10.17625/NKE.2013.015

Nemzeti Közszolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar
Katonai Műszaki Doktori Iskola

VARGA PÉTER JÁNOS

Kritikus információs infrastruktúrák vezeték nélküli hálózatának védelme

Doktori (PhD) értekezés

Témavezető: Prof. dr. Haig Zsolt mk. ezredes, PhD
egyetemi tanár

2012. Budapest

Tartalomjegyzék

Bevezetés 5

1. Fejezet Kritikus információs infrastruktúrák 10

1.1 Az értekezésben használt fogalmak 10

1.1.1 Infrastruktúra fogalma 10

1.1.2 Kritikus infrastruktúra fogalma 11

1.1.3 Kritikus információs infrastruktúra fogalma 16

1.2 A kritikus információs infrastruktúrák függősége 21

1.3 Kritikus információs infrastruktúra függőségének modellezése 24

1.3.1 Kritikus információs infrastruktúra függőségének modell elemei 24

1.3.2 Függések modellezése 27

1.3.3 Hatás gráf felépítése 31

1.3.4 Modellezési szintek 34

1.4 Következtetések 37

2. Fejezet Vezeték nélküli hálózatok a kritikus információs infrastruktúrákban 39

2.1 Kritikus információs infrastruktúrák vezeték nélküli hálózatai 42

2.2. Az IEEE 802.11 vizsgálata 45

2.2.1 Rádiós szabályozások 45

2.2.2 Vizsgálati eredmények a rádiós szegmensben 46

2.2.3 Modulációs eljárások a vezeték nélküli hálózatokban 47

2.2.4 Vizsgálati eredmények a 802.11-es csatornák kihasználására 50

2.2.5 Az IEEE 802.11 szabványok 50

2.2.6 Vizsgálati eredmények a 802.11 protokoll alapján 55

2.2.7 WLAN topológiák 56

2.2.8 Vizsgálati eredmények a WLAN topológiák alapján 59

2.2.9 A vezeték nélküli hálózatok hozzáférési pontjainak gyártói 60

2.3. Vezeték nélküli hálózatok hitelesítési és titkosítási módszerei 61

2.3.1 Hitelesítési protokollok 62

2.3.2 Nyílt és osztott kulcsú hitelesítés vizsgálata 63

2.3.3 A WPA és a WPA2 65

2.3.4 WPA és WPA2 vizsgálata 66

2.3.5 Titkosítási protokollok 67
2.3.6 Titkosítási protokollok vizsgálata 68
2.4 A vizsgálati eredmények összesítése 71
2.5. Támadási útvonalak a vezeték nélküli hálózaton keresztül a kritikus információs infrastruktúra irányába 72
2.5.1 Kritikus információs infrastruktúra hozzáférési pontjának megtámadása 73
2.5.2 Kritikus információs infrastruktúra támadása a hozzáférési pontján keresztül 74
2.5.3 Kritikus információs infrastruktúra támadása egy másik kritikus információs infrastruktúra hozzáférési pontján keresztül 75
2.5.4 Kritikus információs infrastruktúra támadása nyilvános hálózati végpontról 75
2.5.5 Kritikus információs infrastruktúra támadása nyilvános hálózati végponthoz kapcsolódó infrastruktúra felhasználón keresztül 76
2.6. Következtetések 78
3. Fejezet Vezeték nélküli hálózatok támadási és védelmi rendszertana 80
3.1 A támadó személye 80
3.2 A támadó célja, motivációja 84
3.3 A támadások módszertanai 86
3.4 A támadási módszerek vizsgálata 90
3.5 Támadási módszertanok összegzése 105
3.6 Védelmi módszerek a kritikus információs infrastruktúrák vezeték nélküli hálózataiban 106
3.6.1 A védelmi módszerek szakirodalmi osztályozása 106
3.6.2 A kritikus információs infrastruktúrák vezeték nélküli hálózatainak védelmi módszertana 109
3.7 Támadási módszerek és védelmi kontrollok egymásnak való megfeleltetése 116
3.8 Behatolás vizsgálati módszertan mobiltelefonra 118
3.9 Következtetések 126
Összegzett következtetések 128
Új tudományos eredmények 131
Ajánlások 132
Témakörből készült publikációim 133

Irodalomjegyzék..... 136
Ábrák jegyzéke..... 148
Táblázatok jegyzéke 150
Rövidítések jegyzéke..... 151

Bevezetés

Az infokommunikációs technológia fejlődésével a számítógépek, a mobiltelefonok, a hordozható eszközök nem csak a magáncélú felhasználásban, hanem az üzleti világban is egyre inkább elterjednek. Az eladási tendenciák azt mutatják, hogy asztali gépeinket lassan felváltják a hordozható laptopok, tabletek. E mellett néhány éve egy új kommunikációs eszköz is megjelent a piacon, az okostelefon. Ezek a hordozható eszközök már nem vezetékes hálózati kapcsolaton keresztül kommunikálnak, hanem a vezeték nélküli hálózatok nyújtotta előnyöket kihasználva tudnak levelezni, böngészni, hálózati szolgáltatásokat elérni. [1 p. 39]

A privát és az üzleti mobil kommunikációs igény annyira erős, hogy az államigazgatás, a közszféra, a szolgáltatók is kényetlenek ennek megfelelni. Erre jó példa az, hogy a Nemzeti Közszolgálati Egyetem jogelődjénél a Zrínyi Miklós Nemzetvédelmi Egyetemnél az elmúlt évtized végéig a vezeték nélküli hálózatok (WLAN[1]) használata tiltott volt. 2008-ban azonban, egy sikeres pályázatot követően az addig tiltott technológia a tűrt működési lépést kihagyva egyből támogatottá vált.[2] Mára már a hallgatóknak és az oktatóknak is egyre erősebb az az igénye, hogy az egyetem területén „bárhol és bármivel" csatlakozni tudjanak az egyetemi hálózathoz. Ez a fajta technológiai szemléletváltás nem csak az oktatási intézményekre jellemző. Vezeték nélküli hálózatokat lehet találni az infokommunikációs szektorban, a pénzügyi intézeteknél, közoktatásban, egészségügyben és számos más kritikus infrastruktúrában.

Ez a mobilitás a maga pozitívumaival szemben sok veszélyt is hordoz. Míg vállalati titkainkat, információinkat vezetékes hálózaton jól kézben tudtuk tartani, a vezeték nélküli hálózatok világában egyre több fenyegetettséggel kell szembenéznünk. 2004-ben, 2009-ben és 2012-ben Budapesten egy 16 km-es útvonalon detektáltam a különböző vezeték nélküli hálózatokat. A növekedés jelentős: 8 év alatt a végpontok száma 154-ről 998-re nőtt. A legutolsó vizsgálat alkalmával a detektált végpontok – az előző mérésekhez képest meglepően kisebb arányban – 19 %-a gyengén[2], vagy egyáltalán nem volt védett, így csekély informatikai ismeretek birtokában is felhasználhatók támadási végpontként. [3]

[1] WLAN – Wireless LAN

[2] A WEP kódolás a gyakorlatban egy perc alatt törhető, így azokat a végpontokat, amelyek ilyen kódolásúak, gyengén védettnek tekintem [3]

Ezt a sebezhetőséget támasztja alá az is, hogy különböző aktivista csoportok, mint például az Anonymus, internetes felhívásokon keresztül szervezik önmagukat, és a világhálózat lehetőségeit kihasználva támadják meg azokat a szervezeteket, infrastruktúrákat, amelyek döntéseivel, lépéseivel nem értenek egyet.

A kritikus infrastruktúrákban és azok kritikus információs infrastruktúráiban a vezeték nélküli hálózati megoldások megjelentek, felhasználásuk egyre nagyobb hálózati potenciált jelentenek. A vezeték nélküli hálózati szegmens ezekben az infrastruktúrákban a teljes informatikai rendszer szerves részét képezi, ezért az értekezésemben a kritikus infrastruktúrákban alkalmazott vezeték nélküli hálózatokat, ezen belül is az IEEE[3] 802.11-es ajánlás csoport alá besorolt hálózati megoldásokat vizsgálom, fenyegetési formáikat, lehetőségeiket elemzem, és egy támadás-védelmi módszertanra alapozott védelmi megoldásokra teszek javaslatot.

Tudományos probléma megfogalmazása

A vezeték nélküli hálózatok új típusú támadási célpontot jelentenek a kritikus infrastruktúrák infokommunikációs rendszerei, vagyis a kritikus információs infrastruktúrák elemei ellen. A kritikus információs infrastruktúrák és azok vezeték nélküli hálózati komponensei közötti interdependenciák a vezeték nélküli technológia szempontjából nem, vagy csak részben ismertek. Ezenfelül vizsgálni kell még azt is, hogy milyen a kapcsolat a kritikus és a kritikusnak nem minősített egyéb vezeték nélküli infrastruktúrák, illetve a vezeték nélküli hálózat felhasználói végpontok között, valamint azt, hogy az egyéb hordozható eszközök közötti relációk, esetleges támadási vektorok elemzése miért nem történt meg.

A kritikus infrastruktúra szempontjából lényeges, hogy milyen támadási modellek közege vagy célpontja lehet a vezeték nélküli hálózat. A hatékony védelem csak a támadási modellek és a támadási módszerek ismeretében tervezhető meg. Ezért egy egységes struktúrában fel kell tárni és meg kell feleltetni egymásnak a vezeték nélküli hálózat támadási és védelmi modelljeit. A védelem hatékonysága, eredményessége azonban ki kell, hogy egészüljön olyan szempontokkal, amelyek az üzleti szereplők számára alacsony költségvetés és minimális szakmai kompetencia mellett is racionálissá teszik a megfelelő védelem kidolgozását.

[3] IEEE - Institute of Electrical and Electronics Engineers

A védelem és a támadás mindezidáig külön-külön részenként vizsgált, értékelt és elemzett területnek számít. Ezekről több szabvány, módszertani ajánlás is található, azonban ezek mindegyike vagy csak a támadás, vagy csak a védelem szempontjaira fókuszál. Az általam fellelt ide vágó publikus szakirodalmak nem feleltetik meg tételesen egymásnak a támadási és védelmi módszereket. Kutatásom során jelenleg nem találtam egy olyan egységes rendszerbe foglalt támadási és védelmi módszertant, ami sorra venné a vezeték nélküli hálózatok elleni támadásokat és azoknak megfeleltetné a lehetséges védelmi megoldásokat. Egyedi (egyes) támadásokra adandó védelmi lépések természeten léteznek, de ezek jelenleg nincsenek rendszerbe foglalva.

A nyilvános módszertanok másik problémája az, hogy olyan követelményeket állítanak fel, amelyeknek gazdasági, technológiai vagy szakképzési hiányosságok miatt már a közepes méretű szervezetek sem tudnak hiánytalanul megfelelni. A vezeték nélküli végpontok nagy száma azonban nem csak az üzemeltető számára jelent veszélyforrást, hanem közvetve, mint az anonim támadások kiindulópontja, a kritikus infrastruktúra fenyegetettségét is növeli. Szükséges tisztázni azt, hogy milyen technikai, adminisztratív, esetleg jogi eszközökkel lehetne a vezeték nélküli hálózatok védelmi potenciálját növelni úgy, hogy ez a laikus üzemeltetők számára se jelentsen aránytalan többletterhet.

Kutatási célkitűzéseim

A kritikus információs infrastruktúrákban alkalmazott vezeték nélküli hálózatok biztonságos működtetésének vizsgálata során az alábbi kutatási célokat tűztem ki:

1. Megvizsgálni a kritikus információs infrastruktúrák külső és belső függőségi viszonyait. Rendszerszemléletű modellt alkotni a kritikus információs infrastruktúrák inter- és intradependenciáinak felmérésére és a függőségek tartalmának elemzésére.
2. Elemezni és rendszerezni a kritikus információs infrastruktúrák vezeték nélküli hálózataiban alkalmazott technológiákat és a velük szemben támasztott műszaki követelményeket, majd ezek alapján feltárni a lehetséges támadási útvonalakat.
3. Megalkotni egy javasolt védelmi módszertant a vezeték nélküli hálózatok végpontjaira, amely tartalmazza az általános szempontokat és kritériumokat a támadási és védelmi taxonómiák tükrében.
4. Kidolgozni a kritikus információs infrastruktúrák vezeték nélküli hálózataival szembeni támadások és a védelem elméletének és gyakorlatának rendszerszemléle-

tű megközelítését, majd erre alapozva megfeleltetni egymásnak a támadási módokat és a védelmi kontrollokat.

5. Meglévő, nyilvános alkalmazások módszertanba rendezésével kidolgozni a vezeték nélküli hálózatok behatolás vizsgálatának kizárólag mobil telefonra épülő módszertanát, amely könnyen, bárhol és bármikor alkalmazható a kritikus információs infrastruktúrákban a vezeték nélküli hálózatok 24/7[4] vizsgálatára.

Kutatási hipotéziseim

Az értekezésem megírásakor abból az alapfelvetésből indultam ki, hogy a kritikus információs infrastruktúrák belső szerkezeti viszonyai, azaz az információs alrendszerek és a vezeték nélküli hálózatok kapcsolatrendszere jelenleg nem vagy csak annak egyes részterületeire vonatkozóan van meghatározva. Napjainkban nincs olyan publikált modell, amely a kritikus infrastruktúrák és azok infokommunikációs alrendszereinek, vagyis a kritikus információs infrastruktúrák egymáshoz való viszonyát, kapcsolatait a vezeték nélküli hálózatok szempontjából feltárná, illetve a nem kritikus vezeték nélküli végpontoknak és hordozható eszközöknek a kritikus információs infrastruktúrákra gyakorolt hatását elemezné.

Véleményem szerint kidolgozható egy olyan modell, amely egységes szerkezetben kezeli a kritikus infrastruktúrákat és a kritikus információs infrastruktúrákat, valamint azoknak a vezeték nélküli technológiákhoz való viszonyát, illetve tartalmazza a vezeték nélküli hálózatok elleni támadási modelleket. A támadási és védelmi módszerek véleményem szerint tételesen összepárosíthatóak.

Kutatásaim alapján úgy vélem, hogy meghatározható egy olyan általános követelményrendszer, amely széles körben alkalmazva megnövelné a kritikus információs infrastruktúrák vezeték nélküli végpontjainak védelmi potenciálját, méghozzá oly módon, hogy ez egyfelől nem okozna jelentős többletterhelést és aránytalan érdeksérelmet az üzemeltetőnek, továbbá csökkentené a kritikus információs infrastruktúrák egyik rohamosan terjedő infokommunikációs alrendszerének a vezeték nélküli hálózatoknak a fenyegetettségét.

[4] 24/7 - A hét minden napján, a nap 24 órájában

Kutatásaim során alkalmazott módszerek

Kutatómunkám során széleskörű irodalomkutatást folytattam a hazai- és nemzetközi irodalomban. Gyakorlati kutatást folytattam a hazai vezeték nélküli hálózatok alkalmazási sajátosságainak feltérképezésére. Modelleket alkottam a kritikus infrastruktúrák inter és intradependenciái jellegzetességeinek feltárására. A kutatásom során szerzett ismereteimet gyakorló informatikusként a mindennapokban is teszteltem. Rendszeresen részt vettem/veszek hallgatóként vagy előadóként a témával kapcsolatos hazai és nemzetközi tudományos konferenciákon és egyéb szakmai rendezvényeken. Kutatási eredményeimet számos tudományos konferencián ismertettem mind itthon, mind külföldön, magyar illetve angol nyelven. Eredményeimet nem csak konferenciákon, hanem lektorált folyóiratokban is publikáltam.

Az értekezés szerkezete

1. fejezet: A fejezetben áttekintem az infrastruktúra, a kritikus infrastruktúra és a kritikus információs infrastruktúra fogalmait. Elemzem a kritikus információs infrastruktúrák külső és belső függőségi viszonyait, és meghatározom az inter- és intradependenciák függőségi modelljét.
2. fejezet: A fejezetben elemzem és megvizsgálom a kritikus információs infrastruktúrák vezeték nélküli hálózataiban alkalmazott technológiákat és a velük szemben támasztott műszaki követelményeket, majd ezek alapján feltárom a lehetséges támadási útvonalakat.
3. fejezet: A fejezetben elemzem a kritikus információs infrastruktúrák támadási és védelmi megoldásait. Ez alapján kidolgozok egy egymásnak megfeleltetett támadási és védelmi kontrollt. A védelmi módszertanok alapján elkészítek egy javasolt védelmi módszertant a kritikus információs infrastruktúrák vezeték nélküli hálózatára. Kidolgozom a vezeték nélküli hálózatok behatolás vizsgálatának kizárólag mobil telefonra épülő módszertanát.

1. Fejezet
Kritikus információs infrastruktúrák

2010-ben egy széleskörű felmérés kapcsán tizennégy ország, kétszáz, kritikus fontosságú infrastruktúrát üzemeltető vállalatának IT biztonsági felsővezetőjét kérdezték meg rendszerük biztonságáról. A válaszadók negyven százaléka elismerte, hogy iparáguk informatikai sebezhetősége megnőtt és nincsenek megfelelően felkészülve egy esetleges informatikai támadássorozatra.[4 p. 3] Ez is bizonyítja, hogy a minden informatikai eszközt magában foglaló számítógép hálózat védelmét egyre nehezebb biztosítani.

Napjainkban, amikor egy telefon nem csak beszédkommunikációra alkalmas, vagy egy számítógép nem csupán a hagyományos értelemben vett számítástechnikai funkcióknak tesz eleget, a vezeték nélküli hálózatok egyre elterjedtebbekké válnak. Felváltva, vagy kiegészítve a meglévő vezetékes hálózatot megjelentek számos hazai kritikus infrastruktúrában, mint például:

- az Országos Mentőszolgálatnál; [119]
- a Budafok-Tétény Önkormányzata Polgármesteri Hivatalában; [120]
- a Részecske- és Magfizikai Kutatóintézetben. [121]

Az a tény, hogy vezeték nélküli hálózatot is kiépítettek ezekben az infrastruktúrákban, új támadási vektort nyitottak a meglévő hálózatokon.

1.1 Az értekezésben használt fogalmak

Értekezésem szempontjából fontosnak tartom a következő fogalmak egyértelműsítő magyarázatát:

- Mi az infrastruktúra?
- Mi a kritikus infrastruktúra?
- Mi a kritikus információs infrastruktúra?

1.1.1 Infrastruktúra fogalma

A Magyar Értelmező Kéziszótár meghatározása szerint az infrastruktúra olyan angolszász eredetű szó, amely jelentése „*a társadalmi, gazdasági tevékenység zavartalanságát biztosító alapvető létesítmények, szervezetek (pl. lakások, közművek, a kereskedelem, a távközlés, az oktatás, az egészségügy stb.) rendszere.*” [5 p . 593]

A Magyar Larousse Enciklopédia meghatározása szerint az infrastruktúra „*a társadalmi, gazdasági újratermelés zavartalanságát biztosító háttér. Legfontosabb elemei a közművek, az energiaellátás rendszere és a közlekedési, hírközlési hálózat (utak, vasutak, telefonhálózat, stb.) Az ún. lakossági infrastruktúrához tartozik a lakásállomány, a kereskedelmi és szolgáltatási hálózat, az egészségügyi, szociális, kulturális ellátás, az oktatás eszközei és intézményrendszere (kórházak, rendelőintézetek, iskolák).*” [6 p. 235]

Egy másik szakirodalom szerint az infrastruktúra nem más, mint „*egy adott rendszer (termelő vagy elosztó, szolgáltató rendszer, tudományos, állami, magán, nemzeti vagy nemzetközi szervezet, ország, város, vagy régió stb.) rendeltetésszerű működéséhez feltétlenül szükséges intézetek, intézmények, felszerelések és berendezések és a működtetést ellátó személyzet szabályszerűen működő összessége. Az infrastruktúra tehát a fizikai építményekből és berendezésekből és azokat szakszerűen működtetni tudó szakszemélyzetből áll.*” [7 p. 73]

1997-ben az amerikai kormány egyik bizottsága a következőképpen fogalmazta meg az infrastruktúra fogalmát: „*Az infrastruktúrák olyan egymástól függő hálózatok és rendszerek összessége, amelyek meghatározott ipari létesítményeket, intézményeket (beleértve a szakembereket és eljárásokat), illetve elosztó képességeket tartalmaznak. Mindezek biztosítják a termékek megbízható áramlását az Egyesült Államok védelmi és gazdasági biztonságának fenntartása, valamint a minden szinten zavartalan kormányzati munka és a társadalom egésze érdekében.*” [8 p. 5]

Véleményem szerint a Magyar Larousse Enciklopédia meghatározása az infrastruktúráról teljes mértékben kimerítő, és lefedi a hazai infrastruktúrákat. Sorra veszi azokat a legfontosabb infrastruktúra elemeket, amelyek hiánya kihatással lenne életünkre, így az értekezésemben a továbbiakban az infrastruktúra fogalmát ennek megfelelően fogom használni.

1.1.2 Kritikus infrastruktúra fogalma

Míg az infrastruktúra fogalma kellő körültekintés árán kielégítő pontossággal meghatározható, a kritikusság ismérvei sokrétűek, szerteágazóak, tudomány- és iparáganként változnak. A magyar nyelvben a kritikus helyett a létfontosságú kifejezés többet mondana, de a nemzetközi szakirodalom a kritikus szót használja, ezért hazánkban is ez ter-

jedt el. Egy infrastruktúra tehát nagyon sok szempontból lehet kritikus, kritikussá minősítéséhez viszont az is elég, ha csak egyetlen egy kritérium szerint az. [9 p. 66]

A kritériumok a következők lehetnek:

- Hatókör**:** földrajzi kiterjedésben mutatja a kritikus infrastruktúra megsemmisülésének, működésképtelenné válásának hatását. Ezen belül megkülönböztetünk nemzetközi, nemzeti, regionális, territoriális vagy helyi hatókört.[10 p. 21]
- Nagyságrend**:** a veszteség, vagy a hatás nagyságrendje (például: nincs hatás, minimális, mérsékelt, vagy jelentős a hatás). A nagyságrend megállapításához a következő szempontokat is érdemes figyelembe venni:
  - népességre gyakorolt hatás (az érintett lakosság száma, áldozatok, betegségek, súlyos sérülések, kitelepítések);
  - gazdasági hatás (GDP[5]-re gyakorolt hatása, jelentős gazdasági veszteség és/vagy termelés, szolgáltatás fokozatos romlása);
  - környezetvédelmi hatás (a lakosságra és lakókörnyezetére gyakorolt hatás);
  - interdependencia (a kritikus infrastruktúrák elemei közötti függőség);
  - politikai hatás (az államba vetett bizalom). [10 p. 21]
- Időbeli hatás**:** mely megmutatja, hogy az adott infrastruktúra, vagy elemének vesztesége mennyi idővel később fejti ki komoly hatását (ez lehet például .: azonnali, 24-48 óra, egy hét, egyéb). [10 p. 21]

Ezek után célszerű megvizsgálni, hogy a biztonság terén élenjáró Amerikai Egyesült Államok és az Európai Unió milyen fogalmi meghatározásokat alkottak a témában.

2001-ben az Amerikai Egyesült Államokat ért támadások után a nemzeti infrastruktúrák védelmében és a terroristák elleni megfelelő fellépés és információszerzés érdekében a kongresszus elfogadta a Patriot Act[6] törvényt. A 2001. október 26-án kiadott törvényben a kritikus infrastruktúrával kapcsolatban a következőket rögzítették: "*a kritikus infrastruktúrák azok a valós és virtuális rendszerek, eszközök, amelyek alapvető fontosságúak az Egyesült Államok számára, és e rendszerek illetve eszközök működésképtelensége vagy megsemmisülése csökkentené a biztonságot, a nemzetgazdaság biztonságát, a nemzeti közegészséget és annak biztonságát vagy mindezek kombinációját.*" [12 p. 130]

Az Európai Unió dokumentuma szerint: "*a kritikus infrastruktúrákhoz azok a fizikai erőforrások, szolgáltatások és információtechnológiai létesítmények, hálózatok, és inf-*

[5] GDP - Gross Domestic Product
[6] USA Patriot Act **-** Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. George W. Bush 2001. október 26-án írta alá.

rastrukturális berendezések tartoznak, melyek összeomlása vagy megsemmisülése komoly következményekkel járna a polgárok egészségére, biztonságára, védelmére vagy gazdasági jólétére, illetve a kormányok hatékony működésére." [13 p. 20]

A fogalmi meghatározás alapján az Európai Unió illetékes bizottsága a kritikus infrastruktúrák közé az alábbiakat sorolja:

- energiatermelés és hálózat (áramszolgáltatás, olaj- és gáztermelés, energiatárolók és finomítók, energiaátadó és elosztó rendszerek);
- kommunikációs és információs technológia (távközlés, műsorszórórendszerek, szoftver, hardver és hálózatok, beleértve az Internetet);
- pénzügy (bankügyletek, kötvények és befektetések);
- egészségügy (kórházak, egészségügyi és vérellátó intézmények, laboratóriumok és gyógyszertárak, kutató és mentőszolgálatok, mentők);
- vízellátás (gátak, víztározók, víztisztítás és vízhálózat);
- élelmiszerellátás (élelmiszer-biztonság és védelem);
- közlekedés (pl.: repterek, kikötők, vasúti és tömegközlekedési hálózatok, közlekedésirányító rendszerek);
- veszélyes áruk termelése, tárolása és szállítása (kémiai, biológiai, radiológiai és nukleáris anyagok);
- kormányzat (kritikus szolgáltatások, létesítmények, információs hálózatok, eszközök és jelentős nemzeti emlékhelyek műemlékek). [13 p. 24]

Magyarországon a 2112/2004. (V.7.) Kormányhatározat a következő területeket sorolta a kritikus infrastruktúrák közé:

- az energiaellátás;
- a közművesítés;
- a közlekedés és szállítás;
- a távközlés, elektronikus adatforgalom és informatikai hálózat;
- a bankrendszer; a szolgáltatások;
- a média;
- az ivóvíz és élelmiszer alapellátás;
- az egészségügyi biztosítás. [14 p.15]

Ezt a 2080/2008. (VI.30.) Kormányhatározat a kritikus infrastruktúra védelem nemzeti programjáról a következő ágazatokra módosította:

- energia;
- infokommunikációs technológiák;

- közlekedés;
- víz;
- élelmiszer;
- egészségügy;
- pénzügy;
- ipar;
- jogrend – kormányzat;
- közbiztonság – védelem. [15 pp. 4-5]

A fenti ágazatokon túl szerteágazóan 43 alágazatot definiál a határozat, amelyet az 1. táblázat ismertet.

A 2080/2008. (VI.30.) Kormányhatározat megalkotásakor figyelembe vették az Európai Uniós állásfoglalást, és egy teljesebb és szerteágazóbb ágazat és alágazati csoportokat definiáltak.

Kidolgozás alatt van egy törvényjavaslat, amely a „ 2012. évi …. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről” szól.[16] Ez definiálja:

- a létfontosságú rendszert és létesítményt;
- a kritikus infrastruktúra üzemeltetőjét;
- a kritikus infrastruktúra védelmét;
- a horizontális kritériumokat;
- az ágazati kritériumokat;
- a nemzeti kritikus infrastruktúra elemeit;
- az európai kritikus infrastruktúra elemeit.

A törvényjavaslat megtartotta a 2080/2008. Kormányhatározat ágazat és alágazati besorolását.

1. táblázat: Kritikus infrastruktúrák ágazatai és alágazatai

Ágazat	Alágazat
I. Energia	1. kőolaj kitermelés, finomítás, tárolás és elosztás
	2. földgáztermelés, tárolás, szállítás és rendszerirányítás, elosztás
	3. villamosenergia-termelés, átvitel és rendszerirányítás, elosztás
II. Infokommunikációs technológiák	4. információs rendszerek és hálózatok
	5. eszköz-, automatikai és ellenőrzési rendszerek
	6. internet, infrastruktúra és hozzáférés
	7. vezetékes és mobil távközlési szolgáltatások
	8. rádiós távközlés és navigáció
	9. műholdas távközlés és navigáció
	10. műsorszórás
	11. postai szolgáltatások
	12. kormányzati informatikai, elektronikus hálózatok
II. Közlekedés	13. közúti közlekedés
	14. vasúti közlekedés
	15. légi közlekedés
	16. vízi közlekedés
	17. logisztikai központok
IV. Víz	18. ivóvíz szolgáltatás
	19. felszíni és felszín alatti vizek minőségének ellenőrzése
	20. szennyvízelvezetés és -tisztítás
	21. vízbázisok védelme
	22. árvízi védművek, gátak
V. Élelmiszer	23. élelmiszer előállítás
	24. élelmiszer-biztonság
VI. Egészségügy	25. kórházi ellátás
	26. mentésirányítás
	27. egészségügyi tartalékok és vérkészletek
	28. magas biztonsági szintű biológiai laboratóriumok
	29. egészségbiztosítás
VII. Pénzügy	30. fizetési, értékpapírklíring- és elszámolási infrastruktúrák és rendszerek
	31. bank és hitelintézeti biztonság
VIII. Ipar	32. vegyi anyagok előállítása, tárolása és feldolgozása
	33. veszélyes anyagok szállítása,
	34. veszélyes hulladékok kezelése és tárolása,
	35. nukleáris anyagok előállítása, tárolása, feldolgozása
	36. nukleáris kutatóberendezések
	37. hadiipari termelés
	38. oltóanyag és gyógyszergyártás
IX. Jogrend - Kormányzat	39. kormányzati létesítmények, eszközök
	40. közigazgatási szolgáltatások
	41. igazságszolgáltatás
X. Közbiztonság - Védelem	42. honvédelmi létesítmények, eszközök, hálózatok
	43. rendvédelmi szervek infrastruktúrái

Forrás: [15 pp. 4-5]

Véleményem szerint, mivel napjainkban már vezeték nélküli hálózatokat számos társadalmi-gazdasági szereplő használ, ezért tekintettel a fentiekre is az értekezésemben a továbbiakban a 2080/2008. (VI.30.) Kormányhatározat ágazat és alágazati csoportosítását fogom használni a kritikus információs infrastruktúrák vizsgálatára.

1.1.3 Kritikus információs infrastruktúra fogalma

Az, hogy mit tekintünk kritikus információs infrastruktúrának, a kritikus infrastruktúrák védelmére vonatkozó európai programról szóló Zöld Könyv a következőképpen fogalmazza meg: "*Kritikus információs infrastruktúrák közé azok sorolandók, melyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, Internet, műholdak stb.)*". [17 p. 3]

„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." [11]

Rendeltetés szerint az információs infrastruktúrákat két csoportba sorolhatjuk:

- funkcionális információs infrastruktúra;
- támogató információs infrastruktúra.

A funkcionális infrastruktúrák fizikailag lehetővé teszik a társadalom valamilyen információs funkciójának zavartalan működését, vagyis infrastrukturális alapon információs alapszolgáltatásokat végeznek.

A támogató információs infrastruktúrák létrehozzák és folyamatosan biztosítják a funkcionális információs infrastruktúrák nagy halmazainak zavartalan működéséhez és fejlődéséhez szükséges anyagi és szellemi alapokat, valamint támogatási háttereket. [18]

A funkcionális információs infrastruktúrák egyféle megközelítésből a következőek lehetnek:

- légi forgalmat, repülésirányítást és légi navigációt biztosító rendszerek;
- távirányító és robotok vezérlését biztosító rendszerek;

- légvédelmi fegyverirányítást biztosító rendszerek;
- zárt távközlési különhálózatok;
- műsorszóró és tájékoztató hálózatok;
- vezetési rendszerek;
- informatikai hálózatok,
- távérzékelést, távellenőrzést biztosító rendszerek;
- nyílt előfizetői távközlési hálózatok. [19 p. 6]

A funkcionális információs infrastruktúrák a különböző infokommunikációs rendszerek köré csoportosíthatók:

- számítógép-hálózatok (LAN[7], MAN[8], WAN[9]);
- vezetékes távközlő rendszerek (analóg, ISDN[10]);
- vezeték nélküli távközlő rendszerek:
  - mobil cellás rádiótelefon rendszerek (GSM[11]);
  - diszpécser földi mobil hálózatok (TETRA[12]);
  - személyhívó rendszerek;
  - műholdas távközlési rendszerek;
- műholdas navigációs rendszerek (GPS[13]) stb.[19 p. 9]

A támogató információs infrastruktúrák pedig a következők:

- elektronikai és informatikai vállalatok;
- raktárak, nagykereskedelmi ellátó vállalatok;
- elektronikai és informatikai képzéssel foglalkozó tanintézetek;
- villamos energetikai ellátó rendszerek;
- elektronikai és informatikai kutató és fejlesztő intézetek.[7 p. 75]

A fent említett infrastruktúrák egymással valamilyen szinten kapcsolatban vannak, de egyéb szolgáltatásaikat csak különböző korlátozásokkal bocsátják a felhasználók rendelkezésére. Például egy tartalomszolgáltató vagy egy hálózat-rész lehet egy kisebb információs infrastruktúra része úgy, hogy ugyanakkor nem része egy kapcsolódó nagyobb infrastruktúrának.

[7] LAN - Local Area Network
[8] MAN - Metropolitian Area Network
[9] WAN - Wide Area Network
[10] ISDN - Integrated Services Digital Network
[11] GSM - Global System for Mobile Communications
[12] TETRA - Terrestrial Trunked Radio
[13] GPS - Global Positioning System

Az összekapcsolt információs infrastruktúrákat kiterjedésük szerint a következőképpen csoportosíthatjuk:

- globális (világméretű);
- regionális (pl. európai);
- nemzeti (országos). [18]

A *globális információs infrastruktúra* fogalma a következőképpen fogalmazható meg:„*A globális információs infrastruktúra összekapcsolt információs rendszerek és az őket összekapcsoló rendszerek világméretű összessége.*" [18]

„*A globális információs infrastruktúra kommunikációs hálózatok, számítógépek, adatbázisok és felhasználói elektronika világméretű összekapcsolódása, amely óriási mennyiségű információt tesz hozzáférhetővé a felhasználók számára.*" [18]

„*A globális információs infrastruktúra a következő hat elemet foglalja magában: kommunikációs infrastruktúra; számítógépek és berendezések; szoftverek és alkalmazások; az információtartalom; az infrastruktúra összetevőit fejlesztő, gyártó, forgalmazó és szervizelő személyek és szervezetek; valamint az infrastruktúrát használó személyek és szervezetek.*" [18]

A fenti fogalmakból látszik, hogy megfogalmazóik inkább az alkotó elemeket tartották fontosnak és nem az infrastruktúrát magát.

A regionális információs infrastruktúrák a globális információs infrastruktúrák szerves részei. A világot átszövő információs infrastruktúrák régiókra bonthatók, amelyek lehetnek például a kontinensek, vagy valamilyen szövetség által meghúzott határvonalak (pl. EU[14]).

A *nemzeti információs infrastruktúra* fogalmát a következőképpen fogalmazták meg: „*A nemzeti információs infrastruktúra kommunikációs hálózatok, számítógépek, adatbázisok és felhasználói elektronika nemzeti szintű összekapcsolódása, amely óriási mennyiségű információt tesz hozzáférhetővé a felhasználók számára.*" [18]

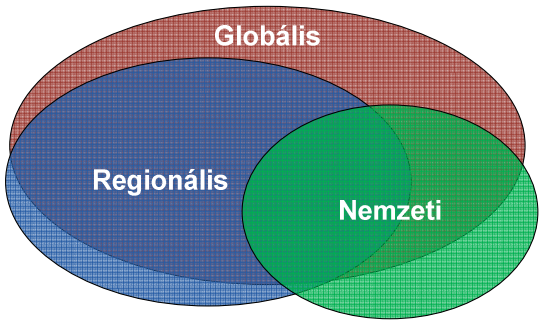
„*A nemzeti információs infrastruktúra szervezetek, eszközök és erőforrások széles körben hozzáférhető, egységes rendszere, amelynek rendeltetése elsősorban egy adott nemzet kormányzati, gazdálkodó és más szervezetei, valamint állampolgárai alapvető információ- és információs szolgáltatás-igényeinek elsősorban az adott ország területén történő kielégítése.*„ [18]

[14] EU - European Union

Ezek alapján a nemzeti információs infrastruktúrák tekinthetőek a világot átszövő hálózat legkisebb alkotóelemeinek, amelyek nélkül nem valósulhatna meg kommunikáció.

Ezen infrastruktúrák nagy hányadának nem az állam a tulajdonosa. Ez nem azt jelenti, hogy az állam nem fordít figyelmet ezen infrastruktúrák védelmére, hanem azt, hogy a védelmet az állami és a magánszektor szereplői közösen valósítják meg.

Az összekapcsolt infrastruktúrák kapcsolatát és egymástól való függőségét az 1. ábra mutatja be.



1. ábra: Összekapcsolt információs infrastruktúrák egymásra hatása kiterjedésük szerint
Forrás: saját szerkesztés

Az 1. ábra jól szemlélteti, hogy egy nemzeti információs infrastruktúra lehet regionális és globális is, de vannak a csoportoknak olyan szereplői, amelyek csak az egyik csoportba tartoznak. Az is jól kivehető, hogy az információs infrastruktúrák egymásra épülnek és csak kis szegmensei különülnek el egymástól. Például egy távközlési vállalat kommunikációs szolgáltatásainak fennakadása alapvetően nemzeti probléma, de ha ez kihatással van a környező országokra, akkor már regionális, amely továbbgyűrűzve globális méreteket is ölthet.

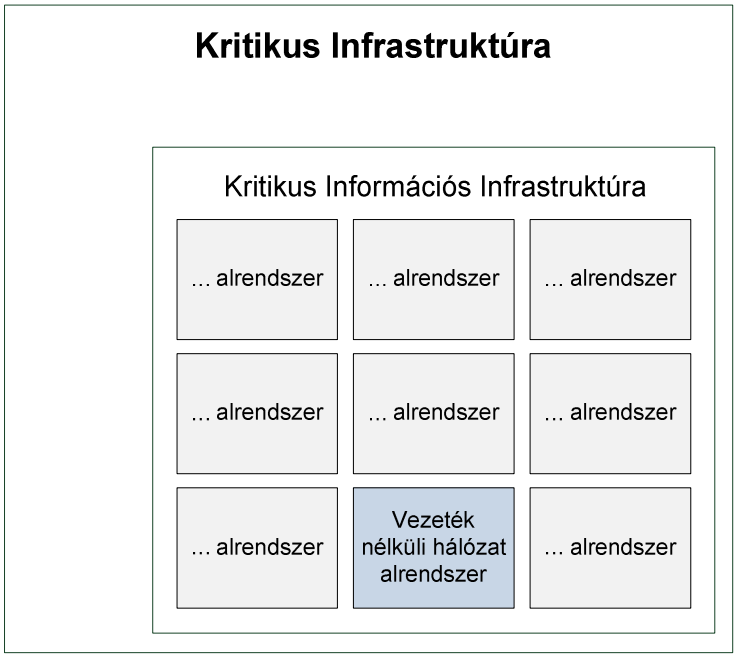
A regionális-nemzeti infrastruktúra függőségét szemlélteti a 2012. júliusában, Indiában a fél országot érintő áramkimaradás. Ennek fő oka, hogy az infrastruktúrák folyamatos bővülésével és fejlődésével párhuzamosan az ország energiaellátó rendszere nem újult meg. Ezért az ország energia-felvétele több, mint a rendelkezésre álló energiakészlet. Az ilyen esetek kiküszöbölésére több nagyvállalat és gyár saját energiaellátó központot létesített.[20]

Az EU Zöld Könyv szerint a kritikus információs infrastruktúrák azok az infrastruktúrák, amelyek önmagukban is kritikus infrastruktúrának minősülnek - ez jelen esetben a 2080/2008. Kormányhatározat szerint az infokommunikációs technológiák ágazat -, illetve azok, amelyek a többi kritikus infrastruktúra működéséhez elengedhetetlenül fontos vezetési, irányítási funkciókat látnak el. Ez alapján a 2080/2008. Kormányhatá-

rozat ágazati besorolásait figyelembe véve a kritikus információs infrastruktúrák alatt az alábbiakat értelmezhetjük:

- energiaellátó rendszerek rendszerirányító infokommunikációs hálózatai;
- infokommunikációs hálózatok (vezetékes, mobil, műholdas);
- közlekedés szervezés és irányítás infokommunikációs hálózatai;
- vízellátást szabályzó infokommunikációs hálózatok;
- élelmiszerellátást szabályzó infokommunikációs hálózatok;
- egészségügyi rendszer infokommunikációs hálózatai;
- pénzügyi-gazdasági rendszer infokommunikációs hálózatai;
- ipari termelést irányító infokommunikációs hálózatok;
- kormányzati és önkormányzati szféra infokommunikációs hálózatai;
- védelmi szféra infokommunikációs hálózatai. [22 p. 175]

A vezeték nélküli hálózatok ezen kritikus információs infrastruktúrák alrendszerében értelmezhetőek. A fentiek alapján a kritikus infrastruktúra, a kritikus információs infrastruktúra és a vezeték nélküli hálózat kapcsolatát a következő struktúrában lehet ábrázolni (2. ábra):



2. ábra: A kritikus infrastruktúra, a kritikus információs infrastruktúra és a vezeték nélküli hálózat kapcsolata

Forrás: saját szerkesztés

Az értekezésemben kutatásaimra és vizsgálataimra alapozva a továbbiakban a kritikus információs infrastruktúrák csoportosításának alapjául Haig Zsoltnak „Az információs társadalom információbiztonsága” című cikkében megfogalmazott csoportosítást fogadom el. [22] Vizsgálataimat ez alapján fogom a későbbiekben folytatni.

1.2 A kritikus információs infrastruktúrák függősége

A gazdaság dinamikus fejlődéséhez nagyban hozzájárult az informatika és a telekommunikáció térhódítása. Ma már nem is tudunk elképzelni olyan modern munkaállomást, ahol a dolgozó munkáját valamilyen technikai vívmány ne segítené. Nincs ez máshogyan a kritikus információs infrastruktúrákban sem.

A fenyegetések minimalizálására több módszer alkalmazható. Ezek közé tartozik a kockázatelemzés, mely valószínűségi számításokat, matematikai logikát, kvantitatív, kvalitatív módszereket tartalmazhat. A technika és az általa nyújtott szolgáltatás nem csak az adott infrastruktúrát hálózza be, hanem az infrastruktúra nyújtotta szolgáltatásai révén szoros kapcsolatban (függésben) van más infrastruktúrákkal is.

A kritikus információs infrastruktúrák közötti függéseket, illetve egy kritikus információs infrastruktúrán belüli függéseket azonban ezek a modellek nem, vagy csak nagyon áttételesen érintik. Ezért dolgozatomban egy olyan rendszerszemléletű modellt alkotok meg, amely alkalmas az inter- és intradependenciák modellezésére, a függőségek tartalmának feltérképezésére.

