Dr. Haig Zsolt

AZ INFORMÁCIÓBIZTONSÁG SZABÁLYZÓI ÉS SZERVEZETEI KERETEI

Absztrakt:

A cikk rövid áttekintést ad a különböző nemzeti és nemzetközi információbiztonsági szabványokról és az incidenskezelő szervezetekről valamint a hazai gyakorlatról.

In this paper is given a short review about national and international information security standards and incident handling organizations as well as Hungarian practice.

Kulcsszavak: *információbiztonság, információbiztonsági szabványok, ajánlások, incidenskezelő szervezetek*

Bevezetés

Az információs társadalom biztonsága érdekében napjainkban a világ számos országában és nemzetközi szinten is egyre több intézkedést hoznak. Ennek mozgatórugója, hogy az infokommunikációs rendszerek ellen fokozódó fenyegetésekkel kell számolnunk, illetve a terrorizmusnak megjelent egy új válfaja az információs terrorizmus, mely elsősorban az információs dimenzióban valósul meg. A biztonság érdekében hozott intézkedések mindegyike azt célozza, hogy a társadalom működése szempontjából létfontosságú információs infrastruktúrák működése, illetve védelmük lehetőleg optimális legyen. Ennek érdekében törvényi, jogszabályi törekvéseket figyelhetünk meg, különböző szabványok és ajánlások látnak napvilágot, és egyre több olyan szervezet jön létre, melyek mindegyike az információbiztonság (informatikai biztonság) bizonyos mértékű fenntartását célozza meg. E cikk ezen intézkedéseket tekinti át, és megvizsgálja e téren a jelenlegi magyarországi gyakorlatot.

1. Törvényi és jogszabályi törekvések

Az információs társadalom működése alapjaiban függ azoktól a nagy integráltságú infokommunikációs rendszerektől, amelyek napjainkban rendkívüli mértékű fejlődésen mennek keresztül. E rendszerekre jellemző az egymáshoz való kapcsolódás, a rendszerek globalitása és ennek következtében a globális hozzáférhetőség. Ezzel párhuzamosan és ezzel egyenes arányban növekszik e rendszerek fenyegetettsége, és ezáltal a sebezhetősége is.

Az infokommunikációs rendszerek integráltságából és komplexitásából fakadóan e rendszerek elleni fenyegetések, illetve az általuk okozott károk nagysága nagyon sok esetben nemcsak egy infokommunikációs rendszer területén, hanem több rendszerben együttesen jelentkeznek. Mindezek alapján az egy infokommunikációs rendszer esetén jelentkező veszélyforrás vagy támadás, hatással lehet több infokommunikációs rendszer működésére is, ezért minden veszélyforrás különös figyelmet igényel. Ez azt is jelenti, hogy pl. a távközlési rendszer lehallgatását, zavarását vagy a szenzorhálózat működésének korlátozását ugyanolyan komolyan kell venni, mint a számítógép-hálózatokban megjelenő különböző támadásokat. [1]

Kormányzati szinten ez különösen nagy problémát jelent, hisz egy ország kritikus infrastruktúrái — amelyek az ország folyamatos működését garantálják — döntően az említett infokommunikációs rendszerekre támaszkodnak. Ezért ezek biztonságát a kormányzatnak törvényi és jogszabályi keretek között kell szabályozni. 2001 előtt a kormányok e területre kevésbé fordítottak figyelmet, a biztonság szavatolását más kapcsolódó jogszabályokkal oldották meg. 2001. szeptember 11-e után azonban gyökeres változás állt be téren. Az ikertornyok lerombolása rávilágított arra a tényre, hogy a jóléti társadalom mennyire sebezhető, amennyiben az új típusú biztonsági kihívásokkal nem számol. Ennek következtében számos nyugati államban, de elsősorban az Amerikai Egyesült Államokban azonnal megalkották azokat a törvényeket, jogszabályokat, melyek jelentős mértékben korlátozták az infokommunikációs rendszerek — azon belül is elsősorban az Internet és a hozzá kapcsolódó szolgáltatások (pl. elektronikus levelezés) — használatát. Ugyanakkor több országban is a nemzetbiztonságért felelős szervezetek kizárólagos jogosultságokat kaptak az infokommunikációs rendszerek megfigyelésére, a felhasználók információs szabadságának korlátozására. Mindezt a terrorista fenyegetések erősödésével és az ellenük való hatékony fellépéssel magyarázták.

Az USA-ban Bush elnök már 2001. október 26-án aláírta az "USA Patriot Act[1]" törvényt, amely a terrorizmus elleni harc szellemében különleges jogokkal ruházza fel az FBI-t és más rendészeti, nemzetbiztonsági szervezeteket. Ennek nyomán e szervek jelentősen erősíthetik felderítő, megfigyelő és ellenőrző képességüket. Néhány ezek közül:

- elektronikus megfigyelés minden formájának lehetővé tétele;
- a CIA és az FBI közötti információcsere mértékének növelése;
- az internetszolgáltatók szorosabb együttműködése a rendőrséggel;
- e-mailek eredetének, címzettjének és időpontjának hozzáférhetővé tétele.

