Dr. Haig Zsolt mk. alezredes, egyetemi docens
ZMNE, BJKMK, Informatikai Tanszék
haig.zsolt@zmne.hu

AZ INFORMÁCIÓBIZTONSÁG KOMPLEX ÉRTELMEZÉSE

Bevezetés

Napjainkban az információs társadalomnak köszönhetően jelentős mértékben megnövekedett az információ értéke, jelentősége. Minden eddiginél fontosabbá vált az információ megszerzése, tárolása, és hatékony felhasználása. Ezzel párhuzamosan pedig törvényszerűen megjelentek az olyan típusú tevékenységek amelyek az információhoz való hozzáférés és felhasználás akadályozására, esetleg tönkretételére irányulnak. Ezért napjainkban egyre markánsabban jelentkezik az igény az információ megóvására, hatékony védelmére. Ezt láthatjuk és tapasztalhatjuk is, hiszen az információbiztonság mint kifejezés és tevékenységi forma teljes mértékben bekerült a szakmai köztudatba.

Ugyanakkor a szakmai közvélemény az információbiztonságot kizárólag csak az informatikai rendszerekre, számítógép-hálózatokra értelmezi, ami e problémakör jelentős leszűkítését jelenti. Jelen cikk megkísérli ráirányítani a figyelmet az információbiztonság egy komplexebb megközelítésére, vagyis annak bizonyítására, hogy **az információbiztonság nem egyenlő az informatikai biztonsággal.**

I. Az információs társadalom működésének korlátozása

A 21. században a világ fejlett országai az információs társadalom kiépítésén fáradoznak. E társadalom néhány országban már kiépült, máshol pedig igen jelentős erőfeszítések zajlanak e téren. Magyarország is ez utóbbiak közé sorolható.

Az információs társadalom kiépítését alapvetően a megfelelő színvonalú információs technológia teszi lehetővé. Korszerű információtechnológiára épülő információs infrastruktúrák nélkül az információs társadalom működésképtelen. De abban az esetben is működésképtelen, illetve működési zavarokkal küszködhet, ha e rendszereket valamilyen ártó szándékú behatás éri. Ezért amellett, hogy e rendszereket működtetjük, szavatolni kell megbízható működésüket is.

Az információs társadalom működésének alapja az infokommunikációs rendszereken alapuló információs infrastruktúrák egymásba kapcsolódó komplex rendszere. A rendszerek komplexitását bizonyítja, hogy a távközlési, informatikai rendszerek, a hozzájuk kapcsolódó távérzékelő, távfelügyeleti, navigációs rendszerekkel, szenzorhálózatokkal és más elektronikai rendszerekkel egységes rendszert képeznek, ami által képesek teljes hatékonysággal működni. Ez azt jelenti, hogy az infokommunikációs rendszerek jóval többet jelentenek, mint csak az informatikai és távközlési rendszerek konvergenciájából kialakuló rendszerek. Ebbe beletartoznak mindazon rendszerek is, melyek az érzékelés, irányítás, vezérlés funkcióit látják el. Így pl. e kategóriába sorolhatók azok a repülőtéri leszállító és irányító rendszerek is, amelyek a távközlési rendszereken és a számítógép-hálózatokon keresztül csatlakoznak más rendszerekhez.

Ennek megfelelően igen korszerű, igen fejlett információtechnológián alapuló infokommunikációs rendszerekkel látják el a különböző kormányzati, gazdálkodó, védelmi szervezeteket, intézményeket, illetve a vállalatokat. Amennyiben e szervek ezeket az

információs rendszereket megfelelően tudják működtetni, ki tudják használni a bennük rejlő lehetőségeket, és ugyanakkor a biztonságos működtetésüket is meg tudják teremteni, akkor ez egy igen komoly erősokszorozó, hatásnövelő képesség-javító és integráló hatású tényezővé válik.