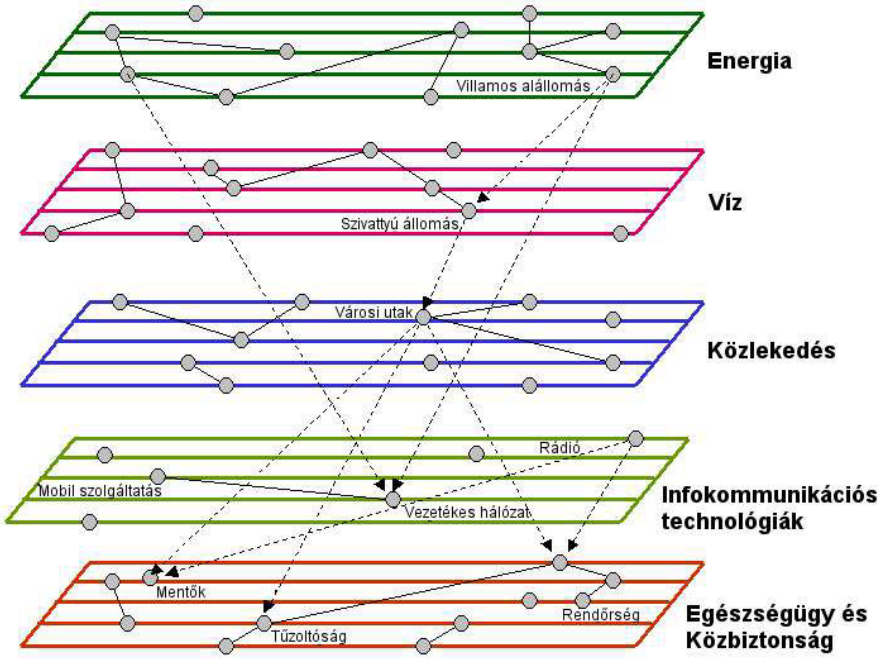
A társadalomban és a gazdasági életben is egyre elterjedtebb az informatika, a telekommunikáció. A gyorsabb, intenzívebb változások megnövelték a társadalom technológiai függését, növekedtek a változásokban rejlő lehetőségek és a potenciális veszélyek is. [23 pp. 200-205]

A kritikus infrastruktúrák és ezen belül a kritikus információs infrastruktúrák azonosítása, priorálása, a veszélyeik és sérülékenységeik felmérése, a védelmi terveik meghatározása és kialakítása egyre égetőbb kérdés és számos országban – így hazánkban is – komoly kihívást jelent.

A kritikus információs infrastruktúra védelmének kialakításakor a kockázatok felmérésének egyik lényeges pontja a kritikus információs infrastruktúrák közötti interdependenciák (kölcsönös függőség) és az egyes kritikus információs infrastruktúrákon belüli intradependenciák (belső rendszerelemtől való függőség) feltárása. A másik lényeges sarokpont ezen függőségek jellegének és tartalmának feltárása, hiszen ezek

kezelése csak megfelelő előismeretek birtokában teszi az inter- és intradependenciát csökkentő védelmet teljes körűvé, zárttá és kockázatarányossá. A függőségek ismeretében a kritikus infrastruktúra működése biztonságosabbá tehető.

A kritikus infrastruktúrák védelmi képességeinek beazonosításakor nem minden esetben történik meg az inter- és intradependencia totális feltérképezése. Nem könnyű ezt a feladatot elvégezni, hiszen a modellezés során figyelembe kell venni a különböző szervezeteket, rendszereket és alrendszereket, illetve ezek kölcsönös kapcsolatrendszerét. A modellezés az első lépés, amellyel közelebb kerülhetünk a helyes megoldáshoz. Az 3. ábra az Amerikai Egyesült Államokbeli New Orleans példáján keresztül mutatja be a kritikus infrastruktúra ágazatait, alágazatait és a köztük lévő kapcsolatokat.



3. ábra: New Orleans infrastruktúra interdependenciái

Forrás: [24 p. 3]

A közelmúlt egyik jelentős környezeti katasztrófája, a Katrina hurrikán megmutatta, hogy az összekapcsolódó infrastruktúrákon keresztül a problémák felhalmozódhatnak, váratlanabb és lényegesen súlyosabb működésbeli zavart okozhatnak az adott állam létfontosságú szolgáltatásaiban. Az infrastruktúrák összekapcsolódásai, és egymástól való függőségei sérülékenyebbé teszi őket támadások, zavarok, megsemmisítésre irányuló tevékenységekkel szemben. Ezt szemlélteti az alábbi láncolat: példának okáért az

energiatermelés függ a szállítástól. A szállítás függ az energiától. Mindkettő függ az infokommunikációs rendszerektől, míg az infokommunikációs rendszerek energiafüggők. [10]

Sajnos hazánk sem maradt ki a negatív tapasztalatgyűjtésből, hiszen a Magyarországon 2010-ben bekövetkezett vörösiszap-katasztrófa is rávilágított arra a tényre, hogy az összekapcsolódó infrastruktúrákon keresztül az esemény megtörténte után azok az infrastruktúrák amelyek sérültek vagy megsemmisültek az interdependenciák miatt, megnehezítették a mentést és a helyreállítást. A katasztrófa következtében a sajnálatos emberáldozatokon túl sérült a közúti-, a vasúti infrastruktúra, továbbá a vízbázisok, a termőföldek, a lakó- és ipari ingatlanok. A mentésre és katasztrófa-elhárításra kiérkezett szakemberek több problémával is szembesültek, de ami az értekezésem szempontjából talán az egyik legfontosabb, hogy a megnövekedett mobiltelefon forgalmat a hálózat nem tudta kiszolgálni. Az elhárításban résztvevő szakemberek rendelkeztek ugyan saját kommunikációs rendszerrel, de ezek összehangolása nehéz feladatnak bizonyult. [25 p. 10] A 4. ábra egy a helyszínre érkezett rádió-kommunikációs állomást mutat.

4. ábra: Kárhelyszíni rádió-kommunikációs állomás

Forrás: [26 p. 19]

Ez a rádió-kommunikációs állomás segítette pár napig a mentésben résztvevő szakembereket.

A kritikus információs infrastruktúrák védelme elsődleges szempont minden nemzet számára. Ma Magyarországon a Zöld Könyv alapján a nemzeti kritikus infrastruktúra védelem végrehajtásának lépései a következők:

- fogalmak tisztázása, keretrendszer alapjainak meghatározása;
- szektorelemzés, ágazati fogalmak, kritériumok meghatározása;
- kölcsönös függőség (interdependencia elemzés);

- kockázat, veszély, és sebezhetőség elemzés;
- védelmi intézkedések megtétele;
- végrehajtás ellenőrzése és értékelés. [27 p. 137]

Ezek a lépések a kritikus információs infrastruktúrák védelme szempontjából is végrehajthatóak. A felsorolásból is jól látható, hogy a kölcsönös függőségek elemzése fontos pillére lehet a kritikus információs infrastruktúrák védelmének. Az inter- és intradependenciák hatékony és eredményes feltárásához, értékeléséhez azonban rendszerszemléletű modell megalkotása szükséges.

A kritikus információs infrastruktúra minden esetben része vagy önmaga egy kritikus infrastruktúrának, függőségei megegyeznek a kritikus infrastruktúra függőségeivel ezért vizsgálataimat a továbbiakban a kritikus információs infrastruktúrákra végzem el. Az elkészült módszerek érvényesek lesznek a kritikus infrastruktúrára is.

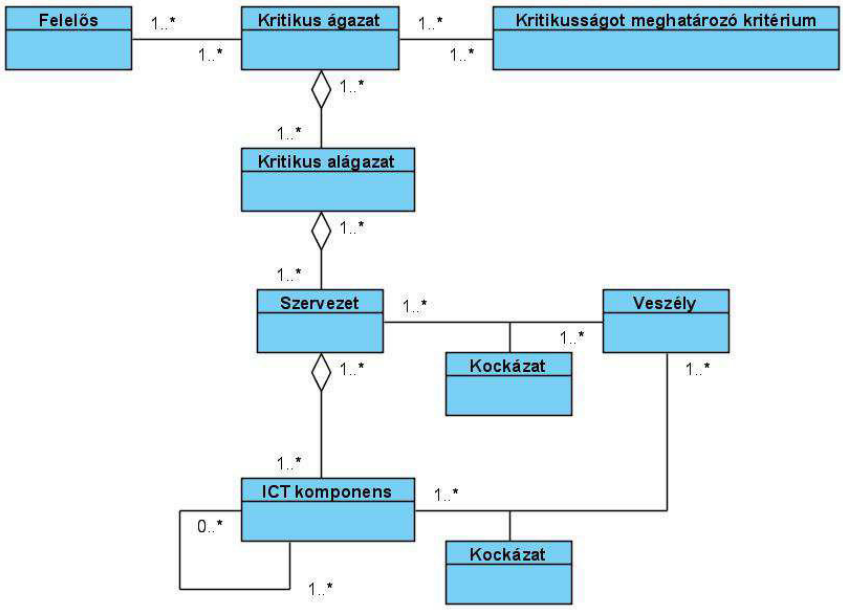
1.3 Kritikus információs infrastruktúra függőségének modellezése

A kritikus információs infrastruktúra függőségi modellezése kapcsán meg kell vizsgálni a függőségi modell elemeit, magát a függőségi modellt, a hatásokat és a modellezés szintjeit.

1.3.1 Kritikus információs infrastruktúra függőségének modell elemei

A kritikus információs infrastruktúra interdependencia modellben szerepelni kell az ún. kritikus információs infrastruktúra hierarchiának, vagyis a nemzetközi, nemzeti, EU kritikus információs infrastruktúra elemeknek; továbbá azonosítania kell az egyedi kritikus információs infrastruktúra szervezeteket, melyeknek kapcsolódniuk kell a 2080/2008. (VI. 30.) Kormányhatározatban felvázolt kritikus ágazat-alágazat struktúrához. (5. ábra)

A vizsgálataim során az UML ábrázolást azért használtam, mert egy egyszerű, általános célú modellező nyelv, amely lehetővé teszi műszaki, grafikus és szöveges modellek elkészítését.



5. ábra: Kritikus információs infrastruktúra hierarchia modell struktúra UML[15] objektum diagramja

Forrás: [28 p. 4]

A kritikus információs infrastruktúra hierarchia modell bemutatja a kritikus információs infrastruktúra szereplőit és ezek egymástól való függését. A modellnek továbbá tartalmaznia kell az egyes kritikus információs infrastruktúrák kritikusságát meghatározó kritériumokat, vagyis egy kritikus információs infrastruktúra elvesztésének a:

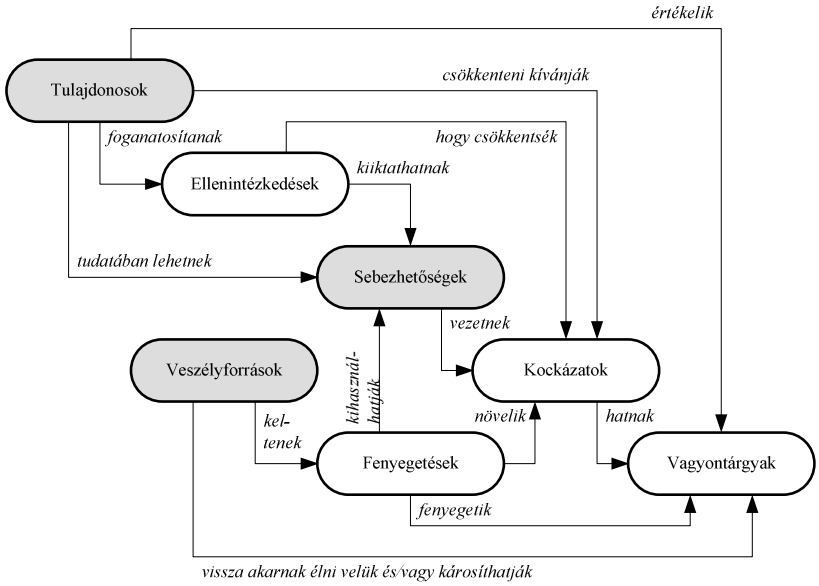
- hatókörét;
- nagyságrendjét;
- időbeni hatását.

A hatókörnél meg kell vizsgálni, hogy a kritikus információs infrastruktúra egészének vagy egy részének elvesztése, elérhetetlensége milyen földrajzi kiterjedésben okoz károkat az állampolgárok gazdasági, szociális jóléte, közegészsége, közbiztonsága, a nemzetbiztonság, a nemzetgazdaság és a kormányzat működése szempontjából. A nagyságrendnél meg kell vizsgálni, hogy a kritikus információs infrastruktúra egészének vagy egy részének elvesztése, elérhetetlensége milyen hatást okoz; továbbá az időbeni hatásnál meg kell vizsgálni, hogy a kritikus információs infrastruktúra egészének vagy egy részének elvesztése, elérhetetlensége milyen időtávon mennyi ideig befolyásolja az infrastruktúra újbóli működését. [27 p. 170]

[15] UML - Unified Modelling Language

Mivel a kritikus információs infrastruktúra inter- és intradependenciáinak értékelése nem egy-egy gazdasági szervezet szintjén és nem csak valamely állami szerv feladataként valósul meg, hanem össznemzeti védelmi feladatként, ezért csak az államigazgatás, a nemzetvédelmi és az érintett gazdasági szervezetek hatékony és eredményes együttműködésével lehet teljes körű, zárt és kockázatarányos védelmet kialakítani. Ennek a feltételnek a teljesítése miatt a modellnek lehetővé kell tennie a top-down elemzést (pl. a kritikus információs infrastruktúra azonosítást és priorálását), a bottom-up tervezést (pl. az egyes kritikus információs infrastruktúra elemek függőségeinek vizsgálatát, kapcsolatainak azonosítását).

Az ismert és elterjedten alkalmazott IT biztonságra, ill. üzemeltetésre vonatkozó ajánlások (TCSEC[16], ITSEC[17], CC[18], ISO27001[19], ITIL[20], COBIT[21] stb.) a kritikus infrastruktúrák esetén is relevánsnak tekinthetők és alkalmazhatók. [122] A kockázatelemzésben felhasználandó elemzendő objektumokra és azok általános kapcsolataira „Az informatikai biztonságértékelés közös szempontjai” (Common Criteria) ad egy a gyakorlatban is tesztelt és használható modellt, ami nem csak az információtechnológia, hanem valamennyi vagyontárgy kockázatainak elemzésére alkalmazható. (6. ábra)



6. ábra: Kockázatelemzés fogalmi modellje

Forrás: [29 p. 12]

[16] TCSEC - Trusted Computer System Evaluation Criteria
[17] ITSEC - Information Technology Security Evaluation Criteria
[18] CC - Common Criteria
[19] ISO27001 - Standards for information security management systems
[20] ITIL - Information Technology Infrastructure Library
[21] COBIT - Control Objectives for Information and Related Technologies

A fenti koncepció modellből látható, hogy a szűken vett kockázatelemzéshez a

- vagyontárgy;
- fenyegető tényező;
- kockázat;
- sebezhetőség;
- ellenintézkedés elem-ötös meghatározása és értékelése szükséges.

A fenti ábrából az is jól látható, hogy a kockázatelemzést egy-egy vagyontárgy-fenyegetés párosra kell elvégezni. Általánosságban, konkrét védendő érték hiányában nincs értelme elemzésről beszélni. A modell alapján kimondható az is, hogy egy eredményes kockázatelemzéshez részletes erőforrásleltárra van szükség, illetve célszerű mind a veszélyforrások, mind az alkalmazott védelmi intézkedések listáját is törzsadatbázis elemként felvenni.

Értekezésemben a továbbiakban csak a kritikus információs infrastruktúra függőséget közvetlenül befolyásoló kérdésekkel foglalkozom.

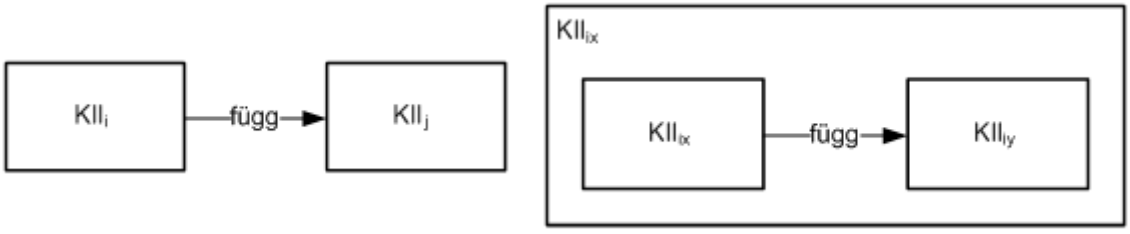
1.3.2 Függések modellezése

A szakirodalomban felmerül az inter- és intradependencia kérdése, amelyet modellezési szempontból is kezelni kell.[10] Az interdependencia (a kölcsönös egymásra hatás) vizsgálata rendkívül fontos. Ennek során a vizsgált infrastruktúra más infrastruktúrákra gyakorolt negatív hatását kell vizsgálni. Hangsúlyozni kell, hogy az interdependencia értékelése nagy fontossággal bír, mert ezek akár egy, akár több ágazat vagy alágazat bevonását illetve ezt követően egységes modellezését is lehetővé teszik. A vizsgálat mennyiségi (kvantitatív) jellemzőkön alapul. [27 p. 171]

Az interdependencia kettő vagy több kritikus információs infrastruktúra közötti függést jelent (javasolt jelölése: $A \rightarrow B$, azaz „B" kritikus információs infrastruktúra elem függ „A" kritikus információs infrastruktúra elemtől). Az intradependencia egy adott kritikus információs infrastruktúra valamely belső elemétől (esetleg önmagától) való függését jelenti (javasolt jelölése: $A \rightarrow A_i$, azaz „A" kritikus információs infrastruktúra elem függ az „A_i" - azaz az i-edik - alrendszerétől). Ez a függés rendszerint az „A" kritikus információs infrastruktúra rendszernek saját belső rész kritikus információs infrastruktúra rendszereinek függését jelenti.

Véleményem szerint modellezési szempontból a kritikus információs infrastruktúra rendszerek, alrendszerek közötti függés kritikus információs infrastruktúra rendszer-

komponensek közti függéseként értelmezhető és ábrázolható. Tehát a modell elemzési részlet finomításával az inter- és intradependencia ekvivalensként kezelhető, az intradependencia elhagyható, amit az 7. ábra b.) része szemléltet.



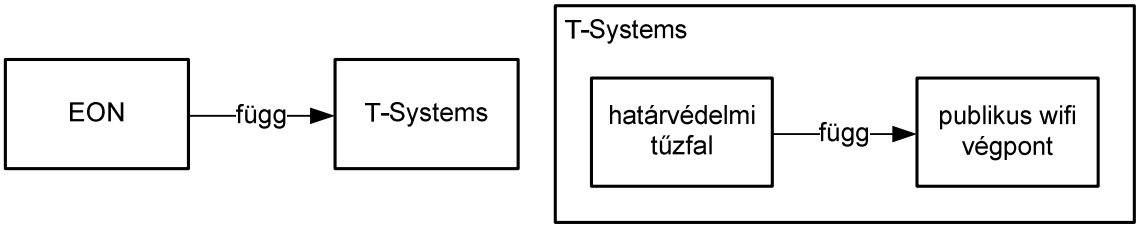
a.) Interdependencia b.) Intradependencia

KII_i,KII_j – különböző kritikus információs infrastruktúrák

7. ábra: Inter és intradependencia helyettesítési modellje

Forrás: [28 p. 7]

Egy példát vázol a következő ábra:



a.) Interdependencia b.) Intradependencia

8. ábra: Kritikus információs infrastruktúrák inter- és intradependenciája

Forrás: saját szerkesztés

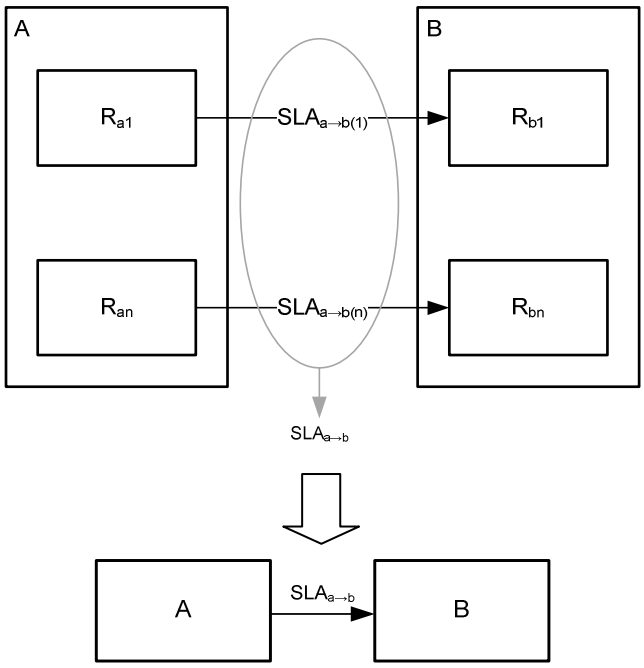
A kritikus információs infrastruktúrák közti függés vizsgálható egyrészt a függésben lévő rendszerelem, másrészt a függés alapjául szolgáló szolgáltatást nyújtó rendszerelem szempontjából.

Véleményem szerint ez a függés modellezhető egy sajátos nyújtott-fogadott szolgáltatási szintmegállapodásként (SLA[22]), amely azonban a rendelkezésre állással kapcsolatos metrikákat tartalmazza, valamint a szolgáltatás elmaradásának következményeit (hatást) mutatja be. A szolgáltatás-alapú megközelítéssel kezelhető lenne az a probléma

[22] SLA - Service Level Agreement

(is), hogy az alacsony modellezési szinten feltárt függőségeket egy magasabb elemzési szinten (szervezet-szervezet, alágazat-alágazat stb.) is értelmezni lehessen.

Javaslatom alapján például egy szervezet-szervezet függőség felírható az igénybevevő szervezet számára szolgáltatást nyújtó alrendszerei szolgáltatásainak halmazaként (a két szervezet „szolgáltatási interfészén” keresztül nyújtott/fogadott szolgáltatások összegeként). A 9. ábra ezt mutatja be.



A,B – szervezetek

R_a,R_b – a szervezeteken belül szolgáltatást nyújtó alrendszerek

SLA – a rendszerek és/vagy szervezetek közötti nyújtott-fogadott szolgáltatási szintmegállapodások

9. ábra: A kritikus információs infrastruktúra szolgáltatási interfész egyedi függéseinek egyszerűsítése kumulált függéssel

Forrás: [28 p. 8]

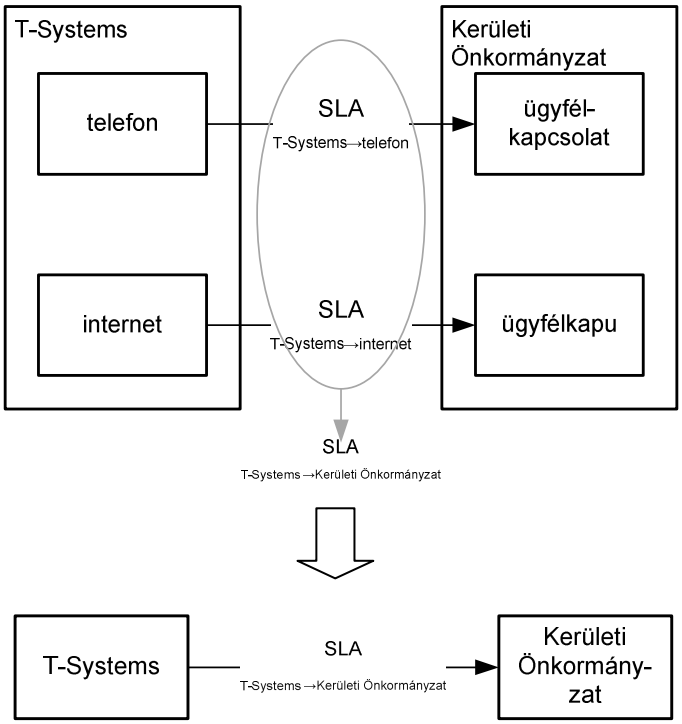
A függést leíró SLA - maga a függést ábrázoló irányított egyenes - javasolt tartalma „A kritikus információs infrastruktúrák meghatározásának módszertana” alapján a következő: [27 p. 171]

2. táblázat: Kritikus információs infrastruktúra SLA mátrix

	Alacsony	Közepes	Magas
Hatókör	0|1	0|1	0|1
Nagyságrend: a népességre gyakorolt hatás	0|1	0|1	0|1
Nagyságrend: a gazdasági hatás	0|1	0|1	0|1
Nagyságrend: interdependencia	0|1	0|1	0|1
Nagyságrend: politikai hatás	0|1	0|1	0|1
Időbeli hatás	0|1	0|1	0|1

Forrás: [28 p. 8]

Ezzel a típusú ábrázolással felírható például egy távközlési szolgáltató és egy Kerületi Önkormányzat függéseinek kapcsolata is. Ezt mutatja a következő ábra:



10. ábra: Távközlési szolgáltató és egy Kerületi Önkormányzat függéseinek kapcsolata

Forrás: saját szerkesztés

Az SLA mátrixot minden függésre fel lehet írni. A következő mátrix a távközlő szolgáltató és a Kerületi Önkormányzat telefon és ügyfélkapcsolat leírását mutatja a „A kritikus információs infrastruktúrák meghatározásának módszertana” alapján: [27 p. 171-173]

3. táblázat: A távközlési szolgáltató és a Kerületi Önkormányzat telefon és ügyfélkapcsolat SLA mátrixa

	Alacsony	Közepes	Magas
Hatókör	1	0	0
Nagyságrend: a népességre gyakorolt hatás	1	0	0
Nagyságrend: a gazdasági hatás	1	0	0
Nagyságrend: interdependencia	1	0	0
Nagyságrend: politikai hatás	1	0	0
Időbeli hatás	1	0	0

Forrás: saját szerkesztés

A távközlő szolgáltató és a Kerületi Önkormányzat függőségeinek egyszerűsített kumulált függési ábrázolásához tartozó SLA mátrix nem lesz más, mint az egyenként felvett mátrixok összegzett értéke. Ezeket az összegzett értékeket a „A kritikus információs infrastruktúrák meghatározásának módszertana” szakirodalom a következőképpen fogalmazza meg: „Az alacsony értéket -1, a közepes értéket 0, a magas értéket 1-gyel számszerűsítve a besorolások egyszerű összegét számoljuk ki.” [27 p. 173]

Ezzel a módszerrel elkészíthető az egyszerűsített kumulált függési ábra és az ábrához tartozó SLA mátrix.

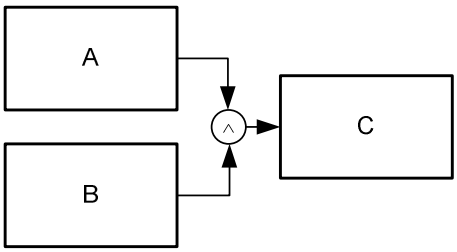
1.3.3 Hatás gráf felépítése

A valós életben a kritikus információs infrastruktúra modellelemek kapcsolata rendszerint nem 1:1 típusú. Egy rendszerkomponens (pl. villamos hálózat irányító rendszere) több más rendszerkomponens működéséhez nyújt alapvető szolgáltatást, illetve egy alkalmazás több egyéb rendszerkomponens működésétől függ (pl. az alkalmazást futtató hardvertől, operációsrendszertől, az adatokat szolgáltató adatbázis-kezelőtől, az ezek közti adatkapcsolathoz nélkülözhetetlen számítógépes hálózatoktól stb.).

A kapcsolatok n:m jellegének (azaz, hogy egy rendszerkomponenstől több más komponens is függhet, illetve, hogy egy rendszerkomponens több más komponenstől is függ) modellezését például hatás gráfok segítségével lehet megvalósítani (a támadási fákhoz hasonló szerkezetben), melyek logikai kapcsolókkal fűzik össze az egyes rendszerelemek egymásra gyakorolt hatását. Az alapként szolgáló támadási fákkal szemben az így kialakított irányított háló (ahol az irányítást a nyújtott/fogadott szolgáltatás iránya

adja meg) nem csak levél-gyökér irányban járható be, hanem lehetséges valamennyi csomópont vizsgálata az abba vezető élek bejárásával.

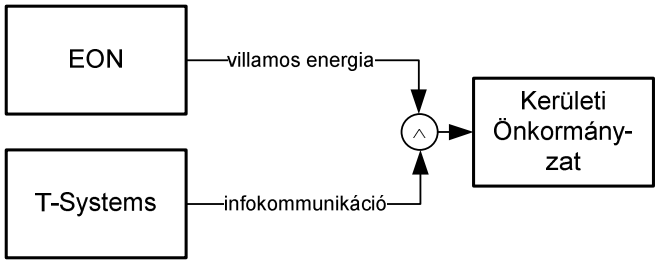
A szolgáltatást igénybevevő rendszerkomponens funkcionalitásának, rendelkezésre állásának fenntartásához egymástól függetlenül is szükséges szolgáltatások esetére alkalmazom az „és” kapcsolót, amelynek jelentése: „C” erőforrás működéséhez „A” és „B” erőforrások együttes szolgáltatása szükséges, bármelyikük kiesése „C” funkcionalitásának és rendelkezésre állásának sérülésével vagy megszűnésével jár együtt. Ezt a kapcsolatot szemlélteti a következő ábra:



11. ábra: „és” kapcsoló

Forrás: [28 p. 9]

Ennek példaszerű felírását a következő ábra mutatja, ahol a Kerületi Önkormányzat működéséhez szükség van villamos energiára és infokommunikációs szolgáltatásra is.

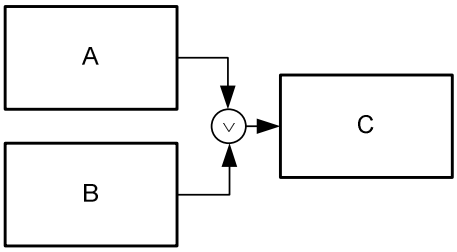


12. ábra: Villamos energia és infokommunikációs szolgáltatás „és” kapcsolatban

Forrás: saját szerkesztés

A szolgáltatást igénybevevő rendszerkomponens funkcionalitásának, rendelkezésre állásának fenntartásához egymást kiegészítő (redundáns) szolgáltatások esetére alkalmazom a „vagy” kapcsolót, amelynek jelentése: „C” erőforrás működéséhez „A” vagy „B” erőforrások szolgáltatásai szükségesek, bármelyikük egyedüli kiesése nem jár együtt „C” funkcionalitásának és rendelkezésre állásának sérülésével.

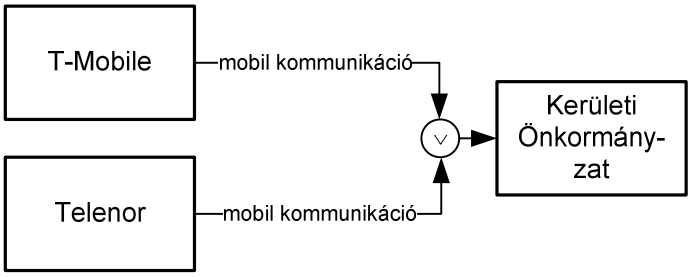
Ezt a kapcsolatot szemlélteti a következő ábra:



13. ábra: „vagy” kapcsoló

Forrás: [28 p. 9]

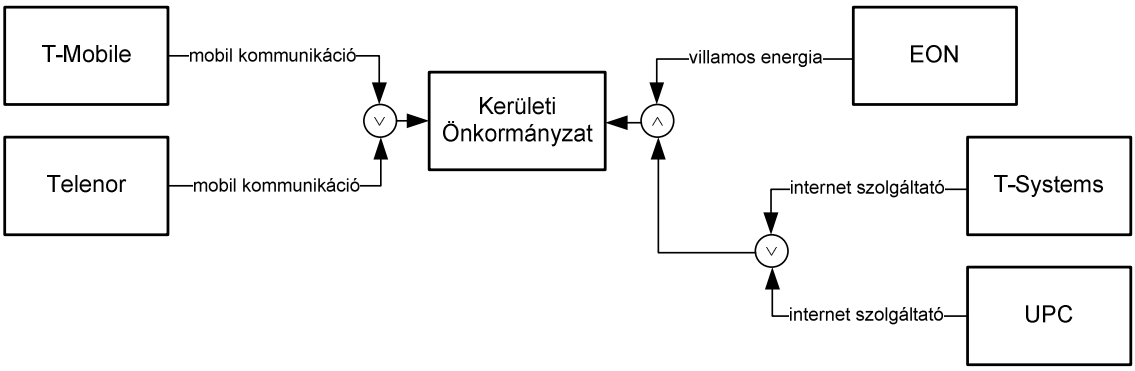
Ennek példaszerű felírását a következő ábra mutatja, ahol a Kerületi Önkormányzat működéséhez szükséges mobil szolgáltatások „vagy” kapcsolatban vannak egymással.



14. ábra: Két mobil szolgáltató „vagy” kapcsolatban

Forrás: saját szerkesztés

Javaslatom szerint a kritikus információs infrastruktúrák közötti rendszerelem kapcsolatok a formális logika, illetve a Fuzzy logika alapján kezelhetők, az irányított háló bejárásával. A háló bejárásával felderíthető, hogy egy adott rendszerelem mely más elemektől függ – tulajdonképpen az elemzés háló csomópontjai közti haladást jelenti a vizsgált elemtől visszafelé. A háló bejárásával azonosítható a függés tartalma és hatása, illetve áttételes függés esetén a függés „mélysége”, vagyis az, hogy hány élnyi távolságban van kritikus szolgáltatási elem az igénybevevőtől. Egy ilyen mintát mutat a következő ábra, amelynek szereplői a mobil szolgáltatók, a villamos energiaszolgáltató, az internet szolgáltatók és a Kerületi Önkormányzat.



15. ábra: Kerületi Önkormányzat kritikus információs infrastruktúra függésé

Forrás: saját szerkesztés

1.3.4 Modellezési szintek

Az elemzés szempontjából megállapítható, hogy a függőségeket legpontosabban az egyes erőforrás-erőforrás kapcsolatok esetében lehet a legpontosabban modellezni, tényadatokat is ilyen szinten lehet begyűjteni, illetve szakértői becsléseket is az egyes rendszerelem kapcsolatok szintjén lehet végezni.

Modellezési szempontból fontos kérdés az is, hogy miként kezelhető egységes szemléletben a makro- és mikrohierarchia, vagyis miként lehet azonos modell elemekkel leírni a kritikus információs infrastruktúrák közötti interdependenciát, valamint egy szervezet erőforrásainak szintjén fellépő erőforrás-erőforrás függéseket, vagyis az intradependenciákat.

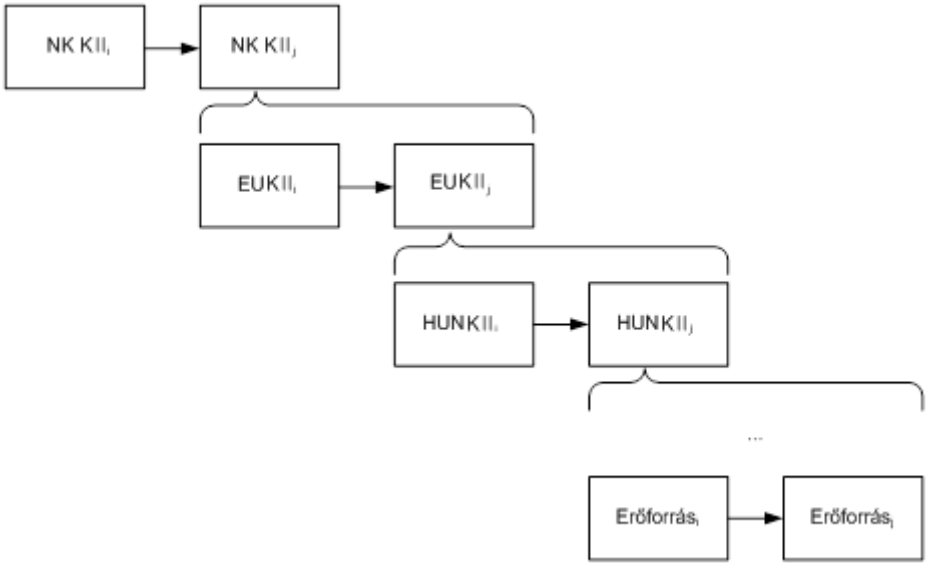
A megoldáshoz az ötletet a virtuális vállalat (virtual business) koncepciója adta, vagyis egy olyan modellezési felfogás, amelyben egy szervezet a vele szoros kapcsolatban lévő más szervezetekkel együtt egy olyan egységet alkot, amelynek a külső és belső kapcsolatrendszere (inter- és intradependenciái) egy külső szemlélő számára nem láthatók, az így kialakult organizáció egységes fellépése és működése helyettesíthető (és modellezhető) egy szervezettel, a tagszervezetek együtteséből felépített virtuális vállalattal. [30]

Ilyen virtuális szervezetet alkot például az autógyár a beszállítóival együtt, ahol az együttműködés szoros keretei a JIT[23] módszertanra épülnek, vagy egy bank az összes kiszervezett funkciót ellátó szervezettel együtt.

[23] JIT - just in time

Ilyen megközelítésben az egyes erőforrás kapcsolatokból felépíthető egy rendszer modellje, a rendszerek kapcsolataiból felépíthető egy szervezet, a szervezetekből felépíthető egy kritikus információs infrastruktúra alágazat, az alágazatokból egy kritikus információs infrastruktúra ágazat, illetve az alágazatokból, ágazatokból egy nemzeti, EU és nemzetközi kritikus információs infrastruktúra is.

Ezt a megközelítést szemlélteti a 16. ábra is:



NK KII – Nemzetközi kritikus információs infrastruktúra
EU KII – Európai Uniós kritikus információs infrastruktúra
HUN KII– Magyarországi/Nemzeti kritikus információs infrastruktúra
i..j – különböző infrastruktúrák, szervezetek, erőforrások, stb.

16. ábra: Kritikus információs infrastruktúra hierarchia, mint virtuális szervezetek kapcsolata

Forrás: [28 p. 6]

Ez a hierarchikus struktúra érvényes a nemzetközi kritikus infrastruktúra, az Európai Uniós kritikus infrastruktúra, a Magyarországi/Nemzeti kritikus infrastruktúra és azok erőforrásai között is.

A modellezési javaslatom alapján megállapítható tehát, hogy a kritikus információs infrastruktúrák alinfrastruktúrájaként értelmezhető annak infokommunikációs alrendszere, amelytől intradependens függésben van.

Az általam javasolt modell programozott támogatással alkalmassá tehető egy kritikus információs infrastruktúra, egy kritikus alágazat vagy teljes ágazat inter- és intradependenciális függőségeinek modellezésére és a hatásalapú vizsgálatára.

A vezeték nélküli hálózati elemek szintén beilleszthetők ebbe a modellbe, mint az infokommunikációs alrendszer további alrendszere, melytől függ az informatikai alrendszer és ezen keresztül a kritikus információs infrastruktúra egésze.

A függés az általános kritikus információs infrastruktúrákkal analóg módon levezethető a kritikus infrastruktúrákra is. A vezeték nélküli hálózat tehát felfogható valamennyi kritikus információs infrastruktúra kritikus információs alrendszerének részeként, amelytől a kritikus információs infrastruktúra, illetve az ezzel kapcsolatban álló további kritikus információs infrastruktúrák függenek.

Az értekezésemben a továbbiakban a vezeték nélküli hálózatokkal tehát mint sajátos kritikus információs infrastruktúra alrendszerekkel foglalkozom, és ennek technikai elemzését, támadhatóságát és védelmét vizsgálom.

1.4 Következtetések

A kritikus információs infrastruktúrák, azok felmérése, kockázatelemzése napjaink egyik égető problémája. Az egyes kritikus információs infrastruktúra ágazatok, alágazatok, szervezetek és egyedi eszközök, rendszerek kockázatelemzésének többféle módszertana létezik. Ezek lehetnek kvantitatív, kvalitatív módszerek, tartalmazhatnak több-kevesebb matematikai logikát, valószínűség számítást, lehetnek grafikusak, leíró jellegűek, egyszerűek, vagy bonyolultak. A kritikus információs infrastruktúra interdependenciákat, illetve egy kritikus információs infrastruktúra intradependenciáit azonban ezek a modellek nem, vagy csak nagyon áttételesen kezelik.

Ennek a problémának a megoldására tettem javaslatot az értekezésemben: egy olyan rendszerszemléletű modellt alkottam meg, amely alkalmas az inter- és intradependenciák modellezésére, a függőségek tartalmának feltérképezésére . Az általam javasolt megoldás a hagyományos kockázatelemzési modellek kiegészítésére is használható, hiszen az egyes erőforrások kockázati részmodelljét egészíti ki egy félformális, a függőségeket és azok tartalmát is leíró modell.

A kritikus információs infrastruktúrák elemzésekor megállapítottam, hogy az egyes kritikus infrastruktúrák, a kritikus információs infrastruktúrák és ezek belső alrendszerei/elemei közötti inter és intradependenciális kapcsolatok modellezhetők.

Kialakítottam egy olyan egységes modellrendszert, amelyben a makroszintű (ágazat-ágazat, alágzat-ágazat, alágazat-alágazat szintű) kapcsolatok azonos módszerekkel ábrázolhatók, mint a mikroszintű (KI-KI, KI-KII, KII-KII, illetve az egyes infrastruktúrán belüli) kapcsolatok.

Az általam javasolt modellben nem csupán a kapcsolatok és azok iránya, hanem azok tartalma (népességre gyakorolt hatás, gazdasági hatás, interdependencia, politikai és időbeni hatás) is ábrázolható és elemezhető.

A kritikus információs infrastruktúrák hatáselemzésére javasolt modellem az értekezésemben nem fejtem ki teljes részletességgel (ez önmagában is szolgálhatna egy értekezés témájául), azonban már elegendő elemet tartalmaz ahhoz, hogy a leírtak alapján kidolgozható legyen egy elemző program prototípusa.

A program és az azzal készített hatáselemzés ellenőrzése, validálása és verifikálása egy olyan feladat, amely további kutatási területeket nyithat meg.

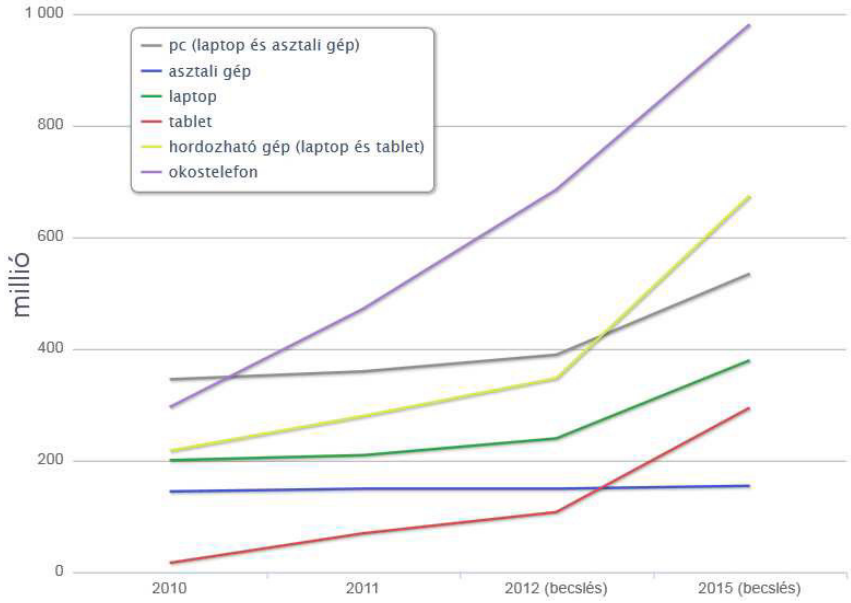
Az inter- és intradependenciák modellje alapján megállapítottam, hogy a vezeték nélküli hálózatok felfoghatók olyan speciális kritikus információs al-infrastuktúraként,

amitől függ(het) minden kritikus infrastruktúra, illetve kritikus információs infrastruktúra is.

