

A NEMZETI KÖZSZOLGÁLATI EGYETEM KIADVÁNYA



Kommunikáció 2014

Communications 2014



Székhely
1036 Budapest, Lajos u. 78.

Tel: +36 (1) 250-4910
Fax: +36 (1) 250-4909



Fercom Kommunikációs Kft.

www.fercom.hu

info@fercom.hu

Telephely
1037 Budapest, Pomázi út 15.

Tel: +36 (1) 250-7940
Fax: +36 (1) 250-7939

Cégismertető

A Fercom Kommunikációs Kft. a Motorola Solutions magyarországi disztribútóri partnere. Fő tevékenységünk a vezeték nélküli távközlés és rádiókommunikáció, ezen belül analóg és digitális rendszerek szállítása, rendszerintegrációja, telepítése-üzembe helyezése és karbantartása.

Cégünk közel 20 éve rendvédelmi és kormányzati szervek megbízható beszállítója. Termékeinket többek között a Magyar Rendőrség, a Magyar Honvédség, a Nemzeti Adó- és Vámhivatal, valamint nagyvállalatok egész sora használja országszerte nap, mint nap a legnagyobb megelégedéssel. Az országban több helyen saját trónkölt rádiórendszerrel rendelkezünk és üzemeltetünk. A kormányzati partnereink mellett a legnagyobb magyarországi közlekedési, szolgáltató és ipari vállalatok is a Fercom Kft. rendszereit használják. A vezeték nélküli kommunikáció mellett cégünk több éves tapasztalattal rendelkezik speciális biztonsági, katonai és rendfenntartó eszközök forgalmazásában és teljes körű integrációjában. A Fercom Kft. ISO 9001:2000 minősítéssel rendelkezik és minősített NATO beszállító.

Motorola rádió terminálok és rendszerek

Analóg és digitális rádiók és rádiórendszerek

Az analóg rádiók piacán a Fercom Kft. 80%-os részesedést tudhat magáénak, a Motorola csúcsmínőségű készülékeit a kormányzati szervek, gyárak, közlekedési, szállítmányozási és közszolgáltató cégek egyaránt használják. Ezen felhasználók számára természetesen biztosítjuk a lehetőséget a modern digitális technológiákra való folyamatos, akár szakaszos átállásra is.

Az elmúlt 3 évben több mint 25 digitális rendszert telepítettünk, többek között a budapesti Liszt Ferenc Nemzetközi Repülőtér is a MotoTRBO-t, a Motorola digitális rendszerét használja.

Motorola Tetra rádiók és rádiórendszerek

Az elmúlt három esztendőben cégünk több mint 7000 Motorola TETRA terminált szállított a kormányzati Tetra rendszer számára, a megrendelők teljes megelégedésére. A legnagyobb felhasználók a Magyar Rendőrség, Tűzoltóság, egyéb készenléti szervek, valamint a Nemzeti Adó- és Vámhivatal.

Távvezérlő és felügyeleti berendezések, rendszerek

A távvezérlésű alkalmazások és felügyeleti rendszerek alapjául szolgáló Motorola SCADA megoldás (MOSCAD) megoldásunk a közszolgáltató cégek (pl. Fővárosi Vízművek) működését támogatja.



SCI-Network Távközlési és Hálózatintegrációs Zrt.

<http://www.scinetwork.hu/>
info@scinetwork.hu

A SCI-Network Távközlési és Hálózatintegrációs Zrt. hálózati rendszerintegrációval foglalkozó szakértő vállalkozás. A szűkebb értelemben vett hálózati rendszerek mellett a cég alaptevékenységébe tartozik a mikrohullámú átvitel, a hálózati biztonság és a rendszerfelügyelet is. A SCI-Network teljeskörű szolgáltatást nyújt ügyfeleinek a hálózatok terén a feladat felmérésétől kezdve, a tervezésen, eszközszállításon, üzembehelyezésem, oktatáson keresztül a garanciális és garancián túli szolgáltatásokig. A folyamatosan gyarapodó létszámmal, bővülő ügyfélkörrel és növekvő forgalommal rendelkező vállalat az informatikai vállalkozások felső harmadába tartozik.

A SCI-Network célja, hogy ügyfelei számára magas színvonalú megoldásokat biztosítson, valamint megismertesse kiváló minőségű termékeit és szolgáltatásait leendő ügyfeleivel.

A vállalat kiemelt figyelmet fordít a minőségbiztosításra, melyet ISO 9001 és AQAP2110 minősítése is tükröz.



Always one step ahead.

A Kapsch Magyarországon a vállalati és intézményi ügyfeleknek professzionális ICT megoldásokat, a távközlési és internet szolgáltatóknak innovatív rendszereket kínál, teljes körű GSM-R, közlekedéstelematikai, valamint Smart Metering megoldásokat szállít.



always one step ahead

Nemzeti Közzolgálati Egyetem

Budapest, 2014. november 12.

A tudományos kiadványt lektorálták:
Prof. Dr. Pándi Erik r. ezredes, f. tanár
Dr. Fekete Károly alezredes, e. docens
Dr. Kerti András alezredes, adjunktus
Dr. Farkas Tibor százados, adjunktus

Szerkesztette:
Dr. Fekete Károly alezredes, e. docens

Kiadja: NKE Szolgáltató Kft.
Felelős kiadó: Hegyesi József ügyvezető igazgató
Nyomdai előkészítés: Tordas és Társa Kft.
Nyomdai munkák: NKE Szolgáltató Kft.
Készült: 120 példányban

ISBN 978-615-5491-94-8

TARTALOMJEGYZÉK

BEVEZETŐ	15
TUDOMÁNYOS KÖZLEMÉNYEK	17
NYIKES Zoltán	17
A MOBILESZKÖZÖK BIZTONSÁGI KÉRDÉSEI, AVAGY, HOGYAN HASZNÁLJUK A NYILVÁNOS WI-FI HÁLÓZATOKAT	17
CZIRÁKY Zoltán	35
NO-WIRELESS ZÓNA - AHOL TILTOTT A VEZETÉK NÉLKÜLI KOMMUNIKÁCIÓ	35
HORVÁTH Zoltán	43
AZ OKTATÁSI TEVÉKENYSÉG TÁMOGATÁSA REJTJELEZÉST, VALAMINT ADATREJTÉST MEGVALÓSÍTÓ PROGRAMCSOMAG ALKALMAZÁSÁVAL	43
NYÁRI László	55
KRITIKUS INFRASTRUKTÚRÁK ÚJ FELFOGÁSÚ ELEMZÉSE	55
TÓTH András	65
A NATO KOMMUNIKÁCIÓS RENDSZERÉNEK ELMÉLETI ÉS GYAKORLATI VIZSGÁLATA	65
TURÁNYI Zoltán	77
A KATASZTRÓFAVÉDELEM INFOKOMMUNIKÁCIÓS RENDSZEREI	77
TÓTH András	89
A NATO HÁLÓZAT NYÚJTOTTA KÉPESSÉG	89
László ZÖMBIK	99
SECURITY OF TELECOMMUNICATION NETWORK MANAGEMENT SYSTEMS	99
KONFERENCIA ELŐADÁSOK	117
BALKU Ferenc	117
IT- ÉS KIBERBIZTONSÁGI TENDENCIÁK	117
CZIRÁKY Zoltán	129
NO-WIRELESS ZÓNA - AHOL TILTOTT A VEZETÉK NÉLKÜLI KOMMUNIKÁCIÓ	129
IMRE László	139
A BIZTOS INFORMÁCIÓ ÉS KOMMUNIKÁCIÓ SZOLGÁLATÁBAN	139
NYÁRI László	159
BIG-DATA, BIG-BUMM	159
NYIKES Zoltán	165
A MOBIL ESZKÖZÖK BIZTONSÁGI KÉRDÉSEI	165
PRISZNYÁK Szabolcs	175
BITFÜGGÖNY	175
SÁGI Norbert – Dr. MAGYAR Sándor	183
A KIBERBŰNÖZÉS LEGÚJABB TRENDJEI	183

TÓTH András	193
A DÖNTÉSHOZATALI FOLYAMATOK HÁLÓZATKÖZPONTÚ	
TÁMOGATÁSI LEHETŐSÉGEI	193
TURÁNYI Zoltán	199
A KATASZTRÓFAVÉDELEM INFOKOMMUNIKÁCIÓS	
RENDSZEREI	199
Gábor VANDERER	205
SECURITY AWARENESS AND SOCIAL RESPONSIBILITY	205

A tudományos konferencia támogatói:



Kapsch Telecom Kft.



TÜV Rheinland Csoport



Hungaro DigiTel Kft.



Equicom Kft.



SCI-Network Távközlési és
Hálózatintegrációs ZRt.



TOTALTEL Távközléstechnika Kft.



Fercom Kommunikációs Kft.
SPESYS Network Security Company



Hírközlési és Informatikai
Tudományos Egyesület



Strategic Assistance and Support Group
Kft.



ELSINCO Budapest Kft.



Biztonságpolitikai Szakkollégium



HTEST Hungary Kft.



Enterprise Communications Magyarország
Kft.



Professzionális műholdas megoldások bárhol–bármikor



Hungaro DigiTel Kft.

2310 Szigetszentmiklós-Lakihegy, Komp u. 2.

tel: 06-1-488-8500 fax: 06-1-488-8501 <http://www.hdt.hu>

FOLYÓIRATOK

A HITE újszöveges hadianyval mellelt hagnonyo-
sian ket folyoiratit jegyez, a **Híradestecnikáit** és
a **Információkion Journalt**. Mig előbbi a hazai
szekszakmai élet tőfőeséet, kerdéseit és melleköt-
ségeit a **Információkion Journal** mat nemzetköz-
es híradestecnika és szett lett. A lap kiadását a Nem-
zeti Híradestecnika és Informatika (NHT) tano-
mányok szelkiesztése pedig folyamatosan szel-
kieszt. A közszekszakmai nemzetközis társapok-
lat a **Információkion Journal** elmséget jelzi,
mely a hazai nemzetközis adatbázisokba is szerez-
get, hogy a **Scopus**, a **Compendex** és az **Inspe-
ct**

Amennyiben „up-to-date” részese szeretne lenni az infokommunikációs tér áramlásának, itt tájékozódhat a **Hírközlési és Informatikai Tudományos Egyesületbe** történő belépés feltételeiről:

www.hte.hu/belepes.

Kérdéseit, észrevételeit, javaslatait az info@hte.hu e-mail címre készséggel várjuk!

Nagy Péter
igazgató igazgató
nagy.peter@tisz.hu

Bartolits István
főtitár
bartolits@mmh.hu

Magyar Gábor
elnök
magyar.g@tke.hu

HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYSÉG ÉS ET

Levelezési cím / iroda:
1051 Budapest, Bajcsy-Zsilinszky út 12. 502. iroda

UTÁNPÓTLÁS BIZTOSÍTÁSA

A HTE az országban tradicionálisan hangsúlyos szerepet kap a hatalommal való kapcsolat megteremtésére, a szakmával széles lakótérbe tudatosítására, a közvélemény elérésére. A HTE tudományos érdeklődéssel bír a diskurzus tanulásának és pályaválasztásának segítése – hiszen ott alkotnak a legfontosabb almasok, akik majd a jövő szakemberei. Az egyesület amellett, hogy az arra érdemes hallgatóknak biztosítja a kulcshozzáférést a tudományok, technológiák, foglalkozások, szakmák és a közvélemény részéért, és ezáltal a szakmák kapcsolatteremtését is, kulcshozzáférést pályaválasztás, pályakezdés, pályafejlesztés, pályaválasztás területein is biztosít, amelyek általános anyagi elismerésben is részesülnek. A HTE Diplomátusa és Szakemberei Pályázatára például az ország 15 legesélyesebb nevezetében, az ematitási érdemei a HTE Akadémiája által kiállított tanúsítvány is, amely szintén támogatja a következő információk kommunikációs, szervezési, szakmai feladatait.



A Hírközlési és Informatikai Tudományos Egyesület tekintélyes, 65 éves múltjával hazánk infokommunikációs szektorának legatnáibb szervezetévé vált. Munkássága a hírközlési és az informatikai ipárgtól, a hagyományos postai szolgáltatókon át, az internetig és a médiavilágig terjed.

Az egyesület közel 60 jogi tagot, valamint majdnem 1000 magánsemélyt számlál. Berkein belül több mint 20 szakmai közösség munkálkodik meghatározott célok érdekében, a legjobb tudása szerint:

A HTE amellett, hogy kiemelt, véleményformáló szerepet tölt be a magyar infokommunikációs szakterület szabályozásában, működésében, fejlődésében, hazai és nemzetközi szakmai rendezvények elismert szervezőjeként is jegyzett.

[illegible]SZAKMAI
RENDEZVÉNYEK
SZERVEZÉSE

A HTE naptárában nem telik el hét szakmai találkozó, előadások, kerekasztal beszélgetések és egyéb szervezett események nélkül, de házigazdája többek között olyan országos szakmai rendezvényeknek, mint

- a projektmenedzserek találkozóját és információszerését segítő **Projektmenedzsment Fórum**,
- a kimagasló hazai médiatechnikai esemény, a **HTE MediaNet** konferencia
- a **HTE Infokom**, amely az infokommunikációs hálózatok és alkalmazások legújabb piaci, műszaki és szabványozási kérdéseinek egyik legjelentősebb rendezvénye.

Az egyesület az utóbbi években számos nemzetközi tudományos konferencia és workshop má-
gyarországi megvalósítását nyerte el pályáza-
ti úton, így öregbítette hazánk szerepét a világ
informatikai kommunikációs szakmájában (bővebb infor-
máció a HTE nagyszervezésénél):

<http://www.hte.hu/ndagyrendezvenyek>).

HITE A
MINDENNAPOKBAN

Az egyesület szerződéses kapcsolatszereplőinek, valamint szakmai taglistájának (amely lefedheti az infokommunikációs szektor szinte teljes területét) köszönhetően teret ad a különböző vélemény- és információcserének, szakmai konferenciáknak, közös cél érdekében folytatott kollektív munkaságnak.

Lehetőséget biztosít arra, hogy az iparág valamennyi képviselője – akár a mindennapi konkurenst is hátrébb szorítva – kommunikáljon fontos kérdéskörökben, kifejtse a jelen nehézségeit illetően jövőbeli elképzeléseit. Mindeközben az egyének szakmai kiemelkedésének, véleményformálásának is útát enged.

A HTE megkérdőjelezhetetlen erőssége, és így több évtizedes elismertségének egyik alapja, hogy mind munkaszabály, mind véleményformálásában **sakszerű, kiegyensúlyozott és független**, felülemelkedik az esetleges politikai vagy éppen vállalati érdekeken.

Bő hat évtizedet és két tucat szakterületet pár mondatban összefoglalni szinte lehetetlen lenne, ezért inkább vázlatpontokban szemléljük, mi minden érinti manapság a HTE tevékenységi körét:

- hazai és nemzetközi konferenciák szervezése, lebonyolítása
- szakmai fórumok az internet technológiák és szolgáltatások elterjesztéséhez
- műsorok és az online média terjesztéséhez
- rádió- és televíziós technológiák ismeretterjesztése
- projektmenedzsment módszerek terjesztése
- szakmai folyóiratok nyomtatványos kiadása
- nemzetközi kapcsolatok együttműködés az IEEE vel és más társaságokkal
- szakmai díjak odaítélése (pl. Puskás Tivadar-díj, Kemény Ferenc-díj, Pollák Virág-díj)

A KONFERENCIA HÁTTÉR INFORMÁCIÓI

A konferencia fővédnöke:

Vass Sándor dandártábornok
Honvéd Vezérkar Híradó, Informatikai és Információvédelmi Csoportfőnökség
csoportfőnök

A konferencia támogatói:

Hírközlési és Informatikai Tudományos Egyesület
TÜV Rheinland Csoport
Hungaro DigiTel Kft.
Kapsch Telecom Kft.
Equicom Kft.
Fercom Kommunikációs Kft.
SCI-Network Távközlési és Hálózatintegrációs Zrt.
TOTALTEL Távközléstechnikai Kft.
ELSINCO Budapest Kft.
SPESYS Network Security Company
Biztonságpolitikai Szakkollégium
HTEST Hungary Kft.
Enterprise Communications Magyarország Kft.
Strategic Assistance and Support Group Kft.

A konferencia rendezői:

Nemzeti Közzolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Üzemeltetési Intézet Híradó Tanszék
Honvéd Vezérkar Híradó, Informatikai és Információvédelmi Csoportfőnökség
Hírközlési és Informatikai Tudományos Egyesület NKE Egyetemi Csoport

A szervező bizottság elnöke:

Dr. Fekete Károly alezredes, e. docens

A szervező bizottság titkára:

Dr. Farkas Tibor százados, adjunktus

A szervező bizottság tagjai:

Dr. Németh József, adjunktus
Tóth András százados, tanársegéd



Az EQUICOM Kft. 2000 óta van jelen a magyarországi ICT piacon telekommunikációs, informatikai és kábeltelevíziós mérés technikai megoldásokkal. Világviszonylatban is vezető pozíciót elfoglaló beszállítóink innovatív megoldásokat kínálnak az adatátviteli és kommunikációs hálózatok létesítési és üzemeltetési méréséhez, analíziséhez, és monitorozásához. Az évről-évre növekvő piaci jelenlétünk, az ügyfeleinkkel kialakított jó kapcsolat, a technológia központú szemléletünk és a hozzáadott érték növelésére való törekvésünk mellett a beszállítók folyamatos fejlesztési munkájának is köszönhető.

BEVEZETŐ

A KOMMUNIKÁCIÓ nemzetközi szakmai-tudományos konferencia-sorozat tizenötödik, jubileumi évfordulóján tisztelettel köszöntjük Önt, kedves olvasó!

Jelentős változások történtek az elmúlt időszakban a világ infokommunikációs színterén. A hálózati szolgáltatások szinte mindenhol és az esetek döntő többségében többplatformos megoldásokkal hozzáférhetővé váltak. Ma már nem az a kérdés, hogy van-e összeköttetés, kommunikáció, még csak nem is az, hogy mennyi, hanem az, hogy milyen tulajdonságokkal, minőségi paraméterekkel rendelkezik egy-egy hálózati sík. Globalizálódott és többsikúvá váltak a világot átfogó kommunikációs kapcsolatok. Időben dinamikusan, a pillanatnyi igényeknek megfelelően cseréljük, váltjuk az éppen használt eszközöket, alhálózatokat, hálózatokat.

Ezek nem csak egyre nagyobb teljesítményűek, de egyre intelligensebbek is. Sokszor a felhasználó előtt rejtve maradt képességekkel felvértezve keresik, kutatják, gyűjtik kommunikációs szokásainkat, jellemző magatartásmintáinkat. Jó esetben a rövid időn belül megalkotott elektronikus személyiségi profilunk hasznos feladatra várva rejtézik a cyber térben. Segíti, hatékonyabbá teszi a hálózaton végzett tevékenységünket, gyorsabbá az információ megtalálását, feldolgozását és eljuttatását másokhoz.

Az exponenciális sebességgel növekvő és egyre szövevényesebb világháló azonban a platformok sokrétűségével, a szolgáltatások egyre nagyobb fokú átláthatatlanságával, az információ nyomon követhetetlenségével az adat és - végső soron - a személy és a szervezet kiszolgáltatottságát is növeli. Idei konferenciánk tehát fő témaként a hálózatok sebezhetőségét, megváltozott jellemzőit, a cyber támadások elleni védekezési lehetőségeket teszi piedesztálra oktatóink, kutatóink, a téma avatott szakemberei, doktoranduszok és kiváló hallgatók előadásában.

Az idén ismét, de vélhetően ebben az arculatban utoljára nyílt lehetőségünk különkiadványt készítenünk, melyet ma, az előadások napján kézbe foghatunk. A megváltozott akadémiai, akkreditációs, tudományos követelmények és ezen belül a tudománymetrikai súlypontok eltolódása miatt oktatóinknak, kutatóinknak már nem előnyös ISBN számmal ellátott kiadványban publikálniuk. Reményeink szerint a jövő évtől helyette - regisztrált és magas tudományos besorolású - ISSN számmal megjelentetett periodikum tematikus különkiadványként láthatjuk viszont a konferencia kötetet. Tisztelettel és azzal a nem titkolt szándékkal ajánljuk rendezvényünk résztvevőinek kiadványunkat, hogy - az előadókon és a meghívott vendégeken túl - minél szélesebb szakmai körhöz jusson el a mai konferencia híre és mondanivalója.

Budapest, 2014. 11. 14.

Dr. Fekete Károly

TOTALTEL

TÁVKÖZLÉSTECHNIKA KFT



A Totaltel Kft. 100%-ban magyar tulajdonban lévő, 1991-ben alapított budapesti székhelyű társaság. Fő tevékenysége: digitális mikrohullámú rádióberendezések fejlesztése, gyártása és forgalmazása. Társaságunknak jelenleg 22 alkalmazottja van, akik közül 17 magasán képzett mérnök. Kooperáló és beszállító partnereinknél több száz szakember járul hozzá termékeink gyártásához.

Fejlesztési munkánk eredményeként készültek el a TDR típusú mikrohullámú digitális rádióberendezések különböző generációi, amelyek egyre magasabb frekvencián működnek és egyre nagyobb átviteli kapacitásra képesek. Ilyen berendezésekkel vállaljuk kulcsrakészen távközlési és adatátviteli összeköttetések vezeték nélküli megvalósítását nyilvános és magánhálózati alkalmazásokra egyaránt.

Különböző TDR berendezésekből több százat szállítottunk a MATÁV és utódja a T-Com számára. Ilyen berendezések tucatjait üzemeltette az Antenna Hungária Zrt. Szállítottunk berendezéseket állami intézmények és szervezetek számára: egyetemek, NAV, Fővárosi Vízművek, FETIKÖVIZIG stb.

Külön említést érdemelnek a rendvédelmi szervek. A Magyar Honvédség (MH) számára 1993. óta szállítottunk berendezéseket. Szállítottunk ezen kívül összeköttetéseket a Határőrség, a Katonai Felderítő Hivatal és a Nemzetbiztonsági Szakszolgálat számára.

Eddigi működésünk alapján elmondható, hogy a Totaltel Kft. a nagy privatizációs hullámban és import dömpingben egyedüli magyar céggént méltó partnere tudott maradni a hazai felhasználóknak. A Totaltel Kft. ismert termékeinek kiváló minőségéről, versenyképes árainról és magas színvonalú szolgáltatásairól.

Munkatársaink tevékenysége felöleli az alábbiakat:

- Rádióhálózat tervezése
- Összeköttetések tervezése
- Hatósági engedélyezés lefolytatása,
- Kulcsrakész projektek megvalósítása, a berendezés fejlesztésétől és gyártásától, a rendszerintegráción át a telepítésig, beleértve a működtető személyzet képzését, és a dokumentálást is.

Fő termékeink:

- TDR-F flexibilis digitális mikrohullámú rádióberendezés 100 Mbit/s sebességig (5, 7, 8, 13, 15, 18, 23, 26 és 38 GHz)
- TDR-F-W nagysebességű digitális mikrohullámú rádióberendezés 350 Mbit/s sebességig (5, 13, 18, 26 és 38 GHz)
- TDR-F-1P5 nagy távolságú digitális mikrohullámú rádióberendezés 2 Mbit/s, azaz 1E1 csatorna átvitelére, sávzsélesség takarékos modulációval (1,5 GHz, BW=500 kHz)
- Mikrohullámú antennák, Hálózattfelügyeleti rendszer (MX-MSS és SNMP).

Telephely: 1116 Budapest, Temesvár u. 20. Postacím: 1519 Budapest, Pf. 425
Tel:(1)-204-7850 Fax:(1)-206-2342 e-mail:totaltel@totaltel.hu www.totaltel.hu

TUDOMÁNYOS KÖZLEMÉNYEK

NYIKES Zoltán¹

A MOBILESZKÖZÖK BIZTONSÁGI KÉRDÉSEI, AVAGY, HOGYAN HASZNÁLJUK A NYILVÁNOS WI-FI² HÁLÓZATOKAT

Rezümé

A publikációmban vizsgálom az okos telefonok és a mobileszközök biztonsági kérdéseit, azok fontosságát. Szemléltetem a mobileszközök biztonsági fenyegetettségének növekedését az elmúlt időszakban. Bemutatom az MDM3-et és BYOD4-t, mint lehetőségeket, azok használat szabályozásának fontosságát a közzsférában. Demonstrálok egy általam létrehozott „fake Wi-Fi hotspot”5-öt, azaz bemutatatok egy konkrét mobil biztonsági sebezhetőséget, egy konkrét eset tanulmányozásán keresztül.

Kulcsszavak

okos telefon, mobiltelefon, okos mobileszközök, biztonság, információbiztonság, internet, Wi-Fi, hotspot, sérülékenység, mobil bankolás, vállalati használat, vírus, kártékony szoftver, átviteli út biztonság, router, hardver biztonság, közzsféra, üzleti alkalmazás, közigazgatási szektor, gazdasági szektor, Mobile Device Management, Bring Your Own Device, ál-Wi-Fi hotspot, SSID, MAC cím, hálózat

Bevezetés

Manapság már nem kérdés, hogy védenünk kell minden elektronikai eszközünket, amelyen valamilyen operációs rendszeren futtatott alkalmazások végzik a mérnökök és programfejlesztők által elgondolt feladatokat. Ezek az alkalmazások megkönnyítik a mindennapjainkat, segítik az ipart, a mezőgazdaságot, az oktatást, az egészségügyet és felsorolni is nehéz, hogy hova nem tört még be a „mobilizáció”. Egy vicces evolúciós elmélet szerint, az ember az evolúciós fejlődés során lejtött a fáról, felegyenesedett, két lábon járt, aztán leült a számítógép elé, majd a mobileszközök hatására újra felegyenesedett. Jelenleg itt tartunk! Aztán ennek az „evolúciós” folyamatnak következő állomása mi lesz, az még nem lehet megjósolni.

A PC⁶-s korszak az elemzők és a piac szerint leáldozóban van. A jövő, de már a jelen is a mobileszközöké. Kezdődött a laptopokkal, notebookokkal, Eee-pc⁷-kkel,

1 Magyar Honvédség 54. Veszprém Radarezred Információvédelmi központ, központparancsnok Óbudai Egyetem, Biztonságtudományi Doktori Iskola, doktorandusz, nyikes.zoltan@mil.hu

² Wireless Fidelity

³ Mobile Device Management

⁴ Bring Your Own Device

⁵ Nyilvános, vezeték nélküli internet hozzáférési pont, amely hamis

⁶ Personal computer

majd folytatódott a mobiltelefonokkal. Ezt a tabletek színrelépése követte. De a fejlesztők itt nem álltak le. Napjainkban kezdődött el a viselhető okos eszközök korszaka. Okos óra, okos szemüveg, okos cipő és még sorolhatnám. Ezek csak azok a termékek, amelyek a divatirányzatot követve jelentek meg a piacon. E mellett nem szabad megfeledkezni, azokról a katonai fejlesztésekről sem, amelyek egy része már publikussá vált ugyan, de jelentős része még nem került a nyilvánosság elé. A viselhető okos-eszközök fejlesztésében csak a képzelet szab határt.

A mobileszközök sérülékenységei

A napjainkban már egyre szélesebb körben használt eszközök biztonsági kérdései is ugyanolyan fontosak, ha nem fontosabbak, mint az adott eszköz alkalmazhatósága, vagy tulajdonságai. Ezen eszközök biztonsága sokrétű és összetett. Mivel ezek az eszközök, és most az okos telefonokról beszélek elsősorban, beható sérülékenysége nagy – mert leejthetjük, összetörük stb. – ezért használhatatlanná válik. Ez a sérülékenység ideiglenes, mivel a készülék javításával, cseréjével a probléma, viszonylag hamar elhárítható. Ez legfeljebb bosszantó, illetve pénzbe kerül. Erre a problémára a szakértők azt javasolják, hogy jobban vigyázzunk az eszközeinkre, továbbá már megjelentek a mobiltelefonokra megköthető biztosítási termékek is.

A biztonság vonatkozásában már komolyabb probléma az, hogyha a telefont elvesztjük, vagy ellopják. Ugyanis ebben az esetben kikerül a személyes felügyeletünk alól, és a telefonon vagy a memóriakártyán tárolt adatokhoz, megfelelő védelem hiányában, illetéktelenek hozzáférnek, hozzáférhetnek.

Mind az iOS8, mind az Android9 alapú okos telefonok, illetve táblagépek régebb óta rendelkeznek különféle titkosítási mechanizmusokkal, amelyek révén az adatok védelme biztosítható. E titkosítási technológiák az operációs rendszerek részét képezik, de különálló titkosító alkalmazások is léteznek. Sajnos azonban ezeket a megoldásokat a felhasználók többsége nem veszi igénybe. Vagy azért, mert nincs mindenki tisztában a létezésükkel, vagy egész egyszerűen nem érzik fontosnak az adatok biztonságba helyezését. Emellett kritikaként vagy kifogásként szokott megfogalmazódni, hogy az adattitkosítás időigényes feladat, és ezért inkább nem is használják. Pontosan látja ezt a helyzetet az Apple és a Google is. A két cég nem kizárólag felhasználói oldalról közelít a problémához, hanem abból a szempontból is, hogy a hatóságok és a különféle arra feljogosított szervek számára adott esetben ki kell adniuk felhasználói adatokat, ami egyik vállalatnak sincs az ínyére. Ezért olyan megoldásokat igyekeznek keresni, amik miatt még akkor sem tudnak adatokat kiszolgáltatni, ha arra kötelezik őket. A két cég azt találta ki, hogy olyan módon titkosítja a készülékeken tárolt adatokat, hogy a kódoláshoz és a dekódoláshoz használt kulcsok soha nem kerülnek a birtokukba. Az Apple a titkosítás hatékonyabbá tételét az iOS 8 kapcsán jelentette be, míg a Google jelenleg is dolgozik a fejlesztéseken. A fentiek kapcsán fontos megjegyezni, hogy a két vállalat erőfeszítései ugyan figyelemreméltóak, de nem szabad figyelmen kívül hagyni azt, hogy az online szolgáltatások esetében a mobilokon való titkosítások nem

⁷ „Easy to learn, Easy to work, Easy to play” personal computer

⁸ Az Apple cég hordozható eszközökre kifejlesztett operációs rendszere

⁹ A Google cég által támogatott és kifejlesztett mobileszközök operációs rendszere

jelentenek automatikus védelmet. Így például az Apple iCloud¹⁰ vagy a Google Drive¹¹ által kezelt adatok, állományok ugyanolyan módon hozzáférhetőek lehetnek a hatóságok számára, mint eddig.[4]

Továbbá arról nem is beszélve, hogy a telefonról indított, a tulajdonos számlájának terhére indított mobilhívások és adatkapcsolatok költségéről. Amennyiben lopás történik, abban az esetben biztosak lehetünk benne, hogy az adatainkhoz hozzá fognak férni, amit a telefonon tároltunk. Amennyiben a telefonunkon be van állítva valamilyen védelem, az sok esetben mind feltörhető, legyen az grafikus kód, vagy PIN kód.

Aki használt már androidos mobilt, tudhatja, hogy beállítható rajta egy feloldó mintázat, amivel lezárható a telefon, de nem egy számot kell a nyitáshoz bepötyögni, hanem egy 3x3-as mátrixban a pontokat összekötve egy előre kiválasztott mintázatot rajzolni. Kutatók vizsgálták ennek a feltörési lehetőségeit, s arra jutottak, hogy az esetek 68 százalékában a teljes feloldó mintázat hiba nélkül megfejthető volt azután is, hogy a felhasználó az arcához is érintette a mobilt, úgy ahogy egy normál telefonhívás közben is. Ha a feloldó mintát csak finom érintésekkel csinálták, akkor is az esetek 30 százalékában megvolt a kód, de a valóság az mutatja, hogy az emberek ezt hüvelykujjal erősen nyomva csinálják az esetek nagy részében, ami szabad szemmel is jól látható nyomvonalat hagy a kijelzőn. Az androidos mobilok feloldó mechanizmusával 389.112 különböző kombináció van, ami jóval több, mint ami egy négy számjegyű PIN12-kóddal elérhető, s tényleg lehetetlen találgatással feltörni. Viszont az ujjnyomok szinte minden esetben legalább annyi segítséget adnak, s annyi lehetőséget zárnak ki, hogy nagy eséllyel megfejthető a minta, mielőtt a túl sok próbálkozás miatt a telefon lezárna magát. Ha valaki paranoiás és azt gondolja, hogy ennek a veszélynek ki van téve, akkor tisztítsa sűrűn mobilja kijelzőjét megfelelő törlőkendővel és tisztítószerrel. Másrészt mosson gyakran kezet szappannal, mert az leszedi a kézről a zsírt, így a kijelző nem koszolódik olyan könnyen. Egyébként sok esetben elég az is, ha valaki egy szűk nadrág zsebében hordja a mobilt, mert mozgás közben a zseb textilje leszedi a szennyeződéseket. Igaz ezzel együtt jár az is, hogy könnyen összekarcolódik a mobil kijelzője, amennyiben nincs ellátva védőfóliával.[14]

Ha már hozzáfértek adatainkhoz, akkor csak a szerencsében bízhatunk, hogy nem fognak vele zsarolni, vagy esetleg pénzért adják csak vissza, esetleg visszaélnék vele, eladják, vagy kéretlenül nyilvánosságra hozzák azokat. De az is előfordulhat, hogy a telefonunk révén férnek hozzá más rendszereinkhez, a felhőben tárolt adatainkhoz, vagy a mi telefonunkon keresztül kompromittálnak másokat, mondjuk a cégünket, amennyiben az adott telefon céges tulajdonát képez.

Egyre több vállalat ismeri fel, hogy mobil eszközök révén jelentősen fokozható az üzleti hatékonyság, azonban a biztonsági kockázatok kezelése nehézkesen megy. A egy neves víruslabor által IT szakemberek körében világszerte elvégzett felmérés megállapította, hogy a vállalatok berkein belül egyre nagyobb problémát jelent a mobil eszközök elvesztése vagy eltulajdonítása. Ebben pedig annak is nagy

¹⁰ Az Apple cég felhő alapú tárhely szolgáltatást biztosító alkalmazása

¹¹ A Google cég felhő alapú tárhely szolgáltatást biztosító alkalmazása

¹² Personal Identification Number

szerepe van, hogy az alkalmazottak nem kezelik megfelelően, vagy nem tudják felmérni a mobilbiztonsági kockázatokat, ami miatt sokszor késlekedve jelentik a mobiljuk elkallódását. A biztonsági cég statisztikái szerint az eszközlopással érintett vállalatok 19 százalékánál eredményezte az incidens üzleti adatok elvesztését, ami azt jelenti, hogy öt cég közül egy szenved el adatvesztést, ha egy vállalati mobilkészítőt eltulajdonítanak. Ráadásul az alkalmazottak egyre lassabban értesítik munkahelyüket eszközük eltűnéséről, a munkavállalóknak csupán a fele jelenti azonnal a lopást. Az alkalmazottak több mint egyharmada (38 százaléka) csak két nap után jelzi mobilkészítőjének ellopását, míg 9 százalékuknak ehhez három-öt napra van szüksége. A mobilkészítőkkel kapcsolatos lopások és adatvesztések növekvő üteme láttán nem csodálkozhatunk azon, hogy a válaszadók 52 százaléka jelezte: „jobban aggódik a mobilkészítőkkel kapcsolatban, mint a korábbi években”. 43 százalékuk még tovább ment, helyeslően azt az állítást, hogy a „mobil munkavégzés túl sok kockázattal jár”. Ugyanakkor azt is elismerték, hogy a mobilkészítők vállalati használatának sok előnye és hatékonyságnövelő szerepe van. A válaszadók több mint egyharmada az utóbbi 12 hónap legfontosabb feladatai közé sorolta a mobilkészítők integrálását. Ezzel kapcsolatban számos biztonsági kihívással szembesülnek az IT szakemberek. A problémák hatékony kezeléséhez jól megtervezett biztonsági politikára és megfelelő védelmi technológiákra van szükség.[2]

De manapság a telefont nem is kell ellopni ahhoz, hogy a rajta tárolt adatainkat megszerezzhessék illetéktelenek. A rosszindulatú kártékony mobil szoftverek korábban már, mindez végbe mehet úgy is, hogy abból a tulajdonos mit sem sejt. A rosszindulatú szoftverek, vírusok, malverek, megszerzik adatainkat és előre megadott helyre továbbítják azt. Vagy nyitnak egy „hátsó ajtót” melyen keresztül távolról manipulálható a készülék. Esetleg egy bothálózat részévé teszik és akarataink ellenére bűnözők eszközévé válik a bűncselekmények elkövetésében. A szoftverbiztonság másik problémája a rosszindulatú vírusok mellett, a hamis alkalmazások használata, melyeket a különböző app13 áruházakból szerzünk be, ami nem biztos, hogy mindig legális. Ezek a hamis alkalmazások is adatokat gyűjtenek rólunk, és tudunkon kívül megküldik azokat illetéktelenek számára.

A csalók biztonsági cégek nevével is visszaélnék, amikor hamis, teljesen haszontalan programokat próbálnak eladni az alkalmazásboltokban. Érdemes jól megnézni, hogy mire költjük a pénzünket. A hamis szoftverek egy ideje már az Android alkalmazások körében is letették névjegyüket, igaz korántsem olyan mennyiségben, mint ahogy korábban a Windows-os társaik. Ennek ellenére közbe-közbe még a viszonylag erőteljesebben ellenőrzött, hivatalos Google Play-re14 is kikerülnek ilyen programok. Biztonsági szakértők szerint a mostani esetek furcsasága, hogy a csalók - az eddigiektől eltérően - nem ingyenesen kínálták a nemkívánatos alkalmazásaikat, hanem rögtön pénzt kértek azokért. Vagyis nem várták meg még feltelepítik a szoftvert a felhasználók, hanem rögtön anyagi haszonra akartak szert tenni. A szakember szerint az ilyen jellegű csalások a jövőben egyre több problémát fognak okozni, ráadásul nem is könnyű a védekezés, különösen nem az

¹³ Applikáció

¹⁴ A Google cég Android alapú alkalmazás-áruháza

áruházak mögött meghúzódó, automatizált védelmi technológiákkal. Ezért a felhasználóknak is résen kell lenniük, és jól meggondolni, hogy milyen programot telepítenek a készülékeikre, és még inkább, hogy milyen szoftverért fizetnek. A biztonsági alkalmazások esetén érdemes mindig a gyártók oldalairól elindulni, és előbb ott szemrevételezni a valódi szoftvereket.[5]

Mivel már rengeteg olyan dolgot végzünk a telefonunkon, amihez szükséges a saját azonosításunk, pl. bankolás, e-mail fiók használata, stb. így az azonosításunkhoz használt felhasználói nevek és jelszavak is veszélybe kerülhetnek ez által.

A mobil banki alkalmazások jelentős része komoly biztonsági hiányosságokat tartalmaz, ami könnyedén a felhasználók adatainak, végső soron pénztárcájának rovására mehet. A mobil bankolás egyre nagyobb népszerűségnek örvend a pénzügyi szektor ügyfeleinek körében, így nem meglepő, hogy a bankok jelentős része már biztosít legalább iOS és Android kompatibilis alkalmazásokat a pénzügyek kezeléséhez. Azonban – hasonlóan, ahogy a webes megoldások – ezek a szoftverek is rejtegetnek kockázatokat. A biztonsági szakemberek azt javasolják a bankoknak, hogy jelentős változtatásokat eszközöljenek a mobil alkalmazásaik esetében, és szigorúbb előírásokat vezessenek be e téren. A fejlesztőknek pedig figyelniük kell arra, hogy az adatkapcsolatok mindig biztonságos csatornákon keresztül valósuljanak meg, és a készülékeken tárolt, kezelt információk oltalmazása se szoruljon háttérbe.[3]

Arról sem szabad elfeledkezni, hogy a telefonokon a felhasználók javarésze nem alkalmaz biztonsági szoftvereket. Vagy ha alkalmazza is azokat, akkor nincsenek rendszeresen frissítve. Egy téves „beidegződés” következtében, amely onnan ered, hogy a telefonok operációs rendszerei nagy többségben nem a Microsoft által készített rendszerek, hanem Android vagy iOS, netán ettől is eltérő, ezért azokra nincs vírus, tehát nem kell ilyen módon védelmi alkalmazást futtatni, sok felhasználó nem alkalmaz biztonsági szoftvert a telefonján. Ezzel végkép nyitott utat adunk a rossz-szándékú bűnelkövetők számára.

