HADMÉRNÖK

IV. Évfolyam 1. szám - 2009. március

Muha Lajos
Zrínyi Miklós Nemzetvédelmi Egyetem
muha.lajos@zmne.hu

INFOKOMMUNIKÁCIÓS BIZTONSÁGI STRATÉGIA[1]

Absztrakt

A nemzeti infokommunikációs biztonsági stratégia kiadása elengedhetetlen feltétele a nemzeti kritikus információs infrastruktúra védelmének.

Publishing Infocommunication Security Strategy is the essential condition of the Critical Information Infrastructure Protection.

Kulcsszavak: *infokommunikációs biztonsági stratégia, kritikus információs infrastruktúra védelem ~ Infocommunication Security Strategy, Critical Information Infrastructure Protection*

Bevezetés

A 2073/2004. (IV.15.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról [1] foglakozik *a biztonsági környezet – fenyegetések, kockázatok, kihívások részben (II.)* az információs társadalom kihívásaival, ezen belül az informatikai és telekommunikációs hálózatok sebezhetőségével és kockázatával. *A terrorizmus elleni védekezés* részben (III. 3.1.) külön megemlíti a kritikus infrastruktúrák védelmének feladatát. Az információs rendszerek védelme részben (III. 3.7.) kiemeli a kormányzati információs rendszerek védelmének fontosságát és felhívja a figyelmet a sikeres védelem érdekében szükséges együttműködésre, az érintett informatikai és távközlési szolgáltatókkal. *„A hosszú távú lemaradás hátrányos következményeinek elkerülése érdekében Magyarország számára kiemelt feladat a felzárkózás a fejlett világ információs és telekommunikációs színvonalához. Az információs forradalom vívmányainak mind szélesebb körű megismertetése, az oktatás színvonalának emelése kulcsfontosságú érdek, ami közvetve pozitív hatással van a gazdaságra, a társadalom életére és az ország érdekérvényesítő képességére. Az informatikai infrastruktúra technikai és szellemi feltételeinek biztosítása mellett ügyelni kell e rendszerek védelmére és a megfelelő tartalékok képzésére is. Az informatika számtalan lehetőséget teremtett a társadalom számára, de fokozta annak veszélyeztetettségét. A számítógépes hálózatok és rendszerek sebezhetősége, túlterhelése, az információlopás, a vírusterjesztés és a*

[1] A cikk a Robothadviselés 7. tudományos konferencián elhangzott *Infokommunikációs biztonsági stratégia* című előadás szerkesztett változata, amely a szerző doktori értekezésében [2] megjelenteken alapul.

dezinformáció kockázati tényezőt jelent az ország számára." [1] Ezen fenyegetésekre válaszul célul tűzi ki, hogy *„A technológia rohamos fejlődésének korában új feladatként jelentkezik a korszerű és biztonságos informatikai infrastruktúra kialakítása és a kormányzati információs rendszerek védelme. A kormányzati információs rendszert fel kell készíteni a kibernetikai támadások megelőzésére és kivédésére. A védelem sikere érdekében szoros koordináció szükséges mind a szövetségesekkel, mind az informatikai és távközlési szolgáltatók, valamint kutatóközpontok között."* [1].

A Magyar Köztársaság nemzeti biztonsági stratégiájáról szóló kormányhatározat 1. c) pontja előírja, hogy *„A Kormány ... felhívja ... az informatikai és hírközlési minisztert az informatikai és információvédelmi stratégia összehangolt, az érintett tárcák bevonásával 2005. december 31-ig történő elkészítésére azzal, hogy a stratégiák tervezetét a Nemzetbiztonsági Kabinet előzetes véleményét követően, jóváhagyásra a Kormány elé terjessze."* [1]. Ez az informatikai és információvédelmi stratégia nem került elfogadásra a mai napig[2].

A kritikus információs infrastruktúrák védelmi feladatai jelentős tervező munkát, gondos előkészítést igényelnek. A központi és ágazati szabályozás, az irányító, koordinációs testületek munkába állása is jelentős időt vesz igénybe. A korábbi években végzett tanácsadó tevékenységem során azt tapasztaltam, hogy a kormány által kiadott biztonsági dokumentumokat, stratégiákat, kormányzati ajánlásokat a gazdasági és civil szféra akkor is felhasználja, ha az nem kötelező[3]. A kritikus információs infrastruktúrák védelmi kérdésében az egyik legfontosabb iránymutatás az *infokommunikációs biztonsági stratégia*, hiszen a kritikus információs infrastruktúrák meghatározó mértékben infokommunikációs rendszerekből állnak, vagy azok szolgáltatásira épülnek.