A modell segítségével bizonyítottam, hogy a vezeték nélküli hálózatok vizsgálata önálló kutatási területként is megállja a helyét a kritikus információs infrastruktúrák védelme terén.

2. Fejezet
Vezeték nélküli hálózatok a kritikus információs infrastruktúrákban

A hagyományos számítógépek eladása évről-évre csökkenő tendenciát mutat. E mellet viszont a hordozható számítógépek, tabletek, okostelefonok forgalmazása hatalmas ütemben fejlődött. Ezt mutatja a következő ábra is:



17. ábra: A infokommunikációs technológia kereskedelmének változása az elmúlt és a következő években

Forrás: [124]

A hordozható infokommunikációs eszközök felhasználásának ilyen gyors növekedése magával hozza a kiszolgáló infrastruktúra fejlődését is. A vezeték nélküli hálózatok robbanásszerű elterjedése elmosta a határvonalat a csak vezetékes és vegyes hálózatok között, és a külön-külön menedzselt és védett hálózati szegmensek helyett a komplex és teljes körű hálózat információbiztonságát kell szem előtt tartani. Az infrastruktúra üzemeltetők a vezetékes hálózatot védeni tudják a külső illetéktelen behatolásoktól. Ezzel szemben a vezeték nélküli hálózatok egy teljesen új korszakot nyitottak a hálózat és információbiztonság terén, amely eleinte nagy kihívásokkal szembesítette az üzemeltetőket. A cél minden esetben az volt, hogy biztosítani tudják az alkalmazottak, esetleg a vendégek mobilitását az infrastruktúrán belül és kívül, de a vezeték nélküli környezet-

ben meg kellett akadályozni a jogosulatlan hozzáféréseket és biztosítani az infrastruktúra teljes informatikai sérthetetlenségét.

Az ilyen hálózatokban a következők miatt még fontosabb a biztonság:

- a vezeték nélküli kommunikáció az éteren keresztül valósul meg, így fizikai határok híján a vezetékek hossza és hozzáférhetősége nem jelentenek neki akadályt. Így a meglévő hálózati szabályozások sokszor nem képesek a határvédelmi funkciójukat ellátni;
- a 802.11-es szabvány, amely a vezeték nélküli hálózatokat szabványosítja, bárki számára elérhető, hozzáférhető, ezért nem csak az eszközgyártók, hanem a rosszindulatú támadók számára is publikus adatok megkönnyítik az esetleges hibák kihasználásával végrehajtható támadásokat;
- a WLAN a nem engedélyköteles 2,4 GHz-es és 5 GHz-es frekvenciákon működtethető. Ez azt jelenti, hogy számos más elektronikai eszköz is használja ezeket a frekvenciasávokat, ezért mérésekkel bizonyítható, hogy a 2,4 GHz-es sáv számos területen már teljesen telített. A Nemzeti Média- és Hírközlő Hatóság (NMHH24) az agresszív és rosszindulatú használat megakadályozása érdekében kötelezővé teszi az ide vonatkozó szabályok betartását, de ezek betarttatásának nehézsége miatt a frekvenciát törvénytelenül használók többnyire nem kapják meg büntetésüket. [125] A következő ábra az NMHH WLAN szabálysértések felderítésére felkészített járművét mutatja.

18. ábra: Az NMHH WLAN szabálysértések felderítésére felkészített járműve

Forrás: [123]

[24] NMHH - Nemzeti Média- és Hírközlési Hatóság

A vezeték nélküli hálózati kapcsolatokról sokáig nem lehetett hallani a kritikus infrastruktúrákban. Ez azért volt, mert az infrastruktúra üzemeltetők nem érezték elég biztonságosnak a WLAN kapcsolatot ahhoz, hogy a vezetékes hálózat mellett párhuzamosan kiszolgálja a dolgozókat. A szemléletváltás kezdetén a WLAN eszközöket olyan helyre telepítették csak, ahol a kényelmi funkciók elsődlegesek voltak. Ilyenek voltak a tárgyalók, belső kávézóhelyek, előterek. Általában ezeket a helyeket szigorúan szegmentálták az infrastruktúra vezetékes hálózatától. Az így önállóan működő WLAN kapcsolatok email és internet szolgáltatást nyújtottak, de a dolgozók nem tudták folytatni megkezdett munkáikat.[31] Ezt a problémát kiküszöbölendő számos eszközgyártó olyan komplex rendszert kínált, amely biztosította a hálózat zártságát és az információ, szolgáltatások elérését a teljes infrastruktúra területén. A technológia elterjedését az is elősegítette, hogy a gyártók olyan infrastruktúra- szegmenseket is megcéloztak termékeikkel, amelyekben eddig még a hagyományos hálózati megoldások sem terjedtek el teljesen. Hazánkban számos kritikus infrastruktúra üzemeltető választotta a vezeték nélküli hálózati megoldásokat az infrastruktúra teljes vagy részterületén. Ilyen infrastruktúra található például az egészségügyi szektorban. A vezeték nélküli hálózati megoldást alkalmazhatják az orvosok telekonzílium megtartására, a betegek eredményeinek azonnali megjelenítésére, s nem utolsó sorban az orvosok, az ápolószemélyzet és a fontosabb műszerek helymeghatározására az infrastruktúrán belül. [126]

Ezek között az ágazatok között számos olyan megtalálható, amely informatikai biztonsági stratégiája tiltotta a vezeték nélküli hálózati kapcsolatot. 2002. és 2008. között a kritikus infrastruktúrákban elsődleges hálózati megoldásként csak a vezetékes kapcsolat volt elfogadott.[31] Ez köszönhető annak, hogy infrastruktúrán belül ekkor még nem készítettek egységes szabályozást a vezetékes és vezeték nélküli kommunikációhoz. 2009. és 2011. között a mobil eszközök elterjedésével megnőtt a WLAN hálózati szegmensek aránya az infrastruktúrákban, de a legnagyobb problémát a két hálózati infrastruktúra menedzsmentje jelentette. [31]

2011-től létrejöttek a tisztán vezeték nélküli infrastruktúrák, amelyekben a vezetékes kapcsolatot csak a fixen telepített eszközök kapták meg. A hálózat teljes menedzsmentje egységes lett.[31] Egyes kritikus infrastruktúrák esetében a teljesen homogén vezeték nélküli hálózat nem megoldható. Ez azért van, mert ezek az infrastruktúrák nem egy épületen belül, vagy nagy területen helyezkednek el, mint például az egyetemvárosok, kormányzati vagy kórházi épületcsoportok. Ebben az esetben két lehetőség áll rendelkezésre a biztonságos informatikai infrastruktúra üzemeltelésére:

- szegmensekre bontjuk a hálózatot, és a menedzsmentet szegmensenként felügyeljük;

- egy egységként kezeljük a rendszert és központosított menedzsment segítségével biztosítjuk a hálózat felügyeletét.

A kritikus információs infrastruktúrák közül a hálózati infrastruktúra rekonstrukciója keretében számos infrastruktúrában alakítottak ki teljes lefedettséget biztosító vezeték nélküli hálózatot. Ennek igazolására felsorolok néhány kritikus információs infrastruktúra részeként megvalósított WLAN hálózatot:

Országos Mentőszolgálat: 2006-ban az Országos Mentőszolgálat hívásfogadó központjainak informatikai és telekommunikációs modernizálása során a vezetékes hálózat mellett helyi szintű vezeték nélküli hálózatok kialakítására is sor került. [119]

Budafok-Tétény Önkormányzata Polgármesteri Hivatala: Az önkormányzat műemlék épületében a vezetékes hálózat kialakítása nem volt lehetséges, ezért alakítottak ki vezeték nélküli hálózatot a hivatali dolgozók és a képviselők számára. [120]

Részecske- és Magfizikai Kutatóintézet: A kutatóintézetben a vezetékes hálózat műszaki színvonala kielégítő volt, azonban az ott dolgozók igényeit figyelembe véve mind a négy épületben teljes lefedettséget biztosító vezeték nélküli hálózatot építettek ki.[121]

Budapesti Közlekedési Vállalat: A forgalomirányítás, illetve ezen belül is az elektronikus járműkövető rendszer eleme a vezeték nélküli hálózat. [123]

A példaként felsorolt kritikus információs infrastruktúrákban a kialakított WLAN a teljes hálózat szerves része, és nem csak egy kritikus információs infrastruktúrát érint, hanem mindegyik külön ágazati csoporthoz tartozik. Ez is azt bizonyítja, hogy ez a technológia nélkülözhetetlen, és a vezetékes hálózati megoldások mellett egyenrangú hálózati megoldásként használják.

2.1 Kritikus információs infrastruktúrák vezeték nélküli hálózatai

Ahhoz, hogy megértsük a vezeték nélküli hálózat működését és alkotóelemeit, a következő alfejezetekben a WLAN szabványosítását, fejlődését, védelmi rendszerét vizsgálom, amely a IEEE 802.11-es ajánlás csoport alá besorolt hálózati megoldásokat tartalmaz. Hogy képet kapjak a vezeték nélküli hálózatok elterjedéséről és felhasználási területéről méréseket végeztem a fővárosban. A mérési eredmények tükrében tudom elemezni a hálózatok különböző paramétereit, és azt, hogy a kritikus infrastruktúrákban milyen hálózati megoldásokat alkalmaztak. Ezeket a mérési eredményeket a szakirodalom ide vonatkozó részeivel támasztom alá.

A világ talán egyik legnagyobb szabadon elérhető vezeték nélküli hálózati végpontokat nyilvántartó szervezete a Wireless Geographic Logging Engine (wigle.net). A szervezet a felhasználók feltöltött adataiból készít statisztikákat, és naprakész térképeket városokról, országokról. Ezt a tevékenységet 2002. óta dokumentálják. Ez alatt az eltelt 10 év alatt 72.894.490 eszközt regisztráltak, amelyből 71.599.191 eszközhöz pontos helymeghatározási adatot is rögzítettek.[32] Vizsgálatomat a témában kiegészítem az ebből az adatbázisból kinyerhető adatokkal, és más mérési eredményekkel is.
A vizsgálathoz a következő eszközöket használtam:

- hordozható számítógép (MSI VR-601);
- külső dual band-es USB-s WLAN kártya (Linksys AE1000);
- bluetooth-os GPS vevő (Visiontac VGPS-700).

A méréseket autóval végeztem két szakaszban. A hordozható számítógépen Windows 7-es környezetben Vistumbler alkalmazással dolgoztam. Az így elkészített adatbázist CSVeD programmal szűrtem a hálózati jellemzőkre és Excel segítségével jeleníttettem meg a mért értékeket.

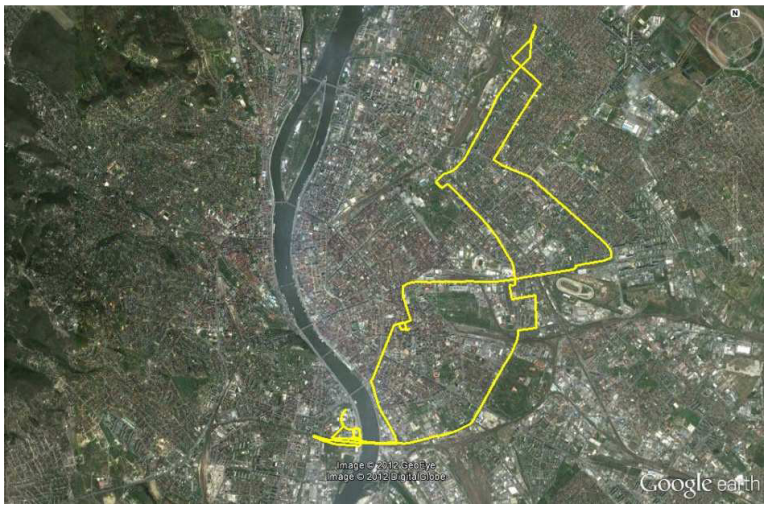
Vizsgálatom során csupán a vezeték nélküli hálózatok mindenki számára elérhető jellemzőit gyűjtöttem össze (SSID[25], AP[26] fizikai elhelyezkedése, AP gyártója, hitelesítés és titkosítási adatok, csatornakiosztás). Ezekből az információkból készítettem el összehasonlításaimat, amelyek kiértékelés szempontjából átfogó képet adnak a hálózatokról. A 35 km-es útvonalon általam azonosított 3233db végpont között vannak otthoni hálózatok, vállalakozások és közintézmények által üzemeltetett hozzáférési pontok. Ezek között természetesen megtalálhatók a kritikus információs infrastruktúrák is.

Az SSID elnevezések és az eszközök fizikai helye egyértelművé teszi, hogy a végpontok jellemző helyei:

- kávézók;
- szórakozóhelyek;
- oktatási intézmények;
- informatikai vállalatok;
- bankok;
- közlekedési vállalatok
- egészségügyi intézmények
- stb.

[25] SSID - Service Set Identification
[26] AP – Access Point

A felsorolásból látható, hogy azok között kritikus információs infrastruktúrának minősülő szervezetek, intézmények, vállalatok is megtalálhatók. A mérés során beazonosított végpontok közül az értekezésemben egyiket sem kívánom konkrétan megnevezni, hogy ne veszélyeztessem ezek működését. Ezért a továbbiakban csak statisztikai összehasonlító elemzéseket fogok bemutatni, illetve az egyes elemzéseimben legfeljebb ágazat szinten azonosítom a kritikus infrastruktúra típusát. A következő képen a vizsgálat útvonala látható.



19. ábra: A vizsgálat útvonala

Forrás: saját szerkesztés

A vizsgálati útvonal kiválasztásánál fő szempont volt különböző ágazatok kritikus információs infrastruktúrájának érintése, melyek fizikai elhelyezkedése számomra ismert volt. A cél az ágazati mintavételezésre és nem a kritikus információs infrastruktúrák mennyiségére irányult. Megbecsülni Budapest vagy az ország kritikus információs infrastruktúráiban működő vezeték nélküli hálózatok darabszámát a mérési eredmények alapján nem lehet. Ezek a mérési eredmények csak arra világítanak rá, hogy kritikus információs infrastruktúrákban jelen van a vezeték nélküli hálózat, és megfelelő védelmét biztosítani kell. Az útvonalon a kritikus információs infrastruktúrák közül (konkrét megnevezésük nélkül) a következőkben sikerült vezeték nélküli hálózatot azonosítanom:

- infokommunikációs hálózatok (vezetékes, mobil, műholdas);
- közlekedés szervezés és irányítás infokommunikációs hálózatai;
- egészségügyi rendszer infokommunikációs hálózatai;

- pénzügyi-gazdasági rendszer infokommunikációs hálózatai;
- kormányzati és önkormányzati szféra infokommunikációs hálózatai;
- védelmi szféra infokommunikációs hálózatai.

A felsorolt kritikus információs infrastruktúrákat biztonsági megfontolások miatt nem nevezem meg konkrétan!

2.2. Az IEEE 802.11 vizsgálata

Az útvonalon azonosított kritikus információs infrastruktúrák vezeték nélküli hálózatait a következő szempontrendszer szerint vizsgálom:

- rádiós szabályozások;
- modulációs eljárások;
- csatornák kihasználása;
- 802.11-es szabványok;
- topológia;
- eszközgyártók.

2.2.1 Rádiós szabályozások

A vezeték nélküli hálózatokban a kommunikáció rádiófrekvenciás csatornán keresztül valósul meg. A rádiófrekvenciás spektrum szabályozása elengedhetetlen ahhoz, hogy az eszközök a számukra kiosztott frekvenciasávban működjenek. A Nemzetközi Távközlési Egyesület Rádiótávközlési Szektor (ITU-R[27]) felelős a globális rádiófrekvenciás spektrum-gazdálkodásért.[33] A következő ábra az öt régiót ábrázolja, amelyet az ITU-R határozott meg.

Régiók	Földrajzi elhelyezkedésük
A	Amerika
B	Nyugat-Európa
C	Kelet-Európa és Észak-Ázsia
D	Afrika
E	Ázsia és Ausztrália

20. ábra: ITU-R régiók térképe

Forrás: [34 p. 9]

[27] ITU-R: The International Telecommunication Union–Radiocommunication

A rádiófrekvenciás kommunikáció minden esetben a régióhoz tartozó ISM (Industrial, Scientific and Medical) sávban kell, hogy megvalósuljon. Hazánkra vonatkozó ISM sávok a következők:

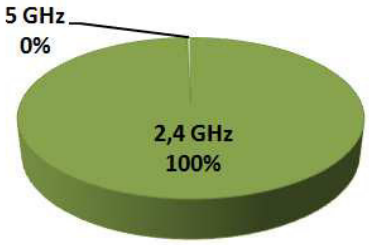
- 2,4 GHz (2,4-től 2,4835 GHz-ig)
- 5 GHz (5,15-től 5,35-ig és 5,725-től 5,825 GHz-ig) [35 p. 55]

A frekvenciakorlátok mellett az eszközök adóteljesítményét is korlátozza a szabályzat. Ez az effektív teljesítményérték Európában nem lehet nagyobb mint 100mW. Ettől eltérően az Amerikai Egyesült Államokban a megengedett teljesítmény jóval nagyobb 1W.[36 p. 2] Számos eszközgyártó nem készít külön berendezést az európai és más régióban lévő piacokra, hanem beállításokkal szabályozza az eszközök adóteljesítményét. Ezt úgy teszi, hogy a készülékben a lokalizáció megadásával lépnek életbe a teljesítménycsökkentési szabályok.

2.2.2 Vizsgálati eredmények a rádiós szegmensben

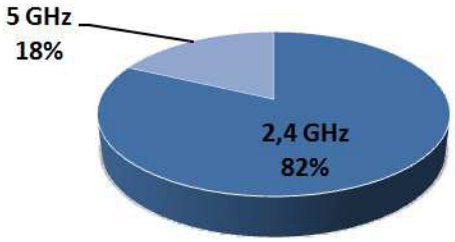
A hálózati eszközök rádiós szegmensének vizsgálata megmutatja, hogy az eszközök milyen arányban használják a 2,4 GHz-es és 5 GHz-es tartományt. Köztudott, hogy a 2,4 GHz-es sávban nem csak a WLAN eszközök nagy száma okozza a zavart, hanem számos olyan hétköznapi eszköz is, amely ezt a szabad frekvenciasávot használja, vagy véletlenül ezen sugároz. Ilyen például a mikrohullámú sütő, vezeték nélküli telefonok, a bluetooth, a modellezők adó-vevő berendezései és még számos más eszköz.

A rádiós szegmensek kihasználásának összehasonlítására nagyon kevés más forrásból származó mérési adatot publikáltak.



21. ábra: WLAN frekvenciasáv használatának adatai a wigle.net alapján

Forrás: [32]



22. ábra: WLAN frekvenciasáv használatának adatai mérési eredményeim alapján

Forrás: saját szerkesztés

A diagramokból jól látszik, hogy a wigle.net adatai alapján az 5 GHz-es sávot használó eszközök száma kevesebb mint 1%, míg Budapesten ez az eszközök 18%-át adja ki. Ez azzal magyarázható, hogy az 5 GHz-es frekvenciasáv kevésbé kihasznált, így kevés az egymást zavaró jel is.

A vizsgált útvonalon több kritikus információs infrastruktúrát sikerült beazonosítanom, amiből hármat választottam ki konkrét nevesítés nélkül. Ezek:

- az infokommunikációs ágazathoz;
- a közlekedés ágazathoz;
- és az egészségügy ágazathoz tartozó információs infrastruktúrák.

A mérési adatokból kiválasztva és megvizsgálva az előzőekben meghatározott kritikus információs infrastruktúrákat megállapítom, hogy:

- az infokommunikációs technológiák és az egészségügy ágazathoz tartozó infrastruktúrában mindkét frekvenciasávban működő eszközök megtalálhatóak;
- a közlekedés ágazathoz tartozó infrastruktúrában csak a 2,4 GHz-es eszközök működnek.

2.2.3 Modulációs eljárások a vezeték nélküli hálózatokban

A vezeték nélküli hálózatoknál nem csak a közeget választhatjuk meg, hanem a frekvencia tartományt és a modulációs technikát is, amelyek hatással vannak a kiépítendő hálózatra. A modulációs eljárások során a vivő jelet képessé teszik az információ továbbítására. A moduláció során a jel három tulajdonsága változtatható meg, az amplitúdó, a fázis és a frekvencia. [37 p. 17]

A rádiófrekvenciát alkalmazó hálózatok a szabadon használható 2,4 GHz és az 5 GHz-es tartományban üzemelnek és alapvetően háromféle jelátvitelt használnak.

FHSS (Frequency Hopping Spread Spectrum)

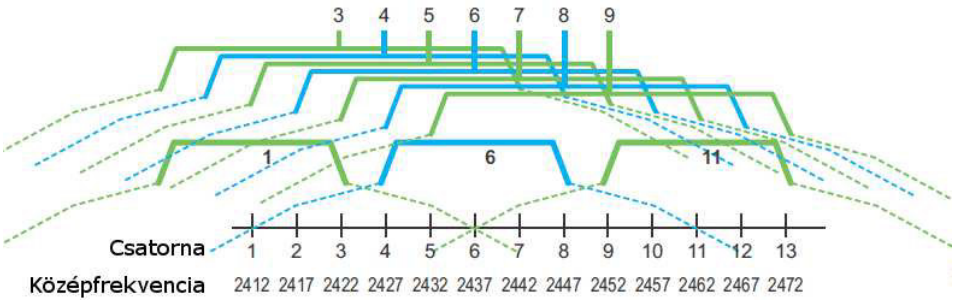
A frekvencia ugratásos szórt spektrum lényege, hogy a kommunikációs állomások nem használják egyszerre a teljes spektrumot. A használatban lévő vivőfrekvencia folyamatosan változik és ezt a folyamatos változást nevezik ugrásnak (hop). Az ugrást egy véletlen sorozat segítségével állítják elő, ami meghatározza, hogy az átvitelnél mely frekvenciákat fogja igénybe venni. A frekvenciák sorrendje definiálja a kommunikációs csatornát. Az adó állomás az ugrási sorozat alapján meghatározza az adás frekvenciáját, majd megadott ideig azon sugároz. Ha ez az idő letelik, az adó a következő frekvencia-

sávra vált. Azt az időt, amíg az adóállomás a frekvencia sávok között vált, ugrási időnek (hop time) nevezik. Abban az esetben, ha az állomás az összes meghatározott sávon sugárzott már, akkor a lista újból elölről indul. Ahhoz, hogy a kapcsolat és az adatforgalom létrejöhessen az adó és a vevő között, szinkronban kell lenniük. Az adott időpillanatban azonos frekvenciát kell használniuk. [37 p. 19]

DSSS (Direct Sequence Spread Spectrum)

A DSSS (közvetlen sorozatú szórt spektrum) a csatornákat 22 MHZ széles egybefüggő frekvenciasávként használja. A csatornák száma országonként különbözik (Japánban 14, Európában 13, és az Amerikai Egyesült Államokban pedig 11 különböző csatorna érthető el). A csatornák középfrekvenciája 5 MHz távolságra van egymástól, és mivel minden csatorna 22 MHz széles ezért a csatornák között átfedés jelentkezik. Tehát legalább 5 csatorna különbségnek kell lennie az átfedés kiküszöbölésére. Így 3 olyan csatorna van amely, nem fedi át egymást, ez az első, a hatodik és a tizenegyedik. [37 p. 20]. A 23. ábra a hazánkra érvényes csatornakiosztást mutatja.

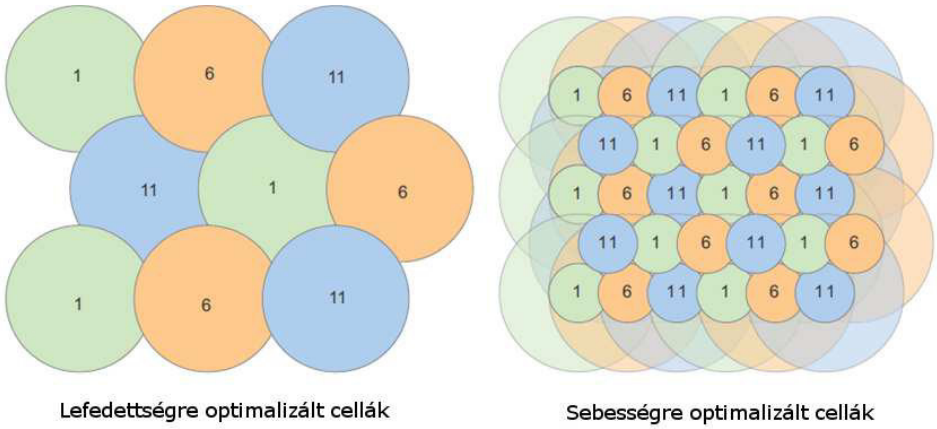
Az egymást át nem fedő cellák között egy 3 MHz-es úgynevezett védősáv található. A DSSS eljárás a jeleket a csatorna maximális sávszélességében terítve továbbítja, ez által teljes egy csatorna kihasználtsága.



23. ábra DSSS 2,4 GHz

Forrás: [38 p. 56]

A kapcsolatok ideje alatt a frekvencia nem változik. Az átfedésmentes AP esetében pedig az adatátviteli sebesség jóval nagyobb, mint az FHSS-nál. Az ütközések kezelésére a redundanciát olyan mértékben megváltoztatták, hogy a továbbított adatok még esetleges csomagsérülésnél is helyreállíthatóak legyenek. Infrastruktúrán belül az eszközök elhelyezését és a csatornák helyes megválasztását két szempont szerint csoportosítják. Az egyik a lefedettségre optimalizálás, a másik a sebességre optimalizálás.

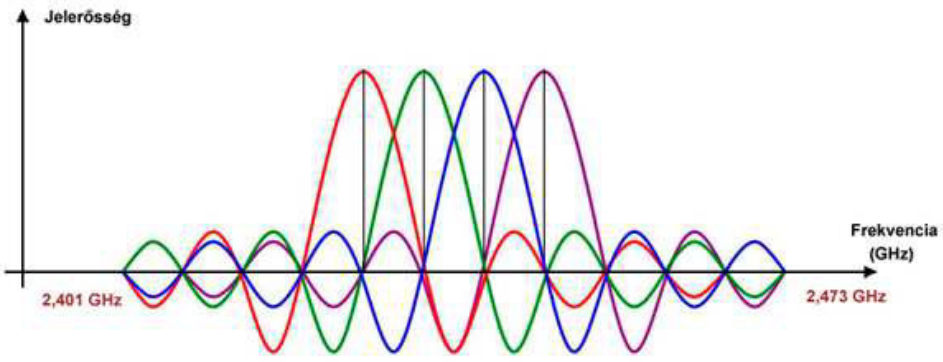


24. ábra: Lefedettség vagy sebesség optimalizált cella

Forrás: [39 p. 12]

OFDM (Orthogonal Frequency Division Multiplexing)

A merőleges frekvenciaosztásos multiplexelés lényege, hogy egy nagysebességű csatornát több kisebb sebességű csatornára oszt és ezeket egyszerre használja. A nagysebességű csatornák 20 MHz szélesek és 52 alcsatornára vannak felosztva. Ezek alapján egy alcsatorna 300 KHz széles. Az OFDM felépítése a következő: az 52 csatornából 4 db csatorna feladata a hibajavítás, a maradék 48 csatornán történik az adatok továbbítása. Az alcsatornákon a sugárzott jelek egymásra mindig merőlegesek, ezáltal a spektrum jobban ki van használva és bizonyos interferenciákra is kevésbé érzékeny mint a DSSS. A következő ábra az OFDM frekvencia / jelerősség mintaképét mutatja. [37 p. 21]

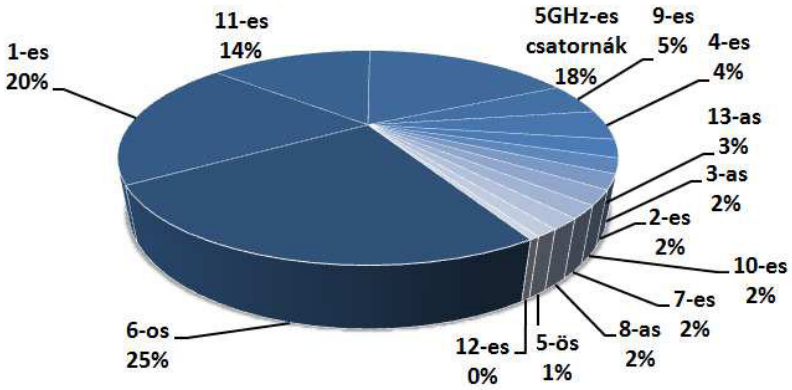


25. ábra: OFDM

Forrás: [40]

2.2.4 Vizsgálati eredmények a 802.11-es csatornák kihasználására

A mérési adatok alapján jól látszik, hogy az AP-k automatikusan, vagy manuális beállítások következtében jó közelítéssel követték az optimális csatornakiosztást, ami azt jelenti, hogy a 2,4 GHz-en használható 13 csatorna közül az ajánlott 1, 6 és 11-es csatornákat használta a legtöbb eszköz. Számos eszközgyártó ajánlása szerint Európában, még ha van is rá lehetőség, nem vagy csak kis mértékben használjuk a 12-es és 13-as csatornákat, mert előfordulhat, hogy bizonyos eszközök az amerikai szabvány miatt nem fognak működni.



26. ábra: Csatornakiosztások alakulása saját mérési eredmények alapján

Forrás: saját szerkesztés

A mérési adatokból kiválasztva, és megvizsgálva az előzőekben meghatározott három kritikus információs infrastruktúrát megállapítom, hogy az infokommunikációs technológiák ágazathoz tartozó infrastruktúrában következetesen az 1-es és a 6-os csatornát használják a 2,4 GHz-es sávban és a 64-es csatornát az 5 GHz-es sávban. A közlekedés ágazatban az 1-es és a 11-es csatornákat alkalmazzák. Az egészségügy ágazathoz tartozó infrastruktúrában az 1-es és a 6-os csatornákat használják a 2,4 GHz-es sávban, míg 5 GHz-en a 60-as csatornát preferálják. A mérési eredmények is azt támasztották alá, hogy csatornakiosztási szempontból mind a három infrastruktúra üzemeltetője törekedett arra, hogy saját eszközei egymást ne zavarják.

2.2.5 Az IEEE 802.11 szabványok

A vezeték nélküli hálózatok kezdete a II. világháborúig visszanyúlik és visszavezethető az amerikai hadsereg által használt rádiós adatátviteli eljárásokra. A háború után ezt a

típusú összeköttetést sikeresen használták pont-pont adatátvitel megvalósítására. Később a Hawaii Egyetem kutatói megalkották a csomag alapú rádiós adatátviteli technológiát. 1971-ben készítették el az első vezeték nélküli hálózatot. A későbbiekben többen csatlakoztak az ilyen irányú kutatásokhoz, de rendszereik nem szabványosított környezetre készültek, így nem tudtak egymással kommunikálni. Az 1980-as években az Amerikai Szabványügyi Testület (FCC[28]) a 802.11-es IEEE szabvány kidolgozását javasolta a helyzet megoldására, ezért 1991-ben több eszközgyártó együttműködésével megalakult a WECA[29] amely a napjainkban Wi-Fi nonprofit szervezetként tevékenykedik. Az IEEE 1997-ben kiadta az első 802.11-es szabványt. A szabvány célja az volt, hogy összehangolja az eszközök együttműködéséhez szükséges paramétereket. A többi 802-es szabványhoz hasonlóan a 802.11 is csak az OSI[30] alsó két rétegét a fizikai (PHY[31]) és a adatkapcsolati szint közeghozzáférés alrétegét (MAC[32]) definiálta.

4. táblázat: 802.11 Fizikai és Adatkapcsolati rétege

<table>
<tr><td>802.2 Logikai kapcsolatvezérlés
(Logical Link Control – LLC)</td><td rowspan="2">Adatkapcsolati réteg
(Data Link Layer – DLL)</td></tr>
<tr><td>802.11 Közeghozzáférés vezérlés
(Media Access Control – MAC)</td></tr>
<tr><td>IR, FHSS,DSSS, OFDM</td><td>Fizikai réteg
(Physical Layer – PHY)</td></tr>
</table>

Forrás: [37 p. 7]

E szabvány két rádiófrekvenciás és egy infravörös átviteli technológiát szabályoz. [41 p. 5] A 802.11 fejlesztése a mai napig nem állt le. Több olyan WLAN szabvány is létezik, amely jelenleg is fejlesztés alatt áll.

A 802.11-es szabványok fő szabálya alapján a különböző eszközök közti vezeték nélküli kapcsolat a létrehozott összeköttetésen keresztül a társ LLC rétegek közti MAC szolgáltatás adategységeinek továbbításával (MSDU[33]) jön létre. A vezeték nélküli hálózatok topológiai összetétele folyamatosan változik. Olyan adatátviteli közeget hasz-

[28] FCC - Federal Communications Commission
[29] WECA - Wireless Ethernet Compatibility Alliance
[30] OSI - Open Systems Interconnection
31 PHY – Physical Layer
32 MAC - Media Access Control
33 MSDU - MAC Service Data Unit

nál, amely nem olyan megbízható, mint a vezetékes, mivel védtelen a külső zavaró és más jelekkel szemben.

A 802.11-es szabvány szerint a vezeték nélküli hálózatnak a MAC alrétegben kell megvalósítana az eszközök mobilitását. Ez azt jelenti, hogy a hordozható eszközöknek a hálózaton belül lefedettségtől függően biztosítani kell az eszközök együttműködését. A WLAN alkotóelemei a felsőbb rétegek számára transzparens módon biztosítják a mobilitást és az összeköttetést.[37 p. 8]

A szabvány megjelenését követően több gyártó is elkezdte forgalmazni a szabványon alapuló termékeit, de a kezdeti stádiumban még több teljesítmény és biztonságtechnikai problémával kellet szembenézniük. [42]

Az IEEE szabványt idővel kiegészítették és az adott változatokat betűjelekkel látták el. A vezeték nélküli hálózatok alapját a mai napig e szabványok adják. A következő táblázat tartalmazza a már elfogadott, és a mindennapokban használatos WLAN technológiák összesítését.

5. táblázat: az IEEE 802.11 összefoglaló táblázata

IEEE 802.11 hálózati szabványok								
802.11 protokoll	Megjelenés dátuma	Frekvencia (GHz)	Sávszélesség (MHz)	Adatsebesség (Mbit/s)	MIMO	Moduláció	Beltéri lefedettség (m)	Kültéri lefedettség (m)
-	1997	2.4	20	1, 2	1	DSSS, FHSS	20	100
a	1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	120
		3.7					-	5000
b	1999	2.4	20	1, 2, 5.5, 11	1	DSSS	35	140
g	2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	DSSS, FHSS	38	140
n	2009	2.4, 5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4	OFDM	70	250
			40	15, 30, 45, 60, 90, 120, 135, 150			70	250

Forrás: [38]

Az IEEE 802.11a

A szabványcsalád második kiegészítése. A frekvencia tartomány területén már az 5GHz, míg az átviteli sebesség esetében az 54 Mbps hálózatokat határozza meg. Az alap protokoll megegyezett a 802.11-es esetében használttal. Az 5 GHz-es tartományban az interferencia jóval kisebb volt, mert a sáv kevésbé foglalt a 2,4 GHz-hez képest. A szabvány merőleges frekvenciaosztásos multiplexelést alkalmaz, aminek köszönhetően 52 alcsatornát használ. [43] Az alcsatornák között 12 db van ami nem fedi át egymást. A hálózat hatótávolsága 54 Mbps-os sebesség mellett 12 méter, míg 6 Mbps mellett akár 90 méter is lehet. A szabvány többféle átviteli sebességet támogat amit a kódolás, illetve a moduláció határoz meg. A BPSK[34] bináris fázisbillentyűzés a különböző adatbit minták reprezentálásához az adási középfrekvencia fázisát tolja el. A QAM[35] a kvadratúra amplitúdó moduláció. A nagyobb adatátviteli sebességeknél használják, a vivőjel amplitúdóját módosítva továbbítja az információt.

Az előnyök mellett természetesen hátrányai is vannak a szabványnak. A problémát a különböző szabványok közötti kompatibilitás okozza, mivel az alap 802.11 illetve a 802.11b szabványok is a 2,4 GHz-es frekvenciát használják. Ezért a 802.11a szabvány eszközei nem vagy csak kiegészítő készülék alkalmazásával képesek kompatibilitásra a többi szabvány eszközeivel. [37 p. 24]

Az IEEE 802.11b

A szabványt 802.11 High Rate néven is ismerik, mert a fizikai réteg nagysebességű átvitelre képes kiegészítését tartalmazza a DSSS rendszerhez. Ez az első protokollja az eredeti 802.11-es szabványnak. A frekvencia területén a 2,4 GHz-es tartományt használja, de az átviteli sebessége már 11 Mbps. A szabvány alkalmas többféle átviteli sebesség támogatására. Az 1 Mbps sebesség DBPSK[36] moduláció és barker kód alkalmazásával lehetséges. [37 p. 22] A DBPSK két egymástól 180 fokban eltérő fázist használ.

A 802.11b szabványra épülő hálózatok pont multipont felépítést alkalmazzák, ami azt jelenti hogy az AP-k gömbsugárzó (omni-directional) antennát használnak. Ezen hálózati kialakítások hatótávolsága épületen belül 30 méter 11 Mbps átviteli sebességgel, illetve akár 90 méter is lehet 1 Mbps átviteli sebesség mellett. Az 11 Mbps átviteli sebesség azonban csak elméleti érték; a valós értékek kb. 5,9 Mbps TCP protokoll ese-

[34] BPSK - Binary Phase Shift Keying
[35] QAM - Quadrature Amplitude Modulation
[36] DBPSK - Different Binary Phase Shift Kexying

tén és 7,1 Mbps UDP esetén. Az ok a protokoll fejrészének továbbításában keresendő, ugyanis minél nagyobb a fejrész, annál kisebb az átviteli sebesség. [44]

Az IEEE 802.11g

A 802.11g szabványt 2003 júliusában vezették be. Jelentősége, hogy a 2,4 Ghz frekvenciasávban képes a maximális 54 Mbps-os elmélet sebességre. Visszafelé kompatibilis a 802.11 és a 802.11b-s szabványokkal. Többfajta átviteli sebességet és különböző modulációkat támogat. Az OFDM modulációt használják a 6; 9; 12; 18; 24; 36; 48; 54 Mbps átviteli sebességeknél, míg a 11; 5,5; 2; 1 Mbps-os sebességeknél már DQPSK[37] illetve DBPSK-t.[37 p. 22] A 802.11g esetében a lefedettségi terület 15 méter az elméleti 54 Mbps-os sebesség mellett, de ez 45 méterre növelhető akár 11 Mbps sebességnél.

Bár a szabvány hatására az adott 2,4 GHz frekvencián sikerült elérni egy jóval magasabb elméleti átviteli sebességet, a korábbi szabványokhoz képest a problémát jelentő frekvencia foglaltság továbbra is megmaradt. A 2,4 GHz frekvencián zavart okoznak az átvitelben egyes lakástelefonok, a mikrohullámú sütők, Bluetooth eszközök, videóátjátszók és még sok más eszköz. Az eltérő moduláció miatt, amelyet a 802.11b illetve a 802.11g használ, számos esetben nem tudnak az eszközök egymással kommunikálni. [45]

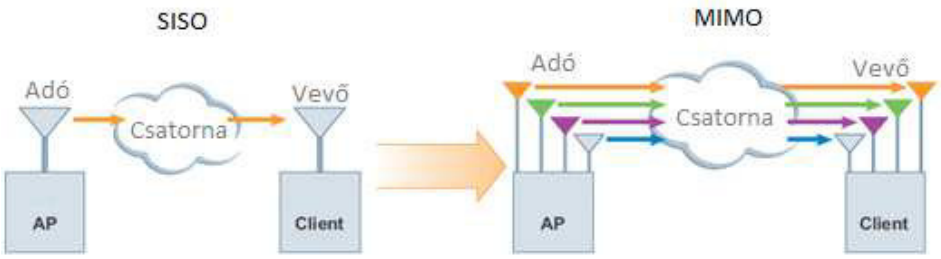
Az IEEE 802.11n

Az IEEE 802.11n változatát 2009. szeptember 11-én hitelesítették. A szabvány elméleti sebessége 600 Mbps, míg a sugárzási tartománya a 802.11a,b,g rendszerekhez képest az 5 GHz-es tartományban nagyobb, a 2,4 GHz-ben pedig megegyezik. A nagy átviteli sebességet úgy tudja elérni, hogy egyszerre használja mindkét frekvenciasávot abban az esetben, ha az eszköz kétsávos. Az 5 GHz-es tartományban huszonegy, míg a 2,4 GHz-s tartományban pedig három át nem lapolt csatorna van és ezeket a csatornákat dinamikusan váltogatja. [42]

Az IEEE 802.11n javított OFDM-et használ, ami szélesebb frekvenciasáv használata mellett nagyobb átviteli sebességet ér el. Az SDM[38] térosztásos multiplexelés pedig növekvő teljesítményt ér el több antenna alkalmazásával. A MIMO[39] a több utas interferenciát használva növeli a teljesítményt. A 20 MHz-es csatornák helyett 40 MHz-es

[37] DQPSK - Differentially Encoded Quadrature Phase Shift Keying
[38] SDM - Space Division Multiplex
[39] MIMO - Multiple Input Multiple Output

csatornákat használnak, ezáltal megduplázódik a sebesség. Az RIFS[40] a korábbinál kisebb várakozási időt tesz lehetővé a két keret továbbítása között. A következő ábrán a SISO[41] és a MIMO felépítése látható.

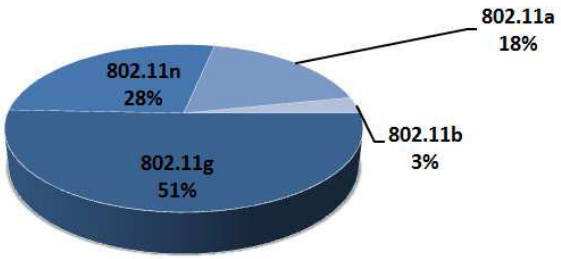


27. ábra: A SISO és a MIMO felépítése

Forrás: [38 p. 53]

2.2.6 Vizsgálati eredmények a 802.11 protokoll alapján

A protokollok eloszlása szintén egy fontos vizsgálati pontja a mérésnek. Hasonlóan a frekvenciasávok eloszlásához megmutatja a technológiai eszközök fejlődésének és elterjedésének tendenciáját. A wigle.net publikus adatbázisában nincs a protokollokra vonatkozó adat. A témával kapcsolatos mérési eredmények között a legkorábbi, ami összehasonlítható a saját adataimmal, 2008-ban készült. Azonban ebben az időben még nem jelentek meg a piacon a „n”-es eszközök, így az összehasonlítás nem teljes körű, így ezt nem tartottam célszerűnek az értekezésemben elvégezni. A 19. ábrán bemutatott útvonalon végrehajtott mérési eredményeim közül a 802.11-es protokollt használó eszközök eloszlásával kapcsolatos mérési eredményeimet a következő ábra mutatja.



