Közszolgálati Nemzetközi Képzési Központ

Információbiztonság

Dr. Haig Zsolt

Oktatási segédanyag

Nemzeti Közszolgálati Egyetem 2013.

Nemzeti Közszolgálati Egyetem
Postacím: 1581 Budapest, Pf.: 15.
Cím: 1101 Bp., Hungária krt. 9-11.,
Telefon: +36(1)432-9000
Web: www.uni-nke.hu

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Tartalomjegyzék

BEVEZETŐ

Az információs társadalom nagyon fejlett, nagyon hatékony, ugyanakkor meglehetősen sebezhető társadalmi és gazdasági rendszer. E társadalom alapvető éltető eleme az információ, melynek mennyisége és minősége létfontosságú a felhasználók számára. Éppen ezért kíméletlen harc folyik az információ gyors megszerzéséért, biztonságos tárolásáért és mind hatékonyabb felhasználásáért. Az optimális mennyiségű és minőségű információ birtoklása jelentős mértékben járulhat hozzá a gazdasági haszon növeléséhez, az esetlegesen bekövetkező károk elhárításához, valamint két fél közötti verseny- esetleg konfliktushelyzetben a másik féllel szembeni fölény kialakításához. Mindezek alapján kijelenthető, hogy az információs társadalomban az egyének, gazdálkodó szervezetek, illetve a kormányzati szervek jelentős információfüggőségben szenvednek. Ez az információfüggőség egyúttal az információs technológiától való függőséget is jelenti, vagyis erősen függenek az információs környezet fejlett, ám sebezhető információs infrastruktúráitól, mint például a távközlési hálózatoktól és a számítógép-hálózatoktól.

Ezt felismerve 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.

Az információs társadalom egyik legjelentősebb kihívása a biztonság megteremtése, amely túlmutat az eddig ismert biztonságfelfogás dimenzióin. A klasszikus biztonságdimenziók, mint a politikai-, gazdasági-, katonai-, környezeti- és a társadalmi dimenzió, mellet az információs társadalom biztonságos működtetése szükségessé teszi egy újabb biztonsági dimenzió, az információbiztonság értelmezését. Mivel az információs társadalom működése elképzelhetetlen az információtechnológia alkalmazása és az infokommunikációs rendszerek működése nélkül, így azok természetszerűleg jelen vannak a politikai, gazdasági, katonai és társadalmi életben. Ennek megfelelően az információbiztonság az előbb említett biztonságdimenziókat átfogó tényezővé vált.

A jegyzet az információs társadalom információbiztonságát tárgyalja. Bemutatja az információs társadalom információfüggőségét, osztályozza és ismerteti a komplex információs támadások fajtáit, módszereit és eszközeit, végül pedig a támadások osztályozása alapján ismerteti a védelemi megoldásokat.

I. FEJEZET

AZ INFORMÁCIÓS TÁRSADALOM KRIITIKUS INFROMÁCIÓS INFRASTRUKTÚRÁI

A 21. század óriási kihívás elé állítja társadalmunkat. Az ipari termelési korszakot egyes országokban már felváltotta, számos országban, napjainkban folyamatosan felváltja az információs termelési kor. Az ipari termelési korszakot felváltó információs termelési kor új társadalmi modellt hoz magával, amelyet információs társadalomnak nevezünk. Az információs társadalomban az információ válik az egyik legfontosabb tényezővé. Ebben a társadalomban már a mindennapi élet alapvető mozgatórugója, valamint társadalmi értéke az információ, a kommunikáció és a tudás.

Az adatok (információk) megszerzését (előállítását), tárolását, feldolgozását, továbbítását biztosító különböző elektronikai, informatikai eszközök és rendszerek közötti legátfogóbb, legmeghatározóbb jelenség ezen területek konvergenciája, amit infokommunikációs konvergenciának nevezzük. Az infokommunikációs konvergencia szerepe döntő az információs társadalom kiépítésében és fejlesztésében, mivel nem szűkül le a technológia szintjére, hanem mind szélesebb köröket von hatása alá, társadalmi jelenséggé válik. Ezt a folyamatot a digitális technológia hatalmas léptékű fejlődése váltotta ki. Az említett eszközök és rendszerek közös technológiai alapja kialakult.

A digitális technológia elterjedésével megkezdődött a számítógép, a vezetékes és vezeték nélküli távközlési eszközök, továbbá az elektronikus média műszaki közeledése, technikai konvergenciája, majd közös termékben való összeolvadása. A műszaki fejlesztések lehetővé tették az áttérést a multimédiás jeltovábbításra ugyanazon a kommunikációs csatornán. Ezáltal megvalósul a beszédhang, zene, szöveg, rajz, álló– és mozgókép egy csatornán történő továbbítása. Lehetővé vált korábban elkülönült információkezelés módok összekapcsolása és kombinálása, infokommunikációs alkalmazások és ezekre épülő vállalkozások létrejötte. Ilyen infokommunikációs alkalmazások a különféle audiovizuális/multimédia szolgáltatások, internet-alkalmazások, elektronikus tartalomszolgáltatások és tulajdonképpen az ún. információs társadalmi szolgáltatások. [1]

A világméretű infokommunikációs hálózatok megjelenése – az internet az elektronikus levelezés (E–mail, Fax, SMS, MMS) szolgáltatásokkal – megteremtették a lehetőséget az új típusú globális gazdaság, az elektronikus tőzsdék, az elektronikus pénzpiac, az elektronikus kereskedelem és más, igen fejlett társadalmi tevékenységek világméretű kialakítására. Ez a műszaki és technológiai lehetőség képezi a gazdasági globalizmus alapját. [2]

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, amelyek 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, közigazgatási, 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 társadalomban mind az egyének, mind pedig a társadalom biztonsága jelentős mértékben függ a különböző, egymással szorosan összekapcsolódó infrastruktúráktól. Ezért ha az infrastruktúrákat nemzetbiztonsági szempontból vizsgáljuk, akkor ki kell emelnünk a **kritikus infrastruktúrákat**, amelyek működése alapvető fontosságú és nélkülözhetetlen a társadalom működtetéséhez. Amennyiben ezek valamilyen beavatkozás következtében működésképtelenné válnak, az beláthatatlan következményekkel járhat az ország gazdaságára és védelmére, azaz maga az ország biztonsága kerülhet veszélybe. Természetesen a kritikus infrastruktúrák mellett és azokon belül is, külön figyelmet kell szentelnünk a **kritikus információs infrastruktúráknak**. Ezért alapvető fontosságú, hogy feltérképezzük, és pontosan behatároljuk azokat, mivel akár egy elszigetelt, akár egy összehangolt támadásnak potenciális célpontjai lehetnek. [2]

A kritikus infrastruktúrának többféle definíciója is létezik. Magyarország az Európai Unió ide vonatkozó Zöld Könyvének figyelembevételével megalkotta a 2012. évi CLXVI. törvényt, amely a kritikus infrastruktúrákat létfontosságú rendszerek és létesítményekként definiálja.

A törvény szerint *„Létfontosságú rendszerek és létesítmények alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, léte-*

sítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.

Létfontosságú rendszernek és létesítménynek minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségére, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére."[3]

Mivel a szakmai közösség körében általánosan elterjedt kifejezés a kritikus infrastruktúra, ezért e jegyzetben a továbbiakban is a fenti definíció alapján ezt a kifejezést alkalmazzuk.

Az elmúlt években több példa is rámutatott a kritikus infrastruktúrák sebezhetőségére és védelmének szükségességére. Elég, ha csak a különböző természeti katasztrófákra (földrengések, szökőár), terrorcselekményekre (World Trade Center, madridi vonatrobbantás, londoni metrórobbantás) gondolunk. Az elmúlt időszakban a különböző infrastruktúrák mindig is jó célpontjai voltak a különböző szintű és típusú támadásoknak. Amíg e támadások csak a fizikai dimenzióban valósultak meg, addig az országhatárok bizonyos védelmet jelentettek számukra. Az információs dimenzió megjelenése és egyre fokozódó előretörése, az infokommunikációs rendszerek globálissá válása azonban e viszonylagos letisztult helyzetet gyökeresen megváltoztatta. Napjainkban korlátozott erőforrások is elegendőek az infokommunikációs rendszerekre alapozott kritikus infrastruktúráink elleni támadások megtervezésére és kivitelezésére. A különböző egyéni aktivisták, jogosulatlan felhasználók és terroristák aszimmetrikus fenyegetései részben kibővítették, részben pedig felváltották a jól ismert háborús fenyegetettségeket. [5] E tekintetben kijelenthetjük, hogy a katonai és polgári természetű fenyegetések közötti hagyományos határvonal egyre inkább elmosódik.

Az információs társadalom működésének egyik meghatározó alapját képezik az infokommunikációs technológiákon alapuló információs infrastruktúrák. A kritikus infrastruktúra elemei között minden esetben megjelentek az infokommunikációs technológiák. Az infokommunikációs technológiák önálló megjelenésén túl figyelemre méltó az a tény, hogy napjainkban szinte valamennyi kritikusnak minősített, ill. minősíthető infrastruktúra nemcsak használja az infokommunikációs technológiákat, hanem egyre erősebben függ is ezektől. Az infokommunikációs technológiáktól függ az egyes kritikus infrastruktúra elemek működése és függ a kritikus infrastruktúra elemeinek együttműködése is. Az infokommunikációs technoló-

giáktól való függőség olyan mértékű, hogy azok összeomlása vagy megsemmisülése súlyos következményekkel járhat nem csak az adott infrastruktúrára, hanem más kritikus infrastruktúrákra nézve is. A kritikus információs infrastruktúra egészére nézve az egyes infrastruktúra elemek infokommunikációs technológiái egy „belső" kritikus infrastruktúrát jelentenek.