A fentiek alapján elkészítettem és javaslatot teszek a hazai infokommunikációs biztonsági ágazati stratégia-tervezetre, amely tartalmazza a nemzeti célokat és feladatokat ezen a téren.

Az infokommunikációs biztonsági stratégiát a **Magyar Köztársaság nemzeti biztonsági stratégiájára** (2073/2004. (IV. 15.) Korm. határozat) **épülve**, azzal **összehangolt ágazati stratégiaként készítettem el.**

A kidolgozás során figyelembe vettem a kutatásaim során levont következtetéseket, valamint a 2073/2004. (IV. 15.) Korm. határozat 1. c) pontjában meghatározottakat, azaz az infokommunikációs technológiai alkalmazások széles társadalmi elterjedtségét, és az infokommunikációs eszközöket kihasználó, illetve ezek ellen irányuló fenyegetettségeket.

A nemzeti biztonsági stratégia II.1.6. (az információs társadalom kihívásai) és a III.3.7. (információs rendszerek védelme) pontjait figyelembe véve, az infokommunikációs biztonsági stratégia védendő értékként azonosítottam az ország működése szempontjából létfontosságú infokommunikációs rendszereket, az úgynevezett kritikus információs

---

[2] Az Információs Társadalom Koordinációs Tárcaközi Bizottság Informatikai Biztonsági Albizottsága 2005. 02. 28-i ülésén ismertetésre került az elkészült informatikai és információvédelmi stratégia absztraktja [3]. Nem hivatalos források szerint ezt a változatot a Nemzetbiztonsági Kabinet nem fogadta el.

[3] A legmarkánsabb példa a MeH ITB 12. sz. ajánlása [4], amelyet a közigazgatás számára bocsátottak ki. A közigazgatásban – anyagi okokra hivatkozva – gyakorlatilag sehol sem vezették be. A közigazgatáson kívüli nagyvállalati szféra (például: MATÁV Rt., Paksi Atomerőmű Rt., TITÁSZ Rt., Dunaferr Rt.) a kiadást követő két éven belül belső szabályzóként bevezette, és használatba vette.

infrastruktúrákat és azok felhasználóit, valamint védendő érdekként határoztam meg az ilyen rendszereken kezelt adatok bizalmasságát, sértetlenségét, és rendelkezésre állását.

A stratégiában elemzem a hazai és nemzetközi biztonsági környezetet, a kockázatokat, fenyegetéseket és kihívásokat.

A stratégia általános célkitűzése a nemzet biztonságának megőrzése azáltal, hogy megakadályozza, vagy elviselhető mértékűre csökkenti a kritikus információs infrastruktúrák elleni sikeres támadások lehetőségét, valamint a bekövetkezett támadások hatását a lehető legkisebbre csökkentse. Ennek érdekében a következő célokat tűzi ki:

- a kritikus információs infrastruktúrák elleni támadások hatékony megelőzése;
- a kritikus információs infrastruktúrák elleni támadások hatékony kivédése;
- a kritikus információs infrastruktúrák elleni támadások hatékony kezelése.

A célok megvalósításához szükséges feladatok terén a stratégia meghatározza az állami koordináció szükségességét, valamint a már meglévő eredményekre épülő monitorozás és reagálás elmélyítését. További feladat az informatikai biztonsági jogszabályok, szabványok, ajánlások aktualizálása, illetve megteremtése, valamint az infokommunikációs rendszerekbe vetett bizalom erősítése a biztonságtudatosság és az ismeretek fejlesztésén keresztül. Kiemelendő, hogy a feladatok végrehajtása az üzleti, civil és akadémia szféra széleskörű bevonását, valamint a nemzetközi szövetségesi rendszer használatát, illetve fejlesztését igényli.

Az infokommunikációs biztonsági stratégia egyben kapcsolódik a NATO és az Európai Unió információbiztonsággal, infokommunikációs biztonsággal kapcsolatos elvárásaihoz és törekvéseihez, továbbá a nemzetközi tapasztalatokra építve figyelembe veszi a hazai közigazgatási, gazdasági és társadalmi környezetet és azok elvárásait.

JAVASLAT A MAGYAR KÖZTÁRSASÁG INFOKOMMUNIKÁCIÓS BIZTONSÁGI STRATÉGIÁJÁRA

I. Értékek és érdekek

Magyarország sikere a globalizálódó világban jelentős mértékben múlhat az információs társadalomba való átmenet hatékonyságán: az egyének és szervezetek birtokában lévő információ ugyanis létfontosságú erőforrás. Mind az információ, mind az ahhoz tartozó folyamatok, rendszerek és eszközök egyre jelentősebb értéket képviselnek, olyan kiemelt jelentőségű erőforrásokká váltak, amelyek semmi mással nem helyettesíthetők. Így megnövekedett a kormányzati szektor és a gazdálkodó szervezetek működőképességének az infokommunikációs rendszerektől való függősége, és új típusú kockázatok jelentek meg, melyek hatékony kezelése nélkül az információs társadalom nem fejlődhet.