28. ábra: 802.11-es protokollt használó eszközök eloszlása

Forrás: saját szerkesztés

[40] RIFS - Redue Inter Frame Spacing
[41] SISO - Single Input Single Ouput

Az eredmények szerint a vizsgált eszközök fele a 2003-ban megjelent „g" protokoll szabványát tudja kihasználni. Ami meglepő, hogy a 2009-ben kiadott „n" protokollt használó eszközök száma kevesebb, mint 3 év leforgása alatt 28%-os használatot mutat. Azt lehet mondani, hogy a „b" protokollt használó eszközök elenyésző mértékben vannak jelen a vizsgált adatokban, viszont az 1999-ben megjelent „a" protokollt használók valószínűleg az 5 GHz-es kevésbé zajos frekvenciasáv miatt 18%-os mértékben terjedtek el. A vizsgálat rámutatott még egy fontos dologra, hogy az 5 GHz-es frekvenciasávban jelenleg csak az „a" protokollos eszközök működnek, míg ezt az „n"-es eszközök nem használják ki.

A mérési adatokból kiválasztva és megvizsgálva az előzőekben meghatározott három kritikus információs infrastruktúrát megállapítom, hogy:

- az infokommunikációs technológiák ágazathoz tartozó infrastruktúrában a 802.11a, „g" és „n" protokollt használó eszközök találhatóak;
- az egészségügy ágazathoz tartozó infrastruktúrában a 802.11a, „g" és" n" protokollt használó eszközök fordultak elő;
- a közlekedés ágazatban a 802.11g és n protokollt használó eszközök találhatók.

Ezek alapján kijelenthető, hogy az általánosan vizsgált eszközök és a kritikus információs infrastruktúrában előforduló eszközök protokoll szempontjából történő eloszlása között nincs számottevő különbség.

2.2.7 WLAN topológiák

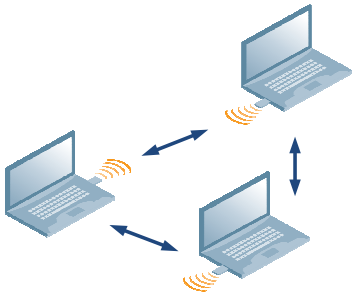
A vezeték nélküli hálózatok kialakításakor három típust különböztetünk meg:

- önálló alap szolgáltatáskészlet (IBSS[42])
- alap szolgáltatáskészlet (BSS[43]);
- kiterjesztett szolgáltatáskészlet (ESS[44]) [46 p. 39]

Az IBSS

A kapcsolatnak ez a fajtája a közvetlen kommunikáció. Ez úgy valósulhat meg, hogy az egymás rádiós hatósugarában lévő gépek peer-to-peer[45] összekapcsolódhatnak. Ezt a típusú hálózati kialakítást ad hoc hálózatnak is nevezik (29. ábra).

[42] IBSS - Independent basic service sets
[43] BSS - Basic service sets
[44] ESS - Extended service sets
[45] peer-to-peer - egyenrangú végpontok közötti közvetlen kapcsolat



29. ábra: IBSS

Forrás: saját szerkesztés

Az ilyen hálózatok akkor jönnek létre, ha a mobil eszközök önállóan alkotnak hálózatot hozzáférési pont nélkül. A neve is erre utal: ad hoc hálózat. A hálózat szereplői általában rövid időre kapcsolódnak egymáshoz. Az egymáshoz kapcsolódó eszközök száma nem korlátozott. Ezekben a hálózatokban az eszközök külső felügyelete nem lehetséges. A kapcsolat minden esetben a felhasználó felelőssége. Ez a típusú összeköttetés nagy kockázatot hordoz magában. Számos támadás érheti a nem megfelelően védett eszközt a másik fél irányából, ezért nem megbízható eszközhöz nem javasolt a kapcsolódás.

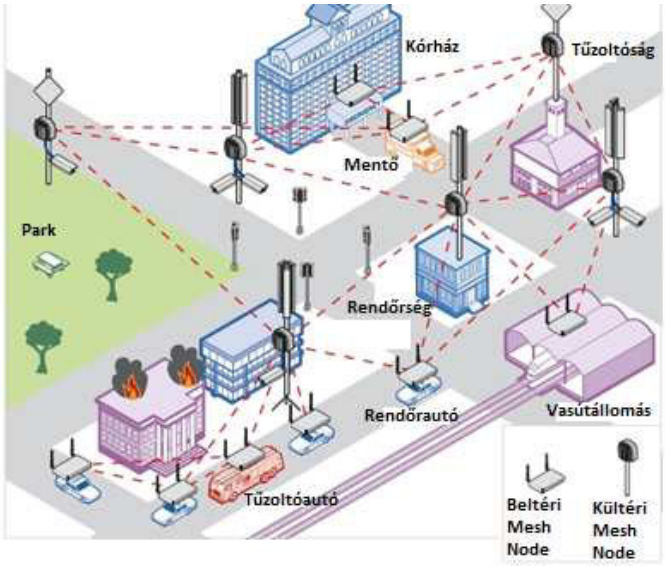
Az ad hoc hálózatoknak létezik egy másik kiépítési lehetősége is, amikor nem a számítógépeket, hanem az AP-okat kapcsoljuk ilyen üzemmódba. Jellemzően kültéri pont-pont összeköttetésesekre használják így az eszközöket. Abban az esetben, ha ezek a kültéri eszközök nem csak egymással, hanem több ilyen eszközzel is kapcsolatot tudnak létesíteni, bizonyos szabályozáson belül, egy úgynevezett MESH hálózatot[46] alkotnak.

A MESH hálózatok alkalmazási területei például a következőek lehetnek:

- videomegfigyelés;
- hangtovábbítás;
- adathálózati felhasználás.

A kritikus információs infrastruktúrákra jellemző MESH hálózati példát a 30. ábra mutatja. Látható, hogy egy ilyen hálózat mennyire szerteágazó, és sokrétű felhasználást tesz lehetővé. Egy ilyen hálózat segítségével közvetlen kapcsolatban lehetnek például a védelmi szervek, a tűzoltóság, a katasztrófavédelem és a mentő-szolgálat.

[46] MESH hálózat - szövevényes hálózat

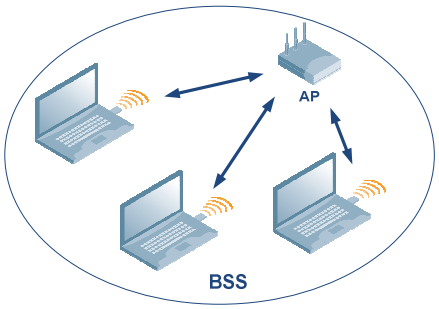


30. ábra: MESH hálózat kritikus infrastruktúrában

Forrás: [47]

A BSS

A BSS egymással kommunikáló vezeték nélküli eszközök, amelyek a kommunikációt egy AP-n keresztül valósítják meg (31. ábra). Az így létrejött kommunikációs csatorna az üzemeltető számára monitorozható, így nagyobb biztonságot jelent a felhasználók számára.



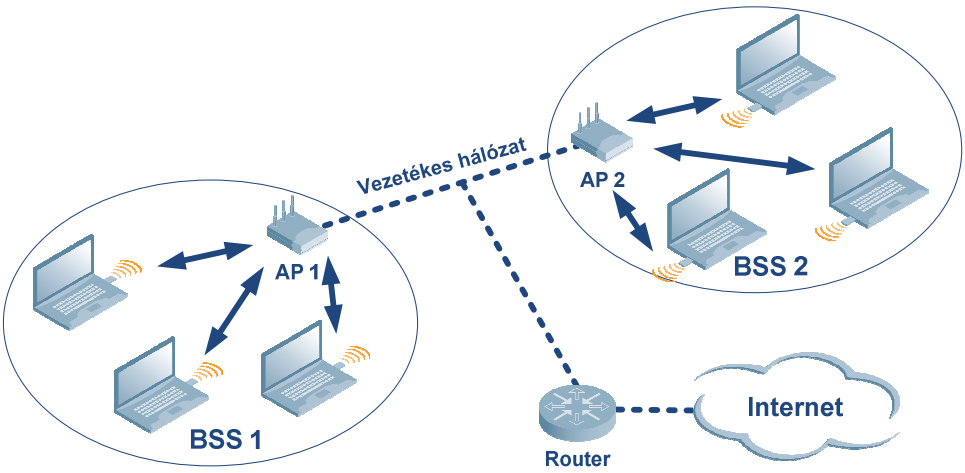
31. ábra: BSS

Forrás: saját szerkesztés

Az ESS

Abban az esetben, ha a hozzáférési pont LAN kommunikáció csatlakozását a vezetékes hálózatra csatlakoztatjuk, a hálózaton belül akár más BSS-t is elérhetünk. A vezetékes

hálózaton keresztül akár szélessávú internetet is tudunk biztosítani a felhasználók számára (32. ábra).

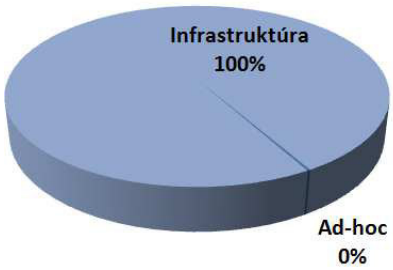


32. ábra: ESS

Forrás: saját szerkesztés

2.2.8 Vizsgálati eredmények a WLAN topológiák alapján

A vizsgálat során az eszközöket a topológiai paraméterei alapján két csoportra tudtam bontani. Az ad-hoc topológiára beállított eszközök csoportjára és az Infrastruktúra módba állított eszközök csoportját. A mérés nem ad pontos értéket arra, hogy melyik hálózat tisztán IBSS, BSS vagy ESS, azt viszont jól tükrözi, hogy milyen eloszlásban találhatók meg az eszközök. (33. ábra)



33. ábra: WLAN topológiák eloszlása

Forrás: saját szerkesztés

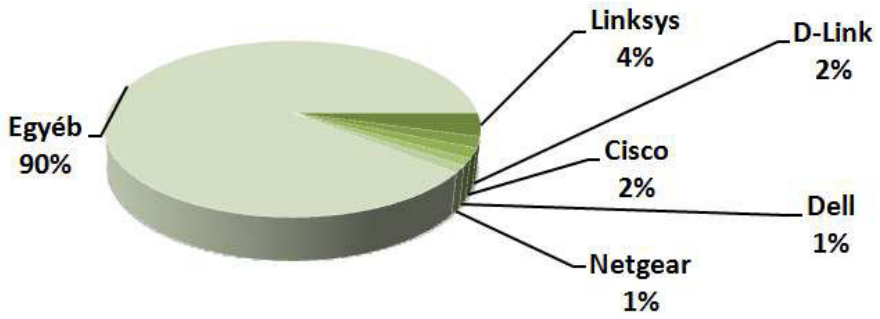
Az ad-hoc módba konfigurált eszközök darabszáma elenyésző volt (7db) a teljes vizsgált mintában. A mérési adatokból kiválasztva és megvizsgálva az előzőekben meghatározott három kritikus információs infrastruktúrát megállapítom, hogy ezen infrastruktú-

rák vezeték nélküli hálózataiban nem található ad-hoc módban beállított eszköz. Ez azért fontos, mert ilyen irányú támadások ellen védettek ezek az infrastruktúrák.

2.2.9 A vezeték nélküli hálózatok hozzáférési pontjainak gyártói

A vezeték nélküli hálózati eszközöket a szabványosítások után számos cég kezdte el gyártani. Ezek között voltak több éves tapasztalattal rendelkezők és új vállalatok is. Léteznek olyan cégek, amelyek saját hitelesítési eljárást is kidolgoztak. A gyártók vizsgálata a védelem és a támadhatóság szempontjából fontos. A wigle.net adatai alapján az eszközgyártók piaca eléggé kiegyensúlyozott. (34. ábra)

A budapesti mérési eredmények más képet mutatnak. Az adatok alapján egy nagyon tetemes – 53%-nyi – csoportot alakítottam ki azok között a gyártók között, amelyek aránya 5% alatt volt, vagy a mérés során nem sikerült az eszközt beazonosítani. (35. ábra)



34. ábra: Eszközgyártók felhasználási rangsora a wigle.net adatai alapján

Forrás: [32]

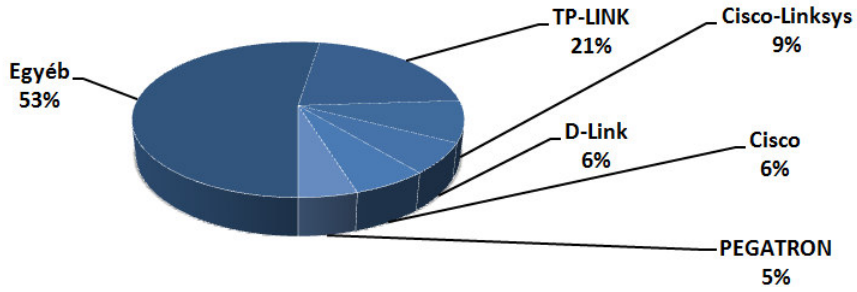
A gyártók között van aki otthoni, kisvállalati (SOHO[47]) környezetbe ajánlja eszközeit, ilyen például a Cisco-Linksys LLC, de azt is be lehet azonosítani, hogy az eredmények tükrében bizonyos, hogy a Cisco adatai szerint több mint 7% vállalati (Enterprise) infrastruktúrához tartozó eszköz. A többi vállalat gyárt eszközöket otthoni és vállalati felhasználásra egyaránt.

A SOHO és az Enterprise eszközök között számos tulajdonságbeli eltérés van. A SOHO eszközök csak önállóan menedzselhetőek, hitelesítési és titkosítási készlete korlátozott és nem támogatja az Enterprise infrastruktúra környezetet, önálló tűzfal funkciója nincsen, de szolgáltatásai egy otthoni és kisvállalati környezet ellátására alkalmasak.

[47] SOHO - Small Office / Home Office

Ezzel szemben az Enterprise eszközök központilag menedzselhetőek, hitelesítési és titkosítási készleteik támogatják az Enterprise infrastruktúra környezetet, e mellett rendelkezhetnek még a következő funkciókkal:

- spektrum analizátor;
- egyéni felhasználó szintű tűzfal;
- monitorozási képesség;
- MESH hálózatba szerveződés.



35. ábra: Eszközgyártók felhasználási rangsora saját mérési adatok alapján

Forrás: saját szerkesztés

A mérési adatokból kiválasztva és megvizsgálva az előzőekben meghatározott három kritikus információs infrastruktúrát megállapítom, hogy ezen infrastruktúrák vezeték nélküli hálózataiban

- az infokommunikációs technológiák ágazathoz tartozó infrastruktúrában csak vállalati felhasználásra szánt eszközöket használnak;
- az egészségügy ágazathoz tartozó infrastruktúrában vegyesen találhatók vállalati és nem vállalati felhasználású eszközök;
- a közlekedés ágazathoz tartozó infrastruktúrában csak nem vállalati felhasználású eszközök találhatóak.

Az infrastruktúra védelmének szempontjából a nem egységes hálózati infrastruktúra egyike lehet a támadási felületeknek.

2.3. Vezeték nélküli hálózatok hitelesítési és titkosítási módszerei

A korábban hivatkozott források, valamint a vizsgálati eredményeim alapján igazolható, hogy a vezeték nélküli hálózatok a kritikus információs infrastruktúrák szerves részeivé váltak. Ahhoz, hogy erre az infrastruktúra elemre is ki lehessen jelenteni azt, hogy olyan

biztonságos, mint a vezetékes hálózat, a következő öt alapvető jellemzőt kell mindig szem előtt tartani:

- az adatok védelmét;
- a hitelesítést, hozzáférést, naplózás egységét;
- szegmentálást;
- monitorozást;
- hálózati politikát. [48 p. 12]

Az infrastruktúra üzemeltetők minden esetben arra törekszenek, hogy ezt az öt alapelemet beépítsék meglévő hálózatukba, vagy tervezéskor ezekre az elemekre építkezzenek.

A mérési adataim alapján a vezeték nélküli hálózatok hitelesítését és titkosítását elemeztem.

2.3.1 Hitelesítési protokollok

Az alapvető hálózati biztonság megteremtéséhez elengedhetetlen a hálózati kommunikáció megfelelő hitelesítése és titkosítása. A következő táblázat az alapvető hitelesítési és titkosítási metódusok fejlődését mutatja be:

6. táblázat: alapvető hitelesítési és titkosítási metódusok

802.11 szabvány	**Wi-Fi tanúsítvány**	**Hitelesítési metódus**	**Titkosítási metódus**
802.11		nyílt hitelesítés vagy osztott kulcsú	WEP[48]
	WPA-egyéni[49]	WPA-jelszó (más néven: WPA-PSK[50])	TKIP
	WPA-vállalati	802.1X/EAP[51]	TKIP[52]
802.11-2007	WPA2-egyéni	WPA2-jelszó (más néven: WPA2-PSK)	AES-CCMP[53] TKIP
802.11-2007	WPA2-vállalati	802.1X/EAP	AES- CCMP TKIP

Forrás: [38]

[48] WEP - Wired Equivalent Privacy
[49] WPA - Wi-Fi Protected Access
[50] PSK - Pre-shared key
[51] EAP - Extensible Authentication Protocol
[52] TKIP - Temporal Key Integrity Protocol
[53] AES - Advanced Encryption Standard

Nyílt hitelesítés

Ez a legegyszerűbb hitelesítési folyamat. Kétirányú üzenetcsere történik, amelyben a kezdeményező eszköz üzenetet küld a hozzáférési pontnak, amely válaszként közli a hitelesítés sikerességét, vagy sikertelenségét. Az SSID birtokában bárki csatlakozhat egy nyílt hitelesítéssel ellátott eszközhöz. Ez a hitelesítés nagyon elterjedt kávézókban, repülőtéren, szórakozóhelyeken ahol az alapszolgáltatás mellett nyílt hitelesítéssel ellátott AP-on keresztül szolgáltatnak internet hozzáférést. Az eszköz és az AP közötti kommunikáció semmilyen biztonsági mechanizmust nem tartalmaz. Ezen eszközök adatforgalma lehallgatható, visszafejthető. [34 p. 341]

Osztott kulcsú hitelesítés

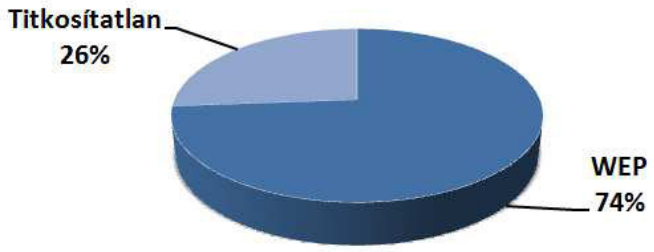
Az osztott kulcsú hitelesítést négyutas kézfogásos hitelesítésnek is nevezik. Összesen viszont 6 lépésből áll:

1. a kezdeményező fél eszköze egy hitelesítési kérelmet küld az AP-nak;
2. az AP egy kihívással válaszol erre a kérelemre;
3. a kérelmező titkosítja a kihívási szöveget a kulcsával;
4. a kérelmező a titkosított üzenetet visszaküldi a hozzáférési pontnak;
5. a hozzáférési pont dekódolja a szöveget;
6. a dekódolt szöveg és egyéb feltételek teljesülésének vizsgálata, majd ennek tükrében engedélyezi, vagy tiltja a kapcsolatot. [49 p. 29]

Az osztott kulcsú hitelesítéskor a kulcsot manuálisan kell megadni az eszközben és az AP-ban is. Ez alapvetően hibalehetőséget hordoz magában. Az ilyen típusú hitelesítés titkosítási lehetőségei között található a WEP, amelynek már több éve jól dokumentált sebezhetőségei vannak. Ezért ezt a típusú hitelesítést infrastruktúrák számára nem ajánlják. [34 p. 342]

2.3.2 Nyílt és osztott kulcsú hitelesítés vizsgálata

Az általam mért adatok között a titkosítatlan és a WEP titkosítással ellátott eszközök arányát a 36. ábra mutatja. A mérési adatokból kiválasztva és megvizsgálva az előzőekben meghatározott kritikus információs infrastruktúrát megállapítom, hogy ezen infrastruktúrák vezeték nélküli hálózataiban a nyitott és az osztott kulcsos hitelesítés szempontjából vegyes képet mutat.



36. ábra: Nyílt és osztott kulcsú hitelesítés arányai

Forrás: saját szerkesztés

Egyedül a közlekedés ágazathoz tartozó infrastruktúra eszközparkja használ erősebb hitelesítést. Az infokommunikációs technológiák ágazathoz tartozó eszközök között volt nyílt hálózati eszköz is, amelyet „Vendég” hálózatként be lehetett azonosítani. Egy jól menedzselt vállalati infrastruktúrában megengedhető egy szegmentált nyílt vállalati vendég végpont.

Az egészségügy ágazathoz tartozó eszközök közt megtalálható a nyílt, az osztott kulcsos és az erősebben védett hálózati végpont is. Támadhatóság szempontjából ez az infrastruktúra véleményem szerint potenciális támadási pont lehet.

802.1x hitelesítés

Az informatikusok idővel rájöttek, hogy a WEP hibáinak kijavítása nem teszi biztonságossá a hálózatot. Akkor mondhatjuk, hogy biztonságos a kapcsolat, ha a kapcsolat felépítésekor a felhasználót és az eszközt is hitelesíti a rendszer. Ennek a problémának a megoldására vezették be a 802.1X protokollt. Ez a protokoll kölcsönös hitelesítést biztosít, azaz a felhasználónak és az eszköznek is azonosítania kell önmagát.

A szabvány előnye, hogy többfajta hitelesítési eljárást is támogat. Azok a hozzáférési pontok, amelyek támogatják a 802.1X szabványt és az általa definiált EAP protokollt, egyfajta interfészként működnek a vezeték nélküli kliensek és a hitelesítő szerver között. Ilyen megvalósítást lehet kialakítani a hálózatba integrált RADIUS[54] hitelesítő szerves segítségével. [37 p. 29]

A vezeték nélküli hálózatok 802.1x alapú hitelesítésének három fő összetevője van:

- hitelesítő (hozzáférési pont),
- kérelmező (kliensszoftver),

[54] RADIUS - Remote Access Dial-In User Service

- hitelesítő szerver (RADIUS).[49]

A RADIUS alapú hitelesítés a felhasználók azonosítását adatbázisok alapján ellenőrzi. *„A RADIUS egy sor szabványt valósít meg, amelyek a hitelesítés, az engedélyezés és a használatkövetés (AAA[55]) területét fedik le. A RADIUS több kiszolgálós környezetben proxy útján hitelesíti az ügyfeleket. Az IEEE 802.1x szabvány szabályozza a 802.11 szerinti port alapú, vezeték nélküli és vezetékes Ethernet hálózatok elérését, és gondoskodik a hitelesítésről."* [49]

2.3.3 A WPA és a WPA2

A WPA olyan továbbfejlesztett biztonsági lehetőség, amely erősíti a vezeték nélküli hálózatok adatvédelmét és hozzáférés-szabályozását. A WPA megvalósítja a 802.1x szerinti hitelesítést és kulcscserét, és csak dinamikus titkosító kulcsokkal használható. A WPA az adattitkosítás erősítése céljából saját TKIP protokollját alkalmazza. [50]
A WPA második generációja a WPA2. Ezt azért alkották meg, mert kiderült a WPA sebezhetősége. A 802.11i szabvány ezeket a gyenge pontokat küszöböli ki. Bevezetéséig mindössze egyetlen titkos kulcsot használtak a hitelesítésre és az adattitkosításra is. Az új szabványban kulcskezelési és generálási hierarchiát dokumentáltak, hogy megoldott legyen a kulcsok rendszeres cseréje. Ez teszi biztonságossá a WPA2-t. [51 p. 2]

A WPA és WPA üzemmódjai

Vállalati üzemmód

Az Enterprise (vállalati) üzemmód RADIUS vagy más hitelesítő kiszolgálóval hitelesíti a hálózati felhasználókat és eszközöket. A WPA 128 bites titkosító kulcsokkal és dinamikus munkamenet-kulcsokkal biztosítja a vezeték nélküli hálózat biztonságát. A vállalati üzemmód a kapcsolat EAP protokollt használja, illetve 802.11x biztonsági szabványt a felhasználói eszközökön. Ebben az üzemmódban biztosítható még a többszintű felhasználói jogosultság kezelés is. A WPA és a WPA2 is támogatja a vállalati üzemmódot.

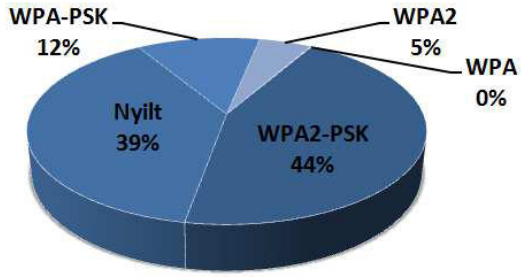
[55] AAA - Authentication, Authorization, Accounting

Személyes üzemmód

A Personal (személyes) üzemmódnál kézileg kell beállítani egy előre közölt kulcsot a hozzáférési pontokon és az ügyfeleken. A PSK jelszóval vagy azonosító kóddal hitelesíti a felhasználókat mind a felhasználó eszközén, mind a hozzáférési ponton. Hitelesítő kiszolgálót nem igényel. A személyes üzemmódot egyszerűsége miatt otthoni és kisvállalati felhasználók esetén célszerű használni. A WPA és a WPA2 is támogatja a személyes üzemmódot.

2.3.4 WPA és WPA2 vizsgálata

A kritikus információs infrastruktúrák vezeték nélküli hálózatának biztonsága szempontjából megvizsgáltam a WPA, WPA2 és a Nyílt hálózatok eloszlását. Fontosnak tartom megemlíteni, hogy a kritikus infrastruktúrák szemszögéből nem csak maga a kritikus információs infrastruktúra vezeték nélküli hálózatának védelme fontos, hanem a többi potenciálisan gyenge védelemmel ellátott, máshol elhelyezkedő végpontok is. Ezek a gyengén védett végpontok lehetnek a kiindulópontjai egy esetleges informatikai támadásnak is. (37. ábra)



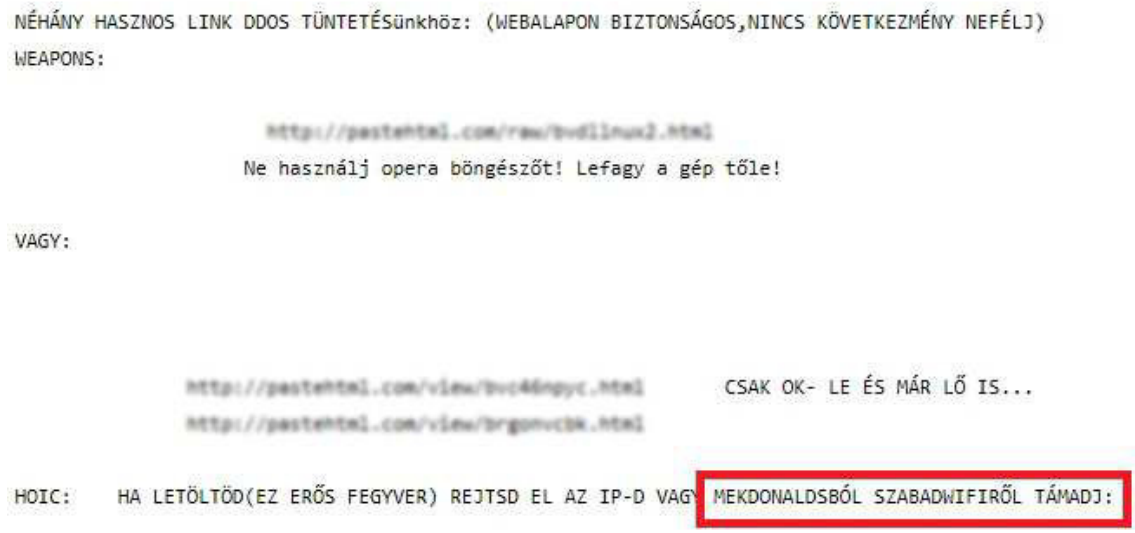
37. ábra: A WPA, WPA2, WPA-PSK, WPA2-PSK és nyílt hálózatok eloszlása

Forrás: saját szerkesztés

A vizsgálati eredmények azt mutatják, hogy az eszközök nagy százaléka a WPA2-PSK-t használja. Ezek a hálózatok biztonságosnak mondhatóak a ma ismert támadások nagy része ellen.

Ami aggodalomra ad okot, hogy a vizsgált hálózatok 39% nyitott volt. Ez azt jelenti, hogy védtelenek az informatikai támadásokkal szemben. Potenciálisan ők, vagy rajtuk keresztül más hálózaton elérhető erőforrásokat lehet megtámadni. Nagyon sok esetben a számítógépes bűnözésre szakosodott „informatikusok” ilyen nyitott végpontokat használnak ki támadásaik indítására. Erre a bűncselekményre buzdított például az Anony-

mus aktivistacsoport 2012. áprilisában.[52] A következő ábra a csoport felhívását mutatja:



38. ábra: Anonymus aktivistacsoport felhívása informatikai támadásra nyílt hálózaton keresztül

Forrás: [52]

A mérési adatokból kiválasztva és megvizsgálva az előzőekben meghatározott három kritikus információs infrastruktúrát megállapítom, hogy ezen infrastruktúrák vezeték nélküli hálózataiban a WPA, WPA2, WPA-PSK, WPA2-PSK és nyílt hitelesítés szempontjából vegyes képet mutat. A közlekedés ágazathoz tartozó infrastruktúrában az eszközök a WPA2-PSK hitelesítési módot használják. Az infokommunikációs technológiák ágazathoz tartozó eszközök között volt nyílt hálózati eszköz is, de a többi eszköz WPA2 Enterprise üzemmódban van.

Az egészségügy ágazathoz tartozó eszközök közt megtalálható a nyílt, az osztott kulcsos és az erősebb WPA2-PSK hitelesítésű eszköz is. A vizsgálati eredmények azt mutatják, hogy a kritikus infrastruktúrák nem minden esetben használják vezeték nélküli hálózati eszközeiket vállalati (Enterprise) üzemmódban.

2.3.5 Titkosítási protokollok

A 802.11i szabványban foglalt kiegészítésekkel együtt három titkosítási protokoll áll rendelkezésre a 802.11 szabványban: WEP, TKIP, AES-CCMP.

WEP

Az IEEE 802.11 WEP titkosítási protokollt az alapszabvány már definiálta. A szabvány két biztonsági szintet tartalmaz, amelyek egyike 64 bites kulcsot használ, a másik pedig 128 bites kulcsot. Titkosítás alkalmazásakor a vezeték nélküli hálózaton lévő valamennyi vezeték nélküli eszköznek ugyanazokat az előre kiosztott titkosítási kulcsokat kell használnia. A hitelesítéshez az RC4[56] titkosító eljárást alkalmazza. A WEP titkosítási algoritmus sebezhető a támadásokkal szemben. [50] Legnagyobb hátránya, hogy a statikus kulcs birtokában bárki hozzáférhet a hálózat erőforrásaihoz. Szakemberek ezt a titkosítást nem tartják kellő védelemnek a vezeték nélküli hálózatokon, ezért az ilyen hálózatokat sokszor automatikusan a nyitott hálózatok közé sorolják.

TKIP

A WEP hibái miatt megalkották a TKIP protokollt, mint egy köztes biztonsági protokollt a WEP és egy sokkal biztonságosabb AES-CCMP között.[49 p. 36] A később elfogadott WPA2 a TKIP mellett tartalmazza és lehetővé teszi az AES titkosítást. A TKIP titkosítási mód kiküszöböli a WEP hibáit, de évekkel később japán tudósok rájöttek, hogy védtelen a visszajátszásos támadással szemben. A támadást egy perc alatt végre tudták hajtani, amit 2009-ben publikáltak is.[53]

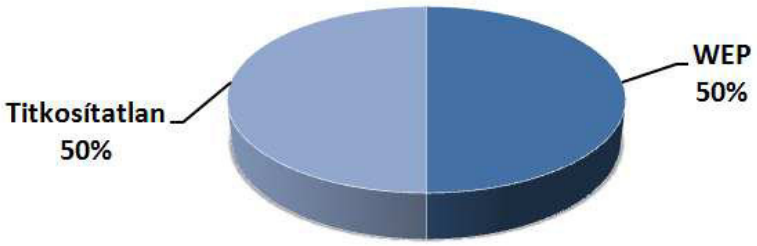
AES-CCMP

A 802.11i szabvány másik titkosítási protokollja a CCMP[57]. A CCMP erősebb titkosítási algoritmus, mint a TKIP – ezért ha lehet, inkább az AES-t használjuk – és szintén biztosítja a bizalmasságot, integritást és a visszajátszás elleni védelmet. [49 p. 36] A CCMP alapja az AES blokkrejtjelező szabvány, mely egy nemzetközi verseny eredményeképpen születetett meg a már elavult DES[58] szabvány helyettesítésére. [54 p. 3]

2.3.6 Titkosítási protokollok vizsgálata

A kritikus információs infrastruktúrák vezeték nélküli hálózatának biztonsága szempontjából a titkosítási protokollok szervesen kapcsolódnak a hitelesítési protokollokhoz.

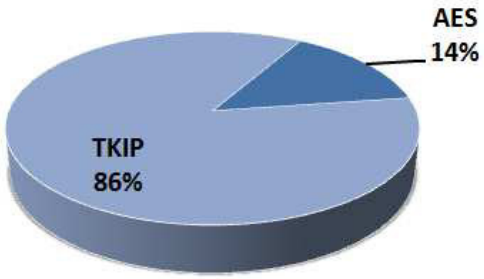
[56] RC4 - Rivest Cipher 4
[57] CCMP - Counter Mode/CBC-MAC Protocol
[58] DES - Data Encryption Standard



39. ábra: Nyílt vagy osztott kulcsú hitelesítés titkosítása

Forrás: saját szerkesztés

A vizsgálat szempontjából megállapítottam, hogy a nyílt vagy osztott kulcsú hitelesítés titkosítása fele-fele arányban fordul elő a teljesen titkosítatlan és a WEP titkosítással ellátott hálózatok között. Az is bizonyos, hogy a WEP titkosítást már nem tekintjük védelmi lépésnek, így az ilyen hálózatokat teljesen nyíltként kezeljük.



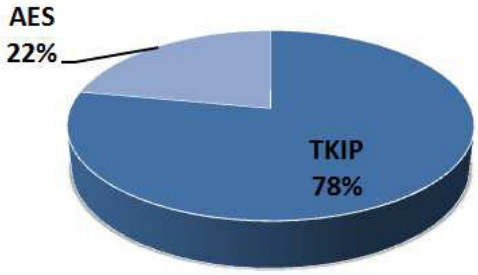
40. ábra: WPA-PSK titkosítása

Forrás: saját szerkesztés

A WPA-PSK titkosítási eloszlása azt mutatja, hogy az eszközök nagy része amely ezt a hitelesítést alkalmazza a gyengébb, és támadható TKIP titkosítást használja.

A WPA-Enterprise titkosítást összesen csak 3 eszköznél azonosítottam be. A WPA2-PSK hitelesítéssel üzemelő eszközök titkosítási eloszlását a 41. ábra mutatja.

Az ábrán jól látszik, hogy a titkosítások eloszlása nem egyenletes. Ez véleményem szerint annak is köszönhető, hogy alapesetben egy WPA2-PSK hitelesítés beállításakor automatikusan az eszköz menüje a TKIP hitelesítést ajánlja fel elsőként.

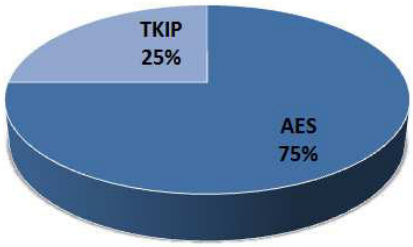


41. ábra: WPA2-PSK titkosítása

Forrás: saját szerkesztés

Mivel nagy valószínűséggel ezek az eszközök lakásokban vagy kisebb infrastruktúrákban üzemelnek, ahol informatikus nem segít az eszközök beállításánál az alapbeállításokat konfiguráláskor a felhasználók nem állítják át.

A következő ábra a WPA2-Enterprise hitelesítéshez tartozó titkosítások eloszlását mutatja:



42. ábra: WPA2-Enterprise titkosítása

Forrás: saját szerkesztés

Az előző megállapításomat támasztja alá a WPA2-Enterprise hitelesítéssel működő eszközök titkosítási eloszlása. Az arány teljesen megfordult, annak köszönhetően, hogy ezzel a hitelesítéssel és titkosítással ellátott eszközöket nagy valószínűséggel képzett szakemberek állították be.

A mérési adatokból kiválasztva és megvizsgálva az előzőekben meghatározott három kritikus információs infrastruktúrát megállapítom, hogy ezen infrastruktúrák vezeték nélküli hálózatai titkosítási beállításai különböznek egymástól:

- a közlekedés ágazathoz tartozó infrastruktúrában az eszközök az AES titkosítást használják;

- az infokommunikációs technológiák ágazathoz tartozók között volt titkosítatlan, TKIP és AES titkosítással ellátott eszköz is;
- az egészségügy ágazatban szintén volt titkosítatlan, WEP és AES titkosítást használó eszköz.

2.4 A vizsgálati eredmények összesítése

A három kritikus információs infrastruktúra vizsgálati eredményeit a következő összesített táblázat mutatja.

7. táblázat: A három kritikus információs infrastruktúra vizsgálati eredményei

	Infokommunikációs ágazat	**Közlekedés ágazat**	**Egészségügy ágazat**
Rádiós szegmens	2,4 GHz, 5 GHz	2,4 GHz	2,4 GHz, 5 GHz
Csatornakiosztások alakulása	1-es,6-os, 64-es	1-es, 11-es	1-es, 6-os, 60-as
802.11-es protokollok eloszlása	802.11a,802.11g, 802.11n	802.11g, 802.11n	802.11a,802.11g, 802.11n
WLAN üzemmódok	Infrastruktúra	Infrastruktúra	Infrastruktúra
Eszköz típusok	Enterprise WLAN	SOHO WLAN	Enterprise, SOHO WLAN
Nyílt és osztott kulcsú hitelesítés	van azonosított „Vendég”	-	van
WPA és WPA2 vizsgálata	WPA2 Enterprise	WPA2 PSK	WPA2 PSK
Titkosítási protokollok	titkosítatlan, TKIP, AES	AES	titkosítatlan, WEP, AES

Forrás: saját szerkesztés

A összesítő táblázat adatai azt mutatják, hogy az infokommunikációs és az egészségügyi ágazat eszközei között megtalálhatóak az 5 GHz-es kevésbé leterhelt rádiós szegmensben üzemelő WLAN-ok.

A csatornakiosztásokat mind a három kritikus információs infrastruktúrában jól alkalmazzák.

A 802.11-es protokollt használó eszközei nem homogének, ami a teljes hálózatba való integrációt megnehezítheti.

Üzemmód szempontjából mind a három helyen csak „Infrastruktúra” módban használt eszközök üzemelnek.

Tisztán Enterprise WLAN eszközöket csak az infokommunikációs ágazat kritikus információs infrastruktúrájában használnak. A közlekedés ágazat infrastruktúrájában pedig csak SOHO eszközöket találtam. Egyedül az egészségügyi ágazat infrastruktúrájában mértem vegyesen Enterprise és SOHO eszközöket. Ez a vegyes megoldás nem teszi lehetővé a hálózat egységes menedzselhetőségét.

A hitelesítés és titkosítás szempontjából is eltérő megoldások találhatóak az infrastruktúrákban. Az infokommunikációs ágazatban mértem nyitott, titkosítatlan hálózati eszközt is, amely jól beazonosítható „Vendég” szegmens volt. E mellett WPA2 Enterprise hitelesítésű és AES titkosítással üzemeltetett eszközöket használnak. A közlekedés ágazat kritikus információs infrastruktúrájában a SOHO eszközök által nyújtható legerősebb hitelesítést és titkosítást használják a WLAN hálózatban. Az egészségügy ágazat infrastruktúrájának vegyes a hálózata. Ezt a hálózatot hitelesítési és titkosítási szempontból számos helyen gyenge – WEP vagy titkosítatlan – beállítások sebezetővé teszi, ezért fontosnak tartottam megvizsgálni a lehetséges támadási útvonalakat a vezeték nélküli hálózaton keresztül a kritikus információs infrastruktúra irányába.

2.5. Támadási útvonalak a vezeték nélküli hálózaton keresztül a kritikus információs infrastruktúra irányába

A világon a legnagyobb és legtöbb országot érintő vezeték nélküli hálózatok elleni támadását[59] a Google hajtotta végre 2006. és 2010. között. A Street view alkalmazásukhoz készített felvételek mellett a gépjárművek nem csak fényképeket, hanem WLAN adatokat is gyűjtöttek. A cég elismerte, hogy abban az esetben, amikor a hozzáférési pont nem rendelkezett hitelesítéssel és titkosítással nem csak alapinformációkat (SSID, koordináták,stb.) gyűjtöttek, hanem magát a forgalmat is rögzítették. 2010-ben, amikor kiderült ez az információ a Google elnézést kért mindenkitől. Minden ország maga dönthette el, mit kezd a helyzettel. Egyes országok kérték az adatok megsemmisítését, de voltak országok, amelyek elkérték a gyűjtött adatokat. Ezt az ügyet még nem sikerült a Google-nak teljesen lezárnia.[55] A 43. ábrán a Németországi Street view flotta látható.

[59] A támadás minősítés lehet, hogy erősnek tűnik – főleg egyértelmű jogi, katonai osztályozás hiányában – azonban az információtechnológiai környezetből történő információszerzés már információs műveletnek minősül a katonai doktrínák és szakirodalom alapján, illetve egyértelműen támadásnak minősül a számítógép hálózatok felderítése (Computer Network Exploitation - CNE) az etikus hekkelés során.

Vizsgálataim és a kutatott irodalmak rámutattak arra, hogy a kritikus információs infrastruktúrák vezeték nélküli hálózat kiépítése, titkosítása és hitelesítése szempontjából eltérnek egymástól. Ez az eltérés a támadók számára a lehetséges támadások több forgatókönyvét teszi lehetővé attól függően, hogy a támadó milyen céllal próbál az infrastruktúra vezeték nélküli hálózatához csatlakozni.