A különböző biztonsági szervek a törvény felhatalmazása alapján elektronikus lehallgatással (eavesdropping) megfigyelhetik az e-maileket vagy a telefonhívásokat, nyomon követhetik az Internet forgalmat (sniffing), jelszavakhoz juthatnak hozzá különböző billentyűzet leütést figyelő programok (keylogger) telepítésével stb. A hatóságok számára a hackerek, crackerek és számítógépes bűnözők által használt eszközök széles tárháza áll rendelkezésre, azzal a különbséggel, hogy ők azokat jogszerűen használhatják. Mindezeken túl, az Internet nyújtotta lehetőségek, mint pl. a hatalmas vásárlói adatbázisok és a nagymennyiségű logfile-ok egyesítve az egyszerű kezelhetőséggel és a más oldalakkal való hatékony összekapcsolással, jelentősen megkönnyíti a hatóságok dolgát.

Természetesen az USA lépései több állam kormányzatát is megerősítette abban, hogy törvényileg kell fellépni a terrorizmus ellen melybe az infokommunikációs rendszerek felhasználásának korlátozása is belefér. Kanada szintén 2001 októberében törvényben tette lehetővé az állampolgárok számítógépeinek és telefonbeszélgetéseinek (elsősorban mobil) lehallgatását. Megnyitotta a légiforgalmi adatbázist a hatóságok részére, így azok bármikor hozzáférhetnek az utas listákhoz.

Franciaországban a törvény szerint a távközlési és Internet-szolgáltatóknak egy évig meg kell őrizniük a lehallgatott beszélgetéseket és a levélforgalmat, és meg kell könnyíteniük a kódolt levelek elolvasását is. Hasonló rendszabályokat vezettek be Nagy-Britanniában és

[1] **U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism Act of 2001

Németországban is. Az Európai Unió pedig ajánlást fogalmazott meg a tagországok számára a cyber-támadások terrorista cselekményekhez hasonlatos büntethetőségével kapcsolatban.

A diktatórikusabb berendezkedésű államok, mint pl. Kína, a terrorista fenyegetésre való hivatkozással megnövelték az Internet elnyomását. Ennek következtében számos Internetes keresőt pl. Google, Altavista is letiltottak. [2]

A polgárjogi szervezetek részéről természetesen nagy az ellenállás a különböző törvényekkel, jogszabályokkal szemben, hivatkozva a szólásszabadságra, emberi jogokra, privátszféra sérthetetlenségére, stb. Ugyanakkor a közvélemény kutatások szerint az emberek többsége toleráns a megnövekedett felügyelettel, biztonsági szigorításokkal szemben.

2. Információbiztonsági szabványok és ajánlások

Világszerte igen nagy erőfeszítéseket tesznek az információbiztonsággal kapcsolatos szabályzók megalkotására és azok nemzetközi jogharmonizációjára. A nemzetközi szervezetek – így az EU és az OECD is – számos irányelvet és ajánlást tesznek közzé, hogy a tagországok ezirányú problémáinak megoldását elősegítsék.

Az információbiztonság hazai szabályozása összhangban kell, hogy legyen a nemzetközi gyakorlattal. Ezért már a 90-es évek közepétől törekvés volt arra, hogy az érvényben lévő nemzetközi szabványokat és ajánlásokat átültessék az itthoni gyakorlatba. Mindezidáig ez csak több-kevesebb sikerrel járt. Az alábbiakban röviden áttekintjük azokat a legfontosabb információbiztonsági szabványokat és ajánlásokat, melyek figyelembevétele mindenképpen szükségszerű a hazai szabályzói környezet kialakításakor. Ezek — a teljesség igénye nélkül — az alábbiak:

- Common Criteria[2] (ISO/IEC 15408);
- ITIL[3] (BS 15000:2000);
- COBIT[4] 4.1;
- ISO/IEC 27000 szabványcsalád.

Common Criteria (ISO/IEC 15408). Az EU, valamint az amerikai és a kanadai kormány támogatásával kidolgozásra került szabvány elsősorban technikai jellegű, főleg az informatikai termékek gyártóinak nyújt támogatást. Nagyon részletes és megbízható követelményeket, eljárásokat biztosít az informatikai eszközök biztonsági minősítésére. Az informatikai rendszerek üzemeltetésével, működtetésével kapcsolatban azonban a felhasználó szervezetek számára nem ad útmutatást. [3] A Common Criteria egységes, a megvalósítás módjától független követelményeket határoz meg, és egységes kiértékelési módszertant ad az informatikai rendszerek, termékek informatikai biztonsági értékeléséhez, tanúsításához. Meghatározza az informatikai rendszerek biztonsági követelményeinek többszintű kategóriákból álló katalógusát. [4]

A szabvány honosítására irányuló munka eredményeként 1998-ban kiadásra került az Informatikai Tárcaközi Bizottság (ITB) 16. sz. ajánlása, majd a Magyar Szabványügyi Testület 2002-ben kiadta „Az informatikai biztonságértékelés közös szempontjai” címen az ISO/IEC 15408 szabványt.