Az információs társadalom szorosan kapcsolódik és függ a funkcionális információs infrastruktúráktól [1] (pl. távközlő hálózatok, számítógép-hálózatok, távvezérlő rendszerek), melyek tevékenysége viszont nem lehetséges a támogató infrastruktúrák [2] (pl. villamos energiaellátó rendszerek) hatékony működése nélkül. Ebből következik, hogy ha az infrastruktúrarendszer bármely csoportját támadás éri, az közvetlenül vagy közvetve negatívan befolyásolja a másik működését is. Ez az információs társadalom biztonsága szempontjából azt jelenti, hogy a biztonságot fenyegető veszélyek nemcsak a funkcionális infrastruktúrákon keresztül jelentkeznek, hanem az azt támogató infrastruktúrákon keresztül is.

Kijelenthetjük tehát, hogy az infrastruktúrák között kölcsönös függőség áll fenn. A támogató információs infrastruktúrákon keresztül az információs társadalom funkcionális információs infrastruktúráinak működését károsan lehet befolyásolni (zavarni, korlátozni, megszüntetni), azon keresztül pedig:

- az információs társadalom információs és vezetési működési rendjére (minőségére, harmóniájára, dinamikus egyensúlyára);
- vezetési rendszerére (a vezetés integrációjára, annak szilárdságára és minőségére);
- a vezetés struktúrájára (szervezettségi fokára);
- a belső és külső kommunikációra és végezetül
- az adott szervezet operatív vezethetőségére lehet igen komoly, negatív hatást gyakorolni. **[1]**

Ennek érdekében igen fokozott erőfeszítések zajlanak az információ megszerzéséért, birtoklásáért, illetve a minél hatékonyabb felhasználásáért. Ebben a kérdésben sokan odáig merészkednek, hogy adott esetben illegális információszerző vagy információs támadási módszereket sem tartanak elképzelhetetlennek alkalmazni, annak érdekében, hogy a saját rendszerük működése még hatékonyabb legyen. A legegyszerűbb példa erre, az ipari kémkedés, amikor olyan kutatás-fejlesztési és gyártási adatokhoz, információkhoz jutnak, amelyet felhasználva korábban tudnak különböző termékeket piacra dobni, és ezáltal jelentős előnyre és profitra szert tenni a versenytársakkal szemben. Ez a fajta tevékenység, az információs technológia megjelenésével és annak a fokozott alkalmazásával jelentős mértékben kibővül.

Abból adódóan, hogy az említett nagy integráltságú infokommunikációs rendszerek rendkívüli mértékben fejlettek, és globálisan hozzáférhetőek, meg kell állapítanunk, hogy ezzel párhuzamosan és ezzel egyenes arányban növekszik e rendszerek fenyegetettsége és ezáltal a sebezhetősége is. A fenyegetések motiváló tényezői különböző politikai, gazdasági, pénzügyi, katonai, szociális, kulturális, ipari, etnikai, vallási, regionális vagy egyéni célok elérése lehet. Az infokommunikációs rendszerek elleni fenyegetések formái és szintjei, a konfliktus helyzetek, a technikai lehetőségek, és a motivációk szerint változhatnak.

---

[1] A funkcionális információs infrastruktúrák fizikailag lehetővé teszik a társadalom valamilyen információs funkciójának zavartalan működését, vagyis információs alapszolgáltatásokat végeznek.

[2] A támogató információs infrastruktúrák létrehozzák, és folyamatosan biztosítják a funkcionális információs infrastruktúrák zavartalan működéséhez és fejlődéséhez szükséges szellemi és anyagi alapokat, valamint támogató háttereket

Jelentőségüket tekintve ezek a veszélyforrások, illetve az általuk adott esetben okozott károk nagysága nagyon sok esetben nemcsak egy infokommunikációs rendszer területén, hanem – mivel az infokommunikációs rendszerek maguk is a globális, regionális, vagy szub-regionális rendszerek szerves részét képezik – 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.