43. ábra: Németországi Street view flotta

Forrás: [55]

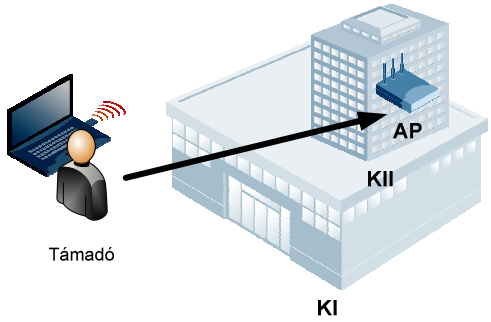
A kritikus információs infrastruktúra vezeték nélküli hálózati eszköze lehet:

- a támadás kiindulópontja;
- a közege és;
- a célpontja.

Ebben a fejezetrészben rendszerezem a kritikus információs infrastruktúrák lehetséges WLAN támadási útvonalait.

2.5.1 Kritikus információs infrastruktúra hozzáférési pontjának megtámadása

Ennél a modellnél a támadó célja a kritikus információs infrastruktúra vezeték nélküli hálózat AP támadása. A támadás célja elsősorban a végpont rendelkezésre állásának megsértése, a többi felhasználó megakadályozása, vagy korlátozása abban, hogy rendeltetésszerűen használja azt (44. ábra). A támadás végrehajtható szándékosan, vagy gondatlanul. Gondatlan végrehajtáskor a támadó vagy valamilyen zavaró jelet bocsát ki, vagy olyan nagy forgalmat generál, hogy azzal lehetetleníti el a normál használatot.



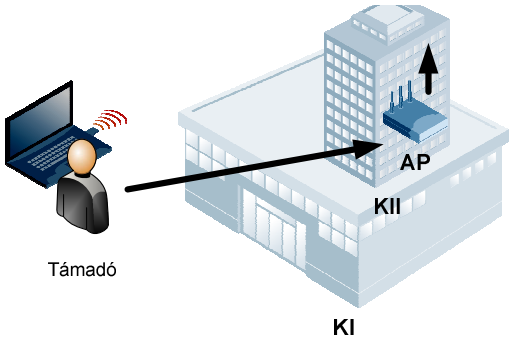
44. ábra: Támadás a kritikus információs infrastruktúra hálózati végpontja ellen

Forrás: saját szerkesztés

2.5.2 Kritikus információs infrastruktúra támadása a hozzáférési pontján keresztül

Ennél a modellnél a lehetséges támadó nem elégszik meg a hozzáférési pont működésének korlátozásával, hanem normál vagy rendszergazdai hozzáférést szerez a hálózati végpont felett és azon keresztül lehallgatja a hálózat egyik kritikus információs infrastruktúra szegmensét, kapcsolódik a megtámadott kritikus információs infrastruktúrához és ott adatokat szerez meg, módosít vagy töröl. Az általam vizsgált adatok alapján ez lehet pl. egy adatbázisszerver amely a betegek, dolgozók és az infrastruktúra adatait tárolja.

Idén februárban támadás érte a FOXCONN elektronikai nagyvállalatot. A cég az Intel, Apple, Nokia, Microsoft, stb. beszállítója. Levelezési felhasználóneveit és jelszavait lopta el a @Swaggsec csoport.[57] A támadás az általam leírt támadási útvonalon is történhetett. A 45. ábra ezt a támadási útvonalat mutatja.



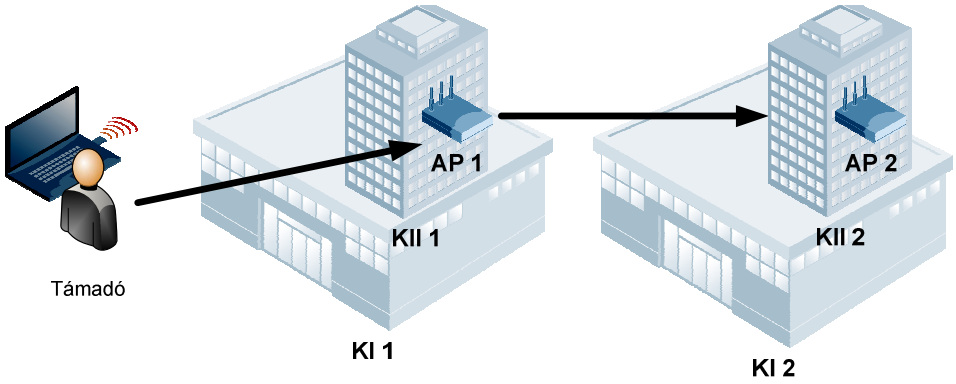
45. ábra: Kritikus információs infrastruktúra támadása a hozzáférési ponton keresztül

Forrás: saját szerkesztés

Ez a támadási modell csak szándékosan hajtható végre.

2.5.3 Kritikus információs infrastruktúra támadása egy másik kritikus információs infrastruktúra hozzáférési pontján keresztül

Ezt a típusú támadást akkor lehet végrehajtani, ha több kritikus információs infrastruktúra található egymás vezeték nélküli hálózati környezetében. Erre tipikus példa, ami számos nagyvárosban, így Budapesten is jellemző, hogy kritikus információs infrastruktúrák egy kerületbe, egy infrastruktúra környezetbe épülnek. Ilyenkor elkerülhetetlen, hogy egymás vezeték nélküli hálózati eszközeinek hatósugara ne találkozzon. A támadásra példa a 2012. júliusában az Anonymus aktivistacsoport akciója, aki 40 GB-nyi vállalati adatot lopott az ausztrál AAPT internet szolgáltatótól tiltakozásul egy új jogszabály bevezetése ellen.[58] A következő ábra egy ilyen lehetséges támadást ábrázol.



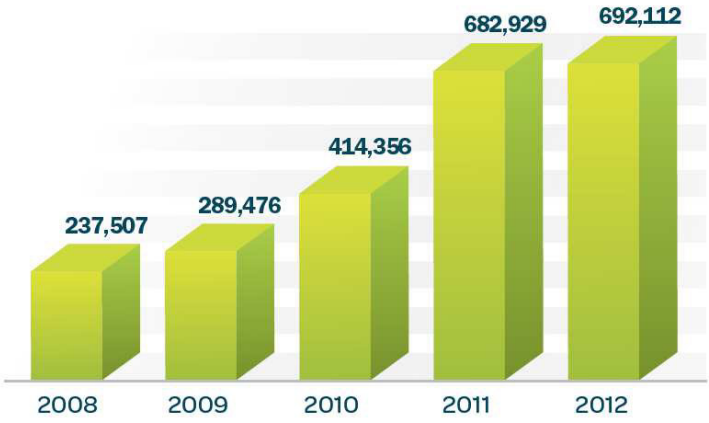
46. ábra: Kritikus információs infrastruktúra támadása egy másik kritikus információs infrastruktúra hozzáférési pontján keresztül

Forrás: saját szerkesztés

2.5.4 Kritikus információs infrastruktúra támadása nyilvános hálózati végpontról

A vezeték nélküli hálózatokról indított támadások közül ez a támadási útvonal a leggyakoribb. A világon évente szinte megduplázódnak a nyilvános hálózati végpontok. Ezt a tendenciát mutatja az 47. ábra.

A nyilvános végpontok az esetek nagy százalékában titkosítatlan és hitelesítés nélküli kapcsolatkiépítést tesztnek lehetővé. Ez által az ilyen végpontokról indított támadások elkövetőit nem, vagy csak nagyon kis esetben lehet megtalálni. A nyilvános végpontokról indított támadások közül a kritikus információs infrastruktúrák elleni támadások sok esetben sikerrel járnak.



47. ábra: Nyilvános WLAN a világban

Forrás: [59 p.10]

Ez azért történhet meg, mert a támadó változtathatja helyét, és bárhol elrejtőzhet egy nyilvános végpont mögött, ahonnan számtalanszor próbálkozhat a támadással. 2012. júniusában a @Zero0Pwm csoport támadást intézett az AT&T telekommunikációs nagyvállalat VOIP szolgáltatásai ellen. A sikeres támadás során hat adminisztrációs hozzáférést sikerült a csoportnak szereznie. [60]

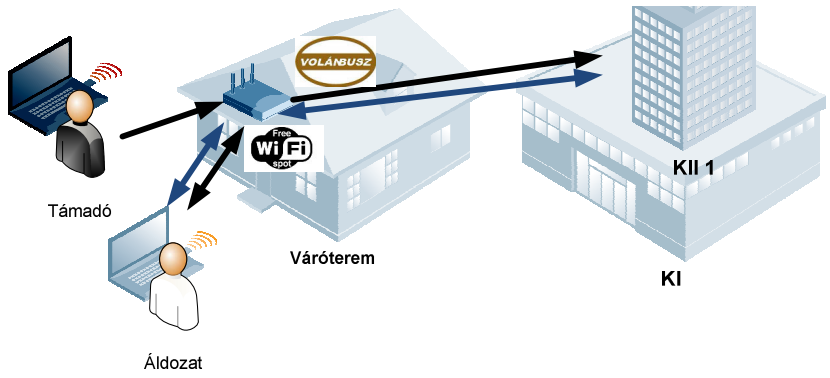
2.5.5 Kritikus információs infrastruktúra támadása nyilvános hálózati végponthoz kapcsolódó infrastruktúra felhasználón keresztül

Ez a támadási út olyan nyilvános hozzáférési pont környékén lehetséges, ahol számos üzletember megfordul. Ilyenek például a repterek, pályaudvarok. Számos lehetőség nyílik ilyenkor a nyilvános hálózat monitorozása során hozzáférési felhasználónév, esetleg jelszó páros megszerzésére. Sokan gondolják azt, hogy az utazás során eltöltött idő kihasználatlan. Ezt felismerve számos személyszállításra szakosodott vállalat nyilvános internet-hozzáférést biztosít járatain, így nem csak a várótermekben, hanem a járatokon is igénybe lehet venni az internet szolgáltatást nyílt hozzáférési ponton keresztül.

Hazánkban a következő személyszállításra szakosodott vállalatok biztosítanak járműveiken nyílt hozzáférési ponton keresztül internet-hozzáférést:

- taxi vállalat;[61]
- busztársaság;[62]
- vasúttársaság.[63]

A támadási modell alapján egy kritikus információs infrastruktúra egy felhasználója nyilvános hálózati végponton keresztül kapcsolódódik a belső hálózathoz. A támadó ezt a kapcsolatot kihasználva vagy a jogosult felhasználót megszemélyesítve (pl. session hijacking) vagy annak számítógépére telepített rosszindulatú kód segítségével kapcsolódik a kritikus információs infrastruktúra WLAN hálózatához. A 48.ábra egy ilyen támadási útvonalat mutat be. Ez a támadási modell csak szándékosan hajtható végre.



48. ábra: Kritikus információs infrastruktúra támadása nyilvános hálózati végponthoz kapcsolódó infrastruktúra felhasználón keresztül

Forrás: saját szerkesztés

Jól látható, hogy a támadási útvonalak mennyire szerteágazóak. A nyilvános és gyengén védett végpontok a támadási útvonal célpontjai vagy kiindulópontjai lehetnek, és potenciális veszélyforrásai a kritikus információs infrastruktúrákat érhető támadásoknak.

2.6. Következtetések

Vizsgálataim és kutatásaim segítségével bebizonyítottam, hogy a vezeték nélküli hálózatok robbanásszerű elterjedése nem kerülte el a kritikus információs infrastruktúrákat sem. Számos kritikus információs infrastruktúrában a teljes hálózat szerves részét képezi a vezeték nélküli hálózat. A Budapesten végzett méréseim azt is bizonyítják, hogy ezekben az infrastruktúrákban az eszközök különböző hitelesítési és titkosítási protokollokat használnak. Az általam kiválasztott három kritikus infrastruktúrában (infokommunikációs ágazat, közlekedés ágazat és egészségügy ágazat) ezek a sajátosságok szintén megfigyelhetőek.

Az eredmények azt mutatták, hogy a közlekedés ágazathoz tartozó infrastruktúra vezeték nélküli hálózata homogén, erős hitelesítéssel és jelszóvédelemmel van ellátva, de SOHO eszközökből áll.

Az infokommunikációs technológiák ágazathoz tartozó infrastruktúra hálózata szerteágazó, szegmentált és nagy kiterjedésű. A nyílt végpontok beazonosíthatóak „Vendég" végpontként, remélhetően megfelelően leválasztva a teljes hálózatról, míg a hálózat többi eszköze ugyan nem egységes, de az eszközökhöz használható erős hitelesítéssel és jelszóvédelemmel működnek.

Az egészségügyi ágazathoz tartozó infrastruktúrában az eszközök és a konfigurációs beállítások sokaságát azonosítottam biztonsági problémaként. A vizsgálati eredményeim alapján megállapítottam, hogy erre a kritikus információs infrastruktúra ágazatra a SOHO és az Enterprise megoldások egyaránt jellemzőek. Ezen eszközök közt számos végpont nyílt hozzáférést tesz lehetővé, de a rendszerben szintén megtalálható még számos WEP titkosítással használt eszköz is. A vezeték nélküli hálózat ennek az infrastruktúrának potenciálisan sebezhető pontja. Véleményem szerint egy ilyen helyzetben mind a vezetékes mind pedig a vezeték nélküli hálózat teljes felülvizsgálata indokolt.

Elemzéseim azt a tényt is alátámasztották, hogy a világon egyre jobban elterjedő nyilvános vezeték nélküli végpontok hazánkban is nagy számban megtalálhatóak. Köszönhető ez az eszközök alacsony árának, és az egyszerű konfigurálhatóságnak. Ezek a végpontok kiindulópontjai lehettek és lehetnek több támadásnak is. Az általam detektált gyenge védelemmel ellátott (WEP), és a védelem nélküli (nyilvános) végpontok nagy száma aggodalomra ad okot. Ezt a problémát kezelni kell annak érdekében, hogy az ezeken keresztül indítható támadások száma csökkenthető legyen. A SOHO eszközök biztonságának növelése nem csak az eszköz üzemeltetője és felhasználója számára je-

lent nagyobb biztonságot, hanem ezzel csökkenthető a kritikus információs infrastruktúrákat fenyegető támadási útvonalak száma is.

A mérési eredményeim és a technológia ismeretek alapján felállítottam több olyan támadási útvonalat, amelyeken keresztült a kritikus információs infrastruktúrák ellen támadásokat lehet végrehajtani. Ezek az útvonalak és a mérési eredmények együtt azt bizonyítják, hogy egy vezetékes és vezeték nélküli vegyes infrastruktúrát akkor lehet maximálisan biztonságosan üzemeltetni, ha az a hálózat egységes, folyamatosan kontrollált, és megfelelően szegmentált részekből áll.

3. Fejezet
Vezeték nélküli hálózatok támadási és védelmi rendszertana

„A kritikus infrastruktúrák elleni információs veszélyeztetések, támadások nem különböznek az informatikai rendszerek elleni, már korábban jól ismert támadásoktól, hiszen a kritikus infrastruktúrák informatikai összetevői (önálló infrastruktúrák, vagy más infrastruktúrák részét képező összetevők) sem különböznek más informatikai rendszerektől, eszközöktől." [64 p. 98] A infrastruktúra vezetékes hálózatának eddig jól körülhatárolható és védhető határai kitolódtak a vezeték nélküli hálózati szegmenssel. A WLAN elleni támadások főként abban különböznek a vezetékes hálózati támadásoktól, hogy a támadónak nem szükséges fizikailag a hálózatra csatlakoznia, mert a vezeték nélküli hálózat hatósugarában bárhonnan elindíthatja a támadását.

A kritikus információs infrastruktúrákban alkalmazott vezeték nélküli hálózatok megfelelő védelmi módszerének kialakításához elengedhetetlennek tartom a támadások széleskörű vizsgálatát, ezért a kutatásaim során megvizsgáltam a CERT[60], a CEH[61], az IASTED[62], a Cisco és az információs műveletek ide vonatkozó szakirodalmait.

Véleményem szerint a kritikus információs infrastruktúrák WLAN hálózatai elleni támadások vizsgálatát az alábbi szempontok szerint célszerű elvégezni:

- a támadó személye;
- a támadó célja, motivációja;
- a támadás módszerei.

3.1 A támadó személye

Az Amerikai CERT szerint a támadó személye a következő lehet:

- hacker;
- kém;
- terrorista;
- belső munkatárs;
- hivatásos bűnöző;

[60] CERT - Computer Emergency Response Team
[61] CEH - Certified Ethical Hacking
[62] IASTED - International Association of Science and Technology for Development

- vandál;
- katonai erő. [65]

Kovács László megfogalmazásában *„A hacker olyan személy, aki internet segítségével hozzá tud férni védett adatokhoz a számítógépeken. Kezdetben külön fogalmat alkottak a hackerek, akik azért törtek fel rendszereket, weboldalakat, illetve programokat, hogy bizonyítsák azok gyenge pontjait, azonban ezeket a hiányosságokat a rendszergazdák tudomására hozták, azaz általában jóindulatúan jártak el. Ők voltak az úgynevezett fehérkalaposok, azaz a "white hat" csoport tagjai. Az ellentábort azok a fekete kalaposok, "black hat" alkották, akik sokszor rosszindulatból, vagy valamilyen haszonszerzés reményében hatoltak be egy-egy rendszerbe.”* [66] A hackerek előszeretettel támadják és használják a vezeték nélküli hálózatokat. Egy támadási lépéssorozatot részletező csoport a következő logót készítette oldalához.

49. ábra: Az eredeti vezeték nélküli hálózatot jelölő logo

Forrás: [67]

50. ábra: A módosított logo

Forrás: [68]

Kritikus infrastruktúrák esetén, ahol a nemzeti kritikus infrastruktúrák 80-90%-a független magánvállalkozások kezében van, a kém személyét inkább ipari, számítógépes kémként használom. [64 p. 100]

Haig Zsolt szerint *„Az illetéktelen felhasználók – adatlopók, számítógépes kémek – a hálózaton található biztonsági rendszerek hiányosságait, vagy a legális belépéshez szükséges kritikus információk jogosulatlan megszerzésével megnyílt lehetőségeket használják ki annak érdekében, hogy az adott helyen meglévő információt megszerezzék.”* [69 p. 5]

A terroristák két csoportba sorolhatók. *„Az első csoportba, azok a terrorista szervezetek tartoznak, amelyek a már említett célokra - propaganda, toborzás, adatszerzés - használják e rendszereket. A másik - sokkal veszélyesebb - csoportba azok a terroristák*

tartoznak, akik nemcsak ilyen úgynevezett "soft"[63] *tevékenységre kívánják használni a rendszereket, hanem azt, illetve azon keresztül rombolni vagy egyéb erőszakos, "hard"*[64] *cselekményeket is végre akarnak hajtani."* [66]

A vezeték nélküli hálózatokon keresztül a kritikus infrastruktúrákban egy ilyen csoport végre tud hajtani „soft" és „hard" típusú támadást is.

Számos támadás visszavezethető egy belső munkatársig. Ők akarva, vagy akaratlanul támadhatják, vagy segíthetnek támadáshoz más elkövetőket eszközeik, hozzáférési azonosítóik segítségével.

A vezeték nélküli hálózatok elleni támadás elkövetője lehet hivatásos bűnöző is. *„A hivatásos bűnöző, aki objektív gondolkodású, felelősségvállalásra alkalmas, gyakran jól képzett, aki szándékosan keresi a bűnelkövetésre nyíló alkalmat, aki ismeri az összes fontos fogást, aki tudatosan választja magának ezt az életformát és manőverezik azon."* [70 p. 16] A hivatásos bűnöző véleményem szerint nyereségvágyból követi el a támadást. Neki nincs politikai, vagy más indíttatása, pénzszerzés motiválhatja.

A vandál támadócsoport tagjai a vezeték nélküli infrastruktúrát csak rongálással, pusztítással tudják támadni. A kritikus infrastruktúrákban a kültéri hálózati hozzáférési pontok lehetnek veszélyben miattuk.

A katonai erővel történő támadás a másik féllel szembeni információs fölény megszerzése és megtartása érdekében lehetséges. Az infomációs fölény *„megszerzésének és megtartásának két azonos fontosságú oldala van, úgymint: kihasználni és megvédeni a saját információs képességeket, illetve gyengíteni az ellenség információs lehetőségeit. Mindezek érdekében adott szervezetek béke, válság és konfliktus időszakában információs műveleteket hajtanak végre."* [69 p. 1]

„Az információs műveletek alkotó- és kapcsolódó elemei a következők:

- *műveleti biztonság;*
- *katonai megtévesztés;*
- *pszichológiai műveletek;*
- *információs infrastruktúrák, vezetési objektumok fizikai pusztítása;*
- *elektronikai hadviselés;*

[63] „Az információs dimenzióban folytatott információs műveleti tevékenységek a különböző információs folyamatok, adatszerzés, adatfeldolgozás, kommunikáció, stb. elektronikus úton való, „lágy típusú" („Soft Kill") korlátozó hatású támadását jelenti annak érdekében, hogy a célpontokra való közvetlen pusztító, romboló fizikai ráhatás nélkül közvetlenül befolyásoljuk azokat"[128 p. 2]

[64] „A fizikai dimenzióban folytatott információs műveleti tevékenységek a különböző információs infrastruktúrák, infokommunikációs rendszerek elemei elleni fizikai, pusztító, ún. „kemény típusú" („Hard Kill",) támadásokat, illetve azok fizikai védelmét jelentik. "[128 p. 2]

- *számítógép–hálózati hadviselés;*
- *polgári–katonai együttműködés;*
- *tömegtájékoztatás."* [69 p. 2]

„*Az Észtország internethálózata ellen 2007. áprilisában és májusában folytatott összehangolt támadás szemléletesen bizonyította, hogy egy információtechnológiailag fejlett ország milyen veszélynek van kitéve az információs szférából érkező összehangolt támadások részéről."* [129 p. 68]

Haig Zsolt szerint a kritikus infrastruktúra információs támadói a következők lehetnek:

- belső munkatársak;
- számítógépes bűnözők;
- hackerek, crackerek[65];
- ipari kémek;
- terroristák (információs terrorizmus);
- reguláris erők (hírszerzés, katonai erők). [72]

Ez a felsorolás több pontban egyezik a CERT megállapításával, de nem tekinti potenciális támadónak a vandálokat.

Napjainkban az informatikai bűncselekmények egy részét fiatalkorúak követik el, akik több éves informatikai tapasztalattal rendelkeznek. Sokszor minden motiváció és cél nélkül próbálnak illegális tevékenységet végrehajtani a számítógépes hálózatokon. [73]

2012. augusztus 28-án egy dunaújvárosi 16 éves fiút vett őrizetbe a rendőrség, aki számos hazai informatikai bűncselekménnyel kapcsolatba hozható. Négy, eddig ismeretlen társával együtt behatoltak az Alkotmánybíróság honlapjára, és átírták az Alaptörvényt. Több ehhez hasonló támadás is kapcsolódik hozzájuk. A vizsgálat alatt azt nyilatkozták, hogy konkrét céljuk nem volt a támadásoknak, mindössze "jópofa heccnek gondolták". [74]

Kovács László szerint az informatikai támadások a cyber térben történnek. Ezek szereplői:

- hackerek;
- hacktivisták;
- számítógépes bűnözők;

[65] a hackerekkel ellentétben a crackerek célja a rendszerben a szándékos károkozás

- ipari kémek;
- belső és külső szakértők;
- terroristák. [66]

A szereplők között szerepelnek a hacktivisták. *„Rendszerint valamilyen politikai motivációval rendelkeznek. Számos olyan akciót hajthatnak végre, amelyek során valamilyen - számunkra fontos - ügy érdekében internetes oldalakat törnek fel, átalakítják azok kinézetét, adatokat lopnak el onnan, illetve akadályozhatják az oldal működését pl. virtuális ülősztrájkkal (flood vagy DoS támadással.) Számos esetben támogatnak olyan terrorista szervezeteket, amelyek céljai vagy akciói partikulárisan egybe esnek az övékével."* [66]

A belső és a külső szakemberek potenciális veszélyt jelenthetnek egy kritikus infrastruktúra informatikai rendszerére. Munkájuk rövidebb-hosszabb ideig tarthat az infrastruktúrában. Sokszor a munkavégzéshez magas hálózati hozzáférést kapnak, amelyet kihasználva támadhatják az infrastruktúrát, akár belülről is.

Összegezve a fentieket véleményem szerint a kritikus információs infrastruktúrák vezeték nélküli hálózatára a következő támadók jelentenek potenciális veszélyt:

- hacktivisták;
- számítógépes bűnözők;
- ipari kémek;
- belső és külső szakértők;
- terroristák;
- belső munkatársak;
- hackerek, crackerek;
- reguláris erők;
- fiatalkorú informatikusok.

A felsoroltak közül két támadócsoportot emelek ki. Ők a belső munkatársak és a belső és külső szakemberek. Ezek az esetleges támadók potenciális előnyben vannak a többi támadóval szemben. Ismerik az infrastruktúra sajátosságait, esetleg megfelelően magas szintű hálózati hozzáférésük van az informatikai rendszerhez, így ők akár belülről is támadhatják azt.

3.2 A támadó célja, motivációja

Az Amerikai CERT szerint a támadás motivációja a következő lehet egy informatikai hálózatban:

- kihívás;

- politikai előnyszerzés;
- gazdasági előnyszerzés;
- károkozás;
- hálózat megsemmisítése. [65]

Haig Zsolt szerint támadás célja lehet informatikai hálózatban:

- illetéktelen hozzáférés az információhoz (adatlopás);
- illetéktelen adatbevitel;
- rosszindulatú szoftverek bevitele;
- információs környezetszennyezés. [69]

Szabó Henrik szerint a számítógépes hálózatok elleni támadás célja:

- információk megszerzése (kémkedés);
- vagyoni haszonszerzés (jogosulatlan banki átutalás)
- vagyoni károkozás (adatok törlése);
- erkölcsi károkozás (honlap megváltoztatása). [75]

A támadások motivációi a következők lehetnek :

- információ megszerzése (személyes, üzleti, katonai, stb.) haszonszerzés vagy károkozás céljából;
- szolgáltatásokhoz való illetéktelen hozzáférés (pl. nyomtatni, filmeket letölteni);
- szolgáltatások megbénítása;
- rendszer feltörése;
- rosszindulatú program(ok) bejuttatása;
- szórakozás, versengés pl. egy weboldal feltöréséért;
- politikai okokból;
- kifejezetten bűnös céllal (szerencsére csak kevés). [76]

Véleményem szerint a kritikus információs infrastruktúrák vezeték nélküli hálózatának támadási célja a fent említettek mindegyike lehet:

- kihívás;
- politikai előnyszerzés;
- gazdasági előnyszerzés;
- károkozás;
- illetéktelen hozzáférés az információhoz (adatlopás);
- illetéktelen adatbevitel;
- rosszindulatú szoftverek bevitele;
- információs környezetszennyezés;

- információk megszerzése (kémkedés);
- vagyoni haszonszerzés (jogosulatlan banki átutalás);
- vagyoni károkozás (adatok törlése);
- erkölcsi károkozás (honlap megváltoztatása).

A felsorolt támadási célok mindegyike lehet a kritikus információs infrastruktúrában található vezeték nélküli hálózatok elleni támadás célja.

3.3 A támadások módszertanai

A kritikus információs infrastruktúra vezeték nélküli hálózatának támadási módszerei sértik az információ:

- bizalmasságát[66];
- sértetlenségét[67] ;
- rendelkezésre állását[68].

„Ezt a hármast szokás az angol rövidítések alapján „CIA" elvnek nevezni. Az informatikai biztonság kialakítása során a cél ezen három feltétel megvalósítása és meglétüknek folyamatos fenntartása." [77]

Alábbiakban a vizsgált szakirodalmak alapján ismertetem a vezeték nélküli hálózatok elleni támadások módszereit.

A CERT a támadások módszereit két nagy csoportra osztotta:

- passzív támadások: más néven „lexikonépítő" támadás, amely a forgalom figyelése és statisztikai vizsgálatok alapján történő dekódolást jelenti;
- aktív támadás: a hozzáférési pont kijátszásával a kód dekódolása a cél.

A támadások megvalósítását a következő eszközökkel látja megvalósíthatónak:

- közbeékelt támadás;
- MAC cím visszaélés;
- WEP, WPA kódszó törés. [78]

Ezek a módszerek és támadási fajták a vezeték nélküli hálózati támadások csak nagyon szűk szegmensét érintik.

Az IESTED és a Cisco szerint a támadásokat szintén két csoportra lehet osztani:

- passzív támadások;
    - lehallgatás;

[66] Confidentiality
[67] Integrity
[68] Availability

    - forgalomelemzés;
- aktív támadások;
    - szolgáltatás megtagadás;
    - középre állásos támadás (megszemélyesítés);
    - jogosultság kiterjesztés, lopás.

Az információs műveletek szemszögéből a vezeték nélküli hálózatok támadási kérdéseivel a számítógép-hálózati hadviselés és az elektronikai hadviselés foglakozik.

Az elektronikai hadviselés szerinti csoportosítás a következő:

- passzív támadások;
    - felfedés;
    - iránymérés;
    - lehallgatás;
- aktív támadások;
    - elektronikai zavarás;
    - elektronikai megtévesztés;
    - elektronikai pusztítás. [79 p. 42]

„A számítógép-hálózati hadviselés az alábbi tevékenységeket foglalja magába:

- számítógép-hálózati felderítés;
- számítógép-hálózati támadás;
- számítógép-hálózati védelem [69 p. 3]

A CEH az alábbi öt nagyobb csoportra osztotta a támadásokat:

- hozzáférés elleni támadások;
- bizalmasság elleni támadások;
- sértetlenség elleni támadások;
- hitelesítés elleni támadások;
- rendelkezésre állás elleni támadások.

E támadási módszerek részleteit az alábbi 8-12. táblázatok ismertetik.

8. táblázat: Hozzáférés elleni támadások

Támadások	Támadás leírása	Eszközök és módszerek
War driving	A vezeték nélküli hálózati eszközök felderítésére, beazonosítására irányuló támadás. A cél minél több végpont információjának meghatározása.	Airmon-ng, Inssider, KisMAC, NetStumbler, Vistumbler, WiFiFoFum
Hamis AP	A támadó célja egy módosított AP elhelyezése, beüzemelése a hálózatában, amellyel bármikor elérheti a hálózat erőforrásait.	Bármilyen hardveres vagy szoftveres AP
Ad-hoc csatlakozás	A támadó egy felderített nyitott hálózaton keresztül támad más állomásokat, vagy a hálózat más elemeit.	Vezeték nélküli hálózati kártya
MAC csere	A vezeték nélküli hálózati kártya MAC címének megváltoztatása. A támadó olyan nyitott hálózatba tud így behatolni, amely csak MAC szűrést végez.	MacChanger, SirMACsAlot, SMAC, Wellenreiter, wicontrol

Forrás: [80]

9. táblázat: Bizalmasság elleni támadások

Támadások	Támadás leírása	Eszközök és módszerek
Lehallgatás	A támadó a vezeték nélküli kommunikációt rögzíti, dekódolja, és ezzel potenciálisan érzékeny információhoz jut.	bsd-airtools, Ettercap, Kismet, Wireshark, smsniff
WEP törés	A támadó a lehallgatott adatcsomagokat rögzíti, kiértékeli és meghatározza a WEP kulcsot.	Aircrack-ng, airoway, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab, wesside
Evil Twin AP	A támadó egy az infrastruktúrában működő AP-nak adja ki magát	cqureAP, D-Link G200, HermesAP
AP adathalászat	Az Evil Twin AP-on keresztül web szervert üzemeltet a támadó a dolgozók bejelentkezési és más adatainak megszerzése céljából.	Airpwn, Airsnarf, Hotspotter, Karma, RGlueAP
Man in the Middle	A támadó az Evil Twin AP-on keresztül támadja az infrastruktúra eredeti AP-ját. A felhasználó a meghamisított AP-n keresztül kommunikál. A támadó a teljes hálózati kommunikációt rögzíteni tudja így.	dsniff, Ettercap-NG, sshmitm

Forrás: [80]

10. táblázat: Sértetlenség elleni támadások

Támadások	Támadás leírása	Eszközök és módszerek
802.11 Frame Injection	A támadó hamis 802.11-es keretekkel támadja a hálózatot.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet
802.11 Data visszajátszás	802.11 keretek rögzítése, és v	Adatfolyam rögzítő és visszajátszó alkalmazás
802.1X EAP visszajátszás	801.X EAP rögzítése egy későbbi visszajátszáshoz	Adatfolyam rögzítő és visszajátszó alkalmazás az AP és a kliens közé
802.1X RADIUS visszajátszás	801.X RADIUS rögzítése egy későbbi visszajátszáshoz	Adatfolyam rögzítő és visszajátszó alkalmazás az AP és az autentikációs szerver közé

Forrás: [80]

11. táblázat: Hitelesítés elleni támadások

Támadások	Támadás leírása	Eszközök és módszerek
Megosztott kulcs támadása	A támadó célja megszerezni a hálózat vendég, vagy más megosztott kulcsát találgatással, vagy jelszótöréssel.	WEP kódtörő alkalmazások
PSK támadása	A támadó az adatfolyam rögzítése után szótár alapú támadással fejti vissza a WPA/WPA2 PSK-t.	coWPAtty, genpmk, KisMAC, wpa_crack
Felhasználói név és jelszó lopása	A támadó rögzíti az adatfolyamot a hálózaton, majd visszafejti belőle például az email címeket és a hozzá tartozó jelszavakat.	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
VPN[69] azonosító támadása	A támadó célja megszerezni az alkalmazott VPN azonosítóját és jelszavát a vezeték nélküli hálózaton keresztül, hogy később támadásait távoli belépéssel is folytathassa.	ike_scan and ike_crack (IPsec), anger and THC-pptp-bruter (PPTP)

Forrás: [80]

[69] VPN – Virtual Private Network

12. táblázat: Rendelkezésre állás elleni támadások

Támadások	Támadás leírása	Eszközök és módszerek
AP támadása	Gyengén védett AP szoftveres támadása.	Vistumbler
AP lopás	Az AP fizikai eltulajdonítása.	A támadó keze
802.11 Beacon Flood	A támadó a Beacon Flood támadási módszer segítségével hamis AP-kat tud generálni.	FakeAP
802.11 Associate / Authenticate Flood	A támadó az Authenticate Flood támadással az infrastruktúra AP-it teszi működésképtelenné.	FATA-Jack, Macfld
802.11 Disassociation Flood	A támadó az infrastruktúra klienseinek az AP-hoz való kapcsolódását teszi lehetetlenné.	Aireplay, Airforge, MDK, void11, commercial WIPS
802.1X EAP-Start Flood	A támadó kellő számú EAP-Start Flood üzenettel lefoglalhatja az AP összes erőforrását.	QACafe, File2air, libradiate
802.1X EAP-Failure	A támadó az AP nevében hamis üzeneteket küld, ennek hatására a kliensek nem tudnak csatlakozni.	QACafe, File2air, libradiate

Forrás: [80]

Véleményem szerint a támadási módszertanok közül a CEH módszertana foglalja össze a támadásokat a legjobban, viszont ez a módszertan nem tartalmazza az elektronikai zavarást, és elektronikai pusztítást. Ezek a támadási fajták a kritikus információs infrastruktúra vezeték nélküli hálózatát teszik működésképtelenné.

További vizsgálataimat a CEH támadási módszertanára építem, kiegészítve a vezeték nélküli hálózatok elektronikai zavarásával és elektronikai pusztításával. Ez a támadási módszertan alkalmazható SOHO és Enterprise WLAN környezetre is.

3.4 A támadási módszerek vizsgálata

Kutatásom során célul tűztem ki a kritikus információs infrastruktúrákban alkalmazott vezeték nélküli hálózatok támadási és védelmi modelljeinek egymással való megfeleltetését. Ehhez összeállítottam egy vizsgálati környezetet, amelyben a támadások és védelmi módszerek egyes csoportjait tudom megvizsgálni. Ezekhez a vizsgálatokhoz kialakított környezetben a következő hardver elemek találhatók:

- hordozható számítógépek (a támadó és az áldozat szimulációjához);

- vezeték nélküli hálózati kártyák;
- antennák;
- GPS vevők;
- AP-ok;
- routerek;
- okostelefonok.

A szoftver környezet kialakításához Windows 7 operációs rendszert választottam a támadó és az áldozat hordozható eszközére egyaránt. A támadó szoftverek egy része linuxos környezetben futtatható, ezért a támadó gépre virtuális számítógép környezetet alakítottam ki, amelyben linux alapú Backtrack 5 keretrendszert használtam. Olyan vizsgálatokat végeztem el, amelyek ezekkel az eszközökkel és szoftver környezetben összeállíthatóak, és a leggyakoribb támadások közé tartoznak.[132]

A támadási módszerek vizsgálatát szakirodalmi leírások és saját mérések alapján végeztem.

Wardriving

A wardriving során a támadó célja, hogy behatoljon egy vezeték nélküli hálózatba és ott kihasználva a hálózat esetleges internet csatlakozását, ő maga ingyen internethez juthasson. Ehhez először keresni kell egy lehetőség szerint gyenge védelemmel ellátott vezeték nélküli hálózatot. Ezt általában egy gépkocsiban elhelyezett laptop segítségével teszi a támadó, és miután célt ért, leparkol és megkezdi a támadást. Innen ered az elnevezés.

A következő képen egy átlagos hardveres összeállítás látható.(51 ábra)

51. ábra: A wardriving elengedhetetlen eszközei

Forrás: [81]

Ez a típusú tevékenység speciális hardver és szoftver környezetet kíván. Hardver oldalról a következő eszközöket lehet használni:

- autó – ez a tipikus wardriving (vagy kerékpár – ebben az esetben a warbiking-ról beszélhetünk);
- hordozható számítógép – ami lehet laptop, kézi számítógép vagy okostelefon, amelyben van, vagy csatlakoztatható a csomagok lehallgatásához szükséges „monitor” módba kapcsolható WLAN hálózati kártya;
- WLAN antenna – erre akkor van szükség, ha nem elégszünk meg az eszközbe épített antenna vételi paramétereivel;
- globális helymeghatározó készülék (GPS) – a pontos helymeghatározáshoz.

A wardriving szoftveres oldalát két csoportra lehet bontani:

- a felderítésért felelős, valamint
- a kiértékelésért, megjelenítésért felelős programok.

A vezeték nélküli hálózatok felderítéséhez használt programok platform szerint szokták megkülönböztetni. Linux-os operációs rendszerekhez a következő programokat használják:

- Airsnort: adatfolyamot analizál;
- Airtraf: hálózati protokoll szkenner;
- Kismet: adatfolyamot analizál.

Microsoft Windows-os rendszerekben az alábbi programok alkalmazhatók:

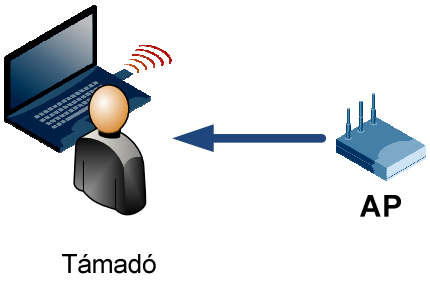
- Inssider: adatfolyamot analizál, megmutatja és tárolja a már megtalált hálózati elemeket;
- Aerosol: adatfolyamot analizál.

Kéziszámítógépes környezetben a következő programokat használhatók, amelyek képesek adatfolyamot analizálni, valamint megmutatni és tárolni a már megtalált hálózati elemeket:

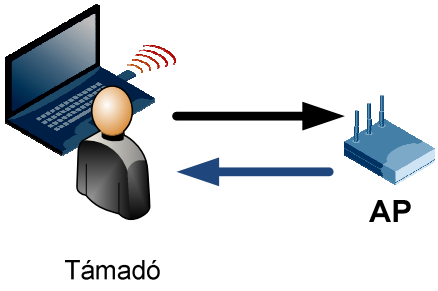
- Ministubler;
- Wififofum;
- Wifi Analyzer.

Az ilyen jellegű támadásokat két részre osztjuk: passzívra és aktívra. Passzív esetén a támadó csak olyan alkalmazásokat és eszközöket használ, amelyek az AP-k által kommunikált csomagokat logolják. (52.ábra) Aktív támadás esetén a támadó küld egy probe request-et az AP felé, ami válaszként egy probe response-t válaszol olyan információ

csomaggal, mely tartalmazza, hogy milyen titkosításokkal lehet hozzá csatlakozni. (53.ábra)



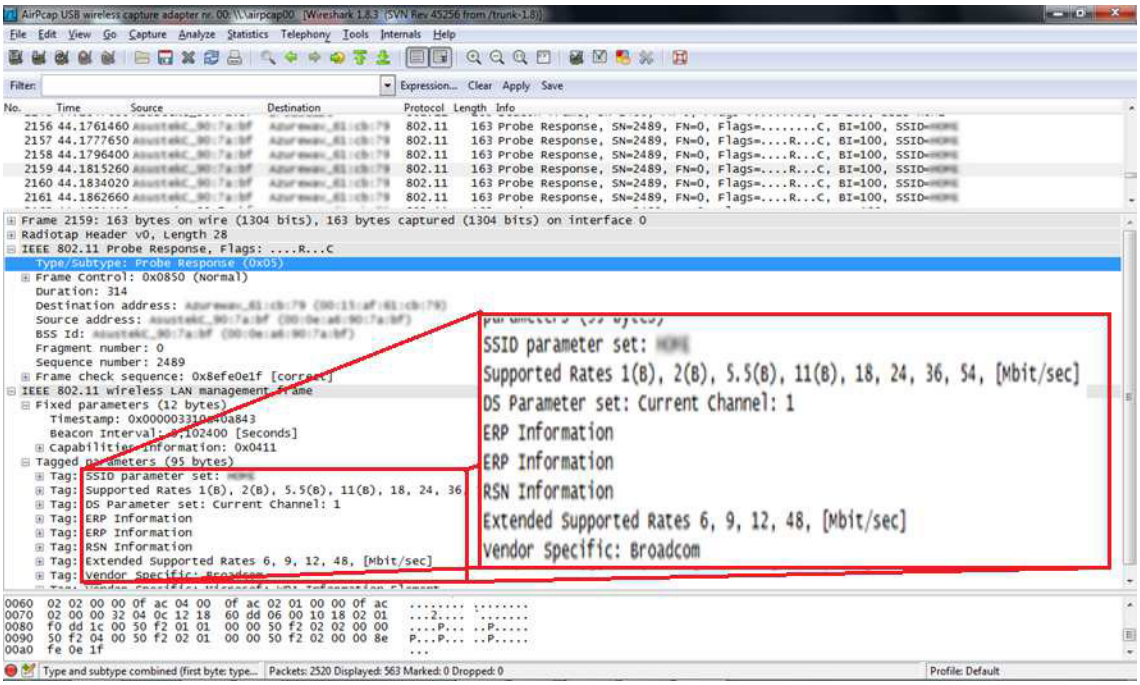
52. ábra: Passzív wardriving



53. ábra: Aktív wardriving

Forrás: saját szerkesztés

A passzív wardriving esetén a támadó rejtve maradhat. Egy ilyen támadást vizsgáltam a laptopon Wireshark alkalmazás, egy Airpcap kártya, egy ASUS router és egy mobiltelefon segítségével. A Wireshark alkalmazást monitor üzemmódba kapcsoltam és a mobiltelefonnal kapcsolatot létesítettem a routerrel. A laptopon rögzített csomagokból kiszűrtem a „probe response” csomagokat, amelyet a következő ábra mutat:

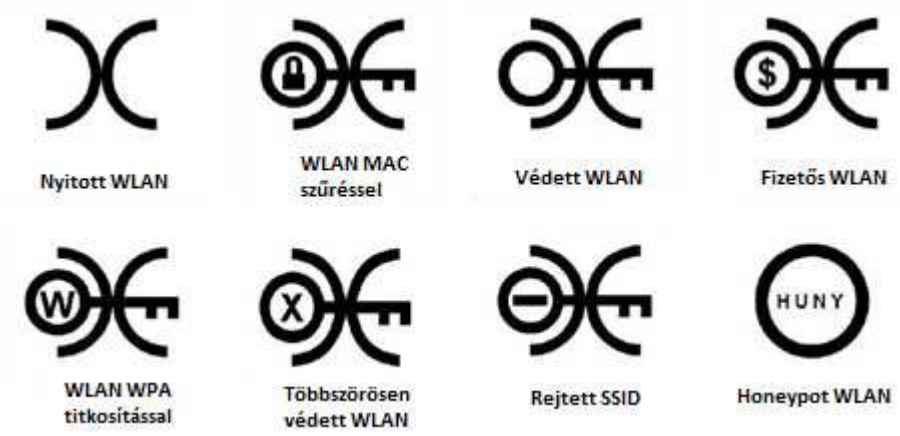


54. ábra: Probe response csomag

Forrás: saját szerkesztés

Az ábrán jól látszik az eszköz SSID, a támogatott sebességek és az aktuális csatornaszám.

