási módokat alkalmazzanak a rendszeresen ismétlődő műszaki és gazdasági feladatokra. Ezeket a műszaki dokumentumokat hivatalos, félhivatalos és informális szervezetek készítik. Azonban ugyanazon témakörben készített szabványok és ajánlások is eltérhetnek egymástól. Olyan nemzetközi szervezetek, mint az EU és az OECD is készítenek ajánlásokat és irányelveket, de az USA mégis vezető szerepet játszik a szabványok és ajánlások készítésében. Ez köszönhető annak is, hogy a hagyományoknak köszönhetően civil és kormányzati téren is tekintélyes szabványosítási infrastruktúrával van ellátva, és ezek meglehetősen jó összhangban tudnak együtt dolgozni.

Az informatikai biztonság területén az alábbi szabványokat és ajánlásokat fontos megemlíteni:

1. Common Criteria (CC):
   Az Európai Közösség, az amerikai és kanadai kormányok támogatásával létrehozott dokumentum, ami a korábbi ajánlások (mint pl.: a TCSEC és ITSEC ajánlások) tartalmi és technikai különbségeit kísérelte meg közös nevezőre hozni. Fő jellemzői a következők:
   - Egységes, a megvalósítás módjától független, követelményeket határoz meg.
   - Egységes kiértékelési módszertant ad az informatikai rendszerek, termékek informatikai biztonsági értékeléséhez, tanúsításához.
   - Meghatározza az informatikai rendszerek biztonsági követelményeinek többszintű kategóriákból álló katalógusát.
   - Egyaránt felhasználható szoftver és hardver elemek vizsgálatához is.
   - A termékek rugalmasan megválaszthatók, mert a követelmények nem hardver vagy szoftver specifikusak.
   - Definiálható a biztonsági funkcionalitás, azaz a CC fogalmai szerint a védelmi profil (Protection Profiles), amely függetlenül besorolható a CC-ben meghatározott hét biztonsági szint (Evaluation Assurance Level: EAL) valamelyikébe.
2. BS 7799
   Ezt a nemzetközileg dicsért és használt szabványt a Brit Szabványügyi Hivatal adta ki. Két fő részből áll, melyek 1995-ben illetve 1998-ban lettek publikálva:
   - Az informatikai biztonság irányításának kézikönyve:
     Ez a szabvány a szervezeti szintű, informatikai biztonságmenedzsment központú szemléletet követi és a szervezet üzleti céljaiból és stratégiájából vezeti le a biztonsági követelményeket és intézkedéseket.
   - Az informatikai biztonsági irányítási rendszer specifikációja
     Az előző rész kiegészítéseként jelent meg és elsősorban a szervezetek menedzsmentje részére fogalmaz meg követelményeket az Információbiztonság Menedzsment Rendszer megvalósítására és dokumentációs rendszerére vonatkozóan, valamint szervezeti szintű informatikai biztonsági intézkedéseket ajánl.
3. ISO/IEC 270xx
   Az ISO/IEC 27000 szabványsorozat az informatikai biztonság irányítási rendszerének "legjobb gyakorlatait" (best practices) fogja össze, és elsősorban a felhasználói oldalon helyet foglaló IT menedzserek számára készült. Az informatikai biztonságmenedzsment rendszer megvalósítására és ellenőrzésére vonatkozó követelményrendszer kidolgozását segíti, úgy hogy mindazon előírásokat magában

foglalja, amik a teljes szervezetre vonatkozó, az összes rendszerelem csoportot átölelő informatikai biztonsági követelmények és védelmi intézkedések és az azok implementálásához, auditálásához, kockázatelemzéséhez szükségesek. A szabványsorozat néhány tagjának rövid ismertetése:

- ISO/IEC 27000: Szószedet és terminológia a sorozat valamennyi szabványához.
- ISO/IEC 27001: Az informatikai biztonság irányítási rendszere (BS 7799-2:2002), a szervezet auditálásához szükséges (megfelelőségi) előírások.
- ISO/IEC 27002: Az informatikai biztonság irányítása gyakorlati előírásait, ellenőrzési célokat és a legjobb gyakorlatot írja le.
- ISO/IEC 27003: Az ISO/IEC 27000 szabvány implementálásához szükséges tanácsokat és útmutatókat fogja tartalmazni.
- ISO/IEC 27004: Egy új szabvány lesz, amely az informatikai biztonság mérésével fog foglalkozni, abból a célból, hogy az informatikai biztonság irányítási rendszerének hatékonyságát mérni tudjuk.
- ISO/IEC 27005: Az informatikai biztonság kockázatkezelésével fog foglalkozni.
- ISO/IEC 27006: az ISO/IEC IEC 27001 szabványnak való megfelelést vizsgáló szervezetek számára tartalmaz követelményeket.
- ISO/IEC 27011: informatikai biztonságirányítási irányelvek lesznek a telekommunikációihoz.

4. MEH ITB 8. sz. ajánlás
   Ez egy tájékoztató az informatikai biztonság megteremtésének legfontosabb elemeiről és célja felkészíteni a szervezetet az informatikai biztonsági koncepciójának kialakítására. Kockázatelemzési módszertanként használják.
5. MEH ITB 12. sz. ajánlás
   A logikai védelem előírásait, részletes követelményeket és védelmi intézkedéseket tartalmaz informatikai biztonság adminisztratív és a fizikai védelem területeire, a szervezeti, személyi és fizikai biztonság témakörét illetően is. Informatikai Rendszerek Biztonsági Követelményei névvel is ismert.
6. MEH ITB 16. sz. ajánlás
   A Common Criteria szabvány magyar változata.
7. KIB 25. számú ajánlás
   A Közigazgatási Informatikai Bizottság 25. számú ajánlása a Magyar Informatikai Biztonsági Ajánlások című ajánlássorozat. A sorozatban 12 önálló ajánlás található, melyek 3 jelentős csoportot ölelnek fel:
   - MIBIK (Magyar Informatikai Biztonság Irányítási Keretrendszere)
   - MIBÉTS (Magyar Informatika Biztonság Értékelési és Tanúsítási Séma)
   - IBIX (Informatikai Biztonsági Iránymutató Kis Szervezetek Számára)

   Az informatikai biztonságot a MIBIK szervezeti oldalról, a MIBÉTS pedig technológiai oldalról közelíti meg. És míg a MIBIK és MIBÉTS olyan szervezeteknek nyújt segítséget, amik rendelkeznek jelentősebb informatikai rendszerrel és/vagy az informatikai rendszerhez elkülönült informatikai személyzettel, addig az IBIX mindazon szervezeteknek hasznos, amik nem rendelkeznek ilyen lehetőségekkel.

A Külügyminisztérium informatikai és információs rendszerei

Magyarországon a külügyekkel foglalkozó közigazgatási csúcsszerv a Külügyminisztérium. A Külügyminisztériumban az informatikai biztonság megteremtéséért és fenntartásáért a Biztonsági Informatikai és Távközlési Főosztály felel. Az informatikai támadások alapvető célját az, adatot informatikai rendszer elemein keresztül is el lehet érni és fenyegethetik. A feladata ellátását jócskán megnehezíti az a tény, hogy a közel 2000 fős köztisztviselői

állomány kevesebb, mint a fele dolgozik csak Magyarországon, a többiek a kb. 100 képviselet egyikén vannak külszolgálaton. A Külügyminisztériumnak, feladatainak jellegénél fogva több informatikai rendszere van és mindegyik rendszer biztonságára ügyelni kell. A Külügyminisztériumban az alábbi jelentősebb nemzeti informatikai és információs rendszerek, illetve azok végpontjai üzemelnek:

a. KIR (Konzuli Információs Rendszer – Consular Information System - CIS):
   A két alapvető konzuli tevékenységet, a vízumkiadást és a klasszikus konzuli ügyek intézését informatikailag támogató rendszer. Célja a konzuli feladatok elvégzésének könnyítése és gyorsítása. A KIR kezeli és elektronikusan tárolja a vízumkérelmeket, az egyéb konzuli ügyeket, a vonatkozó pénzügyi forgalmat (bevételeket) is. Különböző paraméterekkel statisztikák készítésére is alkalmas. És 2007 decembere óta, amióta teljes jogú tagjai vagyunk a Schengeni országoknak, azóta közvetetten a Schengeni Információs Rendszerrel is kommunikál a KIR.
b. VKH (Védett Külügyi Hálózat):
   A Magyar Köztársaság nemzeti érdekeinek hatékony érvényesítése az Európai Unióban koncepcióváltást tett szükségessé a diplomáciai információszerzésben, a tájékoztatásban és az információkhoz való hozzáférés terén, valamint szemléletváltást az információk minősítésében és technológiaváltást az információtovábbításban. A diplomáciai információs tevékenység megújításának technikai feltételeit biztosítja a Külügyminisztérium és a külképviseletek védett hálózata a Védett Külügyi Hálózat. A VKH lehetővé teszi a „bizalmas" és „korlátozott terjesztésű" minősített nemzeti, valamint EU- és NATO-információk gyors továbbítását [18]. A „Bizalmas" és „Korlátozott terjesztésű" minősítéssel ellátott iratokat, táviratokat a szervezeti egységek a Védett Külügyi Hálózat számítógépein készítik, kezelik és ugyanebben a rendszerben továbbítják a Központ szervezeti egységei, illetve a Központ és a bekapcsolt külképviseletek, valamint a Központ és egyes magyar kormányzati szervek között (pl.: egyes minisztériumok).
c. EU DOK (EU Dokumentációs rendszer) [19][20]:
   E rendszer fő feladata, hogy segítse az európai uniós ügyek kormányzati koordinációját. Ebbe beleértjük az elektronikus úton Magyarországra érkező nem minősített Európai Uniós dokumentumok szétosztását és különböző magyar intézkedések végrehajtásának folyamatát (pl.: tárgyalási álláspontok kialakítását). A felhasználók számára kialakított felület egy portálrendszer. Ebben az európai ügyekre szakosodott személyre szabott portálban 60 db úgynevezett közösségi felületek alakítható ki a maximális 1000 felhasználónak. Közösségekben csoportosíthatóak azok a felhasználók, akik közösen dolgoznak. A közösségek között szakértői csoportok[2], tanácsok és az EKTB közössége található meg. A rendszer a különböző témákhoz tartozó információkat (megküldött EU-s tervezeteket, tárgyalási álláspontokat, jelentéseket, jegyzőkönyveket, feladatok, események, fórumüzenetek stb.) úgynevezett dossziékban rendszerezi. Az EUDOK lehetőséget ad arra is, hogy mind az EU-s mind a hazai ülések napirendjeit nyomonkövessük. Az egyes napirendi pontokhoz automatikusan hozzárendeződnek a kapcsolódó dossziék is.

[2] A szakértői csoport tagjai azok a személyek, akik az Európai Unió politikáját illetően összefogják a hazai közigazgatási feladatokat, így többek között a beérkező uniós tervezetre kialakítják a magyar álláspont tervezetet, valamint elkészítik a hozzá kapcsolódó egyéb dokumentumokat (pl. környezetvédelem, tőke szabad áramlása, foglalkoztatás- és szociálpolitika)

A Külügyminisztériumban végponttal rendelkező Európai Uniós rendszerek

A fentebb említett nemzeti rendszereken kívül vannak még olyan informatikai rendszereknek végpontjai a külügyminisztériumban, melyeket az EU-val való kapcsolattartás miatt szükséges fenntartani. Ezen rendszerek kialakítása, üzemeltetése során alapvetően az „EU minősített információk védelmét szolgáló biztonsági szabályokról" elnevezésű és 13885/1/09-es számot viselő tanácsi határozat szerint kell eljárni. Természetesen ez nem írja felül a magyar jogszabályokat, de nem is szükséges, mert a jogharmonizációnak köszönhetően igazodnak ehhez. A Külügyminisztériumban az alábbi Európai Uniós informatikai rendszereknek van végpontja:

a. EU Extranet-L és Extranet-LR hálózatok
   Az Európai Únió Tanácsa ezen a rendszeren keresztül terjeszti a dokumentumokat (pl.: tanácsi munkacsoportok üléséhez az anyagokat, dokumentumokat). A rendszer a felhasználóknak alapvetően 2 féle terjesztési módszert nyújt. Az egyik egy automatikus információküldés a felhasználó e-mail postafiókjába, a másik pedig egy WEB-es elérési opció, ahol egy WEB oldalon van lehetőség a szükséges anyagok, dokumentumok keresésére, megnézésére. Az egyes felhasználók esetében be lehet állítani, hogy milyen anyagokhoz és dokumentumokhoz férjen hozzá. Ennek alapja a következők lehetnek:
   - Acronym[3] (betűszó, mozaikszó),
   - Munkacsoport,
   - Dokumentum típus (DOC, PDF stb.) és
   - Minősítési szint (nyílt, nem nyilvános, korlátozott terjesztésű).

   Jelenleg a Tanács 2 fajta Extranet oldalt üzemeltet:
   1. EU Extranet-L oldalt, a nyílt és nem nyilvános (limite) dokumentumokhoz és az
   2. EU Extranet-R oldalt pedig a korlátozott terjesztésű (restraint) dokumentumok eléréséhez.

b. CORTESY (Correspondance Européenne Terminal System) rendszer
   A CORTESY rendszer titkosított kapcsolatot biztosít a tagállamok külügyminisztériumai, Európai Unió melletti állandó képviseletei, a Bizottság és a Tanács Főtitkársága között. Segítségével történik az úgynevezett COREU üzenetek (diplomáciai táviratok) elektronikus továbbítása a Tanács közös kül- és biztonságpolitikai partnerei számára [21]. Nagyon hasznos rendszer pl.: a multilaterális vagy harmadik államot érintő kérdések politikai elemzéseinek szaktanácskozásaihoz.
   A rendszer felépítése majdnem teljesen megegyezik az ESDP-Net hálózatéval, csak apróbb eltérések vannak.

c. ESDP-Net (European Security and Defence Policy – Európai Biztonság és Védelem Politika)

[3] A különböző témákhoz különböző acronymeket rendelnek (pl.: COAFR: Afrikai vonatkozású téma; COASI: Ázsiát és Óceániát érintő témák, COMELEC: elektronikus kommunikációt érintő témák stb.). Az automatikus terjesztés során az egyes tanácsi munkacsoportok és almunkacsoportok tagjai számára azokat az anyagokat, dokumentumokat küldik automatikusan amelyik acronymre fel vannak iratkozva. Illetve a WEB-es felületen az adott acronymekkel ellátott dokumentumokra is rá lehet keresni. A tanácsi munkacsoportok a készítéskor ellátják rá jellemző acronymekkel az anyagokat és dokumentumokat, így minden az érintett témával foglalkozó személy és csoport megkapja azt az információt, amiről tudnia kell, illetve amivel feladata van.

Az ESDP-Net hálózat titkosított kapcsolatot biztosít a Tanács és annak európai biztonsági és védelmi politikai partnerei között. A hálózat felhasználói:

- külügyminisztériumok,
- hadügyminisztériumok,
- vezérkari főnökök és műveleti főhadiszállások,
- az EU Műhold Központja Torrejonban, Spanyolországban
- a Tanács főtitkárság és
- az Európai Bizottság

A hálózat felépítése majdnem teljesen megegyezik a CORTESY rendszerével, csak apróbb eltérések vannak. A hálózat minden egyes üzenete akkor érhető el, ha meg van hozzá a megfelelő felhatalmazás. A rendszer minden egyes végpontja a beérkezett üzeneteket a saját adatbázisában tárolja. A rendszer minden olyan helyben tárolt üzenetben engedi tallózni a felhasználókat, amihez rendelkezik felhatalmazással, vagyis azok között, amikhez a helyi adatbázisában hozzáférést engedélyeztek számára. Arra nincs lehetőség, hogy egy másik végpont adatbázisához férjen hozzá a felhasználó.