---

[2] Common Criteria for Information Technology Security Evaluation
[3] Information Technology Infrastructure Library
[4] Control Objectives for Information and Related Technology

ITIL (BS 15000:2000) Az Informatikai Szolgáltatás Módszertana. Az ITIL-t jó minőségű, költséghatékony informatikai szolgáltatások támogatása céljából fejlesztették ki, mely kiterjed azok teljes életciklusára, így a tervezésre, bevezetésre, működtetésre és újabb szolgáltatások bevezetésére. Tartalmazza az informatikai iparágban elfogadott eljárások és a legjobb gyakorlati módszertanok gyűjteményét az informatikai szolgáltatások menedzselésének területén. [4] Leírja és definiálja a kulcsfolyamatokat és egy keretet ad az informatikai szolgáltatás irányítására. Ez a keret segítheti egy informatikai szervezetben a folyamatok azonosítását és megvitatását.

COBIT 4.1 Informatikai Irányítási és Ellenőrzési Módszertan. Nemzetközileg elfogadott keretelv, amely garantálja az informatikai alkalmazásoknak az üzleti célok szolgálatába való állítását, erőforrásaik felelős felhasználását és a kockázatok megfelelő kezelését. Segítséget nyújt a vezetésnek a folyamatosan változó informatikai környezet kockázatkezelésében, a kontrollok kialakításához szükséges beruházások mérlegelésében. A felhasználók számára biztosítja az informatikai szolgáltatások kontrollját és biztonságát. Az információs rendszerek ellenőrei számára pedig egységes alapot teremt a belső kontrollok minősítéséhez, illetve a vezetés által megkívánt véleményezési, tanácsadói munkához. [4]

ISO/IEC 27000 szabványcsalád. Az ISO/IEC 27000 szabványcsalád alapját a Brit Szabványügyi Hivatal (BSI[5]) által 1999-ben kiadott BS 7799 szabvány adja, mely többszöri frissítés után a Nemzetközi Szabványügyi Szervezet (ISO[6]) által is elfogadott és elismert ISO szabvány gyűjteménnyé fog válni. A szabványcsalád több eleme még a kidolgozás fázisában jár, mások pedig még csak terv formájában léteznek. A család eddig megjelent és jelenleg kidolgozás alatt álló elemei a következők:

- ISO/IEC 27000 – áttekintést és bevezetést ad a szabványcsaládhoz, valamint tartalmazza az alkalmazott speciális kifejezések gyűjteményét.
- ISO/IEC 27001 – követelményszabvány, mely az információbiztonsági irányítási rendszer (ISMS[7]) kialakításához, megvalósításához, működtetéséhez, figyelemmel kíséréséhez, átvizsgálásához, fenntartásához és fejlesztéséhez szükséges követelményeket írja le. Vagyis egy szervezet auditálásához szükséges (megfelelőségi) előírásokat tartalmazza. Megfogalmazza továbbá azokat a követelményeket, melyek a szervezet információbiztonsági irányítási rendszerének külső szakértő általi ellenőrzését, illetve tanúsíthatóságát teszik lehetővé. E szabványt 2005-ben tették közzé.
- ISO/IEC 27002 – az ISO 17799:2005 gyakorlati útmutató átnevezett, frissített változata, mely az információbiztonság irányításának gyakorlati előírásait, az ellenőrzési célokat és a megvalósításra vonatkozó legjobb gyakorlati megoldásokat (best practice), a szükséges szervezési, szabályozási szempontrendszert tartalmazza. E szabvány 2007-ben lett kiadva.
- ISO/IEC 27003 – az új információbiztonsági irányítási rendszer tanúsíthatóságát bevezető útmutató, mely az ISO/IEC 27000 szabvány implementálásához szükséges tanácsokat és útmutatókat fogja tartalmazni. Jelenleg ez a szabvány kidolgozás alatt áll.
- ISO/IEC 27004 – szabvány az információbiztonság mérésére és ellenőrzésére, amely az információbiztonság irányítási rendszere hatékonyságának mérési módszereit, az ellenőrzés lépéseit fogja tartalmazni. E szabvány is jelenleg előkészületben van.
- ISO/IEC 27005 – az információbiztonsággal kapcsolatos kockázatkezelési eljárásokat tartalmazó szabvány, amely jelenleg kiadáshoz közeli állapotban van.

---

[5] British Standard Institute
[6] International Organization for Standardization
[7] Information Security Management System

- ISO/IEC 27006 – útmutató, amely az ISO/IEC 27001 szabványnak való megfelelést vizsgáló szervezetek számára tartalmazza mindazon követelményeket melyeknek — mint auditáló szervezeteknek — meg kell felelniük. Az útmutató 2007-ben lett kiadva.
- ISO/IEC 27007 – útmutatót tartalmaz az információbiztonsági irányítási rendszer auditáláshoz.
- ISO/IEC 27011 – az ISO/IEC 27002 szabványon alapuló információbiztonság irányítási irányelvek, melyek a távközlés számára nyújtanak útmutatót az információbiztonság megvalósításához. A szabvány kiadáshoz közeli állapotban van.