A wardiving során a támadó felcsatlakozását egy nyitott hálózatra, piggybacking-nek nevezik.[82] A wardriving támadás „eredményeit” nagyon gyakran közzéteszik weboldalakon. Ezzel az esetlegesen nyitott, vagy gyengén védett hálózatok tulajdonosait plusz veszélynek teszik ki. A támadó különböző szimbólumokkal tudja jelezni az úton, vagy a falakon a már azonosított hálózatot. Ezeket az 55. ábra szemlélteti.



55. ábra: Hálózat tulajdonságára utaló szimbólumok

Forrás: [82]

MAC csere

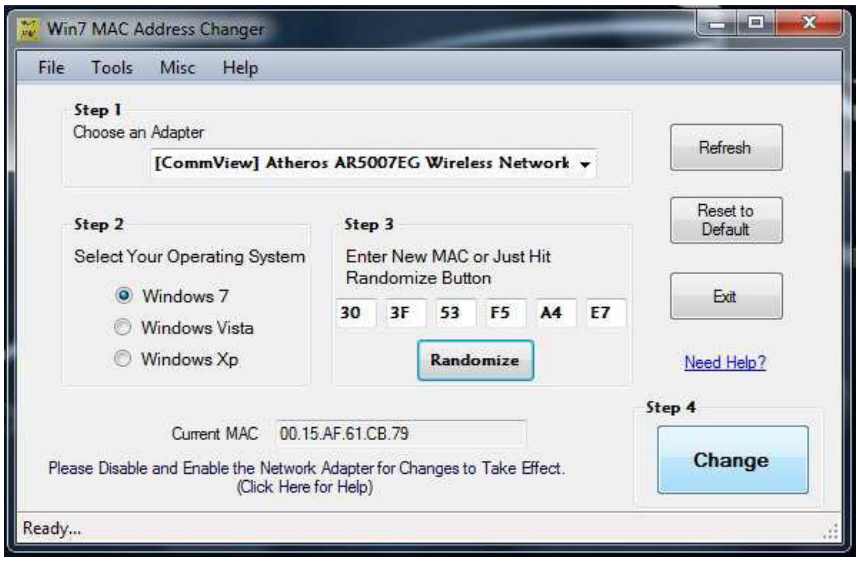
Egyes hálózatokban MAC lista alapú eszköz-beazonosítást is használnak. A támadó a vezeték nélküli kapcsolat monitorozásából ki tudja választani a hálózaton kommunikáló eszközök MAC címét. Amennyiben csak MAC szűrést alkalmaztak a hálózaton a támadónak csak annyi a teendője, hogy amikor egy általa rögzített eszközazonosító nem forgalmaz, annak a MAC címével bejelentkezhet a hálózatba. Minden hálózati eszköz kap egy ilyen azonosítót gyártáskor.

A támadás három fázisból áll:

1. hálózati forgalom monitorozása;
2. MAC csere (56.ábra);
3. hálózati támadás az új eszközazonosítóval.

A következő alkalmazásokkal valósítható meg a módosítás:

- MacChanger;
- SirMACsAlot;
- SMAC ;
- Wellenreiter;
- wicontrol. [80]



56. ábra: Windows alapú program MAC azonosító cseréjéhez

Forrás: saját szerkesztés

Önmagában ez a támadás csak gyengén védett hálózatokban hajtható végre, de olyan esetben ahol több védelmi kritérium is van, ez az egyik alkotóelem is lehet.

Rogue AP (Hamis AP)

Ez a típusú támadás általában a kritikus információs infrastruktúrákat sújtja. Számos infrastruktúra rendelkezik informatikai szabályzattal, ami kimondja, hogy vezetékes hálózati végpontokra csatlakoztatni semmilyen külső hálózati eszközt nem lehet, de a dolgozók sokszor nem tartják ezt be. Gyakran bele sem gondolnak abba, hogy ilyenkor egy rést nyithatnak az infrastruktúra hálózatában, amely egy könnyen támadható felületet biztosít. A dolgozók ezt tehetik szándékosan, egy támadó csoportot segítve, vagy nem szándékosan, esetleg önös érdekből.

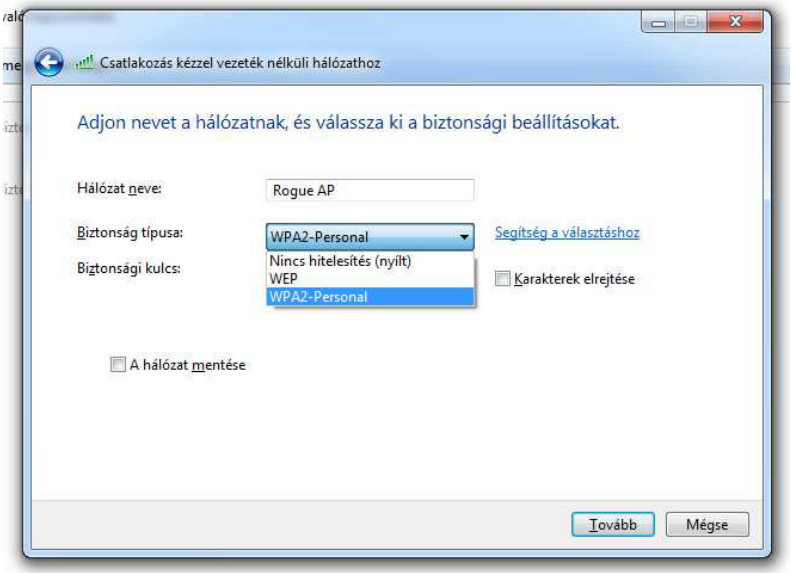
Számos olyan eszköz van amely az ilyen jellegű támadáshoz használható. Az 57. ábra egy olyan routert mutat, amely működhet AP-ként és routerként, esetleg repeaterként is. Kis mérete alkalmassá teszi arra, hogy könnyen elrejthető legyen.

Az ilyen jellegű támadásnak forrása lehet a Windows 7-es operációs rendszer is. Ez a rendszer képes arra, hogy szoftveres AP-ot hozzon létre rajta a felhasználó, hogy megossza dokumentumait, zenéit és nem utolsó sorban hálózati szolgáltatásait.

57. ábra: Mini router és AP egyben

Forrás:[84]

Ebbe az is beletartozik, hogy egy ilyen rosszul konfigurált beállítás mellett a munkahelyi hálózatunkon dolgozva egy újabb rést nyitunk a külvilág felé a hálózaton. Az AP beállításakor van ugyan lehetőség akár WPA2-es titkosítás beállítására is, de a lehetőségek között szerepel a nyitott hálózat létrehozásának lehetősége is.[85] Ezt mutatja a következő ábra is.



58. ábra: Windows 7 AP létrehozásának lépése

Forrás: saját szerkesztés

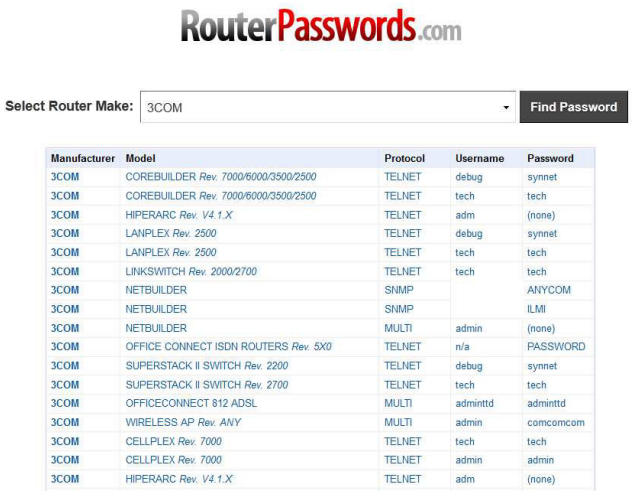
Ez a támadástípus sok más támadás kiindulópontjának tekinthető.

A rogue AP támadáshoz szervesen kapcsolódik a az Ad Hoc Associations támadás. A támadó csatlakozik egy rosszul vagy gyenge védelemmel ellátott eszközhöz – ami

lehet laptop vagy esetleg okostelefon –, amelyen aktív Ad Hoc kapcsolat van. Támadhatja magát az eszközt vagy az eszközön keresztül az infrastruktúrát.

AP támadása

A támadás célja közvetlenül az AP. Ezt akkor lehet végrehajtani, ha a hálózat gyengén védett, vagy nyitott. Sikeres autentikáció esetén az eszközünk IP címet kap és a kapcsolat felépül közte, és az AP között. Ekkor már a támadó része a hálózatnak, és megkezdheti a támadást. Ebben nagy segítségére van számos olyan weboldal, amely tartalmazza az AP eszközök alapbeállításait és jelszavait. Ezen adatok birtokában könnyű hozzáférést szerezni a beállításokhoz. A következő ábra egy ilyen weboldalt mutat be.



Manufacturer	Model	Protocol	Username	Password
3COM	COREBUILDER *Rev. 7000/6000/3500/2500*	TELNET	debug	synnet
3COM	COREBUILDER *Rev. 7000/6000/3500/2500*	TELNET	tech	tech
3COM	HIPERARC *Rev. V4.1.X*	TELNET	adm	(none)
3COM	LANPLEX *Rev. 2500*	TELNET	debug	synnet
3COM	LANPLEX *Rev. 2500*	TELNET	tech	tech
3COM	LINKSWITCH *Rev. 2000/2700*	TELNET	tech	tech
3COM	NETBUILDER	SNMP		ANYCOM
3COM	NETBUILDER	SNMP		ILMI
3COM	NETBUILDER	MULTI	admin	(none)
3COM	OFFICE CONNECT ISDN ROUTERS *Rev. 5X0*	TELNET	n/a	PASSWORD
3COM	SUPERSTACK II SWITCH *Rev. 2200*	TELNET	debug	synnet
3COM	SUPERSTACK II SWITCH *Rev. 2700*	TELNET	tech	tech
3COM	OFFICECONNECT 812 ADSL	MULTI	adminttd	adminttd
3COM	WIRELESS AP *Rev. ANY*	MULTI	admin	comcomcom
3COM	CELLPLEX *Rev. 7000*	TELNET	tech	tech
3COM	CELLPLEX *Rev. 7000*	TELNET	admin	admin
3COM	HIPERARC *Rev. V4.1.X*	TELNET	adm	(none)

59. ábra: AP és Router felhasználónév és jelszó lista

Forrás: [86]

A hozzáféréssel a támadó az eszköz minden beállításához hozzáfér. Esetleg port-ot tud nyitni a világháló felé későbbi támadásaihoz, monitorozni tudja az eszközöket. Akár kialakíthatja támadásai kiindulópontját is. Sajnos a lehetőségek kimeríthetetlenek egy ilyen támadás után.

Client mis-association

Ez nem tipikus direkt támadás, mivel feltételezi a támadó, hogy egy infrastruktúra közelében elhelyezkedő ingyenes nyitott AP-ra a vállalat dolgozója véletlenül felcsatlakozik. Ezt kihasználva megpróbál információkat kinyerni a dolgozó számítógépéből.

Unauthorized association (Illetéktelen hozzáférés)

Ezt a támadást akkor lehet végrehajtani, ha az infrastruktúra dolgozója – mint az előzőekben véletlenül – tudtán kívül egy közeli vezeték nélküli hálózatra csatlakozik, de eközben számítógépe a vezetékes hálózaton is rajta marad. Ekkor a támadó nem csak a gépet, hanem legrosszabb esetben a vállalat vagy infrastruktúra hálózati szegmensét is látja, ameddig a felhasználónak jogosultsága van.

Eavesdropping (Lehallgatás)

Könnyen és minimális szaktudással végrehajtható támadási forma. Mint a neve is utal rá a támadó lehallgatja és rögzíti a kommunikációt, majd a rögzített adatokat később kiértékeli. Elsősorban titkosítatlan hálózatok forgalmának lehallgatására használják, de az adatcsomagok gyűjtése más támadási formákhoz is felhasználható. Titkosítatlan kommunikáció esetén egyszerű programokkal megjeleníthetőek felhasználónevek, jelszavak, ftp elérések. Az ilyen jellegű támadás közvetlenül a felhasználónak okoz kárt, közvetve pedig a hálózat üzemeltetőjének. [87 p. 6]

Az eavesdropping eszközei széles választékban megtalálhatóak. Hordozható számítógépre alkalmasak a következő programok:

- bsd-airtools;
- Ettercap;
- Kismet;
- Wireshark.

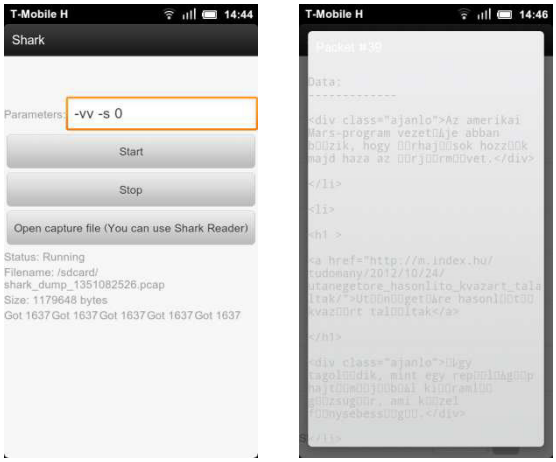
A támadások új lehetőségeit nyitotta meg az okostelefonok robbanásszerű elterjedése. A hordozható számítógépet a támadó nem minden esetben tudja elvinni például egy tárgyalásra, megbeszélésre úgy, hogy valakinek ne tűnjön fel mit végez a háttérben.
Az iPhone OS és Android operációs rendszerrel ellátott okostelefonokra is megjelentek lehallgató alkalmazások. Közismert az a tény, hogy az iPhone OS nagyon szigorú szabályokhoz köti a programok telepítését, ezért az ilyen lehallgató-programok elsősorban módosított operációs rendszerrel ellátott telefonokra telepíthetőek. A Pirni nevű alkalmazás ARP[70] hamisítás segítségével saját magán keresztül irányítja a forgalmat, és így lehetővé teszi a csomagok lehallgatását. [88] A 60. ábra ezt a folyamatot mutatja.

[70] Address Resolution Protocol - címfeloldási protokoll

Android operációs rendszerrel ellátott mobiltelefonokon a lehallgatás és az adatok kiértékelése egymás után végrehajtható a Shark alkalmazással. Ezt a vizsgálatot a teszt-környezetben végeztem el. A 61. ábra ezt mutatja.

60. ábra: Lehallgató alkalmazás Iphone-on

Forrás: [88]



61. ábra: Android lehallgató és csomagmegjelenítő alkalmazás

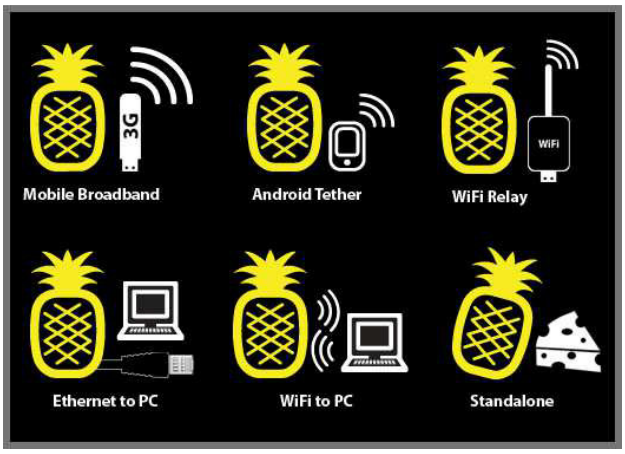
Forrás: saját szerkesztés

Evil Twin (Gonosz iker)

A támadó célja, hogy megszerezze egy már működő AP adatait, és a sajátját ugyanarra konfigurálva rávegye a felhasználót, hogy az ismeretlen eszközre csatlakozzon. Számos esetben ez történhet az eszközök fizikai cseréjével is. A kritikus információs infrastruktúrákban előfordulhat, hogy egy ilyen AP vagy router kerül a hálózatba, amely módosított firmware-rel rendelkezik. Ennek a támadásnak elsődleges célja a felhasználó adatainak, jelszavainak megszerzése.

Man in the Middle (Közbeékelődéses támadás)

Ez a támadás az Ewil Twin továbbfejlesztett változata. A támadó ebben az esetben nem elégszik meg azzal, hogy kiadja magát egy AP-nak, hanem az áldozat és az eredeti AP közé beékelődve a teljes adatfolyamot rögzíteni tudja. Ezt elvégezheti laptopjáról is, de módosított szoftverrel ellátott AP-t is használhat erre a feladatra.[90] A következő ábra egy ilyen módosított AP tulajdonságait mutatja, ahol az ananász képe a módosított firmware-rel ellátott támadóeszköz.



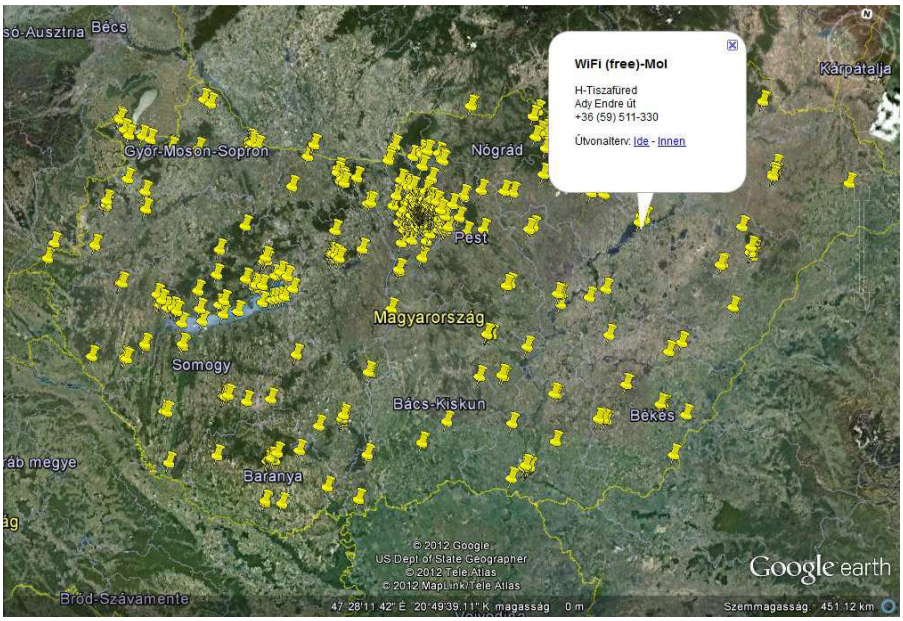
62. ábra: Módosított AP tulajdonságai közbeékelődéses támadáshoz és az AP közvetlenül egy mobil összeköttetéssel

Forrás:[91]

Ezt a támadást előszeretettel használják nyilvános helyeken, például szállodákban, kávézókban. Gyakori, hogy az első kapcsolatfelvételhez a támadó készít egy bejelentkező felületet, ahol az áldozatnak meg kell adnia személyes adatait, esetleg bankkártya információit is.

Honeypot (Mézes csupor AP)

A támadó célja, hogy egy olyan AP-ot konfiguráljon be, amely egy ismert nyilvános vezeték nélküli internetet is biztosító hely. Lehet ez étterem, kávézó, vagy akár egy bank is. Az AP neve fogja odavonzani az áldozatokat, akik a már megszokott szolgáltatást szeretnék igénybe venni. Az ilyen AP-k nyilvános kapcsolatot biztosítanak, így a rajtuk keresztül folyó kommunikáció titkosítatlan, egyszerű adatrögzítésből a személyes adatok, email címek jelszavak kinyerhetőek. A támadónak nem okoz nagy nehézséget AP nevet keresnie. Magyarországon egy 2012-es térkép-adatbázis alapján 764 nyilvános AP található, melynek eloszlását a következő ábra mutatja. [92] Az adatbázis adatai pontosan beazonosíthatóak cím vagy esetleg GPS koordináta alapján. [93]



63. ábra: Nyilvános WLAN-ok Magyarországon 2012-ben

Forrás: saját szerkesztés

Vezeték nélküli hálózat vírusok

A számítógépes vírusok napról-napra kifinomultabb megoldásokat alkalmaznak rendszereink megfertőzésére. Ez alól a vezeték nélküli hálózatok sem kivételek. A „MVW-Wifi" vírus több szempontból is különleges. Az egyik tulajdonsága, hogy többszörösen reprodukálja magát a megfertőzött gépen. E mellett az eszköz vezeték nélküli hálózati kapcsolatát kihasználva rácsatlakozik más vezeték nélküli hálózatokra és megfertőzi azokat. [94]

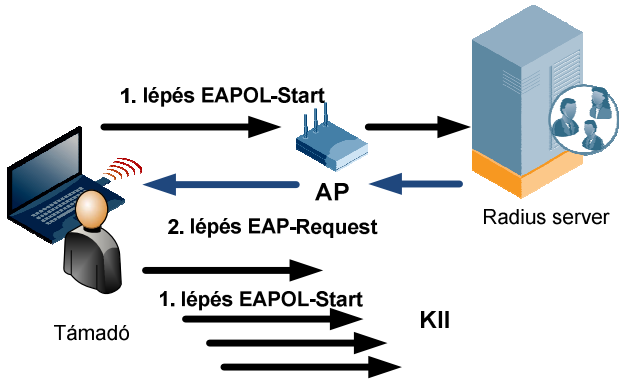
Association Flood

„Az AP-k nyilvántartják a hozzájuk kapcsolódott klienseket egy úgynevezett Association Táblázatban. A támadó hamisított csatlakozási üzenetekkel feltölti ezt a táblázatot, így az AP nem képes újabb klienseket fogadni." [118 p. 69]

EAPOL-Start támadás

„A támadás során a kliens egy EAPOL-Start üzenettel kezdi meg a folyamatot. Erre az AP egy válaszüzenetet generál (kihívás), amely során természetesen erőforrásokat különít el a hitelesítési folyamat számára. A kliens nem válaszol a kihívásra, így ezek a lefoglalt erőforrások csak egy időkorlát túllépése után szabadulnak fel. Kellő számú ha-

misított MAC című EAPOL-Start üzenet elküldésével a támadó lefoglalhatja az AP összes erőforrását." [118 p. 69] Ez a támadás Enterprise WLAN környezetben hajtható végre. Ezt mutatja a következő ábra:



64. ábra: EAPOL-Start támadás

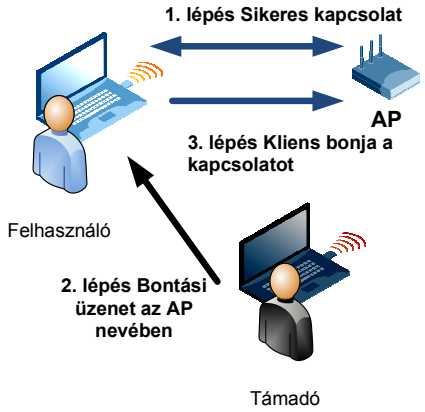
Forrás: saját szerkesztés

Authentication-Failure támadás

„A WLAN hálózatok kliensei egy hitelesítési folyamat végén kerülhetnek csatlakoztatott állapotba. A támadási módszer ennek a csatlakoztatott állapotnak a megszüntetésére irányul, és kétféleképpen is kivitelezhető. A támadó az AP nevében „Authentication Failed" üzeneteket küld a hálózat tagjai számára, emiatt a kliensek nem képesek csatlakozni az AP-hoz. A másik módszer fordított, ekkor a támadó a kliensek nevében hamis hitelesítési üzenetet küld az AP számára, amely erre válaszul kijelentkezteti a klienst." [118 p. 69]

Disassociation Flood

„A támadó első lépésben azonosítja az AP-hez csatlakozott klienseket, majd az AP nevében a kapcsolat bontására szolgáló üzeneteket kezd küldeni. A kliensek az üzenetet fogadva bontják a kapcsolatot, így a hálózat működése lehetetlenné válik." [118 p. 70] Ezt mutatja a következő ábra:



65. ábra: Disassociation Flood támadás

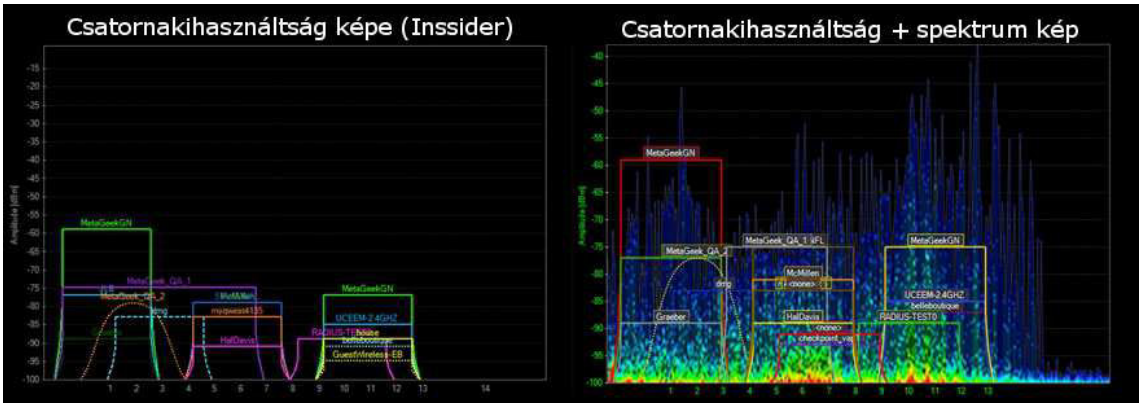
Forrás: saját szerkesztés

Zavarás

Zavarás szempontjából megkülönböztetünk nem szándékos és szándékos zavarást. A nem szándékos zavarást azok az elektronikai eszközök okozzák, amelyek a 2,4 GHz-es szabad sávban működnek. Ilyen eszközök:

- bébi figyelő;
- mikrohullámú sütő;
- modellező eszközök adó-vevő része;
- cordless telefon;
- hibásan működő WLAN eszköz.

A következő kép azt mutatja meg, hogy egy hagyományos csatornakihasználtságot vizsgáló alkalmazás és egy vele együtt működő spektrumanalizátor a mikrohullámú sütő zavarképét hogyan tudja megjeleníteni.



66. ábra: Csatornakihasználtság képe (bal), mikrohullámú sütő spektrumképe (jobb)

Forrás: [130]

A képen jól látható, hogy a mikrohullámú sütő a teljes 2,4 GHz-es WLAN spektrumot zavarja.

A szándékos zavaró eszközök célja a teljes rádiókommunikáció megakadályozása. Ezekből az eszközökből széles választék található akár kereskedelmi forgalomban is. A kis teljesítményű készülékektől egészen a katonai zavaró berendezésekig bezárólag minden megtalálható. A következő táblázat pár példával szemlélteti az eszközök paramétereit.

13. táblázat: WLAN zavaró berendezések

WLAN, bluetooth zavaró berendezés	**WLAN kamera zavaró berendezés**	**Nagyteljesítményű hordozható zavaró berendezés**
Zavarási frekvenciasáv: 850-2500 MHz Zavarási hatókör: 1-5 m Üzemidő: 2 óra	Zavarási frekvenciasáv: 900-2500 MHz Zavarási hatókör: 10-35 m Üzemidő: 2 óra	Zavarási frekvenciasáv: 400-2500 MHz Teljesítmény: 85 W Zavarási hatókör: ~ 200 m Üzemidő: 2 óra
		

Forrás: [131]

EMP[71] támadás

Az elektromágneses impulzus elvén működő fegyverek képesek irányított elektromágneses tér létrehozására, és célzottan az elektronikai eszközökben maradandó kárt tenni. Alkalmaznak egyszer használatos bombaként is ilyen fegyvert (E-bomba), de létezik többször felhasználható, nagy energiájú rádiófrekvenciás fegyver (HERF[72]) kialakításban is. Ezek a támadó eszközök hétköznapi alkatrészekből is elkészíthetőek, így nagy veszélyt jelentenek a kritikus információs infrastruktúra vezeték nélküli hálózatára. [11]

[71] EMP - electromagnetic pulse
[72] HERF - high-energy radio frequency weapons

3.5 Támadási módszertanok összegzése

A kritikus információs infrastruktúra vezeték nélküli hálózatának támadási lehetőségei szerteágazóak. Számos olyan támadási típus megtalálható, amely hétköznapi eszközökkel, minimális szaktudással végrehajtható. Ezek ellen a támadások ellen átfogó védelmi módszerekkel és eszközökkel lehet csak védekezni. A következő táblázatban összefoglalom az általam bemutatott támadásokat a támadói szaktudás szerint. A táblázatban az 1-es érték a kis szaktudást igénylő támadást fogja jelenteni, míg az 5-ös érték a nagy szaktudás igénylő támadást. Az értékeket a szakirodalom és saját mérési gyakorlat alapján vettem fel.

14. táblázat: Támadási módszertanok összefoglaló táblázata

Támadások	**Szaktudás**	**Támadások**	**Szaktudás**
Wardriving	2	Megosztott kulcs támadása	2
Hamis AP	1	PSK támadása	3
Ad-hoc csatlakozás	2	Felhasználói név és jelszó lopása	3
MAC csere	1	VPN azonosító támadása	4
Lehallgatás	2	AP lopás	1
WEP törés	2	802.11 Beacon Flood	3
802.1X EAP visszajátszás	5	802.11 Associate / Authenticate Flood	3
AP adathalászat	3	802.1X EAP-Failure	3
Man in the Middle	3	802.1X EAP-Start Flood	3
802.11 Frame Injection	3	802.11 Disassociation Flood	3
802.11 Data visszajátszás	5	802.1X RADIUS visszajátszás	5
Evil Twin AP	3	Zavarás	1
EMP	1	Honeypot	2
WLAN vírus	1	AP támadása	2

Forrás: saját szerkesztés

A 2. fejezetben vizsgált kritikus információs infrastruktúrák vezeték nélküli hálózatainak paraméterei alapján kijelenthetem, hogy az itt felsorolt támadások alkalmazhatóak a kritikus információs infrastruktúrák vezeték nélküli hálózatai ellen, szem előtt tartva a hálózat paramétereihez illeszthető támadásokat.

3.6 Védelmi módszerek a kritikus információs infrastruktúrák vezeték nélküli hálózataiban

3.6.1 A védelmi módszerek szakirodalmi osztályozása

A kritikus információs infrastruktúrák vezeték nélküli hálózatának védelmét és biztonságát hardveres és szoftveres megoldások alkalmazásával lehet megvalósítani. A cél minden esetben a támadások okozta kár csökkentése, megelőzése. A vezeték nélküli hálózatok és a hozzá kapcsolódó más szegmensek hatásos védelmét többszintű biztonsági rendszerrel célszerű megvalósítani. Ez a rendszer magába kell hogy foglalja a tűzfalakat, a behatolás- detektáló és megelőző megoldásokat valamint az átjáró alapú vírusvédelmi technológiákat. [95 p. 30] Véleményem szerint az általuk nyújtott védelmi megoldások egymást kiegészítik; hatékonyságukat együttes, integrált alkalmazásuk növeli. Ezen felül *„alapvető számítógép-hálózati biztonsági alapelveknek kell tekinteni, hogy*

- *a védelem ne kerüljön többe, mint a védendő információ, illetve, hogy*
- *a védelemnek olyannak kell lennie, hogy ellenálljon a feltörési, eltulajdonítási kísérleteknek addig, amíg a védendő információ értékes.”* [22 p. 140]

A számítógép-hálózatok védelmét aktív és passzív módszerekkel lehet megvalósítani.

A vezetékes hálózat passzív védelmi módszerei és eszközei az alábbiak:

- tűzfalak;
- vírusirtók;
- hozzáférés szabályozás;
- behatolás detektálás, megelőzés;
- eszközök fizikai védelme.

Az aktív védelem közé sorolhatók:

- a megelőző támadások;
- az ellentámadások;
- az aktív megtévesztés. [69 p. 7]

A vezeték nélküli hálózati szegmensben a felsorolt védelmi módszerek szintén jól alkalmazhatóak. Egy komplex vegyes hálózatban, azonban a vezeték nélküli hálózat sajátosságai miatt más módszerek használata is szükséges. Kutatásaim során megvizsgáltam a CERT, a CEH, az IASTED, a Cisco és az információs műveletek ide vonatkozó szakirodalmait.

A CEH a következő védelmi intézkedéseket javasolja a vezeték nélküli hálózatokban:

- MAC cím szűrés;
- SSID elrejtés;
- tűzfal használata;
- DHCP kikapcsolása;
- külső menedzselés tiltása;
- titkosítás használata;
- eszköz helyének megfelelő kiválasztása;
- plusz tűzfal beiktatása a vezeték nélküli és a vezetékes hálózat közé;
- a vezeték nélküli hálózat folyamatos monitorozása. [96]

A CERT javaslatai a következők:

- az AP körültekintő elhelyezése;
- a rádiójelek kiszivárgásának megakadályozása;
- titkosítás használata ;
- az SSID azonosító olyan megválasztása, hogy az ne utaljon a szervezetünkre;
- tűzfal beépítése a vezetékes és a vezeték nélküli hálózat közé;
- MAC cím szűrés;
- DHCP tiltása. [78 p. 118]

Az IESTED szerint a vezeték nélküli hálózat védelmében a következő módszereket javasolt végrehajtani:

- titkosítás engedélyezése;
- SSID tiltása;
- MAC cím szűrése;
- eszköz programjának folyamatos frissítése;
- bonyolult jelszavak használata az eszközökhöz;
- monitorozás;
- DHCP kikapcsolása;
- üresjárati időben az eszköz kikapcsolása. [97]

A Cisco mint eszközgyártó a vezeték nélküli hálózat védelmének módszerei közül a következőket tartja fontosnak:

- eszközök programjainak frissítése;
- titkosítás használata;
- folyamatos monitorozás. [98]

Az információs műveletek szempontjából a számítógép-hálózati hadviselés védelmi eszközei a következőek:

- passzív védelem;
  - tűzfalak;
  - hozzáférés szabályozás;
  - behatolás detektálás és adaptív válaszlépések;
  - vírusírtók;
- aktív védelem;
  - megelőző támadások;
  - ellentámadások;
  - aktív megtévesztés. [69]

Az információs műveleteken belül még az elektronikai hadviselés kapcsán a következő vezeték nélküli hálózat védelmi módszerekről beszélhetünk:

- titkosítás;
- teljesítmény, frekvencia megfelelő kiválasztása;
- EMP védelem (Faraday-kalitka);
- megtévesztés;
- zavarás.

A vizsgált módszertanok alapján a kritikus információs infrastruktúrákban alkalmazott vezeték nélküli hálózatok számára a következő védelmi módszereket javaslom:

- passzív védelem:
  - a hálózat adottságaihoz igazítható erős hitelesítés és titkosítás;
  - az SSID nevének megfelelő kiválasztása (ne utaljon az infrastruktúrára);
  - antennák megfelelő méretezése;
  - folyamatos monitorozás;
  - frissítések nyomon követése;
  - működési idő szabályozása;
  - eszközök megfelelő helyének kiválasztása;
  - MAC cím szűrése;

- tűzfal használata a vezeték nélküli hálózati szegmensen is.

- aktív védelem:
  - ellentámadás;
  - aktív megtévesztés.

Ezeket a védelmi módszereket egymásra épülve kell beépíteni a vezeték nélküli hálózatok tervezése illetve üzemeltetése során. Ily módon - még ha az egyik biztonsági intézkedés gyengének vagy hibásnak bizonyulna is - ott van még a védelmi stratégia számos más rétege, amely továbbra is védi a hálózati szegmenset. Az a fő cél, hogy egyetlen hiba se okozhassa a teljes védelmi rendszer összeomlását.

3.6.2 A kritikus információs infrastruktúrák vezeték nélküli hálózatainak védelmi módszertana

Az ismertetett védelmi módszerek önmagukban nem hatásosak. Egy megfelelő szabályzó rendszer kell az infrastruktúra vezeték nélküli hálózatának üzemeltetéséhez. A szabályzatok segítségével a védelmi módszerek komplex biztonsági rendszert alkotnak. A kritikus információs infrastruktúra vezeték nélküli hálózatának üzemeltetése során a következő általam megalkotott védelmi módszertant javaslom alkalmazni.

A vezeték nélküli technológia megfelelő használata

A vezeték nélküli technológia megfelelő használata körvonalazza a WLAN környezet helyes és helytelen használatát, valamint a megfelelőség hiányának lehetséges következményeit. A felhasználóval alá kell íratni egy végfelhasználói megállapodást, amely bizonyítja, hogy ismerik és megértik a vezeték nélküli technológia használatára vonatkozó irányelveket. A dokumentációban pontosan meg kell határozni, hogy milyen szolgáltatások és alkalmazások engedélyezettek a WLAN hálózaton. [94]

Engedélyezett WLAN eszköz telepítések

Az infrastruktúrán belül meg kell határozni, hogy a szervezet mely egysége jogosult kizárólagosan WLAN szolgáltatások nyújtására. Ily módon megakadályozhatjuk, hogy a felhasználók vagy csoportok úgy érezzék, a WLAN-ok használatának engedélyezése következtében ők saját maguk is biztosíthatják a hozzáférést, ha az ott nem áll rendelkezésre, ahol ők szeretnék. Célszerű egy olyan közlemény közzététele, amely leírja, hogy

mi lesz a sorsa a felhasználó által engedély nélkül telepített saját WLAN készülékeknek.[31]

Engedélyezett hardver

Amennyiben a kritikus információs infrastruktúra WLAN-ban egy bizonyos, konkrét hardver alkalmazására van szükség, határozzunk meg hozzá új felhasználási, alkalmazási irányelveket.

Egységes WLAN architektúra

A kritikus információs infrastruktúrában ki kell dolgozni egy általános architektúrát a WLAN alkalmazások számára. Ily módon szabványosítható a több telephelyes WLAN alkalmazások hardver felépítése és konfigurációja, valamint lehetővé válik a WLAN kiszolgáló eszközök egységesítése. A hozzáférési pontok fizikai biztonságát, és a kapcsolódó infrastruktúrát is az infrastruktúra részének kell tekinteni.

Konfiguráció menedzsment

Az infrastruktúra WLAN szegmensén ki kell alakítani egy központosított konfigurációmenedzselést végző rendszert, amely az infrastruktúra összes vezeték nélküli kiszolgáló hálózati eszközét konfigurálhatja. A rendszernek dokumentálnia kell a változásokat és az esetleges felmerülő hibákat. [99, 100]

A WLAN kliens biztonsága

Minden WLAN kliensnek szánt munkaállomást kellően biztonságossá kell tenni. Egy rosszul konfigurált kliens is támadási felület lehet. A biztonságos üzemeltetéshez a következő lépéseket kell megvalósítani:

- megfelelő hibajavítási szint fenntartása;
- vírusirtó alkalmazás telepítése, futtatása és rendszeres frissítése;
- egyéni tűzfal telepítése és aktiválása a vezeték nélküli kapcsolaton is;
- megfelelő rendszer-biztonsági beállítások elvégzése, ellenörzése.

Naprakész hitelesítés és titkosítás

A titkosítás a védelemnek az a területe, amire a legtöbb figyelem összpontosul a vezeték nélküli technológiával kapcsolatban. A titkosító és hitelesítő rendszerek kiválasztása az

egyik legfontosabb döntés a kritikus információs infrastruktúra WLAN tervezése során. Az alábbi irányelvek betartása javasolt:

- központosított hitelesítést használó működési elvet válasszunk, ha van rá lehetőség;
- használjuk az AES titkosítást WPA2 protokollal, ha lehetséges;
- PKI-t[73] (nyílt kulcsú infrastruktúrát) támogató működési elvet válasszunk, ha rendelkezünk az ehhez szükséges infrastruktúrával;
- kerüljük a már feltört (megfejtett) hitelesítési protokollok használatát;
- olyan rendszert használjunk, ami a lehetőségek szerint támogatja a kölcsönös hitelesítést.[50]

Alapértelmezett konfigurációs beállítások megváltoztatása

A kereskedelmi forgalomban elérhető valamennyi hozzáférési pont esetében az előzetes konfiguráció az SSID és az adminisztratív jelszavak valamilyen alapértelmezett beállításaival történik, amelyeket szintén jól ismernek a támadók. [31]

A WLAN szegmensen belül ne használjuk az infrastruktúrára utaló adatot az SSID azonosítóban. Számos WLAN eszköz biztosít lehetőséget az SSID elrejtésére. Ebben az esetben az egyszerű vezeték nélküli alkalmazások rejtett hálózatként jelenítik meg az eszközt, ami egy hamis védelem-érzetet kelthet. A támadó szoftverek nagy része a rejtett hálózatok SSID-jét is azonosítani tudja.

Alapértelmezett jelszavak megváltoztatása

A kereskedelmi forgalomban elérhető valamennyi hozzáférési pont előzetes konfigurálása alapértelmezett jelszóval történik. Az alapértelmezett jelszavakat jól ismerik a támadók, ami megkönnyíti számukra a hálózat elleni támadásokat. Ezért javaslom minden esetben az alapértelmezett jelszavak megváltoztatását, és központosított jelszókezelését.[31]

Alkalmazottak oktatása

A kritikus információs infrastruktúrán belül biztosítani kell a végfelhasználók megfelelő képzését a vezeték nélküli hozzáférés helyes és helytelen használatáról. A képzés során

[73] PKI - Public-Key Infrastructure

is támasszuk alá a személyi WLAN használatával kapcsolatos infrastruktúra irányelveket.

Új WLAN eszközök konfigurálása

A kritikus információs infrastruktúrán belül új WLAN végpont beüzemelését minden esetben egy szeparált hálózati szegmensen végezzük. Erre azért van szükség, mert így kizárható annak a lehetősége, hogy valaki az alapértelmezett konfiguráció ismeretére támaszkodva intézzen támadást az adott eszköz ellen.