A különféle szervezetek hatékony vezetése és rendeltetés szerinti működtetése csak a szükséges információ birtokában valósítható meg. Ha az információ nem férhető hozzá, elvész vagy illetéktelen kezekbe jut, az jelentős anyagi és erkölcsi károkat okozhat, ezért védeni kell.

Ennek megfelelően az „informatikai biztonság” ma már „infokommunikációs biztonság”, ami nem csak a számítástechnikára, hanem egy szerteágazó területre vonatkozik. Az infokommunikációs rendszerek magukba foglalják az adatok gyűjtésére, felvételére, tárolására, feldolgozására (megváltoztatására, átalakítására, összegzésére, elemzésére, stb.), továbbítására, törlésére, hasznosítására (ideértve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozására használt elektronikus eszközöket, eljárásokat, valamint az üzemeltető és a felhasználó személyeket is. Az infokommunikációs rendszerekhez tartoznak:

– az informatikai rendszerek és hálózatok, ide értve az internet szolgáltatást is;
– a vezetékes, a mobil, a rádiós és műholdas távközlés;
– a vezetékes, a rádiófrekvenciás és műholdas műsorszórás;
– a rádiós vagy műholdas navigáció;
– az automatizálási, vezérlési és ellenőrzési rendszerek (SCADA, távmérő, távérzékelő és telemetriai rendszerek, stb.);
– a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek eszközei, eljárásai, valamint az üzemeltető és a felhasználó személyek is.

I.1. A védelem alanyai és tárgyai

Az infokommunikációs rendszereket már ma is számos célra használjuk, és az információs társadalom továbbfejlődésével folyamatosan bővül azoknak a tevékenységeknek a köre, melyeket elektronikusan lehet majd végezni. Már most is elmondható, hogy a felhasználók infokommunikációs rendszert használhatnak:

– hatósági és intézményi ügyintézésre (központi vagy helyi szinten);
– gazdasági tevékenységek támogatására;
– gazdasági kapcsolatra;
– a gazdálkodó, továbbá az állami és közigazgatási szervezeten belüli irányításra, ellenőrzésre és (vagy)
– magáncélra.

Mindez azt is meghatározza, hogy kik használnak infokommunikációs rendszert, tehát kikre terjed majd ki az infokommunikációs biztonsági szabályozás alanyi hatálya, mint felhasználókra (a továbbiakban együtt: felhasználó):

(a) a központi vagy helyi állami és közigazgatási szervezetre:
   – egyfelől, mint elektronikusan ügyet intéző hatóságra, mint más szervezettel információt cserélő alanyra, mint állam- vagy szolgálati titkok kezelőjére, mint személyes adatok és bizalmas adatok (üzleti és magántitok) kezelőjére, mint elektronikusan szerződést kötő félre, mint információs társadalommal összefüggő szolgáltatások, illetve távközlési szolgáltatások igénybevevőjére, mint infokommunikációs rendszert használók munkáltatójára, esetleg, mint – az informatikai biztonsággal kapcsolatos bűncselekménnyel – érintettre;
   – másfelől az egyes állami és közigazgatási szervezetekre, mint az informatikai biztonság és az ezzel összefüggő szakterületek (pl. infokommunikációs rendszerek vizsgálata, minősített adatok kezelése stb.) szabályozásáért, koordinálásáért, érvényesítéséért, ellenőrzéséért felelős, vagy ebben közreműködni köteles szervezetekre;

(b) a gazdálkodó szervezetre, mint közigazgatási ügyfélre, elektronikusan szerződést kötő és a gazdasági életben résztvevő félre, információs társadalommal összefüggő szolgáltatások, illetve távközlési szolgáltatások igénybevevőjére, mint a személyes adat kezelőjére, mint bizalmas adatok kezelőjére és érintettjére, mint infokommunikációs rendszert használók munkáltatójára, mint információbiztonsággal kapcsolatos kötelezettségek alanyára, esetleg, mint az információbiztonsággal kapcsolatos bűncselekmény érintettjére;

(c) a természetes személyre, mint közigazgatási ügyfélre, fogyasztóra, elektronikusan szerződést kötő félre, információs társadalom, illetve a távközlési szolgáltatások igénybevevőjére, mint a személyes adat „érintettjére”, mint a munkaadójánál infokommunikációs rendszert használó munkavállalóra vagy az információs rendszer fejlesztőjére, esetleg, mint informatikai biztonsággal kapcsolatos bűncselekmény elkövetőjére vagy sértettjére.