A közzé tételre került az elmúlt évre vonatkozó mobil fenyegetettségi elemzéseket. Körülbelül 4 millió rosszindulatú alkalmazást terjesztettek és használtak a kiberbűnözők, amellyel elsősorban az androidos készülékeket célozták. 2013-ban a kutatók közel 145.000 rosszindulatú mobilvírust azonosítottak, amely több mint háromszorosa az előző éves adatokhoz képest, amikor is mindösszesen 40.059 egyedi károkozót észleltek. A 2013-ban észlelt mobilvírusok 98,1 százalékával androidos készülékeket céloztak. Összesen 10 millió rosszindulatú alkalmazást azonosítottak 2012 és 2013 között. A mobilvírusok módosult verzióinak célja az adathalászat, valamint a bankkártyás adatok lopása, amelyek száma 20 százalékkal növekedett. 2013-ban 2.500 banki trójai fertőzési kísérletet azonosítottak, amelyeket sikeresen blokkoltak is. A bank trójaiak messze a legveszélyesebb mobil rosszindulatú programok a felhasználók számára. Kimutatható, hogy 2013-ban számos vírus a felhasználók pénzét célozta, amely jelentősen növelte a felhasználók pénzügyi veszteségeit. Az androidos operációs rendszert érintő támadások magas száma mögött a rendszer architektúrája, valamint egyre növekvő népszerűsége állt 2013-ban. Továbbá az elmúlt évben a banki trójaiak száma ugrott meg a legnagyobb mértékben, ugyanis 2013 elején még csak 67 ismert trójairól tudtak, míg 2013 végén ez a szám már elérte 1321 egyedi mintát.[6]

Más források adatai szerint a 2014 második negyedévben 15 millió fajta új kártevő jelent meg. Ez napi szinten 160.000 új férget, vírust és kémprogramot jelent, amelyek közül néhány sikeres akciót hajtott végre még az eBay¹⁵ és a Spotify¹⁶ ellen is. A kártevők többsége, 62,8 százaléka a statisztika alapján trójai program. Ezekben az a közös, hogy a gépekre jutásuk után „hátsó kaput” nyitnak, ami biztosítja a konkrét géphez (vagy egyre inkább okos telefonhoz) a támadóknak a hozzáférést. A második legnagyobb arányban, 7 százalékból a kémprogramok fordultak elő a három hónapos időszakban, míg a klasszikus vírusok és a férgek részesedése 2,6-2,6 százalék volt. A trójaiak közül 58 százalék volt friss termés. A legérzékenyebb Kína, ahol minden második számítógép fertőzött. A legjobban Svédország, Norvégia és Németország áll, ahol a PC-k és egyéb eszközök az adatok szerint a legbiztonságosabbak.[11]

Egy 2013 évi kutatás általánosságban megállapítja, hogy 2012-ben összességében közel 20 százalékkal nőttek a biztonsági fenyegetések, különösen látványosan emelkedett az alapvetően politikai indíttatású elosztott szolgáltatásmegtagadás típusú (Distributed Denial of Service – DDoS) támadások száma. Öröndetes ugyanakkor, hogy ugyanilyen arányban csökkent a kényszerű levelek, azaz a spamek száma. Ez utóbbiban az a tendencia figyelhető meg, hogy a kártevőket ma már nem a spamek tartalmazzák, hanem az óvatlan felhasználót fertőzött oldalra próbálják irányítani. A mobilkészülékek ellen – általánossá válásuk ellenére – ellen irányuló támadások ugyanakkor alig fél százalékát adják az összes webes támadásnak. Ezen belül viszont az Androidra írt rosszindulatú szoftverek előfordulása közel 26-szorosára nőtt 2013-ban. A webes rosszindulatú programok előfordulásának földrajzi eloszlása jelentős mértékben megváltozott 2012 során. Kína a nemzetközi lista 2011-es második helyéről a hatodikra esett vissza, míg a skandináv országok, például Dánia és Svédország 2013-ban a lista harmadik és negyedik helyét foglalta el. Az élen továbbra is az Egyesült Államok állt. Ami a spameket illeti: a legtöbb levélzet Indiából származott. Régiókból 2013-ban az első tízbe tornázta fel magát Lengyelország. Magyarország viszont javított: a 2011-es 61.helyről "erősödött vissza" 2012-ben a 68.helyre.[1]

A mobiltelefonok másik nagy sérülékenysége az átviteli út biztonságában rejlik. Az egyik ilyen probléma maga a mobiltelefon GSM17 szabvány alapú hálózata és az ott alkalmazott átviteli szabványok hiányosságai, amely kihasználásával már szinte gyerekjáték a telefonbeszélgetés lehallgatása és a telefon a háromszögellés révén történő nyomon követése.

A másik átviteli út probléma Wi-Fi, mint a vezeték nélküli internet egyik lehetősége. A Wi-Fi biztonsága kétségeket von maga után. Könnyen kompromittálható, feltörhető, az alkalmazott védelmi megoldásai kijátszhatóak.

Több gyártó Wi-Fi routerei is érintettek voltak abban a támadásban, amely során több mint 300 ezer eszközt törtek fel. A hackerek nem csak bejutottak az eszközök adminisztrációs felületére, hanem rosszindulatú módosításokat is elvégeztek

¹⁵ Internetes aukciós weboldal

¹⁶ Egy ingyenesen is használható, kereskedelmi zene streamelő szolgáltatás

¹⁷ Global System for Mobile Communication

- írja a hvg.hu. A hackerek az adminisztrációs felületre bejutva a DNS18-beállításokat módosították, ami a gyakorlatban azzal jár, hogy banki és egyéb jelszavakat ellopó szerverekre és weboldalakra tudják átirányítani böngészés közben a felhasználókat. A jelentés szerint a legtöbb érintett router vietnami, tőlünk nem is olyan messze, Lengyelországban és Ukrajnában is több tízezer feltört eszközt találtak.[7]

Az új technikával egy kis felkészüléssel pillanatok alatt feltörhetők a Wi-Fi routerek.

Egy biztonságtechnikával foglalkozó svájci cég alapítója egy olyan támadási formát fedezett fel, amivel pillanatok alatt feltörhető a legtöbb Wi-Fi router védelme. A támadó a Wi-Fi Protected Setup (WPS) eszközök gyenge, vagy egyáltalán nem létező titkosításának hála begyűjtött adatokból offline módban kalkulálja ki a jelszót. Azzal, hogy masszív támadás helyett ezt a módszert használja, a nagyobb vállalatok védelmi hálózata is átcúsúzhat.

A korábbi hackelések során nagyjából 11.000 próbálkozásra és négy órára volt szükség a PIN kód megfejtéséhez, az új módszer már a biztos jelszót adja meg néhány offline számítás elvégzése után. A jelenlegi egyetlen lehetséges megelőzési mód a WPS kikapcsolása. Ez nem nagy feladat, ha ismerjük a routerünk beállítási oldalát, mégis számos veszéllyel és kényelmetlenséggel jár a javítások elkészüléséig.[12]

A hardver biztonság tekintetében az USB19 port használata, mind adatátvitelre, mind töltés céljából óriási biztonsági kockázatot rejt a telefonunk számára, de a másik eszköz, általában PC számára is.

A biztonsági hibáknak megvan az a kényelmetlen szokásuk, hogy kiszivárognak. Az egyik biztonsági konferencián bemutatott BadUSB nevű hibának két hónap kellett ehhez. A világ most kicsit kevésbé biztonságos, ezért ajánlatos „USB-kondomot” használni. Eddig sem volt rossz biztonsági tipp, hogy ismeretlen USB-eszközt ne dugjanak a számítógépükbe. Valójában azonban senki nem tartotta be a szabályt. Az USB megkerülhetetlen szabványa a számítástechnikának, olyan, mint a szivargyújtó az autókban. Az égvilágon minden USB-vel működik. Kivételt talán csak a különutas Apple néhány eszköze jelent, de még az ő laptopjain is ott a csatlakozó. A szabvánnyal egy baj van: az eszközökben használt elektronika vezérlőkódját át lehet írni úgy, hogy egészen ijesztő dolgokat csináljon. Gépelhet, kódot telepíthet, átveheti az uralmat a gép felett. A pendrive, amelyet most aggódva a kezében szorongat, nem egy olyan doboz, amelybe bele lehet dobálni a munkához kellő fájlokat, hanem egy kis számítógép.[13]

Az okos mobileszközök alkalmazása a közsférában

A mai információs korszakban, egyre többen hordjuk magunkkal az irodánkat, telekommunikációs eszközök formájában. Ott lapulnak zsebeinkben, táskáinkban, természetesnek tűnik jelenlétük, a klasszikus kommunikáció mellett céges információkat szinkronizálunk, olvasunk, letöltünk - legyenek ezek kimutatásokat, forgalmi adatokat, szerződéseket - tesszük mindezt folyamatos aktualitásban legyünk, az irodai környezeten kívül is. A felhasználói szabadság érdekében, terje-

¹⁸ Domain Name System

¹⁹ Universal Serial Bus

dőben a nézet, hogy a felhasználók választják meg használati készülékeiket, illetve már meg lévő készüléküket vonják be a vállalati környezetbe. Ennek következménye a heterogén eszközpark, amelynek kezelése is óriási kihívás az ezt működtető osztályoknak.[15]

Napjainkban az üzleti alkalmazások széleskörű alkalmazása lehetséges a mobil eszközökön, pl. a munkavégzést igazoló munkalap rögzítő alkalmazások használata, vagy rendelések felvétele. Az ilyen jellegű alkalmazások használatával nő a hatékonysága. Az adatfeldolgozás rendkívül felgyorsulhat, csökkenthető a hibás adatbevitel lehetősége. A mobil eszközök integrációja akkor lehet sikeres, ha a felhasználói élmény nem csökken és a cég adatai is biztonságban vannak. Olyan megoldást kell választani, amihez nem szükséges lépten-nyomon a név és jelszó megadása, hanem az azonosítást tanúsítványok alkalmazásával lehet megvalósítani. Az intranet eléréséhez elegendő egy biztonságos böngésző elindítása, amely képes titkosított csatornán kommunikálni a tűzfal mögött működő kiszolgálóval. A céges dokumentumtár eléréséhez ne kelljen a teljes hálózatra nyitott VPN20 elérést felépíteni. A céges erőforrások eléréséhez szükséges beállítások pl. a Wi-Fi, VPN, levelező rendszer, automatikusan beállításra kerüljenek. A megoldás rugalmasan kialakítható az integrált szabályrendszer segítségével automatikusan biztosítja a felhasználók számára a céges adatvagyon és erőforrások biztonságos elérését. Üzemeltetői beavatkozás nélkül gondoskodik arról, hogy a szabályrendszernek nem megfelelő eszközökről eltávolításra kerüljenek a cég által publikálásra került alkalmazások és adatok. Lehetővé teszi az alkalmazás és adat konténerizációt, vagyis biztosítja, hogy az üzleti adatok titkosítva és a magánjellegű adatoktól elkülönítve tárolódjanak az eszközökön és csak az általunk engedélyezett alkalmazásokkal lehessen hozzájuk férni. A mobil eszközök alkalmazására szabott üzleti folyamatokkal, valamint azzal hogy a dolgozók mobilitását támogatjuk és számukra kedves munkaeszközt biztosítunk, jelentősen növelhetjük a termelékenységet és nem utolsósorban a dolgozói elégedettséget.[9]

A gazdasági szektorban már elterjedt mobil megoldások lehetőségeit a közigazgatási szektor is próbálja alkalmazni. Ami az egyik esetében jól működik, a másik miért ne vehetné át annak alkalmazási lehetőségét. Viszont akadnak problémák. Míg az vállalati szektorban nincs megkötés a beszerzéseket és a fejlesztéseket illetően, annak kizárólagos határát a pénzügyi lehetőségek és a cég szükségletei korlátozzák, addig a közzsféra esetében a nagyon gondosan megtervezett költségvetés, a jogszabályi előírások, és nem utolsósorban a közbeszerzési eljárás lefolytatása lassítja, vagy esetleg akadályozza meg a szükséges fejlesztések, beruházások megindítását, lefolytatását. De szerencsére, látszik az, hogy azért a felsorolt nehézségek ellenére az állami szektorban is megindultak a mobilitás irányába az első lépések, a szolgálati laptopok, tabletek, okos telefonok beszerzésével és alkalmazásával. Habár még a vezeték nélküli hálózatok, annak sebezhetősége okán, a közigazgatásban még nem elterjedt, viszont az előfizetéses internetről elérhetőek különböző közigazgatási weboldalak, munkahelyi elektronikus levelező rendszerek. Láthatjuk, hogy ezeknek az eszközöknek az alkalmazását is szabályozni és felügyelni kell. Ezekre a feladatokra gazdasági életben már alkalmazott MDM, azaz

²⁰ Virtual Private Network

Mobile Device Management, megfelelő megoldás lehet. Továbbá, már számos helyen lehetőség adódik a belső e-mail fiók szinkronizációjára a saját tulajdonú okos telefonok esetében, ami már a BYOD, azaz Bring Your Own Device, mint alkalmazási lehetőség bevezetése felé vezető út.

Mi az az MDM?

Az MDM (Mobile Device Management) a mobil eszközök és a rajtuk tárolt információk, alkalmazások, illetve a kommunikációs folyamatok központi, távoli védelme, flottában történő menedzselése.

Az MDM fő funkciói

Üzembe helyezés: a készülék beszerzése, üzembe helyezése, cégprofil kialakítása, a device management rendszerhez csatlakoztatása távolról (OTA – Over The Air).

Távoli közczynmenedzsmnt napi szinten: alkalmazás-menedzsmnt, távsegítés, hibaelhárítás, eszközvédelem, törlés, zárolás, biztonsági előírások betartatása.

Adatbiztonság: biztonsági mentések, telepített szoftverek nyilvántartása, készülék-beállítások követhetősége, készüléktartalom - tárolt adatok és beállítások - gyors visszaállítása.

Jelentések készítése az üzemeltetésről, felhasználásról.

Az MDM előnyei a felhasználók számára

- A munkatársaknak az esetek nagy részében nem kell a vállalat IT helpdesket személyesen felkeresniük
- Nem kell időt tölteniük a készülék karbantartásával, így hatékonyabban végezhetik a munkájukat

Az MDM előnyei a vállalat és az üzemeltetés számára

- Nagyobb hatékonyság a mobil alkalmazások, illetve a naprakész információk rendelkezésre állásával
- A vállalati mobilkészülékek központonlag pro-aktívan menedzselhetők
- Nagyobb IT biztonság
- Rövidebb telepítési idő
- A támogatásra fordított idő csökkenthető
- Alacsonyabb üzemeltetési költségek
- Hatékonyabb eszköz- és alkalmazás- menedzsmnt (pl. alkalmazások tömeges implementálása)
- A készülékeken futó alkalmazások kontrollja
- Gyors problémamegoldás, hibaelhárítás.[15]

Egy, a mobilkészülékek felügyeletére (MDM) létrehozott biztonsági politika, amely integrálódik a meglévő végpont-biztonsági szoftverrel, hatalmas értéket képviselhet a mobilbiztonsági kihívásokkal szembesülő IT szakemberek számára. Ha ugyanazon a konzolon történik az MDM politika megvalósítása és más végpontbiztonsági szoftverek kezelése, a rendszergazdák minden egyes alkalmazott esetében egyedi módon szerezhetnek érvényt az előírásoknak.[8]

A BYOD

A saját eszközök vállalati infrastruktúrában való használata – ún. BYOD, azaz bring your own device – évek óta az egyik leggyakrabban emlegetett jelenség a

vállalati IT-szakemberek körében. A hazai szervezetek többsége azonban még mindig csak részben vagy egyáltalán nem gondoskodik arról, hogy biztonságossá tegye a privát vagy vállalati tulajdonú mobil készülékek használatát a vállalatban belül. Pedig a megfelelő eszközök és intézkedések bevezetése nem csupán biztonságossá, de egyszerűbbé és hatékonyabbá is teszi a mobil munkavégzést. Az alábbi lépések és megoldások javasoltak az átfogó BYOD stratégia kialakításához:

1. Oktassuk a felhasználókat!

A biztonságos BYOD stratégia egyik alappillére, hogy a vállalat vezetői és alkalmazottai egyaránt tisztában vannak a saját eszközök használatából eredő veszélyekkel, illetve a különféle biztonsági intézkedések okaival. Folyamatosan oktatni kell a felhasználókat az újonnan felmerülő fenyegetésekről is. Bizonyos időközönként pedig érdemes tesztelni az alkalmazottak tudását és reakcióit.

2. Tartassuk be a hozzáférés-felügyeleti házirendeket!

Meg kell győződni arról, hogy csak a megfelelő személyek és eszközök számára biztosítsunk hozzáférést a cég adataihoz és alkalmazásaihoz! Ne engedjük, hogy egy adott okos telefon vagy táblagép elérje a vállalati erőforrásokat.

3. Felügyeljük a mobilról történő hozzáféréseket!

Gondoskodni kell a nem szabványos készülékekről elért és használt vállalati információk felügyeletéről. Külön beállításokat alkalmazhatunk többek között olyan esetekre, amikor az alkalmazottak távoli helyről dolgoznak az adatokkal. A céges fájlokat soha ne a készülékre mentse a rendszer, így biztonságban maradnak az érzékeny adatok.

4. Használjuk a SIEM²¹ megoldások monitorozási képességeit!

A biztonsági információ- és eseménykezelő (SIEM) rendszerek segítségével monitorozható minden eszköz, amely hozzáfér a vállalati erőforrásokhoz, így azonnal felhasználható, személyazonosságokhoz köthető és szükség esetén auditálható információkat kapunk.

5. Terjesszük ki az eszközfelügyeletet a mobilkészülékekre is!

Ha az alkalmazottak az okos telefonokat és a tableteket ugyanúgy használják napi munkájukhoz, mint az asztali számítógépeket, akkor ezeket a mobilkészülékeket ugyanúgy kell felügyelni, mint a biztonságos vállalati infrastruktúrában belül található eszközöket.

6. Titkosítsuk az érzékeny adatokat!

Célszerű titkosítva tárolni minden olyan, nem szabványos eszközön tárolt adatot, ami céges tulajdonnak számít, beleértve az alkalmazottak vállalati e-mail üzeneteit. Így akkor sem kerülnek illetéktelen kezekbe a céges információk, ha elveszítik vagy ellopják a készüléket.[16]

Egy mobil biztonság vizsgálata ál-Wi-Fi hotspot alkalmazásával.

A WLAN²² képes mobileszközeinket előszeretettel használjuk olyan környezetben, ahol az internetért nem kell fizetni. Ez a felhasználói magatartás teljesen természetes. Senki sem az ellensége saját zsebének, ez esetben az internet előfizetésben szabott kvótájának, persze, ha rendelkezik ilyen szolgáltatással. Magyarorszá-

²¹ Security Information and Event Manager

²² Wireless Local Area Network

gon is, mint általában a Világon mindenhol, egyre több és több az ingyenes Wi-Fi elérési lehetőség, melyet úgynevezett hotspotok biztosítanak.

A hotspot

A hotspot általában nyilvános vezeték nélküli internet-hozzáférést biztosító szolgáltatás. Általában a hatótávolsága megközelítőleg 50 méter. A hotspotot szolgáltatását mindenki használhatja, ha rendelkezik olyan mobil eszközzel, aminek van Wi-Fi adaptere. Az internet elérése lassan már az alap emberi jogok közé is fog tartozni, azaz mindenkinek joga van az internet infrastruktúrájának használatára. Ezt szolgálja egyre több telepített, a közjót szolgáló nyilvános hotspot. Először kereskedelmi és vendéglátóhelyeken kerültek telepítésre, majd egyre több közforgalmú helyen. Ezek a hotspotokon keresztül általában ingyenesen lehet az internetre csatlakozni, de előfordul, hogy a csatlakozást valamilyen feltételhez kötik. Ez a feltétel lehet a fogyasztás függvénye, vagy egy emelt díjas SMS23-sel aktivált időkorlátos csatlakozás. Ezen kívül még az üzemeltetők alkalmazhatnak egy úgynevezett captive portált, amely egy speciális szoftver, mely a routeren vagy egy külső gépen fut és kezeli a hozzáféréseket. Ezzel biztosítva a jogosulatlan felhasználók kiszűrését. A captive portál lényege, hogy a böngésző addig nem tölt be a bejelentkezési lapon kívül mást ameddig a felhasználó nem azonosítja magát. De előfordul az is, hogy az adott hotspot nincs védve semmilyen jelszóval, vagy azonosítóval, egyszerűen csak csatlakozni kell. Ebben az esetben a felhasználó szinte korlátlan hozzáférést kap az internethez az adott hotspoton keresztül. A mobil eszközök operációs rendszerei eltárolják ezeket a csatlakozási pontokat, sőt adott esetben a jelszavakat is. Így, a legközelebbi csatlakozás esetén már nem kell azonosítania magát az illetőnek, illetve nem kell engedélyezni a kapcsolódást. Amennyiben a mobil eszköz Wi-Fi-je aktív állapotban van, akkor a rendszer automatikusan csatlakozik a hotspothoz, anélkül, hogy arról a felhasználó bármilyen tudomást is szerezne. A felhasználó csak azt látja, hogy van internet. Csak abban az esetben jut tudomására az adott hotspothoz történő csatlakozás, hogyha a menüben azt ellenőrzi.

A hackerek ezt a jóhiszeműséget és könnyelműséget kihasználva juthatnak el a mobil eszközeinkhez és a rajta tárolt adatainkhoz, vagy azon keresztül az általunk használt szolgáltatásokhoz, hogy azt mi tulajdonosok észre sem vesszük, sőt mi magunk „hagytuk azt jóvá” azzal, hogy korábban csatlakoztunk egy publikus hotspothoz.

Es hogyan teszik mindezt? Hát egy pofonegyszerű dologgal. Létrehoznak egy ál (angolul: fake) Wi-Fi hotspotot egy meglévő publikus hotspot SSID24-jának a felhasználásával.

Én magam is elvégeztem egy kísérletet, melyben azt vizsgáltam, hogy hogyan lehet ilyen környezetet kialakítani, valóban csatlakoznak-e az eszközök a fake Wi-Fi hotspothoz.

A kísérletbe a családban fellelhető mobil eszközöket, egy már nem használt Wi-Fi routeremet és egy asztali számítógépet vontam be.

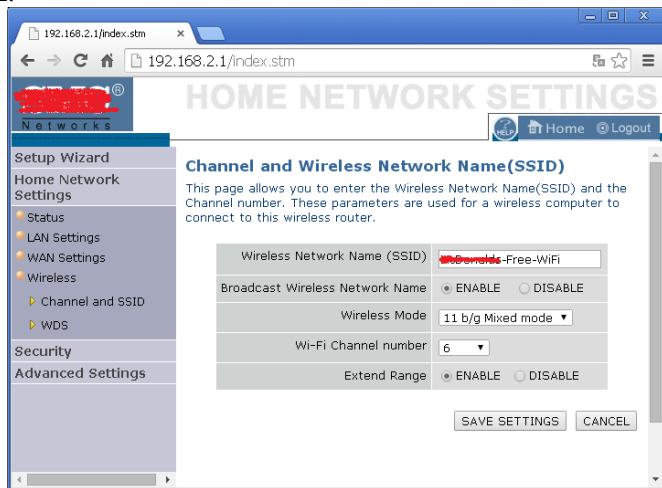
A kísérlet

²³ Short Message Service

²⁴ Service Set Identifier

Családommal és a már említett mobileszközökkel egy vasárnapi fagyaltozással egybekötött lakóhelyem, Veszprém belvárosába sétálni mentünk. A séta különböző pontjain megállva a mobileszközöket csatlakoztattuk a nyilvános hotspotokhoz. A csatlakoztatott nyilvános internet elérési pontok között volt telefonszolgáltatók által biztosított elérési pont, éttermek és kávézók elérési pontjai, valamint a városi önkormányzat által biztosított nyilvános és ingyenes Wi-Fi hotspotok. Ezeknek a hotspotoknak az SSID-ét pontosan, karakter-hűen a telefonom jegyzetömbjébe feljegyeztem. A séta végére 10 szolgáltató azonosítóját rögzítettem, amelyekhez a család mobileszközeit mind csatlakoztattuk, ezáltal azok adatbázisába ezen pontok mind bekerültek.

Amikor hazaérkeztünk, az otthoni egyik asztali számítógép és a használaton kívüli Wi-Fi routerem segítségével létrehoztam – kizárólag a kísérlet elvégzése céljából – a feljegyzett SSID-k megadásával egy-egy fake hotspotot. A mobileszközök rövid időn belül érzékelték a már „ismert” hotspotot és mind csatlakozott is hozzá úgy hogy arról engem, mint felhasználót már nem is „értésített”. Ezt több SSID alkalmazásával is megpróbáltam. Az eredmény minden esetben megdöbbentő volt. Az eszközök feltétel nélkül mind csatlakoztak a létrehozott fake hotspothoz.

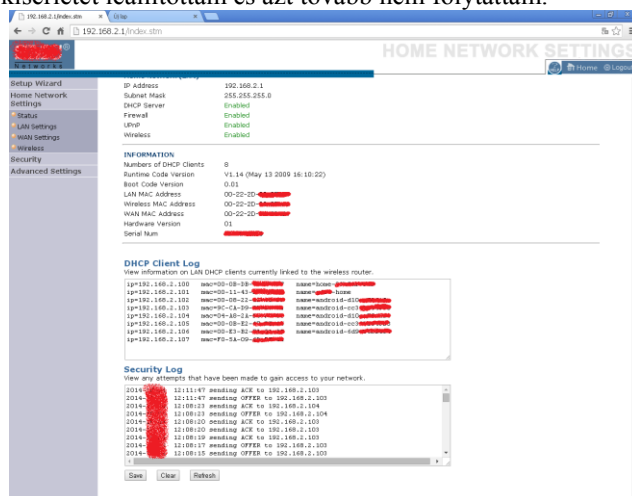


1. ábra Az ál-Wi-Fi hotspot beállítása (a szerző által készítve)

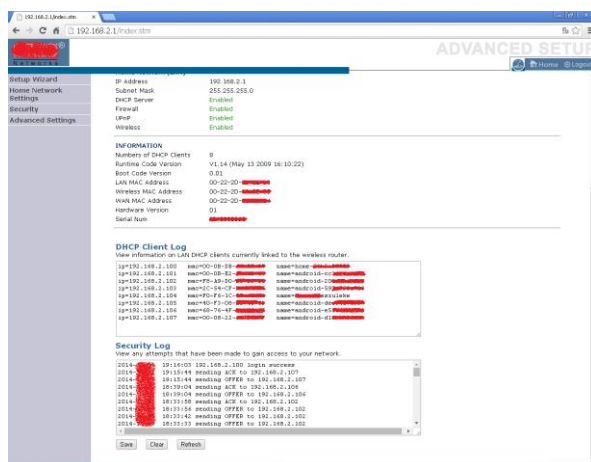
A vizsgálat következő eleme az volt, hogy lecsatlakoztam az eszközeimmel a létrehozott hotspotról, majd mindegyikben kikapcsoltam a Wi-Fi elérési alkalmazást. Majd az eszközt bizonyos időre bekapcsolva hagytam, mint ál-hotspotot. A sejtésem beigazolódtott. A népszerű, a fiatalok körében gyakran látogatott gyorsétterem-lánc helyi kirendeltségének SSID-jére társasházunk lakói közül többen is rácsatlakoztak. Tették mindezt úgy, hogy ők maguk mit sem sejtettek az egészről. A vizsgálatot követően az ál-hotspotot megszüntettem, viszont a vizsgálatot dokumentáltam mentett képernyőképek és a router log állományának mentésének formájában. Majd ezt másik 3 SSID alkalmazásával megismételtem. A begyűjtött adatok elemzése során megállapítást nyert, hogy a környezetemben élők körében az általam begyűjtött és beállított 4 hotspot közül csak egy „örvend” népszerűség-

nek. Természetesen a fenti vizsgálatom csak abban az esetben működőképes, hogyha az adott eszköz éppen nem csatlakozik egy Wi-Fi hálózathoz sem.

A vizsgálat bebizonyította az elméletet, miszerint ha a mobilkészülékkel egyszer csatlakozunk egy nyílt Wi-Fi hotspothoz, és nem töröljük később az adatállományból ezt a tételt, akkor a telefon, ha nincs másképp beállítva, automatikusan csatlakozik minden olyan Wi-Fi hotspothoz, amelyik SSID-ja fellelhető az adatbázisában. Vizsgálatom kizárólag ennek a ténynek a megállapítására szolgált, a begyűjtött információk kizárólagosan a hipotézis alátámasztásául szolgálnak. Azokkal semmilyen formában nem éltem vissza. A nem saját eszközök csatlakozását követően a kísérletet leállítottam és azt tovább nem folytattam.



2. ábra A saját eszközök csatlakoztatása (a szerző által készítve)



3. ábra Az idegen eszközök csatlakozása (a szerző által készítve)

De a megszerzett MAC címmel, annak klónozásával is visszaélések követhetők el. Például ismerve az elmúlt időszakban elkövetett és felderített rendszerfeltöréseket, azt lehet tudni, hogy az elkövetők úgy jutottak be a különböző rendszerekbe, hogy kulcspozícióban lévő személyek adatait szereztek meg. Azt felhasználva, azzal visszaélve jutottak be a kiszemelt rendszerbe, ugyanis ezek a személyeknek szinte korlátlan jogosultsággal rendelkeztek az adott hálózatban és azok erőforrásai felett. [17] Ezeket ismerve, könnyen megállapítható, hogy ha egy felsővezető céges, vagy szolgálati okos telefonját ilyen jellegű támadás éri, akkor az adott felsővezető céges rendszerébe történő behatolás már idő kérdése.

MAC Address Lookup

Enter any MAC address, OUI, or IAB below to lookup the manufacturer, location, and more

Where can I find my MAC Address?

MAC Address Details

Company	Apple
Address	Cupertino CA 95014 UNITED STATES
Range	F0:F6:1C:00:00:00 - F0:F6:1C:FF:FF:FF
Type	IEEE MA-L

MAC Address Lookup

Enter any MAC address, OUI, or IAB below to lookup the manufacturer, location, and more

Where can I find my MAC Address?

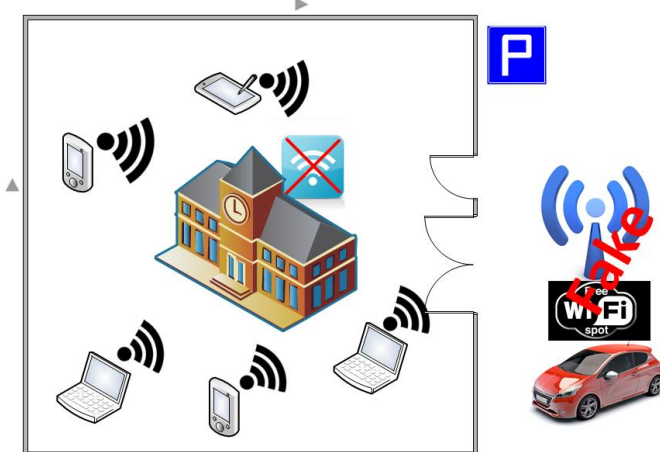
MAC Address Details

Company	Sony Mobile Communications AB
Address	Lund SE 221 88 SWEDEN
Range	68:76:4F:00:00:00 - 68:76:4F:FF:FF:FF
Type	IEEE MA-L

4. ábra A MAC cím beazonosítása a www.macvendorlookup.com oldalon (a szerző által készítve)

A vizsgálatot követően, az adatok elemzésével a következőket tudtam megállapítani:

A mobileszközök a csatlakozáshoz minden esetben a router részére megadják a saját MAC25 azonosítójukat, ha be van állítva, akkor a nevüket, valamint androidos eszköz esetében azt, hogy azon Android rendszer fut. A csatlakozó eszközről ezek az adatok a router log állományában tárolásra kerülnek. A MAC cím első hat karakteréből beazonosítható az adott eszköz gyártója. Az ál-hálózathoz csatlakozott eszközökhöz, a megszerzett információk birtokában én képes lehettem volna egy hálózati adatelemző szoftver alkalmazásával kideríteni, hogy az adott eszköz milyen irányba kommunikál és milyen típusú adatokat küld vagy kap. Képes lettem volna az eszközön tárolt, megosztott fájlokhoz hozzáférni, beállítástól függően azokat törölni vagy felülírni. Ezeken túlmenően egy hacker szinte bármire képes lehetett volna és adott esetben képes is. Képes az adatforgalmat figyelni, manipulálni. Képes az eszközt feltörni, arra rossz-szándékú szoftvereket juttatni, azokat futtatni. Képes „hátsó kaput” nyitni, és ezzel az adatokhoz hozzáférni, ezáltal azokkal már azt tud csinálni, amit csak akar. Továbbá, botnet részévé tudja azt tenni az eszközt és ezt követően a csatlakoztatott eszköz máris önmaga követ el bűncselekményeket, úgy hogy a tulajdonos arról mit sem tud.



5. ábra Ál-Wi-Fi hotspot működése „Wi-Fi szegény” környezetben (a szerző által készítve)

Amennyiben az ál-hotspot egy olyan környezetben kerül kialakításra ahol maga a környezet „Wi-Fi szegény”, akkor egy ilyen módszerrel szinte az összes, a hatáskörébe kerülő mobileszköz csatlakozni fog az ál-hálózathoz. Elegendő egy kiszemelt helyszín közelében parkoló autó akkumulátoráról működtetett Wi-Fi router. A hackernek elegendő a hatótávolságban tartózkodnia és egy mobiltelefon segítségével menedzselheti az ál-hálózatot. Ilyen helyszínek általában azok a közigazgatási intézmények lehetnek, amelyek esetében erőforrás hiányában nincs, vagy egyszerűen biztonsági okokból tiltott a Wi-Fi hálózat kiépítése, alkalmazása. Viszont ezeken a helyszíneken is sok embernek bekapcsolt állapotban van a telefonján a Wi-Fi, valamint, mint ahogyan azt az írásomban is említettem, a közigazgatásban

²⁵ Media Access Control

is egyre terjed a vezetői szinteken a céges/szolgálati okos telefonok alkalmazása. Ennek ismeretében a védelmi megoldások alkalmazása során a szabályozás kérdése rendkívül fontos, viszont egyre jobban látszik a felhasználók – képzés és tájékoztatás útján történő – biztonság tudatosságának a növelése.

Összegzés

Látható, hogy okos mobileszközök sérülékenységei mennyire figyelemre méltóak, főleg akkor, hogyha nem csak a magánjellegű adatokat tároljuk rajta, hanem a vállalati adatokat is. Ezért elengedhetetlen egy olyan lehetőség alkalmazása, amely a közigazgatásban bevezetendő okos eszközök távfelügyeletét biztosíthatja a kor színvonalának megfelelő elvárások teljesítése mellett. A bemutatott, egy általam lefolytatott kísérlet is azt erősíti, hogy mennyire védtelen még mindig a vezeték nélküli technológia. A „mobilizáció”, ahogyan a jelentünket, úgy a jövőnket is nagyban fogja befolyásolni, nem csak a munkahelyünkön, de magánéletünkben is.

Irodalomjegyzék:

- [1] Bitport – Kulcsszerepbe kerülnek az MDM alkalmazások, 2013.03.08.
<http://bitport.hu/biztonsag/it-biztonsag-a-joevoben-kulcsszerep-jut-az-mdm-alkalmazasoknak>, letöltve: 2014. október 5.
- [2] Kristóf Csaba – Nehezen valljuk be, ha elvesztjük a mobilunk, 2014.09.23.
<http://biztonsagportal.hu/nehezen-valljuk-be-ha-elvesztjuk-a-mobilunk.html>, letöltve: 2014. szeptember 25.
- [3] Kristóf Csaba – Sok sebből véreznek a mobilos banki alkalmazások, 2014.01.17. <http://biztonsagportal.hu/sok-sebbol-vereznek-a-mobilos-banki-alkalmazasok.html>, letöltve: 2014. szeptember 25.
- [4] Kristóf Csaba – Titkosítási háború tört ki az okostelefonok között, 2014.09.22.
<http://biztonsagportal.hu/titkositasi-haboru-tort-ki-az-okostelefonok-kozott.html>, letöltve: 2014. szeptember 26.
- [5] Kristóf Csaba – Vigyázat: hamis mobil alkalmazások terjednek, 2014.05.19.
<http://biztonsagportal.hu/vigyazat-hamis-mobil-alkalmazasok-terjednek.html>, letöltve: 2014. szeptember 15.
- [6] Prím Online – A legtöbb mobilvírus a pénzünkre utazik, 2014. március 2.
http://hirek.prim.hu/cikk/2014/03/02/a_legtobb_mobilvirus_a_penzunkre_utazik, letöltve: 2014. szeptember 15.
- [7] Prím Online – Több százezer Wifi routert törtek fel - ellenőrizze beállításait!, 2014. március 5.
http://hirek.prim.hu/cikk/2014/03/05/tobb_szazezer_wifi_routert_tortek_fel_-_ellenorizze_beallitasait, letöltve: 2014. szeptember 15.
- [8] Prím Online – Az alkalmazottak késve jelentik mobileszközeik ellopását, 2014. szeptember 22.
http://hirek.prim.hu/cikk/2014/09/22/az_alkalmazottak_kesve_jelentik_mobileszkozeik_ellopasat, letöltve: 2014. szeptember 25.
- [9] Humansoft – Mi az a mobil eszközmenedzsment, http://mdm.humansoft.hu/MDM_-_Mobil_eszkozok_a_munkaban/Mi_az_a_mobil_eszkozmenedzsment.html, letöltve: 2014. szeptember 26.
- [10] Erdős Márton – Felejtsd el a Wi-Fi ac-t: Itt a 10x gyorsabb utód!, 2014. október 6. <http://pcworld.hu/hardver/felejtsd-el-a-wi-fi-ac-t-itt-a-10x-gyorsabb-utod.html>, letöltve: 2014. október 10.

-
- [11] Harangi László – Egyre több a kártevő, 2014. szeptember 24.
<http://pcworld.hu/kozosseg/egyre-tobb-a-kartevo.html> , letoltve: 2014. szeptember 26.
 - [12] T.Gábor – Egy másodperc alatt feltörik a WiFi routered, 2014. augusztus 31.
<http://pcworld.hu/kozelet/egy-masodperc-alatt-feltorik-a-wifi-routered.html>, letoltve: 2014. szeptember 15.
 - [13] Szedlák Ádám – Használjon óvszert! Minden USB-eszköz fertőzőtté válhat, 2014. október 3. http://vs.hu/magazin/osszes/hasznaljon-ovszert-minden-usb-eszkoz-fertozove-valhat-1003?utm_source=hrkrs&utm_medium=rss#!s1, letoltve: 2014. október 5.
 - [14] Dojcsák Dániel – A zsír árulja el a jelszavakat, 2010. augusztus 13.
<http://www.hsw.hu/hirek/45083/erintokepernyo-okostelefon-ujjlenyomat-biztonsag.html>, letoltve: 2014. szeptember 15.
 - [15] iNFOBEX – MDM! De, mi is ez? , <http://www.infobex.hu/hirek/mdm!-de-mi-is-ez/hu>, letoltve: 2014. szeptember 25.
 - [16] mattheus – 6 tipp a biztonságos „dolgozz saját eszközzel” stratégia kialakításához, 2014. júl. 16. <http://www.technokrata.hu/www/2014/07/16/6-tipp-a-biztonsagos-dolgozz-sajat-eszkozzel-strategia-kialakitasahoz/>, letoltve: 2014. szeptember 25.
 - [17] Az ISCD 2014 konferencián elhangzott előadások alapján, Budapest, 2014. 09. 08-09.



ENTERPRISE
GROUP

ICT
ÜZLETÁG

PLM
ÜZLETÁG

SOFTWARE
ÜZLETÁG

CONSULTING
ÜZLETÁG

Enterprise Communications Magyarország Kft.

Száz százalékban magyar tulajdonú vállalatunk 2010-ben a több évtizedes szakmai tapasztalattal rendelkező Siemens Enterprise Communications Magyarország Kft. felvásárlásával indult, és kezdetben a jogelődötől örökölt üzleti kommunikációs és rendszerintegrációs szolgáltatást kínált. 2011-től stratégiai átalakulásunkat követően Enterprise Group néven kibővített portfólióval, új üzletágakkal állunk ügyfeleink rendelkezésére.

Az Enterprise Group az innovatív informatikai és infokommunikációs szolgáltatások és megoldások egyik vezető hazai rendszerintegrátora. Üzletágaink komplex megoldásokat kínálnak az infokommunikáció (ICT), a mérnöki tervezés és termékéletrajz-menedzsment (PLM), az integrált medikai szoftverfejlesztés (Software), valamint az informatikai tanácsadás és SAP bevezetés területén (Consulting).

ICT Üzletág

Egy nyelvet beszélünk

Komplex IT infrastruktúra, IP telefónia és csoportmunkát támogató Egységes Kommunikációs megoldások (UCC)

Komplex infokommunikációs megoldásainknak és innovatív, piacvezető Unify technológián alapuló Unified Communications & Collaborations, IP telefónia, illetve Call Center szolgáltatásainknak köszönhetően vállalatunk a hazai ICT piac meghatározó szereplője és szakértője.

ICT üzletágunkat a legújabb infokommunikációs trendeknek, valamint a telekommunikációs és informatikai technológiák összefonódásából eredő, egyre szerteágazóbb felhasználói igényeknek megfelelően hoztuk létre.