Szinte minden fajta kritikus infrastruktúrát különböző szintű és rendeltetésű infokommunikációs rendszerek vezérelnek, irányítanak és ellenőriznek. Így tehát egy ország információtechnológiára alapozott infrastruktúrája joggal nevezhető a társadalom idegrendszerének, és ennek következtében az információs infrastruktúrák, illetve azok részei is a kritikus infrastruktúrák közé sorolandók. E megállapítás szerint, pl. egy ország nyilvános mobil távközlő hálózatai, mint önmagukban is kritikus infrastruktúrák, egyben kritikus információs infrastruktúráknak is minősülnek, illetve pl. az energiaellátó rendszert irányító, vezérlő számítógép-hálózat is ez utóbbiak közé sorolandó.

Bár az információs társadalom zavartalan működésének megbontására irányuló támadások tényleges célpontjai a kritikus infrastruktúrák — hiszen ezek adják működésének alapját —, azonban az ellenük irányuló információalapú támadások és fenyegetések a különböző szintű és fontosságú infokommunikációs rendszereket érintik. Ezek a rendszerek mára a fenyegetések stratégiai célpontjaivá váltak, mivel a támadó fél kis erő- és eszközbefektetéssel igen jelentős károkat tud előidézni. Az infokommunikációs rendszerek globális jellegéből adódóan e rendszerek bárhonnan, bármikor elérhetők, és az információtechnológia vívmányait ellenük fordítva támadhatók. Miközben az informatikai és kommunikációs technológia konvergenciájából adódó közös platformok és alkalmazások lehetővé teszik az átjárhatóságot és a felhasználóbarát elterjedést, egyúttal jelentős mértékben növelhetik a kockázatokat is. Egyértelműen kijelenthető, hogy a kritikus információs infrastruktúrák közötti szoros kapcsolat jelentősen növeli az információs társadalom sebezhetőségét. Minél nagyobb e rendszerek integráltsága, komplexitása, minél kiterjedtebb a köztük lévő kapcsolatrendszer, annál nagyobb mértékben vannak kitéve az új típusú fenyegetéseknek, és ennélfogva annál erősebb a kényszer a védelem és biztonság megvalósítására. [6]

A 2012. évi CLXVI. törvény ágazati besorolása [3] alapján a kritikus információs infrastruktúrák alatt az alábbiakat értelmezhetjük:

- energiaellátó rendszerek rendszerirányító infokommunikációs hálózatai;
- infokommunikációs hálózatok;
- közlekedés szervezés és irányítás infokommunikációs hálózatai;
- vízellátást szabályzó infokommunikációs hálózatok;

- agrárgazdaság infokommunikációs hálózatai;
- egészségügyi rendszer infokommunikációs hálózatai;
- pénzügyi-gazdasági rendszer infokommunikációs hálózatai;
- ipari termelést irányító infokommunikációs hálózatok;
- jogrend - kormányzati szféra infokommunikációs hálózatai;
- közbiztonság - védelmi szféra infokommunikációs hálózatai.

Az információs társadalom információs infrastruktúráinak komplex rendszere egymásra épülő, egymást feltételező, egymást kölcsönösen támogató infrastruktúrák szövevényes hálózataiból tevődik össze. Ezt egymástól való függőségnek, interdependenciának nevezzük. Az összekapcsolódó infrastruktúrákon keresztül az esetleges üzemzavarból vagy szándékos támadásból fakadó problémák felhalmozódhatnak, váratlanabb és lényegesen súlyosabb működésbeli zavart okozhatnak az adott állam létfontosságú szolgáltatásaiban. Az infrastruktúrák összekapcsolódásai és egymástól való függőségei sérülékenyebbé teszi őket a különböző fizikai és információs támadásokkal szemben. [7] Amennyiben az infrastruktúrarendszer bármely csoportját támadás éri, az közvetlenül vagy közvetve negatívan befolyásolja a másik működését is.

II. FEJEZET
INFORMÁCIÓS TÁMADÁSOK

Az információs társadalom kritikus információs infrastruktúráit napjainkban számtalan veszély fenyegeti. Amennyiben szeretnénk ezeket kategorizálni, vagy egyáltalán csak felvázolni és csoportosítani, akkor általánosságban a következő olyan veszélytípusokat tudjuk megkülönböztetni, amelyek közvetlenül vagy közvetve fenyegetést jelenthetnek a kritikus információs infrastruktúra egészére vagy annak egyes elemeire:

- természeti katasztrófák:
  - vízkárok (közművek sérülése, árvíz, belvíz);
  - geológiai katasztrófák (földrengés, talajsüllyedés);
  - meteorológiai jellegű károk (rendkívüli erejű vihar, villámcsapás);
- civilizációs, ipari katasztrófák:
  - nukleáris balesetek (erőművi balesetek);
  - veszélyes anyagok kikerülése (gyárak, üzemek, raktárak szállítójárművek sérülése, robbanások);
  - közlekedési balesetek (közúti, vasúti jármű, repülőgép véletlen vagy szándékos becsapódása);
- fegyveres konfliktusok:
  - háborúk;
  - fegyveres csoportok támadása;
  - belső fegyveres konfliktusok, polgárháborúk, sztrájk;
- terrorizmus:
  - robbantások, támadások (állami intézmények, távvezetékek, hírközpontok, adók, légiforgalmi létesítmények, Internet szolgáltatók stb. ellen);
  - a fenti rendszereket üzemeltető kulcsfontosságú személyek kiiktatása;
  - bűnözés (adatok erőszakkal való megsemmisítése, megszerzése, irányítórendszerek befolyásolása, megbénítása);
- információalapú támadások. [7]

Mint látható, a kritikus információs infrastruktúrák elleni támadások igen szerteágazóak lehetnek. E jegyzet keretei között nem foglakozunk a különböző természeti eredetű veszélyekkel, ipari katasztrófákkal, stb. A jegyzet témájából adódóan vizsgálatunk tárgya elsősorban az információs jellegű, információalapú fenyegetések köré összpontosul.

Tekintettel napjaink információs fenyegetettségi tendenciáira, egyértelműen kijelenthetjük, hogy a támadások a célpontokat illetően két csoportra oszthatók, úgymint: az informatikai rendszerek elleni fenyegetések illetve más infokommunikációs rendszerek elleni veszélyek. Célszerűnek látszana tehát a fenyegetéseket e szerint csoportosítani, azonban ez nem elég egzakt kategorizálás, hiszen a célpontok a legtöbb esetben komplexek, átfedik egymást, azaz egy-egy rendszer többféle komponenst is takarhat. Ez az átfedés alapvetően az információtechnológiai eszközök konvergenciájából fakad.

Egy másik csoportosítási elv szerint a fenyegetés módszerei szerint célszerű kategorizálni az információs támadásokat. Eszerint az alábbi támadási módszereket különböztethetjük meg:

- számítógép-hálózati támadás;
- elektronikai felderítés;
- elektronikai támadás. [6]

2.1. Számítógép-hálózati támadás

A számítógép-hálózati támadások alapvetően kettős célt szolgálnak. Egyrészt a hálózatok felderítését, az adatokhoz való hozzáférést, másrészt pedig az adatok, információk befolyásolását, tönkretételét, a hálózatok működésének tényleges akadályozását, megbontását.

A hálózat felderítése tulajdonképpen olyan behatolást jelent a számítógépes rendszerekbe, hálózatokba, amely lehetővé teszi az adatbázisokban tárolt adatokhoz, információkhoz való hozzáférést, és azok saját célú felhasználását. A felderítés során lehetőség nyílik:

- a számítógépes hálózatok struktúrájának feltérképezésére;
- a forgalmi jellemzőik alapján hierarchikus és működési sajátosságainak feltárására;
- a hálózaton folytatott adatáramlás tartalmának regisztrálására, illetve
- az adatbázisban tárolt adatok megszerzésére, azok saját célú felhasználására.

E tevékenység során a rendszer nem sérül, és a benne tárolt adatok sem módosulnak, vagy törlődnek, viszont azok illetéktelen kezekbe kerülése jelentős veszteséget okozhat a támadást elszenvedőnek. Tehát e támadás során a rendszerben tárolt adatok bizalmassága sérül. Ezenkívül, ha figyelembe vesszük, hogy a megszerzett adatok birtokában a rendszer könnyebben támadhatóvá válik, akkor láthatjuk, hogy e tevékenység éppen olyan komoly veszélyforrás, mint a tényleges kárt okozó támadás.

A tényleges és egyértelműen észlelhető kárt okozó **hálózati támadás** olyan behatolást jelent a másik fél számítógép-hálózataiba, amelynek eredményeképpen tönkretehetők, módosíthatók, manipulálhatók, vagy hozzáférhetetlenné tehetők az adatbázisban tárolt adatok, infor-

mációk, illetve a támadás következtében maga a rendszer vagy hálózat sérül. E tevékenység a hálózatokban folyó megtévesztő, zavaró tevékenységet illetve a célobjektumok program-, és adattartalmának megváltoztatását, megsemmisítését jelenti. Ennek következtében a rendszerben tárolt adatok sérülékenysége nő, a szolgáltatások elérhetősége pedig csökken. [6]

A számítógép-hálózati támadás eszközei közé tartoznak a különböző kártékony, rosszindulatú programok, melyeket Malware[1]-eknek nevezünk. A Malware azon szoftverek gyűjtőneve, amelyek közös jellemzője, hogy anélkül jutnak a rendszerbe, hogy arra a felhasználó engedélyt adott volna. Minden olyan szoftver rosszindulatúnak minősíthető, amely nem a számítógépes rendszer vagy hálózat rendeltetésszerű működését biztosítja.

A Malware kifejezés számos rosszindulatú szoftvert takar. Napjainkban e szoftverek típusai és fajtái folyamatosan gyarapodnak, ezért egyértelmű kategorizálásuk igen nehéz. Alapvetően két nagy kategóriájukat lehet megkülönböztetni:

- a program típusú Malware-ket és
- a szöveg típusú Malware-ket.