További az ISO/IEC 27000 szabványcsaládhoz tartozó, de még csak tervezett szabványok[8]:
- ISO/IEC 27031 – egy esetlegesen bekövetkező információtechnológiai katasztrófa utáni helyreállításra vonatkozó szabvány.
- ISO/IEC 27032 – cyber-biztonságra vonatkozó irányelvek.
- ISO/IEC 27033 – az ISO/IEC 18028 új (tervezett) elnevezése, amely a hálózatbiztonságra vonatkozik.
- ISO/IEC 27034 – alkalmazás biztonságra vonatkozó irányelvek.
- ISO/IEC 27799 – az egészségügyi szektorban az ISO/IEC 27002 szabvány megvalósítására vonatkozó irányelveket tartalmazza. [3; 4; 5]

Mint az ismertetett szabványok és ajánlások címéből és tartalmából kiderül, azok szinte kizárólag az informatika területére koncentrálnak. Több szervezet is kiadja saját ajánlását, melyek sokszor, sok tekintetben átfedik egymást. Az ISO/IEC 27000 szabványcsalád kidolgozásánál látszik elsőként az a törekvés, hogy egy több területre kiterjedő, átfogó, a Nemzetközi Szabványügyi Szervezet által is elfogadott szabályozó kerüljön kidolgozásra. Itt már fellelhetők a komplex információbiztonság szemléletmód kezdeti lépései is, amit az is tükröz, hogy e kérdéskörben a távközlési hálózatok számára is biztonsági ajánlás kerül kidolgozásra (ISO/IEC 27011).

Hazánkban jelenleg több jogszabály is foglalkozik az információbiztonság kérdésével Jelenleg a közigazgatásra érvényes alapvető informatikai biztonsági jogszabályok az alábbiak:
- 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.

Mindezek mellett még számos jogszabály érinti az információbiztonság egyes területeit, de átfogó szabályozás mindezidáig nem születetett. Mint ahogy arra már az előzőekben is utaltunk, hazákban törekvés mutatkozik a különböző nemzetközi szabványok és ajánlások hazai viszonyoknak történő megfeleltetésére. Erre jó példák a MEH ITB[9] alábbi ajánlásai:
- ITB 8. számú ajánlás: Informatikai biztonsági módszertani kézikönyv (1994.);
- ITB 12. számú ajánlás: Informatikai rendszerek biztonsági követelményei (1996.);
- ITB 16. számú ajánlás: Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertana (1997.).

Bár mindezek a dokumentumok a kormányzati és a közigazgatási információs rendszerek biztonságos működtetésének szabályozására születtek, azok mindezidáig a közigazgatási szférában nem kerültek bevezetésre. Az ismertetett ajánlások átdolgozása jelenleg

[8] E tervezett szabványok elnevezése még bizonytalan
[9] Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság

folyamatban van, és a tervek szerint 2008 első negyedévére elkészül a Magyar Informatikai Biztonsági Ajánlások (MIBA) c. anyag, mely már figyelembe veszi a legújabb nemzetközi dokumentumokat is. Az ajánlás főrésze (törzsanyag) az infokommunikációs biztonság szükségességéről, helyéről és szerepéről szól, mellékletei pedig a szervezeti szintű informatikai biztonságról, a technológiai szintű informatikai biztonságról szól, és a kis szervezetek, különösen az önkormányzatok informatikai biztonsága kérdéseit tárgyalja. [6] Ugyanakkor, mint, ahogy az anyag címéből és tartalmából is látható ez az ajánlás is hasonlóan az előzőekhez csak az informatikai rendszerek biztonságát szabályozza, tehát egy átfogó, komplex információbiztonsági szabvány hazánkban továbbra is várat magára.

3. Információbiztonsági szervezetek

Az 1990-es évek végétől az információtechnológia felhasználásában élenjáró országok, köztük az Európai Unió tagállamai fokozatosan különböző operatív és jogi szervezeteket alakítottak ki a kritikus információs infrastruktúrák hatékonyabb védelme, és az infokommunikációs rendszerek elleni támadásokra való megfelelőbb reagálás érdekében. A lehetséges támadások felderítése és elhárítása sok esetben azon múlhat, hogy a megtámadott szervezetnek milyen kapcsolata van a nemzetközi és nemzeti információbiztonsági szervezetekkel, incidenskezelő csoportokkal. E pontban röviden és a teljesség igénye nélkül áttekintjük e szervezeteket és azok főbb funkcióit.

Nemzetközi információbiztonsági szervezetek:

- **ENISA**[10] Európai Hálózat- és Informatikai Biztonsági Ügynökség;
- **CERT-ek** [11] Számítógépes Vészhelyzeti Reagáló Csoportok és **CSIRT-k** [12] Számítógépes Biztonsági Incidens Reagáló Csoportok;
- **TF-CSIRT**[13] az Európában működő CERT szervezetek közös szervezete;
- **FIRST**[14] incidenskezelő szervezetek fóruma;
- **EGC**[15] Európai kormányok CSIRT csoportja.