Üzletágunk a közép- és nagyvállalatok, illetve az állami intézmények komplex és egyedi igényei szerint állít össze speciális megoldásokat. A vállalat többi üzletágával szorosan együttműködve biztosítjuk a gyors és rugalmas üzleti működéshez szükséges informatikai struktúra teljes körű tervezését, kiépítését, bevezetését és fenntartását.

Szolgáltatásaink az alapinfrastruktúra megtervezésétől és kiépítésétől a különálló alközpontokon keresztül a globális nemzetközi kommunikációs hálózatok kialakításáig, illetve üzemeltetéséig terjednek. Jellemzően összetett és nagy rendelkezésre állást biztosító informatikai háttérrel építünk ügyfeleink üzletileg kritikus rendszerei számára, ezért nagy hangsúlyt fektetünk az adat- és információbiztonsági szolgáltatásokra.

Megoldásainkat mindig a valós igényeknek, technológiai és üzleti környezetnek megfelelően alakítjuk ki. Hazai és nemzetközi partnereink termékei pedig garantálják, hogy az üzleti folyamatokba bekerülő új elemek tökéletes összhangban működjenek együtt a már meglévő eszközökkel. Gyártói kapcsolataink mellett szakembereink több évtizedes tapasztalata biztosítja szolgáltatásaink magas színvonalát és megbízhatóságát.

ENTERPRISE COMMUNICATIONS MAGYARORSZÁG KFT.

H-1138 Budapest, Váci út 117-119. ■ Tel.: +36 (1) 471-2400 ■ Fax: +36 (1) 471-2402
info@enterprisegroup.hu ■ www.enterprisegroup.hu

CZIRÁKY Zoltán¹

NO-WIRELESS ZÓNA - AHOL TILTOTT A VEZETÉK NÉLKÜLI KOMMUNIKÁCIÓ

Összefoglalás

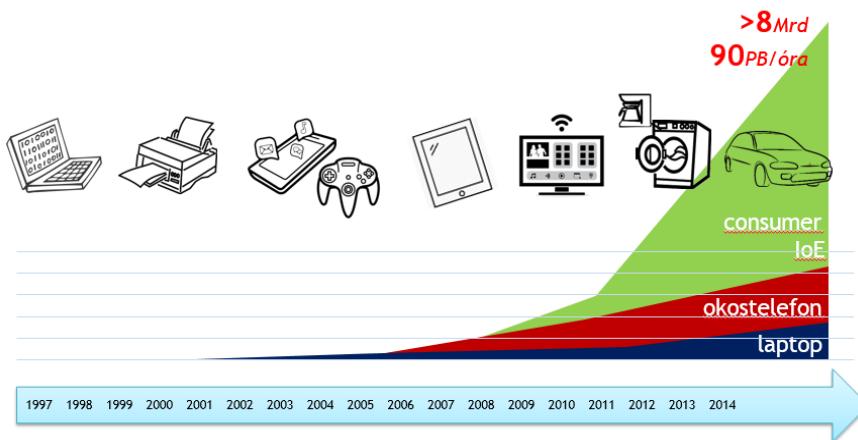
A vezetékes kommunikációs megoldásokkal ellentétben a Wi-Fi esetében a fizikai hálózati hozzáférés lényegesen egyszerűbb, ami tovább növeli a kockázatot. Nem feledkezhetünk meg továbbá azokról a kritikus területekről sem (pl. bankok, nemzetbiztonsági intézmények, büntetés végrehajtás, stb.), ahol semmilyen mobil kommunikáció nem megengedett, de mindössze táblákkal tiltják a mobiltelefon vagy Wi-Fi képes eszközök használatát. Ezek a területeken a tiltásokon túl felügyeleti monitorozó eszközökkel kell biztosítani a szabályok betartását. Előadásunkban erre mutatunk egy kézzel fogható megoldást.

Bevezetés

Ha WLAN evolúcióról beszélünk, érdemes a megvizsgálni, hogy mi történt az elmúlt pár évben és mi várható a jövőben. A vizsgálatot három területen végezhetjük:

1.) Eszközök és adatmennyiség

A WiFi szabvány megjelenését követően legelőször a vezetékes hálózati eszközökben jelent meg a WiFi technológia, a kényelmesebb felhasználás érdekében. Ilyenek voltak a hordozható számítógépek, a vezeték nélküli nyomtatók, majd később a PDA-k. Idővel a technológia olcsóbbá, egyszerűbbé vált, így begyűrűzött a háztartásokba is, megjelentek például a vezeték nélküli játékvezérlők.



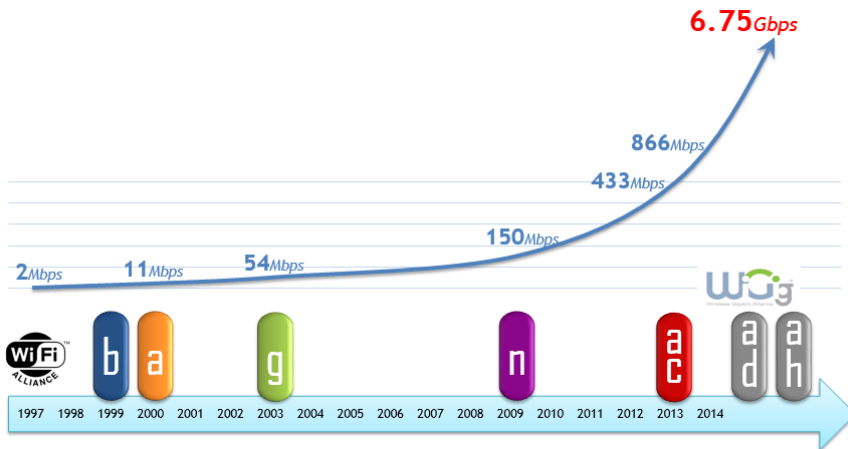
Míg 2010-ben a világon körülbelül 1 milliárd eszköz csatlakozott Wi-Fi-n, addig 2016-ra ez a szám meghaladja a föld lakosságának számát, köszönhetően az M2M (machine to machine) és az IoE (Internet of Everything) trendeknek. Csak ez utóbbi technológiák több mint 2 milliárd új Wi-Fi képes eszközt fognak eredményezni. Természetesen ezzel együtt a Wi-Fi-n továbbított adatok mennyisége is exponenciá-

¹ ügyvezető igazgató, EQUICOM Méréstechnikai Kft.

lisan fog növekedni. Ma becslések szerint 30 PetaByte a WiFi adatforgalom óránként, ami 2018-ra 90 PetaByte-ra fog növekedni, amit ha DVD lemezekre írunk ki, majd ezeket egymás tetejére halmozzuk, óránként 300-szor olyan magas DVD hegyet építhetünk, mint a Mount Everest.

2.) Sebesség és technológia

Természetesen az eszközök számának drasztikus növekedése, és az adatforgalom mennyisége megköveteli a technológiai váltásokat is. A WiFi 1997-es megjelenésekor az elméleti adatsebesség maximálisan 2Mbps volt. Ez 2010-re 75-szörösére nőtt, a mai elfogadott szabványok szerint már 400-szoros is lehet, de 1-2 éven belül a tervezett új WiFi szabványok már a kezdeti sebesség akár 3000-szeresét is tudni fogják.



3.) Felhasználási területek

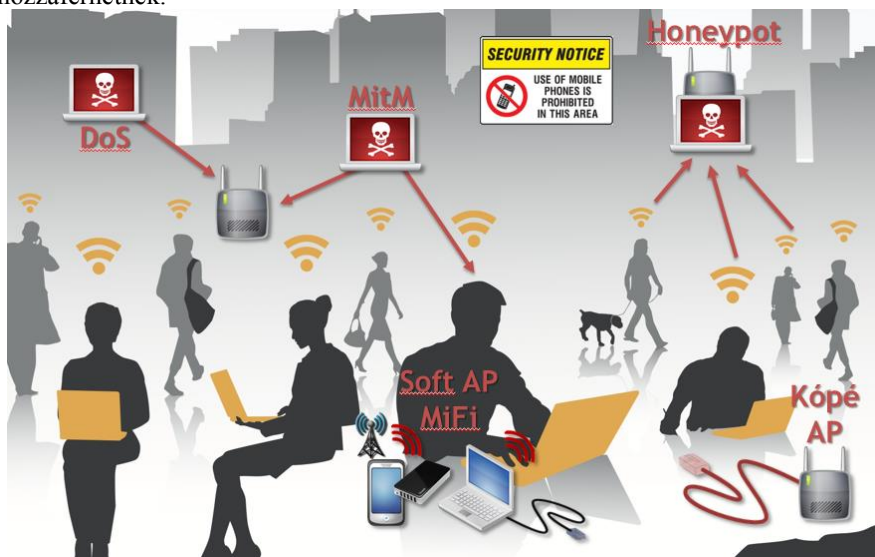
Végezetül a felhasználási területekről is érdemes pár szót szólni. Még néhány évvel ezelőtt is csak „good-to-have” státuszban volt a WiFi, azaz örültünk, ha ki tudtuk váltani a vezetékes kapcsolatot mondjuk egy tárgyalóban, vagy akár az otthonunkban vezeték nélküli megoldással. Mára eljutottunk oda, hogy a vezeték nélküli technológia egyre inkább megjelenik az üzleti életben, különféle iparágakban. Mivel üzletileg kritikus adatok továbbítása történik, igen nagy szerepet kap a biztonság és a megbízhatóság kérdése.



Biztonsági fenyegetések

Sajnálatos módon a technológia megjelenésével együtt jár a fenyegetések megjelenése is. Vezetékes hálózataink esetében a fizikai védelmen túl a kénytelen hozzáférés biztosítása egyszerűbb feladatnak tűnik, hiszen az intézményünk vagy vállalatunk néhány átjárón keresztül kapcsolódik a külvilághoz, ahol egy lineáris védelmi rendszer hatékonyan működhet. Nagy probléma ezzel szemben a vezeték nélküli hálózatok esetében, hogy az adattovábbító közeg (fizikai réteg) maga a levegő, amelyhez a fizikai hozzáférést nem tudjuk megakadályozni.

Nem véletlen, hogy sorra jelentek meg az olyan vezeték nélküli fenyegetések és támadások, mint pl. a honeypot vagy fake AP, amely egy a kliens által használt hálózatot szimulálva rábírja a felhasználókat, hogy hozzá csatlakozzanak. Innentől kezdve már csak a hacker fantáziája szab határt, hogy milyen információkat gyűjt be a kientől, például hamis belépési oldalon bekért jelszavakat és egyéb információkat. Hasonló problémát jelent a saját informatikai infrastruktúránkra csatlakoztatott hozzáférési pont is, melyet a dolgozóink előszeretettel alkalmaznak áthágva a belső informatikai szabályozásokat. Ezzel gyakorlatilag ajtót nyitnak a kénytelen támadások előtt a biztonságosan felépített vezetékes infrastruktúrát megkerülvén. Sajnos ezt már kevésbé gyakorlott felhasználók is könnyedén megtehetik egy mobil hotspot vagy un. MiFi (mobile wifi hotspot) aktiválásával. Hasonlóan kellemetlen perceket szerezhetnek az üzemeltetőknek az un. szolgáltatás megtagadási támadások (DoS), melyek közvetlen biztonsági fenyegetést nem jelentenek, azonban egy üzletileg kritikus WiFi hálózat működését ellehetetlenítik, ezzel okozva súlyos károkat a felhasználóknak. A man-in-the-middle (MitM) jellegű támadások pedig azért rendkívül kritikusak, mert akár a teljes WiFi-n továbbított adattartalomhoz hozzáférhetnek.



És végezetül nem szabad megelégednünk azokról a területekről sem, ahol tiltott a WiFi vagy akár mindenféle vezeték nélküli kommunikáció, mint pl. egy

adatközpontban, büntetés végrehajtási intézményekben, nemzetvédelmi intézményekben vagy egyetemi vizsgákon. Többségében ezeket intézményi vagy vállalati szabályozások kontrollálják, azonban ezek sok esetben nem elegendők, meg kell bizonyosodni azok betartásáról is. Hasonlóan pl. a repülőtereken, ahol figyelmeztető táblák és szabályozások korlátozzák vágó és szűrőeszközök felvitelét a repülőgépekre, de ennek ellenére detektor kapukkal és röntgen berendezésekkel vizsgálják azok betartását.

A megoldás

A hálózatmonitorozó megoldások folyamatos felügyeletet garantálnak a WLAN infrastruktúra és a kliens oldal védelmével, valós idejű és minden frekvencia sávra kiterjedő csatornavizsgálattal, azonosítással, lokalizálással és proaktív teljesítmény-optimalizálással.

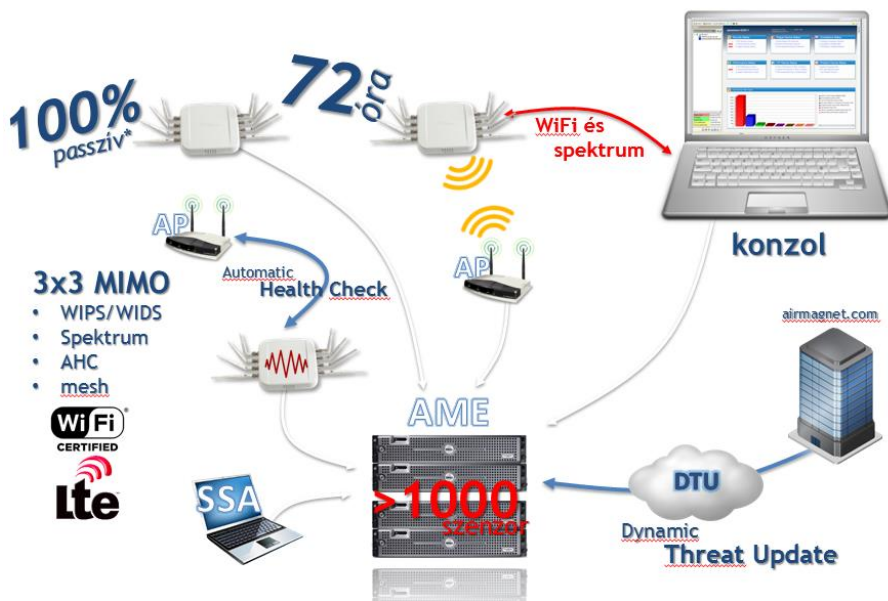
A hálózatmenedzsmentet és monitorozást sokan összetévesztik, pedig két élesen elkülönítendő területről van szó. A menedzsmentet sokszor az infrastruktúra rendszer önmagában támogatja, vagy külön NMS rendszerrel oldják meg. A monitorozó rendszer ezzel szemben céleszköz, amit nem forgalomtovábbításra terveztek. Az idő 100%-ban kizárólag a felügyelettel, forgalomanalízissal, biztonsági rések okozta károk csökkentésével, riasztásokkal és automatizált folyamatokkal foglalkozik.

Nem véletlen, hogy vezetékes hálózatok esetében is külön tűzfalakkal, forgalomszűrő eszközökkel, és egyéb dedikált megoldásokkal biztosítják a hálózat határvédelmét. Vezeték nélküli hálózatok esetében sem más a helyzet. Egy vezeték nélküli kontrollerekből és vékony hozzáférési pontokból felépített WiFi infrastruktúra tökéletes a forgalomtovábbítás kiszolgálására és a központi menedzsmentre. Azonban a vezeték nélküli határvédelemre már kevésbé, hiszen ahhoz a fizikai közeg folyamatos monitorozása és vizsgálata szükséges.

Nemhogy javasolt, egyenesen kötelező a teljes infrastruktúrát és a monitorozást külön választani, a biztonság és a teljesítmény-optimalizálás szemszögéből is. Ez utóbbit is csak akkor tudjuk hatékonyan megvalósítani, ha egy független rendszer szolgáltat adatokat arról, hogyan teljesít a hálózatunk egészében.

A Fluke Networks AirMagnet Enterprise (www.equicom.hu/ame) lefedő architektúrájú vezeték nélküli hálózat monitorozó rendszer pont ezekre a kihívásokra ad hathatós megoldást. A rendszer rendelkezik ugyan egy központi szerverrel, azonban a „tudás” és a monitorozási feladat a határterületeken lévő hardver vagy szoftver szenzorok feladata. Tehát szemben egy infrastruktúra rendszerrel, ahol az access point a kontroller nélkül csak egy hasznavehetetlen doboz, az AME esetében minden képesség és tudás a szenzorokba lett integrálva. Így ezek a központi szerver nélkül is képesek ellátni védelmi feladataikat, akár 72 órán keresztül is. Akár 3 dedikált rádió antennájával (802.11n 3x3 MIMO) képes folyamatos monitorozásra, miközben betörést hárít el, vagy hálózati performancia mérést végez. Beépített spektrum antennája alkalmas akár a mobil frekvenciák, akár nem licencelt ISM sávok folyamatos figyelésére, így a nem-wifi fenyegetések vagy teljesítmény romlást okozó RF források is kiszűrhetők. Vezetékes kapcsolat hiányában a szenzor képes az egyik antennáját MESH hálózatként használva vezeték nélkül csatlakozni. Természetesen ezek a szenzorok elérhetőek közvetlenül is tá-

volról, így a Föld bármely pontján elhelyezett szenzort úgy használhatjuk mélyebb WiFi és RF spektrum analízisre, mintha ott ülnénk mellette. Attól sem kell tartanunk, ha időközben egy újabb fenyegetés jelenik meg, hiszen a rendszer – hasonlóan a víruskeresőkhöz – automatikusan frissíti fenyegetettség adatbázisát, így mindig napra kész lesz még külső beavatkozás nélkül is.



A rendszer előnyei:

- 100%-ban passzív (kivéve AHC és betörés elhárítás), így nem detekálható, nem támadható;
- csak monitorozási feladatokat végez, forgalomtovábbításra nem használjuk;
- automatikusan frissülő sérülékenységi adatbázis;
- Layer 1-2 folyamatos monitorozása, WiFi és RF spektrum is, kiterjesztett csatornák monitorozása;
- audit a megfelelőségi és informatikai biztonsági előírások szerint (pl. Sarbanes-Oxley, HIPAA, PCI, GLBA, DoD 8100.2, ISO 27001, BASEL 2 és CAD3)
- könnyedén bővíthető, rugalmas infrastruktúra;
- hardver és szoftver szenzorok, 3 dedikált rádió antennával, spektrum analízissel.

Mivel képes a mobil és WiFi spektrumok folyamatos monitorozására is, a segítségével létrehozhatunk valódi no-wireless zónákat, ahol nem csak tiltjuk, de kontroll alatt is tarthatjuk a vezeték nélküli technológiák használatát, legyen szó akár idegen WiFi eszközökről, bluetooth berendezésekről vagy mobil kliensekről,

nem is beszélve a nem-wifi vagy nem szabványos, de a mobil frekvenciasávokban működő zavaró RF jelforrásokról.

The screenshot displays the AirMagnet Enterprise Console interface. On the left, a 'Sensors' tree lists various locations including AME-REVIEW, Charter, Colorado Springs, Duluth, GA, USA, EMEA, LAUSD, Russia, Santa Clara, CA, USA, South Africa, Sunnyvale, and Time Warner BC. The main area shows a table of 'Mobile Cellular Event Detected' alarms with columns for Source, Time, Score, and Location. A detailed alarm panel at the bottom provides specific information about the detected event.

Source	Time	Score	Location
Mobile Cellular Event Detected [3000]			
CDMA Freq: 1748.0 MHz BW: 1250 ...	10/30/2014 13:50:06	100	airmagnetent.dcloudapp.net/EMEA/UK/London/Ruslsp/EMEA_UK_Lon_Ru01_v4Cel
CDMA Freq: 1766.5 MHz BW: 1250 ...	10/30/2014 13:59:53	100	airmagnetent.dcloudapp.net/EMEA/UK/London/Ruslsp/EMEA_UK_Lon_Ru01_v4Cel
LTE Freq: 1731.6 MHz BW: 5000 kHz...	10/30/2014 13:32:22	100	airmagnetent.dcloudapp.net/EMEA/UK/London/Ruslsp/EMEA_UK_Lon_Ru01_v4Cel
CDMA Freq: 1725.7 MHz BW: 1250 ...	10/30/2014 13:05:43	100	airmagnetent.dcloudapp.net/Duluth, GA, USA/FNET Duluth/3rd Floor/GA3
LTE Freq: 1752.3 MHz BW: 10000 k...	10/30/2014 13:07:30	100	airmagnetent.dcloudapp.net/Duluth, GA, USA/FNET Duluth/3rd Floor/GA3
CDMA Freq: 1888.7 MHz BW: 1250 ...	10/30/2014 13:10:31	100	airmagnetent.dcloudapp.net/Duluth, GA, USA/FNET Duluth/3rd Floor/GA1
CDMA Freq: 1754.3 MHz BW: 1250 ...	10/30/2014 13:10:38	100	airmagnetent.dcloudapp.net/Duluth, GA, USA/FNET Duluth/3rd Floor/GA3
CDMA Freq: 1750.3 MHz BW: 1250 ...	10/30/2014 13:10:49	100	airmagnetent.dcloudapp.net/Duluth, GA, USA/FNET Duluth/3rd Floor/GA3
LTE Freq: 1753.5 MHz BW: 5000 kHz...	10/30/2014 13:17:48	100	airmagnetent.dcloudapp.net/EMEA/UK/London/Ruslsp/EMEA_UK_Lon_Ru01_v4Cel
GSM Freq: 1757.2 MHz BW: 200 kHz...	10/30/2014 13:18:58	100	airmagnetent.dcloudapp.net/EMEA/UK/London/Ruslsp/EMEA_UK_Lon_Ru01_v4Cel
CDMA Freq: 1710.1 MHz BW: 1250 ...	10/30/2014 13:49:24	100	airmagnetent.dcloudapp.net/EMEA/UK/London/Ruslsp/EMEA_UK_Lon_Ru01_v4Cel
LTE Freq: 1731.1 MHz BW: 5000 kHz...	10/30/2014 13:32:21	100	airmagnetent.dcloudapp.net/EMEA/UK/London/Ruslsp/EMEA_UK_Lon_Ru01_v4Cel
CDMA Freq: 1714.7 MHz BW: 1250 ...	10/30/2014 13:37:34	100	airmagnetent.dcloudapp.net/Duluth, GA, USA/FNET Duluth/3rd Floor/GA3
GSM Freq: 1713.5 MHz BW: 200 kHz...	10/30/2014 13:38:53	100	airmagnetent.dcloudapp.net/EMEA/UK/London/Ruslsp/EMEA_UK_Lon_Ru01_v4Cel

Alarm

Mobile Cellular Event Detected

AirMagnet Enterprise has detected a Mobile Cellular Event in the wireless environment. Communication from a Cell Phone to a Cellular Base Station has been detected. Details for the event:

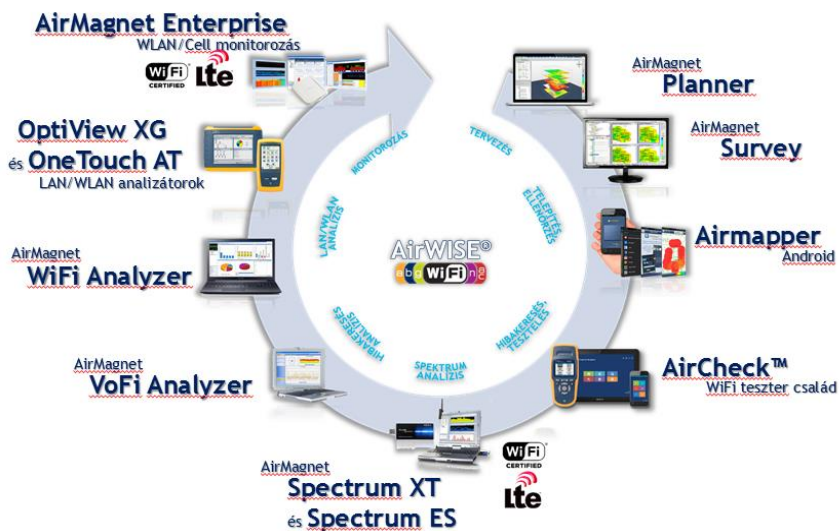
- Event Type: **Call Detected Mobile**
- Network: **DCS 1800 UP**
- Technology: **CDMA**
- Center Frequency: **1748.0 MHz**
- Bandwidth: **1250 kHz**
- Power: **-92 dBm**
- Duty Cycle: **2.11 %**

Severity	Channel	Src Device	Det Device
Urgent	N/A	N/A	N/A

Time	Sensor Name
30/2014 13:50:06	EMEA_UK_Lon_R...
30/2014 13:31:06	GA3
30/2014 12:51:45	EMEA_UK_Lon_R...
30/2014 12:44:19	GA3
30/2014 11:35:57	GA3
30/2014 10:47:52	EMEA_UK_Lon_R...
30/2014 10:24:09	GA3
30/2014 09:58:08	GA3

Konklúzió

A vezeték nélküli hálózatok sokkal inkább ki vannak téve a kérletlen fenyegetéseknek, mint vezetékes társaik. A WiFi és mobil technológia begyűrűzése az ipari és üzleti környezetbe még inkább kritikussá teszi a hálózat védelmét valamint a maximális elvárható teljesítmény biztosítását. A WLAN életciklus a tervezéssel és telepítéssel kezdődik ugyan, de a hatékony üzemeltetéshez elengedhetetlen egy átfogó, infrastruktúra független monitorozó megoldás használata. Az olyan kritikus helyeken, ahol pedig tiltott a vezeték nélküli kommunikáció, szinte kötelező annak betartatása és ellenőrzése.



Az EQUICOM-ról

Az EQUICOM Méréstechnikai Kft. 15 éve foglalkozik telekommunikációs, informatikai és kábeltelevíziós méréstechnikai megoldásokkal. Világviszonylatban is vezető pozíciót elfoglaló beszállítói innovatív megoldásokat kínálnak az adatátviteli és kommunikációs hálózatok létesítési és üzemeltetési méréséhez, analizálásához, és monitorozásához. Ez az egyedülállóan széles termékkála, a beszállítókkal kialakított hosszú távú jó kapcsolat, valamint a technológia központú szemlélet biztosítja az ügyfelek maradéktalan kiszolgálását és megelégedettségét.



Strategic Assistance and Support Group

www.strasg.hu

A Strategic Assistance and Support Group Kft. (STRASG) alapítói igazolt szakmai tapasztalatokkal bíró biztonságpolitikai és pénzügyi szakértők, akiket kreativitás, kiváló nyelvtudás, pontosság és szolgálatkészség jellemez. Lendületes csapatunk rendelkezik mindazon szakmai ismeretekkel, tapasztalattal és kapcsolati tőkével, amely lehetővé teszi partnerei igényeinek való maximális megfelelést.

A STRASG a kompromisszumoktól mentes, magas színvonalú szakértői magatartást helyezi tevékenysége középpontjába. Ez magában foglalja a vonatkozó szabályzók betartását és alkalmazását, valamint a legmagasabb etikai normáknak való megfelelést.

KÜLDETÉSÜNK

A STRASG küldetése, hogy napjaink összetett és egyre bonyolultabb nemzetközi és hazai biztonsági környezetében komplex, hiteles és etikus értékelést, elemzést és tanácsokat adjon partnerei számára. E küldetés elérésére a STRASG multidiszciplináris csapata egyedülálló módon kínál hatékony, partner-központú megoldásokat.

FELADATUNK

Egyrészt értékelni, elemezni és összegezni a jelenlegi és a jövőben felmerülő gazdasági, politikai, társadalmi, környezeti, információs és katonai biztonsági kockázatokat, kihívásokat, veszélyeket és fenyegetéseket; másrészt a fenti területekhez kapcsolódóan támogatást adni és asszisztenciát nyújtani partnereink számára.

SZOLGÁLTATÁSAINK

Kockázatelemzés és értékelés tanácsadás, stratégiai/politikai kommunikáció, szakmai programok tervezése, szervezése és lebonyolítása, biztonsági felülvizsgálatok, konfliktus- és válságkezelés, stratégiai tervezés, pályázati tevékenység és tanácsadás, üzleti partner keresés, biztonsági szűrés

HORVÁTH Zoltán¹

**AZ OKTATÁSI TEVÉKENYSÉG TÁMOGATÁSA
REJTJELEZÉST, VALAMINT ADATREJTÉST
MEGVALÓSÍTÓ PROGRAMCSOMAG
ALKALMAZÁSÁVAL**

Rezümé

Jelen cikkben a szerző arról számol be, hogy a képzés során az elektronikus információvédelem területi specialitásának megfelelően milyen számítógépes programok kerültek kifejlesztésre, melyek alkalmazása – a gyakorlati feladatok végrehajtása során – a megszerzett elméleti ismeretek gyakorlati úton történő elmélyítését szolgálja, különös tekintettel a szimmetrikus és az aszimmetrikus rejtjelezés, valamint a szteganográfia egy-egy megvalósított demonstrációja alapján.

Kulcsszavak

Szimmetrikus kódolás, aszimmetrikus kódolás, szteganográfia

Bevezetés

Az oktatás során az elektronikus információbiztonság célkitűzése és területei jól levezethető, logikailag egységes képet alkotó ismeretanyagként közölhető. Számos példa felhozható, mely alátámasztja a rejtjelezés és adatrejtés szerepét a bizalmaság, sértetlenség és rendelkezésre állás megvalósítása érdekében.

Az ismeretanyag közlését követő tanulási folyamat hatékonysága jelentősen növelhető gyakorlati feladatok megoldásán keresztül, bár megjegyzendő, hogy gyakorlati alkalmazásra a „számológépek aritmetikai képessége” enyhén fogalmazva csekély.

A hallgató az elméletben tanultakat nem tudja gyakorlati tapasztalattal alátámasztani, ismereteit megerősíteni. Ennek a problémának az áthidalhatósága érdekében született egy programcsomag, mely segítségével – szinte valós időben – tanulmányozható a szimmetrikus- és aszimmetrikus rejtjelezés, valamint a szteganográfia megvalósítása.

Ez a „játszva tanulás” lehetőségét rejtjelel magában, mikor a hallgatók önfeledten, a programok alkalmazásán keresztül gyakorlati ismereteket is szerevezve mélyítik el ismereteiket.

Ezen programcsomag az igény megfogalmazódásától az oktatásba történő alkalmazásáig mintegy egyéves kutató-fejlesztő munka eredménye.

A számábrázolás problémaköre

A hagyományos, de még a tudományos kalkulátorok között sem találhatók olyan eszközök, melyek képesek bemutatni az egyes rejtjelező algoritmusok működését. Az egyes algoritmusok megvalósítása során előfordulhat, hogy pl.: 30.000 számjegyet tartalmazó természetes szám feldolgozása válik szükségessé.

Példaként említendőn a feladat a következő, számítsa ki:

$$Y = 855^{2753} \text{ értékét!}$$

¹ adjunktus, horvath.zoltan@uni-nke.hu

Tudományos kalkulátort alkalmazna az eredmény a következő:

$$Y = 5.0432888958416068734422899127394 * 10^{8071}$$

Ez az eredmény az egyes rejtjelezést megvalósító algoritmusok szempontjából használhatatlan, mivel létkérdés az egész számok pontos ábrázolása, hatványozás és egészosztás végrehajtása, maradékképzés, primellenőrzés és kongruens számpárok keresése.

A pontos érték:

Y =

504328889584160687344228991273944666314538783600355093155549
675645
010556286120825599787442454281100543834986542893363849302464514
4...
...2474905369399277611426179640710012764328042870608353159458
230594
6326827861270203356980346143245697021484375

A mintegy 8072 karaktert tartalmazó szám (ez A/4-es méretben 2 lapot jelent) már alkalmas további aritmetikai műveletek végrehajtására.

A megvalósíthatóság egyik lehetséges módja a karaktersorozat (sztring) alapú aritmetika, mely gyakorlatilag „papíron, ceruzával tanult módszer alapján” hajtja végre az összeadást, kivonást, szorzást, osztást. Valamennyi magasabb rendű művelet ezekből az alapműveletekből származtatható.

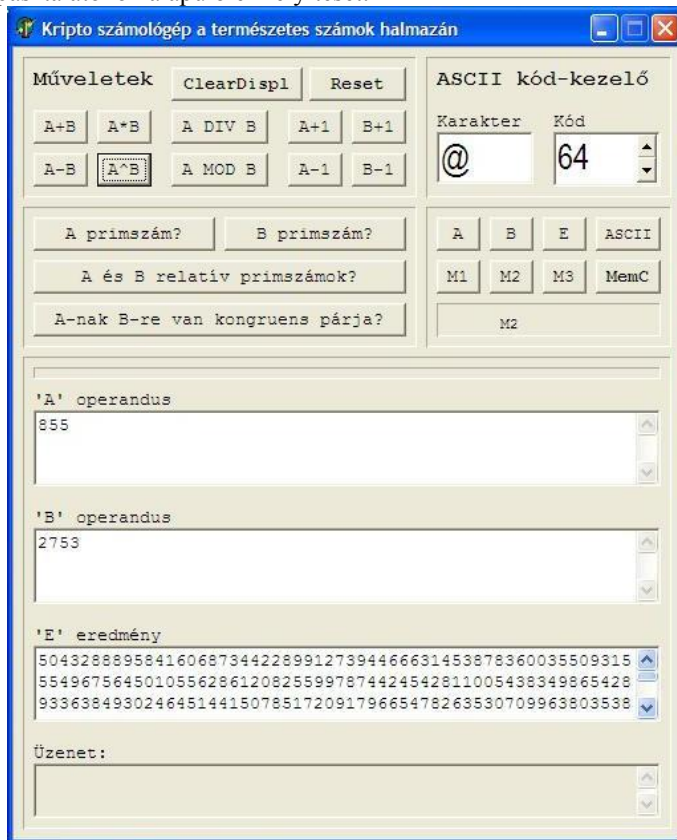
Kripto-számológép a természetes számok halmazán

A rejtjelezés algoritmusainak megértése és az ismeretek gyakorlati úton történő elmélyítése érdekében a következő funkciók kialakítása indokolt (a természetes számok halmazán).

Funkciók:

- Alapműveletek végzése:
 - összeadás, kivonás, szorzás;
 - egészosztás, maradékképzés;
 - operandusok inkrementálása, dekrementálása;
- Hatványozás;
- Primellenőrzés:
 - az aktuális operandus prímszám?;
 - az aktuális operandusok relatív prímek?;
 - primellenőrzés során (közös) szorzótényező megállapítása, ha van;
- Kongruens számpár ellenőrzése;
- ASCII kódtáblázat kezelése (kód és karakter alapján);
- Operandusok (input, output adatok), ASCII táblázat és memória közötti műveletek végrehajtása (drag and drop módszerrel).

Belátható, hogy egy kriptó-számológép felépítése és működése rendhagyó, viszont alkalmazásával a hallgatók képessé válnak egy folyamat végrehajtására (kulcsgenerálás, kódolás-dekódolás). Ez lehetővé teszi az elméleti ismeretek gyakorlati tapasztalatokon alapuló elmélyítését.



1. ábra: A kriptó-számológép képernyőképe

Szimmetrikus kódolás Polübiosz-tábla alkalmazásával

A kriptográfiában a Polübiosz-négyzet, vagy Polübiosz-tábla az ókori görög történész, Polübiosz által feltalált eszköz, amely feltördeli az eredeti szöveg karaktereit, hogy azokat egy kevesebb szimbólumból álló karakterhalmazzal fel lehessen írni.

A görög ábécé 24 betűből áll, amely mindössze egy üres rubrikával elfér egy hasonló négyzetben. Minden egyes betű, a rácsban elfoglalt helyének koordinátáival jellemezhető, például a "BAT" betűhalmaz "12 11 44" alakban írható fel (1. táblázat).

Az egyes betűk koordinátáinak karakteres helyettesítésével a kódtábla kulcsolása valósul meg.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

1. táblázat: Polübiosz-tábla²

A Polübiosz-tábla struktúráját követve kialakítható egy kibővített kódtábla, melynek elemszáma (oszlopainak és sorainak szorzata) lefedi a felhasználni kívánt karakterkészletet. A jelenlegi szövegfájlok (*.txt) karakterkészlete kb. 120 betű.

	1	2	3	4	5	6	7	8	9	W
A	0	1	2	3	4	5	6	7	8	9
B	K	L	É	Á	?	Ó	Ü	Ö	,	Ű
C	J	H	G	F	D	S	A	!	Y	Í
D	P	Ő	Ú	M	N	B	V	C	X	:
E	O	I	U	Z	T	R	E	W	Q	.
F	/	y	g	SP	x	>	{	i	o	j
G	a	#	~	<	+		w	"	\	ő
H	t	_	d	ó	@	q	(	é	f	&
I	;	k	n	b	÷	D E L	[	s	C R	}
J	e	\$	)	LF	§	l	í	c	-	p
K	...	ü	r	v	ú	z	T A B	%	ű	u
L	]	*	h	`	ö	=	m	á	^	'

2. táblázat: Kulcsolt kódtáblázat

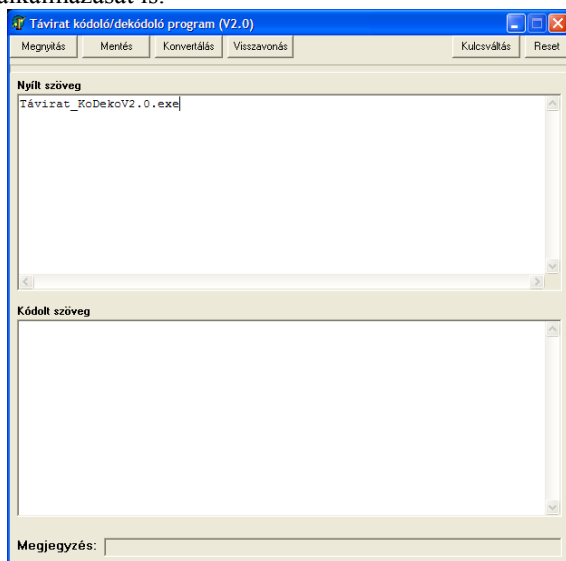
² [1] alapján

A karakterkészlet növelése magával hozza a kulcs méretének növekedését. Ez egy 10x12-es táblázat esetén természetesen 10+12 karaktert tartalmazó kulcs.

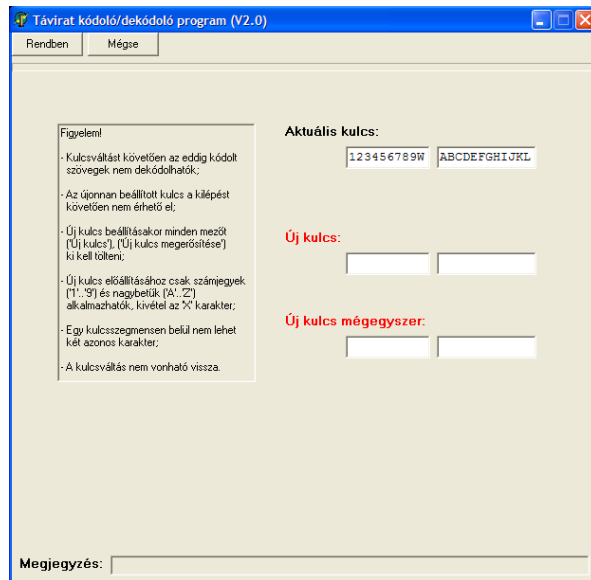
Távírat kódolása során a kódot 5-ös betűcsoportokban hozzák létre. Az utolsó betűcsoport 'X' karakterekkel kerül kiegészítésre, hogy az is 5 karaktert tartalmazzon.

A 2. táblázat alapján, a kulcsolt kódtáblázat alkalmazása során (ahol a kulcs: 123456789W-ABCDEFGHIJKL) a "BAT" távírat kódja megfelel a "D6C7E 5XXXX", a "BATU" távírat kódja megfelel a "D6C7E 5E3XX", karaktersorozatnak.

A távírat jó olvashatósága érdekében a kulcs természetesen csak nagybetűket, illetve számjegyeket tartalmazhat. Az egyes kulcsszegmensben (oszlopszegmens, sorszegmens) természetesen nem lehetnek azonos karakterek. A kulcsban a félreérthetőség elkerülése érdekében a "0" (azaz nulla) karaktert ne alkalmazzuk, mert könnyen összetéveszthető az "O" (azaz nagy o-betű)-vel. Mivel töltelékkarakter, kizárjuk az "X" alkalmazását is.