Az infokommunikációs rendszert használó gazdálkodó szervezetek között meg kell különböztetni a közszolgáltató és a „felügyelt tevékenységet” végző, valamint az e kategóriákba nem tartozó gazdálkodó szervezeteket. E cégeket, illetve ágazatokat az informatikai biztonság tekintetében összefoglaló néven kritikus infrastruktúrának szokták nevezni. Kritikus infrastruktúraként kell kezelnünk *azon létesítményeket, eszközöket vagy szolgáltatásokat, amelyek működésképtelenné válása, vagy megsemmisülése a nemzet biztonságát, a nemzetgazdaságot, a közbiztonságot, a közegészségügyet vagy a kormány hatékony működését gyengítené, továbbá azon létesítményeket, eszközöket és szolgáltatásokat, amelyek megsemmisülése a nemzeti morált vagy a nemzet biztonságába, a nemzetgazdaságba, vagy a közbiztonságba vetett bizalmat jelentősen csökkentené.* Kritikus információs infrastruktúrák *azon az infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikus infrastruktúra elemek, továbbá a kritikus infrastruktúra elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása, vagy megsemmisülése a kritikus infrastruktúrák működésképességét jelentősen csökkentené.*

A Magyar Köztársaság kritikus információs infrastruktúrái közé tartoznak:

1. Az informatikai rendszerek és hálózatok;
2. Automatizálási, vezérlési és ellenőrzési rendszerek (SCADA, távmérő, távérzékelő és telemetriai rendszerek, stb.);
3. Internet szolgáltatás (infrastruktúra is);
4. Vezetékes távközlési szolgáltatások;
5. Mobil távközlési szolgáltatások;
6. Rádiós távközlés és navigáció;
7. Műholdas távközlés;
8. Műsorszórás;
9. Közigazgatási informatika és kommunikáció;
10. A kritikus infrastruktúrák létfontosságú infokommunikációs rendszerei.

Az infokommunikációs biztonság szempontjából azért kell megkülönböztetni a kritikus információs infrastruktúrákat a többi gazdálkodó szervezet infokommunikációs rendszereitől, mert amíg az utóbbiak elsősorban saját biztonságukat kockáztatják, ha gondatlanul járnak el, addig az előbbiek nem megfelelő működése sokkal szélesebb körben, jelentősebb károkat okozhat. Ezért velük kapcsolatban indokolt a többi gazdálkodó szervezetre vonatkozónál részletesebb infokommunikációs biztonsági követelmények betartásának és az ellenőrzési rendszerek kialakításának előírása és felügyelete.

Az infokommunikációs biztonsággal kapcsolatos kötelezettségeket azokra a szervezetekre is ki kell terjeszteni, amelyek az infokommunikációs rendszereket működtetik, vagy ezzel összefüggő szolgáltatásokat nyújtanak:

1. a távközlési szolgáltatók;
2. az internet-szolgáltatók (akik a távközlési szolgáltatók körébe tartoznak, de az infokommunikációs biztonság kérdéskörének különösen lényeges szereplői);
3. az információs társadalommal összefüggő szolgáltatásokat nyújtók;
4. a hitelesítés-szolgáltatók;
5. a távközlési és informatikai tanúsító szervezetek.

I.2. A védendő érdekek

A kritikus információs infrastruktúrák védelme a nemzetközi szabványokkal, a szövetségi rendszerekben előírtakkal összhangban az infokommunikációs rendszerben kezelt

adatok bizalmassága, sértetlensége és rendelkezésre állásának, valamint a rendszer elemeinek sértetlensége és rendelkezésre állásának megőrzésére kell, hogy kiterjedjen.

A bizalmasság arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról. Ez számos jogot érint, így:

- **az államtitok és a szolgálati titok védelmét**, ami közérdek, tehát azt az infokommunikációs rendszerek használata során – a fokozottabb veszélyeztetéssel összhangban – fokozottan kell védeni;
- **a személyes adatok védelmét**, ami a természetes személyek alapvető joga, tehát azt minden, az infokommunikációs rendszerekkel adatkezelést végző szervezetnek garantálnia kell;
- **az üzleti titok és a magántitkok védelmét**, ami méltányolandó magánérdek, tehát elsősorban az érintetteknek kell a védelemről gondoskodnia, de ebben jogi és szakmai segítséget kell kapniuk.

A sértetlenség arra vonatkozik, hogy az adat fizikailag és logikailag teljes és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik. A sértetlenség megőrzése:

- **az e-kormányzat, az e-önkormányzat területén** az elektronikus ügyintézés során különös szerepet kap, mert itt a köz- és az egyéni érdek azonos;
- **az e-szolgáltatások, az elektronikus gazdasági folyamatok** területén méltányolandó magánérdek, tehát elsősorban az érintetteknek kell a védelemről gondoskodnia, de ebben jogi és szakmai segítséget kell kapniuk.