Használaton kívüli menedzselési interfész letiltása

Valamennyi Enterprise kategóriájú hozzáférési pontot többféle menedzselési lehetőséggel szállítanak. Az eszközmenedzselésre aktívan nem használt valamennyi interfészt tiltsuk le, mivel azok adott esetben támadási útvonallá válhatnak.

Naplózás és monitorozás

A legtöbb Enterprise szintű hálózat már rendelkezik olyan mechanizmussal, ami lehetővé teszi a hálózati berendezéseknek mind a távoli naplózását, mind pedig a monitorozását. A hálózat állapotának valós idejű nyomon követése figyelmeztethet minket a WLAN-on előforduló problémákra, de sokszor szükség van az elmúlt eseményekről készült naplóbejegyzésekre is ahhoz, hogy például támadási mintákat rekonstruáljunk. [31]

Antennák megfelelő méretezése

A WLAN eszközök telepítésekor a tervezők figyelembe veszik az épület adottságait, paramétereit és a lefedni kívánt területet. Ennek megfelelően választják ki a hálózati végpontokat. A hálózati végpontokra a következő antennatípusok csatlakoztathatóak:

- omni;
  - dipólus;
  - co-linear;
- irányított;
  - panel, patch;
  - helix;
  - Yagi;

- parabola. [101]

A megvalósítás célja, hogy az eszközök és antennák segítségével az infrastruktúrában a legjobban behatárolt, de optimálisan a legmagasabb sávszélesség legyen a kívánt helyeken. Tervezés és kivitelezés után a WLAN hőtérkép segítségével lehet leellenőrizni a rádiós lefedettséget.

2012-ben a Londoni olimpián számos legális és illegális vezeték nélküli végpontot üzemeltettek az olimpia területén. Ezek beazonosítása, elhelyezkedése és esetleges lekapcsolása óriási problémát jelentett. A következő kép egy mobil egységgel felszerelt munkatársat ábrázol munka közben.

67. ábra: Engedély nélküli WLAN hozzáférési pontok beazonosítása a 2012-es Londoni olimpián

Forrás: [102]

Vezeték nélküli behatolás érzékelő / megelőző rendszerek alkalmazása

A kritikus információs infrastruktúra vezetékes hálózat védelmi megoldásai (tűzfal, vírusvédelem, vezetékes behatolás detektáló rendszer, VPN) nem biztosítanak kellő védelmet a komplex vegyes hálózatok biztonságos üzemeltetéséhez. Azt a tényt figyelembe véve, hogy a vezeték nélküli végpontok száma napról-napra nő, a kritikus infrastruktúrákban üzemeltetett vezeték nélküli eszközökre és végpontokra potenciálisan több támadási eszköz jut. [103]

A kritikus infrastruktúrák vezetékes hálózatának védelme a legtöbb esetben egy jól definiált szegmensre koncentrálódott, ami az infrastruktúrába bejövő külső hálózati kapcsolat volt. A kialakítás lehetővé tette, hogy a bejövő és kimenő adatforgalmat a beérkezés helyén a hálózati szabályoknak megfelelően jogosultság és más szempontok

alapján átvizsgálják, a veszélyes adatforgalmat blokkolják. Erre a legmegfelelőbb eszközök a tűzfallal és az IDS[74] és IPS[75] rendszerrel kiegészített megoldások. [103]

A vezeték nélküli hálózatok esetén a fent említett védelmi rendszer nem elég hatékony. A rádióhullámokat nem állítja meg az épület fala, a vezetékes hálózat eddig jól körülhatárolható és védhető határai kitolódtak és elmosódtak. A vezeték nélküli hálózatot az infrastruktúrával szemközti étteremből, parkoló autóból vagy gyalogosan is lehet támadni.

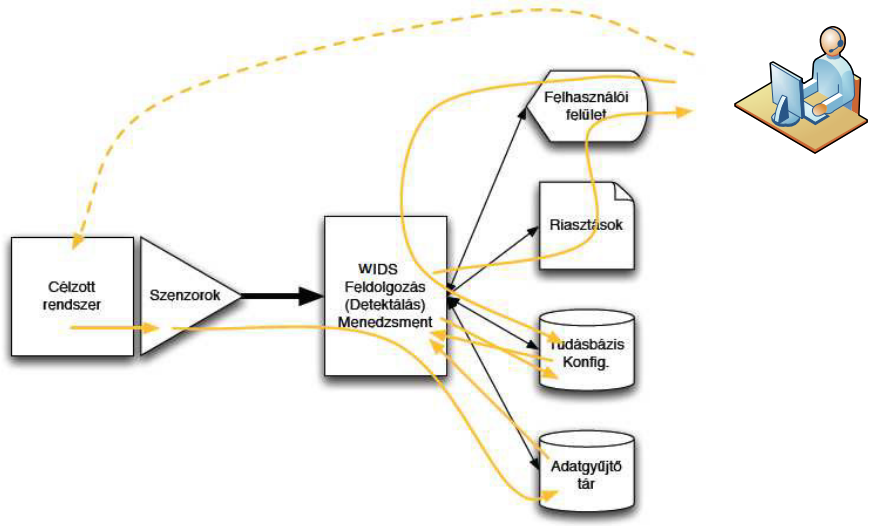
A vezeték nélküli hálózatok védelmének legerősebb bástyái a WIDS[76] és a WIPS[77] rendszerek. A vezeték nélküli hálózati csomópontokban elhelyezkedő rádiós vezérlő egységek WIDS funkciója nem más, mint egy mintát kereső programszál, amely különböző támadási típus beazonosítását tudja elvégezni. Valamennyi rádiós csomóponton áthaladó adatforgalmat bevizsgál. Ennek segítségével olyan támadásokat rögzít, amelyek a kiértékelés után a későbbiekben kizárhatóak lesznek. A módszerrel beazonosíthatóak a nem megengedett adatkeret fajták és a nemkívánatos AP-ok is. [103]

A felfedett potenciális veszélyforrások a hálózat adminisztrátorához kerülnek továbbításra. A felderített hibák száma alapján valamint az adminisztrátori beavatkozás szükségessége miatt az WIDS csak kisebb méretű kritikus információs infrastruktúrákban alkalmazható biztonságosan. A 68. ábra egy WIDS rendszer szerkezeti felépítését mutatja.

A 68. ábrán látható útvonalak az esetleges támadások és a kiértékelések folyamatát mutatják.

A WIPS rendszer abban különbözik a WIDS rendszertől, hogy nem csak a támadási típusok mintázatát figyeli, hanem protokoll analízist is végez, így két független elemző módszerrel vizsgálja a hálózati forgalmat. Különbség még az is, hogy a WIPS dedikált szenzorokat igényel, ami lehet az AP-be építve vagy önálló rádiófrekvenciás egység.

[74] IDS - Intrusion Detection System
[75] IPS - Intrusion Prevention System
[76] WIDS - Wireless Intrusion Detection System
[77] WIDS - Wireless Intrusion Prevention System



68. ábra: WIDS rendszer felépítése

Forrás: [104]

Nagy különbség a két megoldás között, hogy a WIPS a detektálás helyett sokkal aktívabb részt vállal a veszély elhárításában: a felfedett idegen eszközt azonnal kizárja a hálózatból. [103]

Radius szerver biztonság

Ha a hitelesítési infrastruktúránk Radius (távoli hitelesítést lehetővé tevő) szervert tartalmaz, akkor az alábbi biztonsági kérdésekre kell figyelnünk:

- ne használjuk ugyanazt a Radius osztott titkos kulcsot a hálózat valamennyi készülékéhez, inkább készülékenként, vagy legalább készülékcsoportonként állítsuk be a titkos kulcsokat;
- megfelelően hosszú, osztott titkos kulcsot használjunk a Radius szerverhez;
- gondoskodjunk arról, hogy csak a használatban levő hitelesítési típusokat engedélyezzék a Radius szerveren, ami csökkenti a közbeékelődéses támadások veszélyét. [105]

Szisztematikusan végezzük el a WLAN biztonsági szempontból történő kiértékelését

Ciklikusan ellenőrizzük a WLAN konfigurációit és biztonsági mechanizmusait. Tartsunk lépést a WLAN-ok hitelesítésére és engedélyezésére szolgáló rendszerek fejlődé-

sével, és helyettesítsük újakkal a már feltört rendszereket. Ennek egyik módszere a behatolás vizsgálat.

Az általam elkészített védelmi módszertant a kritikus információs infrastruktúra üzemeltetői számára a vezeték nélküli hálózat védelmének minimum követelményének ajánlom. A védelmi módszertan elősegítheti a meglévő hálózat biztonságának növelését, ami a támadhatóság kockázatának csökkentését vonja maga után. A módszertan illeszkedik a kritikus információs infrastruktúrákban alkalmazott IT biztonságra ill. üzemeltetésre vonatkozó ajánlásokkal.

3.7 Támadási módszerek és védelmi kontrollok egymásnak való megfeleltetése

Kutatásom során fontosnak tartottam a kritikus információs infrastruktúra vezeték nélküli hálózatait fenyegető támadások és védelmi megoldások rendszerezését. Véleményem szerint ez a kutatási cél akkor teljesül, ha a vezeték nélküli hálózatok támadási típusait az alkalmazható védelmi kontrolokkal egymásnak megfeleltetem. Ezt a megfeleltetést tartalmazza a 15. táblázat.

A támadási módszerek és védelmi kontrollok egymásnak való megfeleltetését a szakirodalmak és saját több éves informatikai tapasztalataim alapján állítottam össze. Ezzel az egymásnak való megfeleltetéssel a kritikus információs infrastruktúra üzemeltetők a vezeték nélküli hálózatukat fenyegető támadások kivédésére tudnak felkészülni.

15. táblázat: A vezeték nélküli hálózatok elleni támadások és az alkalmazható védelmi kontrollok egymásnak való megfeleltetése

Támadások fajtája	**Védelmi kontroll**
Wardriving	antennák méretezése, működési idő szabályozása
Hamis AP	tűzfal, MAC cím szűrése, folyamatos monitorozás
Ad-hoc csatlakozás	tűzfal, folyamatos monitorozás
Lehallgatás	SSID megfelelő kiválasztása, erős titkosítás, hitelesítés
WEP törés	erős titkosítás, hitelesítés
Evil Twin AP	folyamatos monitorozás, ellentámadás
AP adathalászat	folyamatos monitorozás, aktív megtévesztés
Man in the Middle	erős titkosítás, hitelesítés
802.11 Frame Injection	folyamatos monitorozás, ellentámadás
802.11 Data visszajátszás	működési idő szabályozása, erős titkosítás, hitelesítés
802.1X EAP visszajátszás	működési idő szabályozása, erős titkosítás, hitelesítés
802.1X RADIUS visszajátszás	működési idő szabályozása, erős titkosítás, hitelesítés
Megosztott kulcs támadása	erős titkosítás, hitelesítés, aktív megtévesztés
PSK támadása	erős titkosítás, hitelesítés, aktív megtévesztés
Felhasználói név és jelszó lopása	MAC cím szűrése, folyamatos monitorozás, ellentámadás
VPN azonosító támadása	MAC cím szűrése, folyamatos monitorozás, ellentámadás
AP lopás	AP fizikai izolációja
802.11 Beacon Flood	folyamatos monitorozás, ellentámadás
802.11 Associate / Authenticate Flood	folyamatos monitorozás, ellentámadás
802.11 Disassociation Flood	folyamatos monitorozás, ellentámadás
802.1X EAP-Start Flood	folyamatos monitorozás, ellentámadás
802.1X EAP-Failure	folyamatos monitorozás, ellentámadás
Zavarás	antennák megfelelő méretezése, folyamatos monitorozás
EMP	Faraday-kalitka
Honeypot	erős titkosítás, hitelesítés
AP támadása	tűzfal, MAC cím szűrése, folyamatos monitorozás
WLAN vírus	folyamatos monitorozás, ellentámadás

Forrás: saját szerkesztés

3.8 Behatolás vizsgálati módszertan mobiltelefonra

A kritikus információs infrastruktúrák vezeték nélküli hálózatainak zártságát biztosítani tudjuk a már ismertetett WIDS és WIPS rendszerekkel. Abban az esetben ha nem áll rendelkezésre ilyen rendszer, más vizsgálatokkal kell meggyőződni rendszerünk zártságáról. Az egyik ilyen módszer a behatolás tesztelése (penetration testing). A tesztelés nem tudja garantálni, hogy nem lehet sikeresen támadni a rendszert, de eredményeinek betartásával csökkenhet ennek a valószínűsége. [107]

A vezeték nélküli hálózatot fenyegethetik olyan illetéktelen és több esetben névtelen próbálkozások, amelyek a hálózati infrastruktúrához akarnak hozzáférni. A behatolás tesztelés a támadó szemszögéből vizsgálja a rendszert, biztosítva hogy a tesztelés feltételei valóságosak legyenek. Az ilyen folyamat egy ellenőrzött próbálkozás egy infrastruktúra hálózati védelmének áttörésére, gyenge pontjainak feltárására. A vizsgálatot végző olyan eszközöket, hardver és szoftver környezetet használhat, amelyet egy éles támadás során egy támadó is megtehet.

„Behatolás tesztelést különböző célokból lehet végezni, illetve végeztetni:

- a technikai rendszerek biztonságának fejlesztése érdekében;
- a sebezhetőségek azonosítására;
- az IT biztonság külső fél általi megerősítése (igazolása) céljából;
- a szervezeti és személyzeti infrastruktúra biztonságának javítása érdekében.” [106 p. 11]

Az behatolási teszt eredménye több kell legyen, mint a létező sebezhetőségek felsorolása, megoldási javaslattal is kell szolgálnia.

A vizsgálat során a következő kérdésekre kerestem a választ:

- Milyen károkat tud okozni egy külső támadó, aki nem rendelkezik semmilyen információval az infrastruktúra informatikai rendszeréről?
- Milyen károkat tud okozni egy volt munkatárs, alkalmazott, aki ismeri a belső infrastruktúrát?
- Mennyire működik hatékonyan az informatikai biztonsági és védelmi rendszer egy támadás alatt? [107]

Ezekre a kérdésekre egy átfogó vizsgálat adhat csak választ, amelyet az infrastruktúra üzemeltetőivel minden esetben egyeztetni kell. A szimulált támadásokat minden esetben úgy kell végrehajtani, hogy a rendszer működési stabilitása ne kerüljön veszélybe. A vizsgálat életciklusa a következő ábrán látható.

69. ábra: Behatolás vizsgálat életciklusa

Forrás: [108]

A hat lépés egymásra épül és minden esetben a ciklus megismételhető. A feltárás magában foglalja a vizsgálat tárgyát, ami lehet a komplex hálózat, vagy csak a vezeték nélküli hálózati szegmens. A vizsgálat során egy prioritási sorrendet kell felállítani a vizsgálat menetével kapcsolatban, ami három lépésből áll:

- blackbox vizsgálat;
- greybox vizsgálat;
- whitebox vizsgálat. [107]

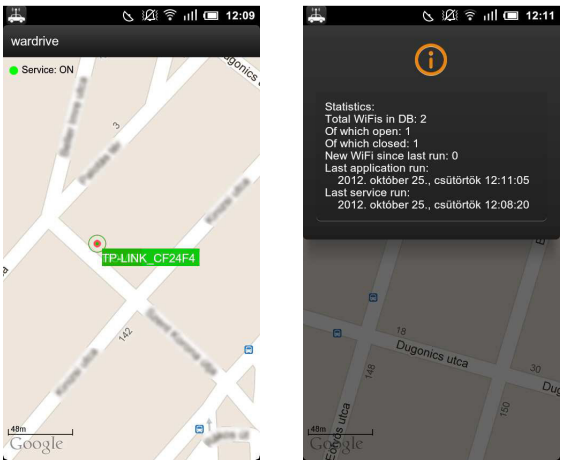
Kutatásaim során a behatolási vizsgálat elvégzésére számos eszközplatformra elkészült módszertanokat találtam. Az okostelefonok fejlődése és a vezeték nélküli hálózat vizsgálatához szükséges szoftverek fejlődése lehetővé tette számomra egy olyan vizsgálati modell kidolgozását, amely a telefonunkkal végrehajtható. Okostelefonjaink teljesítménye és tudása vetekszik egy asztali számítógép tudásával. Ez tette lehetővé számomra egy saját vizsgálati módszer megalkotását, amely már meglévő Androidos alkalmazások szisztematikus módszertani összerendezése. Azért választottam az Android környezetet, mert a linux alapú operációs rendszerre számos a módszerhez szükséges alkalmazás már rendelkezésre áll. A kidolgozott módszer lépéssorozatai lehetővé teszik a kritikus infrastruktúra üzemeltetői számára, hogy külön erre a vizsgálatra vásárolt eszköz nélkül, csak az okostelefon segítségével bármikor és bárhol ellenőrizzék hálózatuk zártságát.

Blackbox vizsgálat

A vizsgálat azt szimulálja, mint amikor egy rosszindulatú támadó a hálózatunk felé kívülről indítja a támadást. Nincs tisztában a hálózat sajátosságaival, csak egy nyitott ajtót keres, amin keresztül támadhat. Ezt a vizsgálatot három részre bontottam:

- az eszközök felderítésére;
- az eszközök fizikai helyének meghatározására;
- az eszközök vezeték nélküli paramétereinek feltérképezésére.

A WLAN eszközök felderítését egy wardriving alkalmazás segítségével lehet megvalósítani, amit a következő ábra mutat.



70. ábra: Wardriving alkalmazás android környezetben

Forrás: saját szerkesztés

A kritikus infrastruktúra körbejárásával beazonosítható a vezeték nélküli hálózati pontok elhelyezkedése az útszakaszon. Jól látszik pirossal a védett, zölddel a nyitott hálózati végpontok elhelyezkedése. Az így kapott eredmények pontosan azonban nem tudják beazonosítani az infrastruktúránk felöl érkező WLAN forrásokat. Ehhez szükségünk van iránymérésre is. Ezt teszi lehetővé a "Wifi Radar" alkalmazás, amely segítségével egy pár perces mérés után be tudjuk azonosítani az előzőekben megtalált WLAN eszközök pontos irányát. A 71. ábra ezt az alkalmazást mutatja be.

A vizsgálat után ismerjük az infrastruktúra irányából sugárzott WLAN jeleket, be tudjuk azonosítani azok irányát, elhelyezkedését.

71. ábra: "Wifi Radar" alkalmazás a WLAN eszközök sugárzási irányának meghatározásához

Forrás: saját szerkesztés

Ahhoz, hogy felderített hálózatokról több információt megtudhassunk a "Wifi Analyzer" alkalmazást kell használni. Az alkalmazás segítségével megtudhatjuk a hatótávolságon belüli WLAN hálózatok nevét, csatorna elhelyezkedését, titkosítását, hitelesítését és jelerősségét. A következő ábra az alkalmazás által biztosított vizsgálati lépéseket mutatja:

72. ábra: "Wifi Analyzer" androidos alkalmazás mérési lehetőségei

Forrás: saját szerkesztés

Ezekkel a vizsgálatokkal felderíthetőek az infrastruktúránkon belül szabálytalanul üzemeltetett hozzáférési pontok, amelyek potenciális veszélyforrást jelentenek az infrastruktúrára.

Greybox vizsgálat

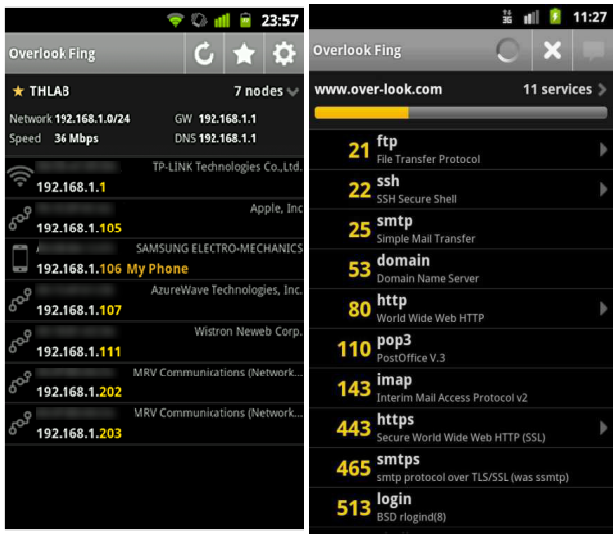
A vizsgálat annyiban különbözik a Blackbox vizsgálattól, hogy ekkor már rendelkezünk részleges információval az infrastruktúráról. A módszer segítségével a hálózatot belül-

ről tudjuk vizsgálni. Rendelkezésünkre áll még egy hálózati azonosító és jelszó, amely segítségével keressük a hálózat gyenge pontját.

A gyenge pontok közé tartoznak a:

- nyitott hálózati portok;
- hamis AP-k;
- a hálózatra felcsatlakozott illetéktelen eszközök;
- rosszul konfigurált monitorozó rendszerek.

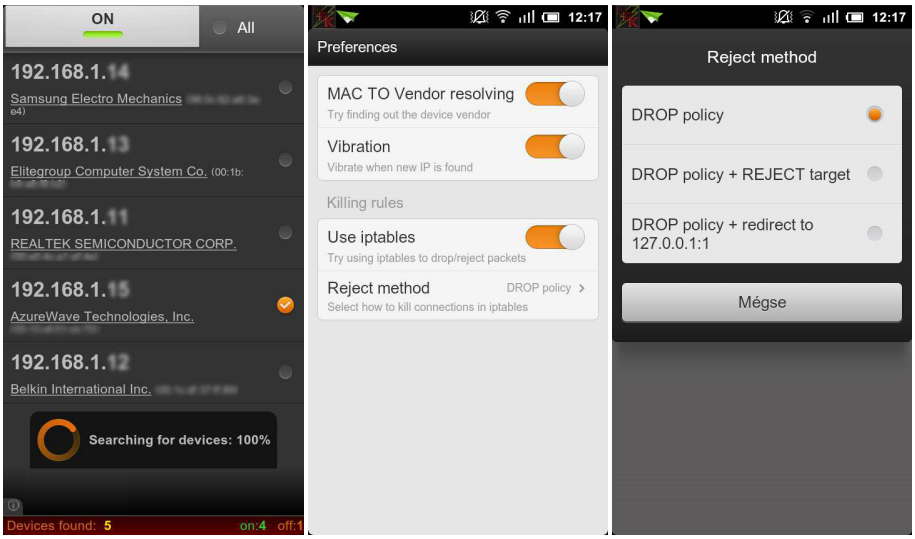
A vizsgálatok egyes részeit az "Overlook Fing" alkalmazással végezhetjük el. Az alkalmazás lehetőséget ad a vezeték nélküli hálózaton keresztül a vezetékes és a vezeték nélküli hálózatot használó eszközök felderítésére, eszköztípusának beazonosítására, portjainak vizsgálatára. A következő ábra az eszköz és port vizsgálatot mutatja.



73. ábra: "Overlook Fing" alkalmazás vizsgálati képei

Forrás: saját szerkesztés

A rosszul konfigurált, vagy hibásan működő monitorozó rendszert a "WifiKill" alkalmazással lehet vizsgálni. Az alkalmazás hálózatvizsgálatot végez, majd a találati lista alapján el lehet dönteni, hogy mely IP címeket, eszközöket támadjunk meg. Az alkalmazás a nevével ellentétben nem csak a vezeték nélküli hálózati eszközök kapcsolatát képes megszakítani, hanem a vezetékes eszközökét is. A következő ábra az alkalmazást mutatja futtatás közben.



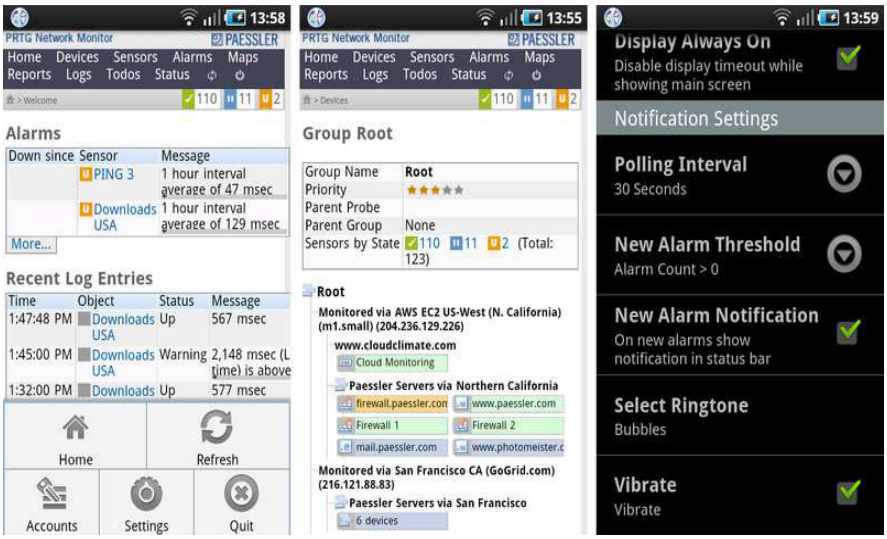
74. ábra: A "WifiKill" alkalmazás hálózat felderítés közben

Forrás: [110]

Whitebox vizsgálat

Ez a vizsgálat a kritikus információs infrastruktúra vezeték nélküli hálózatának teljes feltérképezését jelenti. A vizsgálat során rendelkezünk rendszerazonosítókkal, jelszavakkal, beállításokkal, alaprajzokkal. Ezek birtokában átfogó vizsgálatot lehet végezni a vezeték nélküli hálózati szegmensről. A vizsgálathoz a mobil alkalmazáson kívül szükségünk lesz a vezeték nélküli hálózati szegmens egyik hordozható számítógépére is. A hordozható számítógépen egy hálózatmonitorozó rendszert futtatunk (PRTG Network Monitor) amely a vezeték nélküli hálózati szegmenset figyeli. A következő ábra a monitorozó rendszer felületét mutatja vizsgálat közben.

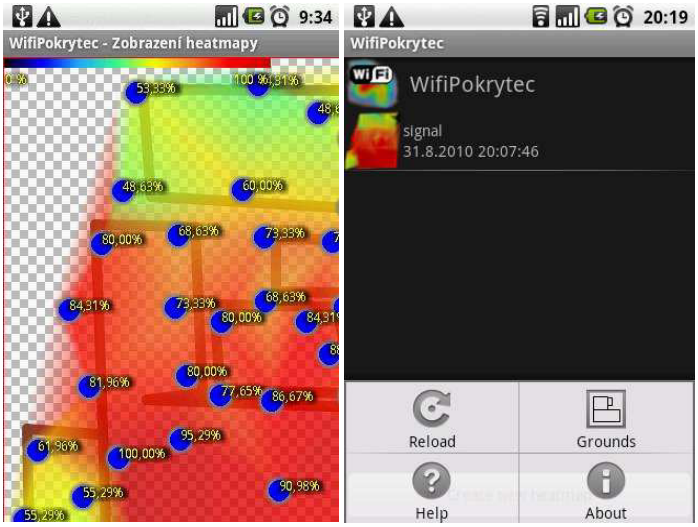
Az alkalmazás segítségével képet kapunk a hálózati eszközökről, tűzfalakról, beállításokról. Ahhoz hogy láthatóvá tegyük a vezeték nélküli hálózat lefedettségét hőtérképet tudunk készíteni az infrastruktúráról a megadott tervrajz segítségével.



75. ábra: A "PRTGdroid" alkalmazás vizsgálat közben

Forrás: [111]

Ezt a "WifiPokrytec" alkalmazás segítségével tehetjük meg. Az okostelefonba feltöltött tervrajz alapján a területet körbejárva megkaphatjuk az infrastruktúra hőtérképét. Ezzel felderíthetőek a rosszul működő AP-k, és az esetlegesen engedély nélkül üzemeltetett végpontok is. A következő kép a lefedettségi vizsgálatot mutatja.



76. ábra: A "WifiPokrytec" alkalmazás hőtérképe.

Forrás: [112]

A megalkotott vizsgálati módszertan segítségével a kritikus információs infrastruktúra üzemeltetője teljes képet kaphat a vezeték nélküli hálózat zártságáról bárhol és bármikor. Az esetlegesen felmerülő problémákat, támadásokat szó szerint kézben tudja tartani, és ha teljes hálózatot érintő menedzsment rendszert használ a kritikus információs

infrastruktúra, az okostelefonról elvégezhető a szükséges hibajavítás, vagy a védelmi lépés. A módszertanhoz használt alkalmazások ingyenesek, így a kritikus információs infrastruktúrán belül akár több informatikus is használhatja vizsgálataihoz.

3.9 Következtetések

A fejezetben három fő területtel foglalkoztam:

- a vezeték nélküli hálózatok egyesített támadási és védelmi rendszertanával;
- a kritikus információs infrastruktúrákban működő vezeték nélküli hálózatok védelmével;
- a vezeték nélküli hálózatok behatolás vizsgálatának csak mobiltelefonra épülő módszertanával.

A vezeték nélküli hálózatok védelmére és támadására a jelenlegi szakirodalmak, mint önálló és egymással közvetlen kapcsolatban nem lévő problémaként tekintenek. Az értekezésemben ezért elkészítettem egy olyan egységesített rendszertant, amely nem csak a támadások vagy csak a védelem szempontjai alapján foglalkozik a vezeték nélküli hálózatokkal, hanem valamennyi releváns támadást megfeleltet az azt semlegesítő vagy hatásának, bekövetkezési valószínűségének csökkentését szolgáló intézkedésekkel. A kölcsönös megfeleltetés során figyelembe vettem a támadások által fenyegetett követelményeket (bizalmasság, sértetlenség, rendelkezésre állás). Az így kidolgozott egységes szemléletű modell véleményem szerint növeli a védelem hatékonyságát és eredményességét, mivel a kockázatelemzés során azonosított problémák kezelésére egyértelmű választ ad.

A támadási technikák és védelmi kontrollok egységes rendszertanának tükrében kidolgoztam egy olyan módszertani javaslatot, amelyet véleményem szerint valamennyi vezeték nélküli hálózatot üzemeltető kritikus infrastruktúrában meg kell követelni.

Az infokommunikációs technológia fejlődésével a mobiltelefonok mérete jelentősen csökkent (nehezen detektálható), viszont jelentősen megnőtt ezeknek az eszközöknek a számítási teljesítménye, adattároló kapacitása, és jelentősen bővült a funkcionalitása. A mai okostefonok képességei vetekszenek az asztali/ hordozható számítógépek tudásával. Az értekezésemben kidolgoztam egy olyan behatolás vizsgálati módszertant, ami pusztán okostelefonokra épül.

A módszertan megalkotásának kettős célja volt. Egyrészt demonstrálni kívántam a vezeték nélküli hálózatokra leselkedő mobil veszélyek valósságát, illetve bemutattam, hogy a jelenleg bárki számára elérhető ingyenes alkalmazásokkal milyen sok információ gyűjthető össze a vezeték nélküli hálózatokról. A módszertan elkészítésének célja másrészt egy olyan, a gyakorlatban is egyszerűen használható útmutatás kidolgozása volt, amelyet a védelmi szférában dolgozók is felhasználhatnak az általuk felügyelt kri-

tikus információs infrastruktúrák vezeték nélküli hálózatának sebezhetőség vizsgálatára. Az általam kidolgozott módszertan nyílt forráskódú és szabadon elérhető szoftverekre épül, így költséghatékony módon vizsgálhatók bárhol és bármikor a célrendszerek.

Összegzett következtetések

Az informatikai eszközök és az őket összekötő hálózatok egyre nagyobb szerepet kapnak hétköznapjainkban. Nagyon nehéz olyan területet találni, ahol a munkavégzés eszközeként, vagy irányítójaként ne alkalmaznának informatikai berendezéseket hálózatban. A kritikus információs infrastruktúra területén is elengedhetetlen a zavartalan működéshez a megfelelő számítógépes hálózati összeköttetés. Vizsgálatokkal bizonyítottam, hogy a kritikus információs infrastruktúrákban a hagyományos vezetékes hálózati összeköttetés mellett fontos szerepet kaptak a vezeték nélküli hálózati megoldások, ezen belül is az IEEE 802.11-es ajánlás csoport alá besorolt eszközök. Azzal, hogy egyes kritikus információs infrastruktúrának vezeték nélküli hálózati szegmense lett, új támadási felületet nyitottak az üzemeltetők. E miatt szükségesnek tartottam annak vizsgálatát, hogy a vezeték nélküli hálózat esetleges működési zavarai milyen hatással vannak a kritikus információs infrastruktúrára és ezen keresztül más kritikus információs infrastruktúrára. Ezért rendszerszemléletű modellt alkottam, hogy a kritikus információs infrastruktúrák inter- és intradependenciái felmérhetők legyenek, a kapcsolataik tartalma elemezhetővé váljon mikro és makro szinten egyaránt. Az elkészített modell alapján megállapítottam, hogy a vezeték nélküli hálózat speciális al-infrastruktúraként értelmezhető és vizsgálható valamennyi kritikus információs infrastruktúrában. A modell utat nyit további kutatásokhoz, amelyek segíthetik a kritikus infrastruktúra és kritikus információs infrastruktúra inter és intradependenciáinak jobb megértését és pontosabb elemzését.

Kutatásaim során a vezeték nélküli hálózati szegmenseket 2004 óta vizsgálom az alkalmazott technológia és az eszközök elterjedése szerint. A legutolsó átfogó vizsgálat elsősorban a kritikus információs infrastruktúrákra irányult. A vizsgálati eredményekből kiemelt három kritikus információs infrastruktúrában heterogén hálózati és védelmi megoldásokat alkalmaznak. Ez a heterogenitás támadhatóvá teszi ezeket az infrastruktúrákat, ezért feltártam azokat a lehetséges támadási útvonalakat, amelyek a vezeték nélküli hálózaton keresztül közvetlenül, vagy közvetve fenyegetik a kritikus információs infrastruktúra biztonságát.

A vezeték nélküli hálózatok védelmére és támadására a jelenlegi szakirodalmak, mint önálló és egymással közvetlen kapcsolatban nem lévő problémaként tekintenek. Egyedi (egyes) támadásokra adandó védelmi lépések természeten léteznek, azonban ezek jelenleg nincsenek egy egységes rendszerbe foglalva. Ezért fontosnak tartottam elkészíteni

egy olyan egységesített rendszertant, amely nem csak a támadások vagy csak a védelem szempontjai alapján foglalkozik a vezeték nélküli hálózatokkal, hanem valamennyi releváns támadást megfeleltet az azt semlegesítő vagy hatásának, bekövetkezési valószínűségének csökkentését szolgáló intézkedésekkel. Tesztkörnyezetben megvizsgáltam a támadások közül a leggyakrabban alkalmazott módszereket. Arra a megállapításra jutottam, hogy a támadások nagy százaléka kis szaktudással és kevés anyagi ráfordítással kivitelezhető gyengén védett hálózat esetén, így potenciális veszélyforrásai az ilyen kritikusi információs infrastruktúrák vezeték nélküli hálózatának. A vizsgálat azt is bebizonyította, hogy a kritikus információs infrastruktúrában használnak Enterprise illetve SOHO vezeték nélküli hálózati eszközöket. Az Enterprise eszközök a hálózat védelmének több elemével rendelkeznek, mint egy hagyományos SOHO eszközökből kiépített hálózat. Az általam elkészített védelmi módszertan alkalmazható mind a két környezetben, azzal a feltétellel, hogy a védelmi lépéseket az adott hálózat lehetőségeihez képest legjobban ki kell használni. A módszertan bevezetését ajánlom minden kritikus információs infrastruktúra üzemeltető, illetve biztonsági vezető számára, mint egyfajta vezeték nélküli hálózatokra alkalmazható biztonsági minimum követelményrendszer.

Kutatásaim és a szakirodalmak ide vonatkozó részei alapján kidolgoztam a kritikus információs infrastruktúrák vezeték nélküli hálózataival szembeni támadások és a védelem elméletének és gyakorlatának rendszerszemléletű megközelítését, majd ez alapján megfeleltettem egymásnak a vezeték nélküli hálózatok elleni támadási technikákat és a védelem kontrolljait. Az így elkészített rendszertan az infrastruktúra üzemeltetői számára útmutatást ad a támadásoknak megfeleltetett védelmi intézkedéssorozat végrehajtására.

Az infokommunikációs technológia fejlődésével a mobiltelefonok számítási teljesítménye, adattároló kapacitása, és funkcionalitása jelentősen bővült. A mai okostefonok képességei vetekszenek az asztali / hordozható számítógépek tudásával. Az értekezésemben kidolgoztam egy olyan behatolás vizsgálati módszertant, ami pusztán okostelefonokra épülő már elkészített android alkalmazások módszertani összefogása. Ezzel a célom kettős volt. Egyrészt demonstrálni kívántam a vezeték nélküli hálózatokra leselkedő mobil veszélyek valósságát, illetve bemutattam, hogy a jelenleg bárki számára elérhető ingyenes alkalmazásokkal milyen sokrétű információ gyűjthető össze a vezeték nélküli hálózatokról. A módszertan elkészítésének célja másrészt egy olyan, a gyakorlatban is egyszerűen használható útmutatás kidolgozása volt, amelyet bárki, így a védelmi szférában dolgozók is felhasználhatnak az általuk felügyelt kritikus információs

infrastruktúrák vezeték nélküli hálózatának sebezhetőség vizsgálatára. Az általam kidolgozott módszertan nyílt forráskódú és szabadon elérhető szoftverekre épül, így költséghatékony módon vizsgálhatók bárhol és bármikor a célrendszerek.

Új tudományos eredmények

Az elvégzett kutatómunkám és vizsgálataim alapján új tudományos eredménynek tekintem az alábbiakat:

1) Rendszerszemléletű modellt alkottam a kritikus információs infrastruktúrák inter- és intradependenciáinak felmérésére és a függőségek tartalmának elemzésére, amely alkalmas egy kritikus információs infrastruktúrán belüli függőségek és több kritikus információs infrastruktúra közötti kapcsolatrendszer egységes szerkezetű ábrázolására, valamint a kritikus információs infrastruktúrák függőségi kockázatelemzésére.

2) Hazai környezetben elvégzett mérések alapján rendszereztem a kritikus információs infrastruktúrák vezeték nélküli hálózataiban alkalmazott technológiákat és a velük szemben támasztott műszaki követelményeket. Az elméleti követelmények és a mérési eredmények alapján meghatároztam a kritikus információs infrastruktúrák vezeték nélküli hálózatait is magában foglaló lehetséges támadási útvonalakat.

3) A támadási és védelmi taxonómiákra alapozva megalkottam egy javasolt védelmi módszertant a vezeték nélküli hálózatok végpontjaira, amely tartalmazza a hálózat biztonságos üzemeltetésének minimum követelményrendszerét.

4) Kidolgoztam a kritikus információs infrastruktúrák vezeték nélküli hálózataival szembeni támadások és a védelem elméletének és gyakorlatának rendszerszemléletű megközelítését, majd ez alapján megfeleltettem egymásnak a vezeték nélküli hálózatok elleni támadási technikákat és a védelem kontrolljait.

5) Kidolgoztam a vezeték nélküli hálózatok behatolás vizsgálatának kizárólag mobiltelefonra épülő módszertanát, amely - kapcsolódva a számítógépekre alkalmazott ilyen jellegű vizsgálatokhoz - önmagában lehetővé teszi a kritikus információs infrastruktúrák informatikai üzemeltetése számára a vezeték nélküli hálózat 24/7 vizsgálatát.

Ajánlások

Munkám során igyekeztem kellő alapossággal körüljárni a vezeték nélküli hálózatok és a kritikus információs infrastruktúrák kapcsolatát. Értekezésemet javaslom felhasználni a felsőoktatásban a hálózatokkal és a kritikus információs infrastruktúrákkal kapcsolatos tantárgyak keretében.

Az értekezésemben szereplő egymásnak megfeleltetett támadási és védelmi kontrollok szakmai továbbképzések kiegészítő anyagaként is felhasználhatóak.

A teljes értekezést javaslom alap irodalomként kritikus információs infrastruktúra üzemeltetőinek.

Az általam megalkotott védelmi minimumkövetelmény technikai alapként felhasználható a kritikus infrastruktúrákkal kapcsolatos törvényalkotás során a vonatkozó részterület normatív követelményeinek megfogalmazásakor.

Budapest, 2012. október 26.