ENISA. 2004-ben az Európa Parlament és Tanács 460/2004 sz. rendeletével ötéves időtartamra létrehozták az Európai Hálózat- és Informatikai Biztonsági Ügynökséget. Az ENISA a tervek szerint olyan tudásközponttá fog válni, amelynek segítségét a tagországok és az uniós intézmények is igénybe vehetik az információbiztonság területén felmerülő problémáik megoldásában. Az ENISA mind a tagállamok, mind az EU intézményei számára szakértői központként működik, amely információbiztonsági kérdésekben tanáccsal látja el a hozzáforduló szervezeteket. Ebben a minőségében az ENISA támogatja a tagállamok, az EU intézmények és a vállalkozások azon képességének megerősítését, amely az információbiztonsági problémák megelőzésére és kezelésére irányulnak.

Az ENISA tevékenységei a következőkre irányulnak:

- információbiztonsági kérdésekben tanácsadással segíti a Bizottságot és a tagállamokat;
- az iparral együttműködve segít megoldani a hardveres és szoftveres biztonsági problémákat;

[10] European Network and Information Security Agency
[11] Computer Emergency Response Team
[12] Computer Security Incident Response Team
[13] TERENA (Trans-European Research and Education Networking Association) által létrahozott projekt
[14] Forum of Incident Response Teams
[15] European Government CSIRTs

- az elektronikus hírközlő hálózatok terhelhetőségére, továbbá az információk hitelességére, sértetlenségére és bizalmasságára vonatkozó információk gyűjtése a kockázatok elemzése céljából;
- Európában már előfordult biztonsági problémákra, illetve a felmerülő veszélyekre vonatkozó adatgyűjtés és elemzés végzése;
- az információbiztonsággal kapcsolatos problémák megelőzésére szolgáló közös módszerek kidolgozása;
- olyan kockázatértékelési és kockázatkezelési módszerek ösztönzése, amelyek lehetővé teszik az információbiztonságot fenyegető veszélyek kezelését;
- a legjobb gyakorlatra vonatkozó tapasztalatcsere az információbiztonság területének különböző szereplői között;
- a hálózat- és információbiztonság területén működő különböző szereplők közötti együttműködés fokozása;
- az információs társadalom termékeire és szolgáltatásaira vonatkozó szabványok fejlesztésének nyomon követése. [3; 7]

CERT, CSIRT. A Számítógépes Vészhelyzeti Reagáló Csoportok és Számítógépes Biztonsági Incidensekre Reagáló Csoportok (a továbbiakban: CERT/CSIRT) az internetes biztonsági problémákkal foglalkozó meghatározó koordinációs központok, melyek közül az USA-ban az elsőt 1988-ban hozta létre a DARPA. Jelenleg ezt a CERT-et a Carnegie Mellon Egyetem üzemelteti. A CERT/CSIRT-k a köz- vagy magánszféra technikai csoportjai, akik figyelnek, figyelmeztetnek, és támadásokra reagálnak.

Országonként és régióként különböző CERT/CSIRT-k működnek, melyeknek különböző támogatott szervezeti vannak. Így a kormányzatnak, a vállalkozói szervezeteknek és az akadémiai szférának (oktatás, tudományos kutatás) külön incidenskezelő szerve van. 2006 májusában 89 CERT/CSIRT működött Európa 30 államában, s közülük 49-t akkreditált a TF-CSIRT. Számos tagállamban – köztük Magyarországon is – találhatunk kormányzati CERT/CSIRT-t, melyek feladata elsősorban az állami információs rendszerek elleni támadások lereagálása. [3]

TF-CSIRT. A TF-CSIRT az Európában működő CERT/CSIRT-k közös szervezete, melyet alapvetően a CERT/CSIRT szervezetek közötti információcsere hatékony biztosítása, valamint a globális fenyegetésekkel szembeni közös fellépés elősegítése érdekében hozták létre. Ez az ernyőszervezet fórumot biztosít a tapasztalatok és ismeretek kicseréléséhez, és kísérleti szolgáltatásokat nyújt az európai CERT/CSIRT-k számára. A különböző információbiztonsági incidensekre való reagálás érdekében szabványokat és ajánlásokat dolgoz ki. Támogatja az új CERT/CSIRT-k létrehozását és biztosítja a munkatársak szakmai továbbképzését. Mindezeken túl az EU és más döntéshozó szervezetek illetve az európai CERT/CSIRT-k között közvetítő szerepet tölt be.