A legismertebb program típusú Malware-k közé tartoznak a vírusok, a programférgek, a trójai programok, a rootkitek, a böngésző eltérítők, a hátsó ajtó (backdoor) programok, a keyloggerek, a spam proxyk, a spyware és az adware programok, és a sort még folytathatnánk. A szöveg típusú Malware-ek közé sorolhatók többek között a spam-ek, hoax-ok, a phishing és a pharming, amelyek szöveges információk formájában hordoznak veszélyt a rendszerre és felhasználójára.[2]

Mindegyik Malware-nek megvan a maga speciális funkciója, ami a rendszer működésének megzavarástól az adatlopásig vagy a rendszer feletti vezérlés átvételéig terjedhet. Látható, tehát, hogy az előzőekben ismertetett számítógép-hálózati támadások minden típusánál alkalmazhatók a Malware-ek. A rosszindulatú szoftverek módosíthatják a programokat, erőforrásokat foglalhatnak le, adatokat módosíthatnak, hardverhibát eredményezhetnek, eltávolításuk pedig megfelelő eszközöket, időt és energiát, egyes esetekben pedig különleges szakértelmet igényelhet.

A támadás különböző módszerei ötvözve az eszközökkel lehetővé teszik a hálózatba való behatolást, működésének akadályozását, megbontását, illetve az adatokhoz való hozzáférést. A támadó egy távoli számítógéphez és annak adataihoz egy egyszerű, egylépéses folyamattal a legritkább esetben fér hozzá. Jellemzőbb, hogy a támadóknak számos támadási mód-

[1] Malicious Softwares

[2] Részletes ismertetésüket lásd: Dr. Kovács László: Az információs terrorizmus eszköztára. Egyetemi jegyzet, ZMNE, 2008. Budapest

szert és eszközt kell kombinálniuk, hogy kikerüljék mindazokat a védelmi eljárásokat, melyeket a hálózatok biztonsága érdekében alkalmaznak. A hálózatok támadására nagyon sokféle módszer létezik, így a támadóknak csak a megfelelő szakértelemre van szükségük, hogy a támadás eszközeit a megfelelő eljárásokkal kombinálják. Íme a sokrétű támadási formák közül néhány legismertebb: sniffing; spoofing; denial of service; distributed denial of service; man-in-the-middle attack; SMTP backdoor command attack; IP address Spoofing attack; IP fragmentation attack; TCP Session High jacking; JavaScript,- applet attack; cross site scripting (XSS), és még sok más.

E jegyzet keretében a számos támadási módszer közül egy hálózati felderítésre és egy konkrét támadásra alkalmas eljárást mutatunk be röviden.

A **sniffing** (szimatolás) nem más, mint a hálózaton zajló információáramlás folyamatos nyomon követése, vagyis a hálózat felderítése. Az e célra alkalmas szoftver és hardver eszközökkel meg lehet figyelni az adatátvitel fő jellemzőit, mint pl., hogy honnan hová, milyen típusú és tartalmú adatok kerülnek továbbításra. Ezen túlmenően bizonyos típusú adatok kiszűrhetők a nagy adathalmazból, vagy e módszer alkalmazásával jelszavakhoz is hozzá lehet jutni. A lehallgató (sniffer) egy olyan program, amelyet üzenetszórásos hálózatokban alkalmazhatnak az áramló információ illetéktelen megfigyelésére, kinyerésére. A sniffer program a hálózati kártyák meghajtóját megfelelő, ún. promiscuous[3] módba állítva képes az adott médián folyó minden forgalmat megfigyelni, elemezni. Ismertebb lehallgató programok, pl. az Ethereal, vagy a tcpdump, amelyek segítségével a támadó a hálózaton átküldött jelszavakat, vagy egyéb bizalmas információkat ismerhet meg. [8]

A **Denial of Service (DoS)** támadások — ami magyarul túlterheléses támadást jelent — kiemelt jelentőséggel bírnak az internet biztonsági problémái között. A DoS támadások során a támadó célja, hogy megakadályozza a hálózat megfelelő, üzemszerű működését. Ezt úgy éri el, hogy a válaszadó rendszert hamis kérésekkel megbénítja, így az a más forrásból érkező valós kéréseket már nem tudja kiszolgálni. Ezek a támadások nehezen megelőzhetőek, és nehezen akadályozhatók meg, mivel igen nehéz annak eldöntése, hogy melyik kérés valós, és melyik nem. Ezzel szemben megvalósításuk nem túl bonyolult, mivel a támadónak csupán megfelelő mennyiségű automatizált rendszerre van szüksége, ami elégséges a cél megbénításához. [9]

[3] válogatás nélküli csomagelkapás

A DoS támadások többnyire ún. **elosztott túlterheléses támadások[4],** ahol több támadó, egy időben több végpontról, együttesen kívánja előidézni a rendszer összeomlását. A DDos támadásoknál igen gyakran olyan gépeket vesznek igénybe, amelyek nem is tudnak arról, hogy egy ilyen típusú támadás aktív részesei. Ehhez természetesen ellenőrzést kell szerezni a támadásra szolgáló számítógépek felett. Ebben az esetben egy automatizált alkalmazás felderíti az interneten lévő sebezhető számítógépeket. Ezt követően automatikusan vagy elektronikus levelekben küldött, esetleg egyes honlapok látogatásakor „összeszedett" Malware-ekkel feltelepítenek rá egy rejtett támadóprogramot. Ezzel a kiszemelt gépet „zombivá" teszik. Ez annyit jelent, hogy azokat egy „mester-gép" távolról vezérli, utasítja a kiválasztott honlap elleni támadás megkezdésére. A zombik egyenként ugyan kevés adattal dolgoznak, de együttes fellépésük hatalmas – bénító erejű – adatáramlást eredményez. Az ilyen - zombinak nevezett - számítógépek hálózatba szervezhetők, amelyekkel veszélyes támadások indíthatók. Ezeket a hálózatokat **botneteknek** nevezik. Ugyanúgy, mint a hagyományos DoS támadásokat, a DDoS akciókat is lehetséges a hálózati rétegben vagy az alkalmazási rétegben kivitelezni. [10]

Az információs rendszerek védelme gyakran olyan mértékű, hogy technikai eszközökkel nem vagy csak nagyon kis hatékonysággal lehet róluk megfelelő információhoz jutni. E probléma kiküszöbölésére terjedt el egy igen hatékony információszerzési forma, melyet a magyarra igen nehezen lefordítható Social Engineering-nek neveznek. A **Social Engineering** az emberek természetes, bizalomra való hajlamát használja ki a számítógép-hálózatokba való bejutáshoz. E tevékenység keretében a hálózat gyenge pontjaira vonatkozó adatokat, a legfontosabb jelszavakat, stb. attól a személytől szerzik meg félrevezetés, zsarolás, csalás, esetleg fenyegetés útján, aki azokat kezeli, vagy aki azokhoz hozzáfér. E tevékenység igen nagy szerepet játszik abban, hogy a támadó megkerülhesse a különböző biztonsági megoldásokat, mint pl. tűzfalakat vagy behatolás detektáló rendszereket.

2.2. Elektronikai felderítés

Az információs társadalom technológiai fejlettségéből adódóan fokozottan jelen vannak, sőt meg is sokszorozódott a számuk, azoknak az elektronikai eszközöknek, rendszereknek, amelyek potenciális adat- vagy információforrást jelentenek. Ugyanakkor – köszönhetően éppen az új technológiákban rejlő információvédelmi lehetőségeknek – rendkívüli módon megnehezült ezekből a potenciális forrásokból a közvetlenül felhasználható információ kinyerése.

[4] Distributed DoS - DDoS

Az elektronikai felderítés, mint információszerző tevékenység általában kettős céllal kerülhet végrehajtásra:

- az infokommunikációs rendszerekben tárolt és továbbított adatokhoz való hozzáférés és azok felhasználása céljából, illetve
- a hatékony támadás kivitelezéséhez szükséges célinformációk megszerzése céljából.

A kritikus információs infrastruktúrák elleni támadások hatékonysága nagymértékben függ attól, hogy a támadást elkövető tudja-e, hogy:

- az adott objektum (rendszer) fizikailag hol helyezkedik el;
- milyen a strukturális összetétele;
- milyen hardver és szoftver elemekből áll;
- milyen célú és mennyiségű adatforgalom zajlik rajta keresztül;
- vannak-e gyenge pontjai, és ha igen hol, illetve
- kik az adott információs rendszer vagy hálózat üzemeltetői, és felhasználói. [4]

Napjainkban e célra a legkülönfélébb módszerek és technikai eszközök alkalmazhatók, melyek jelentősen megnövelik, megsokszorozzák az emberi érzékelés határait. A felderítés céljára alkalmazott technikai eszközök képesek a teljes frekvenciaspektrumban adatokat gyűjteni, azokat akár automatikusan is a fúziós technológián alapuló adatfeldolgozó központokba továbbítani, ahol értékes felderítési információkat lehet nyerni belőlük. [11]

A mai korszerű infokommunikációs eszközöket alapul véve kijelenthető, hogy az elektronikus úton végzett felderítő tevékenység jelentősen képes hozzájárulni a célpontul kiszemelt objektumok és rendszerek mindenoldalú feltérképezéséhez. A frekvenciaspektrum szinte minden tartományában az adatgyűjtő szenzorok, rendszerek rendkívül széles skálájával találkozhatunk. Ezek többek között képesek a mechanikai rezgések tartományában az akusztikus, hidroakusztikus és szeizmikus rezgések detektálására; a rádiófrekvenciás tartományban a rádióhíradás felderítésére, objektumok helyének, mozgási paramétereinek meghatározására (pl. radar), illetve az optikai és az elektro-optikai tartományban (látható fény és az infra tartományban) álló és mozgó képi információk előállítására.

A korszerű **rádióelektronikai felderítő eszközök** a teljes rádiófrekvenciás sávban lehetővé teszik a különböző aktív kisugárzás elvén működő elektronikai berendezések (rádiórendszerek, radarok stb.) felfedését, lehallgatását, helymeghatározását és technikai jellemzőik kiértékelését. Napjaink korszerű, kis valószínűséggel felderíthető elektronikai eszközei (pl. frekvenciaugratásos illetve szórt spektrumú rendszerek) sem jelentenek akadályt e rendszerek számára, mivel az új generációs felderítő vevők képesek detektálni e kisugárzásokat, és meg-

határozni a sugárforrás helyét, ami az esetleges fizikai vagy elektronikai támadás végrehajtásához szükséges.