A **rendelkezésre állás** az infokommunikációs rendszerek elemeinek a szükséges időben és időtartamra használhatóságára vonatkozik.

II. Biztonsági környezet – fenyegetések, kockázatok, kihívások

II.1. A hazai helyzet

Mind az államigazgatásban, mind a gazdaságban a rohamosan terjedő infokommunikációs alkalmazások (adatfeldolgozás, kommunikáció, média, stb.) hatékonysága, működőképessége, megbízhatósága – ezzel együtt az adott ágazat tevékenysége – alapvetően függ az infokommunikációs biztonság megfelelő kezelésétől, irányításától. Ezzel a fejlődéssel azonban újfajta veszélyek és fenyegetések is megjelennek.

A szervezetek, valamint infokommunikációs rendszereik egyre gyakrabban szembesülnek igen sokféle forrásból származó biztonsági fenyegetéssel, többek között gazdasági hírszerzéssel, ipari kémkedéssel, számítógépes csalással, szabotázzsal, vandalizmussal, vagy akár tűzzel vagy árvízzel, de egyre nagyobb fenyegetést jelent a terrorizmus új válfaja a kiberterrorizmus is.

A fejlett országok gyakorlatával ellentétben, az infokommunikációs biztonság helyzetére hazánkban jellemző, hogy súlya, kezelése nincs arányban a fontosságával, nincs egységesen alkalmazott módszertan, és nem kapcsolódik a fő nemzetközi irányzatokhoz.

Az infokommunikációs biztonság megoldatlan kérdései hosszú távon veszélyeztethetik a közigazgatás működőképességét és az infokommunikáció dinamikus továbbfejlődését. Ezek a hiányosságok nem mentesítik a felelősség alól az informatikai rendszerekben feldolgozott adatok védelméért felelős vezetőket, ugyanakkor megnehezítik, akadályozzák munkájukat.

Hazánkban hiányoznak a mai technológiai rendszerek szerepének, illetve veszélyeztetettségének megfelelő, az infokommunikációs biztonságra vonatkozó jogi keretek.

Az államtitokról és a szolgálati titokról szóló hatályos, 1995. évi LXV. törvény a módosításaival együtt sem harmonizál a NATO, EU, EURATOM és NYEU titokvédelmi előírásaival.

A szervezeti keretek Magyarországon szétforgácsoltak, és lefedetlen területek is vannak. A legtöbb fejlett országban az infokommunikációs biztonságot egy központi kormányszerv fogja össze (pl. UK: CESG, Németország: BSI, Franciaország: DCSSI, USA:

NSA és NIST), a legtöbb – fejlett informatikai szinten álló – európai országban létezik ún. *InfoSec* hatóság. Magyarországon nincs központi felügyelet, irányítás. Több szervezet felelős a különböző részterületekért, és ezek döntő többsége is csak a minősített információk védelmére irányul, ezért maradnak lefedetlen részterületek.

Hazánkban az infokommunikációs biztonságra vonatkozó ajánlásokat tíz éve nem frissítették, azok elavultak. A közigazgatásban nincsenek érvényes informatikai biztonsági, infokommunikációs biztonsági követelmények, mert már a korábbi ajánlásokat sem tették kötelezővé. Bár születtek ajánlástervezetek, ezeket hivatalosan nem adták ki, így a felhasználókat az „állami akarat" kimutatásának hiánya visszatartja alkalmazásuktól.

Az állami szerepvállalás, támogatás is hiányzik a biztonsági szempontok érvényesítése, a biztonságos információs rendszerek kialakításának és fenntartásának támogatása területén.

II.2. Fenyegetések

Az internet az információs társadalmak alapvető infrastruktúrájává válik, és így az informatikai jellegű támadások megvalósítása is áttevődött az internetre, amely lehetővé teszi a nagy távolságokról történő támadásokat, viszonylagos anonimitást és védelmet biztosítva az elkövető számára.

A kritikus információs infrastruktúrákra nem fizikai jellegű fenyegetettségeit a támadó, valamint az elkövetés módja alapján csoportosíthatjuk. Az elkövető szándéka, rendelkezésére álló erőforrásai és szakértelme eltérő lehet. Veszélyeztető tényező lehet:

- a kiberterrorizmus;
- az információs hadviselés;
- a hírszerzés;
- az ipari kémkedés;
- a számítógépes bűncselekmények;
- a hanyagság és a felelőtlenség.