A „jól megválasztott" támadás, amely egy infokommunikációs rendszer ellen irányul akár az egész ország, vagy akár egy szub-regionális infokommunikációs rendszer sérüléséhez, vagy akár teljes leálláshoz vezethet. Mivel a gazdasági élet szereplői – a termelő vállalatok, a kereskedelem, a tőzsde, stb. – napi működéséhez sok esetben elengedhetetlenek egyes infokommunikációs rendszerek, ezért ezek támadásával, időszakos bénításával, működésképtelenné tételével, vagy akár végleges kiiktatásával igen nagy anyagi károk is előidézhetők. [1]

Az információs társadalom infokommunikációs rendszerei elleni fenyegetések a következők lehetnek:

- illetéktelen hozzáférés az információkhoz, vagy illetéktelen adatbevitel;
- rosszindulatú szoftverek bevitele a rendszerbe, ezáltal megváltoztatva, vagy lehetetlenné téve annak működését. Ezek a szoftverek különböző vírusok, „logikai bombák" és szoftverek lehetnek, melyek a védelmi programokat (tűzfalakat, víruskeresőket) kikerülve kerülnek a rendszerbe;
- rosszindulatú szoftverek útján az adatbázis lerontása, módosítása, felhasználhatatlanná tétele;
- elektronikai felderítés útján az infokommunikációs rendszer adatainak megszerzése;
- elektronikai támadások, úgymint elektronikai zavarások, hamis jelkisugárzások vagy elektromágneses impulzusok által generált robbantások végrehajtása. Elektronikai zavarokkal vagy megtévesztésekkel egyaránt támadhatók a katonai és a polgári kommunikációs rendszerek. Mind a kommunikációs rendszerek, mind a felderítő eszközök különösen érzékenyek az elektromágneses impulzusok káros hatásaira, amelyeket napjainkban nagy energiájú elektromágneses impulzus fegyverekkel is előállíthatnak;
- a katonai vezetési rendszerek, kommunikációs rendszerek, fegyverirányító rendszerek és a katonai célokra felhasználható polgári rendszerek elemeinek fizikai megsemmisítése, pusztítása. A felhasználható fegyverek skálája a terroristák által alkalmazott bombáktól a tüzérség– és rakéták alkalmazásán keresztül, a közvetlen légi csapásokig terjedhet. [2]

A fenyegetések származhatnak egyes személyektől, jogosulatlan felhasználóktól, terroristáktól, különböző nemzeti szervezetektől, külföldi hírszerző szolgálatoktól vagy akár katonai szervezetektől is. Az infokommunikációs rendszer elleni tevékenység eredetét nehéz azonosítani, mivel e csoportok között a határok elmosódnak, pl. egy illetéktelen felhasználói behatolásnak látszó tevékenység valójában származhat egy külföldi hírszerző szolgálattól is. [3] A támadók körét vizsgálva megállapíthatjuk, hogy pl. a jogosulatlan felhasználók a támadó eszközök széles skálájából csak egynéhányat vesznek igénybe, és azok is a kevésbé agresszív támadási módszerek közé tartoznak. Nem így a terroristák, akik a legpuhább támadó

módszerektől kezdve a pusztításig bármilyen információs támadást alkalmazhatnak. Ezért napjainkra igen nagy veszélyt jelent az infokommunikációs rendszerek terroristák általi elérésének lehetősége, és az un. „cyber-hadviselési" módszerek alkalmazása.

A konfliktusok szintje általában kifejezi az infokommunikációs rendszer elleni ellenséges tevékenység érdeklődési körét és mértékét. Békeidőben a számítógép-hálózatokba való illetéktelen behatolás és a különböző passzív eszközökkel végzett elektronikai felderítés a leggyakoribb információs tevékenység, mert ezáltal képesek kipróbálni az infokommunikációs rendszer gyenge pontjait, felmérni a sebezhetőségét. Amint a válság a nyilvánvaló konfliktus helyzet vagy háború irányába mozdul el, az infokommunikációs rendszerek ellen több közvetlen támadással lehet számolni. Az intenzív katonai cselekmények kibontakozását és a katonai műveletek megkezdését rendszerint összehangolt információs támadások előzik meg, illetve vezetik be. [3]

Ha az információs társadalom működésének korlátozásáról beszélünk, akkor azt is hangsúlyoznunk kell, hogy e támadások nem pusztán csak technikai, technológiai megközelítésben értelmezhetők. Ennél jóval komplexebbek e tevékenységek, amelyek egymásután vagy egymással párhuzamosan, egyszerre több színtéren, dimenzióban realizálódhatnak. A komplex információs támadás – és ebből adódóan a komplex védelem is – céljai elérése érdekében fizikai-, információs- és tudati – vagyis az emberi felfogóképesség és megértés – dimenzióiban fejti ki hatásait.