Az európai CERT/CSIRT-k nyilvántartását és státuszát a TF-CSIRT Trusted Introducer elnevezésű projektje végzi. Ennek megfelelően bejegyzett, akkreditált, és akkreditálásra készülő CERT/CSIRT-ket különböztetnek meg. [8]

FIRST. A FIRST a CERT/CSIRT szervezetek világszervezete, aminek célja a CERT/CSIRT szervezetek együttműködésének elősegítése globális szinten, valamint a globális fenyegetésekkel szembeni közös fellépés elősegítése. [3] Ennek érdekében technikai információkat osztanak meg egymás között, illetve az incidensek kezeléséhez szükséges technikai eszközöket, eljárásokat és a legjobb gyakorlatokat fejlesztik ki és terjesztik. Támogatják a biztonsági eszközök, eljárások és szolgáltatások fejlesztését. Elősegítik a

CERT/CSIRT-k alapítását, bővítését. A FIRST egy közösségbe gyűjti a kormányzati, a vállalkozói és az akadémiai szféra CERT/CSIRT-jeit. Jelenleg a FIRST-nek több mint 180 tagja van szerte a világon. [3; 9]

EGC. AZ EGC az európai kormányok CERT/CSIRT szervezeteinek informális csoportja, mely célul tűzte ki a szervezetek közötti hatékony együttműködés fejlesztését, a kormányzatokat érintő incidensek közös kezelését. Ennek érdekében közösen fejlesztik azokat az eljárásokat, melyekkel a nagyszabású információbiztonsági incidenseket kezelhetik. Elősegíti az információbiztonsággal, a fenyegetésekkel és a sebezhetőséggel összefüggő információ megosztást és a technológia cseréjét a tagok között. Szorgalmazza az európai országokban a kormányzati CERT/CSIRT-k megalakítását.

Jelenleg 10 tagja van a szervezetnek (Finnország, Németország, Svájc, Franciaország, Hollandia, Norvégia, Svédország, Nagy-Britannia és Magyarország kormányzati CERT/CSIRT szervezetei.) [10] Érdekesség, hogy Nagy-Britannia két kormányzati CERT/CSIRT szervezettel is képviselteti magát.

Nemzeti kormányzati információbiztonsági szervezetek

- **DCSSI**[16] - Központi Információbiztonsági Igazgatóság (Franciaország);
- **CESG**[17] - Távközlési Elektronikai Biztonsági Csoport (Nagy-Britannia);
- **BSI**[18] - Szövetségi Informatikai Biztonság Hivatal (Németország).

A DCSSI-t mint a francia állam központi információbiztonsági szervezetét 2001-ben rendeletileg hozták létre a Védelmi Minisztérium alárendeltségében. Alapvető funkciói, hogy:

- segítse a minisztériumok közötti információbiztonsággal összefüggő kérdések értelmezését;
- a nemzeti információs rendszerek számára biztonsági garanciákat, tanúsításokat szolgáltasson;
- kriptográfiai és más információbiztonsági eszközöket és eljárásokat biztosítson;
- értékelje az információs rendszerek elleni fenyegetéseket, azok kockázatait, és incidenskezelő szervével tegye meg a megfelelő ellenlépéseket a fenyegetések elhárítására;
- képzésekkel és továbbképzésekkel biztosítsa az információbiztonsági tudatosság erősítését.

A DCSSI incidenskezelő szerve a CERTA[19] mely tagja az EGC-nek. [11]

A CESG a brit kormány nemzeti információbiztonsági technológiai ügynöksége, amelynek célja tanácsadás és segítségnyújtás különböző elektronikus adat és információs rendszerekben jelentkező fenyegetések esetén. Biztosítja mindazon információbiztonsági szabályzókat, szolgáltatásokat, melyek szükségesek ahhoz, hogy a kormányzat és más felhasználók megvédjék a számukra létfontosságú információikat és információs rendszereiket. A CESG rendelkezik mindazon képességekkel, melyek alapján megfelelő tanácsokat tud adni az aktuális vagy az előrelátható kockázatok kezeléséhez.

A CESG szolgáltatási az alábbiak köré csoportosulnak:

---

[16] Direction centrale de la sécurité des systèmes d'information
[17] Communications-Electronics Security Group
[18] Bundesamt für Sicherheit in der Informationstechnik
[19] Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques

- technikai tanácsadás: biztonságos infokommunikációs rendszer kiépítéséhez, nemzeti információbiztonsági szabványok (pl. BS7799) értelmezéséhez, kriptográfiai és más információbiztonsági eszközök és eljárások használatához;
- dokumentáció szolgáltatás: infokommunikációs rendszerek biztonsági dokumentációink kidolgozása, technikai dokumentációk értelmezése;
- egyéb szolgáltatások: információ biztosítása infokommunikációs termékek beszállítóiról, Help-desk típusú telefonos tanácsadás, továbbképzések, stb. [12]

A CESG incidenskezelő szerve a GovCertUK, mely szintén tagja az EGC-nek. A CESG a kormányzati információbiztonság területén számos más szervezettel is együttműködik, mint pl. a Nemzeti Infrastruktúrák Biztonsági Koordináló Központjával (NISCC[20]) vagy a Védelmi Tudományos és Technológiai Laboratóriummal (DSTL[21]) [3]

A BSI a német szövetségi kormány központi információbiztonsági szerve, mely felelős a társadalom és a kormányzat belső információbiztonságáért. A BSI mindenféle információs dimenzióból érkező fenyegetést kivizsgál, ami az információtechnológiával kapcsolatos, és kidolgozza az azokra adandó legmegfelelőbb válaszokat. Az információs támadásokkal járó kockázatok elkerülése vagy minimalizálása érdekében a BSI az információtechnológiai eszközök gyártói, a forgalmazók és a felhasználók számára egyaránt segítséget és támogatást nyújt. A szervezetben külön csoportok foglalkoznak:
- az alkalmazásbiztonsággal, a kritikus infrastruktúrákkal és az Internettel;
- a kriptográfiával és az elektronikus lehallgatás elleni védelemmel, valamint
- az új technológiákkal és a tanúsítással.