Az elektronikai felderítés céljára felhasználható eszközök jelentős része kereskedelemi forgalomban szabadon hozzáférhető és megvásárolható. Ezekkel a berendezésekkel mindazon információs rendszerről beszerezhetőek a legfontosabb adatok, amelyek valamilyen elektromágneses kisugárzó eszközt alkalmaznak működésük során.

Azon infokommunikációs rendszerek esetében, amelyek nem, vagy csak nagyon kis számban alkalmaznak elektromágneses kisugárzó eszközöket, vagy a védelmi szintjük igen magas fokú, az információk megszerzése természetszerűleg más forrásokra támaszkodik. Ilyen lehet pl. a különböző vezetékeken zajló adat vagy kommunikációs forgalom technikai eszközökkel való felderítése. Ezek az eszközök, amelyek a vezetékeken folyó elektromos jelek által keltett mágneses mezőt felhasználva indukciós módszerrel nyerik ki az információkat, szintén beszerezhetők kereskedelemi forgalomban is. [4]

A korszerű elektronikai felderítésben egyre inkább jellemzővé válik, hogy az adatokat olyan eszközökkel szerzik meg, melyek az élőerőt nem veszélyeztetik. Ezek lehetnek egyrészt különböző hordozóeszközökön kijuttatott eszközök, mint pl. a pilóta nélküli repülőeszközön elhelyezett szenzorok, illetve a felderítendő objektum körzetébe letelepített úgynevezett **felügyelet nélküli földi szenzorok.** Ez utóbbiak olyan mini– mikro– és nanoméretű érzékelő- és mérőműszerek, amelyek a környezeti méret– és állapotváltozásokat, torzulásokat, ingadozásokat stb. képesek érzékelni, mérni, és automatikus úton jelenteni. E szenzorok olyan állapotváltozásokat mérnek, mint pl.: hőváltozások, mechanikai változások, akusztikus változások, vegyi állapotváltozások, mágneses változások, elektrooptikai változások, vagy esetleg biológiai változások.

A felügyelet nélküli szenzorok számos előnyös tulajdonsággal bírnak, mint pl. hogy a telepítés után a nagyon kis méretüknek köszönhetően alig felderíthetők, illetve hogy nagyon kis áramfelvételük miatt a saját akkumulátoraikról igen hosszú ideig képesek működni. [11]

2.3. Elektronikai támadás

Az elektromágneses környezetben működő elektronikai eszközök párosulva bizonyos természeti jelenségekkel (hullámterjedési sajátosságokkal) gyakran forrásai különböző káros, (szándékos és nem szándékos) elektromágneses kisugárzásoknak. Ezeket ún. **elektromágneses környezeti hatásoknak** nevezzük.

Az elektromágneses környezeti hatások közé a következők sorolhatók:

- elektrosztatikus kisülések, melyek különböző elektromos potenciálú testek közötti elektrosztatikus töltés átvitelt jelenti;

- nagy energiájú elektromágneses impulzusok, melyek általában földfelszín feletti nukleáris robbantások során keletkeznek;
- irányított energiájú eszközök által keltett pusztító, rongáló hatások;
- szándékos elektronikai zavarok;
- nem szándékos interferenciák.

Mint a felsorolásból is kitűnik az elektromágneses környezeti hatások egy része szándékos tevékenységek következménye, amelyeket az elektronikai támadás eszközeivel és módszereivel lehet elérni. Az elektronikai támadás minden olyan technikát, módszert és eszközt felhasznál, ami az elektromágneses és más irányított energiák felhasználásával képes lerontani az ellenség infokommunikációs rendszereinek hatékonyságát, csökkenteni vezetési és irányítási lehetőségeit, működésképtelenné tenni fontosabb technikai eszközeit és megtéveszteni információs rendszereit.

Ezek az eszközök minden esetben valamilyen energiát sugároznak ki, sugároznak vissza, vagy vernek vissza a célobjektum működésének akadályozása, korlátozása vagy rongálása érdekében. E tevékenység az elektronikai hadviselés egyik alapvető összetevője, melynek körébe az elektronikai zavarást, elektronikai megtévesztést és az elektronikai pusztítást soroljuk.

Az elektronikai zavarás az elektromágneses energia szándékos kisugárzását, visszasugárzását vagy visszaverését jelenti abból a célból, hogy a különböző fajtájú infokommunikációs rendszerek rendeltetésszerű működését megakadályozzuk, korlátozzuk, vagy túlterheljük. Az elektronikai zavarás mind aktív (zavarójelet kisugárzó, vagy visszasugárzó), mind passzív (elektromágneses hullámokat visszaverő) eszközökkel megvalósítható.

Az elektronikai zavarok olyan elektromágneses sugárzások, melyek a berendezések vevőegységére hatva torzítják a megfigyelt és a végberendezés által rögzített jeleket, információkat, megnehezítik, illetve kizárják a rádióforgalmazás lehetőségét, az adatátvitelt, a cél felderítését, csökkentik a felderítő eszközök megkívánt hatótávolságát és az automatizált vezetési rendszerek pontosságát, megtévesztik a kezelőket.

Az elektronikai zavaráshoz erre a célra tervezett és szerkesztett berendezésekre, úgynevezett zavaróállomásokra, speciális sugárzókra vagy visszaverő eszközökre van szükség. Az esetek túlnyomó többségében ezek bonyolult, és drága berendezések, amelyek rendszerint az egyes országok elektronikai hadviselési erőinek kötelékében találhatók meg. Számolni kell ugyanakkor azzal is, hogy hozzáértő szakemberek képesek előállítani egyszerűbb kivitelű, korlátozott képességekkel rendelkező eszközöket, amelyek pl. nem reguláris erők, vagy akár

terroristák kezében az ismertetett zavarási feladatokra hatékonyan felhasználhatók. [4] Ilyen kisméretű és olcsó, könnyen beszerezhető zavaró eszközök pl. a mobiltelefonokat és a GPS navigációs vevőket zavaró berendezések.

Az elektronikai megtévesztés hamis jelek szándékos kisugárzását, visszasugárzását vagy visszaverődését jelenti, amely megtéveszti, félrevezeti, az elektronikai rendszerben működő humán, vagy gépi döntéshozatali folyamat működését. E tevékenység során a cél, hogy az adott rendszerbe bejuttatott jelek, információk szintaktikailag és szemantikailag is egyaránt helytállóak legyenek, megfeleljenek a helyzetnek, ugyanakkor hamis voltuk miatt hibát okozzanak, helytelen döntéseket eredményezzenek a megtámadott rendszerben. Mindemellett olyan veszélyek is kialakulhatnak, mint például egy repülőtér közelében elhelyezett és ott működésbe hozott hamis jeladó, amely a valóságostól eltérő adataival látja el a körzetében repülő repülőgépeket. [4]

Az elektronikai megtévesztés során alkalmazható eszközök és eljárások az alábbiak lehetnek:

- infracsapdák, válaszadók, hamiscél generátorok, melyek megtévesztő kisugárzásokat hoznak létre;
- különböző imitációs technikai eszközök, melyek helyettesítik a rádiólokátor-, navigációs- és kommunikációs kisugárzásokat;
- dipólok és egyéb visszaverő eszközök, amelyek álcáznak, vagy hamis célokat hoznak létre;
- rádióhullámokat elnyelő anyagok, védő festékek és bevonatok, melyek csökkentik a hatásos visszaverő felületet;
- hőenergiát elnyelő vagy szétszóró anyagok, védő festékek és bevonatok, melyek csökkentik az infravörös kisugárzásokat.

A hatékony elektronikai megtévesztés feltétele egyrészt, hogy a másik félnek érzékelnie kell a megtévesztő jeleket, másrészt pedig e tevékenységeknek – hogy a félrevezetést ne lehessen felfedezni – valóságosnak kell látszaniuk. Ennek érdekében az elektronikai megtévesztés részletes és alapos tervezést, koordinációt és végrehajtást igényel.

Az elektronikai pusztítás, rongálás az elektromágneses és egyéb irányított energiák, alkalmazását jelenti abból a célból, hogy a megtámadott elektronikai eszközökben tartósan, vagy ideiglenesen kárt okozzanak.

Az elektronikai eszközökben, számítógépekben használt mikroprocesszorok miniatürizálása következtében a vezetőrétegek vastagsága rendkívüli mértékben lecsökkent. Ez a nagy-

mértékű csökkenés azt eredményezheti, hogy megfelelő nagyságú sztatikus – külső vagy belső forrásból származó – túlfeszültség hatására villamos átütés jöhet létre a rétegek között, amely roncsolja, és így javíthatatlanná teszi az alkatrészeket. [4]

Az elektromágneses impulzus elvén működő fegyverek tulajdonképpen ezt használják ki. Képesek megfelelő nagyságú elektromágneses tér létrehozására, és mindezt irányítottan, célzottan a mikroprocesszorokat, illetve mikroelektronikai áramköröket tartalmazó eszközök közelébe juttatni. Ezek az eszközök alkalmazhatók bombaként (E-bomba) amely egy bizonyos magasságban berobbantva, közel kör alakú területen működő összes elektronikai berendezést tönkre teszi. Másik alkalmazási mód, amikor az eszköz, pl. a nagy energiájú rádiófrekvenciás fegyver az adott célpont felé irányítva nagy energiájú impulzusokkal rongálja a berendezéseket. Ez utóbbi előnye, hogy míg az E-bomba csak egyszer alkalmazható, addig a ez az eszköz többször is bevethető.