A fizikai dimenzióban folytatott információs tevékenységek a különböző információs infrastruktúrák, infokommunikációs rendszerek elemei elleni ún. „kemény típusú" („Hard Kill") támadásokat illetve azok fizikai védelmét jelentik.

Az információs dimenzióban folytatott információs tevékenységek a különböző információs folyamatok, adatszerzés, adatfeldolgozás, kommunikáció, stb. többnyire elektronikus úton való „lágy típusú" („Soft Kill") támadását jelenti annak érdekében, hogy a célpontokra való közvetlen pusztító, romboló fizikai ráhatás nélkül közvetlenül befolyásoljuk azokat. Másik oldalról ide tartozik a másik fél saját információs folyamatainkra irányuló hasonló támadásának megakadályozása is.

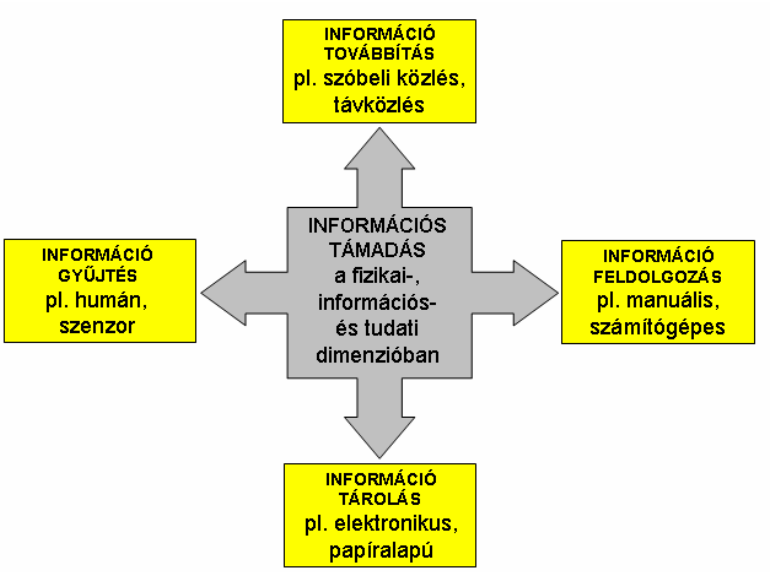
A tudati dimenzióban megvalósuló információs tevékenységek közvetlenül az emberi gondolkodást – észlelést, érzékelést, értelmezést, véleményt, vélekedést – veszik célba valós, csúsztatott vagy hamis üzenetekkel, amelyeket többnyire elektronikus és nyomtatott médián keresztül vagy közvetlen beszéd formájában továbbítanak. [4]

Ez alapján egyértelműen kitűnik, hogy ha az információs társdalom működésének korlátozása vagy akadályozása a cél, akkor az a komplex információs infrastruktúrák (számítógép-hálózatok, távközlő hálózatok, műsorszóró hálózatok, távirányító rendszerek, légi irányító rendszerek, navigációs rendszerek, stb.) elleni összehangolt támadássorozattal valósulhat meg az említett három – a fizikai, az információs, és a tudati – dimenzióban. Látható tehát, hogy e tevékenységek nem csupán az információs infrastruktúra egy szegmense ellen irányulnak, pl. csak a számítógép-hálózatok ellen. Így ez azt is jelenti, hogy a védelem megtervezése, megszervezése és kivitelezése is e három dimenzióban kell, hogy megvalósuljon. Vagyis az egyirányú információbiztonság helyett csakis a komplex információbiztonság megvalósítása vezethet eredményre.