A BSI incidenskezelő szerve a CERT-Bund, mely szintén tagja az európai kormányzati CSIRT csoportjának. [13]

Magyarországon a kormányzati és közigazgatási szervek informatikai biztonságának felügyeletét a közigazgatási informatikáért felelős miniszter látja el az általa kinevezett informatikai biztonsági felügyelő útján, akinek feladatait a 195/2005. (IX. 22.) Korm. rendelet szabályozza. Rajta kívül – más országokhoz hasonlóan - hazánkban is kialakultak azok az incidenskezelő szervezetek, melyek a közigazgatási, a vállalkozói és az akadémiai szféra információbiztonságát szavatolják. Ezek az alábbiak:
- PTA[22] CERT-Hungary;
- SZTAKI Hun-CERT;
- NIIF CSIRT;

A PTA CERT-Hungary a magyar kormány informatikai biztonsági incidenskezelő központja, mely a Miniszterelnöki Hivatal Elektronikuskormányzat-központ felügyelete alatt áll. Feladata a teljes magyar privát, üzleti és állami szféra informatikai rendszereinek biztonsági támogatása. A Központnak kiemelt szerepe van a nemzetgazdaság és az állami működőképesség szempontjából alapvető fontosságú informatikai rendszerek védelmében. A szervezet egyben tudásközpont szerepét is betölti a magyar polgárok és informatikai szakemberek számára. A CERT-Hungary számos szolgáltatást biztosít a védett szervezetek számára:
- jelzéseket, figyelmeztetéseket és értesítéseket továbbít a védett szervezetek felé biztonsági résekről, vírustámadásokról, behatolásokról, újonnan észlelt

[20] National Infrastructure Security Coordination Centre
[21] Defence Science and Technology Laboratory
[22] Puskás Tivadar Közalapítvány

sérülékenységekről és behatoló eszközökről stb., és javaslatot tesz a problémák megoldására;
- a biztonság növelését célzó információkat szolgáltat, mint pl.: a központ elérhetősége, általános biztonsági útmutatók, segédletek, incidensekkel kapcsolatos statisztikák, trendek stb.;
- értékeli, elemzi a kapott incidensjelentéseket és reagál azokra (pl. a behatolók aktivitásának figyelésével, a hálózati forgalom szűrésével stb.);
- analizálja a hardver és szoftver sérülékenységeket, és megoldásokat dolgoz ki azok felfedésére és javítására;
- átvizsgálja a különböző támadásra használt rosszindulatú programokat (Malware-eket), elemzi a működési mechanizmusukat és alkalmazásuk módjait, majd megoldásokat dolgoz ki detektálásukra, eltávolításukra és az ellenük való védekezésre;
- oktatási, képzési és továbbképzési tevékenységet folytat, hogy megismertesse a védett szervezetekkel a biztonsági problémákat, illetve a védekezési lehetőségeket és módszereket. [14]

A CERT-Hungary nemzetközi téren is aktívan közreműködik a kormányzati hálózatbiztonsági központok munkájában, aminek következtében 2007-ben az Európai kormányzati CERT-ek csoportjának tagjává vált.

A Hun-CERT az MTA SZTAKI-ban működő csoport, amely az Internet Szolgáltatók Tanácsának (ISZT) támogatásával jött létre és működik. Feladata, hogy az ISZT tagszervezeteinél előforduló információbiztonsági incidensek felderítésénél, elemzésénél és kezelésénél segítséget nyújtson. A Hun-CERT fontosnak tartja a biztonsági tudatosság növelését, amely elsősorban az ISZT tagok felhasználói számára biztosítja mindazon információkat, melyek alapján képessé válnak az Internet biztonságos használatára. [15]

A Hun-CERT felhatalmazással bír az előforduló vagy előfordulással fenyegető mindennemű számítógépes biztonsági események közlésére a hazai Internet szolgáltatók felé. A szervezet által nyújtott támogatás mértékét meghatározza, hogy milyen típusú, mennyire komoly az incidens vagy probléma, milyenek az összetevők típusai, mekkora az érintett közösség és milyen erőforrások állnak rendelkezésre az incidens kezelésére. [8]

Az NIIF-CSIRT a Nemzeti Információs Infrastruktúra Fejlesztési Intézet (NIIF) számítógép biztonsági és incidens kezelő csoportja, amely a magyar felsőoktatás, kutató intézetek és közgyűjtemények szolgáltatója. Az NIIF-CSIRT segíti a számítógép és hálózati incidensek kezelését és koordinációját minden olyan esetben, amikor valamelyik NIIF tagintézmény érintett. Ezen túlmenően fontos, információbiztonsággal kapcsolatos információkat továbbít az NIIF tagintézményeinek, amelyek alapján az egyes intézmények növelhetik saját infokommunikációs rendszereik biztonságát. Az NIIF-CSIRT együttműködik a Hun-CERT-el -el és a kormányzati CERT-Hungary-val is. [16]