Napjainkban a nagy veszély abban áll, hogy az elektromágneses impulzus hatás elvén működő eszköz könnyen hozzáférhető elemekből alig 1000 dollárért, házilag is összebarkácsolható. Ezek teljesítménye természetesen ebben az esetben korlátozott, de ahhoz pontosan elegendőek, hogy egy-egy jól megválasztott helyre elhelyezve, kulcsfontosságú információs rendszereket részlegesen, vagy teljesen megbénítson. [4] Ezt természetesen jól tudják a fejlett információs rendszerekkel rendelkező államok is. Talán éppen ezért Bush amerikai elnök nem sokkal az ikertornyok elleni támadást követően elrendelte a kritikus információs infrastruktúrák elleni esetleges támadásokkal szembeni védekezés stratégiájának kidolgozását.

III. FEJEZET
AZ INFORMÁCIÓBIZTONSÁG MEGVALÓSÍTÁSA

3.1. Az információbiztonság értelmezése

Az információ a szervezetek számára a legfőbb erőforrások egyike, a megfelelő és megbízható működés alapja. Kiemelt erőforrásként még nagyobb hangsúlyt kap a gazdálkodó szervezetek életében, ezért minden esetben gondoskodni kell megbízhatóságáról és biztonságáról, hiszen ez alapvetően befolyásolhatja egy szervezet működését, szolgáltatásainak, termékeinek minőségét.

Annak érdekében, hogy az információk megfelelően védettek legyenek, az alábbiakat kell biztosítani:

- bizalmasság;
- rendelkezésre állás;
- sértetlenség;
- hitelesség;
- letagadhatatlanság.

A bizalmasság olyan biztonsági tulajdonság, amely lehetővé teszi, hogy az információ jogosulatlan egyedek (emberek, folyamatok) számára ne legyen elérhető, vagy ne kerüljön nyilvánosságra. A bizalmasság elvesztése az információ illetéktelenek általi hozzáférését, megismerését jelenti.

A rendelkezésre állás a biztonság azon szempontja, amely lehetővé teszi, hogy a feljogosított szubjektum (humán közreműködő vagy gépi folyamat) által támasztott igény alapján az adott objektum elérhető és használható legyen. A rendelkezésre állás elvesztése azt jelenti, hogy az információhoz vagy az informatikai rendszerhez való hozzáférés vagy annak használata akadályokba ütközik, vagy adott időtartamra vagy teljes mértékben megszűnik.

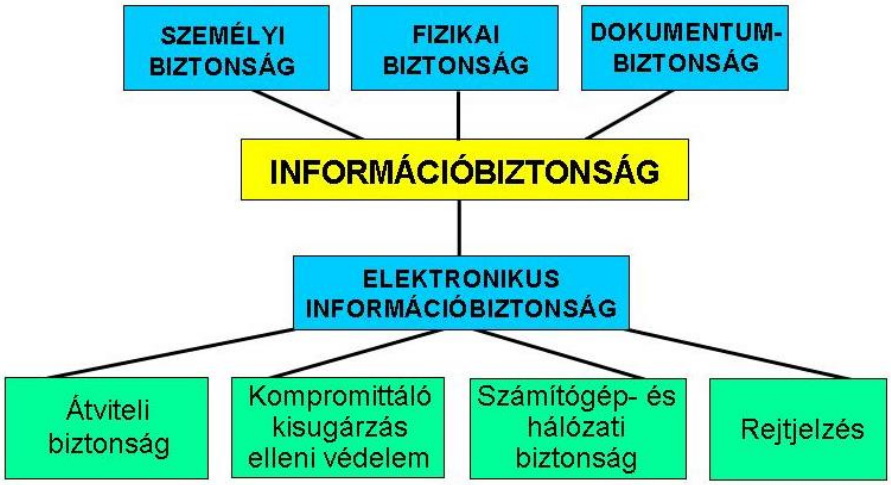
A sértetlenség olyan biztonsági tulajdonság, amely azt jelenti, hogy az adatot, információt vagy programot csak az arra jogosultak változtathatják meg és azok észrevétlenül nem módosulhatnak és nem törölhetők, semmisíthetők meg. A sértetlenség elvesztése az információ jogosulatlan módosítását vagy megsemmisítését jelenti. A sértetlenség fogalmába beleértendő az információk hitelessége és letagadhatatlansága is.

A hitelesség az entitás olyan biztonsági tulajdonsága, amely egy vagy több hozzá kapcsolódó tulajdonságot más entitás számára bizonyíthatóvá tesz. Egy információ akkor tekinthető hitelesnek, ha mind tartalmának, mind létrehozójának (küldőjének) sértetlensége garantálható.

A letagadhatatlanság olyan biztonsági tulajdonság, amely megfelelő bizonyítékokkal szolgál az infokommunikációsi rendszerben végrehajtott tevékenységek későbbi ellenőrizhetőségét illetően. [12]

Ennek megfelelően az információbiztonság területei az alábbiak:

- a személyi biztonság;
- a fizikai biztonság;
- a dokumentumbiztonság;
- az elektronikus információbiztonság. (20. ábra)



1. ábra:

A komplex információbiztonság elemei

A **személyi biztonság** azt jelenti, 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.

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.

A **dokumentumbiztonság** 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 információbiztonsághoz, hiszen valamennyi elektronikus adathordozó egyben dokumentumnak is minősül.

Az **elektronikus információbiztonság** (INFOSEC[5]) 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, sértetlenségének és rendelkezésre állásának véletlen, vagy szándékos csökkenése ellen.

Az elektronikus információbiztonság területei:

- az átviteli biztonság (TRANSEC[6]);
- a kompromittáló kisugárzás elleni védelem (EMSEC[7]);
- a rejtjelzési biztonság (CRYPTOSEC[8]);
- a számítógép biztonság (COMPSEC[9]) és
- a hálózati biztonság (NETSEC[10]).

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.

[5] Information Security
[6] Transmission Security
[7] Emanations Security
[8] Cryptographic Security
[9] Computer Security
[10] Network Security

A **számítógép- és hálózati biztonság** az önálló, vagy hálózatba kapcsolt 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. [2]

A továbbiakban, a II. fejezetben leírt osztályozás szerint bemutatjuk a számítógép-hálózatok elleni támadásokkal, az elektronikai felderítéssel és az elektronikai támadással szembeni védelem módszereit és eszközeit.

3.2. Az információs támadásokkal szembeni védelem eszközei és módszerei

Az információs támadások osztályozása alapján a védelem területei az alábbiak:

- elektronikai felderítés elleni védelem;
- elektronikai támadással szembeni védelem;
- számítógép-hálózati védelem.

3.2.1. Elektronikai felderítés elleni védelem

Az elektronikai felderítés elleni védelem célja észlelni, megbecsülni és megakadályozni a felderítési adatok gyűjtését, továbbítását, feldolgozását és szétosztását. E tevékenység tartalmazza a másik fél teljes felderítő, adatgyűjtő rendszerének feltárását, a saját sebezhető pontok megállapítását, valamint a biztonsági rendszabályokat és azok értékelését.

Az elektronikai eszközökről és rendszerekről azok üzem közbeni kisugárzása során, valamint a funkcionális feladataikból adódó áruló jellemzők alapján szerezhetők be információk.

Az elektronikai felderítéssel szembeni védelem alapvető módszerei a következők:

- a felderítő eszközök és azok hordozói, valamint az információgyűjtő és felderítő központok fizikai megrongálása;
- a felderítő berendezések és az adatokat továbbító kommunikációs eszközök elektronikai zavarása;
- elektronikai eszközök sugárzásainak korlátozása;

- a felderítés ellen védendő objektumokra, eszközökre és tevékenységekre utaló áruló jelek megszüntetése, elektronikai álcázása;
- a felderítés hatékonyságának technikai módszerekkel való csökkentése;
- kompromittáló kisugárzás elleni védelem.

A felderítő eszközök rongálása és zavarása alapvetően konfliktushelyzetben alkalmazható hatékony, aktív védelmi megoldások.

Az elektromágneses kisugárzás korlátozása az eszközök rendeltetésszerű működését korlátozza. A korlátozás történhet időben, frekvenciában, teljesítményben esetleg üzemmódban stb. Leginkább az időbeni korlátozást alkalmazzák, ami azt jelenti, hogy az adóberendezéseket csak a feladat végrehajtásához szükséges időtartamig szabad bekapcsolni, mivel a túl hosszú kisugárzási idő alatt a másik fél könnyebben felderítheti, analizálhatja rendszereinket és megkeresheti azokat a kisugárzásokat, amelyekből használható információt nyerhet.

Az elektronikai álcázás az elektronikai eszközök és a tevékenységek lényeges, csak rájuk jellemző „áruló” tulajdonságaik kiküszöbölésével, meghamisításával, illetve a másik fél számára hozzáférhetetlenné tételével érhető el. Az elektronikai álcázás magába foglalja:

- az elektronikai megtévesztést és
- az elektronikai rejtést.

Az **elektronikai megtévesztés** az elektronikai támadás egyik fajtája, amely a felderítő rendszerek félrevezetésével, hamis információk továbbításával a felderítés elleni védelem érdekében is végrehajtásra kerülhet.

Az **elektronikai rejtés** aktív és passzív tevékenységek és rendszabályok összességét jelenti. Az aktív elektronikai rejtő tevékenységek közé a következők sorolhatjuk az elektronikai zavarás különböző formáit.

A passzív elektronikai rejtő tevékenységek közé az alábbiak sorolhatók:

- az elektronikai eszközök áruló jeleinek megszüntetése;
- a rádiólokátorok passzív zavarása (szögvisszaverőkkel, tükrökkel, dipólusokkal, lencsékkel);
- elektro-optikai felderítés elleni álcázás (füstökkel, ködökkel, festékkel és egyéb anyagokkal);
- akusztikai álcázás (zajcsökkentő megoldásokkal);
- elektromágneses kisugárzások árnyékolása (árnyékoló eszközök alkalmazásával).