A továbbiakban – egy másik megközelítésben – vizsgáljuk meg egy infokommunikációs rendszer támadhatóságát a funkcionális területeken keresztül. Egy infokommunikációs rendszer alapvetően az alábbi négy funkcionális területen folytat információs tevékenységet:

- információgyűjtés (humán vagy szenzor alapú);

- információtovábbítás (szóbeli közlés vagy távközlés);
- információfeldolgozás (manuális vagy számítógépes);
- információtárolás (papíralapú vagy elektronikus). (1. sz.ábra)



1. sz. ábra: Információs támadási felületek

Ha e négy funkcionális területet a támadhatóság szempontjából elemezzük, akkor szintén megállapíthatjuk, hogy a támadó félnek jó lehetőségei vannak beavatkozni a folyamatokba mind három dimenzióban, mind a négy területen. Támadás érhet:

- egy szenzorhálózatot (pl. elektronikai zavarás útján), amellyel a döntéshez szükséges fontos információk megszerzését lehet akadályozni;
- a távközlési hálózatot (felderítés vagy zavarás útján) amivel az információ továbbítását lehet akadályozni vagy a továbbított információhoz lehet hozzáférni;
- a számítógép-hálózatot, ahol különböző rosszindulatú programokkal szintén adatokhoz lehet hozzáférni vagy korlátozni lehet a feldolgozási folyamatot;
- az adattároló rendszert – mely napjainkban már számítógépes adattárolókat jelent – ahol szintén különböző programokkal hamis adatokat lehet bevinni vagy módosítani, illetve tönkre tenni a tárolt adatbázist.

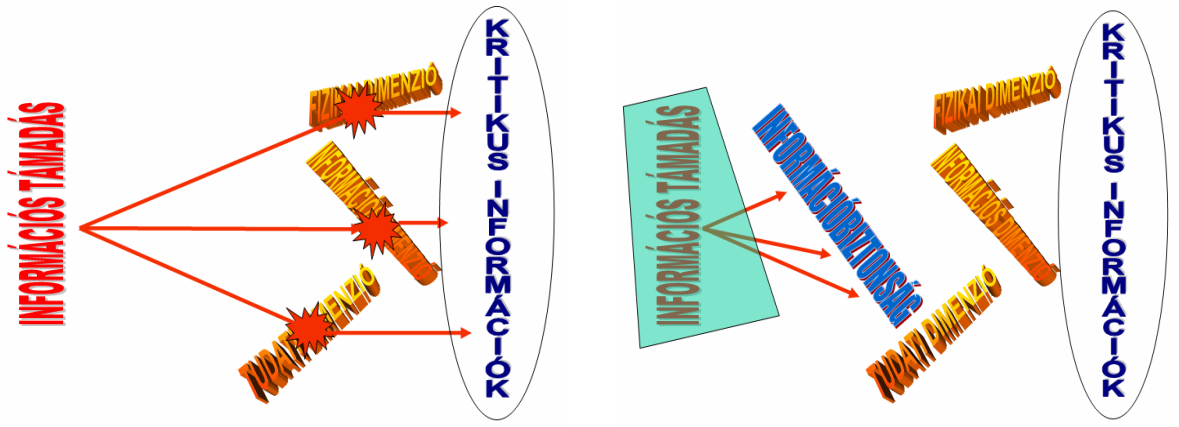
A fentiek alapján szintén látható, hogy a támadó a céljait nem csak és kimondottan az informatikai rendszer támadásával tudja elérni. Különböző részcélok elérhetők csak egy-egy dimenzióban megvalósuló és csak egy-egy funkcionális terület ellen irányuló támadással is. De amennyiben a támadó az egész rendszert kívánja támadni annak érdekében, hogy jelentős zavarokat idézzen elő a társadalom működési folyamataiban, akkor a megoldás a komplex támadási formák alkalmazásában rejlik. Ezért nem elégedhetünk meg az információbiztonság leszűkített értelmezésével, vagyis csak az informatikai rendszerre való értelmezésével, mivel itt láthatóan többről van szó.

2. A komplex információbiztonság

Az előzőekben leírtak alapján tehát ha az információs társadalom információvédelméről beszélünk, akkor az alatt mindenképpen a három dimenzióban megvalósuló komplex információbiztonságot kell értenünk. A komplex információbiztonság tehát nem egyenlő az

informatikai biztonsággal, annál jóval több és komplexebb, bonyolultabb tervezési, szervezési és végrehajtási folyamat.