Az információs társadalom nagyfokú sebezhetősége ráirányította a figyelmet arra, hogy csak összehangolt közös fellépéssel lehet az esetleges információs támadásokat kezelni, kivédeni. Ennek következtében napjainkra egyre több olyan szervezet jön létre, melyek mindezeket a célokat tűzik zászlóikra. Mint az a fentiekből látható a különböző nemzetközi és nemzeti információbiztonsági szervezetek mindegyike azonos funkciókat lát el, csak más-más szervezeteket képviselnek. Ezek a közös feladatok, funkciók az alábbiak köré csoportosíthatók:
- támadások elemzése;
- információcsere biztosítása;

- adatbázis létrehozása és folyamatos frissítése;
- együttműködések a különböző szervezetek között;
- intézkedések kidolgozása az incidensek kezelésére;
- K+F együttműködések megvalósítása.

Összegzés

Összességében megállapíthatjuk, hogy az információbiztonság hatékony megvalósítása csak nemzeti és nemzetközi szinten összehangolt, koordinált tevékenységként, törvényi és jogszabályi keretek között képzelhető el. Ezek a törvényi szabályozások, jogszabályok egyes esetekben természetesen együtt járnak a szabadságjogok bizonyos fokú korlátozásával is, melyeket azonban a közvélemény többsége a biztonságosabb környezet érdekében elfogad.

A szabványok és ajánlások terén látható a törekvés az egységesítésre, ugyanakkor még mindig az tapasztalható, hogy a kidolgozók csak az informatikai biztonságot tekintik szabályozandónak, és az átfogó információbiztonsági szabályzás kevésbé fontos, holott a társadalom kritikus információs infrastruktúrái olyan komplex infokommunikációs rendszert alkotnak, melyek túlmutatnak az informatika területén.

A különböző információbiztonsági szervezetek a — fenyegetések gyakoribbá és komolyabbá válásával párhuzamosan — egyre nagyobb szerepet kell, hogy kapjanak az információs társadalom biztonságának megőrzésében. Az is látható, hogy nagyon sok egymás mellett működő ilyen szervezet jön létre, és feladataik — melyek döntően szintén csak az informatikai rendszerek védelmét célozzák — átfedik egymást.

Magyarország vonatkozásában megállapíthatjuk, hogy hazánk mindezidáig e téren un. követő magatartást tanúsított mind a szabályzók átvétele terén, mind pedig a különböző szervezetek kialakításakor. Mindenképpen szükségesnek tartjuk egy átfogó, komplex, a teljes infokommunikációs rendszer védelmét szolgáló biztonsági szabályzat vagy ajánlás kidolgozását, a kormányzati és a közszféra vonatkozásában a jelenlegi — egy fő informatikai biztonsági felügyelőnél — komolyabb szervezet létrehozását (lásd pl. Németországban vagy Franciaországban) illetve a jelenlegi meglévő szervezetek feladatkörének kibővítését a teljes információbiztonság területére.

Felhasznált irodalom:

1. Dr. Haig Zs.: Az információbiztonság komplex értelmezése. Robothadviselés 6. tudományos konferencia kiadványa. Hadmérnök különszám 2006. nov. 22. ISSN 1788-1919. http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles6/haig_rw6.htm
2. Weimann G.: Terror on the Internet: The New Arena, the New Challenges. The United States Institute of Peace, 2006. ISBN-10: 1929223714
3. Muha L.: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme Doktori (PhD) értekezés, 2007.
4. Kürt Rt. weboldala: Szabványi háttér. http://www.kurt.hu/szabvanyihatter
5. ISO 27001 weboldala: http://www.iso27001security.com/html/iso27000.html
6. Dr. Dedinszky F.: Információbiztonság a Magyar Köztársaság közigazgatásában. Előadás a Robothadviselés 7 szakmai konferencián. 2007. nov. 27.
7. Európai Hálózat- és Információbiztonsági Ügynökség (ENISA). http://europa.eu/agencies/community_agencies/enisa/index_hu.htm

8. Becz T., Martos B., Pásztor Sz., Rigó E., Tiszai T., Tóth B.: Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai. MTA SZTAKI, 2006. http://mek.oszk.hu/02200/02233/02233.pdf
9. FIRST weboldala. http://www.first.org/
10. EGC weboldala. http://www.egc-group.org/
11. DCSSI weboldala. http://www.ssi.gouv.fr/en/dcssi/index.html
12. CESG weboldala. http://www.cesg.gov.uk/indexNS.cfm
13. BSI weboldala. http://www.bsi.de/english/index.htm
14. PTA CERT-Hungary weboldala. http://www.cert-hungary.hu/
15. Hun-CERT weboldala. http://www.cert.hu
16. NIIF-CSIRT weboldala. http://www.niif.hu/hu/csirt