2. ábra: A távírat kódoló/dekódoló program képernyőképe



3. ábra: A távírat kódoló/dekódoló program kulcsváltó felülete

Aszimmetrikus kódolás, az RSA algoritmus alkalmazása³

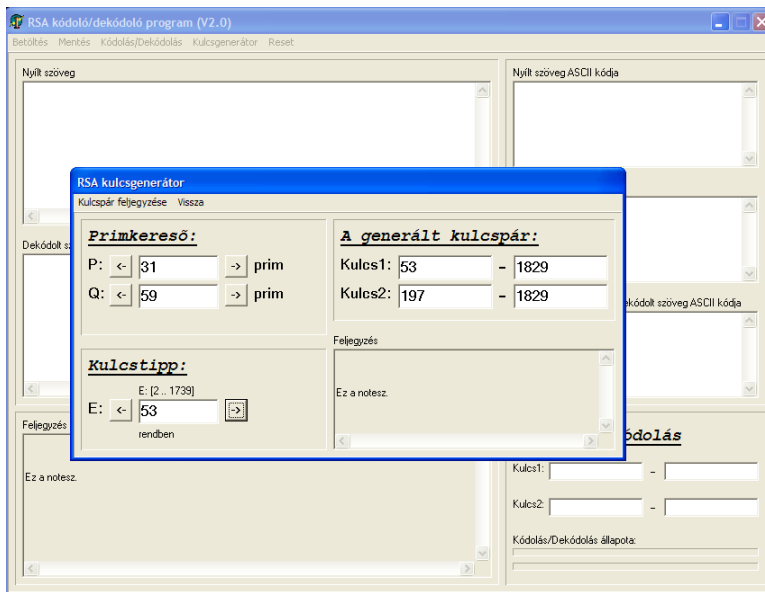
Az RSA-kódoláshoz egy nyílt és egy titkos kulcs tartozik. A nyílt kulcs mindenki számára ismert, s ennek segítségével kódolhatják mások a nekünk szánt üzeneteiket. Valamely kulccsal kódolt üzenet csak a kódoló kulcs kulcspárjával dekódolható.

Az RSA-kódoláshoz a következő módon generáljuk a kulcsokat:

- Véletlenszerűen válasszunk két prímet, p -t és q -t;
- Számoljuk ki $\{N = p \cdot q\}$ -t, N lesz a modulusa mind a nyilvános, mind a titkos kulcsnak is (a kulcs második szegmense);
- Számoljuk ki $\{F = (p-1) \cdot (q-1)\}$ -t;
- Válasszunk egy olyan egész számot $\{e\}$ -t, mely $\{F\}$ -re relatív prím;
- Válasszunk egy olyan egész számot $\{d\}$ -t, mely $\{e\}$ -vel kongruens számpárt alkot $\{F\}$ -re, azaz $\{F\}$ -nek van olyan egészszámú többszöröse, mely érték $\{e\}$ -re és $\{d\}$ -re számított modulusa $\{1\}$;
- A kulcspár ezek alapján $\{e \text{ és } N\}$, valamint $\{d \text{ és } N\}$.

Mindezek a lépések a program kulcsgenerátorának alkalmazásával egyszerűen végrehajtható (4. ábra).

³ [2] alapján



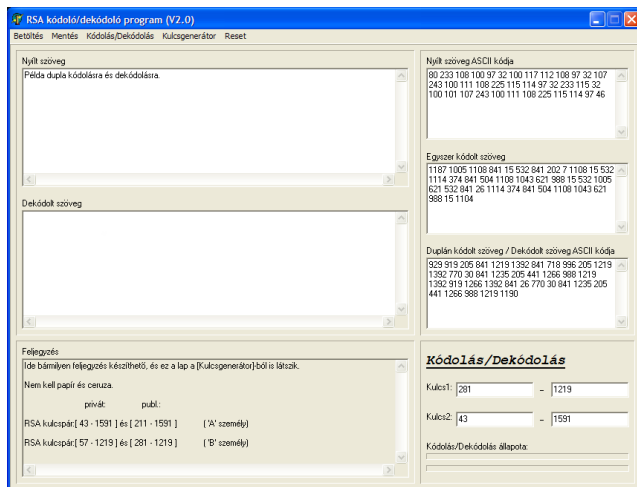
4. ábra: Az RSA kódoló/dekódoló program kulcsgenerátora

Az üzenetek kódolása és dekódolása ezt követően az alábbiak szerint valósul meg, ahol m az üzenet egy karaktere, c a kódolt karakter és $\text{mod } N$ a maradékképzés N -re:

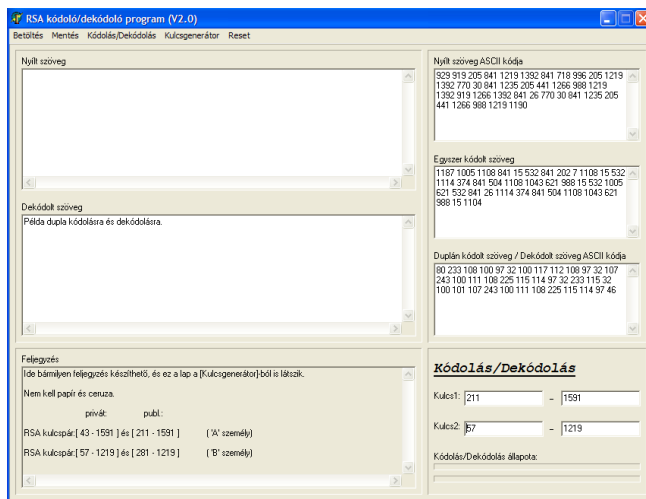
- $c = m^e \text{ mod } N$, és;
- $m = c^d \text{ mod } N$.

Az üzenetek kétszeri, két kulcspárral végzett kódolása-dekódolása képes bemutatni a hitelesség és a letagadhatatlanság problémakörét. A kódolási és dekódolási sorrend ebben az esetben viszont nem tetszőleges.

Legyen $K_1\{(e_1;N_1) \text{ és } (d_1;N_1)\}$, valamint $K_2\{(e_2;N_2) \text{ és } (d_2;N_2)\}$ kulcspárok. Kódolás során a helyes kódolási sorrendet N_1 és N_2 érkeke határozza meg. Ha $(N_1 < N_2)$, akkor a helyes kódolási sorrend először K_1 kulccsal, majd azt követően K_2 kulccsal történik. Ellenkező esetben a sorrend fordított. A dekódolási sorrend a kódolási sorrend fordítottja.



5. ábra: Példa dupla kódolásra



6. ábra: Duplán kódolt szöveg dekódolása

A program segítségével a hallgatók körbejárhatják a kulcselosztás és a nyílt kulcsú rejtjelezés problémakörét.

Adatrejtés (szteganográfia)⁴ 24 bites tömörítetlen BMP képfájl alkalmazásával

A szteganográfia nem az üzenet titkosításával, hanem elrejtésével foglalkozik. Fontos, hogy az üzenet létezéséről csak a címzett tudjon. A szteganográfia előnye a kriptográfiával szemben, hogy az üzenet nem hívja fel magára a figyelmet.

⁴ [3] és [4] alapján

A digitális adatok sok lehetőséget kínálnak arra, hogy elrejtünk valamit valamilyen. Ilyenek például a képfájlok is. Mivel nagy mennyiségű adatot hordoznak, ezért a legkisebb helyiértékű bit (least significant bit, LSB) megváltoztatása minimális torzulást eredményez a képen.

Legalkalmasabb formátum talán a BMP, amely tömörítés nélkül tárolja a képet. Például egy TrueColor (24 bites), BMP kép minden képpont leírására 3 bájtot használ. Ezek a vörös, zöld és a kék összetevő intenzitását írják le (RGB). Ha kép mérete (elhagyva a fejléceket): $1024 \times 768 \times 3 \times 8 = 18 \text{ Mbit} = 2304 \text{ kByte}$, és ha minden képpont RGB komponenseiben alkalmazzuk a legsó (LSB) biteket, a kép nem változik érzékelhetően. A rejtendő adat mennyisége így $1024 \times 768 \times 3 \times 1 = 2,25 \text{ Mbit}$, azaz $= 288 \text{ kByte}$. Ez az eredeti kép 12,5%-a. Ez tekintélyes adatmennyiséget jelent, és a fájlhossz sem változik.

A TrueColor (24 bites nem tömörített BMP képfájl három, jól elkülöníthető részből áll:

- Fájl fejléc (14 bájt). A fájlra vonatkozó alapvető adatokat tárolja;
- Információs fejléc (40 bájt). Az eltárolt kép jellemzőit írja le (felbontás, színmélység, stb.);
- Bittérkép. A kép tényleges tárolási helye, ahol képpontról képpontra jegyzik fel azok színeit (a program ezt a területet alkalmazzza).

A fejlécek a megfelelő képfájlformátum azonosíthatóságát szolgálják. Hossza állandó (14+40 byte). A fejlécek meghatározott helyein található bájtok értékei alapján meghatározható a fájlformátum (pl.: BMP), színmélység (pl.: 24 bites TrueColor), tömörítés (pl. nem tömörített). Ezek a legalapvetőbb információk. Hasznos információként egyéb paraméterek mellett meghatározható még például a képméret (kép szélessége, magassága pixelben). Ez alapján becsülhető a rejtendő bitek mennyisége.

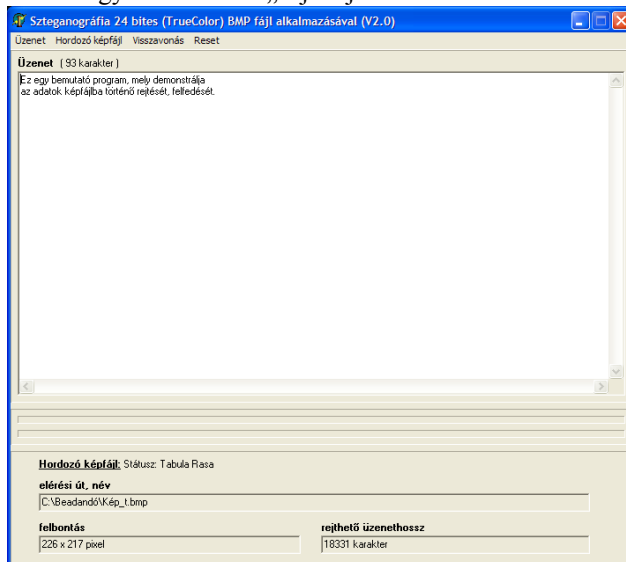
A bittérkép felépítése soronként, a kép aljától felfelé történik. Fontos sajátosság, hogy egy sort leíró bájtok száma osztható kell legyen négygel. A bittérkép felépítése során, ha ez nem teljesül, automatikusan #0 bájtokkal kerül kiegészítésre.

Például legyen egy 55 pixel széles kép. Ebben az esetben egy sorhoz 3×55 , azaz 165 bájt tartozik. Mivel ez nem osztható négygel, ezért e sorinformáció kiegészítésre kerül további három #0 bájtal ($165+3=168$, és így $(168 \bmod 4)=0$).

Tekintettel arra, hogy ezen #0 bájtok jól meghatározható helyen találhatók a bittérképben, ha ezek legalacsonyabb helyiértékű biteit (LSB) is módosítjuk, ez rögtön elárulhatja az adatrejtés tényét. Legegyszerűbb szabály ennek elkerülése érdekében, hogy a bittérkép #0 bájtjait változatlanul hagyjuk. Ennek következménye lehet, hogy a töltelék #0 bájtok mellett a bittérképben található pixel színkomponens intenzitást leíró egyéb #0 bájtok miatt csökken a képfájl kapacitása, de természetes fényképeken ezek előfordulási gyakorisága csekély.

A rejtés színtorzítása a legalacsonyabb helyiértékű bitek (LSB) módosításának hatására csekély, szemmel észrevehetetlen. Az RGB komponensek intenzitásváltozása 1/255-öd része az értékkészletnek [0..255].

Tovább csökkenti a rejtés kimutathatóságát, ha a rejtéshez nem használt RGB komponensek legalacsonyabb helyiértékű bitjeit változatlanul hagyjuk, vagy véletlenszerűen beírunk "0" vagy "1" bitekkel „zajosítjuk”.



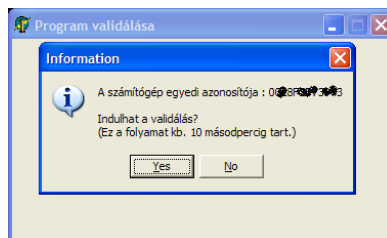
7. ábra: A szteganográfiát megvalósító program képernyőképe

A programcsomag védelme

A programcsomag programjainak (kivétel a kriptó-kalkulátor) illetéktelen felhasználás elleni védelme érdekében kialakításra került egy program. Ez bejegyzi a jogosult számítógépre másolt programba a jogosult számítógép hálózati kártya MAC-címét.

A programcsomag programjai csak a számítógép hálózati kártya MAC-címének azonosítását követően futnak (Egy nem validált másolat nem fog futni.).

Javasolt a védelmet megvalósító program közvetlen futtatása külső meghajtóról, illetve hogy erről a programról ne készülhessen illetéktelen másolat.



8. ábra: A programok futtathatóvá tétele

Összefoglalás

A szimmetrikus és a nyilvános kulcsú rejtjelezés, valamint az adatrejtés az alapja számos biztonságos kommunikációs protokoll kialakításának. A teljesség igénye nélkül említem meg a digitális aláírás, hibrid titkosítás, stb. kialakítását. Nem mellékes a kulcselosztás problémakörének körbejárása.

Bár ez a programcsomag összességében csak három (a programok illetéktelen felhasználás elleni védelme miatt négy) programot tartalmaz, a következő, alább felsorolt gyakorlati lehetőségeket tartalmazza:

- a gyakorlati tapasztalatokon keresztül akár a „játszva tanulás”, akár irányított, előre kiadott feladatok végrehajtásán keresztül az elméleti ismeretek gyakorlati elmélyítése;
- a kulcselosztás problémakörének gyakorlati megtapasztalása, a kulcs értékének felismerése;
- az elmélyített ismeretek alapján biztonságos kommunikációs protokollok kialakítása akár problémafelvető kérdés, akár irányított gyakorlati feladat végrehajtása során.

Összességében egy olyan programcsomag készült, mely a megszerzett elméleti ismeretek gyakorlati alkalmazásán keresztül képes az ismeretek elmélyítésére, és a programcsomag alkalmazásán keresztül biztosítja a biztonságos kommunikációs protokollok kialakításának megismerését.

Irodalomjegyzék

- [1] <http://hu.wikipedia.org/wiki/Polubiosz-negyzet> (2014. 05. 24.)
- [2] <http://hu.wikipedia.org/wiki/RSA-eljaras> (2014. 05. 24.)
- [3] <http://hu.wikipedia.org/wiki/Szteganografia> (2014. 05. 24.)
- [4] <http://hu.wikipedia.org/wiki/BMP> (2014. 05. 24.)



Az 1980-ban alapított ELSINCO kezdettől fogva az elektronikus mérőrendszerek és mérőműszerek marketingjére, értékesítésére és szervizére összpontosította tevékenységét, innen ered nevünk is:

ELectronic **S**ystems & **I**Nstrument **C**ompany

Cégünk, az ELSINCO Budapest Kft. a magyarországi mérőműszer piac meghatározó szereplője immár 24 éve.

Főbb üzletágaink:

Távközlés, száloptika

Nagyfrekvenciás és mikrohullámú; vezeték nélkülikommunikáció

Teljesítményelektronika, tápmegoldások

Az ELSINCO rangos világmárkák hazai, illetve közép európai képviselője.

Képviselet gyártóink:



Discover What's Possible™



Elérhetőségeink:

ELSINCO Budapest Kft.

1136 Budapest, Pannónia u. 8. IV/4.

Tel: +36/1/339-0000; Fax: +36/1/339-4444

e-mail: office@elsinco.hu, web: www.elsinco.hu

KRITIKUS INFRASTRUKTÚRÁK ÚJ FELFOGÁSÚ ELEMZÉSE

Bevezetés, Big Data/Big Bumm

1. Sok számítás nagy győzelem

A gondolat Szun Ce (Kr.e. 561-496) az egyik legnagyobb kínai hadvezértől származik. Míg korábban csak a katonai teoretikusok szűk körében volt ismert, tanításait ma már az egyre agresszívabb üzleti hadviseléshez is felhasználják.

„Korunkban úgy harcolnak a nagyvállalkozások, mint egykor a kis kínai háborúzó államocskák, és ma is az marad életben, aki terjeszkedik, befolyása, uralma alá vonja vagy megsemmisíti a vetélytársakat.”²

Ehhez pedig hosszú távon jó stratégia, rövid távon kiterjedt információszerzés – a cselekvések és dezinformációk indirekt módszere – szükséges. Magyarra fordítva:

Minél több információ, annál biztosabb siker!

A XXI. század új típusú kihívásainak rendszerében a 2001. szeptember 11-i támadások következményeképpen Európában is erőteljesebben megjelent a kritikus infrastruktúrák védelmének kérdésköre.

A kritikus infrastruktúra fogalma az utóbbi évtizedben jelent meg a hazai szakmai életben és várhatóan egyre nagyobb teret hódít a köznyelvben is. A kritikus infrastruktúrák védelme olyan komplex, magas szinten koordinált, különleges felkészülést igénylő védelmi igazgatási feladat, amelynek keretében a lehető legkörültekintőbb mechanizmusok kialakítására és működtetésére kell törekedni annak érdekében, hogy mindennapi életünk folyamatosságát biztosító infrastruktúrák üzemeltetése garantált legyen.

Annak ellenére ugyanis, hogy biztonságpolitikai szakértők szerint hazánk terrorfenyegettsége nem változott a közelmúltbeli támadásokat követően, nem szabad megfeledkezni a felkészülési illetve a védekezési óvintézkedések fontosságáról.

Az uniós törekvések is felhívják az államok figyelmét arra, hogy a terror jelentette veszélyeken kívül számos más esemény is okot ad infrastruktúránk szervezett védelmének kialakítására.

1.1 Előzmények (nemzetközi áttekintés)

Az Észak-atlanti Szerződés Szervezete (NATO) Felsőszintű Polgári Veszélyhelyzeti Tervezési Bizottság 2002 novemberében meghatározta a szövetség szempontjából meghatározó aspektusok alapján a kritikus infrastruktúra definícióját. Az SCEPC égisze alatt nyolc tervező munkacsoport és bizottság működik, amelyek feladata, hogy tanulmányozza és értelmezze az egyes szövetséges államok kritikus-infrastruktúra-védelemre irányuló intézkedéseit.

¹ Nyári László, KMDI B7I0B2/2014, lnyari@t-online.hu

² Földi Pál: A hadművészet története, Püedlo kiadó ISBN 9789632490977

Az Irányelv alapvetően egy eljárási rendet állapít meg, az európai kritikus infrastruktúrák (ECI) azonosítására és kijelölésére. Az Irányelv felülvizsgálata a jogharmonizációs tapasztalatok és tagállami alkalmazásokból származó visszajelzések alapján 2012 januárjában vehette kezdetét.

A három évvel korábban kezdődött folyamat a tervezetek elkészítését követően elérte mélypontját. A további egyeztetések, az érdekek és értékek összehangolása folyamatosan akadályokba ütközött. A tagállamok ugyan megkezdték saját nemzeti programjuk összeállítását és a sajátosságok, egyéni jellemzők felmérését, de az egységes európai kezdeményezéssel kapcsolatban nem mutattak olyan intenzív hozzáállást, mint a kezdeti lelkesedés idején. Nyilvánvalóvá vált, hogy az Európai Uniónak is szembe kell néznie azzal a ténnyel, hogy tagállamainak növekvő száma egyre komolyabb egyeztetési problémákat vet fel. A hivatalos Irányelv pontosítása során a Zöld Könyvben található, az egységes európai program véglegesítését elméletben már meghatározó, iránymutató jellegű javaslatokat sorra utasították el, vagy könnyítették a tagállamok. Az eredmény több szempontból is elkeserítő.

Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmünk javítása érdekében végrehajtandó kormányzati feladatokról szóló 1249/2010. (XI. 19.) kormányhatározat új fejezetet nyitott a hazai kritikus infrastruktúrák védelmének tekintetében.

A kormányhatározat a belügyminiszter hatáskörébe utalta:

- a nemzeti kapcsolattartó pont feladatait,
- az európai kritikus infrastruktúrák védelmével kapcsolatos kérdések koordinálását;
- az azonosítás és kijelölés folyamataihoz szükséges két- vagy többoldalú egyeztetések lebonyolítását;
- valamint a további érintett miniszterek bevonásával egy kritikusinfrastruktúra-védelmi tárcaközi szakmai munkacsoport felállítását.

A nemzeti fejlesztési miniszter feladataként nevesítette:

- a Magyarországon található európai kritikus infrastruktúrák kijelölését;
- érintettek bevonásával létre kell hozni egy konzultációs fórumot.

A kormány részére feladatul szabta az Európai Bizottság felé való éves jelentési kötelezettséget az elvégzett feladatok végrehajtásáról, a kijelölt infrastruktúrákról és az alkalmazott kritériumokról.

A kormányhatározat 4. pontja alapján tárcaközi szakmai munkacsoportot alakítottak az Irányelv végrehajtására. A kormányhatározat 8. a) pontja értelmében a nemzeti fejlesztési miniszter, a belügyminiszter és az érintett miniszterek részéről kijelölt vezetők részvételével, valamint az érintett infrastruktúra-tulajdonosok, üzemeltetők, érdekvédelmi szervezetek, tudományos testületek bevonásával Kritikus Infrastruktúra Védelmi Konzultációs Fórumot hívott össze.

A KIV Tárcaközi Szakmai Munkacsoport 2010. 11. 30-án megalakult a Belügyminisztérium (BM), Nemzetgazdasági Minisztérium (NGM), Honvédelmi Minisztérium (HM), BM OKF, Magyar Energia Hivatal (MEH), Alkotmányvédelmi Hivatal (AH), Nemzeti Közlekedési Hatóság (NKH), Nemzeti Biztonsági

³ Több mint 15 szervezet összehangolása..... nem egyszerű feladat!!

Felügyelet (NBH), Nemzeti Fejlesztési Minisztérium (NFM), Országos Rendőr-főkapitányság (ORFK), BM Terrorelhárítási Központ (TEK), Közigazgatási és Igazságügyi Minisztérium (KIM), Magyar Kereskedelmi Engedélyezési Hivatal (MKEH) részvételével, és határidős feladatot kapott az európai kritikus infrastruktúrák (ECI) beazonosításához szükséges kritériumok kidolgozására, a potenciális ECI-kre vonatkozó javaslatok kialakítására.

A KIV Konzultációs Fórum hosszú távú célkitűzései:

- magas szintű kritikusi infrastruktúra-védelmi módszertan kialakítása;
- a szabályozási feladatok tudományos igényességgel történő előkészítése;
- döntés-előkészítő fórumként való működés.

A fórum elnöke az NFM biztonsági igazgatója, tagjai az érintett minisztériumok, intézmények, valamint az energetikai, hírközlési és közlekedési szektor érintett hatóságai és szolgáltatói, illetve tudományos testületek. Az eredményesség kulcsfeltétele az érintett védelmi igazgatási szervek közötti hiteles és titkos adatok szigorú keretek közötti megosztása.

2. Amivel egyet értek

Manapság minden védelmi vezető és szakember számára egyre fontosabbá, sőt tudatossá vált a kritikus infrastruktúrák védelme.

A védelmi felkészülés egyik alapeleme a létfontosságú infrastruktúrák megóvása, terrortámadások „sorozata” kellett ahhoz, hogy egységesen felismerjük: ma már nem feltétlenül a sok áldozatot követelő támadások végrehajtása. A terrorszervezetek fő célja, hanem az, hogy minél nagyobb káoszt, általános pánikot, lehetőleg súlyos anyagi károkat okozzanak, hanem mindenképp előtte a kormányokba vetett hitet akarják megrendíteni. A folyamat akár minősített helyzet kihirdetésére is okot adhat abban az esetben, ha a helyzet eszkalálódása a kormányzat működését akadályozza. Ebből fakadóan a védelmi szféra olyan feladattal szembesült, amelyet egy-egy megközelítés, közös érdekképviselet, szigorú elvárások útján valósíthat csak meg.

2.1 Mitől lesz egy infrastruktúra (vagy annak eleme) kritikus?

Általánosságban kijelenthető, hogy kritikus infrastruktúrának mindazokat a létesítményeket és szolgáltatásokat tekintjük, amelyek sérülése, esetleges megsemmisülése súlyos következményekkel jár mind az emberek élete, mind a környezet szempontjából.

A fogalom a gazdaságtudományban jelent meg, mint olyan gazdasági feltételek (úthálózat, kikötők, közművek, műtárgyak, közoktatás stb.) gyűjtőneve, amelyek nem vesznek részt közvetlenül a termelési folyamatban, de közvetve befolyásolják a termelés fejlesztésének lehetőségeit.

A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXXVIII. törvény végrehajtásáról szóló 234/2011. (XI. 10.) kormányrendelet 1. § 25. pontja a következő definíciót adja. Kritikus infrastruktúra: „azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy

megsemmisítése, e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna”

KRITIKUS INFRASTRUKTÚRA VÉDELME

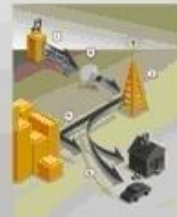
KRITIKUS INFRASTRUKTÚRÁK

Általános fogalom:

azoknak a **létesítményeknek** és **szolgáltatásoknak** összessége, amelyek bármilyen nemű meghibásodása, esetleges megsemmisülése **súlyos hatással van a környezetre, az emberi életre és vagyoniágra** egyaránt



- interdependencia
- informatikai biztonság
- üzemeltetés
- dominó-elv
- leggyengébb láncszem & rész-egész elv



kritikus infrastruktúrák fogalma, jellemzői

(Katasztrófa védelem, online: <http://heves.katasztrofavedelem.hu/a-kiv-rol-roviden>
letöltve: 2014.10.22)

Ennek analógiája alapján megkülönböztethetünk:

- műszaki infrastruktúrát az alapvető létesítmények, létesítményrendszerek, hálózatok alkotják, amelyek alapjait– létesítési és üzemeltetési feltételek képezik,
- társadalmi értelemben vett infrastruktúrát, amelyek mindazon szervezetek, létesítmények, létesítményrendszerek, hálózatok összessége, amelyek egy országon belül a lakosság szellemi és tárgyi életfeltételeit megteremtik.

Nem egy komplex elektromos ellátási rendszer a kritikus, hanem az, ha az ellátási rendszer meghibásodik és a szolgáltatását igénybe vevők helyzete negatívan változik, hiszen ez utóbbi szélsőséges esetben akár emberéletekbe kerülhet.

A fenti fogalmat az alábbi 5 alapvető tulajdonság jellemzi:

- interdependencia – egymástól való függőség,
- üzemeltetés – sajátosságok, egyedi jelleg,
- dominóelv – láncreakciószerű sérülés/károsodás,
- leggyengébb láncszem & rész-egész elv – összekapcsolódó hálózatok stabilitása a leggyengébb elem erősségétől függ,

-
- informatikai biztonság⁴ – kiemelt terület, adatbázisok és munkafolyamatok.

A kritikus infrastruktúrák védelme össznemzeti feladat kell, hogy legyen. Sikeres végrehajtásához magas szinten koordinált védelmi vezetés, normál és válsághelyzetbeli mindenre kiterjedő jogszabályi háttér, szakképzett – a kritikus infrastruktúrákat felügyelő és védelmező - apparátus és megfelelő eszközrendszer biztosíthat.

3. Amihez értek

Az EPCIP megvalósítására vonatkozóan végül 2008 decemberében született végleges döntés, ekkor látott napvilágot a kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint ezek védelmi fejlesztéseinek szükségességéről szóló 2008/114/EK tanácsi Irányelv (Irányelv), amelynek végrehajtására 2011. január 12-ig kaptak határidőt a tagállamok.

Az Irányelv célkitűzései három fő irányvonal szerint határozhatók meg,

- a *megelőzés*, (A tagállamok közötti konzultációs eljárások)
- *felkészülés*, a terrorizmus elleni harctól kezdve a mindenfajta veszélyrel szembeni védelemig,
- *ellenálló képesség kialakítása*, a felkészülés közben keletkezett hozzáadott érték beépítése az uniós védelmi programokba.

Sokáig a megelőzés, a detektálás és a visszacsatolás volt a védelem három legfontosabb alappillére, azonban napjainkban már érdemes egy lépéssel tovább haladni, ami a gyakorlatban a prediktív eljárások és folyamatok kialakítását jelenti. Vagyis a cél nem más, mint hogy a rendelkezésre álló adatok, információk alapján bizonyos valószínűséggel előre lehessen jelezni a fenyegetettségeket, és fel lehessen készíteni a proaktív védelmi vonalakat a várható eseményekre.

Amennyiben ezt jól sikerül kivitelezni, akkor a megelőzésre szolgáló biztonsági eszközök, technológiák jóval hatékonyabban lesznek képesek megakadályozni egy-egy incidens bekövetkezését

A hagyományos védelmi modellek egyre kevésbé hatékonyak a mindennapi használat során. Új fenyegetések. Új kihívások. Új célok. Válaszul, a fejlesztők folyamatosan új termékeket és technológiákat dolgoznak ki folyamatosan.

3.1 Kollektív Intelligencia

Az új „intelligens” rendszer központilag tárolja a programok viselkedési mintáit és gyűjti őket, a fájl lenyomatokat, új malware⁵ mintákat. Ezeket az információkat gyűjtik a kollektív intelligencia rendszerei az illetékes védelmi szervezetek részére. Az adatgyűjtésnek ez a kiterjedt formája pontosabb (naprakész) **észlelést és teljesebb nyomon-követési lehetőséget** biztosít az új malware technikákkal és terjesztési pontokkal összhangban.

Automatikus kategorizálás

A rendszer automatikusan analizálja és osztályozza a nap, mint nap beérkező több ezer új mintát. A rendszer összehasonlítja a felhasználói közösségből beérke-

⁴ Ez az a biztonsági terület amelynek elemzése a szakterületem

⁵ internetes fenyegetések összessége

ző adatokat a Labor kiterjedt malware adatbázisaival. A rendszer automatikusan döntést hoz - malware vagy goodware- ha új ismeretlen szerkezetű fájl érkezik⁶. Így ha elindítjuk az ellenőrzést, az tapasztalhatjuk, hogy a keresés sebessége nőtt, és minimálisra csökken az erőforrások felhasználása a védett gépeken.

4. Amit másképp gondolok

Hipotézis: A kritikus infrastruktúrák védelmével foglalkozó tanulmányok jelentős része abból a felfogásból indul ki a mely szerint a rendszereket érő támadások - magára az adott vagy érintett infrastruktúra ellen, annak elpusztítására, tönkretételére irányulnak.

Ebből a nézőpontból kiindulva a tervezett/felállított védelemi stratégiák is alapvetően magára az adott struktúrák védelmére irányulnak. Kiemelten igaz ez a kritikus infrastruktúrák védelmére.

Szerintem⁷: nagyságrendekkel fontosabb lenne az információs hálózatok védelme helyett (mellett) a forgalmazott információk, a feldolgozott, gyűjtött adatok/adatbázisok fokozott védelme!

A tönkretett vagy elpusztított struktúrákat helyreállítani vagy újraépíteni nem egyszerű de lehetséges, **az elveszett adatok információk pótlása lehetetlen!**

4.1 Egy kis történelem (inkák)

Az egyik legnagyobb (út)hálózat megtervezése, és kialakítása az Inkák nevéhez fűződik. A hálózatok építésének alkalmazott alapelvei – alternatív útvonalak, kijelölt csomópontok stb.- a mai napig is érvényesek. Eredménytelen lenne bármelyik vonalat lerombolni, hiszen a hálózat egy másik vonalát választva ugyanúgy el lehet érni a kijelölt helyre.

Az Inka Birodalomban az utak a főbb központokat kötötték össze egy rendkívül nagy kiterjedésű területen (mai Peru, Ecuador, Bolívia, Chile és Argentína egy része). Quitától Cuzcón át a mai Tucumán területéig húzódott az 5200 km hosszú Királyi út, amely a legfontosabb útvonal volt.⁸

Az utak mentén 4 km-enként futárok részére kialakított állomáshelyek voltak. A futárok szóbeli vagy csomókkal zsinórokra rögzített üzeneteket vittek. A partvonalat egy a Királyi úttal párhuzamosan haladó 4000 km hosszú út követte.

⁶ folyamatosan frissülő white list több, mint 10 millió fájl tart nyilván

⁷ alapvetően az IT struktúrák védelmére vonatkoztatva

⁸ Huayna Capac uralkodása idején az Inka Birodalom 16 000 km úttal bővült.



Az Inka úthálózat

Érdeemes elgondolkodni rajta.

A Spanyol hódítók gyors előrehaladásának, titka éppen az volt miszerint, az inkák szenzációs úthálózatát kihasználva tudtak sikeresen behatolni a föld-rész belsejébe.

Tanulság: a kritikus infrastruktúrákat elsősorban nem támadni kell, sokkal inkább a támadás eszközeként kell (lehet) sikeresen alkalmazni!

Inka úthálózat, Forrás: Inkák. online:

<http://www.doksi.hu/news.php?order=ShowArticle&id=652>

letöltve: 2014.10.23

4.2 Időzített bomba (napjaink története)

Védelmi hiba.⁹ Iránban valószínűleg az izraeliek sikeresen semmisítették meg egy szupertitkos nukleáris létesítményt. Az atomerőmű védelmi vezetője szerint a sokszorosán biztosított, több emelet mélyen kialakított létesítményben semmilyen külső támadás sem okozhat komolyabb károsodást. Az elektromos hálózat meghibásodása sem lehet gond, de a vészvilágítás tartalék hálózatába épített távirányítású bombaindító rendszer indítása ellen nincs orvosság.

4.3 Szuper kritikus „Piszkos struktúrák”

Elképzelni is nehéz milyen súlyos következményekkel járna a különböző infrastruktúrák rosszindulatú „piszkos” fegyverként való alkalmazása. A különböző terrorista szervezetek pontosan tudják milyen – az atomfegyvernél is nagyobb pusztítóbb – hatása lehet főleg a kritikus hálózatokon elindítható abnormális akcióknak.

Elég csak néhány piszkos alkalmazást átgondolni,

- Elektromos hálózat: elég csak a földvezetéket egy másik fázisvezetékkel felcserélni. Az eredmény katasztrofális, minden 220V-ra tervezett készülék azonnal leég, haszna-vehetetlenné válik.

⁹ Vince Flynn; azonos című regénye alapján

- Vízközmű hálózat: szinte a legegyszerűbben támadható! Megmérge-zése az élő szervezetek azonnali pusztításával járhat.
- Gázmű-hálózat: mérges gázzal keverve kivédhetetlen fegyver, és ma már minden területen általánosan elterjedt.

Nem folytatom, - anélkül hogy újabb tippeket adnék - még átgondolni is szörnyű lenne, milyen pokoli lehetőségeket rejthetnek a különböző infrastruktúrák az ilyen irányú felhasználása.

A felsorolt példákat elemezve, - a kritikus infrastruktúrák védelmével kapcsolatban - érdemes lenne néhány új szempontot is átgondolni. A felsorolt példák szerint: nem egy komplex ellátási rendszer a kritikus, hanem az, ha az ellátási rendszer működése hibásodik meg miáltal szolgáltatását igénybe vevők helyzete tragikusan változik, hiszen ez utóbbi szélsőséges esetben akár milliók életébe kerülhet.

Összegezve

- nagyságrendekkel fontosabb lenne az információs hálózatok védelme helyett (mellett) a forgalmazott információk, a feldolgozott, gyűjtött adatok/adatbázisok fokozott védelme!
- A tönkretett vagy elpusztított struktúrákat helyreállítani vagy újraépíteni nem egyszerű, de lehetséges, az elveszett adatok információk pótlása lehetetlen!
- A kritikus infrastruktúrákat elsősorban nem támadásoktól kell megóvni, sokkal inkább a támadás eszközeként is használható piszkos fegyverként való alkalmazásoktól!

A kritikus infrastruktúrák védelme újragondolt össznemzeti feladat kell, hogy legyen. Sikeres végrehajtásához magas szinten koordinált védelmi vezetés, normál és válság-helyzetben is érvényes mindenre kiterjedő jogszabályi háttér, szakképzett – struktúrákat felügyelő és védelmező - apparátus és megfelelő eszközrendszer biztosíthat.

Utóirat

"Az emberiség történetének legerősebb elnyomó fegyverét építjük, de az igazgatók kihúzzák magukat a felelősségre vonás alól. Keith Alexander, az NSA igazgatója hazudott a képviselőházban, amit bizonyítani is tudok. (...) A kiberhadműveletekkel kapcsolatban a kormány hivatalos álláspontja az, hogy továbbra sem állnak rendelkezésre a szükséges eljárási keretek. Ez is hazugság. Létezik egy részletes szabályozási keretrendszer, egyfajta, a kiberakciókat szabályozó marshall-törvény, amelyet a Fehér Ház dolgozott ki. Az elnök húszas számú politikai irányelvének hívják, és tavaly év végén véglegesítették. Ezt is tudom bizonyítani."¹⁰

No komment!

¹⁰ Snowden nyilatkozat, Forrás, online: <http://www.origo.hu/techbazis/20141021-snowden-fessen-celkeresztet-a-hatamra.html> letöltve: 2014.10.24

Irodalomjegyzék:

- [1] Az informatikai biztonság alapjai, ZMNE jegyzet, 2000.
- [2] Bartha Mária: Machu Picchu - Rejtély és harmónia, Pannónia Könyvek (Pro Pannonia Kiadói Alapítvány, Molnár Nyomda, Pécs, 2004) ISBN 963-9498-23-8
- [3] Endrődi István: Katasztrófavédelmi információs rendszer, Hadtudomány, XII. évfolyam, 1.szám, 2002.
- [4] Földi Pál: A hadművészet története, Püldo kiadó ISBN 9789632490977
- [5] Üveges László: A Magyar Köztársaság katasztrófa-veszélyeztetettsége és az arra adandó válaszok, PhD értekezés, 2002, IV fejezet: A katasztrófa-veszélyeztetettségre adott technikai válaszok, műszaki fejlesztés
- [6] Vince Flynn: Protect and Defend, Generál Press Kiadó, 1997. ISSN 1416-7026
- [7] Katasztrófa védelem, online: <http://heves.katasztrofavedelem.hu/a-kiv-rol-roviden>
- [8] letöltve: 2014.10.22
- [9] Inkák. online:<http://www.doksi.hu/news.php?order=ShowArticle&id=652> letöltve: 2014.10.23
- [10] Snowden nyilatkozat, Forrás, online: <http://www.origo.hu/techbazis/20141021-snowden-fessen-celkeresztet-a-hatamra.html> letöltve: 2014.10.24

TÓTH András

A NATO KOMMUNIKÁCIÓS RENDSZERÉNEK ELMÉLETI ÉS GYAKORLATI VIZSGÁLATA

Rezümé

A NATO kommunikációs rendszerét a hálózatközpontúság határozza meg, amely jelen van mind a vezetékes, mind a vezetés nélküli összeköttetéseknek egyaránt. A folyamatos modernizációnak köszönhetően a teljes rendszer lecserélésre kerül, amely eredményeképpen egy IP-alapú összeköttetéseket biztosító összetett és interoperábilis környezet kerül kialakításra. .

Kulcsszavak

Hálózat központú hadviselés, NATO Általános Célú Kommunikációs Rendszere, csomóponti rendszer, műveletirányító rendszer, műveleti helyzetkép

Bevezetés

A NATO fejlettebb hadseregekkel rendelkező tagállamai a 2002-es Csúcson meghozott döntéseket követően megkezdtek a hálózatközpontú hadviselés irányába történő fejlesztéseket. Telepítésre kerültek olyan nagy sávzsélességű gerinchálózatok, amelyek képesek öt kilences¹ rendelkezésre állást nyújtani, és biztosítani a csatlakozást a NATO informatikai gerinchálózatahoz, és ez által összekötni a hasonló hálózattal rendelkező országok hadseregeit. Ez a rendszer biztosítja mind az állandó telepítésű, mind a mobil vezetéki pontok részére az összeköttetés lehetőségét a világ bármely pontján. Az alapját egy vezetékes és mikrohullámú hálózat adja, amely kiegészítésre került műholdas kapcsolatokkal a nagyobb távolságok elérése céljából. Az állandó telepítésű rendszerek mellett úgyszintén kialakításra kerültek a NATO mobil és tábori rendszerei. A hatályban lévő szabványoknak és strukturális követelményeknek köszönhetően ezek lehetőséget biztosítanak a gerinchálózatra csatlakozás mellett a nemzeti kommunikációs rendszerekkel történő összeköttetések kiépítésére egyaránt.