Komplex és integrált védelmet kell megvalósítanunk, ami azt jelenti, hogy azokat a kritikus információkat[3] kell megvédenünk, amihez a másik fél a fizikai, információs és a tudati dimenzióban – megfelelő védelem hiányában – hozzáférhet, azt felhasználhatja a saját döntési folyamatiban, vagy esetleg tönkreteheti, és ezáltal a saját döntési folyamatainkat akadályozhatja. A megoldás, ha ezeket a kritikus információkat elrejtjük a másik fél elől, vagy megakadályozzuk, hogy hozzájuk férjenek. Erre alkalmasak a komplex információbiztonsági rendszabályok, megoldások. (2. sz. ábra) A komplex információbiztonság területén tehát olyan megoldásokat kell keresnünk, amelyek az információs infrastruktúrák és az infokommunikációs rendszerek teljes vertikumát, teljes spektrumát lefedik a biztonság oldaláról. Ezáltal biztosítható csak az információs sértetlenség, a fenyegetettség és sebezhetőség csökkentése.



Védelem nélkül

Komplex információbiztonság alkalmazásával

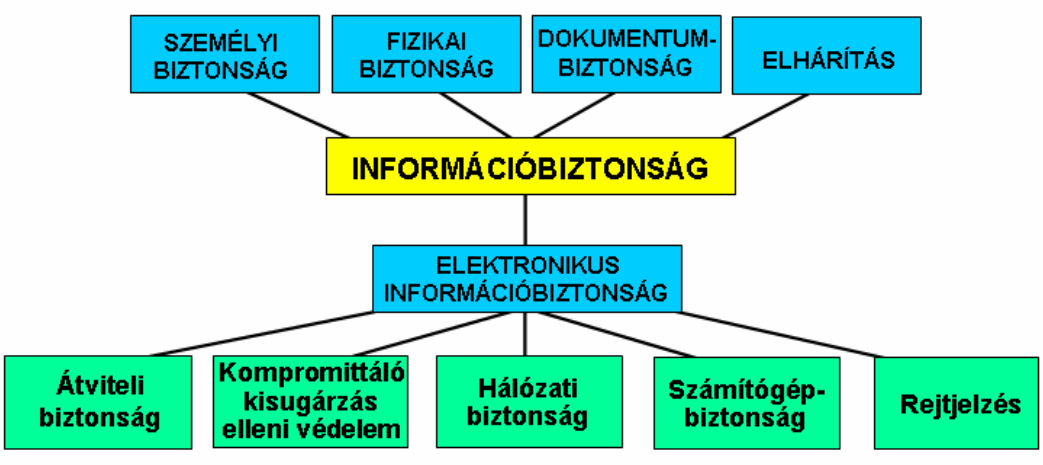
2. sz. ábra: Komplex és integrált védelem

Az információs társadalom információbiztonsága szempontjából tehát a fő cél a kritikus információk megóvása. Ezt a célt számos egymással összefüggő és egymáshoz kapcsolódó, összehangolt rendszabállyal, eljárással lehet elérni. A kritikus információkhoz való hozzáférés megakadályozható olyan tevékenységekkel, intézkedésekkel és módszerekkel, mint a tevékenységek folyamatos figyelemmel kísérése, vagy az információs rendszerek elleni tevékenységek kiértékelése. Ezeken kívül – a teljesség igénye nélkül – igen sok más biztonsági komponens, védelmi megoldás is alkalmazható az információbiztonság területén. Ezek a következők:

- a személyi biztonság;
- az elektronikus információbiztonság;
- a fizikai biztonság;
- a dokumentumbiztonság;

[3] A kritikus információk azok a saját szándékokra, képességekre, tevékenységekre vonatkozó fontos információk, amelyek a másik fél számára feltétlenül szükségesek saját tevékenységük hatékony tervezéséhez és végrehajtásához.

- az elhárítás vagy felderítés elleni tevékenység. (3. sz. ábra)



3. sz. ábra: A komplex információbiztonság elemei

A személyi biztonság magába foglalja a felforgató tevékenység és a terrorista akciók veszélyének felismerését, a mozgási lehetőségek korlátozását. Az információhoz való hozzáférés szempontjából is értelmezhető a személyi biztonság, vagyis, hogy a minősített információ csak olyan személynek juthat birtokába, aki megfelelő szintű személyi biztonsági követelményeknek igazoltan megfelel, illetve az adott minősítésű információ megismerése számára hivatalos célból szükséges. A személyi biztonság megteremtésének egyik legfontosabb eljárása a nemzetbiztonsági ellenőrzés.