Az internet alapú támadások sajátos jellegei önmaguk megmagyarázzák azoknak gyakoriságát és hatását. Az internet lehetővé teszi a nagy távolságokról történő támadásokat, amely magasabb fokú anonimitást és védelmet biztosít az elkövető számára. Ez a sajátosság csökkenti a jogszabályok hatékonyságát is. Számos esetben a támadásokat a nemzeti határokon túlról intézik. Más infokommunikációs jellegű támadásokhoz hasonlóan, az internetes támadások során is gyakran használják fel a számítógépeket bizonyos eljárások automatikus ismétlődésére, mint például a szótár alapú kereső programok jelszavak feltörésére, vagy vírusok, melyek korlátlanul replikálják önmagukat. Ez a sajátosság kiegészítheti az egyén szakértelmét globális kihatással járó infrastruktúra megtámadására is. Ilyen esetben a bekövetkezett hatás nincs összefüggésben a támadó rendelkezésére álló erőforrásokkal. Figyelembe veendő, hogy az előre megírt, automatizált támadási eszközök egyre szélesebb körben elérhetőek az interneten, s olyan személyek által is használhatóvá válnak, akik nincsenek tisztában magával az eszközzel vagy a hatásukkal.

III. Célok

A Magyar Köztársaság nemzeti biztonsági stratégiájával (2073/2004. (IV. 15.) Korm. határozat) összhangban az infokommunikációs biztonsági stratégia általános célkitűzése a nemzet biztonságának megőrzése azáltal, hogy megakadályozza, vagy elviselhető mértékűre csökkenti a kritikus információs infrastruktúrák elleni sikeres támadások lehetőségét, valamint a bekövetkezett támadások hatását a lehető legkisebbre csökkenti. Ennek érdekében a következő célokat határozza meg:

III.1. A kritikus információs infrastruktúrák elleni támadások hatékony megelőzése

Szükséges, hogy az ország működéséhez létfontosságú információs infrastruktúrák védelme készüljön fel a támadások megelőzésére a védendő kör beazonosításával és felkészítésével, valamint a potenciális támadások észlelésével és a támadók jogi-technikai elrettentésével.

III.2. A kritikus információs infrastruktúrák elleni támadások hatékony kivédése

Szükséges, hogy az ország működéséhez létfontosságú információs infrastruktúrák védelme képes legyen a támadások elhárítására megfelelő reagáló-kapacitások kialakításával.

III.3. A kritikus információs infrastruktúrák elleni támadások hatékony kezelése

Szükséges, hogy az ország működéséhez létfontosságú infrastruktúrák védelme terjedjen ki a bekövetkezett támadások hatásának csökkentésére, a helyreállítási idő minimalizálására, valamint a támadók beazonosítására, elfogására.

IV. Feladatok

IV.1. Állami koordináció

A kritikus információs infrastruktúrák védelmének alapvető eszköze a – más államokban már létrehozotthoz hasonló – kormányzati koordináció. Ennek elsődleges feladata:

- a nemzeti infokommunikációs biztonsági stratégiában foglaltak megvalósítása;
- az állami, önkormányzati és a magánszektor koordinációja és integrációja;
- a nemzeti infrastruktúra sérülékenységeinek, fenyegetettségeinek feltérképezése;
- a nemzeti infrastruktúra védelmi terv elkészítése.

Rövidtávon a fenti feladatok ellátásához szükséges koordinációt a Miniszterelnöki Hivatal Elektronikus Kormányzati Központja láthatja el, a következő szervezetek bevonásával:

- Gazdasági és Közlekedési Minisztérium;
- Igazságügyi és Rendészeti Minisztérium;
- Nemzeti Hírközlési Hatóság;
- Katasztrófavédelmi Főigazgatóság;
- Országos Rejtjelfelügyelet;
- Nemzeti Biztonsági Felügyelet.

A nemzetközi gyakorlatot alapul véve közép- és hosszútávon a kormányzati koordinációhoz szükséges egy kormányzati Információ Biztonsági Felügyelet, az úgynevezett **InfoSec Hatóság** felállítása, amely:

- gondoskodik az infokommunikációs rendszerek és eszközök – különösen a minősített adatot kezelő rendszerek és eszközök – biztonsági követelményeinek, szabványainak és ajánlásainak kidolgozásáról (honosításáról) és karbantartásáról;
- ellátja az infokommunikációs eszközök (termékek) infokommunikációs biztonsági tanúsításának felügyeletét, a tanúsítás alapján kiadja az infokommunikációs rendszerek és eszközök infokommunikációs biztonsági minősítését;
- ellátja az infokommunikációs rendszerek vagy eszközök biztonsági vizsgálatát végző személyek és szervezetek működésének engedélyezését;
- ellátja a központi közigazgatási szervek és a helyi önkormányzati közigazgatási szervek hitelesítő szolgáltató feladatát;