A NATO Általános Célú Kommunikációs Rendszere

A NATO Általános Célú Kommunikációs Rendszerét (NGCS2) összetett rendszerek, alrendszerek és alhálózatok alkotják hang és adat szolgáltatások biztosítására. A NATO szövetségi területeken kívül történt gyors műveleti terjeszkedésének köszönhetően szükséges volt nagy és független alhálózatok kiépítésére a műveleti parancsnokságok támogatásához, valamint a honi területeken elhelyezkedő parancsnokságokhoz történő bekapcsolásukhoz. Az összeköttetéseket szolgáltatás átjárók biztosítják, melyek jól megtervezettek, fenntarthatóak és vezérelhetőek, továbbá a NATO szabványoknak megfelelő szerkezeti struktúrával és menedzsmenttel kiépí-

¹ Az öt kilences kifejezést gyakran használják a magas elérhetőségű rendszerek leírására, ami 99,999%-os működést jelent. Az öt kilences olyan rendszereket ír le, amelyek alapvetően 100%-osan elérhetőek, de természetesen néhány leállás elkerülhetetlen - http://www.tankonyvtar.hu/hu/tartalom/tamop425/0046_adatbazis_adminisztracio/ch11s02.html

² NATO General Purpose Communication System

tettek és megfelelnek a biztonsági, szolgáltatás minőségi és az interoperabilitási követelményeknek. Az NGCS négy alappillérből áll, melyek: az átvitel menedzsment, a sávszélesség menedzsment, a vonalkapcsolt rendszer és a csomagkapcsolt rendszer.

- Az átvitelmenedzsment a szolgáltatások alapja, amely az átviteltechnika rendkívül változatos és gazdag változatait foglalja magába. Ezek a szolgáltatáselemek lehetnek állandó telepítésűek, mobilak (NATO tagországok határain kívül, például missziókban bevethető), valamint tábori körülmények között a belső kommunikációért felelősek. Összességük alkotja a komplex átviteli hálót, ami magába foglalja az optikai kábeleket, rézkábeleket, műholdas és egyéb vezeték nélküli kapcsolatokat, amelyek akár teljesen független rendszereket is alkothatnak egymástól.
- A sávszélesség menedzsment vizsgál minden kiépített kapcsolatot és irányítja a kommunikációt, hogy ne alakuljon ki túlterheltség a hálózaton. Emellett biztosít egy közös hozzáférési lehetőséget a többi pillér részére (vonalkapcsolt, csomagkapcsolt) egy dinamikus és hatékony kapcsolódás eléréséhez.
- A vonalkapcsolt rendszer biztosít egy NATO szintű ISBN távbeszélő hálózatot automatikus kapcsolású alközpontok (PABX³) segítségével, amelyek összekapcsolják a belső kommunikációs hálózatot a nyilvános központon kívüli hálózatokkal. 2014-től egy projekt keretében IP alapú kommunikációs rendszerekre kerül lecserélésre. Ezáltal egy modernizált NGCS jön létre, amely teljes körben IP alapú szolgáltatásokat fog nyújtani a NATO állandó telepítésű és mobil rendszereket alkalmazó felhasználóinak egyaránt.
- A csomagkapcsolt rendszer biztosítja az IP infrastruktúrát a három al-retegen (fizikai, adatkapcsolati és hálózati), ezáltal az adatátvitelt NATO titkos és nyílt hálózatokon egyaránt.

A négy alappillér mindegyike egy különálló rendszer, melyeket összekapcsolva kapjuk meg az NGCS-t, amely kapcsolódási lehetőséget biztosít a NATO-n belül, valamint a szövetséges csapatok között azok elhelyezkedésétől függetlenül.

Az NGCS-en belül kialakításra került egy védett alhálózat, amely biztonságos kommunikációs csatornákat szolgáltat a felhasználók számára. Ez az alhálózat szintén további alhálózatokat használ az összeköttetések fenntartására. Megtalálható benne a NATO nem minősített alhálózat, amely csatlakozási lehetőséget biztosít például az internetre, valamint ezen továbbítható minden minősítés nélküli adat. Itt kerültek kiépítésre a nyilvános távbeszélő vonalak is művelési területekről ugyanúgy, mint a nemzeti védelmi hálózatokról (NDN⁴). A következő alhálózat a biztonságos IP alhálózat, ahol már védett hang- és adatvonalak kerültek kiépítésre. Itt már a NATO információvédelmi követelményeknek megfelelő kommunikáció folyik.

³ Private Automatic Branch eXchange

⁴ National Defense Network



6. ábra A NATO kommunikációs és információs hálózata

Forrás: saját

Az NGCS-en a fenti csoportok mindegyike képes kommunikálni egymással különböző csomópontok használatával. Amennyiben egy missziós csapat vagy egy harcoló alakulat számára szükséges az összeköttetés műveleti csomópontok segítségével képesek kapcsolódni egymáshoz. A műveleti csomópontok a csapatok méretétől és feladatától függően lehetnek hadászati, hadműveleti és harcászati csomópontok. Abban az esetben, ha egy tagállam egy szervezete honi területéről kíván csatlakozni úgynevezett NATO vezetési csomópontok kerültek kiépítésre ennek megvalósítására, amelyek képesek fogadni a nemzeti védelmi hálózatoktól érkező minden egyes kérést, és biztosítani a kommunikációt. Ezek a csomópontok különböző módon kerültek összekapcsolásra, nagy többségük mikrohullámú vagy műholdas linkeket használ, de vannak olyan megoldások is, ahol az NDN vonalak kerültek felhasználásra.

NATO csomóponti összeköttetések

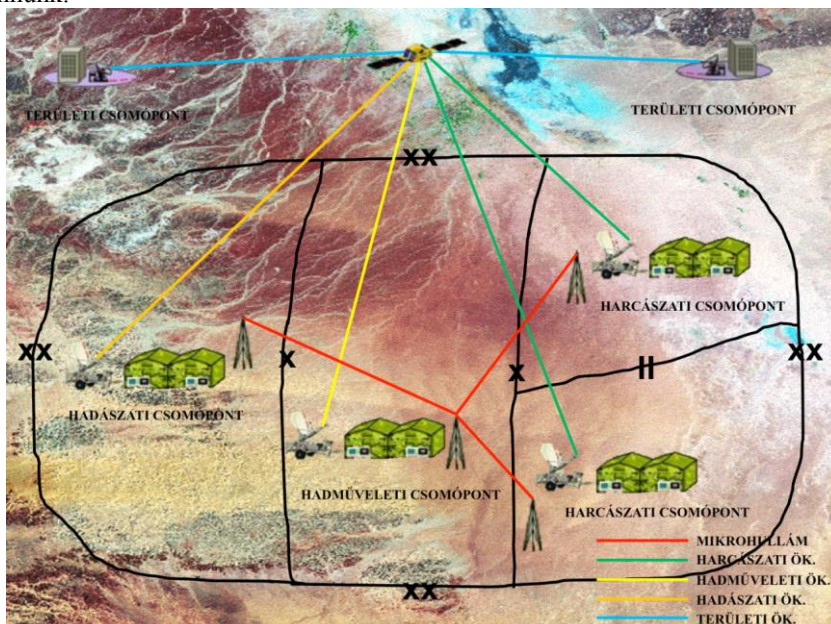
Ahhoz, hogy a világ bármely pontján alkalmazott csapatok irányába tudjuk biztosítani a megfelelő kapcsolatokat különböző szintű lecsatlakozási pontok szükségessé válnak. Az első a területi csomópont, amely egy fixen telepített csomópont, és kapcsolódási lehetőséget biztosít minden egyes alegység, egység és magasabb egység részére attól függetlenül, hogy éppen hol hajtja végre tevékenységét. Műholdas kapcsolatok segítségével biztosít hang- és adatszolgáltatásokat, és ezen keresztül érhetőek el a nemzeti katonai intranet hálózatok is. Mivel ez egy állandó telepítésű központ ennek következtében alkalmas arra, hogy központi szervereket helyezzenek itt el úgy, mint levelező, vagy fájl szerver. Végrehajthatóak ide a biztonsági mentések is, mivel a területi csomópontok egymással összeköttetésben állnak így minden esetben elérhetőek a kért információk a világ bármely pontjáról.

A következők a hadászati szintű csomópontok, amelyek hadosztályok, hadtestek és többnemzeti környezetben tevékenykedő megerősített dandárok részére teszik lehetővé, hogy csatlakozzanak a területi csomópontokhoz. Ezek már mobil, telepíthető berendezéseket tartalmaznak, amelyek lehetővé teszik a globális ge-

rinchálózathoz való csatlakozást, valamint az alárendelt egységekkel, alegységekkel történő kapcsolattartást.

A hadműveleti szintű csomópontok dandár szinten kerülnek alkalmazásra, és összeköttetést biztosítanak a hadászati szintű csomópontokkal, valamint az alárendelt zászlóaljakkal.

A harcászati csomópont pedig a zászlóaljak felől biztosít kapcsolatot a dandár felé. A híradás duplikálása és a folyamatos kapcsolattartás érdekében, mikrohullámú összeköttetés kerül telepítésre a különböző vezetési pontok között. Ezeken úgyszintén folyhat mind adat, mind hangtovábbítás és megosztásra kerülhet minden olyan információ, ami az aktuális helyzetkép kialakításához szükséges. A harcászati csomópontok esetében azonban fenn áll annak a lehetősége, hogy nem tudunk csatlakozni a területi csomópontokhoz a nagy távolságok miatt. Ilyenkor szükséges egy a magasabb műveleti csomópontokon elhelyezett szerverekhez történő csatlakozás, amelyek szintén képesek valós idejű információ biztosítására, de csak egy adott területről, nem garantált egy teljes hadszíntér lefedettsége. Ez függ az aktuálisan csatlakoztatott szerveren tárolt információktól, hogy az éppen milyen szintű adatokkal rendelkezik. Amennyiben ez csak egy hadműveleti szinten telepített szerver, ebben az esetben nem fogunk kapni információt a hadászati szinten alkalmazott elemekről, így ha egy ilyen alegységről/egységről szeretnénk valamit megtudni, vagy esetleg támogatást kérni egy másik rendszeren keresztül kell megtennünk.



7. ábra A NATO csomóponti összeköttetése

Forrás:

http://en.citizendium.org/wiki/Warfighter_Information_Network%E2%80%99Tactical

A fenti összeköttetések mindegyike egy hatékony hálózati menedzsmentet követel meg. Ilyenek többek között a központosított jelentési, ellenőrzési és javítási elemek, amelyek lehetővé teszik, hogy a felhasználó bármilyen fellépő hibát azonnal tudjon jelenteni és a hálózati menedzser arra azonnal tudjon reagálni. Biztosítja emellett a rendszer folyamatosan felügyeletét, így az egyes csomóponti elemek kiesése esetén az a lehető legrövidebb időn belül javítható, vagy cserélhető. Egy fejlett védelmi rendszer kiépítésével az esetleges hálózatba történő behatolások azonnal észlelhetők és a szükséges ellenlépések megtehetők. Emellett alkalmazásra kerülhetnek olyan beállítási elemek is, mint például a konfiguráció- és felhasználó-kezelés. Az előbbi előnye, hogy a hálózatunk minden egyes elemének hardver és szoftver konfigurációja nyilván van tartva egy adatbázisban, így annak meghibásodása esetén könnyebben lehet reagálni, és a hibát elhárítani. A felhasználó-kezelés lényege, hogy mindenki hozzáférhető a számára szükséges alkalmazói csoportokhoz, és ez által felruházzható minden olyan jogosultsággal, amely szükséges feladata végrehajtásához. Ezáltal illetéktelen személyek nem férhetnek bizalmas adatokhoz, azok védve lesznek a jogosulatlan felhasználókkal szemben.

Területi hírszisztem

A fenti kapcsolatok kiépítésével egy olyan gerinchálózat kerül kialakításra, amely integrálja a harcvezetési rendszerből kinyerhető összes információt. Ezek elérhetőek az állandó telepítésű vezetési pontokról ugyanúgy, mint a táboriakról, valamint a mobilakról. A NATO-ban erre egy vezetési pont platform került létrehozásra, amely lehetővé teszi a felhasználók számára a többi harcvezetési rendszer szoftver és az azok által nyújtott információk elérését. Magába foglalja a műveletirányítási, harci C2, tűzérségi és logisztikai támogató rendszereket, valamint a légvédelmi állomásokat. Támogatja a digitális térképi megjelenítést, ezáltal segíti a csapatmozgásokat, ellenség-barát felismerő modullal rendelkezik, illetve meteorológiai információkat is szolgáltat. Egy valós hadműveleti helyzetképet vagyunk képesek a rendszer által kialakítani, mely magába foglalja a saját csapatok mellett a szövetséges, a koalíciós, a semleges, az ismeretlen és az ellenséges erőről rendelkezésünkre álló összes információt. Minden egyes felhasználó számára lehetővé válik, hogy úgy kezelje a rendszert, hogy az részére csak a hasznos információ tartalommal bíró adatokat szolgáltatassa, ezáltal minden felesleges tényező kizárható és a döntéshozatali folyamat jelentősen meggyorsítható. A parancsnok képessé válik a rendszer segítségével, hogy csapatait egy valós idejű frissítésekkel rendelkező helyzetképpel vezesse, ezzel növelve a feladat végrehajtás hatékonyságát.

Ahhoz, hogy a fenti tevékenységek meg tudjanak valósulni szükséges egy olyan technikai háttér, amely minden lehetséges helyzetben képes az összeköttetés megvalósítására a parancsnokok és alárendeltjeik között. Ezt biztosítja a NATO-n belül, valamint a fejlettebb tagállamai esetében a globális vezetés-irányítási rendszer, ami az alábbi képességeket nyújtja:

- különböző harcvezetési rendszerek kapcsolódásának lehetőségét (szárazföldi, légierő, haditengerészeti), az erők összekapcsolását, ezáltal koalíciós képességek kialakítását;
- interfészeket és információcsere lehetőségeket számos összekapcsolt rendszeren keresztül;

- egy hídként szolgál a magasabb szintű hadszínterek, valamint a stratégiai, a hadműveleti és a harcászati szintű parancsnokok között;
- támogatja a magasabb szintű tervezést, végrehajtást és ellenőrzést (hadosztály, hadtest).

A rendszer védett vonalakon működik, akár titkos szintig és a világ bármely pontján használható, ahol az adott katonai szervezet települ, vagy bevetésen van (akár missziós környezetben is). Biztosít egy automatizált döntés támogató képességet minden olyan katonai művelet tervezéséhez és végrehajtásához, amely megköveteli az alegységek, egységek mozgékonyágát, telepíthetőségét, alkalmazhatóságát, fenntarthatóságát, hogy ez által képesek legyenek akár összhaderőnemi szintű feladatok végrehajtására is.

A vezetés-irányítási rendszerhez történő csatlakozáshoz szükség van egy megfelelő vezetési pont infrastruktúrára, amely lehetővé teszi a parancsnokok és törzsek részére a digitális tervezési, előkészítési és végrehajtási folyamatokat, amelyek összekapcsolják a harcászati kommunikációs rendszereket, valamint minden egyes művelettámogató alkalmazást egy közös platformon. Mindezek által kialakításra kerül egy hálózat központú vezetés-irányítási képesség, amely kihasználja a hadseregek C2 kommunikációs és információs rendszereit és megjeleníti a valós műveleti helyzetképet minden egyes parancsnok részére. A fent említett platform egy C4ISR5 által támogatott vezetési pont platform, amely magába foglalja a gyorsan telepíthető, interoperábilis, hálózat központú képességek által nyújtott kommunikációs, LAN, videó és távközlő rendszereket. Ezeket különböző infrastruktúrák szolgálják ki, melyek mindegyike más és más szolgáltatást nyújt a felhasználóknak:

- A számítógépes infrastruktúra lehetővé teszi hadseregen belüli, összhaderőnemi, valamint többnemzeti alkalmazások futtatását. Ezáltal lesznek mindenki számára elérhetőek az olyan alapvető információk, mint az aktuális helyzetkép, különböző térképi felületek és valós idejű kommunikációs lehetőségek.
- A beszéd alapú infrastruktúrák összefognak minden olyan eszközt és hálózatot, amelyek hang továbbítására alkalmasak, amelyeket egy művelettámogató képességgel rendelkező szolgáltatásban központosítják. Ide tartoznak a rádiók, távbeszélő berendezések, mint IP telefonok, VoIP6 készülékek.
- A rádiós infrastruktúrák amellet, hogy alkalmasak hangtovábbításra is egyidejűleg képesek adattovábbítást is biztosítani amennyiben digitális képességekkel bíró többfunkciós rádióeszközökből telepített hálózatot hozunk létre.

A fenti elemek összekapcsolása egy egységes rendszerré alkotja a vezetési pont kommunikációs hálózatát, ahol minden felhasználó maga választja ki, hogy melyik átviteli eszközt / eszközöket szeretné alkalmazni a folyamatban lévő feladatok

⁵ Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance - Vezetés, Irányítás, Kommunikáció, Számítógép, Hírszerzés, Megfigyelés és Felderítés

⁶ Voice over IP: IP alapú rendszeren keresztül biztosított hangkommunikáció

végrehajtásához. Ez egyszerűbb esetben lehet csak egy csatorna, de sokkal inkább jellemző, hogy több csatornán is folyik a kommunikáció, például telefonon és számítógépes hálózaton egyaránt. Egy megfelelően kiépített platformon az összes felhasználó rendelkezik távbeszélő modulokkal, amelyek alkalmasak pont – pont összeköttetésre, valamint konferenciabeszélgetésre egyaránt. Emellett mindenki részére hozzáférést biztosít a rádiós rendszerekhez, ahol beszéd és adatkapcsolat építhető ki az alárendeltek és az előljáró irányába egyaránt, függetlenül attól, hogy fixen telepített munkahelyen, vagy éppen mozgásban lévő harc-, illetve gépjárműben tevékenykednek. Amennyiben ez a távolság nagyobb, mint a rádiónk hatótávolsága az összeköttetés megvalósítható műholdas összeköttetéssel. A katonai kommunikációk esetében két sáv kerül jellemzően alkalmazásra, a Ku- és a Ka-sáv. Ezek a centiméteres tartományban dolgozó sávok, ahol a Ku-sáv esetében a „u” betű az angol „under” szóból ered és azt mutatja, hogy ez egy K-sáv alatti kommunikáció, amelynek frekvencia tartománya 12–18 GHz. A Ka-sáv-nál az „a” az angol „above” szóra utal és K-sáv feletti összeköttetést mutat 24–40 GHz frekvenciákkal. A vezetési pont hálózata rendeltetésénél fogva integrálja és összekapcsolja az alkalmazásra kerülő rendszereket és platformokat.

Műveletirányítási rendszer

A vezetési ponton belül az egyik alkalmazásra kerülő rendszer a műveletirányítási rendszer, ami egy olyan platform, amely összekapcsolja a műveleti parancsnokokat zászlóalj szinttől egészen hadtest szintig. Központilag készíti és kezeli a kritikus információkat úgy, mint a baráti és ellenséges erők elhelyezkedése, célok, előrevonási és utánpótlási útvonalak. Ahhoz, hogy a parancsnok megfelelően tudja kezelni ezeket az információkat információs fölényre van szüksége. Ezzel a fölényrel az a parancsnok rendelkezik, akinek jóval magasabb a harcéri vizualizációs képessége, mint ellenségeinek. A harcéri vizualizáció az a folyamat, ahol a parancsnok:

- kialakít egy mindenki számára érthető képet a jelenlegi állapotokról az ellenséggel és a környezettel összekapcsolva;
- meghatározza a kívánt végcélokat, amelyek bemutatják a küldetés megvalósításának módját;
- meghatározza a tevékenységek sorrendjét a saját csapatokra vonatkozóan a jelenlegi állapotoktól a végcélokig.

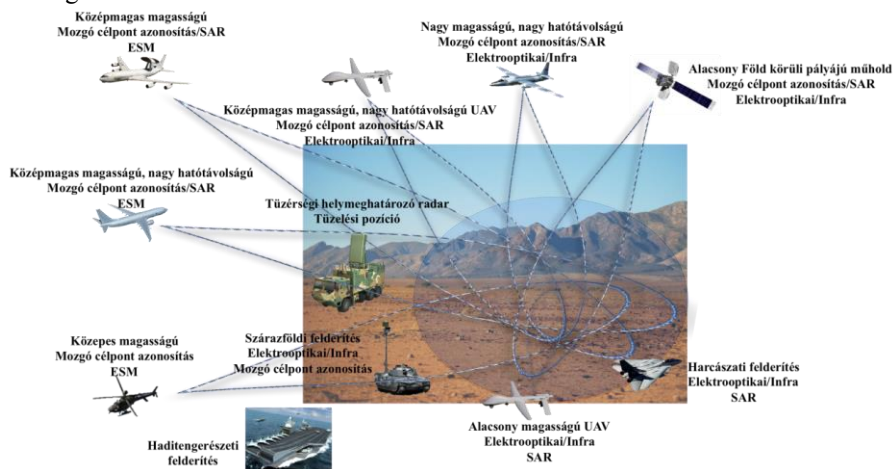
Ezeket támogatja a műveletirányítási rendszer, amely magába foglalja a felderítő és egyéb adatszolgáltató rendszereket és szenzorokat a teljes harcterén, valamint egy kommunikációs csatornát biztosít az általuk megszerzett információk továbbítása részére. Integrálja az így szerzett adatokat és megosztja a csomópontokon keresztül egy közös műveleti helyzetképként, amely minden szintű parancsnok részére elérhető.

A műveletirányítási rendszerben fut össze az összes alrendszer által gyűjtött és feldolgozott felderítési, logisztikai, tűzérési és minden egyéb harcászati/hadműveleti információ.

Felderítési rendszer

A NATO felderítési rendszerek lényege az összes információszerző berendezés egy hálózatba történő kapcsolása. Ezeknél a rendszereknél fontos, hogy ne csak a szövetségi rendszerek legyenek képesek együttműködni, hanem a megfelelő szab-

ványoknak köszönhetően a nemzeti hálózatok is beintegrálhatóak legyenek. Ennek köszönhetően egy sokkal szélesebb, nagyobb területre kiterjedő információs kapcsolatot kapunk, amely képes a szárazföldi, légi és haditengerészeti adatokat integrálni. Ezáltal összekapcsolásra kerülnek a kamerák, szenzorok, radarok, felderítő repülőgépek, pilóta nélküli repülők (UAV7) és minden olyan eszköz, amely információval szolgálhat a feladatunk sikeres végrehajtásához. Lehetőség nyílik az elsődleges (IMINT8, SIGINT9, ELINT10 stb.) és a másodlagos (képi, térképes, jelentésekből adódó) felderítési adatok tárolására, rendelkezésre bocsátására és feldolgozására.



8. ábra Koalíciós felderítési szenzor környezet

Forrás: <http://www.defenseindustrydaily.com/Shared-ISR-More-MAJIC-for-NATO-06812/>

A képen látható koalíciós felderítési rendszer megvalósításához létrehozásra került a NATO Hírszerzési, Megfigyelési, Felderítési Interoperabilitási Architektúra (NIIA¹¹), amely megfogalmazza, hogy a felderítési és megfigyelési eszközök milyen módon érhetik el az interoperabilitást a felelősségi körzeten belül. Az NIIA a NATO minden szintjén és koalíciós környezetben úgyszintén elérhető az V. cikkely (háborús műveletek) és a nem V. cikkely (békétámogató műveletek) szerinti műveletekben egyaránt. Lefektetésre került benne minden olyan szabvány, amely biztosítja a nemzeti felderítési rendszerek és a NATO rendszerek összekapcsolásának lehetőségét. Ennek megfelelően egy olyan összehangolt hálózat jön létre, amely képes a legmagasabb szintű felderítési támogatást biztosítani a következők érdekében:

- időben történő jelzések és figyelmeztetések küldéséhez;
- a hadszíntér felderítő értékeléséhez;

⁷ Unmanned Air Vehicle

⁸ Imagery Intelligence – képi felderítés

⁹ Signal Intelligence – rádióelektronikai felderítés

¹⁰ Electromagnetic Intelligence – elektronikus hírszerzés

¹¹ NATO Intelligence, Surveillance, Reconnaissance (ISR) Interoperability Architecture

- az ellenséges harci tevékenységek azonosításához;
- helyzetértékelés kialakításához;
- ellenséges tevékenységek megfigyeléséhez;
- saját csapatok védelmének támogatásához;
- célobjektumok meghatározásához;
- felmérések készítéséhez úgy, mint például háborús kárfelmérés.

Logisztikai támogató rendszer

A művelet irányítási rendszer részeként ez a platform biztosítja a valós idejű logisztikai helyzetképet. A rendszer nem arra szolgál, hogy ezen keresztül tudunk logisztikai rendeltést benyújtani, sokkal inkább a tervezést hivatott segíteni. Az állomány általa egy logisztikai C2 képességet kap, amely segíti a kitelepülések, átszortosítások, visszatelepülések, a konvoj menetek tervezését és a logisztikai jelentések elkészítését, valamint a beérkezett, illetve a kiadott anyagok nyilvántartását. Amennyiben a parancsnoknak, vagy a törzsnek információra van szüksége például egy úton lévő konvojunkról, a rendszer képes azt egy térképi felületen megjeleníteni így az folyamatosan követhető. A beérkezett, illetve a területünkön (laktanya, tábor) tárolt konténerekben elhelyezett anyagokról adatokat biztosít a felhasználók részére. Ezáltal támogatja a valós műveleti helyzetkép biztosítását a parancsnok részére, folyamatosan mutatja a logisztikai és harckészültségi állapot-információkat.

Tűztámogató rendszerek

A NATO-n belül több nemzet is rendelkezik saját hálózat központú tűztámogató rendszerrel (amerikai: AFATDS, angol: BATES, német: ADLER, francia: ATLAS, olasz: SIR). A rendszer elsődleges feladata a tűztámogatás irányítása és koordinálása a harctéren. Emellett szintén szerepet játszik a harctér valós helyzetkép kialakításában azáltal, hogy tűztámogatási információkkal és ahhoz szükséges adatokkal látja el a parancsnokot. Összhaderőnemi tűztámogatási C2 rendszerek, amelyek többnyire támogatják a következő fegyverplatformokat:

- tarackok;
- aknavetők;
- rakéták;
- közvetlen légi támogatás;
- harci helikopterek;
- haditengerészeti tüzérségi tűz.

Egy teljesen automatikus tűztámogatási tervezési, koordinációs és ellenőrzési képességet biztosítanak a közvetlen tűztámogatáshoz, az ellenlökésekhez és lefogásokhoz, valamint az ellenséges légvédelmi és tüzérségi eszközök megsemmisítéséhez.

A különböző nemzetek rendszerei annak érdekében, hogy együtt tudjanak működni közös szabványokon alapuló interfészekon keresztül összekapcsolhatóak vezetékes és vezeték nélküli kapcsolatokkal egyaránt. Az így kialakított hálózatok minden esetben IP-alapúak, így rádiós összeköttetés esetében csak szoftverrádiók kerülnek alkalmazásra. LAN kapcsolatok esetében védett hálózatok is kiépítésre kerülhetnek, így a rendszeren minősített információk is továbbíthatók.

Harctéri azonosító rendszerek

A rendszer lényege a harctéren a saját, illetve ellenséges csapatok azonosítása, követése, ezáltal egy esetleges baráti tűz elkerülése. Egy feladat centrikus harcászati vezetési információs rendszerről beszélhetünk, amely képes valós időben harcászati, vezetés-irányítási üzenetek küldésére, fogadására és megjelenítésére. Az aktuális helyzetkép kialakításához biztosítja az információt a saját elhelyezkedésünkről, a baráti erőkről, a felfedett ellenséges erőkről és a harctéren megjelenő minden egyes veszélyforrásról. Ezáltal a saját erőink (járművek, személyzet) pontos információkkal rendelkeznek a számukra szükséges elemekről. A rendszer minden frissítést automatikusan továbbít egy tároló- és feldolgozó rendszerbe, ahonnan a felhasználói platformok meghatározott időnként azokat szintén automatikusan letöltik. A rendszerrel szemben támasztott követelmények:

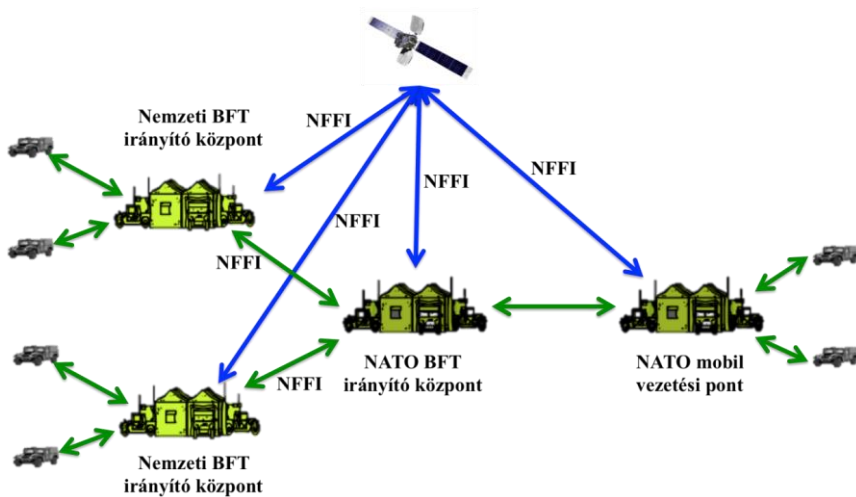
- „pontos helymeghatározás (városi, utcai harcokban legalább 5 méteren belül);
- valós idejű (real time) adatbázis a saját erők pozíciójáról;
- nagy megbízhatóságú, magas fokú titkosítással, erős zavarvédelességgel és alacsony felderíthetőséggel rendelkező digitális rádióháló;
- rendkívül nagy sebességű adatkezelés;
- személyekre, járművekre meghatározott azonosító kódrendszer;
- a berendezések magas fokú ellenálló képessége a mechanikai igénybevételek, valamint a szélsőséges időjárási körülményekkel szemben.”ⁱⁱⁱ

A rendszer általában dandár szinten és az alatt kerül alkalmazásra. A digitális rádióháló ennek következtében alkalmas a folyamatos összeköttetések biztosítására, de amennyiben valamilyen zavaró tényező ezt megakadályozná kiépítésre került egy másodlagos műholdas hálózat is, ahol ilyen esetekben folyhat a kommunikáció.

Ahhoz, hogy a NATO és a nemzeti azonosító rendszerek összekapcsolhatóak legyenek kialakításra került a NATO Baráti Erők Információja szabvány (NFFI12), amely alapvetően az ISAF-en belül alkalmazásra került többnemzeti erők kommunikációs kapcsolatainak megvalósítására jött létre. A szabvány alkalmazásával kialakított hálózaton a műveletekben résztvevő összes nemzet képes egy baráti erő követő (BFT13) rendszer segítségével egymással információkat megosztani, illetve az együttműködő csapatokat egy térképi adatbázison valós időben nyomon követni, ezzel a baráti tüzet elkerülni.

¹² NATO Friendly Forces Information

¹³ Blue Force Tracking



9. ábra NATO Baráti Erők Információja szabvány alkalmazásával kialakított baráti erőkövető rendszer elvi vázlata

Forrás: Károly Krisztián: Erőkövetési rendszerek az afganisztáni hadszíntéren

Összegzés

A NATO kommunikációs és információs rendszerét a nemzeti hálózatokhoz hasonlóan szintén két részre bonthatjuk. Először is kialakításra került egy stacioner gerinchálózat, amely nagy sáv szélességű összeköttetést biztosít a világ bármely pontján elhelyezett csapatok, valamint vezető szervek között. Emellett lehetőséget biztosít a tagállamok nemzeti kommunikációs rendszereinek felcsatlakozására, így biztosítva a kapcsolatot a más országok hadseregei között.

A tábori területi hírendszerek lényege pedig egy interoperábilis környezet kialakítása a feladatban résztvevő különböző nemzetiségű csapatok között támogatva ezzel feladatuk végrehajtását. Támogatja egy egységes műveleti helyzetkép kialakítását, azonos platformon történő kommunikációs képességeket, valamint az el-lenség-barát felismerő képességeket.

Felhasznált irodalom

- [1] Molnár Ferenc: NATO-csúcstalálkozó Washingtonból Bukarestig, Nemzet és Biztonság 2008. Április
- [2] NATO Handbook 2006
- [3] The Strategic Defence Review: A New Chapter, Presented by The Secretary of State for Defence By Command of Her Majesty
- [4] NC3 Common Operating Environment and Transformation to the NATO Network Enabled Capability”, NATO C3 Technical Architecture
- [5] Miklós Hóka: The Tactical Internet, Overview of a new type communications system for command and controls, AARMS, Vol. 2, No. 2 (2003), ZMNE
- [6] Farkas Tibor főhadnagy: A válságkezelő műveletek vezetését és irányítását támogató híradó- és informatikai rendszer megszervezése a Magyar Honvédség többnemzeti műveleteinek tükrében, Doktori (PhD) értekezés, Budapest 2010

Hivatkozások jegyzéke

¹Miklós Hóka: The Tactical Internet, Overview of a new type communications system for command and controls, AARMS, Vol. 2, No. 2 (2003), ZMNE, p.: 272

¹AEDP2 - NATO Intelligence, Surveillance, Reconnaissance (ISR) Interoperability Architecture

¹<http://www.zmne.hu/tanszekek/ehc/konferencia/may/szalai.htm> (Letöltve: 2014. április 15.)

A KATASZTRÓFAVÉDELEM INFOKOMMUNIKÁCIÓS RENDSZEREI

Absztrakt

A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (továbbiakban: BM OKF) által vezetett hivatásos katasztrófavédelmi szervek biztosítják Magyarország lakosságának védelmét egy-egy természeti, vagy ipari katasztrófa esetén. A BM OKF, és területi szervei a katasztrófahelyzetek kapcsán három nagyon fontos időszakban végeznek elengedhetetlenül fontos informatikai, távközlési tevékenységet:

A megelőzés időszakában: Legfontosabb a lakosság folyamatos felkészítése, az igénybe vehető erők, eszközök folyamatos és naprakész nyilvántartása, a kockázatok elemzése.

A védekezés időszakában: Azonnali lakosság tájékoztatási feladatokat kell megoldani, és ezzel egyidőben a beavatkozást végző szervek pontos, és gyors tájékoztatása a legszükségesebb.

A helyreállítás időszakában: A nyilvántartások pontosítása, a helyreállítást, újjáépítést végző szervek műveleti tevékenységének koordinálása a legfontosabb feladat.

Az alábbi dokumentum bemutatja, hogy a katasztrófavédelmi szervek részére biztosított infokommunikációs lehetőségek, hogyan segítik a fenti feladatok megoldását.

Kulcsszavak

katasztrófavédelem, segélyhívás, lakossági riasztó és riasztó-tájékoztató rendszer, viharjelző, térinformatikai támogatás,

Bevezetés

A 2000-es években a katasztrófavédelmi szervek és a közöttük lévő kommunikációt biztosító hang- és adatátviteli lehetőségek az akkori szervezeti és jogszabályi követelményeknek maximálisan eleget tettek. A telephelyek száma közel száz volt, melyek között az ingyenes távbeszélő hálózat és korlátozott sebességű (256kbps-2Mbps) informatikai összeköttetések az akkor jelentkező igények kielégítésére elég kapacitással rendelkeztek.

2010-től egy jelentős szervezeti átalakulás vette kezdetét, melynek csúcspontját az új katasztrófavédelmi törvény jelentette (2011. évi CXXVIII. Törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról, továbbiakban: Katved. Tv.). Első ütemben átalakultak a hivatásos katasztrófavédelmi szervek, majd 2012. január 01-től, a Hivatásos Önkormányzati Tűzoltóságok (továbbiakban: HÖT) állami integrációjával a szervezet létszáma több mint 10 000 főre, és több mint kétszáz telephelyre bővült.

A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság Informatikai Főosztály (továbbiakban: BM OKF IFO) szervezetében és létszámában szintén

¹ Turányi Zoltán tűzoltó alezredes zoltan.turanyi@katved.gov.hu

átalakult, ezzel biztosítva a jelentős országos bővülés infokommunikációs infrastruktúrájának biztosításához szükséges kapacitásokat.

2010-től a katasztrófavédelmi szervek a korábbiaktól eltérően jelentős energiát fektettek Unió pályázatok kidolgozására, majd sikeres pályázat esetén azok megvalósítására. Az elnyert támogatások jelentősen megnövelték a beruházásra fordítható források összegét. Az így megvalósított beruházások segítségével, valamint a jogszabályi változások által támasztott követelmények miatt a katasztrófavédelmi szervek által használt infokommunikációs lehetőségek tárháza, valamint a rendelkezésre álló hardver, szoftver háttér 2014-re jelentős mértékben megváltozott. Ez a változás nagyon sok részelemből tevődik össze, de összességében igazodik a XXI. század által biztosított infokommunikációs trendekhez.

Egységes Katasztrófavédelmi Távközlési Rendszer

A Katved. Tv. hatálya lépése előtt a lakosságtól beérkező 105-ös segélyhívások a HÖT-ök ügyeleti szolgálatánál végződtek, sok esetben hangrögzítés nélkül. Esetleges működési terület változásnál, vagy alközponti hibánál minden tűzoltóság saját hatáskörben intézte a segélyhívások átirányítását. A HÖT-ök több tízféle különböző gyártótól származó alközponttal rendelkeztek, sok esetben karbantartási szerződés nélkül.

A megyei katasztrófavédelmi igazgatóságokon (továbbiakban: MKI) olyan létszámú, és szaktudású ügyelei szolgálat került felállításra, amely lehetővé tette a segélyhívások centralizálását. 2012 februártól a Nemzeti Média és Hírközlési Hatósággal szoros együttműködésben köteleztük a távközlési szolgáltatókat (~100 különálló vállalkozás), hogy meghatározott hívószámra adják át a szolgáltatási területükről indított 105-os segélyhívást. Ezt megelőzően a Magyar Telekommal szorosan együttműködve a katasztrófavédelmi igazgatóságok telefonközpontjainak fővonalai oldalán jelentős bővítéseket végeztünk, az egyidejű hívások fogadásának biztosítására.

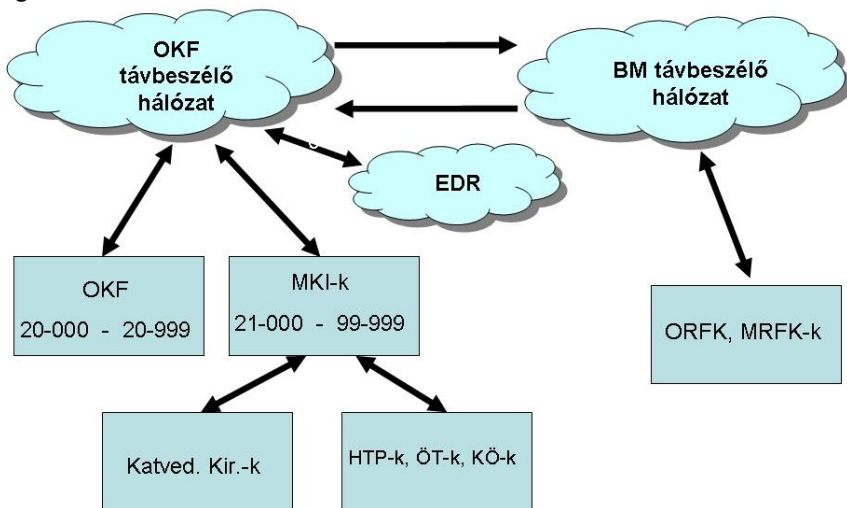
A katasztrófavédelem esetében egy-egy lokális időjárési, vagy katasztrófavédelem esetén jelentősen megnő az egyidejű bejelentések száma. Ezt a problémát azonban a HÖT-ökből megalakuló Hivatásos Tűzoltó Parancsnokságok (továbbiakban: HTP), örökölt, nem egységes távközlési hálózatai, berendezései nem tudták megoldani.

A probléma megoldására az MKI-k telefonközpontjai egy újabb, jelentősen nagyobb kapacitású alközpontra kerültek lecserélésre. Ezzel a fejlesztéssel lehetővé vált a bejövő segélyhívások úgynevezett „lecsorgatása”, ami azt jelenti, hogy az MKI maximális hívásfogadó kapacitásának elérésekor a lakossági bejelentést az adott megyében lévő HTP-re automatikusan átirányítjuk. A HTP-ken ezen hívások fogadása IP mellékeken történik a Nemzeti Távközlési Gerinchálózat (továbbiakban: NTG) felhasználásával. Az MKI-król leszerelt alközpontok egy-egy frekvenciát több megyei HTP-n kerültek letelepítésre.

A katasztrófavédelem a fejlesztéseket megelőzően a BM zártcélú távközlő hálózatát használta. A bővítés során korlátként jelentkezett, hogy a hálózatból nem volt lehetséges további több ezer mellék hívószám kiadása. A jelentősen megnövekedett mellékszámot a BM OKF IFO által kialakított tipizált, beosztáshoz kötött hívószám rendszer indokolta. A BM zártcélú távközlési hálózatát üzemeltető Nem-

zeti Infokommunikációs Szolgáltató Zrt.-vel (továbbiakban NISZ) folytatott tárgyalások eredményeként a megyei rendőrségi telefon alközpontok átprogramozásával egyidejűleg, a BM OKF egy önálló, saját, ötjegyű számmezőből álló zártcélú távközlő hálózatot hozott létre.