Az elektronikus információbiztonság (INFOSEC[4]) a távközlési és informatikai, valamint egyéb elektronikus rendszerekben és támogató infrastruktúráikban alkalmazott rendszabályok összessége, amelyek védelmet nyújtanak az előállított, feldolgozott, tárolt, továbbított és megjelenített információk bizalmasságának[5], sértetlenségének[6] és rendelkezésre állásának[7] véletlen, vagy szándékos csökkenése ellen.

Az elektronikus információbiztonság területei:

- az átviteli biztonság (TRANSEC[8]);
- a kompromittáló kisugárzás elleni védelem (EMSEC[9]);
- a rejtjelzési biztonság (CRYPTOSEC[10]);
- a számítógép biztonság (COMPSEC[11]) és
- a hálózati biztonság (NETSEC[12]).

---

[4] Information Security
[5] A bizalmasság (Confidentiality) azt jelenti, hogy az adatok nem fedhetők fel illetéktelen személyek vagy alkalmazások számára, illetve a kommunikációs és informatikai csatornákat nem lehet átirányítani.
[6] A sértetlenség (Integrity) biztosítja, hogy a kezelt információkat jogosulatlan személy, vagy művelet által nem lehet észrevétlenül módosítani, megsemmisíteni.
[7] A rendelkezésre állás (Availability) olyan rendszabályok és eszközök alkalmazását jelenti, amelyek biztosítják, hogy szándékos támadás, véletlen esemény, vagy egyéb körülmények ellenére is, a jogosultak hozzáférjenek az érzékeny, vagy kritikus információkhoz.
[8] Transmission Security
[9] Emanations Security
[10] Cryptographic Security
[11] Computer Security
[12] Network Security

Az átviteli biztonság olyan rendszabályok által előidézett állapot az információátvitel védelme érdekében, amely meghiúsítja az átviteli folyamatban történő bármilyen illetéktelen beavatkozást. Ez azt jelenti, hogy e rendszabályok betartása mellett a továbbított információ megváltoztatása, törlése, az átviteli csatorna átirányítása, vagy üzemeltetési paramétereinek megváltoztatása jelentősen megnehezül, vagy lehetetlenné válik.

A kompromittáló kisugárzás elleni védelem alatt olyan aktív és passzív rendszabályok, eszközök alkalmazását kell érteni, amelyek célja az elektronikai eszközök, berendezések másodlagos sugárzása következtében kialakuló vezetett (kábeleken megjelenő) vagy sugárzott elektromágneses energia elemzése során, az információhoz való illetéktelen hozzáférés megakadályozása.

A rejtjelzés olyan tevékenység, eljárás, amelynek során valamely információt abból a célból alakítanak át, hogy annak eredeti állapota a megismerésére törekvő illetéktelenek számára rejtve maradjon. A rejtjelzés az egyik legrégebbi információ titkosítási forma. A rejtjelzés részét képezi a rejtjelzett információ eredetivé való visszaállítása is.

A számítógép- és hálózati biztonság az önálló, vagy hálózatba kötött gépek, és a hálózat szolgáltatásainak védettségét jelenti a szolgáltatások csökkenése, vagy megakadályozása, valamint a kezelt információk illetéktelen megismerése, megváltoztatása, vagy megsemmisítése ellen. Természetesen e biztonsági terület tartalmazza a hálózatok összekapcsolásának védelmi feladatait is. Az elektronikus információ biztonságot a kockázatok folyamatos elemzése, a kialakított védelmi rendszer jóváhagyása/akkreditálása, a feladatok írásban történő szabályozása révén, és az időszakosan ismétlődő ellenőrzési rendszeren keresztül kell felügyelni. Az információs társadalomban az elektronikus adatforgalom jelentős megnövekedésével az elektronikus információ biztonság kiemelt szerepet kap.