d. EU CIRCA (Communication & Information Resource Centre Administrator) [22]
A CIRCA az egy extranet eszköz, melyet az Európai Bizottság IDA programja keretében fejlesztettek ki, és hangoltak a kormányzati igényekhez. Hasonlóan a magyar EUDOK rendszerhez, ez is egy WEB alapú portál. A földrajzilag szétszórt EU-s intézmények és partnereik használják információ és dokumentumok megosztásához, továbbá eszmecserék, viták, tanácskozások lefolytatásához és számos más funkcióhoz is. A CIRCA rendszer a felhasználókat közösségekbe szervezi és minden egyes közösségnek biztosít egy úgynevezett magán tárhelyet, aminek az eléréséhez csak internet elérésre és egy internet böngészőre van szükség. Minden magán tárhely esetében a tanácsi munkacsoportokhoz hasonlóan az közösség egyik tagja a moderátor, az elnök vagy, ahogy a CIRCA nevezi a vezető (leader).

e. SESAME (Secured European System for Automatic Messaging) [23]
A SESAME rendszer ma még nem „élő" rendszer. 2002-ben kezdték a kifejlesztését és a kezdeti céldátum 2004 Júliusa volt, mely különböző okok miatt[4] 2012-re módosult. Az alapötlet szerint a jelenlegi CORTESY és ESDP-Net rendszereket fogja kiváltani. Ugyan azon a fizikai összeköttetésen 2 logikai szintet hoznak létre rejtjelző eszközökkel: egy korlátozott terjesztésű (az EU korlátozott terjesztésű és alacsonyabb minősítésű anyagoknak) és egy titkos szintű (az EU bizalmas és EU titkos minősítésű anyagoknak) kommunikációs csatornát. A két rendszer nem egyszerűen lecserélik, hanem további kommunikációs lehetőségekkel és felhasználói funkciókkal bővítik is. Mivel a rendszer még mindig tervezési fázisban van, ezért még sokat változhat a végső kiépítettsége is.

Következtetések

A ma alkalmazott informatikai rendszerek minden elemére kiterjed a fenyegetettség. Veszélybe kerülhetnek a következő alábbi tényezők:

- hardver környezet

[4] A különböző okok közül néhány: 1) a tagállamok küldöttei nem tudtak megegyezni abban, hogy miként kezeljenek bizonyos fajta érzékeny információkat. 2) alábecsülték az időszükségeltét a szigorú akkreditációs eljárásnak, hogy megszerezzék a tanács biztonsági tanúsítványt 3) ugyancsak alábecsülték a projekt műszaki összetettségét is.

- szoftver környezet
- kommunikációs rendszer
- emberi erőforrás, a jól képzett munkaerő.

Ahhoz, hogy kellően felkészülten reagáljunk az informatikai támadásokra, hogy meg tudjuk tenni a kellő lépéseket azok megelőzéséhez, a károk enyhítéséhez, és a következmények felszámolásához, az alábbiak végig gondolása nélkülözhetetlen.

Szükséges, hogy létezzenek olyan szervezetek, szakemberek, eszközök és módszerek, amelyeket különböző fajta informatikai támadásokra való megelőző lépésként meg tudunk lépni, illetve bekövetkezésük esetén fel lehet használni a védekezéshez, és kárenyhítéshez. Az ilyen helyzetekre való sikeres reagálás és válasz miatt, hozták létre a szabványokat, ajánlásokat és jogszabályokat. A jól átgondolt és használható szabványokat és ajánlásokat a különböző szervezetek még úgy is elkezdik alkalmazni, hogy azok alkalmazása nem kötelező érvényű. Ez pedig az első legjobb automatikus lépés az informatikai biztonság irányába.