A hivatásos katasztrófavédelmi szervek távközlési igényeit, a fejlesztések után közel 100 korszerű alközpont, és több mint ezer IP mellék biztosítja. A fejlesztés után, természetesen megmarad az ingyenes hívás lehetősége a társ rendvédelmi és kormányzati szervek felé, ugyanakkor a segélyhívások területi hangrögzítése is megoldásra kerül.



1. ábra: A katasztrófavédelem távkészelő hálózata

Viharjelző Rendszerek

A BM OKF viharjelző rendszereket üzemeltet a Balatonon, a Velencei tavon, a Fertő tavon, valamint a Tisza tavon. A rendszerek bővítése, technológiai fejlesztése 2000 óta folyamatosan zajlik. 2000-ben még csak a Balaton térségében és még csak „viharjelző rakétás” jelzések voltak. Az azóta eltelt időben négy tóra bővült a szolgáltatás, és már a harmadik technológia váltást vezettük be a végpontoknál, mely fejlesztés célja a lakosságvédelem megfelelő ellátása, és a költséghatékony működés biztosítása.

Jelenleg a Balaton térségében 31 viharjelző végpont működik, melyből már 12 korszerű LED-es technológiát használ.

Fertőrákoson, a tó térségében az osztrák partner által működtetett rendszerhez kapcsolódóan egy magyarországi végponttal rendelkezünk.

A Velencei-tó térségében jelenleg 3 végpont üzemel.

A Tisza-tó partján jelenleg 5 viharjelző állomás működik.

A viharjelző állomások az Országos Meteorológiai Szolgálat által kerülnek elindításra. Az állomások, a vezérlésüket kiszolgáló, és az ehhez kapcsolódó adatátviteli rendszerek folyamatos korszerűsítése a pénzügyi és a technikai keretekhez igazodva folyamatosan zajlik.



2. ábra: Viharjelző végpont

Monitoring és Lakossági Riasztó Rendszer (MoLaRi), Lakossági Riasztó, és Riasztó-Tájékoztató Rendszerek

A MoLaRi rendszer kialakításának gondolata a 2000-es évek második felében kezdődött, amikor is felmerült az igény arra, hogy a veszélyes vegyi anyagot feldolgozó üzemek körzetében élő lakosság biztonsági kockázata a lehető legkisebb mértékre kerüljön csökkentésre.

A Kat. törvényben és végrehajtási rendeleteiben foglaltak alapján a veszélyes anyagokkal foglalkozó üzemeket három kategóriába kell besorolni: küszöbérték alatti, alsó és felső küszöbértékű üzem. Az üzemekben előforduló anyagok összetétele, mennyisége, valamint az üzem környezetében élő lakosságszám függvényében kijelölésre került 21 alsó és felső küszöbértékű ipari létesítmény. A kijelölt üzemek belterületén, illetve a közvetlen környezetükben monitoring végpontok gyűjtik a veszélyes anyagok jelenlétére utaló adatokat. A mérő végpontok üzem specifikus szondákkal kerültek felszerelésre, mely szondák végpontonkénti duplikációja biztosítja a megfelelő redundanciát. A végpontok egy része meteorológia információkat is szolgáltat. A mérések eredményét a végpontok zárt belső hálózaton keresztül továbbítják a területi központokba. A központokba továbbított adatok az üzemben, az MKI-n, valamint az országos központban is megjeleníthetők.

A rendszerbe implementálásra került egy olyan döntéstámogató modul, melyben a mért adatok automatikusan megjelennek, és a bementi adatok alapján egy egzakt modellezés futatható le a kiszabadult veszélyes anyag terjedésének irányára és sebességére vonatkozóan.

A modellezés alapján az ügyeleti szolgálatok kiválasztják az érintett lakosság területén lévő riasztó végpontokat, amelyek segítségével tájékoztathatják, illetve riaszthatják a veszélyeztetett személyeket. A sziréna rendszeren történő tájékoztá-

tás tartalmazhat magatartási szabályokat, gyülekezési helyeket, menekülési útvonalakat is. A rendszer jelenlegi kiépítettségében mintegy 440 000 lakos biztonságát szolgálja.

A rendszerben lévő eszközök mennyisége megyénkénti bontásban:

- Borsod-Abaúj-Zemplén: 90 monitoring végpont, 45 riasztó végpont
- Csongrád: 6 monitoring végpont, 5 riasztó végpont
- Heves: 6 monitoring végpont, 19 riasztó végpont
- Fejér: 29 monitoring végpont, 59 riasztó végpont
- Komárom-Esztergom: 33 monitoring végpont, 37 riasztó végpont
- Pest: 37 monitoring végpont, 27 riasztó végpont
- Tolna: 13 monitoring végpont, 19 riasztó végpont
- Veszprém: 47 monitoring végpont, 50 riasztó végpont
- Zala: 8 monitoring végpont, 8 riasztó végpont
- Budapest: 52 monitoring végpont, 317 riasztó végpont

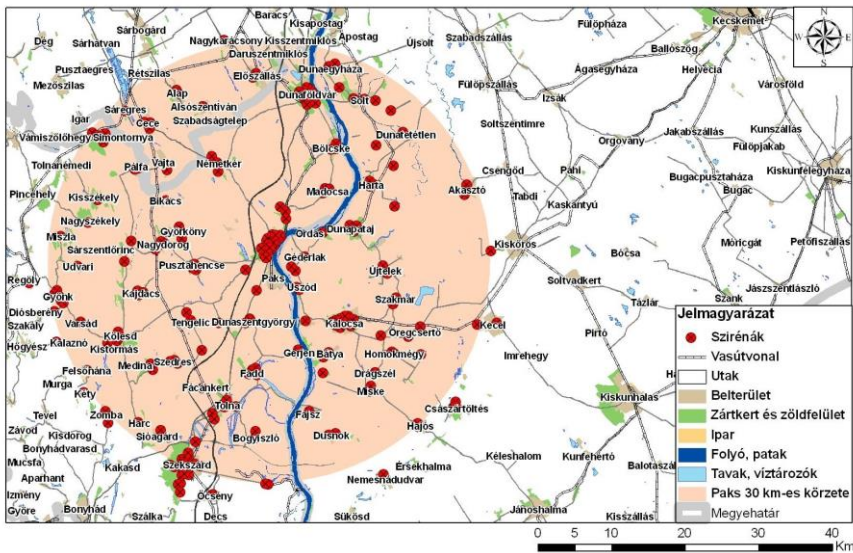
A MoLaRi rendszer fejlesztése természetesen nem állt le. A 2014-ben Budapesten letelepített végpontok már az EDR rendszeren működő rádiókkal üzemelnek. A következő fejlesztési ciklusban elérhető Uniós támogatás megléte esetén további üzemek, és ezáltal Magyarország lakosságának további része kerülhet nagyobb biztonságba.



3. ábra: Monitoring végpont



4. ábra: Riasztó végpont



5. ábra: Paks-on és 30 km-es körzetében telepített szirénarendszer

A BM OKF, valamint a települési polgármesteri hivatalok kezelésében jelenleg 4831 db elektromechanikus (motoros sziréna), 202 db elektronikus lakossági riasztó-tájékoztató eszköz működik. A Paksi Atomerőmű 30 km-es körzetében a 2000-2012 között telepítésre került a lakossági tájékoztatását és riasztását szolgáló rendszer, 227 elektronikus riasztó sziréna-végponton. A rendszer kiépítésekor trónkölt

rádió átviteli úton került vezérlésre. Az átviteli eszközök mára már elavultak, gyári támogatásuk megszűnt. 2013-ban megkezdődött az átviteli rendszer rekonstrukciója, ami 2014-ben tovább folytatódik. Jelenleg már 124 eszköz használja adatátvitelre a rendvédelmi szervek által is használt EDR rendszert. A hálózat korszerűsítése 2015 első félévében befejeződik.

Pályázati lehetőségek

A hazai költségvetési források szűkülése miatt a katasztrófavédelmi szervek is egyre inkább kihasználják az uniós pályázati források adta lehetőségeket.

Ez a tevékenység két szinten valósul meg. Az igazgatóságok elsősorban a határmenti együttműködések miatt közös pályázati lehetőségeket keresnek, illetve használnak ki. Ilyen pályázatok kapcsán az északi a keleti, és a déli határaink mentén jelentős helyi együttműködések, és fejlesztések valósultak meg a korábbi években.

A pályázati tevékenység felsőbb, országos szintjén a BM OKF vezetésével, országos infrastrukturális beruházások valósulnak meg. Uniós pályázati lehetőség kapcsán újult meg a katasztrófavédelem központi, de országosan 21 összekapcsolt szerveren működtetett, több ezer felhasználót kiszolgáló ügyviteli rendszere.

A BM OKF IFO térinformatikai képességeinek felhasználásával valósul meg a „Közös kockázatbecslés és felkészülés a Duna makrorégióban” című, 9 ország részvételével zajló projekt. A pályázat célja, hogy egységes kockázatbecslési módszertant alakítson ki a délkelet-európai országok katasztrófavédelmi szervei részére a klímaváltozás következtében felerősödő természeti katasztrófákra való megfelelő felkészüléshez.

Központi költségvetési forrásból valósul meg minden évben az Önkéntes Tűzoltó Egyesületek részére nyújtott pályázati lehetőség. Ezen pályázatok kapcsán, több éve, jelentős forrás kerül bevonásra a hivatásos és önkéntes katasztrófavédelmi szervek rádiókommunikációját biztosító EDR rendszer kiterjedtebb használatára, a korábban beszerzett, elavult, vagy megsemmisült eszközök pótlására.

2013-2014 folyamán került megvalósítási szakaszba a BM OKF IFO által menedzselte, az EKOP 1.1.10 „Katasztrófavédelmi informatikai rendszerek döntéstámogató szerepének és biztonságának növelése” című projekt. A projekt négy fejlesztési irányban jelentett előrelépést az infokommunikációs területen. Ezek: infokommunikációs technológia, informatikai infrastruktúra, komplex térinformatika rendszer és alkalmazásfejlesztések, valamint fix és mobil vezetési pontok, oktatókabinet kialakítása, fejlesztése.

Térinformatikával támogatott műveletirányítási, nyilvántartási rendszerek

A katasztrófavédelmi szervek felé támasztott egyre nagyobb követelmények, a térinformatikai technológia egyre nagyobb elterjedése, valamint a rendelkezésre álló pályázati lehetőségek megkövetelték, illetve lehetővé tették ezen területek nagymértékű fejlesztését.

A tűzoltósági műveletirányítás (a kárhelyszínre kikerkező erők optimalizálása, tájékoztatása, statisztikák készítése stb.) a HÖT-ök meglétekor nagyon szerteágazó és inhomogén rendszert alkotott. A tűzoltóságok integrációjakor felmerült az egyértelmű igény, hogy a lakossági bejelentést követően az erők, eszközök mozgását, koordinálását, majd a következtetések levonását térinformatikai eszközökkel

kell támogatni. A megfelelő személyzeti, technikai és nem utolsó sorban anyagi lehetőségek megléte, lehetővé tette, hogy mára egy jelentős térinformatikai támogatással bíró, redundáns adatátviteli hálózatot használó, a beavatkozást jelentősen megkönnyítő tűzoltósági műveletirányítási rendszert sikerült kialakítani.

A rendszer az alábbi szolgáltatásokkal segíti a mindennapi döntéstámogatási feladatokat:

Katasztrófavédelmi Adatszolgáltatási Program

A szakmai terület számára kialakított központi rendszer alapja egy statisztikai rendszer (on-line KAP), melynek elsődleges feladata az országos, területi és helyi szervektől való adatbekérés és adatkinyerés. A rendszer célja, hogy az adatbevitel ott történjen, ahol az adat keletkezik és – a hozzáférés függvényében – minden hierarchia szinten ugyanazt az adatot kapjuk vissza.

PAJZS

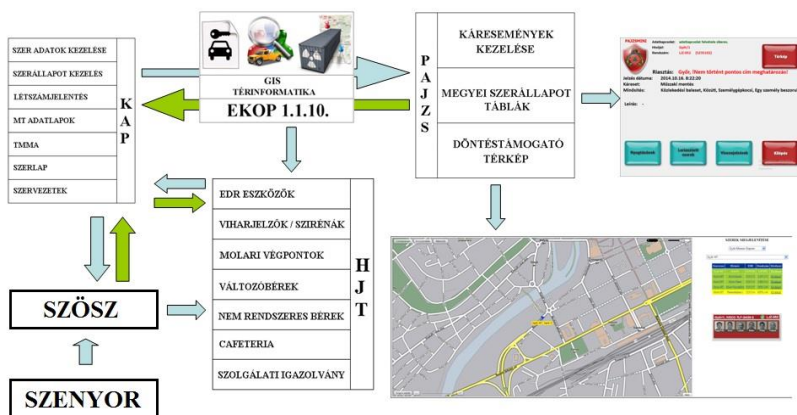
Az ügyeletek egyre több adattal és információval dolgoznak, amelyeknek a nap 24 órájában rendelkezésre kell állniuk ahhoz, hogy a szükséges erőket, eszközöket másodpercek alatt a helyszínre lehessen irányítani. E téren a BM OKF-en komoly fejlesztési háttérmunka folyt, amelynek eredményeként rendszerbe állt a PAJZS program. A térinformatikával támogatott központi informatikai rendszer rendelkezik azzal a káresemény-kezelési és riasztási modullal, amellyel a tűzoltó gépjárműveket a káreseményekhez lehet rendelni; megyei szintű szerátcsoportosítási modulal, amely az erő- és eszközgazdálkodást szolgálja.

HUNOR/HUSZÁR Riasztási Rendszer

Az alkalmazás célja egy olyan rendszer biztosítása, amely lehetővé teszi a nehéz (HUNOR), valamint a közepes (HUSZÁR) kategóriájú városi kutató-mentő, magyar csapatok riasztását. A rendszer segítségével a riasztás pillanatában a területi szervek ügyeletei értesítést kapnak a riasztható személyek adatairól, elérhetőségeiről.

Szolgálat Összesítő Szoftver

A 2013-ban bevezetett országos szintű szolgálat összeállítási rendszer on-line módon képes kezelni mind a hivatali, mind váltásos munkarendben dolgozó állomány beosztási rendjét és annak tervezését. Az alkalmazás a napi létszámról, a távollétekről, a túlszolgálatról és a pótlékjelentésekről szóló naprakész, pontos kimutatások a gazdasági szakterület munkáját segíti, míg a szerekre, gépjárművekre beosztott létszámadatok a katasztrófavédelem riasztási és döntéstámogatási rendszerét szolgálja. Az alkalmazás két fő pillére a személyügyi nyilvántartó rendszer és a Katasztrófavédelmi Adatszolgáltatási Program.



6. ábra: A műveletirányítási és nyilvántartási rendszerek háttértámogatása

HELIOS

A katasztrófavédelem műveletirányítási tevékenysége azonban nem merül ki a tűzoltási szakterületben. Egy-egy rendkívüli időjárási helyzet, egy természeti katasztrófa megköveteli a hivatásos és civil segítségnyújtó szervezetek pontos, és folyamatos koordinációját. A kialakított térinformatikai adatbázisokkal, kliens oldali adatfelvételi, és megjelenítési lehetőségekkel rendelkező polgári védelmi támogató rendszer a fenti követelményeket teljes mértékben képes kielégíteni. Az EKOP 1.1.10 projekt kapcsán megvalósított fejlesztés, a HELIOS nevű, a Polgári védelmi és civil mentő szervezetek központosított erő-eszköz nyilvántartását és mozgósítását segítő rendszer lehetővé teszi a:

- Polgári Védelmi szervezetek adatainak nyilvántartását,
- A tagok nyilvántartását,
- Az igénybe vehető eszközök nyilvántartását,
- A rendelkezésre álló speciális gépjárművek nyilvántartását,
- Az erők és eszközök mozgósítását,
- Valamint tömeges útvonaltervezést.

Veszélyes áru szállítás

A katasztrófavédelem egyre több hatósági jogkört tudhat magáénak. A hatósági feladatok végrehajtásának segítésére, egy, a veszélyes áruk közúti és vasúti szállításának koordinálást biztosító szoftverrendszert is sikeresen üzembe állítottunk. A veszélyes anyagok szállításának kezelését biztosító szoftverrendszer lehetővé teszi:

- Veszélyes anyagok gyors azonosítását,
- Terjedési modellezést, a veszélyes anyagra és az időjárásra vonatkozó adatok bevitelének és kezelésének lehetőségével,
- A vasúti veszélyes áru szállítások bejelentéséhez webes elérésű felület biztosít.

A bejelentéshez kapcsolódóan az alábbi szolgáltatások kerültek kialakításra:

- A BM OKF által biztosított regisztrációs, szigorú autentikációs bejelentkezés,
- A feltöltött bejelentések adatbázisban rögzítése,
- A bejelentett adatok (belépési pont, útvonal stb.) térképes megjelenítése.

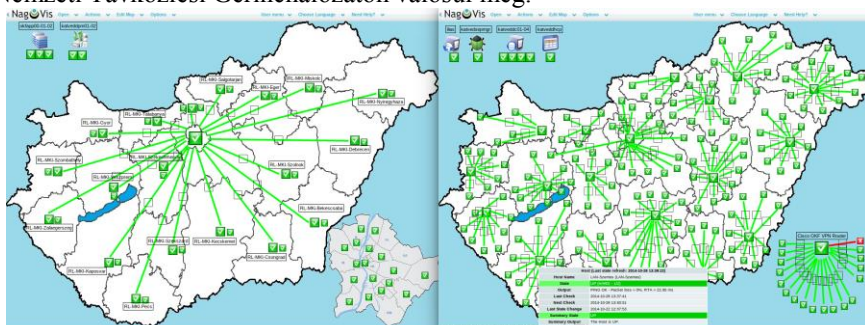
Gépjármű nyilvántartás

Nem tartozik teljes mértékben a műveletirányítás fogalomkörébe, azonban a folyamatos üzemeltetés miatt rendkívüli fontosságú gépjármű nyilvántartási rendszerünk is kifejlesztésre került. A rendszer biztosítja a járművek teljes élettartama alatt azok minden adatának adatbázisban történő rögzítését, statisztikák készítését. A „Szolgálati gépjárművek kezelése” című fejlesztés lehetővé teszi:

- A szolgálati gépjárművek nyilvántartását,
- Az elektronikus gépjármű igénylés biztosítását a felhasználók számára,
- Az üzemanyag felhasználások kimutatását,
- Vonulási statisztikák készítését,
- Kötelező szerviz és műszaki vizsgáról történő értesítés küldését,
- A karbantartások és felújítások nyilvántartását.

Informatikai rendszerek

A BM OKF más államigazgatási intézményhez hasonlóan telephelyei közötti adatkapcsolatok kialakítása érdekében a kormányzati szolgáltatótól veszi igénybe az összeköttetések kialakítását. A katasztrófavédelem telephelyeinek száma mára már meghaladja a 200-t, melyek között az adat- és hangkapcsolat titkosított módon, a Nemzeti Távközlési Gerinchálózaton valósul meg.



7. ábra: A Nagios hálózati felügyeleti rendszer

Mivel az egyes telephelyek közötti adatkapcsolat működése, rendelkezésre állás néhol kritikus fontosságú, ezért az informatikai szakterület monitoring rendszert alakított ki, mely képes felügyelni az egyes helyszínek adatkapcsolatának megléte és egyben rendelkezésre álló kapcsolat minőségét.

A jogszabályváltozással létrehozott, több mint 10 000 fős szervezet, több mint kétszáz telephelyen, több ezer gyengeáramú informatikai végponttal működik. A központi szolgáltatásokat a felhasználók ezen informatikai alpinfrastruktúra felhasználásával érik el. A biztosított informatikai szolgáltatások (telefonía – VoIP, levelezés, ügyviteli feladatok, szakirányítási rendszerek, műveletirányítás) a szer-

vezet életébe beépült, nélkülük az intézményre háruló feladatok ma már nem lennének elvégezhetőek. Ezért a monitoring rendszer kiterjesztésre került az országos informatikai szolgáltatásokra is.

A monitoring rendszer alapjában véve nem sokat ér állandó felügyelet nélkül. Ezért a szervezetünk az informatikai szakterületen informatikai ügyeleti szolgáltatást tart fenn, akik képesek a munkaidőn kívül elvégezhető karbantartási feladatok elvégzésére, továbbá a 24 órás felügyeletet igénylő IT rendszerek menedzselésére. A szolgálat kapcsolatban van más kormányzati és államigazgatási intézmény informatikai ügyeleti szolgálatával az esetleges meghibásodások azonnali kezelése érdekében.

Intézményünk a feladatrendszeréből adódóan több más szervezettel is kiépített adatkapcsolattal rendelkezik. Ezen adatkapcsolatok felhasználásával a szakmai szervezeti egységeink a munkájukhoz szükséges információkhoz képesek hozzájutni a nap 24 órájában.

A 2013-as év az informatikai biztonság szabályozottságában komoly változást jelentett. Megjelent az állami és önkormányzati információs rendszer biztonságáról szóló 2013. évi L. törvény, és annak végrehajtási rendeletei. A BM OKF az elsők között tett eleget annak, hogy a megfelelő biztonsági osztályba sorolja információs rendszereit és a besorolásnak megfelelő fizikai, logikai és adminisztratív védelmi intézkedéseket tegye. Az intézményünk jó kapcsolatot ápol a kormányzati eseménykezelő központtal (Gov-CERT), akik megfelelő mennyiségű információval látják el a BM OKF-et az államigazgatási és más informatikai rendszereket esetlegesen érintő sérülékenységekről.

Az informatikai szakterületünkön belül kialakításra került a fejlesztési terület is. Hathatós munkájukkal kialakításra került a BM OKF műveletirányítási rendszere, mely nem csak fejlesztési, de komoly térinformatikai, távközlési és rendszerintegrációs feladat elé is állította az informatikai szakterületet. A rendszer közös munkával elkészült és évek óta hatékonyan szolgálja a katasztrófavédelmi műveletirányítási, döntéstámogatási és egységes adatgyűjtési, adatszolgáltatási munkákat.

Összegzés

2010-től a magyar katasztrófavédelmi szervek jelentős átalakuláson mentek keresztül. A BM OKF és ezen belül az informatikai szervek, a fejlődés élén járva, felismerték a problémákat, majd ezekre a problémákra megpróbálták gyors, és egyszerű informatikai, távközlési, térinformatikai megoldásokat szállítani a katasztrófavédelem tűzoltási, polgári védelmi, iparbiztonsági, valamint logisztikai szervei számára. Ez az átalakulás, valamint a technikai, technológiai lehetőségek, természetesen pénzügyi erőforrásokkal párosítva, lehetővé tették, hogy az ország lakosságának katasztrófavédelmi biztosítását végző szervek 2014 végére olyan rendszereket vehessenek igénybe, amelyek megfelelnek a kor színvonalának. Az új kockázatelemzési módszerek, valamint az egyre egységesebb és nagyobb adatbázisok, a szervezetek közötti szélesebb adatkommunikációs lehetőségek magukban rejtik a további fejlődés lehetőségét.

**HTEST**

Your partner for electronic test & measurement solutions.

**KEYSIGHT
TECHNOLOGIES****HAEFELY
HIPOTRONICS****ADLINK
TECHNOLOGY INC.**

H TEST group is a leading supplier of test & measurement instruments and systems for industry, education and telecommunications. We are currently operating in the Czech republic, Slovakia, Austria and Hungary. Our company was established in summer 1999 in Prague, Czech republic and starting 1st September 1999 we were appointed as an authorized distributor of Agilent Technologies test and measurement products for Czech republic. In 2001 we have opened subsidiary sales office at Slovakia . In May 2010, our subsidiary company x.test GmbH started its business in Wien, Austria.

And finally, in July 2013 our last subsidiary company H TEST Hungary Kft. was found in Győr, Hungary. We are offering instruments and systems for measurement of electrical and non-electrical quantities. We are supplying wide variety of test instruments, test solutions and accessories from renowned manufactures such as: Amplifier Research, Haefely Hipotronics EMC, EMSCAN, Pasternack enterprises, Keysight Technologies, Adlink Technologies, etc.



H TEST Hungary Kft.
 Gesztenyefa u. 4.; 1.em/No.3;
 H-9027 Győr, Hungary
 Phone: +36 203 137 079
 +36 96 999 262
 Fax: +36 96 999 263
 E-mail: info@htest.hu
www.htest.hu



A NATO HÁLÓZAT NYÚJTOTTA KÉPESSÉG

Rezümé

A NATO hálózatközpontú hadviselésének alapvető szervezési eleme a Hálózat Nyújtotta Képesség, amely magába foglalja a teljes technikai infrastruktúrát, a kiépített IP alapú kommunikációs és információs hálózatokat, valamint a kezelő személyzetet. Rendeltetése a parancsnok és törzse részére a döntéshozatali folyamatok támogatása, az aktuális műveleti kép kialakítása, valamint a csapatok minél szélesebb körű valós idejű információval történő ellátása.

Kulcsszavak

Hálózat központú hadviselés, NNEC, Hálózati és Információs Infrastruktúra, integrált rendszerszolgáltatás

Bevezetés

A NATO Hálózat Nyújtotta Képesség (továbbiakban: NNEC) alapelveit az NATO Tanácsadó, Vezetési és Irányítási Tanácsnak ¹ a „NATO Network Enabled Capability Feasibility Study”² című tanulmányában fogalmazta meg. Ebben került lefektetésre megalakításának alapvető módja, célja, műveleti használhatósága és kulcsfontosságú elemei, amelyek a következők:

- a hálózati információs infrastruktúrákban történő egységes nézőpont,
- egy biztonságos, strukturált, adatfeldolgozó és szolgáltató mechanizmus kidolgozása,
- IP alapú kompatibilis kommunikációs infrastruktúra kiépítése,
- a kompatibilitás elérése érdekében egy egységes interfész szabványrendszer kidolgozása,
- szoftverrádiók szabványosítása a szövetségi kommunikáció zavartalan működése céljából,
- NATO szintű hálózati információs infrastruktúra kidolgozása.

„A NATO Hálózat Nyújtotta Képesség úgy írható le, mint egy erős, globálisan összekapcsolt hálózati környezet megvalósítása (beleértve az infrastruktúrát, a rendszereket, a folyamatokat és az embereket), ahol az adatok megfelelő időben és zavartalanul kerülnek megosztásra a felhasználók, az alkalmazások és a platformok között polgári és katonai együttműködési (CIMIC)³, valamint háborús körülmények között egyaránt. A biztonságos csatornákon összekapcsolt emberek és rendszerek, időtől vagy helytől függetlenül, a hálózatközpontú képességek lehetőségei miatt egy továbbfejlesztett képet kapnak a jelenlegi helyzetről, és jelentősen lerövidül a döntéshozatali folyamat”^{iv}

A jelenlegi és jövőbeli katonai tevékenységek hatását nagymértékben azok képességének hálózati kialakítása fogja meghatározni. A hálózatokban rejlő erő nem

¹ NATO Consultation, Command and Control Board (NC3B) – NATO Tanácsadó, Vezetési és Irányítási Tanácsnak

² NATO Hálózat Nyújtotta Képesség megvalósíthatósági Tanulmány

³ Civil-Military Co-operation

új keletű dolog. Technikai fejlődések időről – időre meggyorsították az információ továbbítását, megosztását kezdve a géptávírótól egészen az optikai, illetve műholdas összeköttetésekig. A Hálózat Nyújtotta Képesség kellő időben a megfelelő helyen képes biztosítani az információkat, felderítési adatokat, ezzel támogatva a parancsnoki döntéshozatali folyamatokat és tevékenységeket. Ennek kialakításához szükséges a rendelkezésre álló eszközök, szoftverek, eljárasmódok, struktúrák és személyzet fejlesztése alátámasztva egy biztonságos, robosztus, kiterjedt hálózattal. A NNEC a következő képességeket nyújtja a felhasználók, illetve szervezetek részére:

- a felderítési adatok és információk széles körét, ezzel támogatva a katonai döntéshozatali folyamatokat,
- integrálja a felhasználó személyzet, a fegyverrendszerek, a szenzorok és a támogató elemek képességeit,
- erősíti a saját erők védelmét, valamint csökkentik a baráti tűz lehetőségét,
- növelik az interoperabilitást és együttműködést a szervezeten belül, valamint a különböző szervezetek között mind nemzeti, mind nemzetközi környezetben,
- optimalizálja a rendelkezésre álló források felhasználását,
- fejleszti az információmegosztó képességet,
- lehetővé tesz egy jóval hatékonyabb vezetési és menedzselési struktúrát.

A NATO hivatalos megfogalmazásában a NNEC a következő:

„A NATO hálózat nyújtotta képessége a szövetség kognitív és technikai képessége, amely egyesíti a műveleti környezet különböző alkotóelemeit a stratégiai szinttől a taktikai szintig a hálózati és információs infrastruktúrán keresztül.”^V

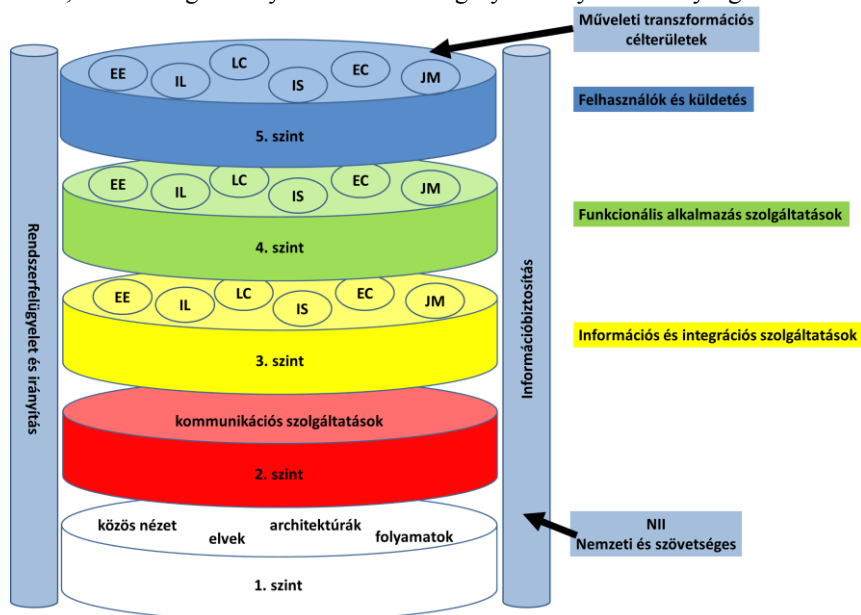
A Hálózati és Információs Infrastruktúra

A Hálózati és Információs Infrastruktúra (továbbiakban: NII)⁴ biztosít egy olyan gerincet, amelyen keresztül az együttműködés és az információ megosztás megvalósulhat a felhasználók között, és csökkenti a döntésciklus időt. A NNEC Megvalósíthatósági Tanulmány egy szövetségi szintű NII kiépítését javasolja, „amely biztosít egy hálózatközpontú környezetet, ahol az információs rendszer minden szintje interoperabilitás egymással azáltal, hogy egyesíti a jelenlegi és a jövőbeli nyílt szabványokat egy közös kialakuló globális keretben, amely alkalmazza a közös elveket és folyamatokat...”. Az új NII lehetőséget nyújtana rugalmas, alkalmazkodó, együttműködő alkalmazások és információs szolgáltatások fejlesztésére, amelyek támogatják a jövőbeni NATO-műveleteket a C4ISR5 minden területén ugyanúgy, mint egyéb igényeket, amelyeket a NATO Stratégiai Parancsokság transzformációs célterületeivel azonosítottak.

⁴ Networking and Information Infrastructure

⁵ Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance – Vezetés, Irányítás, Kommunikáció, Számítógép, Hírszerzés, Megfigyelés és Felderítés

Az NII-t négy képesség komponens alkotja, amelyek a közös nézet, az elvek, az architektúrák és a folyamatok. Ezen komponensek segítségével képes támogatni többek között olyan területeket, mint a kommunikáció, az információbiztosítás, az integráció, a rendszermenedzsment és a felügyeleti szolgáltatások. A műveleti transzformációs célterületek, mint az NII által úgyszintén támogatott területek, az Expedíciós Műveletek (továbbiakban: EO)⁶, az Integrált Logisztika (továbbiakban: IL)⁷, Megerősített CIMIC (továbbiakban: EC)⁸, Összhaderőnemi Manőver (továbbiakban: JM)⁹ és az Információs Rendszer (továbbiakban: IS)¹⁰, mint az információs főlény alapelemei. Az információs főlény az a képesség, amely lehetővé teszi, hogy a megfelelő információ a megfelelő személyek részére a megfelelő időben álljon rendelkezésre. A NATO úgy határozza meg az információs főlényt, mint egy műveleti előny, amely azokból a képességekből ered, amelyek biztosítják az információ gyűjtését, feldolgozását, és terjesztését zavartalan információáramlás mellett, illetve megakadályozzák az ellenség ilyen irányú tevékenységeit.



10. ábra A NNEC fejlesztésének kerete

Forrás: NATO Network Enabled Capability Feasibility Study

A fenti ábrán látható, hogy az NII biztosít minden olyan információs folyamatot, ahol az 1. szinten megtalálható alapelemeknek megfelelően az információ különböző kommunikációs szolgáltatásokon és alkalmazásokon keresztül eljutnak a felhasználókhoz a célok megvalósításának támogatása érdekében. Ebben az eset-

⁶ Expeditionary Operations

⁷ Integrated Logistics

⁸ Enhanced CIMIC

⁹ Joint Maneuver

¹⁰ Information System

ben az NII nemzeti és NATO által nyújtott kommunikációs hálózatokból és információs infrastruktúra képességekből épül fel. Ez több szemszögből is megvizsgálva azt jelenti, hogy az NII az „elérhető hálózatok hálózata”, amely támogatja a NATO Hálózat Nyújtotta Képesség fejlesztését. Ez a hálózatok hálózata elv egy olyan kapcsolati rendszert takar, amely egy IP kommunikáción alapul, és minden egyes olyan összeköttetést magában foglal, amely a legkisebb elemtől a legmagasabb szintekig felmerülhet. „... az adatnak, hangnak és videónak csatlakoztathatónak és átvihetőnek kell lenni a hálózaton keresztül, amely biztos működést kell ellásson bármilyen média továbbítása esetén, annak érdekében, hogy biztosítsa a megfelelő információt a megfelelő helyen és időben. Az IP az egyetlen technológia, amely ezeket a követelményeket kielégíti.”^{vi} Az alapja a már meglévő kommunikációs hálózatok egymáshoz csatolása olyan módon, hogy az képes legyen minden típusú információ továbbítására bármilyen körülmények között. Ez a környezet az állandó telepítésű hálózatoknál könnyedén kialakítható, és egy missziós környezetben is, ahol az abban részt vevő alegység egy fixen telepített vezetési ponton, táborban helyezkedik el. Farkas Tibor a következőt írta doktori disszertációjában: „Minden esetben széleskörű képességekkel és szolgáltatásokkal rendelkező híradó- és informatikai rendszer került kiépítésre, amely biztosította a kontingensek vezetését és irányítását.”^{vii} Ebből látható, hogy missziós környezetben úgyszintén egy nagyterjedésű, széles spektrumú kommunikációs hálózatot kell kiépíteni, mely megfelel a NATO, illetve a szövetséges szabványoknak a hazai kapcsolattartás és az együttműködés folyamatos fenntartása érdekében. A problémát az interoperabilis környezet kiépítése esetében a mobil hálózatok jelentik. Ebben az esetben több olyan probléma is felmerülhet, ami miatt az összeköttetés nem valósítható meg. Ilyen lehet például, hogy két különálló hálózat nem ugyanazokat a protokollokat alkalmazza, ezáltal nem képesek egymással kommunikálni. Ennek kiküszöbölésére szükséges olyan hálózati csomóponti elemek üzemeltetése (például egységes, szabványosított csatlakozó elemek), amelyek szükségesek harcászati adatkapcsolat vagy harcászati szoftverrádiók alkalmazása esetén, illetve a nem IP-alapú kommunikációk alkalmazásánál, mint például a fentebb említett nagytávolságú vezetékes távbeszélő hálózatok. Ezek segítségével már képesek vagyunk kiépíteni egy mobil telepítésű hálózati környezetet, ahol megtalálhatóak az ad-hoc hálózatok, az interoperabilis nagy sáv szélességű hálózatok és a megfelelő biztonsági eljárásokkal védett szoftveralapú rádióhálózatok. A rejtett vezetés, a biztonságos összeköttetések elérése céljából nem csak a rádióval történő kapcsolattartás során szükséges a rejtett csatornák használata, hanem ez ugyanúgy meg kell, hogy jelenjen minden egyes kommunikációs hálózat esetében is. „Az átviteli utak védelme (Transmission Security: TRANSEC) az adatok és vezérlő jelek védelmét jelenti, az átviteli folyamatba történő beavatkozás, vagy a jogosulatlan felhasználás ellen. Ennek hiányában lehallgatással, forgalomanalízissel olyan adatokat lehet összegyűjteni, amelyek támogatják az információs rendszerek elleni támadást; megtevesztéssel többfajta módon is zavart lehet okozni a hálózatokban, vagy egyéb módon lehet befolyásolni a hálózat működését.”^{viii} Információvédelmi szempontból megkülönböztetünk „RED” és „BLACK” oldalt, amely alapvetően a védett információt kezelő elemek elkülönítését jelenti. A „RED” olyan eszközök jelzése, amelyek a minősített adatot nyílt formában kezelik, a „BLACK” pedig olyan ele-

mek összessége, amelyek a rejtjelezett adatokat kezelik. Ez a Hálózat Nyújtotta Képesség esetében úgy jelenik meg, hogy minden biztonságos szolgáltatás egy „BLACK” IP alapú gerinchálózatra csatlakozik fel. Ez megköveteli, hogy minden forgalmat lebonyolító hálózatnak titkosítottak kell lennie, és magában foglalja a titkosítási technológiákat, amelyek támogatják a gerinchálózaton az információs szállítási követelmények valamennyi biztonsági elvárását.

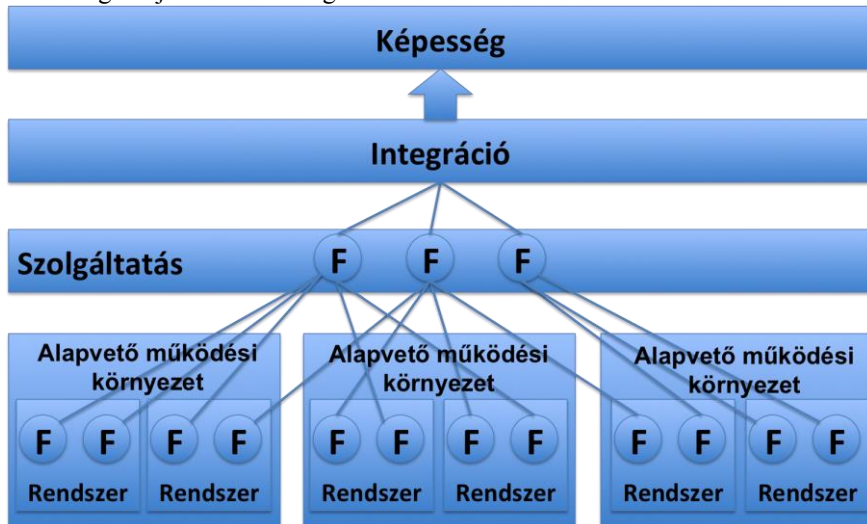
Az NII alapvető információs és integrációs elemei azok a szolgáltatásorientált felépítést támogató eszközök, funkciók és folyamatok összessége, amelyek támogatják az információ zavartalan megosztását és egy olyan rugalmas mechanizmust biztosítanak, amelyek alkalmasak egy a jövő kihívásaihoz jobban illeszkedő hálózati környezet kialakításához. Ehhez az szükséges, hogy egy szabványosított, interoperabilitás környezet kerüljön megalakításra, amely alkalmas a gerinchálózathoz történő kapcsolódásra, és az azon keresztül történő szolgáltatás megosztásra úgy, mint hálózati adattárolás, levelezés, biztonsági szolgáltatások, azonosítás és szolgáltatás menedzsment. A szolgáltatásorientált felépítésnek köszönhetően a rendelkezésünkre álló információk minden esetben hozzáférhetőek, láthatóak, értelmezhetőek lesznek attól függetlenül, hogy milyen más információs közegből érkeznek. Ezek biztosítják, hogy egy rugalmas, biztonságos szervezett információ hozzáférési és menedzselési mechanizmust tudjunk kiépíteni, amely támogatja a parancsnok döntéshozatali folyamatát, és a feladatok minél hatékonyabb végrehajtását.