- felügyeli az infokommunikációs biztonsági (vészjelző és beavatkozó) központot;
- az államtitokról és a szolgálati titokról szóló törvény hatálya alá tartozó minősített adatot (továbbiakban: minősített adat) kezelő infokommunikációs rendszerek létesítését, működtetését és megszüntetését engedélyezi;
- ellátja a minősített adatot tartalmazó infokommunikációs rendszerek infokommunikációs biztonsági szempontból történő felügyeletét;
- kivizsgáltatja a közigazgatás, az állami irányítás alatt álló szervezetek, a stratégiai feladatokat ellátó szervezetek infokommunikációs rendszerei biztonságával kapcsolatos eseményeket.

IV.2. Monitorozás és reagálás

A 2001. szeptember 11-i terrortámadás során a nyugati világ felismerte, hogy szüksége van olyan központokra, amiknek a segítségével képes a lehető leggyorsabban reagálni az egyes vészhelyzetekre. Ennek alapján Magyarországon a Nemzeti Hírközlési Hatóság keretei közt megalakult az Országos Informatikai és Hírközlési Főügyelet (OIHF), illetve a kormányzat 2005-ben létrehozta a Puskás Tivadar Közalapítvány keretében a CERT-Hungary Központot, amelynek feladatául szabta a kormányzati és a kritikus információs infrastruktúrák védelmét, valamint a hálózatbiztonsági tudatosság növelését. 2006 januárjában az OIHF ügyeleti szolgálata kiszervezésre került a CERT-Hungary-hoz, azóta megtörtént a két ügyelet üzemeltetésének, ügyeleti tevékenységének és jelentési rendjének összehangolása. A CERT-Hungary akkreditált tagja a hálózatbiztonsági központok európai (TF-CSIRT) és nemzetközi (FIRST) szervezeteinek, valamint részese a kormányzati hálózatbiztonsági központokat, döntéshozókat és számítógépes bűnüldöző szerveket tömörítő International Watch and Warning szervezetnek. Emellett a CERT-Hungary tevékeny részt vállal a hazai internetes támadások elhárításában, 2006 decemberében a Bankszövetség és a Nemzeti Nyomozó Iroda felkérésére szüntette meg a magyar bankokat külföldről támadó adathalász honlapokat.

A CERT-Hungary további kormányzati támogatása javasolt, részére feladatként kell szabni:

- a kritikus infrastruktúrához tartozó elektronikus hírközlési és informatikai rendszerek védelmének támogatását hálózatbiztonsági felügyelettel és incidenskezeléssel;
- a nyílt hálózati rendszerekhez kapcsolódó rendszereket (internet) ért támadások figyelését, felismerését, és a kritikus infrastruktúrákat üzemeltetők figyelmeztetését;
- az internet biztonsági kockázatainak folyamatos figyelését és értékelését;
- a kritikus információs infrastruktúrák védelemhez kapcsolódó tevékenységének kialakítását, fejlesztését és koordinációját;
- az infokommunikációs rendszerek vagy eszközök biztonsági vizsgálatával, a kritikus infrastruktúrához tartozó infokommunikációs rendszerek biztonságával kapcsolatos oktatások, a szükséges továbbképzések és vizsgáztatások lebonyolítását;
- a terrorizmus és a számítógépes bűnözés felderítésében a nemzetbiztonsági szolgálatokkal és a rendőrséggel történő együttműködést.

Utóbbi feladat érdekében szükséges, hogy a Nemzetbiztonsági Szakszolgálat és a Nemzeti Nyomozó Iroda, valamint a CERT-Hungary operatív kapcsolatai intézményesüljenek a nemzetközi gyakorlatnak megfelelően.

IV.3. Jogszabályok, szabványok és ajánlások

IV.3.1. Jogszabályok

A jelenlegi egyenetlen és szétszórt szabályozás helyett szükséges egy egységes és összetett szabályozási rendszert kialakítani törvényi és rendeleti szinteken.

Első lépésként a Miniszterelnöki Hivatal Elektronikus Kormányzati Központját kell kijelölni a közigazgatás területén egységesen érvényes infokommunikációs biztonsági jogszabályi, technológiai követelmények meghatározására és felügyeletére, valamint az infokommunikációs technológiákkal szemben fellépő veszélyek elleni védekezésre alkalmas biztonsági szabványok, rendszerek kialakítására, tanúsítására és alkalmazására.

A titokvédelemben a papíralapú minősített adatok védelmével azonos hangsúlyt kell kapnia az infokommunikációs rendszerekben kezelt minősített adatok védelmének. A védelmi előírásoknak összhangban kell lenniük a NATO, az EU, az EURATOM és a NYEU titokvédelmi előírásaival és elvárásaival.