Irodalmi hivatkozás

[1] Muha Lajos (szerk.): Az informatikai biztonság kézikönyve.: Informatikai biztonsági tanácsadó A-tól Z-ig., Budapest: Verlag Dashöfer Szakkiadó, 2005. 3210 p., ISBN:963 9313 12 2

[2] Információbiztonság a másik oldalról: Hackerek Magyarországon
http://www.zmne.hu/tanszekek/ehc/konferencia/prez/Krasznay_Csaba.ppt
(letöltve: 2010.05.18)

[3] Krimináltechnika szerepe az informatikai védelem területén
http://www.hadmernok.hu/2009_1_illesi.pdf
(letöltve: 2010.05.16)

[4] Muha Lajos: Az informatikai biztonság evolúciója és revolúciója In: Magyar Tudomány Ünnepe - Gábor Dénes Főiskola (Informatikai rendszerek biztonságtechnikája Konferencia), Budapest, 2006.11.08.,
http://www.mtakpa.hu/kpa/download/1233544.pdf
(letöltve: 2010.05.17)

[5] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme (PhD disszertáció), ZMNE, Budapest, 2007.
http://www.mtakpa.hu/kpa/download/1228916.pdf
(letöltve:2010.05.30)

[6] Az informatikai biztonság alapjai
http://e-oktat.pmmf.hu/webgui/www/uploads/images/1497/Informatikai_biztonsag_1.pdf
(letöltve 2010.05.18)

[7] Az üzleti titkok védelméről - 2. rész
http://www.ugyvezeto.hu/cikk/60415/az-uzleti-titkok-vedelmerol-2-resz?area=595
(letöltve: 2010.05.28)

[8] Mi minősül az üzleti titok megsértésének?
http://www.feketelista.hu/mi-minosul-az-uzleti-titok-megsertesenek/
(letöltve:2010.05.28)

[9] Banktitok
http://www.bankkartya.hu/?cikk=2578&lap=1
(letöltve:2010.05.28.)

[10] Személyes adatok védelme az Európai Unióban
http://ec.europa.eu/justice_home/key_issues/data_protection/data_protection_0108_hu.pdf
(letöltve: 2010.05.28)

[11] Elektronikus aláírás
http://srv.e-szigno.hu/menu/?lap=tudasbazis_elektronikus_alairas
(letöltve:2010.05.29)

[12] Elektronikus aláírás
http://www.csatolna.hu/hu/eloadas/savo/elektronikus_alairas.pdf
(letöltve:2005.05.29)

[13] Szabvány
http://hu.wikipedia.org/wiki/Szabvány
(letöltve:2010.05.29)

[14] 1995. évi XXVIII. törvény a nemzeti szabványosításról

[15] Szabványosítás
http://www.recoware.hu/biometria/szabvanyositas_es_ajanlasok.html
(letöltve:2010.05.29)

[16] Az információbiztonság sarokkövei: szabványok és ajánlások
http://www.isotanusitas.hu/hu/cikkolvas/informaciobiztonsag
(letöltve:2010.05.29)

[17] Muha Lajos: Az informatikai biztonság mérése, In: Tudomány Hete a Dunaújvárosi Főiskolán: interperszonális nemzetközi tudományos konferenciasorozat. Dunaújváros, 2009.11.09-2009.11.13.
(http://www.mtakpa.hu/kpa/download/1278547.pdf letöltve:2010.05.17)

[18] A külügyminiszter 12/2004. KÜM utasítása a Védett Külügyi Hálózat használatáról

[19] EU-s ügyek kezelése a Synergon segítségével.
http://www.terminal.hu/cikk.php?article_id=5565
(letöltve: 2009-11-10)

[20] Synergon MAGASYN - 2005. tél, 16-17. oldal: EUDOK – uniós ügyek e-koordinációja
http://www.synergon.hu/data/cms9687/msyn_tel2005.pdf
(letöltve: 2010.05.26)

[21] The main bodies specific to the CFSP
http://www.diplomatie.gouv.fr/en/european-union_157/eu-in-the-world_1491/common-foreign-and-security-policy_5463/operation-of-the-cfsp_5467/the-main-bodies-specific-to-the-cfsp_5472/cfsp-communication-networks_8757.html
(letöltve: 2009.12.15)

[22] A Quick Reference Guide to CIRCA 3.4
http://circa.europa.eu/docs/circa_quick_guide.pdf
(letöltve: 2010.04.26)

[23] Official Journal of the European Union, 10.11.2009 NOTICES FROM EUROPEAN UNION INSTITUTIONS AND BODIES: COURT OF AUDITORS
http://eca.europa.eu/portal/pls/portal/docs/1/3258349.PDF
(letöltve: 2010.05.20)