Az integrált rendszerszolgáltatás által nyújtott képesség

Mint azt már fentebb említettem a hálózatközpontú műveletekhez elengedhetetlenül szükséges a kommunikációs eszközök, az adatok és szoftverek közötti interoperabilitás annak érdekében, hogy képesek legyünk a felhasználókat, a szenzorokat és a különböző működési területeket hálózati környezetbe hozni. A teljes technológiai kivitelnek képesnek kell lennie egy gyors kommunikációs képesség biztosítására a felhasználók között mindenfajta szolgáltatás területén átviteli közegtől függetlenül, ami lehet akár vezetékes (például: optikai kábel), vagy vezeték nélküli (például: rádió eszközzel sugárzott, mikrohullámú, infra, lézer, műhold). Annak érdekében, hogy a rendszer folyamatos rendelkezésre állást biztosítson, azt úgy kell megtervezni és kiépíteni, hogy egy, vagy több csomópont esetén is képes legyen a zavartalan információáramlást biztosítani, ezért öngyógyító és újjászerveződési képességekkel kell ellátni. Olyan szabványokon alapuló gerinchálózatot kell kiépíteni, amely garantál egy biztonságos összeköttetést az együttműködéshez más nem katonai szervezetekkel (kormányzati és nem kormányzati szervekkel, humanitárius szervezetekkel), kereskedelmi és civil kutatás-fejlesztési cégekkel.

Az információ megosztó hálózatok mellett megjelennek a NNEC esetében olyan fegyverrendszerek is, amelyeket szintén csatolni kell a gerinchálózathoz, ezzel támogatva a csapatok harctevékenységét. Itt beszélhetünk föld-föld, levegő-föld rakétákról, pilótánélküli repülőgépekről és minden olyan eszközről, amely rendelkezik hálózati képességgel. Egy ilyen hálózatba kötött fegyverrendszer esetében például a rakéta kilövését követően is módosítható a célpont helye, amennyiben az már elmozdult, vagy maga a célpont. Minél több ilyen eszközt használunk annál fontosabb a nagy sebességű gerinchez történő csatlakoztatásuk, amely képes

támogatni a hálózat minden egyes elemét, és ezáltal összehangolhatóvá válik a feladat végrehajtásához szükséges eszközök és rendszerek alkalmazása.



11. ábra Az integrált rendszerszolgáltatás által nyújtott képesség

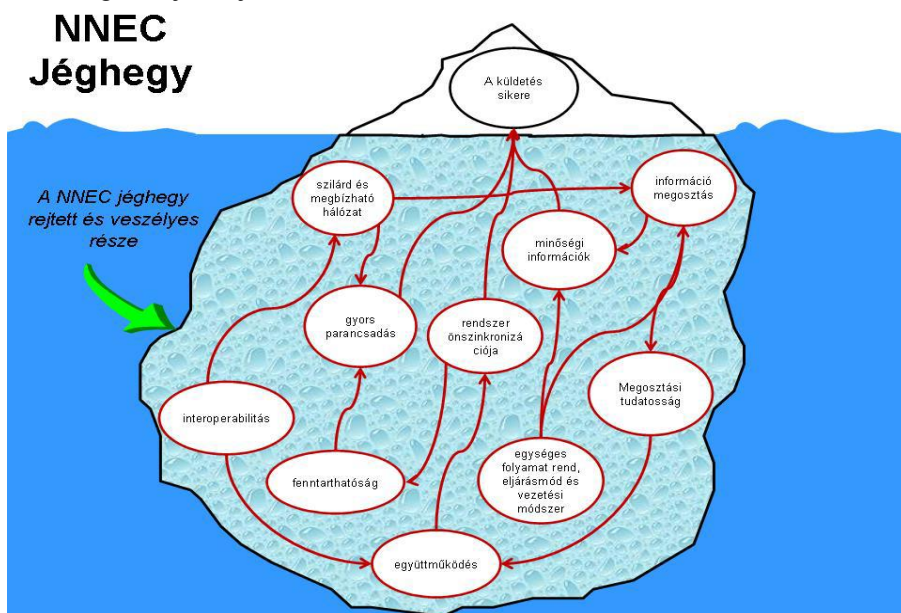
Forrás:

http://www.wrgrid.org.uk/Resources/Leaflets/WRG_NECTISE_Sept2007.pdf

A szolgáltatásorientált felépítés esetében jól látható, hogy különböző rendszerek biztosítanak számunkra fontos funkciókat. Nem szükséges, hogy ezek a funkciók feltétlenül egy szolgáltatótól érkezzenek, maga a környezet alkalmas arra, hogy ezeket centralizálja, és mindez egy olyan képességgel ruház fel minket, ahol különböző platformokon¹¹ el tudunk érni minden számunkra szükséges információt, adatbázist, alkalmazást. Katonai viszonylatban ez annyit jelent, hogy képesek vagyunk minden egyes elemről, mint alapvető működési környezettől funkciókat (információkat) kiemelni, az abból számunkra fontos elemeket kiszűrni, integrálni, ezáltal a vezetés –irányítás képességét javítani. A hálózat nyújtotta képesség egy ilyen rendszer integrációt követel meg, amely összefogja az egymástól független elemeket, amelyek egy fejleszthető, működő és költséghatékony környezetet biztosítanak. Az integrációnak köszönhetően megkapjuk az úgynevezett rendszerek rendszerét, amely biztosítja a hálózati képességet a kapcsolatokon, az információ megosztáson, a személyeken, eszközökön és folyamatok hálózatba kapcsolásán keresztül. Ez a nagytekercsű hálózat alkalmas nagy méretű felhasználói kört kiszolgálni. Katonai környezetben ez jelenthet egy dandárt, vagy magasabb egységet, ahol a katonák fegyvernemtől, szakcsapattól függetlenül közvetlen összeköttetésben állhatnak akár a legmagasabb szintű parancsnokokkal is, amennyiben rendelkeznek a megfelelő jogokkal és hozzáférési engedélyekkel. Amennyiben

¹¹ Platform: Alapvető működési környezet, amely egy számítógép vagy információs elektronikus eszköz hardver és szoftver elemeiből áll, és meghatározza az ott futtatható alkalmazásokat, programokat.

nyiben a rendszer megfelelően került megtervezésre és kiépítésre egy szilárd és megbízható hálózatot kapunk, mely minőségi információt biztosít a legmagasabb szintektől a legalacsonyabb szintekig, ezáltal garantálva az együttműködés lehetőségét a műveletben részt vevő minden egyes csapat és személy számára. Ehhez szükséges a rendelkezésre álló adatok tudatos megosztása, valamint egy egységes folyamat rend, eljárasmód és vezetési módszer alkalmazása. Ezek együttesen képesek garantálni a NNEC hatékony működését. Kerti András doktori disszertációjában mutatta be a NNEC jéghegy ábráját, amely bemutatja, hogy a fenti elemek milyen módon kapcsolódnak egymáshoz annak érdekében, hogy a küldetésünket sikeresen végre tudjuk hajtani.



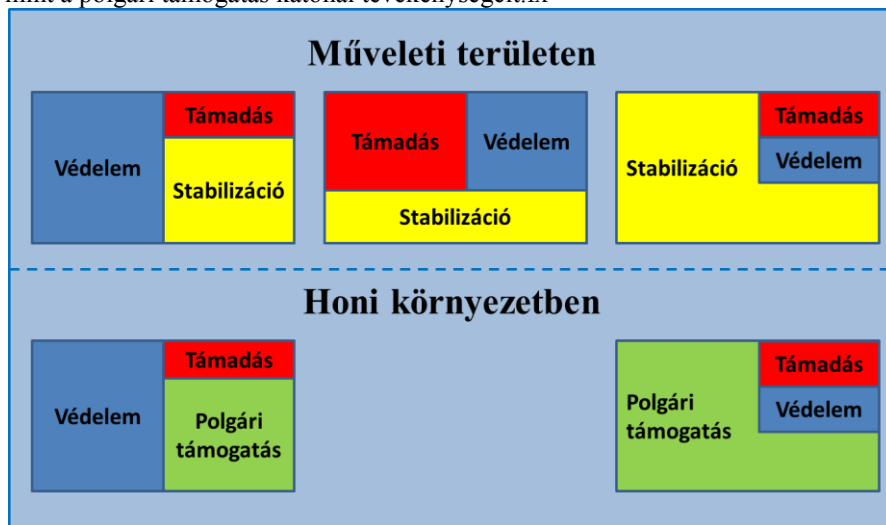
12. ábra A NNEC jéghegy

Forrás: Kerti András alezredes: A vezetési és információs rendszer technikai alrendszerének vizsgálata különös tekintettel a minőségbiztosításra és az átvitelbiztonságra, p.:33

A NNEC megfelelő működése nem csak az eszközök és alkalmazások együttműködésén alapul, hanem nagyon nagy hatással vannak rá a felhasználói személyzet megbízható információkon alapuló tudatos döntései is. Ehhez, az ábrából is látható, minőségi információkra van szükség, amiket a felhasználók tudatosan megosztanak egymással egy biztonságos és szilárd hálózaton. A szilárdság ebben az esetben a folyamatos és biztonságos rendelkezésre állásban mutatkozik meg, amit egy redundáns hálózat kiépítésével érhetünk el. Ebben az esetben egy-egy elem kiesése esetén is megmarad az összeköttetésünk, amely segíti a fenntarthatóságot és a gyors parancsadást. Amennyiben ezt megfelelően kialakítottuk a NNEC által garantálhatóvá válik küldetésünk sikere.

A NATO hálózat nyújtotta képesség műveletekre gyakorolt hatása

A NNEC nagymértékben befolyásolja a műveletek végrehajtásának módját. A tervezés a vezetés minden szintjén támogatásra kerül egy megfelelően kialakított hálózati környezet által. A parancsnokok egy sokkal részletesebb és könnyebben rendelkezésre álló felderítési adatbázist kaphatnak, amely egy biztosabb képet nyújt az aktuális műveleti helyzetről, és lehetővé teszi egy valós idejű döntéshozatal véghezvitelét. A tervezési folyamatok is felgyorsulnak, könnyebb együttműködést biztosít a tervezésben részt vevő személyek és törzsek között, valamint a parancsnok szándéka is nagyobb körben, gyorsabban és pontosabban terítésre kerülhet. Alkalmazásával kialakításra kerülhet egy térképi felületen megjelenített Összhaderőnemi Műveleti Kép (továbbiakban: ÖMK), amelyen megtalálható a saját csapatok mellett az ellenséges, illetve semleges csapatok egyaránt. Az ÖMK-n megjelenhetnek személyek, eszközök, alegységek, fegyverrendszerek és logisztikai elemek, azok helye, felelősségi körzete és mozgása. Alkalmazható összhaderőnemi műveletek esetében, amely azt jelenti, hogy a szárazföldi csapatok mellett megjelenhetnek a légierő, a haditengerészet elemei is, valamint a különböző speciális alakulatok is alkalmazhatják. A parancsnokok a hálózatközpontúságnak köszönhetően képesek minden egyes rendelkezésükre álló eszköz esetében annak csak a számukra fontos elemének alkalmazására, amelyet koalíciós környezetben úgyszintén lehetőségük nyílik megválasztani a közös együttműködés sikeres kiépítésének megvalósításához. A szenzoroknak köszönhetően meghatározhatóak a saját, illetve ellenséges szárazföldi, repülő eszközök, valamint hajók és ezek rögzíthetőek egy térképi felületen, amely valós időben a szervezet, szövetség valamennyi parancsnoknál megjelenik. Támogatja a Teljes Spektrumú Műveleteket, amelyek magukba foglalják a támadást, védelmet, stabilizációs műveleteket, valamint a polgári támogatás katonai tevékenységeit.



13. ábra A Teljes Spektrumú Műveletek felosztása
Forrás: Field Manual (FM) 3-0, *Operations*, Chapter 3

Ez a támogatás azonban csak akkor valósítható meg, ha az adott állam rendelkezik olyan költségvetési háttérrel, amely az összes műveletet támogató rendszer kiépítését képes biztosítani. Dr. Szenes Zoltán 2005-ben a következőket írta ezzel kapcsolatban: *„...Ebből fakadóan teljes spektrumú katonai műveletekre a NATO-ban egyedül az USA képes. (Még akkor is, ha az amerikai hadseregből is hiányoznak a „post-conflict” típusú „nemzetépítő” civil és katonai képességek) Széleskörű expedíciós képességekkel az európai országok egy kis csoportja (Nagy-Britannia, Franciaország, Olaszország, Hollandia, Spanyolország) rendelkezik, célirányos expedíciós képessége pedig csak néhány országnak (Németország, Belgium, Kanada, Dánia, Norvégia) van. Szelektív expedíciós képességeket tudhat magának Törökország és Lengyelország. A NATO-tagországok fele azonban (köztük Magyarország is) csak stabilizációs katonai képességek fölött diszponál...”^X*

Napjainkban azonban már több nyugati tagállam fordított nagyobb hangsúlyt a teljes spektrumú műveletekre mind honi, mind műveleti területeken. Magyarország jelenleg még mindig stabilizációs képességekkel rendelkezik, de amennyiben nagyobb hangsúly kerülne a hálózatközpontú hadviselésre a honi területen végrehajtott védelmi tevékenységek és polgári támogatás is egy biztos információs támogatást kapna. Ahhoz, hogy egy ilyen gerinchálózat megfelelő hatékonysággal működjön véleményem szerint egy homogén felhő alapú rendszer kiépítésére van szükség. A homogén környezet egy olyan hálózatot jelent, amely egy típusú munkaállomásokból, szerverekből, hálózati kártyákból, és operációs rendszerből áll, valamint korlátozott számú alkalmazást futtat. Minden egyes eleme egy eladótól, szolgáltatótól származik. A hálózati csomópontok ugyanazokat a protokollokat és ellenőrzési eljárásokat alkalmazza. Hatalmas előnye a rugalmasság. Az ilyen rendszerek könnyedén automatizálhatóak, ezáltal kevesebb manuális beavatkozást igényelnek, így a felesleges emberi erőforrások alkalmazása megszűnik, miközben a humán hibalehetőség is csökken.

Összegzés

A fentiekből levonható tapasztalatokat összegezve és értékelve megállapítható, hogy a NATO hálózat nyújtotta képesség alapját az interoperabilitás adja. Egy interoperabilis környezetben, mint integrált szolgáltatás képes összehangolni a kezelő személyzetet, a szenzorokat, a fegyverrendszereket és minden olyan eszközt, amely támogatja a vezetés-irányítási folyamatokat. Műveleti környezetben lehetőséget biztosít egy összhaderőnemi műveleti kép kialakítására, amely minden olyan információt tartalmaz, amely szükséges a parancsnoknak döntései meghozatalához.

Felhasznált irodalom

- [1] Molnár Ferenc: NATO-csúcstalálkozók Washingtontól Bukarestig, Nemzet és Biztonság 2008. Április
- [2] NATO Handbook 2006
- [3] C4ISR Architecture Framework version 2.0
- [4] NC3 Common Operating Environment and Transformation to the NATO Network Enabled Capability”, NATO C3 Technical Architecture

Hivatkozások jegyzéke

- ¹ NC3 Common Operating Environment and Transformation to the NATO Network Enabled Capability”, NATO C3 Technical Architecture, Volume 5, Version 7.0
- ¹ ACT Transformation Network Portal: <https://transnet.act.nato.int/WISE/Information>
- ¹ Magyar Sándor mk. őrnagy: Katonai kommunikációs igények, lehetőségek a békefenntartás vezetésének támogatásában, Doktori (PhD) értekezés, Budapest 2008, p.: 71
- ¹ Farkas Tibor főhadnagy: A válságreakáló műveletek vezetését és irányítását támogató híradó- és informatikai rendszer megszervezése a Magyar Honvédség többnemzeti műveleteinek tükrében, Doktori (PhD) értekezés, Budapest 2010, p.: 87
- ¹ Kassai Károly mk. alezredes: A Magyar Honvédség Információvédelmének – mint a biztonság részének – feladatrendszere, Doktori (PhD) értekezés, Budapest 2007, p.: 51
- ¹ Field Manual (FM) 3-0, *Operations*, Chapter 3
- ¹ http://www.biztonsagpolitika.hu/documents/1276888013_dr_szenes_zoltan_a_nato_jovoje_uj_strategiai_koncepciora_van_szukseg_-_biztonsagpolitika.hu.pdf (Letöltve: 2014. március 18.)

SECURITY OF TELECOMMUNICATION NETWORK MANAGEMENT SYSTEMS

Abstract

Telecommunication networks are considered as part of critical infrastructure. Network Management Systems (NMS) are responsible for monitoring, supervising and maintaining Telecommunication networks. These responsibilities also include Security Management, to ensure that the telecommunication networks are kept in a secure state. Furthermore Management Security is an essential task of Network Management Systems, in order to mitigate attacks targeting network management functions or to protect against malicious activities targeting managed telecommunication networks via network management functions. In this paper, key concepts in the security perspective of telecommunication network management are explained. Essential controls for Management Security and the most specific functions for Security Management are also presented.

Introduction

Trends show that in 2020 the connected devices reach 50 billion. These devices communicate each other directly, they can connect to local networks, or they communicate through global telecommunication networks such as GSM, WCDMA and LTE, while the core part of the above radio networks (e.g. IMS) are also used. These telecommunication networks are belongs to the critical infrastructure as they are vital for business and society.

Telecommunication networks consist of different heterogeneous network elements. There are nodes, which communicating in different radio networks simultaneously. Nodes can have different access coverage from pico-sized cells to supercells. There are nodes which can even be placed into less trusted environment and attackers might have even physical access of it. There are also networks, which do not follow the monolithic trust-ownership scenarios. In virtual networks, network resources are leased from competitors. In shared networks, competitors establish alliance and build a common unified network. In the future, serving excessive number of connected devices require telecommunication networks with enormous number of network elements.

Management of those volumes of heterogeneous networks is not easy. On the other hand, management functions must be well protected. As possessing a single node in the managed network cause less impact than successful attack on the management system. Though disabling the management system cause infinitesimal impact on the managed system, attacks from management systems could severely danger telecommunication networks. This is a good reason, why Telecommunication Network Management Systems should be considered to the critical infrastructure.

¹ Budapest University of Technology and Economics, Department of Telecommunications and Media Informatics, Ericsson Hungary

In the following chapter, the essential telecommunication security concepts are summarized, and then in Chapter III, the communication protocols of the Telecommunication Management System are presented. Amongst other perspectives, the security perspective in management systems is shown in Chapter IV. In the consecutive chapters, controls for Management Security and Security Management functions are detailed.

Telecommunication Management concepts

Management of the telecommunication networks can be performed at different management function layers [TMN]. Node or Element Management (EM) manages only a single network element in the telecommunication network. Node management may contain some control and monitoring functions, which are unique to the specific network element, like low level management functions, initial configuration or bootstrapping, or commands can only be used with direct physical access. Node Management can be used in emergency situation, or when higher level management systems are unavailable but connectivity in the management plane still exists. Furthermore, higher level management systems may utilize the services of Node Management (Figure 1).

Several, network elements of a similar type can be managed together, by forming *Domain Management*. Domain may consist of similar nodes in terms of functionality. It is typical that domains are built from nodes provided by same suppliers.

Network Management layer performs network-wide management functions on managed network elements. This includes the network level view of the managed network elements, provision and configuration of the managed nodes as well as the maintenance of the network capabilities. Furthermore, collecting and analyzing information about the managed network for fault detection and analysis, for statistical and performance analysis and for security.

Service management provides service monitoring and Service Level Agreement (SLA) management, where e.g. the status of the service is compared to SLA thresholds. Customer and service provider interface and interaction can belong to this management function layer.

Business management layer is quite different from the previous management functional layers. Its main purpose is to set up business goals for optimal investment and operation, and for the best capitalization. For this it needs interactions with the earlier mentioned management function layers. The business management layer was originally defined [TMN] to help in optimal investment in new resources, while the rest of the management layers provide optimal utilization of existing resources.

FCAPS Model

Management functions can be divided into five distinct parts according to FCAPS model, which is originally defined in OSI management functional areas [X700]. This approach is especially used in Network Management Systems (NMS).

Task of *Fault Management* is to recognize, to report and to correct faults. Abnormal operation in the system or abnormal input from the environment

generates notifications or alarms through the management system to the operators which can initiate corrective actions to resolve the problem.

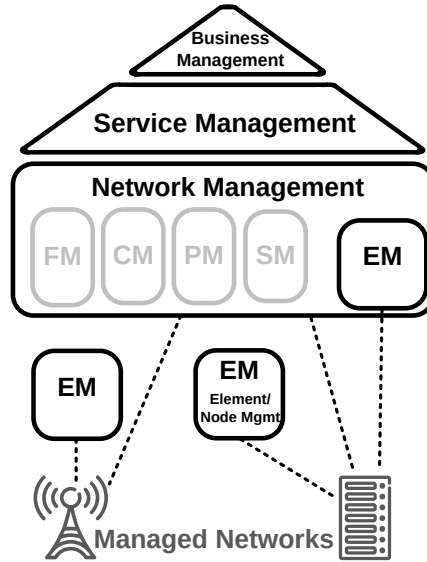


Fig.1. Management Function Layers and FCAPS model

Configuration Management deals with the parameterization, initialization and termination of the managed services. This also includes hardware management and software upgrade besides setting configuration parameters for the software of the managed network elements.

Performance Management gives the possibility to assess the effectiveness of the managed system. It has the task to collect statistical information, determine the quality of the system and initiate corrective actions to improve the effectiveness of the managed system. Corrective actions can be optimization and re-planning of network resources.

Accounting Management creates the ability to associate charges with the utilized resources, based on the amount of used, and the cost of the resources. Accounting includes functions to inform the users about the consumed resources, set up accounting limits in the resource consumption and provide complex function, where multiple resources and multiple cost paradigms are combined.

Security Management makes the enforcement of security policies possible, by managing security services and mechanisms. Security Management performs the distribution of security related information and it reports the security related events occurred in the managed system.

Deviations from FCAPS Model

Though the FCAPS model was a good logical partitioning to understand the main functions of the management system, in these days there are blurred borders in between them as in the following examples show.

Accounting functionality is achieved in telecommunication by charging functions, nodes and systems. The charging functionality is usually distinct from the management plane [TS32240] and rather part of the signaling/control plane.

Performance degradation caused by denial of service attacks can be observed by Performance Management, but detection of such attacks logically belongs to Security Management. This implies that Security Management has to contain a function, which has the same functions as Performance Management.

Similarly, to avoid duplication of functionality in Security Management; Configuration Management may also set up some security related configurations as remote configuration function is implemented in Configuration Management. In this case, configuration of security parameters may only differ from other configuration management activities in that it is using different access control assigned for configuration of security than used by other Configuration Management activities.

Furthermore, there are parameters, which are not considered as security related parameters, but they are essential for establishing security. For example setting up the date and time is considered as pure Configuration Management functions, while having incorrect date and time would render observability and accountability in security useless. Likewise Fault Management and Security Management has overlapping functionality, as reporting faults or reporting security related faults can be performed with the same functionality. Here again, only access control on viewing security related faults can be the difference (on the other hand other, distinct fault management for some security functions may also be implemented). FCAPS model does not cover the recently increasing importance of privacy, which may be classified as part of Security Management, too.

In the following, the interconnectivity of Telecommunication Network Management System is aligned with FCAPS model.

Connectivity architecture of Telecommunication Network Management system

Network Management Systems (NMS) shall be connected to its managed networks. The collection of such communication channels is called as southbound interface. Management system can also be connected to higher level (service, business) management layers, via the northbound interface. Human operators manage the NMS on the UIbound interface either via graphical or command line interface.

In the south- and northbound interfaces, the basic structure of the FCAPS model can be found. For fault management [TS32111], CORBA, CMIP, SOAP and SNMP [RFC3877] protocols can be used. Configuration Management amongst others uses CORBA, CMIP, SOAP [TS32600], SNMP, Restconf, NETCONF [RFC6241] protocols. Furthermore for bulk data transfer - like software update - file transfer protocols are used. Performance Management [TS32401] for control messages CORBA, CMIP, SOAP can be used, on the other hand, retrieving of performance data can be achieved by using bulk file transfer protocol or streaming data channels as well (e.g. IPFIX [RFC7011]). Security Management can use CORBA, CMIP [TS32371], on the other hand NETCONF can also be used for installation, configuration and management of security services. For key and trust

management, a more secure alternative of the above configuration management protocols is CMPv2 [RFC4210] or SCEP [SCEP]. Collection of security audit trail and security alarms typically performed via syslog protocols.

UIbound communication can be proprietary, any client-server communication solution is allowed. On the other hand, implementations are often bound to development solutions, where user-friendly and useable graphical interfaces can be quickly developed; or they bound to development solutions, which have designer-friendly graphical interface development toolset, like Java. Java RMI and CORBA communication, HTTP based protocols are used there. Furthermore, for bulk configuration, solutions support command line interface (CLI) access as well. They are typically based on SSH.

Perspectives in Telecommunication Management

Telecommunication systems, including telecommunication management systems have several conspicuous properties. When designing or operating such systems, they must be considered from the perspectives [Arch] of these properties. These perspectives are performance, capacity, scalability, flexibility, usability availability, location, regulation, privacy and security perspectives.

A system shall meet performance expectations, which means that the system in some specific situations fulfils some predefined characteristic requirements. Performance can be defined as rate or burst of request handling capability, behavior under overload, processing time of a transaction, or the expected load on the system in terms of CPU, memory. For example a telecommunication management system has to manage a network while the CPU consumption shall not exceed 50% load during 90% of the time, while 95% of the performance data has to be collected from the nodes, and 99% of the security configuration change must be propagated to the nodes, and 99.99% of the incoming alarms must be handled by the management system.

Capacity perspective is where the system is able to handle some quantitatively defined capability. In management system capacity can be defined as the number of managed nodes, the number of managed radio cells. For example, the management system is required to handle 10000 LTE eNodeBs, or 10000 GSM RBS, or 5000 number of 2G and 4G network elements, or 30000 radio cells.

Scalability is an ability of the system to process increased (or decreased) volumes effectively. This means that by increasing the processing capability, the overall capacity is expected to be roughly linearly increased or expected to be increased following a predefined curve. In management system the scalability can be interpreted as follows. When the number of managed network elements or the number of managed radio cells are increased due to increased demand for the telecommunication service, then it is possible to add further processing capacity so that the management system is able to monitor and provision the growing network. It is important to emphasize that managing increased volumes shall not have any negative influence on other perspectives, like performance, security, usability and availability.

Flexibility at deployment is an ability of a system to alter its actual deployment configuration compared to the originally defined reference architecture. Flexibility

during operation is an ability to adapt to the continuously changing needs effectively. The effectiveness is measured as the cost of flexibility considering investment in development and cost of operational change.

Usability is a quality measure how easily a human can interact with a system. Usability is a supreme perspective when considering Telecommunication Management Systems. This is in contrast with managed nodes, where the capacity, performance, scalability, flexibility and availability perspectives have more focus than usability.

Availability - though there is a definition as being one function of security - in telecommunication terminology, the ability of providing some functions despite having multiple unintended, unpredicted or randomly occurring faults in the system. The term robustness is also related to availability, robustness means being fault-tolerant and stable.

Location perspective considers issues related to topological or geographical distribution of the processing components of the system, or problems related to scattered information across the system. Location perspective tries to address (geographically) location agnostic systems so that neither the location nor the distance (measured in space or in time) would have impact. There are situations, when considering location has advantages. For example, in an area, where earthquakes happen quite often, it is necessary to deploy redundant systems, and those systems must have a minimal geographical distance in order to provide availability. Some functions of the management system can be optimized by topologically placing them closer to the managed nodes. For example, if collectors of fault and performance data, or configuration management storages are multiplied and distributed locally in the managed network, then the effectiveness of such services, due to close proximity (lower delays and redundant availability) would be much better.

The telecommunication system shall be considered from Regulation perspective to be able to comply with laws that are in force. An example is the compliance to export restrictions of cryptographic algorithms.

Privacy perspective deals with subscriber privacy to be able to keep their personal information secret.

Security perspective is the viewpoint from where all security related issues are considered.

Security perspective

With regard to telecommunication network management systems, there are security expectations. These expectations in increasing importance are: self-protection, asset management, asset security management and asset protection.

Self-protection means the capability to protect itself against various attacks. Asset management is the capability to perform remote monitor, provision and maintenance functions of its managed networks. Asset security management is a subset of asset management, however to emphasize its importance from security perspective, it is discussed separately. Asset protection is the ability to protect the managed nodes and networks. It is obvious, that in case of attacks, the management system shall be able to protect itself. In case, some non-essential part of the mana-

gement system is compromised, it is also important to keep manageability of the network. Amongst the FCAPS model, security management is much more important, as by disabling security management, the consistency and the validity of security information in managed nodes and networks can render them vulnerable. On the other hand, even if security management cannot be handled, the most important single task is not to compromise the managed nodes and networks. The reason is that even if the management system is compromised, even if the manageability is lost, the managed nodes and networks can operate for a while. Though alarms, notifications or performance data will not be collected, security and other configurations are not going to be refreshed, the telecommunication nodes and networks are still able to serve.

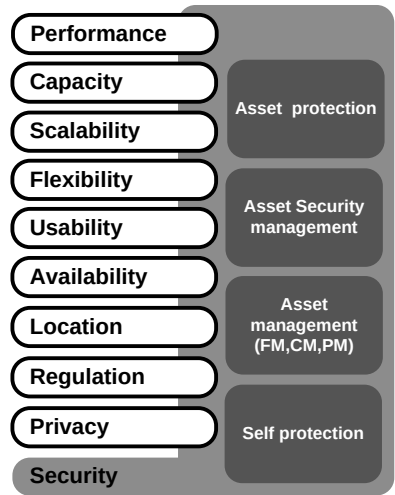


Fig.2. Security Perspective

There are situations where other perspectives are overlapping (Figure 2.) with security perspective as follows.

Perspectives linked with Security in NMS

Security and usability shall concur and not compete with each other. A management system with weak usability and strong security would motivate operators working with such management system to create shortcuts to simplify their daily work. These shortcuts circumvent the security, which would result in an unfriendly and unsecure system. A management system with good usability but weak security puts too much trust in the operators and too many expectations on the environment. Having immense trust gives authority to operators and it increases work agility. On the other hand, disgruntled operators may abuse this opportunity. Furthermore, the effect of unintended errors made by operators may also be formidable.

Regulation for Security defines technical, operational or other mandatory requirements on systems being part of critical infrastructure. Violating or ignoring them can result disciplinary actions.

Privacy has quite strong relation to security, as in most cases security (confidentiality) could provide protection to privacy. On the other hand, correlating non-confidential, distinct information may lead to the violation of privacy.

Security, Privacy and Location perspectives are overlapping in radio networks, as telecommunication radio networks provide freedom of movement, while for communication, location of the users is needed to be known. Location of the users can be considered as one privacy attribute. For this reason the location of the users are protected by security (as confidential information).

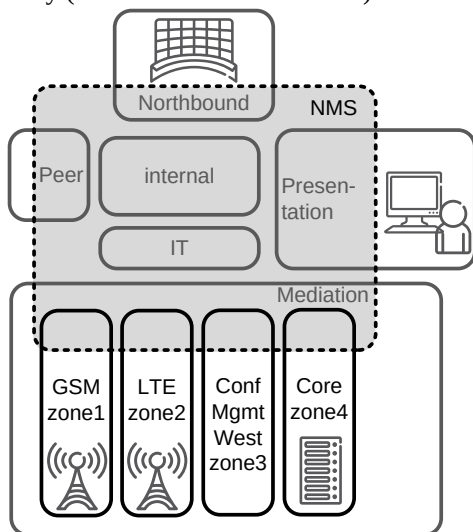


Fig.4. Zones in NMS and in Management Plane

Availability and Performance can be defined in Security as being able to withstand against attacks and even being able to provide services. This resiliency against malicious activities belongs to security perspective.

Location is also related in the logical plane concept of telecommunication as security function. The traffic, signaling and management planes are independent from each other and telecommunication equipment shall be at least attached to the management and the signaling planes (e.g. signaling gateway case) as in Figure 3. Another example where location and security perspective meet is the security network operation center concept. In this concept, the security management of several management systems are aggregated and integrated into one management system. This security network operation center only handles security management, but it can handle different networks, regions and countries.

Keeping in mind the security perspectives and expectations, two main goals of the security of telecommunication management can be formulated: Management Security and Security Management. The Management Security deals with the expectation of self-protection and asset protection; while the Security Management deals with asset security management.

Management Security

Management security deals with self- and asset protection expectations, thus how to protect the management and managed systems. There are several technical controls which could achieve these goals. Those can be classified into classical categories (architectural, hardening, access control, security event and audit logging, communication protection and data protection), which can be applied to any information security systems.

Architecture

Considering the security architecture of network management system, we can identify the following properties. Telecommunication nodes can connect to three distinct logical planes, to user, signaling and management planes. However, management system can only reside in the management plane (Figure 3.).

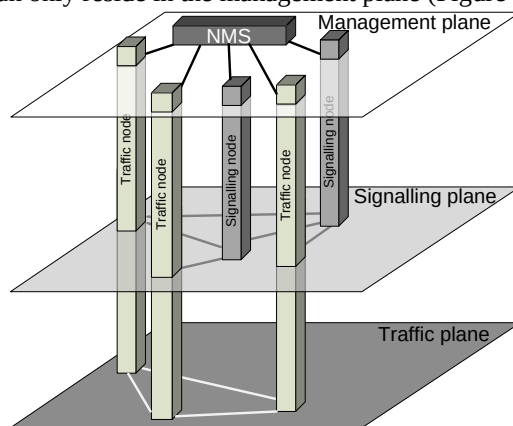


Fig.3. Telecommunication planes

On the management plane, in addition to the telecommunication management systems, management related interfaces of all telecommunication nodes are located. In order to decrease the attack possibility, compartmentalization on the management plane is necessary. The management plane is divided into distinct zones, and in one zone managed nodes with the same risk level are collected. Zones are separated by VLANs, Firewalls. In several cases, zones can be further divided based on technology (GSM, WCDMA, LTE, core network), based on node type (RBS, BTS, RNC), based on geographical location, or based on any other reasons. There could be for example, further refined zones determined by the tasks of the FCAPS model.

In each zones, the management system is connected.

The management system itself can be divided into several zones, based on main functionalities. Peer, presentation, internal, northbound, mediation (southbound) and IT zones can be identified. In the presentation, the UIbound communications, while in the IT zone, the management system related low level IT communications are grouped. Peer zone can contain communication with another management system (e.g. in case of hot standby redundant solutions). Internal zone contains communication of business logic of the management system. In the northbound and mediation zones, northbound and southbound communications are collected.

Mediation zone may be further divided; and in general as many mediation zones can be defined as many zones are defined in the managed network.

Authentication and Access Control

Access control category - amongst others - deals with the administration of the operators, including setting authentication and authorization credentials. Single-sign on (SSO) to management systems means that only a single authentication procedure is necessary and after successfully performing it, the operator is identified to all parts to, including all applications of the management system. For that to work, handing over the identity and proof of identity of the requestor in NMS shall be performed. Authentication is desired to be multi-factor to ensure strong identification. In addition to what the operator knows (e.g. password) proof shall be presented what the operator have (e.g. certificate, hard/softtoken) or objective evidence may be shown what the operator is (biometric identification). Authorization is sophisticated in management systems as it is not just an access control to the file system or to management system resources. When an operation is requested to be performed by an authenticated operator (human person) of the network management system, first the operation needs to be verified against the authorization database of the management system. In case the authorization is not denied, further authorization check needs to be performed, as the requested operation can have several influences on the managed system. Therefore, operations in NMS needs to be disassembled into atomic tasks and each atomic tasks needs to be authorized as well. For example if an operator requests performance measurements on some part of an LTE network, first the operator shall be checked, whether he is allowed to request performance measurements. Then checks have to be carried out whether the operator is allowed to collect the specific requested measurement. In case the operator is allowed, then it may trigger performance data collection operations from the managed network. Operators may also not be allowed to request such operations from some specific network elements in the management network. In this case, the authorization of a performance measurement operation fails; regardless the measurement 'in general' was allowed. This authorization mapping of NMS to managed nodes is essential, as it prohibits information leakage or misuse in NMS, and it prohibits unauthorized activities in the managed networks unintendedly initiated from NMS.

There are typical works performed by the operators of the management systems. These can be translated into workflows in the NMS, and there exists such predefined workflows. For example, a software upgrade needs to be performed on specific network elements in order to support new network functionality. The operator, who has received the work order to perform the software upgrade, is assigned in the authorization database of management system the software upgrade workflow. Though this authorization setting might be too wide, with having the software upgrade authority the operator is able to update software on live nodes in operation, nodes in different domains (GSM, WCDMA, LTE and core), nodes across the network (capital city, western part, etc.), and he is able to perform such action at any time with any version of the software to be upgraded. With this power, a disgruntled or careless operator is able to perform software upgrade on all

managed network elements in the network. In case an operator would do this, the entire managed network would start software downloads and activation, and finally the software upgrade ends with restart of managed nodes. In the best case, this would mean temporary unavailability of the nodes, so temporal network performance degradation. In case the uploaded software is faulty or malicious, the entire telecommunication network can be rendered useless. Therefore it is essential that an authorization workflow is always combined with further restrictions, including the location of the target nodes, target node types, specific target node identification, or any other restrictions on the workflow. Restriction can be based not only on network elements, but there can be any managed resources, like radio cells; or in WCDMA network, RNC domains (set of specific RBSes) as well.

There are tasks which are unique to NMS and tasks, which are unique to the network elements. There are tasks, which can be found in both the network element as well as in NMS. Expanding the authorization with the originator (interface) of the request can be important. There could be cases, when a task is not allowed for an operator to perform by using NMS, but in case by using node management or with direct access, the same operator is allowed to perform the same task. For example the command 'reboot' can be restricted to direct access only, and rejected from the NMS. The rationale behind by using direct access only is that it gives more awareness of the operator about the target node. On the other hand, there could be tasks which can only be performed in NMS and not in the node directly. For example, configuring the addresses of performance collectors would be much more reasonable to be specified in NMS as this information is primarily available there.

In Network Management Systems, there are atomic tasks for which authorization is associated. Chaining those tasks, new workflows can be built. This improves usability, as new workflows enable operators to adopt the behavior of management system to their operational processes, and not the operational processes are required to be adjusted to the behavior of the management software. An operator is authorized to execute a workflow, if for all atomic tasks of the workflow, the operator is authorized.

Atomic tasks are handled at different parts of the NMS within different software components. In these software components, authorization check needs to be enforced, to verify whether the requested atomic tasks are allowed. This also requires the unambiguous identification of the requestor. Therefore the identity traversal (handing over the identity and the proof of identity) is necessary. The most effective implementation is, when the software component receives a request to perform a task, it calls an identification/authentication function. If identity is successfully determined, an authorization enforcement function is performed. Authorization decision can be on the same software component, or in a dedicated decision point. In both cases, authorization decision shall be based a single authorization information point. This information point is the authorization database of the NMS. XACML [XACML] uses LDAP as the backend database for Authorization Information point. XACML implements Attribute Based Access Control (ABAC), (by defining policy sets, policies and rules), which quite cover the needs of authorization in NMS.

There are automated jobs of the management system which perform actions both in the management system and in the managed network. These jobs usually cannot be associated with any human operator. For example, checking the connectivity towards the nodes is a system function. This is needed for the management system and useful for all users of the management system. For automated jobs, instead of an operator is identified as the requestor, the NMS is associated with the request. For this, NMS itself has to have identification and authentication credentials, as well as NMS has authorization settings.

Hardening, Communication and Data protection, and Security logging

Into Hardening category - amongst others - the following tasks belongs: OS security hardening, software striping, configuration hardening, software patching, closing down unneeded ports, setting up personal firewalls, using virus and malware protections, setting strong crypto primitives, software signing and integrity protection.

Those tasks are classical information security tasks, likewise as in communication protection category. The specialty in telecommunication network management system is that in some cases, quite specific communication protocols are used. SNMP communication can be protected by using SNMPv3, though instead of, using IPsec or SNMP over DTLS [RFC6347] provides much more flexibility and stronger security. CMIP protocol is quite similar and less used as SNMP, TLS and IPsec can be used there. NETCONF use SSH [RFC6242] or TLS [RFC5539].

Security management provides AAA functions, amongst others LDAPs, RADIUS, DIAMETER can be used. Bulk file transfers are secured by either sFTP (SSH) or FTPs (TLS).

SOAP, HTTP protocols are protected by TLS. Command line interfaces can be tunneled into SSH. Java RMI can be secured by placing onto TLS. CORBA can be protected with TLS, in this case the solution is called as SSLIOP. It is important to emphasize, that even though the peers would use SSL/TLS, the communication to the name server shall also be secured, or name server should not be used.

For certificate, identity and trust management SCEP and CMPv2 can be used. In any other case IPsec could provide IP level communication protection.

For Security Event and audit logging, syslog can be secured by DTLS or TLS. As usual, security and audit events happened in NMS shall be created, collected.

Amongst others, logs and authentication information are quite important, as some logs are received from the managed networks, and some authentication credentials, authorization information are used in the managed networks as well. Furthermore, some performance related, and some other events may contain sensitive information, and the protection of those data has to be ensured. Relying only on the file system access control might not be the best approach; some information shall not even be in any storage. Integrity of the used software as well the confidentiality of the storage can be achieved by using hardware security modules, like TPM.