A fizikai biztonság azon rendszabályok és tényleges akadályok – sorompók, torlaszok, falak, szögesdrótok, behatolás jelzők, beléptető rendszerek stb. – összessége, amelyek megfosztják az illetékteleneket a minősített, kritikus információkhoz, dokumentumokhoz, eszközökhöz való hozzáféréstől, a tiltott bázisokra vagy tiltott körzetbe történő belépési lehetőségektől, és meghiúsítják vagy megakadályozzák a fizikai támadást. Jelentőségük a terrorista támadások gyakoribbá válásával jelentősen megnő.

A dokumentumbiztonság a titokvédelem tágabb értelmezése, amely azt jelenti, hogy az összes dokumentumot minősítésének, érzékenységének, vagyis titkossági osztályba sorolásának megfelelően kell védeni. Az érzékeny adatokat tartalmazó dokumentumokhoz való hozzáférés azon körre kell, hogy korlátozódjon, akik számára feltétlenül szükséges, hogy annak tartalmát megismerjék. A dokumentumbiztonság közvetlen módon kapcsolódik az elektronikus információ biztonsághoz, hiszen valamennyi elektronikus adathordozó egyben dokumentumnak is minősül. [5]

A felsorolt területek mindegyike igen fontos részterülete az információbiztonság megteremtésének. Mint látható mindegyik az információs tevékenységek egy-egy igen fontos területével foglalkozik, és ajánl megoldásokat a biztonság megteremtéséhez. A társadalom információbiztonságát azonban csak az említettek együtt, egymással összehangolt, koordinált alkalmazása tudja biztosítani. Csak a különböző információvédelmi megoldások komplex alkalmazása képes megakadályozni, vagy nagymértékben csökkenteni a különböző információs támadások hatásait.

Összegzés

A különböző információs támadások minden esetben a társadalom funkcionális és támogató információs infrastruktúrái ellen irányulnak. Az infrastruktúrákon belül lévő különböző infokommunikációs rendszereket vagy rendszerelemeket próbálják meg támadni, hiszen azok a leginkább hozzáférhető pontok, azokon keresztül lehet behatolni egy rendszerbe. De természetesen nem ezek az információs támadás végső célpontjai, hanem a politika, a gazdaság, a kultúra, a védelmi szféra, stb. és az itt lévő döntéshozók, akik egy adott terület vonatkozásában megfelelő döntéseket kívánnak hozni. A támadó ezt akarja megakadályozni.

Ha tehát a támadás végső célja különböző stratégiai fontosságú döntéshozatal megakadályozása, akkor az mindenképpen fontos nemzetbiztonsági kihívás, nemzetbiztonsági feladat, mind össztársadalmi szinten, mind pedig a mikrorendszerek szintjén. Hiszen lehetnek olyan vállalatok, cégek, intézmények, amelyeknek a támadása – a rendszerek összekapcsolódása, globalitása következtében – igen komoly lavinát indíthat el akár gazdasági vagy politikai színtéren vagy egyéb más területeken, ami egy ország teljes biztonságát veszélyeztetheti.

Tehát a kiinduló alaphipotézis alapján, megállapíthatjuk, hogy az információbiztonság jóval szélesebb területet fed le, mint az informatikai biztonság. Össztársadalmi szinten mindenképpen téves az a felfogás, és helytelen következtetésekhez vezet, ha az információbiztonságot leegyszerűsítve csak a számítógépek és a számítógép-hálózat védelme szempontjából értelmezzük.

Felhasznált irodalom:

[1] Dr. Haig, Zsolt–Kovács, László–Dr. Makkay, Imre–Dr. Seebauer, Imre–Dr. Vass, Sándor–Ványa, László: Az információs társadalom veszélyforrásai. A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban. Tanulmány. MEH Informatikai Kormánybiztosság, 2002

[2] FM 100-6, Information Operations. Department of the Army, Washington DC, 1996.

[3] Haig, Zsolt–Várhegyi, István: A vezetési hadviselés alapjai. Egyetemi jegyzet, ZMNE, Budapest, 2000.

[4] Waltz, Edward: Information Warfare Principles and Operaions. Artech House, Inc. Boston, London. 1998. ISBN: 0-89006-511-X.

[5] Haig Zsolt, Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005. 286 p. ISBN: 963-327-391-9