Varga Péter János

Témakörből készült publikációim

Lektorált folyóiratban megjelent cikkek

1. **Varga Péter; Illési Zsolt**: Wardriving és a térinformatika.
   Hadmérnök V. Évfolyam 3. szám - 2010. szeptember 80-86.p. ISSN 1788-1919
   Honlap: http://www.hadmernok.hu/2010_3_varga.pdf

2. **Varga Péter; Illési Zsolt**: Kritikus infrastruktúrák hatás alapú modellezése.
   Hadmérnök, IV. évf. 4. sz., 2009.december 390-399.p. ISSN 1788-1919
   Honlap: http://www.hadmernok.hu/2009_4_vargap_illesi.pdf

3. **Varga Péter**: A kritikus információs infrastruktúrák értelmezése.
   Hadmérnök, III. évf. 2. sz., 2008. június 149-156.p. ISSN 1788-1919
   Honlap: http://www.hadmernok.hu/archivum/2008/2/2008_2_varga.pdf

Idegen nyelvű kiadványban megjelent cikkek

1. **Varga Péter**: Wi-Fi enumeration. 8th Students' Science Conference
   Lengyelország, Szklarska Poręba 2010.augusztus 288-293.p. ISSN 1732-0240

Konferencia kiadványban megjelent előadás

1. **Varga Péter**: Defence taxonomy of wireless networks.
   XXVII. Nemzetközi Kandó Konferencia 2011. november 17-18.
   Honlap: http://kvk.uni-obuda.hu/konf2011 ISBN 978-615-5018-20-6

2. **Varga Péter**: International and Domestic Regulations of Wireless Network Defense. XXVI. Nemzetközi Kandó Konferencia 2010. november 4-5.
   Honlap: http://regi.kvk.uni-obuda.hu/konf2010/ ISBN 978-963-7158-04-9

3. **Varga Péter**: Okostelefon a vezeték nélküli hálózatok zártságának vizsgálatában. Emcom 2011 2011. május 3-4. Eger Honlap: http://www.hte.hu/event/emcom2011ivveszelyhelyzetikommunikaciokonf

4. **Varga Péter**: Rádiós hálózatok elleni támadások rendszertana. Robothadviselés 10. 2010. november 24. Budapest Honlap: http://robothadviseles.hu/program_rw10.html

5. **Dr. Lukács György;Varga Péter**: EMC/EMI probléma. EMC 2010., 2010. március 9., Budapest Honlap: http://kvk.bmf.hu/emc2010/doc/emc2010_lukacs_gyorgy.ppt

6. **Illési Zsolt; Varga Péter**: Rádiós hálózatok krimináltechnikai vizsgálata XXV. Kandó Konferencia, 2009. november 23., Budapest Honlap: http://kvk.bmf.hu/konf2009/

7. **Varga Péter**: A kritikus infrastruktúrák és a vezeték nélküli hálózat kapcsolata EMCOM 2009 konferencia, 2009.november 13. Hévíz Honlap: http://kvk.bmf.hu/emcom2009/

8. **Varga Péter; Illési Zsolt**: Kritikus infrastruktúrák hatásalapú vizsgálata Robothadviselés 8. konferencia, 2008.november 27., Budapest Honlap: http://www.zmne.hu/tanszekek/ehc/konferencia/eloadas_rw8.html

9. **Varga Péter; Illési Zsolt**: Kritikus infrastruktúrák hatásalapú modellezésének kérdései XXIV. Nemzetközi Kandó Konferencia, 2008. november 7., Budapest Honlap: http://regi.kvk.uni-obuda.hu/konf2008/doc/eloadasok/32.ppt

10. **Varga Péter**: Kritikus információs infrastruktúrák informatikai támadás elleni védelme. Veszélyhelyzeti kommunikáció konferencia, 2007. szeptember 11., Budapest Honlap: http://kvk.bmf.hu/emcom2007/eloadasok.htm

Konferencia előadás

1. **Varga Péter**: Rádiós hálózatok védelmének rendszertana.
   Robothadviselés 11. 2011. november 24. Budapest
   Honlap: http://robothadviseles.hu/program_rw11.html

2. **Varga Péter**: Kritikus infrastruktúrák kapcsolatainak modellezése
   XIII. Tulajdonvédelmi konferencia, 2008.október 17., Hajduszoboszló
   Honlap: http://www.securifocus.com/p_images_db/
   hir_fckeditor/userfiles/File/programtervezet
   %202008%2009_05_%20valtozat.doc

3. **Varga Péter**: Mitől kritikus egy információs infrastruktúra.
   A tudomány iskolája a Kandóban konferencia, 2007. november 29., Budapest
   Honlap: http://konferenciakalauz.hu/files/conferenc
   e/1004/szimpozium_program_2007.doc

4. **Varga Péter**: Kritikus információs infrastruktúrák biztonsága
   Robothadviselés 7. konferencia, 2007. november 27. Budapest
   Honlap: http://www.zmne.hu/tanszekek/ehc/konferencia/program.html

Irodalomjegyzék

1. **Kerti Andárs, Pándi Erik, Töréki Ákos**: A vezetési és információs rendszerek elméleti megközelítése. Kommunikáció 2010. [Online] Budapest, 2010.október 6. [Letöltve: 2012.június 3.] http://193.224.76.4/download/hirado/kiadvanyok/konf2010.pdf. ISSN 978-963-7060-21-2
2. **ZMNE**: Fejlődik a ZMNE informatika rendszere. [Online] Budapest, 2010.július 22. [Letöltve: 2012.május 6.] http://portal.zmne.hu/portal/page?_pageid=34,151003&_dad=portal&_schema=PORTAL
3. **Bruce Schneier**: Breaking WEP in Under a Minute. [Online] 2007.április 4. [Letöltve: 2012.március 5.] http://www.schneier.com/blog/archives/2007/04/breaking_wep_in.html
4. **Stewart Baker, Shaun Waterman, George Ivanov**,: In the Crossfire - Critical Infrastructure in the Age of Cyber War, McAfee [Online] 2010. [Letöltve: 2012.szeptember 15.] http://www.mcafee.com/au/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf
5. **Magyar Értelmező Kéziszótár**. Budapest : Akadémiai Kiadó, 1978./2003.
6. **Magyar Larousse Enciklopédia**. Párizs-Budapest : Librairie Larousse-Akadémiai Kiadó, 1994. ISBN 963-055-856-4.
7. **Haig Zsolt, Várhegyi István**: Hadviselés az információs hadszíntéren. Budapest: Zrínyi Kiadó, 2005. ISBN 963-327-391-9.
8. **Robert T. Marsh**: Critical Foundations Protecting America's Infrastructures. [Online] Washington 1997.október 13. [Letöltve: 2012.február 14.] http://www.fas.org/sgp/library/pccip.pdf
9. **Précsényi Zoltán, Solymosi József**: Úton az európai kritikus infrastruktúrák. Hadmérnök. [Online] 2007. március . [Letöltve: 2007.augusztus 27.] http://w3.zmne.hu/hadmernok/archivum/2007/1/2007_1_precsenyi.html ISSN 1788-1919
10. **Muha Lajos**: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme [Online] Budapest 2007, Doktori (PhD) értekezés. [Letöltve: 2010. szeptember 3.] http://193.224.76.4/download/konyvtar/digitgy/phd/2008/muha_lajos.pdf

11. **Haig Zsolt**: Az információs társadalmat fenyegető információalapú veszélyforrások. Hadtudomány [Online] Budapest 2007. szeptember [Letöltve: 2008.január 10.] http://www.zmne.hu/kulso/mhtt/hadtudomany/2007_3_4.html ISBN 963-04-5226-X
12. **U.S.Goverment**: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. (USA Patriot Act 2001) [Online] 2001. október 26. [Letöltve: 2012.június 17.] http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf
13. **European Communities**: Green Paper on a European Programme for Critical Infrastructure Protection. [Online] Brussels 2005. november 17. [Letöltve: 2010.április 14.] http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf
14. **Kormányzati portál**: 2112/2004. (V. 7.) Kormány határozat a terrorizmus elleni küzdelem aktuális. [Online] Budapest 2004. [Letöltve: 2010.május 5.] http://pvir.bm.hu/jog/File/Terrorizm_ell_kuzd_akt_feledatai.doc
15. **Kormányzati portál**: 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. [Online] Budapest 2008. [Letöltve: 2011.január 11.] http://pvir.bm.hu/jog/File/Krit_Infrast_Ved_Nemz_Prog.doc
16. **Kormányzati portál**: Törvény javasat - 2012. évi …. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. [Online] Budapest 2012. [Letöltve: 2012.szeptember 3.] http://www.kormany.hu/download/3/ae/70000/torvenyjavaslat.pdf
17. **European Communities**: Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the fight against terrorism [Online] Brussels 2004. [Letöltve: 2010.augusztus 24.] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF
18. **Munk Sándor**: Információs színtér, információs környezet, információs infrastruktúra. Vezetés- és Szervezéstudomány [Online] Budapest 2002. [Letöltve: 2008. január 10.] http://193.224.76.4/download/konyvtar/digitgy/20022/vszt/munk.html ISSN 1417-7323.

19. **Haig Zsolt**: Kritikus információs infrastruktúrák védelme az információs terrorizmus tükrében I. ITTK-Szakmai Klub [Online] Budapest 2007. február 15. [Letöltve: 2008.május 28.] www.ittk.hu/web/docs/klub/HaigZs_ITTKKlub53.ppt
20. **Hír24**:Áram nélkül maradt fél India. [Online] Budapest 2012.július 31. [Letöltve: 2012.augusztus 21.] http://www.hir24.hu/kulfold/2012/07/31/aram-nelkul-maradt-fel-india/
21. **Budai Balázs Benjámin:** M-kormányzat Technológiai meghatározók. [Online] Budapest 2007. [Letöltve: 2008.május 28.] http://www.m-government.hu/m-gov%20techno.ppt
22. **Haig Zsolt**: Az információs társadalom információbiztonsága. Bolyai Szemle [Online] Budapest 2008. [Letöltve: 2010. március 5.] http://portal.zmne.hu/download/bjkmk/bsz/bszemle2008/4/12_Haig_Zsolt.pdf ISSN 1416-1443
23. **Szádeczky Tamás**: Terrorizmus a kibertérben. Infokommunikáció és jog [Online] 2008. [Letöltve: 2011. február 16.] http://www.jogiforum.hu/folyoiratok/1/734 ISSN 1786-0776
24. **U.S.Goverment**: Critical Infrastructure Interdependency Modeling. A Survey of U.S. and International Research [Online] 2009. [Letöltve: 2009.december 13.] http://www.inl.gov/technicalpublications/Documents/3489532.pdf
25. **Maros Dóra**: GSM. Budapest 2001.
26. **Jamrik Péter**: Devecser - Evecsedr. Emcom2011[Online] Eger 2011. május 3. [Letöltve: 2012.február 25.] http://regi.hte.hu/uploads/File/Jamrik%20P%C3%A9ter_Devecser.ppsx
27. **Haig Zsolt, Hajnal Béla, Kovács László, Muha Lajos, Sik Zoltán Nándor**: A kritikus információs infrastruktúrák meghatározásának módszertana. [Online] Budapest 2009. augusztus 01. [Letöltve: 2011.december 20.] http://www.cert-hungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf
28. **Illési Zsolt, Varga Péter**: Kritikus Infrastruktúrák hatásalapú modellezése. Hadmérnök. [Online] Budapest 2009. [Letöltve: 2010. január 8.] http://hadmernok.hu/2009_4_vargap_illesi.pdf ISSN 1788-1919

29. **ISO.ORG**: ISO/IEC 15408-1-3:2005. Information technology – Security techniques – Evaluation criteria for IT security. [Online] 2005. [Letöltve: 2010. március 10.] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40612
30. **Wikipedia**: Virtual business. [Online] 2012 [Letöltés: 2009.december 13.] http://en.wikipedia.org/wiki/Virtual_business : ismeretlen szerző, 2009..
31. **Kocsis Tamás**: Médiafüggetlen vállalati hálózatok, avagy az ethernet és a Wi-Fi összeolvadása. [Online] 2012. április 17 [Letöltve: 2012.07.02.] http://vimeo.com/40511268
32. **Wigle.net**: Wireless Geographic Logging Engine. [Online] [Letöltve: 2012. május 20.] http://www.wigle.net/.
33. **Wikipedia**: Nemzetközi Távközlési Egyesület. [Online] 2012 [Letöltve: 2012.május 11.] http://hu.wikipedia.org/wiki/Nemzetk%C3%B6zi_T%C3%A1vk%C3%B6zl%C3%A9si_Egyes%C3%BClet
34. **Robert J.**: **Bartz** Certified Wireless Technology Specialist Official Study Guide. Indianapolis. Wiley Publishing, 2009. ISBN: 978-1-1183-5911-2
35. **Cisco**: Enterprise Mobility 4.1 Design Guide. [Online] 2012 [Letöltve: 2012.június 21.] http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/eMob4.1.pdf
36. **Gyányi Sándor**: Informatikai WLAN-hálózatok zavarása. Bolyai Szemle [Online] Budapest 2009. [Letöltve: 2011. november 20.] ISSN 1416-1443 http://portal.zmne.hu/download/bjkmk/bsz/bszemle2009/4/10_gyanyisandor.pdf
37. **Szőke Lajos**: Vezeték nélküli hálózat tervezése [Online] Debrecen 2007. [Letöltve: 2012. január 5.] http://tiszai.tricon.hu/WiFi/Szakdolgozat.pdf
38. **Aruba:** Outdoor MIMO Wireless Networks. [Online] 2012. [Letöltve: 2012. április 18.] http://www.arubanetworks.com/pdf/technology/OMWN_VRD_2012-01-04%20%281%29.pdf
39. **Aruba:** Indoor 802.11n Site Survey and Planning. [Online] 2012. [Letöltve: 2012. április 18.] http://www.arubanetworks.com/wp-content/uploads/indoor80211n_2012-05-31.pdf

40. **Krüpl Zsolt:** A rádiócsatorna spektrális képe. [Online] 2003. [Letöltve: 2012.június 05.] http://www.ham.hu/radiosatvitel/digitalis_spektrum/
41. **Horák György**: WLAN hálózatok biztonsági analízise. [Online] Budapest, 2004. március 30. [Letöltve: 2012.június 14.] http://horak.hu/diploma.pdf
42. **Wikipedia**: IEEE 802.11n-2009. [Online] 2012. [Letöltve: 2012.június 20.] http://en.wikipedia.org/wiki/IEEE_802.11n-2009
43. **Wikipedia**: IEEE 802.11a-1999. [Online] 2012 [Letöltve: 2012.június 20.] http://en.wikipedia.org/wiki/IEEE_802.11a-1999
44. **Wikipedia**:IEEE 802.11b-1999. [Online] 2012 [Letöltve: 2012.június 20.] http://en.wikipedia.org/wiki/IEEE_802.11b-1999
45. **Wikipedia**:IEEE 802.11g-2003. [Online] 2012 [Letöltve: 2012.június 20.] http://en.wikipedia.org/wiki/IEEE_802.11g-2003
46. **Pejman Roshan, Jonathan Leary**: 802.11 Wireless LAN Fundamentals. Cisco 2004. ISBN-10: 1587050773.
47. **Canfone**: WiFi Citywide Mesh Network. [Online] [Letöltve: 2012.június 12.] http://www.canfone.com/custom-solutions/wireless-solutions/wifi-citywide-mesh-network/
48. **David D. Coleman, David A. Westcott,Bryan E. Harkins,Shawn M. Jackman**: Certified Wireless Security Professional. Wiley Publishing. 2009. ISBN 978-0-470-43891-6.
49. **Rózsa Gábor**: Vezeték nélküli hálózatok biztonságának vizsgálata. [Online] Debrecen 2009. [Letöltve:2012.február 16.] http://ganymedes.lib.unideb.hu:8080/dea/bitstream/2437/90312/1/Szakdolgozat-RG.pdf
50. **Intel**: A biztonsági vonatkozások áttekintése. [Online] [Letöltve: 2012.április 25.] http://support.elmark.com.pl/rgd/drivery/S15S/WLAN/INTEL/XP_VISTA/XP/Docs/HUN/overview.htm
51. **Faigl Zoltán**: Az IEEE 802.11i kapcsolat-felépítés vizsgálata. [Online] Budapest 2005 [Letöltve: 2012.április 20.] http://www.mcl.hu/oktatas/802.11i_meres.pdf
52. **Index**: Lelőtte a Jobbik weboldalát az Anonymous [Online] 2012 [Letöltve: 2012. június 10.] http://index.hu/tech/2012/04/20/a_jobbik_ellen_vonul_az_anonymous/.
53. **Adatvédelem**: Egy perc alatt feltörhető a wifi. [Online] 2009. szeptember 15. [Letöltve: 2012.január 21.] http://adatvedelem.blog.hu/2009/09/15/egy_perc_alatt_feltorheto_a_wifi

54. **Buttyán Levente, Dóra László:** WiFi biztonság – A jó, a rossz, és a csúf. [Online] Budapest [Letöltve: 2012.június 04.] http://www.hit.bme.hu/~buttyan/publications/ButtyanD06ht.pdf
55. **SG**: Street View-botrány. [Online] 2010.május 24. [Letöltve: 2012.május 06.] http://www.sg.hu/cikkek/74549/street_view_botrany_megszolalt_eric_scmidt_es_larry_page
56. **Seroundtable**: Where Google Street View Cars Sleep. [Online] 2012. augusztus 3. [Letöltve: 2012. augusztus 21.] http://www.seroundtable.com/photos/google-street-view-cars-15517.html
57. **Cyber War News:** Massive data leak from foxconn.com by @SwaggSec. [Online] 2012. február 8. [Letöltve: 2012. augusztus 5.] http://www.cyberwarnews.info/tag/swaggsec/.
58. **News.com.au**: Anonymous hackers claim ISP user data stolen from AAPT. [Online] 2012. július 26. [Letöltve: 2012. augusztus 5.] http://www.news.com.au/technology/hacked-anonymous-steals-user-data-from-aussie-isp/story-e6frfro0-1226435629217.
59. **JiWire**: Mobile Audience Insights Report. [Online] 2012 Q1. [Letöltve: 2012.július 06.] http://www.jiwire.com/sites/default/files/JiWire_Insights_Q1_2012.pdf
60. **Cyber War News:** AT&T VOIP Service Hacked, Data leaked for #WikiBoatWednesday by @Zer0Pwn. [Online] 2012. június 28. [Letöltve: 2012. augusztus 6.] http://www.cyberwarnews.info/2012/06/28/att-voip-service-hacked-data-leaked-for-wikiboatwednesday%E2%80%AC-by-zer0pwn/.
61. **6x6 taxi**. [Online] [Letöltve: 2012. augusztus 5.] http://www.6x6taxi.hu/.
62. **Volánbusz**: Wifi hotspot a Volánbusz távolsági járatain. [Online] [Letöltve: 2012. augusztus 5.] http://www.volanbusz.hu/hu/wifi/.
63. **MÁV-Start**: Internetezzen ingyen a 3. generációs IC vonatokon! [Online] [Letöltve: 2012. augusztus 5.] http://www.elvira.hu/wifi/index.php.
64. **Munk Sándor**: A kritikus infrastruktúrák védelme információs támadások ellen. Hadtudomány. [Online] 2008. [Letöltve: 2012. május 2.] ISSN 1215-4121 http://www.zmne.hu/kulso/mhtt/hadtudomany/2008/1_2/096-106.pdf.
65. **John D Howard**: Complete Computer and Network Attack Taxonomy. [Online] 1997. [Letöltve: 2011. április 20.] http://www.cert.org/research/JHThesis/Start.html.

66. **Kovács László**: Az információs terrorizmus eszköztára. Hadmérnök. [Online] 2006. november 22. [Letöltve: 2011. augusztus 12.] ISSN 1788-1919 http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html.
67. **CGIL Fermo**: Attivata la WiFi Zone. [Online] 2010. [Letöltve: 2012. március 25.] http://www.informazione.tv/index.php?action=index&p=61&d=840&art=27033.
68. **Seth Nitesh**: Wi-Fi hack: How to hack a Wi-Fi [Online] [Letöltve: 2011. november 20.] http://www.gizmowatch.com/entry/wi-fi-hack-hack-wi-fi-network/
69. **Haig Zsolt**: Számítógép-hálózati hadviselés rendszere az információs műveletekben. Bolyai Szemle [Online] 2006. [Letöltve: 2011. május 17.] ISSN 1416-1443 http://portal.zmne.hu/download/bjkmk/bsz/bszemle2006/1/06_Haig_Zsolt.pdf.
70. **Gönczöl Katalin**: Bűnös szegények. [Online] 1991. [Letöltve: 2012. augusztus 15.] http://www.fszek.hu/szociologia/szszda/gonczol_bunos.pdf.
71. **Haig Zsolt, Kovács László**: Fenyegetés a cybertérből, Nemzet és Biztonság [Online] Budapest, 2008. május [Letöltve: 7 8, 2012.] http://www.nemzetesbiztonsag.hu/letoltes.php?letolt=57.
72. **Haig Zsolt**: Kritikus Információs Infrastruktúrák sebezhetősége. [Online] 2009. június 10. [Letöltve: 2012. június 26.] http://scinetwork.hu/docs/eloadasok/20090609-10-wireless-technologiak/HaigZsolt_20090609-10.pdf.
73. **Szegediné Lengyel Piroska**: Számítógépes bűnözők avagy fiatal a Cyber-térben. Hadmérnök. [Online] 2010. június. [Letöltve: 2011. június 3.] http://www.hadmernok.hu/2010_2_szegedine1.pdf. ISSN 1788-1919
74. **MTI**: Megtalálták az Anonymous-hackercsoport hazai tagjait. [Online] 2012. szeptember 8. [Letöltve: 2012. 9 10.] http://www.sg.hu/cikkek/91948/megtalaltak_az_anonymous_hackercsoport_hazai_tagjait
75. **Szabó Henrik**: Számítógépes hálózatok elleni támadás. Bűnmegelőzés. [Online] [Letöltve: 2012. május 6.] http://bunmegelozes.uw.hu/szamitogepes.pdf.
76. **Póserné Oláh Valéria**: Számítógép-hálózati támadások. Hadmérnök [Online] 2006. [Letöltve: 2012. május 21.] ISSN 1788-1919 http://hadmernok.hu/kulonszamok/robothadviseles6/poserne_rw6.html.

77. **Miniszterelnöki Hivatal**: Tervezés az IT biztonság szempontjából [Online] 2008. [Letöltve: 2012. április 12.] http://www.ekk.gov.hu/hu/emo/ekozigkeretrendszer/ek3-itbiztonsag/EKK_ekozig_ITbiztonsagiutmutato_080728_V1.pdf
78. **Hun-CERT**: CERT WLAN tanulmány. [Online] 2011. [Letöltve: 2011. november 4.] http://www.cert.hu/images/stories/tanulmanyok/szalai.pdf.
79. **Ványa László**: Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre. [Online] Budapest 2001 Doktori (PhD) értekezés [Letöltve: 2011. szeptember 14.] http://193.224.76.4/download/konyvtar/digitgy/phd/2003/vanya_laszlo.pdf
80. **Lisa Phifer**: A list of wireless network attacks. [Online] [Letöltve:2011.november 07.] http://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks
81. **Shawnville:**WarDriving [Online] 2007. július 14. [Letöltve: 2008. szeptember 11.] http://shawnville.com/notebook/2007/07/14/wardriving/.
82. **Wikipedia:** Wardriving [Online] 2012. [Letöltve: 2012.május 20.] http://en.wikipedia.org/wiki/Wardriving
83. **Blackbeltjones**: Warchalking [Online] 2002. [Letöltve :2012.június 03.] http://www.blackbeltjones.com/warchalking/archives/2002_06.html
84. **Macrotronics**: TP-Link Nano Router TL-WR702N [Online] 2012. [Letöltve: 2012.július10.] http://www.macrotronics.net/product_info.php/tp-link-nano-router-tl-wr702n-p-2139
85. **Vivek Ramachandran**: Enterprise Wi-Fi worms, Backdoors and Botnets fo Fun and Profit. Hactivity [Online] Budapest, 2011. november 17. [Letöltve: 2012.február 20.] http://www.youtube.com/watch?v=YGIayOhCrSI
86. **Routerpasswords**: Default router passwords [Online] 2012. [Letöltve: 2012. május 5.] http://www.routerpasswords.com/.
87. **Jakó András**: Wireless LAN a Műegyetemen, Networkshop 2004 [Online] Győr, 2004 [Letöltve: 2011.július 02.] http://splash.eik.bme.hu/papers/bmewlan.html

88. **Gulyás Gábor:** WLAN lehallgatás zsebből[Online] 2010.január 4. [Letöltve: 2012.március 04.] http://pet-portal.eu/old/?page=blog&topic=pet&func=read&id=253
89. **Networksasia**: Networking and security apps for your rooted Android, Security asia [Online] 2011. szeptember 28. [Letöltve: 2012. június 5.] http://security.networksasia.net/content/networking-and-security-apps-your-rooted-android?page=0%2C2
90. **Dd-wrt**: DD-WRT Privacy [Online] [Letöltve: 2012. augusztus 14.] http://www.dd-wrt.com/site/index
91. **Hakshop**: WiFi Pineapple Mark IV [Online] 2012. [Letöltve: 2012. május 22.] http://hakshop.myshopify.com/products/wifi-pineapple
92. **Poiplaza**: Nyilvános WIFI Magyarországon [Online] 2012. [Letöltve: 2012.július 23.] http://poiplaza.com/index.php?p=sdb&d=3745&lstpg=search
93. **Wührl Tibor**: Robotkutatások és a térinformatika kapcsolata, Hadmérnök [Online] 2006. június. [Letöltve: 2011. május 4.] http://hadmernok.hu/archivum/2006/1/2006_1_wuhrl.html.
94. **Anu Odusami**: Wi-Fi: Unknown risks to enterprise Networks in Lagos Metropolis. X-wireless Project [Online] [Letöltve: 2012. augusztus 10.] http://xwireless-psdn.lexium.net/wifi%20threats.pdf.
95. **Peleskey Miklós Pál**: Hálózati csomópontok védelme hardver és szoftver eszközökkel [Online] Debreceni, 2009. [Letöltve: 2012.május 08.] http://ganymedes.lib.unideb.hu:8080/dea/bitstream/2437/85575/1/szakdolg.pdf
96. **CEH**: Certified Ethical Hacker, Career Academy [Online] 2011. [Letöltve: 2011. november 4.] http://www.careeracademy.com/index.asp?PageAction=VIEWPROD&ProdID=74.
97. **Iyad Al Khatib:** Performance Analysis of Wireless LAN, Royal Institute of Technology [Online] 2003. [Letöltve: 2011. november 4.] http://web.it.kth.se/~ikhatib/lic/final/iyad_lic_final.pdf.
98. **Horváth Tamás**: E-alkalmazások hálózati védelme Cisco eszközökkel. Albacomp. [Online] 2007. [Letöltve: 2011. 11 4.] http://www.extraprofit.hu/pp_konferenciakozpont/2007-03-08_E-alkalmazasok_megoldasok/Cisco_Systems_Magyarorszag_Kft/CISCO_E-onkormanyzat_2007.ppt

99. **Katona Krisztina**: Informatikai rendszerek konfiguráció konfiguráció-menedzsmentje [Online]2009. február 5. [Letöltve: 2012. augusztus 5.] http://users.nik.uni-obuda.hu/erdelyi/IRKM/IRKM1.pdf.

100. **Beinschróth József**: Adat és információvédelem, Informatikai biztonság [Online] [Letöltve: 2012. július 10.] http://kandotav2.uw.hu/8.f%E9l%E9v%20Alkalmazott%20Sz%E1mtech%20%E9s%20Inf.v%E9delem/02_22.pdf.

101. **Jakó András**: Wireless Lan, BME EISZK [Online] 2003. [Letöltve: 2011. november 20.] http://splash.eik.bme.hu/papers/wlan.pdf.

102. **Iphone-ticker**: London verbietet Nutzung in Olympia-Spielstätten, W-Lan Polizei lokalisiert User [Online] 2012. [Letöltve: 2012. augusztus 29.] http://www.iphone-ticker.de/personlicher-iphone-hotspot-london-verbietet-nutzung-in-olympia-spielstatten-w-lan-polizei-lokalisiert-user-36731/.

103. **BCS Hungary**: Motorola WIDS es WIPS [Online] 2011. [Letöltve: 2012. május 20.] http://www.bcs.hu/?akt_menu=717.

104. **Heckenast Tamás:** Behatolás detektálás, IDS rendszerek. [Online] [Letöltve: 2012. augusztus 20.] http://www.sze.hu/~heckenas/okt/ids.pdf.

105. **Linux Wiki**: FreeRADIUS [Online] 2008. [Letöltve: 2012. 9 2.] http://unixlinux.tmit.bme.hu/FreeRADIUS.

106. **Complex**: Útmutató rendszer értékelőknek. e-Közigazgatási Keretrendszer Kialakítása projekt. [Online] 2008. [Letöltve: 2012. augusztus 12.] http://kovetelmenytar.complex.hu/doc.php?docid=EKZ_EKK_EKOZIG_UTMUTATO_RENDSZER_ERTEKELOKNEK_080919_V3.DOC&filedownload=1&docdb=koz

107. **Silent Signal**: Etikus hackelés [Online] 2009. [Letöltve: 2011. május 20.] http://silentsignal.hu/etikus_hack.

108. **IT Secure**: Sérülékenység vizsgálat [Online] 2010. [Letöltve: 2011. május 20.] http://www.itsecure.hu/etikus_hack

109. **Areacellphone**: Android Application WarDrive: Stores Scans And Displays Wifi Networks [Online] 2010. [Letöltve: 2011. május 20.] http://areacellphone.com/2010/05/android-application-wardrive-stores-scans-displays-wifi-networks/.

110. **Slideme**: Wifikill [Online] 2011. szeptember 5. [Hivatkozva: 2012. július 6.] http://slideme.org/application/wifikill.

111. **Paessler**: PRTGdroid. [Online] 2012. [Letöltve: 2012. május 2.] http://www.paessler.com/apps/androidapp.

112. **Ivo Šmíd**: WifiPokrytec [Online]2011. [Letöltve: 2012. május 15.] http://bit.ly/aGaJSD

113. **Aruba**: Indoor 802.11n Site Survey and Planning [Online] 2012. [Letöltve: 2012. június 25.] http://www.arubanetworks.com/wp-content/uploads/indoor80211n_2012-05-31.pdf

114. **Wirelessdefence**: MAC Address Changer [Online] 2010. [Letöltve: 2012.április 15.] http://www.wirelessdefence.org/Contents/MAC%20Address%20Changer.htm

115. **Colarik Andrew M**.: Cyber Terrorism: Political and Economic Implications, Idea Group Publishing, 2006. ISBN 1-59904-021-2.

116. **Robert A. Maksimschuk, Eric J. Naiburg**: UML földi halandóknak, Budapest, Kiskapu Kft., 2006. ISBN 963-9637-14-9.

117. **Takács Péter, Rajnai Zoltán:** WiFi hálózatok veszélyei, Hadmérnök. [Online] Budapest 2007. március . [Letöltve: 2008.március 20.] http://hadmernok.hu/archivum/2007/2/2007_2_takacs.pdf ISSN 1788-1919.

118. **Gyányi Sándor**: Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem, PhD értekezés [Online] Budapest 2012. [Letöltve: 2012.május 2.] http://193.224.76.2/downloads/konyvtar/digitgy/phd/2012/gyani_sandor.pdf

119. **Prim** : D-Link alapokon az Országos Mentőszolgálat IP hálózata [Online] 2006. október 22. [Letöltve: 2012.szeptember 29.] http://hirek.prim.hu/cikk/55428/

120. **D-link**: Budafok-Tétény Önkormányzata Polgármesteri Hivatala [Online] [Letöltve: 2012.szeptember 29.] http://b2b.dlink.hu/hir.php?idhir=30

121. **D-link:** Részecske- és Magfizikai Kutatóintézet Hivatala [Online] [Letöltve: 2012.szeptember 29.] ftp://ftp.dlink.hu/marketing/Esettanulm%E1ny_RMKI_new_small.pdf

122. **Beinschróth József**: Informatikai rendszerekkel támogatott folyamatok működésfolytonossági kérdései a védelmi szférában, PhD értekezés, [Online] Budapest, 2007. [Letöltve: 2012.szeptember 29.] http://193.224.76.4/download/konyvtar/digitgy/phd/2008/beinschrot_jozsef.pdf

123. **Straub Ádám**: Zavart kelthet a wifi az éterben [Online] Budapest, 2010. július 16. [Letöltve: 2012.szeptember 30.] http://www.origo.hu/techbazis/20100716-wifi-zsinor-nelkuli-telefon-kelt-zavart-az-eterben.html

124. **The Guardian**: iPad to dominate tablet sales until 2015 as growth explodes, says Gartner [Online] 2011. szeptember 22. [Letöltve: 2012.augusztus 10.] http://www.guardian.co.uk/technology/2011/sep/22/tablet-forecast-gartner-ipad

125. **Index**: A wifi zavarja az időjárás-előrejelzést [Online] 2012. augusztus 26. [Letöltve: 2012.augusztus 30.] http://index.hu/tech/2012/08/26/a_wifi_zavarja_az_idojaras-elorejelzest/

126. **Prim Online**: Elkészült a Bethesda Gyermekkórház világszínvonalú informatikai rendszere [Online] 2007. október 9. [Letöltve: 2012.augusztus 10.] http://businessonline.prim.hu/cikk/63563/

127. **Kovács László, Krasznay Csaba**: Digitális Mohács, Nemzet és Biztonság [Online] 2010.február [Letöltve: 2012.július 8.] http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf

128. **Haig Zsolt, Várhegyi István:** A cybertér és a cyberhadviselés értelmezése Hadtudomány [Online] Budapest, 2008. [Letöltve: 2012.augusztus 12.] http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf ISBN 963-04-5226-X

129. **Haig Zsolt, Kovács László:** Fenyegetések a cybertérből, Nemzet és Biztonság [Online] 2008.május [Letöltve: 2012.július 18.] http://www.nemzetesbiztonsag.hu/letoltes.php?letolt=57

130. **Metageek**: Improve Your Wireless Network [Online] [Letöltve: 2012.október 10.] http://www.metageek.net/land/take-inssider-to-the-next-level-with-wi-spy/

131. **Best jammer**: WIFI BLUETOOTH RADIO JAMMERS [Online] 2012. [Letöltve: 2012.október 10.] http://www.bestjammers.com/index.html

132. **Lisa Phifer**: Top Ten Wi-Fi Security Threats, eSecurity Planet [Online] 2010. március 8. [Letöltve: 2012.október 10.] http://www.esecurityplanet.com/views/article.php/3869221/Top-Ten-WiFi-Security-Threats.htm

Ábrák jegyzéke

1. ábra: Összekapcsolt információs infrastruktúrák
egymásra hatása kiterjedésük szerint 19
2. ábra: A kritikus infrastruktúra, a kritikus információs
infrastruktúra és a vezeték nélküli hálózat kapcsolata 20
3. ábra: New Orleans infrastruktúra interdependenciái 22
4. ábra: Kárhelyszíni rádió-kommunikációs állomás 23
5. ábra: Kritikus információs infrastruktúra hierarchia
modell struktúra UML objektum diagramja 25
6. ábra: Kockázatelemzés fogalmi modellje 26
7. ábra: Inter és intradependencia helyettesítési modellje 28
8. ábra: Kritikus információs infrastruktúrák inter- és intradependenciája 28
9. ábra: A kritikus információs infrastruktúra szolgáltatási
interfész egyedi függéseinek egyszerűsítése kumulált függéssel 29
10. ábra: Távközlési szolgáltató és egy Kerületi Önkormányzat
függéseinek kapcsolata 30
11. ábra: „és” kapcsoló 32
12. ábra: Villamos energia és infokommunikációs szolgáltatás „és” kapcsolatban 32
13. ábra: „vagy” kapcsoló 33
14. ábra: Két mobil szolgáltató „vagy” kapcsolatban 33
15. ábra: Kerületi Önkormányzat kritikus információs infrastruktúra függésé 34
16. ábra: Kritikus információs infrastruktúra hierarchia,
mint virtuális szervezetek kapcsolata 35
17. ábra: A infokommunikációs technológia kereskedelmének
változása az elmúlt és a következő években 39
18. ábra: Az NMHH WLAN szabálysértések felderítésére felkészített járműve 40
19. ábra: A vizsgálat útvonala 44
20. ábra: ITU-R régiók térképe 45
21. ábra: WLAN frekvenciasáv használatának adatai a wigle.net alapján 46
22. ábra: WLAN frekvenciasáv használatának adatai mérési eredményeim alapján 46
23. ábra DSSS 2,4 GHz 48
24. ábra: Lefedettség vagy sebesség optimalizált cella 49
25. ábra: OFDM 49
26. ábra: Csatornakiosztások alakulása saját mérési eredmények alapján 50
27. ábra: A SISO és a MIMO felépítése 55
28. ábra: 802.11-es protokollt használó eszközök eloszlása 55
29. ábra: IBSS 57
30. ábra: MESH hálózat kritikus infrastruktúrában 58
33. ábra: WLAN topológiák eloszlása 59
34. ábra: Eszközgyártók felhasználási rangsora a wigle.net adatai alapján 60
35. ábra: Eszközgyártók felhasználási rangsora saját mérési adatok alapján 61
36. ábra: Nyílt és osztott kulcsú hitelesítés arányai 64
37. ábra: A WPA, WPA2, WPA-PSK, WPA2-PSK és nyílt hálózatok eloszlása 66

38. ábra: Anonymus aktivistacsoport felhívása informatikai támadásra nyílt hálózaton keresztül ... 67
39. ábra: Nyílt vagy osztott kulcsú hitelesítés titkosítása ... 69
40. ábra: WPA-PSK titkosítása ... 69
41. ábra: WPA2-PSK titkosítása ... 70
42. ábra: WPA2-Enterprise titkosítása ... 70
44. ábra: Támadás a kritikus információs infrastruktúra hálózati végpontja ellen ... 74
45. ábra: Kritikus információs infrastruktúra támadása a hozzáférési ponton keresztül ... 74
46. ábra: Kritikus információs infrastruktúra támadása egy másik kritikus információs infrastruktúra hozzáférési pontján keresztül ... 75
47. ábra: Nyilvános WLAN a világban ... 76
48. ábra: Kritikus információs infrastruktúra támadása nyilvános hálózati végponthoz kapcsolódó infrastruktúra felhasználón keresztül ... 77
49. ábra: Az eredeti vezeték nélküli hálózatot jelölő logo ... 81
50. ábra: A módosított logo ... 81
51. ábra: A wardriving elengedhetetlen eszközei ... 91
52. ábra: Passzív wardriving ... 93
53. ábra: Aktív wardriving ... 93
54. ábra: Probe response csomag ... 93
55. ábra: Hálózat tulajdonságára utaló szimbólumok ... 94
56. ábra: Windows alapú program MAC azonosító cseréjéhez ... 95
57. ábra: Mini router és AP egyben ... 96
58. ábra: Windows 7 AP létrehozásának lépése ... 96
59. ábra: AP és Router felhasználónév és jelszó lista ... 97
62. ábra: Módosított AP tulajdonságai közbeékelődéses támadáshoz és az AP közvetlenül egy mobil összeköttetéssel ... 100
63. ábra: Nyilvános WLAN-ok Magyarországon 2012-ben ... 101
64. ábra: EAPOL-Start támadás ... 102
65. ábra: Disassociation Flood támadás ... 103
66. ábra: Csatornakihasználtság képe (bal), mikrohullámú sütő spektrumképe (jobb) 103
67. ábra: Engedély nélküli WLAN hozzáférési pontok beazonosítása a 2012-es Londoni olimpián ... 113
68. ábra: WIDS rendszer felépítése ... 115
69. ábra: Behatolás vizsgálat életciklusa ... 119
70. ábra: Wardriving alkalmazás android környezetben ... 120
71. ábra: "Wifi Radar" alkalmazás a WLAN eszközök sugárzási irányának meghatározásához ... 121
72. ábra: "Wifi Analyzer" androidos alkalmazás mérési lehetőségei ... 121
73. ábra: "Overlook Fing" alkalmazás vizsgálati képei ... 122
74. ábra: A "WifiKill" alkalmazás hálózat felderítés közben ... 123
75. ábra: A "PRTGdroid" alkalmazás vizsgálat közben ... 124
76. ábra: A "WifiPokrytec" alkalmazás hőtérképe. ... 124

Táblázatok jegyzéke

1. táblázat: Kritikus infrastruktúrák ágazatai és alágazatai 15
2. táblázat: Kritikus információs infrastruktúra SLA mátrix 30
3. táblázat: A távközlési szolgáltató és a Kerületi Önkormányzat telefon és ügyfélkapcsolat SLA mátrixa 31
4. táblázat: 802.11 Fizikai és Adatkapcsolati rétege 51
5. táblázat: az IEEE 802.11 összefoglaló táblázata 52
6. táblázat: alapvető hitelesítési és titkosítási metódusok 62
7. táblázat: A három kritikus információs infrastruktúra vizsgálati eredményei 71
8. táblázat: Hozzáférés elleni támadások 88
9. táblázat: Bizalmasság elleni támadások 88
10. táblázat: Sértetlenség elleni támadások 89
11. táblázat: Hitelesítés elleni támadások 89
12. táblázat: Rendelkezésre állás elleni támadások 90
13. táblázat: WLAN zavaró berendezések 104
14. táblázat: Támadási módszertanok összefoglaló táblázata 105
15. táblázat: A vezeték nélküli hálózatok elleni támadások és az alkalmazható védelmi kontrollok egymásnak való megfeleltetése 117

Rövidítések jegyzéke

Rövidítés	Angol	Magyar / Jelentés
AAA	Authentication, Authorization, Accounting	Hitelesítés, engedélyezés és nyilvántartás
AES	Advanced Encryption Standard	Fejlett titkosítási szabvány
AP	Access Point	Hozzáférési pont
BPSK	Binary Phase Shift Keying	Bináris fáziseltolásos kódolás
BSS	Basic Service Sets	Alapszolgáltatás készlet
CC	Common Criteria	Informatikai termékek és rendszerek biztonsági értékelésének módszertana
CCMP	Counter Mode/CBC-MAC Protocol	Titkosítási és adatintegritás ellenőrzési protokoll
CEH	Certified Ethical Hacking	Minősített etikus hacker
CERT	Computer Emergency Response Team	Számítógépes vészhelyzetek elhárításért felelős csoport
COBIT	Control Objectives for Information and Related Technologies	A COBIT a nemzetközileg elfogadott informatikai kontroll
DBPSK	Different Binary Phase Shift Keying	Különbségi bináris fáziseltolásos kódolás
EAP	Extensible Authentication Protocol	Átfogó azonosító protokoll
ESS	Extended Service Sets	Megnövelt szolgáltatás készlet
EU	European Union	Európai Unió
FCC	Federal Communications Commission	Szövetségi Kommunikációs Bizottság
GDP	Gross Domestic Product	Bruttó hazai össztermék
GPS	Global Positioning System	Globális helymeghatározó rendszer
GSM	Global System for Mobile Communication	Globális vezeték nélküli kommunikációs rendszer
IASTED	International Association of Science and Technology for Development	Non-profit nemzetközi szervezet., Célja, hogy elősegítik a gazdasági és műszaki fejlesztéseket a világon
IBSS	Independent basic service sets	Független alapszolgáltatás
IDS	Intrusion detection system	Behatolás detektáló rendszer
IEEE	Institute of Electrical and Electronics Engineers	Villamos- és Elektromérnöki Szabványügyi Szervezet
IPS	Intrusion prevention system	Behatolást megakadályozó rendszer
ISDN	Integrated Services Digital Network	Integrált szolgáltatású digitális hálózat
ITSEC	Information Technology Security Evaluation Criteria	Információtechnológia Biztonsági Értékelési Kritériumok
JIT	Just in time	Éppen időben
LAN	Local Area Network	Helyi kiterjedésű hálózat
MAC	Media Access Control	Közegelérés vezérlés

Rövidítés	Angol	Magyar / Jelentés
MAN	Metropolitan Area Network	Nagyvárosi hálózat
MIMO	Multiple Input Multiple Output	Több bemenet több kimenet modell
NMHH		Nemzeti Média- és Hírközlési Hatóság
OSI	Open Systems Interconnection	Nyílt rendszerek összeköttetése
PHY	Physical Layer	Fizikai réteg
PKI	Public-Key Infrastructure	Nyilvános kulcsú titkosítás
PSK	Pre-shared key	Osztott kulcs
QAM	Quadrature Amplitude Modulation	Kvadratúra-amplitúdómoduláció
RADIUS	Remote Access Dial-In User Service	Távoli hitelesítő, betárcsázós felhasználói szolgáltatás
SDM	Space Division Multiplex	Térosztásos nyalábolás
SISO	Single Input Single Output	Egy bemenet egy kimenet
SLA	Service Level Agreement	Szolgáltatási szint szerződése
SSID	Service Set Identification	Bejelentkezési azonosító kód
TCSEC	Trusted Computer System Evaluation Criteria	Biztonságos Számítógépes Rendszerek Értékelési Kritériumai
TETRA	Trans European Trunked Radio	Európai Trönkölt Rádió
TKIP	Temporal Key Integrity Protocol	Időszakos kulcs sérthetetlenségi protokoll
UML	Unified Modelling Language	Általános célú modellező nyelv
VPN	Virtual Private Network	Virtuális magánhálózat
WAN	Wide Area Network	Nagy kiterjedésű hálózat
WECA	Wireless Ethernet Compatibility Alliance	Vezeték Nélküli Ethernet Kompatibilitás Szervezet
WEP	Wired Equivalent Privacy	Kábellel egyenértékű titkosság
WIDS	Wireless Distribution System	Vezeték nélküli behatolás detektáló rendszer
WIPS	Wireless intrusion prevention system	Vezeték nélküli behatolást megakadályozó rendszer
WLAN	Wireless LAN	Vezeték nélküli helyi hálózat
WPA	Wi-Fi Protected Access	Wi-Fi védett elérés