Rendelkezni kell továbbá az infokommunikációs rendszerek, eszközök biztonsági vizsgálatainak szabályairól, az állami irányítás és felügyelet – az EU irányelveivel összhangban történő – megoldásáról.

IV.3.2.Szabványok és ajánlások

A nemzetközi szervezetek által kidolgozott szabványok, standardok átvétele által a nemzetközi szinten kidolgozott és használt infokommunikációs biztonsági értékelési, minősítési rendszerek bekerülhetnek a magyar szabályozás rendszerbe, a külföldön elvégzett értékelés, minősítés értelmezhető, alkalmazható lesz Magyarországon is.

A kritikus infrastruktúrához tartozó infokommunikációs rendszerek esetében törekedni kell arra, hogy értékelt informatikai termékeket és rendszereket alkalmazzanak. Ehhez vagy az ISO/IEC 15408 (Common Criteria) szerinti tanúsítvánnyal rendelkező informatikai termékek beszerzése és felhasználása szükséges (az ilyen termékek további értékelésére nincs szükség), vagy amennyiben az adott termékkörben nincs az ISO/IEC 15408 szerinti értékelés, de biztonsági szempontból értékelt termék használata indokolt, úgy azt egyszerűsített eljárás, a Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) keretében is értékelni lehessen. Ezért szükséges az ISO/IEC 15408 (Common Criteria) szabvány szerinti tanúsítványok hazai kibocsátásának lehetőségének megteremtése.

A kritikus információs infrastruktúrákat üzemeltető szervezetek kapcsán szükséges, hogy a felhasználók világosan megfogalmazhassák az elvárásaikat a fejlesztés, üzemeltetés során. Ehhez az ISO/IEC 27000 nemzetközi szabványsorozatra épülő irányítási és követelményrendszer, a Magyar Informatikai Biztonság Irányítási Keretrendszer (MIBIK) bevezetése alkalmat ad. Az egységes elveken nyugvó előírások alapján elkészíthetők a különböző szervezeteknél az informatikai biztonság alapdokumentumai (az információbiztonsági politika, az infokommunikációs biztonsági stratégia és az Infokommunikációs Biztonsági Szabályzat). Emellett a keretrendszer segítséget ad a biztonságos működéshez szükséges szervezeti struktúra, a személyi, a fizikai és az infokommunikációs védelem kialakításához és ellenőrzéséhez.

IV.4. Az informatikai rendszerekbe vetett bizalom erősítése, az információbiztonsági tudatosság és ismeretek fejlesztése

A kritikus információs infrastruktúrák védelme során figyelembe kell venni azt a tényt, hogy biztonsági előírásaik csak akkor hatékonyak, ha felhasználóik alkalmazzák őket. Ezért fontos cél, hogy minden szereplőben tudatosuljanak a támadások korán felismerhető jelei és az eredményes támadások súlyossága. Folyamatossá kell tenni a szakemberek számára a biztonsági továbbképzéseket, valamint az egyéni felhasználó számára a felvilágosítást, valamint az infokommunikációs biztonsággal kapcsolatos ismeretek oktatását.

IV.5. A nemzetközi szövetségi rendszer használata és fejlesztése, a hazai üzleti, civil és akadémiai szféra bevonása

A kritikus információs infrastruktúrák védelmi feladatainak ellátását a kritikus információs infrastruktúrák nemzetközi beágyazottsága és valamint magántulajdon túlsúlya együttesen befolyásolja. Ezért elengedhetetlen, hogy a védelem kialakításánál a hazai üzleti, civil és akadémiai szféra bevonásra kerüljön, továbbá a kritikus információs infrastruktúrák védelmére szakosodott nemzetközi szervezetekben Magyarország aktívan vegyen részt.

Felhasznált irodalom

[1] 2073/2004. (IV. 15.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról

[2] MUHA Lajos: *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme*, doktori (Phd) értekezés – Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskola, tudományos vezető: Dr. KOVÁCS László mérnök őrnagy, 2007.

[3] GERENCSÉR András: *Informatikai és információvédelmi nemzeti biztonsági stratégia* – előadás az Információs Társadalom Koordinációs Tárcaközi Bizottság Informatikai Biztonsági Albizottság, Budapest 2005. 02. 28-i ülésén http://www.itktb.hu/Resource.aspx?ResourceID=docstorefile&f=899&t=stored

[4] Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 12. számú ajánlása – BODLAKI Ákos-CSERNAY Andor-MÁTYÁS Péter-MUHA Lajos-PAPP György-VADÁSZ Dezső: *Informatikai Rendszerek Biztonsági Követelményei* – Budapest, 1996.