A felderítés hatékonyságának technikai eszközökkel való csökkentése többek között az új modulációs eljárásokat, korszerű adásmódokat (pl. szórt spektrumú adásmódok), telje-

sítménnyel való manőverezést, információtömörítési eljárásokat, irányított kisugárzások alkalmazását stb. jelenti. [13]

Az elektronikus berendezések kompromittáló kisugárzásának lehallgatása napjaink egyik fontos problémája. A hardver elemek elleni felderítésnek ezt a módját TEMPEST[11] támadásnak szokták nevezni.

Működése során minden elektronikus eszköz létrehoz olyan elektromágneses erőteret, amelynek érzékelésével a működésre vagy a kezelt (továbbított) adatokra vonatkozó információk szerezhetők be, akár illetéktelen személyek által is.

A kompromittáló kisugárzások lehallgatás megakadályozás érdekében az eszközöket olyan aktív és passzív védelmi elemekkel kell kiegészíteni, amelyek ezeket a nem szándékosan kisugárzott jeleket árnyékolják, vagy más módon semlegesítik. Védendő eszközök alatt nemcsak a végberendezéseket kell érteni, hanem ide kell sorolni az összes olyan eszközt (kapcsolók, szerverek stb.), amelyek az összetett átviteli út során biztosítják az adatok továbbítását. [14]

Azokat a helységeket, ahol nagy mennyiségű elektronikai-, informatikai eszköz van elhelyezve egy, ún. Faraday-hálóval, azaz a helység mind a hat falába beépített földelt fémhálóval szokták védeni. Elektromágneses kisugárzás ellen védeni kell a helyi hálózatokat is. Ehhez árnyékolt kábeleket célszerű használni. Előfordulhat, hogy az elektronikus eszközökből a táphálózatra jutnak ki jelek, amelyek a tápáramra szuperponálódnak. Ezeket megfelelő eszközökkel a támadó távolabbról is kiszűrheti, ezért az elektromos hálózat szűrésére, leválasztására is szükség van. [15]

3.2.2. Elektronikai támadás elleni védelem

Az elektronikai támadás elleni védelem jelentősen kötődik az elektronikai felderítés elleni védelem módszereihez, rendszabályaihoz és eszközeihez. Amennyiben az elektronikai felderítés ellen hatékonyan tudunk védekezni, akkor jelentős lépést teszünk az elektronikai támadás elleni védelem irányába is. Megfelelő információk (pl. frekvencia, üzemmód, elhelyezkedés stb.) hiányában ugyanis a támadó nem képes célirányos, hatékony, az adott infokommunikációs rendszernek megfelelő elektronikai támadást (pl. elektronikai zavarást) megvalósítani. Ezért az előzőekben ismertetett elektronikai felderítés különböző módszerei elleni védelmi megoldások többnyire eredményesen alkalmazhatók a támadás kivédésére is, így az elektronikai támadás elleni védelmet az elektronikai felderítéssel összhangban kell megvalósítani.

[11] Transient ElectroMagnetic Pulse Emanations Standard

Az elektronikai zavarás elleni tevékenységgel kapcsolatban használjuk a zavarstabilitás és zavarvédettség fogalmát.

A **zavarstabilitás** az elektronikai rendszerek azon tulajdonsága és képessége, amely kifejezi, hogy az adott rendszer az elektronikai zavarás viszonyai között képes-e funkcionális feladatainak végrehajtására.

A **zavarvédettség** az elektronikai eszközök azon tulajdonsága, hogy milyen mértékű, intenzitású, típusú zavaró jelekkel szemben védettek. Ez azt jelenti, hogy a rendszeren belül minél zavarvédettebb eszközök vannak, annál nagyobb a rendszer zavarstabilitása.

Az egyes eszközök zavarvédettségét alapvetően a fejlesztés-, tervezés-, kivitelezés során kell biztosítani, és lehetővé tenni, hogy a berendezések minél nagyobb mértékben legyenek képesek kiszűrni a zavarokat.

Az elektromágneses zavarás kialakulásának folyamata bár egyszerűnek tűnik, a valóságban bonyolult folyamatot takar. A bonyolultságot az okozza, hogy a valós közvetítő közegben alkalmazott rendszereket az esetek döntő többségében előre meg nem határozható zavarforrások veszik körül, miközben a rendszerek elemei is létrehozhatnak belső eredetű zavarokat.

A szándékos zavarás hatékonyságát csökkentő általános módszerek a következők lehetnek:

- a zavarás és zavarok felismerése;
- a zavar eredetének meghatározása (a zavar külső, ha a zavar az antennán keresztül jut be a vevőbe; a zavar belső, ha a zavar nem az antennán keresztül jut be a vevőbe);
- a zavar hovatartozásának meghatározása (a zavar szándékos, a zavar nem szándékos, pl. saját eszköz zavarása, atmoszféra zavarok stb. estén);
- a zavarás és a zavarok hatékonyságának csökkentése;
- az üzemelés folytatása (a zavarhatékonyság felmérésének akadályozása céljából);
- a hasznos jel és a zavaró jel arányának javítása;
- a vevőberendezés beszabályozása (helyi oszcillátor, sávszélesség, hangerő stb. beszabályozása);
- az adó kimenő teljesítményének növelése;
- az antenna beszabályozása vagy megváltoztatása (pl. az antenna polarizáció megváltoztatása minden eszközön);
- átjátszó eszközök létesítése;
- az antenna helyének a megváltoztatása;
- alternatív átviteli útvonalak alkalmazása;

- frekvencia megváltoztatása;
- műholdas kommunikáció esetén másik műholdra való átállás.

A szándékos zavarok elleni védelem általános módszerei alapján megállapítható, hogy azokat egyrészt szervezési (pl. alternatív híradó útvonalak), másrészt technikai (pl. az adó kimenő teljesítményének növelése) módszerekkel lehet biztosítani.

Az elektromágneses impulzusfegyverek elleni védelem alapvető problémája, hogy nem ismert az elektromágneses impulzus nagysága a védett eszköznél. Így nehéz megállapítani, hogy milyen nagyságú elektromágneses impulzust kell lecsökkenteni olyan mértékre, amelyet még károsodás nélkül elviselnek az érzékeny elektronikai eszközök. A szükséges érték ismeretében lehetőség lenne meghatározni azt az optimálisan szükséges védelmi módszert és eszközt, így nem kellene minden esetben a maximális védelmi értéket biztosító eljárást vagy eszközt alkalmazni.

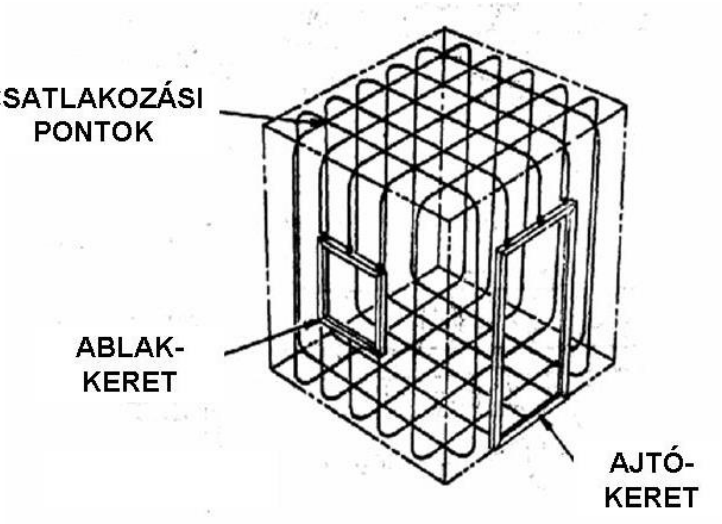
Két alapvető módszer létezik az elektromágneses impulzusok elleni védelemre. Az egyik, hogy olyan elektronikai áramköröket építenek az eszközökbe, amelyek ellenállnak az elektromágneses impulzus hatásainak, a másik pedig, hogy árnyékolással megakadályozzák, hogy az elektromágneses impulzus bejusson a védett térbe. Természetesen az a legjobb, ha mindkét módszert egyszerre alkalmazzuk, mivel ez adja a legnagyobb védelmet.

Az elektromágneses hullámok elleni árnyékolással ideális védelem biztosítható az elektromágneses impulzusok ellen. Az elektromágneses hullámok ellen abszorbeáló (elnyelő) vagy reflektáló (visszaverő) árnyékolást lehet alkalmazni.

Az abszorbeáló árnyékolási módszernél rádiófrekvenciás energiát elnyelő anyagokat alkalmaznak, ahol az energia elnyelés nagyságától és a frekvenciasávtól függően a vastagság a 60 cm-t is elérheti. Az árnyékolt területen átlátszó, üvegezett felületek nem megengedhetők. Ezt az árnyékolási módszert általában laboratóriumoknál alkalmazzák.

A reflektáló árnyékolási módszernél a védendő teret rádiófrekvenciásan reflektáló anyagokkal vonják be oly módon, hogy a bevonat folyamatos legyen. Az árnyékolás elválasztja a külső teret a védendő belső tértől, a jel a reflektáló rétegen csak erősen csillapítva (50-120 dB) juthat át.

A számítógéptermek, műszerszobák, fontos elektronikai eszközökkel felszerelt helyiségek védelme esetén a teljes védendő tér körül Faraday-kalitkát kell kialakítani. Ez egy fémből, vagy fémhálóból készült doboz, amelybe belehelyezve az adott elektronikai eszközt, az védve van a külső elektromágneses tér elől. [16] A 2. ábrán egy egyszerű Faraday kalitka felépítése látható, ahol különböző nyílások is megengedhetők.



2. ábra:

Faraday kalitka [13]

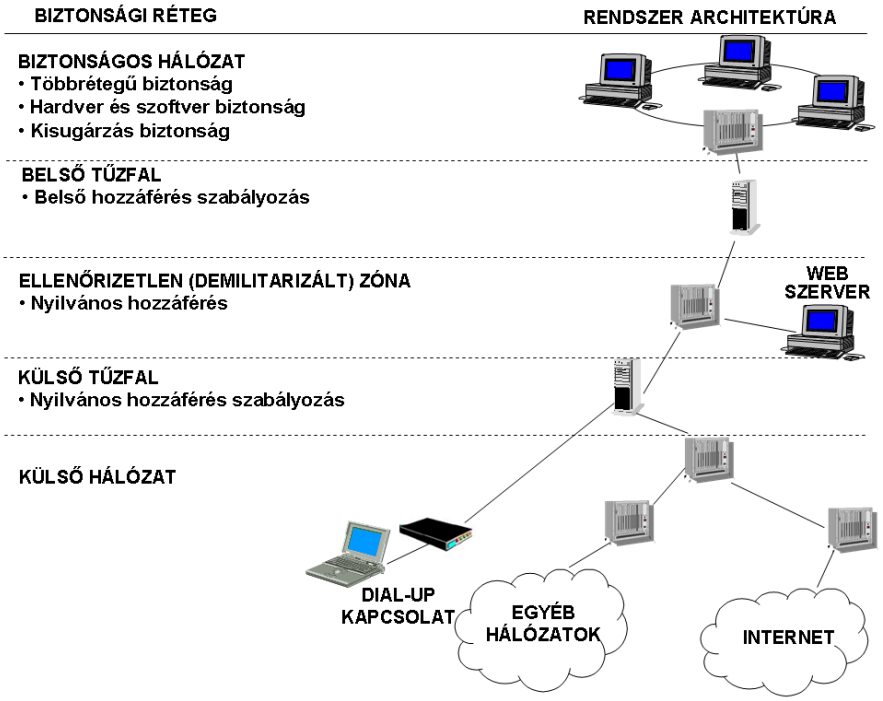
Faraday kalitka alkalmazásakor a teret határoló teljes falfelületet vezetőanyaggal kell borítani, a vezetőképesség nem szakadhat meg a felületek találkozásánál, sőt a nyílászáróknál sem. A védett térbe belépő vezetéket (erősáram, telefon, beléptető rendszer, biztonságtechnikai és tűzvédelem, számítógépes hálózat stb.) megfelelő szűréssel kell ellátni. Külön gondot kell fordítani a védet térbe vezető klíma- és szellőzőrendszer kialakítására, a megfelelő potenciálra hozására, ellenkező esetben ezek mint szekunder antennák és csatolók továbbítják a sugárzott jelet. Az ekvipotenciális felületek minél ritkábban szakítandók meg ablakokkal és ajtókkal, mivel ezek árnyékolása lényegesen költségesebb, és potenciális hibaforrást is jelenthetnek.

Az árnyékolások kivitelezésére és azok tesztelésére számos szabvány létezik, amelyek betartásával megfelelő védelem biztosítható az elektromágneses impulzus bombák és nagy energiájú rádiófrekvenciás sugárforrások ellen.

3.2.3. A számítógép-hálózatok védelme

A számítógép–hálózatok védelme a saját számítógép–hálózat megóvását jelenti a jogosulatlan hozzáféréssel és behatolással szemben, amelyet abból a célból hajtanak végre, hogy megszerezzék az adatbázisokban tárolt adatokat és információkat, illetve, hogy szándékosan lerontsák, működésképtelenné tegyék információs rendszerünket. [2]

A megbízható számítógép–hálózatoknak[12] rendelkezniük kell a már korában ismertetett információk bizalmasságának, sértetlenségének és rendelkezésre állásának követelményével. E követelmények teljesítése érdekében a hálózatot – biztonság szempontjából – többrétegűen kell kialakítani. A réteg koncepció lényege, hogy minden réteg biztonsága önállóan is biztosított, és a rétegek közötti információátvitel védelme érdekében a rétegekhez való hozzáféréshez különböző rendszabályokat alkalmaznak. Ilyen többrétegű hálózat biztonsági felépítést mutat be a 3. ábra. [2]



3. ábra:

Többrétegű hálózat biztonsági felépítése [2]

A számítógép–hálózatok passzív védelmének megvalósítása lehet passzív és aktív. A jegyzet kereteiben a passzív védelemmel foglalkozunk.

A passzív védelmi módszerek és eszközök az alábbiak:

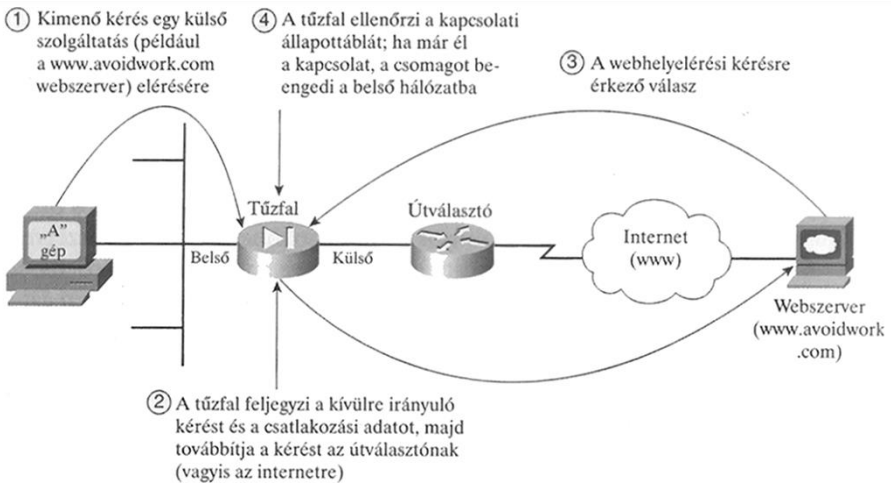
- tűzfalak[13];
- vírusirtók[14];
- hozzáférés szabályozás[15] és

[12] Trusted Networks
[13] Firewall
[14] Antivirus Softwares
[15] Access Control

- behatolás detektálás és adaptív válaszlépések[16].

A számítógép–hálózat más hálózatoktól (pl. Internet) való elválasztásának az egyik elterjedt módja a **tűzfal,**[17] amelyet a saját hálózat és az internet közé építenek be, tehát az internet, valamint a saját hálózat határfelületén dolgoznak. Feladatuk a határfelületen keresztül áramló **forgalom szűrése**. Céljuk nem a támadás lehetőségeinek kiküszöbölése, hanem akadály állítása a támadás elé, a sikeres behatolás valószínűségének csökkentése. A tűzfal nem a védelem alapeszköze, inkább annak fontos kiegészítője.

A tűzfal működését szemlélteti a 4. ábra. Az „A” gép mögött ülő személy a böngészőjében meg szeretné jeleníteni a www.avoidwork.com weboldalt. A kívülre irányuló kérést a tűzfal megjegyzi (beírja az úgynevezett munkamenet állapot-nyilvántartó táblába), és továbbítja azt az útválasztónak. A kérés eljut a külső szolgáltató webszerveréhez, amely fogadja a kérést és válaszol rá. A választ először a tűzfal kapja meg, és ha a kapcsolat már él, akkor beengedi a belső hálózatba, így a kért webtartalom megjelenik az internetező böngészőjében. [17]



4. ábra:

A tűzfal működési elve [17]

A korábban bemutatott többrétegű megbízható hálózatban (3. ábra) egy külső tűzfal a teljes helyi hálózatot részben izolálja az internettől, míg az ún. belső tűzfal a helyi hálózat egy különösen védendő részét zárja el annak többi részétől és így az internettől is. Ha lehetséges, akkor csak egy ponton kell csatlakozni a nyilvános hálózathoz, s ezt a csatlakozó számítógé-

[16] Intrusion Detection and Adaptive Response Tools

[17] A "tűzfal" nevet is onnan kapták, hogy szerepük hasonló, mint régen a fából készült házsorokba beépített téglafalaké, amelyek megakadályozták a tűz továbbterjedését.

pet látják el tűzfal funkciókkal, ez a külső tűzfal. Ez a védelem azonban nem elegendő, gondoskodni kell arról is, hogy ha azon átjutott a behatoló, akkor se férhessen hozzá adatainkhoz. A tűzfalak működése ezért azon alapul, hogy a rendszergazda beállíthatja, melyik IP–forgalmat engedje át, és melyiket tiltsa le. Ha az üzenetek szűrése nincs körültekintően beállítva, a védelem hatékonysága máris csökken. [2]

Meg kell jegyezni, hogy a tűzfalak beépítése sem ad százszázalékos védelmet, mert a tűzfalak tipikusan a feladó és a címzett címe szerint, valamint a portok címe szerint végzik el a beállított szelekciót. Ha a behatoló képes olyan megtévesztő üzeneteket előállítani, melyeket a tűzfal átengedhetőnek minősít, akkor a védelem feltörhető.

A különböző rosszindulatú programok (Malware) elleni küzdelem leghatékonyabb eszközei a különböző **antivírus szoftverek**, amelyek elsősorban a vírusazonosító adatbázisaik alapján, illetve heurisztikus vagy egyéb módszerek segítségével ismerik fel a rosszindulatú programokat. A vírusirtók működésének hatékonyságát nagymértékben befolyásolja vírusazonosító adatbázisuk frissessége. Ezért a vírusirtó szoftverek adatbázisaikat automatikusan, napi többször is frissítik.

A víruskereső programok lehetnek:

- háttérben futó, vírusazonosító mintákat használó keresőprogramok;
- alkalmi vírusellenőrző és memóriarezidens programok;
- heurisztikus keresést alkalmazó programok.

A háttérben futó víruskeresők jellemzője, hogy a számítógép indításával egyidőben – a beállított paramétereknek megfelelően – azok is elindulnak, és folyamatosan ellenőrzik az operációs rendszer működését, a használatba vett lemezek boot szektorát, automatikusan ellenőrzik az összes megnyitott fájlt, keresik azokat a rosszindulatú programokat, melyek az adatbázisukban tárolt vírusazonosító mintákkal megegyeznek. E szoftverek alkalmasak a Malware-ek eltávolítására, törlésére, esetleg karanténba helyezésére, ahol már nem okozhatnak kárt. Természetesen alkalmasak arra is, hogy eseti módon ellenőrizzék a számítógép összes lemezét vagy csak egyes meghatározott lemezeket, objektumokat.

Hálózatba kötött gépek esetében a központi szervereken telepített vírusellenőrzés is igen hatékony védelmet biztosít, amennyiben a munkaállomások adatállományaikat hálózati meghajtókon hozzák létre és tárolják. Ilyen rendszereken viszonylag csekély a vírustámadások kockázata. Ebben az esetben a munkaállomásokon elegendő alkalmilag futtatandó vírusirtókat telepíteni és használni.

Az **alkalmilag futtatandó vírusirtók** csak akkor lépnek működésbe, ha a felhasználó elindítja, és meghatározza az ellenőrizendő lemezeket, objektumokat, fájlokat. Ezeknek a vírus-

keresőknek a folyamatosan futókkal szemben jóval kisebb az erőforrásigényük. Ezért ezeknek elsősorban ott van létjogosultságuk, ahol kicsi a számítógép teljesítménye.

A **heurisztikus víruskeresők** nem a vírusadatbázisok alapján kutatnak vírusok után, hanem a vizsgált program viselkedése, működése, utasításai alapján próbálják eldönteni, hogy vírussal állnak–e szemben. A heurisztikus keresés általános formája, amikor a program olyan műveleteket figyel, amelyek általában rosszindulatú programokban fordulnak elő. Ilyen gyanús művelet lehet például, a végrehajtható állományokba való írás. A heurisztikus víruskeresők segítségével még fel nem fedezett vírusok is felismerhetők. [2] Meg kell jegyezni, hogy a manapság alkalmazott vírusirtók szinte mindegyike képes mindhárom módban működni.

A hozzáférés szabályozás két leginkább alkalmazott módszere a jelszó és a hitelesítés.

Egy adott számítógéphez való hozzáférés a legtöbb esetben **jelszóhoz** kötött. A jelszó használatánál kétféle megoldás lehetséges: alkalmazhatnak többször felhasználható és csak egyszer felhasználható jelszót. Az első esetben a jelszó hosszabb ideig lehet érvényben, a másik esetben egy adott jelszóval csak egyszer lehet belépni a rendszerbe. Ez az utóbbi nyilvánvalóan nagyobb biztonságot ad, de lényegesen bonyolultabb megoldásokat igényel.

Biztonságosan védett számítógép–hálózatokban gyakran többszintű jelszavas védelmet alkalmaznak, azaz a rendszer egymás után, különböző szinteken több jelszót kér. A jelszavas védelem más módszerekkel is kombinálható pl. PIN kártyával, ujjlenyomat ellenőrzéssel, írisz letapogatással stb.

A hitelesítés[18] a hálózati hozzáférés másik fontos módszere. Üzenetek, levelek, osztott dokumentumok és adatbázisok használata esetén fontos, hogy valóban a vélt személy küldte–e az üzenetet, végezte–e a módosítást, valamint illetéktelenek nem fértek–e hozzá az adatokhoz. Emellett fontos, hogy az adatok hitelességét ellenőrizni tudjuk, vagy kellő alapunk legyen abban megbízni.

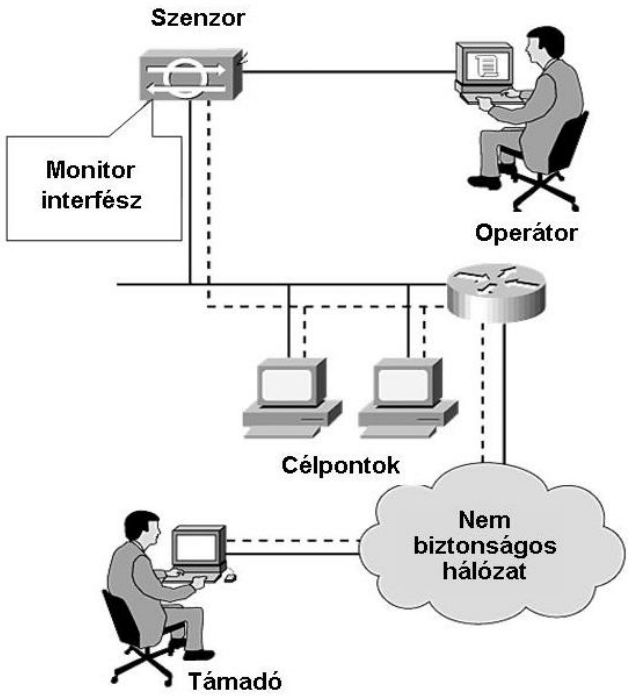
A hitelességet legtöbbször az biztosítja, hogy csak az illetékes személy jogosult az adott művelet végrehajtására, pl. csak neki van hozzáférési joga. Mindazonáltal a hitelesség nehezen igazolható csak ilyen módon, különösen, ha többen is (esetleg illetéktelenül is) rendelkeznek az adott hozzáférési joggal.

Az operációs rendszerek, adatbázis–kezelők, levelező rendszerek jegyezhetik, hogy ki, mit, mikor tett, de egyrészt ezeket sokszor be lehet csapni, másrészt nem mindig könnyű a visszaellenőrzés. A dokumentumok, üzenetek formája is árulkodhat azok hitelességéről. [18]

[18] Authentication

A hitelesítésnek az előbbinél hatásosabb módszere a **titkosítás (kriptográfia)**. A titkosítás olyan matematikai eljárás, melynek során egy üzenetet úgy változtatunk meg felismerhetetlenül, hogy abból az eredeti üzenet csak valamilyen, kizárólag a küldő és a címzett által ismert eljárás segítségével fejthető vissza. A titkosítással a legtöbb esetben biztosítható a tartalom rejtettsége, érintetlensége, letagadhatatlansága és a forrás igazolhatósága.

A behatolás detektálás és adaptív válaszlépések az informatikai biztonsági rendszer olyan aktív elemeit fogja össze, amelyek képesek a hálózatot fenyegető betörési kísérleteket észlelni, azonosítani, és a támadót elszigetelni. (5. ábra)



5. ábra:
Behatolás detektálás

E módszer a betörési kísérleteket nem korlátozza csak a külső fenyegetésekre, hanem kiterjed a szervezeten belüli szabotázsakciókra is. A külső behatolási kísérletek általában a szervereket és munkaállomásokat veszik célba, de nem ritka a hálózati elemek "piszkálása" sem. A behatolás detektáló rendszer[19] feladata a betörési kísérletek tényének feltárása. Ezek az eszközök azon az alapelven működnek, hogy a betörőket a hálózati forgalom elemzésével és a rendszerben észlelt abnormális események alapján azonosítani lehet. A hálózatban elhelyezett érzékelők és monitorprogramok ezeket az eseményeket időrendi sorrendben rögzítik, majd ezt az adatbázist a behatolás–védelmi rendszer elemzi. [4]

[19] Intrusion Detection System – IDS

FELHASZNÁLT IRODALOM

1. Sallai, Gyula – Abos, Imre: A távközlés, információ- és médiatechnológia konvergenciája. Magyar Tudomány, Infokommunikációs hálózatok. 2007. július. 844-851. p. ISSN 1588-1245
2. Haig, Zsolt–Várhegyi, István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005. ISBN 963 327 391 9
3. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről http://www.complex.hu/kzldat/t1200166.htm/t1200166.htm (letöltve:2013.04.02)
4. Haig, Zsolt – Kovács, László – Makkay, Imre – Seebauer, Imre – Vass Sándor – Ványa, László: Az információs társadalom veszélyforrásai. A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban. Tanulmány. MEH Informatikai Kormánybiztosság, 2002.
5. Gerencsér, András: Rövid összefoglalás kritikus információs infrastruktúrák védelméről. http://isaca.hu/ISACA-HuC/CIIP_GerencserAndras.pdf (Letöltve: 2009. 08. 30.)
6. Haig, Zsolt: Az információs társadalmat fenyegető információlapú veszélyforrások. Hadtudomány 2007/3. ISSN: 1215-4121
7. Muha, Lajos: A Magyar Köztársaság információs infrastruktúráinak védelme. Doktori (PhD) értekezés. ZMNE, Budapest, 2007.
8. Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai. MTA SZTAKI, 2004.
9. Előházi, János: Internetbiztonság. Robothadviselés 5. Tudományos szakmai konferencia, Bolyai Szemle 2006. 1.sz. ZMNE, Budapest, 160-178. p. ISSN 1416-1443
10. Gyányi, Sándor: DDoS támadások veszélyei és az ellenük való védekezés. Hadmérnök, Robothadviselés 7 tudományos szakmai konferencia különszám. http://hadmernok.hu/kulonszamok/robothadviseles7/gyanyi_rw7.html (Letöltve: 2009. 08. 30.)
11. Ványa, László: Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre. PhD értekezés, ZMNE, 2002.
12. Útmutató az IT biztonsági szintek meghatározásához**.** http://www.ekk.gov.hu/hu/emo/EKK_ekozig_ITbiztonsagiszintekmeghatarozasa_080822_V101.doc (Letöltve: 2009. 08. 30.)

13. Balajti, István – Vass, Sándor: Elektronikai védelem. Egyetemi jegyzet, ZMNE, 2000
14. Kassai, Károly Az elektronikus információk védelmének területei. http://www.zmka.hu/kulso/mhtt/hadtudomany/2002/3/kassaikaroly/chapter1.htm (Letöltve: 2009. 08. 30.)
15. Géczy, Gábor: Fémezett szövetek alkalmazása az elektronikában. Elektronet, Budapest, 1998/6-7
16. Elemental Faraday Cage. http://www.boltlightningprotection.com/Elemental_Faraday_Cage.htm (Letöltve: 2009. 08. 30.)
17. Thomas, Tom: Hálózati Biztonság – Panem Könyvkiadó Kft, 2005. ISSN 1785-3346, ISBN 963-545-425-2
18. Dravecz, Tibor – Párkányi, Balázs: Hogyan védjük hálózatra kötött számítógépes rendszereinket? NIIF Információs Füzetek II./8. Budapest, 1996.