Security Management

In the following, the most relevant Security Management functions of NMS are explained. The centralized authentication and authorization solutions, Security configuration management, trust distribution, centralized log management security log analytics and secure bootstrapping functions are the most essential functions to achieve asset security management.

Centralized Authentication and Authorization for Managed Nodes

Administration of the accounts of the nodes can be done locally within the network element. In this case for each node, the administration needs to be performed distinctively, which puts high burden on the manageability and usability, especially in large volumes of network elements. Instead of the above, account provisioning can be centralized. Centralization would introduce other problems; a centralized account database needs to be synchronized to the network elements and it would be impossible to create new accounts in the network element. The industry best practice is that some minimal number of accounts is defined locally, and the operational accounts are defined centrally. The local accounts may have special privileges, usually for emergency situations or for troubleshooting purpose.

Not only the provisioning of the accounts can be centralized, but also the authentication can be performed by using a centralized authentication system. Centralized authentication can be divided into two distinct types, for those, which authentication decision is performed locally on the node (e.g. by using LDAPs), and for those, where authentication decision is performed centrally (e.g. by using DIAMETER protocol). The former places authentication decision to the node, therefore the node has to be well trusted. The latter case the node is only notified about the authentication decision; therefore nodes operating in more hostile environment can use this solution. For example, core nodes are expected to be placed into more secure environment than radio base station nodes with small radio cell size. As for small radio cells, the distance from radio source to an attacker is expected to be small.

In case the decision is made locally, then by caching authentication credentials is possible. In case network outage, authentication can be performed by using locally cached data. On the other hand, caching might not be wise. Cached authentication credentials may be revoked centrally. Meanwhile - due to (deliberate) malicious activities - network connectivity between the node and the central authentication system is broken. This results that credentials revoked centrally, remain still valid on the node.

Not only single-sign on (SSO) within NMS system can be used, but SSO from NMS towards the managed nodes. This means that operators, who successfully authenticated to the NMS is able to login to the managed network elements from NMS, without the need of re-authentication. This means, when the operator launches an element manager (EM, Figure 1.) or command line (CLI) access to a managed node, then no authentication needs to be performed. Since in this case, the user is already authenticated in the management system and the identity, authentication is forwarded to the managed network element. Note, that this does

not mean that the operator has also gained any access, as there might be that the operator has no authority on that particular node.

Authorization can also be centralized, similarly as authentication. Centralized authorization is used by using e.g. LDAPs, DIAMETER protocols. By using LDAP, the authorization information point is centralized, and the authorization decision and enforcement point is performed at the node. This approach can be used for secure nodes in trusted environment, for nodes in hostile environment may use technology, in which the authorization information and decision point is centralized, and only the enforcement point is local to the node.

Telecommunication nodes have quite sophisticated authorization settings, each command and action can be tagged with access control. For example, in Configuration Management, the authorization has to be detailed till Managed Object (MO) level. In some case, even this granularity requires further refinement: even in some cases MO values and parameters needs to be decided, whether allowed to be set. This sometimes places quite heavy burden to store all access control information in a centralized authorization information point.

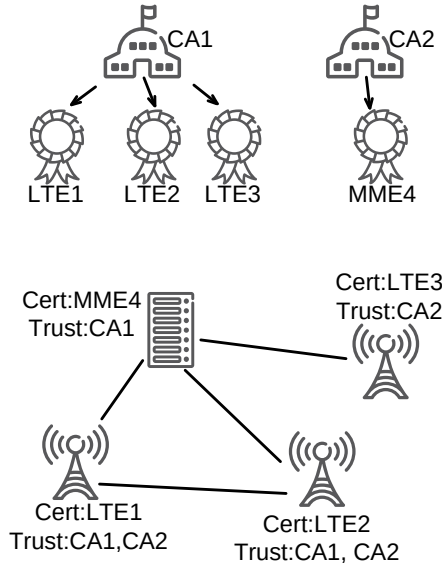


Fig.5. Trust Management and communication

CA1 and CA2 are Certificate Authorities issue certificates for LTE radio base stations and MME nodes respectively. Those nodes, which communicate with LTE base stations shall have CA1; and LTE base stations, communicate with MME shall have CA2 as trust anchor.

For that reason, authorization information point for network elements can be divided to two parts (as opposed to the authorization information point of NMS). Let us define the ‘user-role relation’ as the association of human user with some abstract authorization settings called roles. Furthermore, let us define the ‘role-access control relation’ as the association between the abstract authorization

settings with the set of access control settings the role defines (so a role is a grouping of the access control attributes defined in the node). The ‘user-role relation’ can be stored in the centralized authorization server, while the ‘role-access control relations’ are stored in the node locally. The disadvantage is that the role-access control relation may be different in different nodes. For that reason, predefined, managed system-wide role-access control relation is necessary. Furthermore, for those role-access control relations, which are not system-wide, central provisioning and distribution is advantageous.

Security Configuration Management

Security configuration management deals with the setting of the security properties of the managed nodes. It can even handle the security settings of the network management system. Its main purpose is to enforce security policy by configuration. It is imperative that the identity of the requestor of the configuration change is known, not only for audit logs, but for authorization as well. For that, identity delegation from NMS to the managed node is needed, with proof for the managed node that which operator requested the command. The delegated requestor can then be authorized (user-role and role-access control relation is verified). Note that here dedicated authentication procedure of the operator may not be needed, if there is an objective proof that the operator has requested the command.

Security configuration management handles key and password management for shared symmetric and for asymmetric keys. These passwords and keys can be used in traffic and signaling plane as well as for management plane (e.g. secrets for IPsec SAs; symmetric and public keys for IKEv2 or passwords for SNMPv3 USM).

Trust Management

Trust distribution and certificate management also belongs to Security configuration management, on the other hand, there are specific protocols for that purpose besides the usual configuration management solutions (which are e.g. over CORBA, SSH, SFTP). For trust distribution, certificate enrollment and management, SCEP and CMPv2 protocols can be used.

A certificate can expire therefore certificate management must provide solutions for recertify expired certificates. Certificate renewal case, certificate is only re-certified; the re-key procedure replaces the public key in the certificate. Modification of the certificate results some change in the parameters of the certificate only [RFC3647]. Likewise, compromised or unused certificates have to be revoked and for such events either Certificate Revocation List and distribution service, or online status query (OCSP) [RFC6960] service needs to be provided.

The Trust infrastructure is important function of security management. New certificate authorities (CA) can be set up or the trust infrastructure can be integrated under existing certificate authorities. It is advantageous to create sub-CAs, and certify nodes having the same remote communication peers with the same sub-CA. The reason is that in this case, for the remote communication peers, the sub-CA should be set as trust anchor. Setting higher level CAs might compromise the security as it widens the trust to that extent that nodes which originally were neither allowed to communicate nor trusted are became trusted

peers. (Note that some implementations like openssl currently do not support verification of trust up to only a sub-CA level. For this reason, for such implementations, distinct CA structure needs to be used as in Figure 5.). Usually, nodes with the same properties are certified under the same sub-CA. For example LTE radio base stations are certified by one sub-CA, and MME nodes are certified by another sub-CA.

Replacement of trusts, for both normal and emergency operation shall be provided. In case of normal operation, trusts are replaced in a seamless way, while in emergency case the compromised trusts must be promptly invalidated, regardless the caused disturbance. It is obvious that when a trust is compromised, then peers (managed nodes), which still trust in the compromised trust, are in danger. Poisoning the trust infrastructure provided by NMS therefore, can lead to the compromise and swift collapse and slow and hard recovery of the managed telecommunication networks.

Centralized Log Collection, Log Analysis

For the above reasons, observability is important. In order to detect malicious activities, logs should not only be stored on the managed nodes, but centralized security and audit log service in NMS shall guarantee that even if a node is compromised evidences about malicious activities still persists. From the events in the collected log database, security log analysis and IDS/IPS can further provide analytics to detect any other, even holistic malicious activities.

Initial configuration management of the managed nodes is called as secure bootstrapping [TS33310]. Nodes situated in hostile environment, having some hardware security (TPM) modules, can utilize secure bootstrapping, where the hardware identification is cryptographically bound to the identity of the managed network. The software integrity of the node is verified and the security settings, including keys, certificates and trusts are securely downloaded and stored. This procedure - as extensively increasing number of devices require large volumes of managed network elements - are performed with as little human interaction as possible.

Conclusion

In addition to telecommunication networks and systems, Network Management Systems are also part of the critical infrastructure. The main reason is that attacks through them threaten and could compromise the entire managed telecommunication infrastructure.

Telecommunication Network Management Systems have to fulfill requirements from several perspectives, amongst these, one essential is security. From security perspective, two major goals can be formulated; one is called Management Security, to provide controls for protecting the managed and management systems. The other goal is called Security Management, to provide management functions for security towards the managed networks.

The crucial and management system specific controls are architectural controls (compartmentalization in the management plane with zoning), and access control, where in workflows are disassembled to atomic tasks, each carry an authorization

enforcement. The access control is combined with further restrictions based on the managed resources.

The principal Security Management functionalities are the centralized authentication and authorization of managed network elements, security configuration management, trust and identity management, centralized security and audit log management, the security log analytics on that and the support for secure bootstrapping of the managed network elements.

To conclude, Network Management Systems have to provide easy to manage security features and mechanisms, and shall assure the security quality meeting industry best practice requirements for information security on mission critical systems.

References

- [TMN] ITU-T M.3010: Telecommunications management network - Principles for a Telecommunications Management Network
- [M3016] ITU-T M.3016.0-4 Security for the management plane
- [Arch] Nick Rozansky, Eoin Woods. Software Systems Architecture ISBN 0-321-1229-6
- [TS32240] 3GPP TS 32.240 V12.5.0: Charging architecture and principles
- [X700] ITU-T X.700 Management Framework For Open System Interconnection for CCITT Applications
- [TS32111] 3GPP TS 32.111 1-7 V12.0.0 3G Fault Management
- [RFC3877] RFC3877 Alarm Management Information Base (MIB), (Proposed Standard), 2004
- [TS32600] 3GPP TS 32.600 Telecommunication management; Configuration Management (CM) Concept and high-level requirements
- [RFC6241] RFC 6241 Network Configuration Protocol (NETCONF), (Proposed Standard), 2011
- [TS32401] 3GPP TS 32.401 Telecommunication management; Performance Management (PM); Concept and requirements
- [TS32371] 3GPP TS 32.371 Telecommunication management; Security Management concept and requirements
- [RFC4210] RFC4210, Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP) (Proposed Standard), 2005
- [SCEP] Simple Certificate Enrollment Protocol, IETF draft, work in progress. <http://tools.ietf.org/html/draft-nourse-scep-23>
- [RFC7011] RFC 7011, Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information, (Internet standard), 2013
- [XACML] OASIS Standard: eXtensible Access Control Markup Language (XACML) V3.0. <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cos01-en.pdf> 2012
- [RFC6347] RFC 6347, Datagram Transport Layer Security Version 1.2, (Proposed Standard), 2012
- [RFC6242] RFC 6242, Using the NETCONF Protocol over Secure Shell (SSH), (Proposed Standard), 2011
- [RFC5539] RFC 5539, NETCONF over Transport Layer Security (TLS), (Proposed Standard), 2009
- [RFC6960] RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, (Proposed Standard), 2013
- [RFC3647] RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, (Informational), 2003
- [TS33310] 3GPP TS33.310 Network Domain Security (NDS); Authentication Framework (AF) V12.2.0, 2014

KONFERENCIA ELŐADÁSOK

BALKU Ferenc

IT- ÉS KIBERBIZTONSÁGI TENDENCIÁK

Kapsch BusinessCom Kft.

kapsch >>>

IT- és kiberbiztonsági tendenciák

12. 11. 2014.



Kapsch BusinessCom Kft.

kapsch >>>

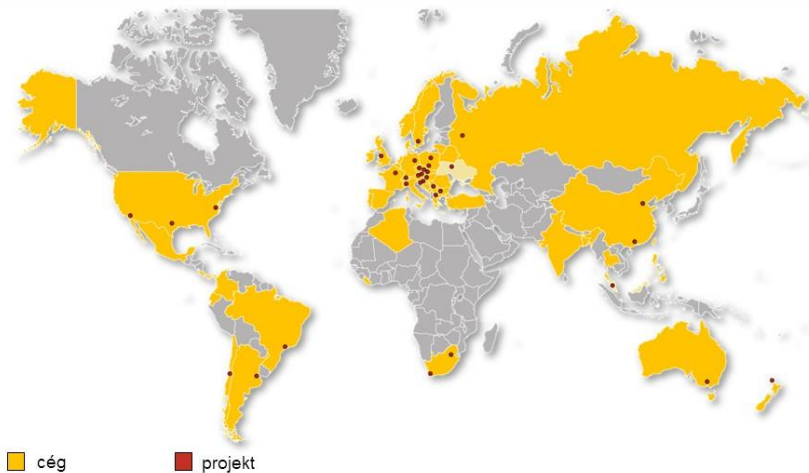
Tartalom

- Kapsch: integrátor a biztonság területén
- Tapasztalataink
- Néhány újdonság
 1. Juniper újdonságok az IT biztonság területén
 - DDoS Secure
 - Argon Secure
 2. Rohde & Schwarz speciális megoldásai
 - TopSec Mobile: mobil telefónia kódolása
 - SITLine ETH: Ethernet kódolás

A Kapsch csoport



Kapsch – a világ 46 országában



Kapsch BusinessCom Magyarországon

- Alapítás: 1991.
- Központ: Budapest, területi iroda: Győr
- Ügyfelek: +100
- Forgalom: ~17 millió EUR
- Leányvállalatok:
 - Kapsch BusinessCom – ICT szolgáltatások vállalati ügyfelek számára
 - Kapsch CarrierCom – ICT szolgáltatások és GSM-R rendszerek hálózati szolgáltatók számára

Tartalom

- Kapsch: Integrátor a biztonság területén
- Tapasztalataink
- Néhány újdonság
 1. Juniper újdonságok az IT biztonság területén
 - DDoS Secure
 - Argon Secure
 2. Rohde & Schwarz speciális megoldásai
 - TopSec Mobile: mobil telefónia kódolása
 - SITLine ETH: Ethernet kódolás

Kapsch az IT biztonság területén

Több éves tapasztalattal rendelkezünk – akár speciális ügyfélkör terén is:

- Állami - kormányzati
- Banki - pénzügyi
- Ipari és ipari fejlesztési
- Közlekedési
- "Nem tudom - nem emlékszem"

Rovidítés	Megnevezés
ISO9001:2008	Minőségirányítási rendszer
ISO14001:2004	Környezet Irányítási Rendszer
ISO27001:2013	Információ Biztonsági Irányítási Rendszer
TBT és SZBT	Telephely Biztonsági Tanúsítvány Személyi Biztonsági Tanúsítvány
AQAP 2010	Állami / Katonai Minőség Irányítási Rendszer
NATO BOA	NATO Basic Order Agreement
	NATO beszállításra alkalmas

MINŐSÍTÉSEK:



Tapasztalataink / tevékenységi körünk

- Biztonsági (Fizikai /IT) és biztonságpolitikai tanácsadás, audit
- Adatközpont, cloud és virtualizáció biztonság
- "Klasszikus" hálózatbiztonság (routing, switching, terheléelosztás, tűzfalak, betörésérzékelés)
- Storage, storage hálózat és adatközpont biztonság



TARTALOM

- Kapsch: integrátor a biztonság területén
- Tapasztalataink
- Néhány újdonság
 1. Juniper újdonságok az IT biztonság területén
 - DDoS Secure
 - Argon Secure
 2. Rohde & Schwarz speciális megoldásai
 - TopSec Mobile: mobil telefónia kódolása
 - SITLine ETH: Ethernet kódolás

A DDoS támadás – mint “műfaj”

Nagy volumen

- Könnyű felismerni
- Egyre nagyobb méretű támadások
- Támadások gyakorisága mérsékelten növekszik

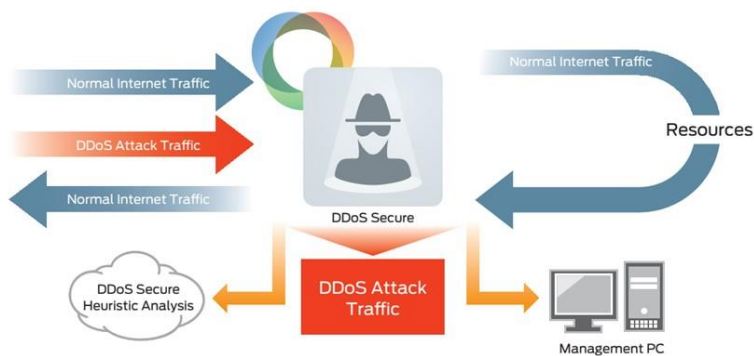
Erőforrások lefoglalása

- „Flash mob”-ok, közösségi oldalak szervező ereje
- Események, amelyek rövid idejű nagy forgalmat tudnak generálni.

„LOW AND SLOW”

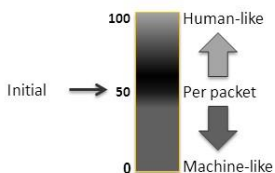
- Kifinomult, nehéz felismerni
- Cél a back-end gyengesége
- Kis mennyiségű kérés is képes nagy web szolgáltatás kiesést okozni
- 25% több ilyen jellegű támadás, mint nagy volumenű

Juniper DDoS Secure – alapkoncepció



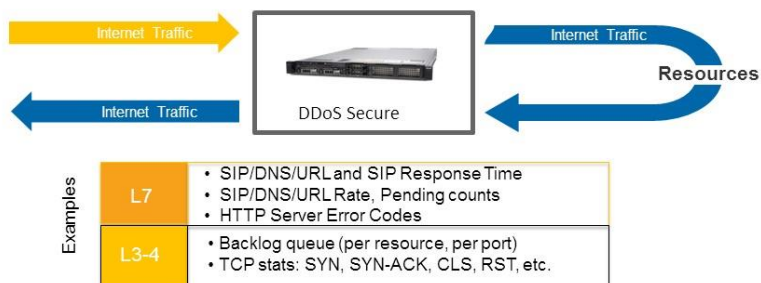
Juniper DDoS Secure - CHARM

CHARM: Valós idejű rizikófaktor-hozzárendelés forrás IP címhez



- Emberi forgalom: egyenetlen, szabálytalan
- Gép/robot: szabályos, egyenletes
- Algoritmus frissítés

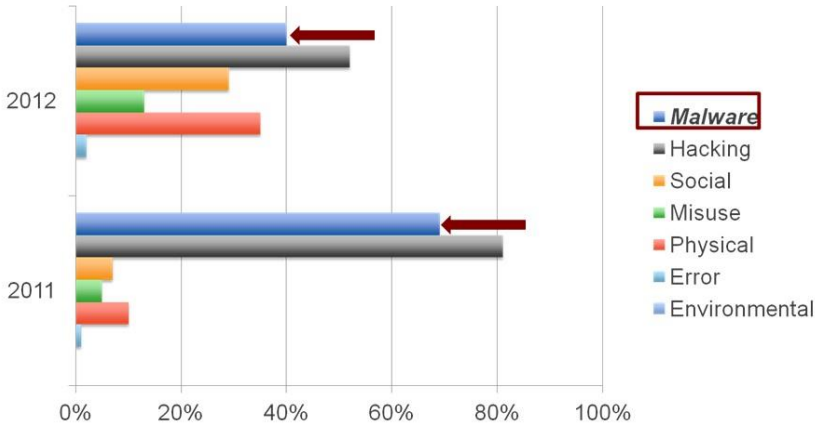
Juniper DDoS Secure – “És mi van hátul?”



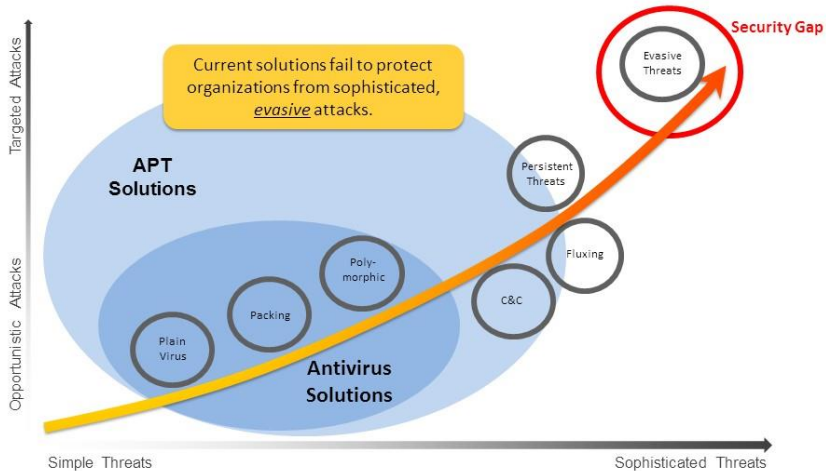
Tartalom

- Kapsch: integrátor a biztonság területén
- Tapasztalataink
- Néhány újdonság
 1. Juniper újdonságok az IT biztonság területén
 - DDoS Secure
 - Argon Secure
 2. Rohde & Schwarz speciális megoldásai
 - TopSec Mobile: mobil telefónia kódolása
 - SITLine ETH: Ethernet kódolás

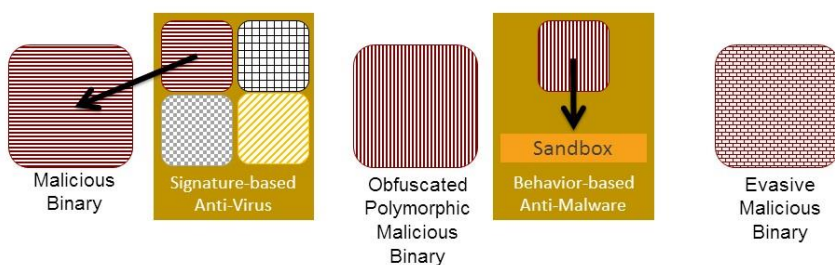
Juniper Argon Secure – sikeres támadási módszerek



Juniper Argon Secure – a támadások egyre körmonfontabbak



Juniper Argon Secure - modern fegyverkezési verseny

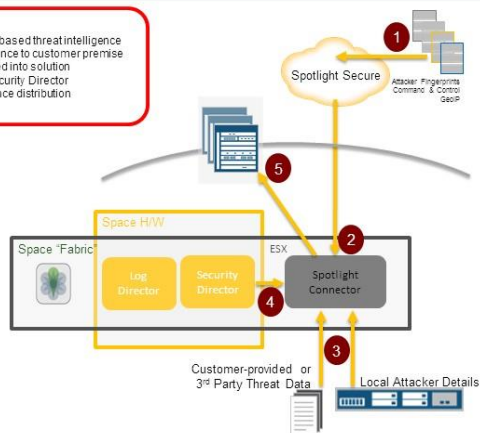


Juniper Argon Secure

- **Feljövőben lévő megoldás**
 - Advanced Anti-Malware + védett hoszt figyelés
 - Jobb biztonság elérése tartalom és összefüggések együttes figyelésével
- **A Juniper IDS sikerére épül**
 - A hálózat és a végpontok együttes figyelése és elemzése
 - A támadásokat több lehetséges ponton és fázisban képes detektálni
 - IA hálózatban már alkalmazott több mint 50 módszert is használja
 - A rosszindulatú kódokat már a hálózatba jutáskor képes kiszűrni
- **A megjelenésekor teljesen integrálható lesz:**
 - SRX Tűzfalakkal
 - Spotlight Secure Threat Intelligence-szel
 - Space, Security Director and Log Director - szoftverekkel

Juniper Argon Secure – architektúra

1. Aggregated & Optimized cloud-based threat intelligence
2. Juniper-provided threat intelligence to customer premise
3. Local Customer data aggregated into solution
4. Centralized management by Security Director
5. Scalable (aggregated) intelligence distribution



Juniper Argon Secure – korreláció és “pontozás”

- Korreláció
 - Kiküszöböli az “információtenger” effektust
 - Jobb döntési képesség és reagálási lehetőség
- “Pontozás” Scoring
 - Az események jobb prioritizálását teszi lehetővé
 - A telítési értékek gyorsabb reakciót tesznek lehetővé
- Integráció SRX tűzfalrendszerrel
 - A hálózati intelligenciát a végpontokra lehet “tolni”
 - Spotlight Secure integráció az ügyfeleket védi

Tartalom

- Kapsch: integrátor a biztonság területén
- Tapasztalataink
- Néhány újdonság
 1. Juniper újdonságok az IT biztonság területén
 - DDoS Secure
 - Argon Secure
 2. Rohde & Schwarz speciális megoldásai
 - TopSec Mobile: mobil telefónia kódolása
 - SITLine ETH: Ethernet kódolás

Rohde & Schwarz TopSec Mobile és SITLine ETH

TopSec Mobile: mobil telefónia kódolása



SITLine ETH: Ethernet kódolás



Köszönöm a figyelmet!

Balku Ferenc

információbiztonsági szakértő

Kapsch BusinessCom Kft.

1113 Budapest | Bocskai út 77-79. | Magyarország

Telefon +36 1 372 6400

E-Mail ferenc.balku@kapsch.net | www.kapsch.hu

Please Note:

The content of this presentation is the intellectual property of Kapsch AG and all rights are reserved with respect to the copying, reproduction, alteration, utilization, disclosure or transfer of such content to third parties. The foregoing is strictly prohibited without the prior written authorization of Kapsch TrafficCom AG. Product and company names may be registered brand names or protected trademarks of third parties and are only used herein for the sake of clarification and to the advantage of the respective legal owner without the intention of infringing proprietary rights.

CZIRÁKY Zoltán

NO-WIRELESS ZÓNA - AHOL TILTOTT A VEZETÉK NÉLKÜLI KOMMUNIKÁCIÓ

equicom
az Ön ICT mérés-technikai szakértője

No-wireless zóna

ahol tiltott a vezeték nélküli kommunikáció

2014. november 12.

Czirák Zoltán
ügyvezető igazgató
vállalati hálózatok

EXFO
FLUX
FTEL
AIRMAGNET
Accedian
SUNEDGE TELECOM
VEX

equicom
az Ön ICT mérés-technikai szakértője

No-wireless zóna

A vezeték nélküli kommunikációs megoldásokkal ellentétben a Wi-Fi esetében a fizikai hálózati hozzáférés lényegesen egyszerűbb, ami tovább növeli a kockázatot. Nem feledkezhetünk meg továbbá azokról a kritikus területekről sem (pl. bankok, nemzetbiztonsági intézmények, büntetés végrehajtás, stb.), ahol semmilyen mobil kommunikáció nem megengedett, de mindössze táblákkal tiltják a mobiltelefon vagy Wi-Fi képes eszközök használatát. Ezeken a területeken a tiltásokon túl felügyeleti monitorozó eszközökkel kell biztosítani a szabályok betartását. Előadásunkban erre mutatunk egy kézzel fogható megoldást.

EXFO
FLUX
FTEL
AIRMAGNET
Accedian
SUNEDGE TELECOM
VEX

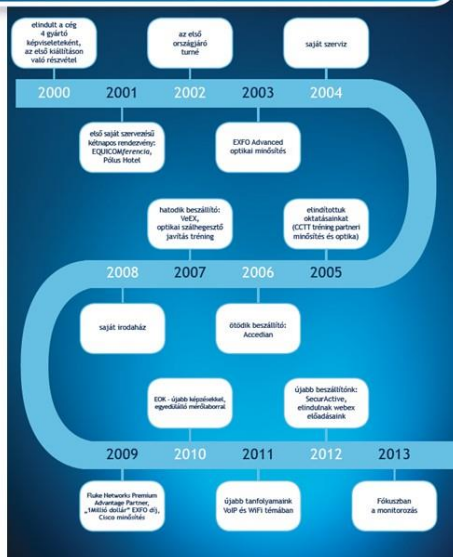
Az EQUICOM-ról dióhéjban

equicom
az Ön ICT mérés-technikai szakértője

- Kizárólag ICT mérés-technikai megoldásokra szakosodva
- Több mint 15 éves szakmai múlt
- Világviszonylatban vezető beszállítók kizárólagos magyarországi képviselője

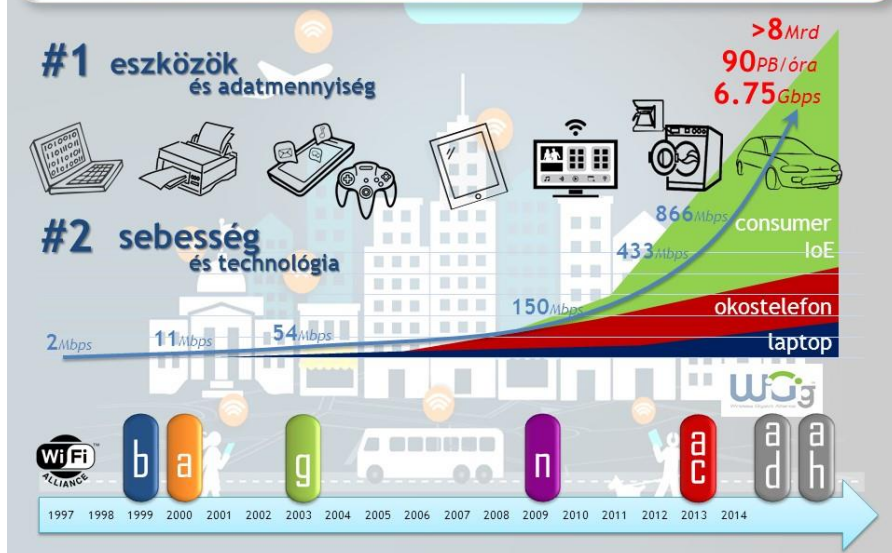


- Piaci jelenlét: szolgáltatók és vállalati szegmens
- Közvetlen kapcsolat a felhasználó és a gyártó között
- Szakértelem, tanácsadás, támogatás, szakmai oktatások (9 tematikus EOK tanfolyam)



Wi-Fi evolúció

equicom
az Ön ICT mérés-technikai szakértője



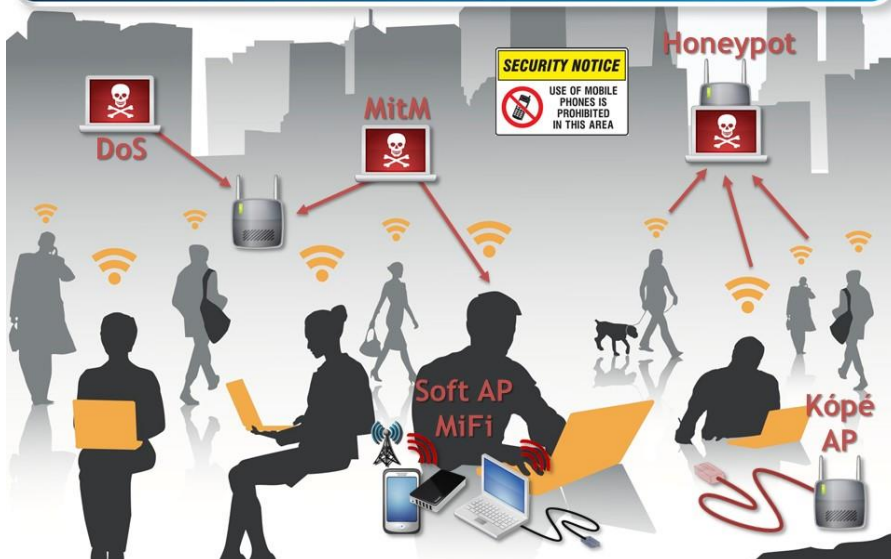
eequi.com
az Ön ICT mérés-technikai szakértője

eequi.com
az Ön ICT mérés-technikai szakértője

a biztonság



Wi-Fi veszélyek/támadások ...és a mobil is itt van

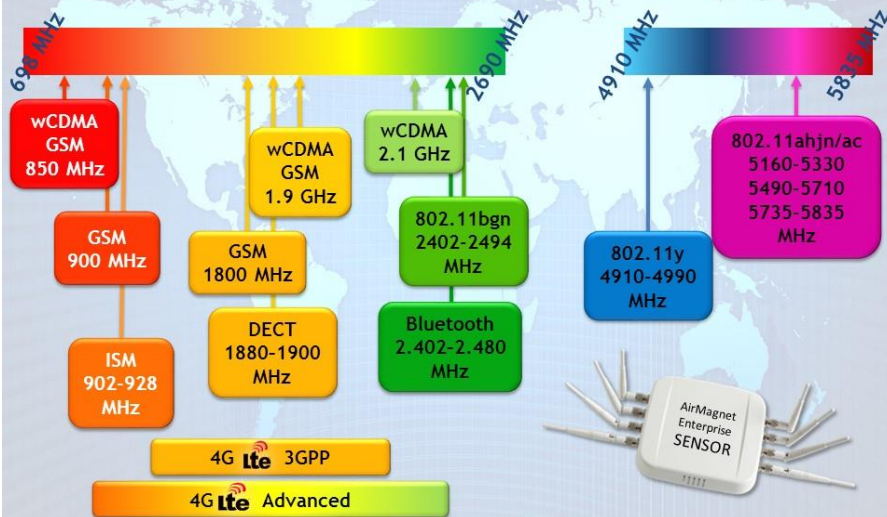


AirMagnet Enterprise - architektúra



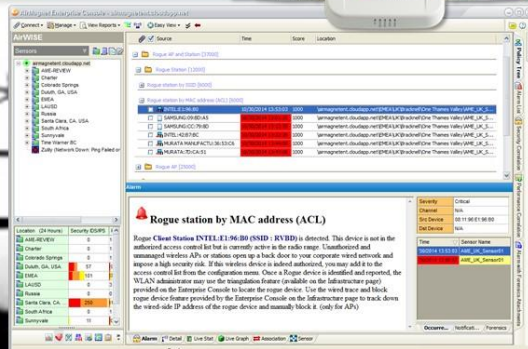
AirMagnet Enterprise - vizsgált frekvenciák

equ.com
az Ön ICT mérnöki szakértője



AirMagnet Enterprise - No-Wireless zóna

- Bluetooth**
- FHSS Cordless Phone**
- Wireless Video Camera**
- Mobile Cellular Event**
- Non-Cellular Energy**
- Rogue Station/Access Point**
- Stb. stb. stb. (>100 security)**



WLAN életciklus

equicom

az Ön ICT mérés-technikai szakértője



Köszönöm a figyelmet!

equicom

az Ön ICT mérés-technikai szakértője

Tesztelje saját hálózatán! ➔ info@equicom.hu

- Kérje személyes konzultációnkat

Fluke Networks WLAN megoldások

- www.equicom.hu/wlan

Szakmai cikkeink ➔ info@equicom.hu

- BYOD - a jelenség
- WLAN hálózatsbiztonság és megfelelőségi irányelvek
- Lefedő vs. Integrált vezeték nélküli hálózatsvédelem

Webex előadásaink

- <http://www.equicom.hu/webex>

Monitorozó megoldásaink

- <http://www.equicom.hu/monitoring>



EXFO

FLUKE NETWORKS

FITEL

AIRMAGNET

equicom

ACCEDIAN

SOMAX TELECOM

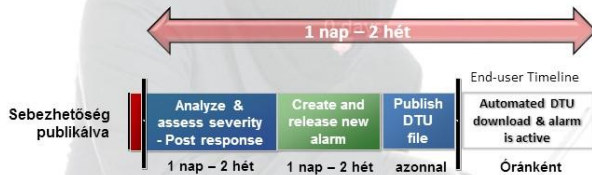
VeX

Háttér diák

AirMagnet Enterprise - BIZTONSÁG

SECURITY

Dinamikus Sérülékenység adatbázis Frissítés (DTU)



Az új fenyegetések szignatúrái automatikusan beépülnek a meglévő szabályrendszerbe, a szenzorokba töltődnek, leállítás és beavatkozás nélkül!

SECURITY

Wireless/Wired Blocking



Rendkívül alacsony csatorna terhelés blokkoláskor.
Akár 10 eszköz 10 csatornán történő blokkolása egyetlen szenzorral.

A kliensek problémái

Performance

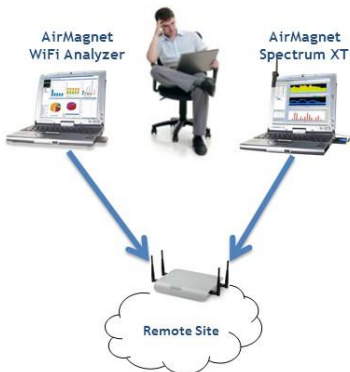
- Nem látszik egyetlen AP sem!
- Nem tudok csatlakozni a WLAN hálózathoz/Internetre!
- Leszakadtam a WLAN-ról!
- Lassú hálózat/alkalmazás!
- A 802.11n nem azt nyújtja, amit ígértek!
- Roaming közben megszakadt a hívás!
- stb. stb. stb.

Üzemeltetés a karosszékből

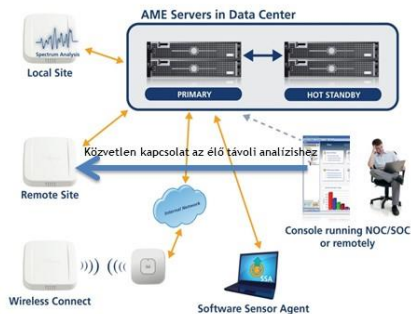
equ.com
az Ön ICT mérés-technikai szakértője



Remote Analyzer



AirMagnet Enterprise
(Remote Test Kit)



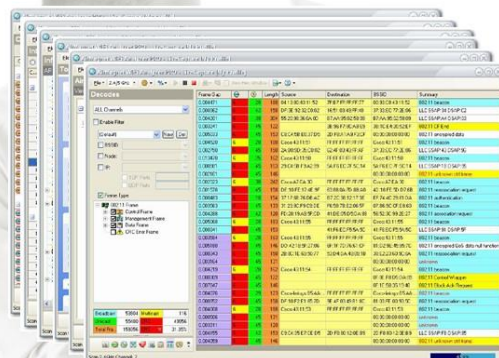
Üzemeltetés a karosszékből

equ.com
az Ön ICT mérés-technikai szakértője



WiFi analízis

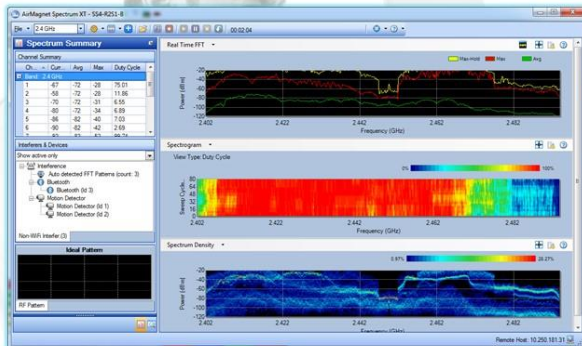
- Csatornák
- Interferenciák
- Infrastruktúra felépítése
- Top Traffic tesztek
- AirWise policy
- Decode
- Riportok



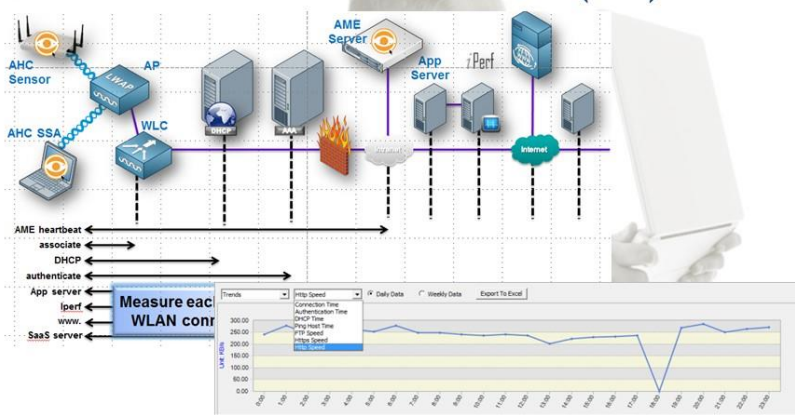


RF spektrum analízis

- Spektrum intelligencia
- Eszköz felismerés
- Bluetooth tesztek
- Riasztások

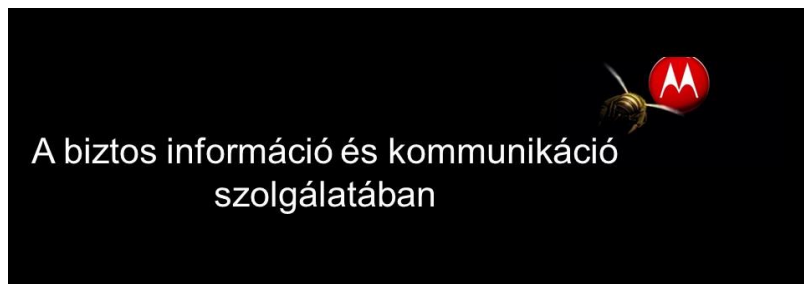


Automatic Health Check (AHC)



IMRE László

A BIZTOS INFORMÁCIÓ ÉS KOMMUNIKÁCIÓ SZOLGÁLATÁBAN



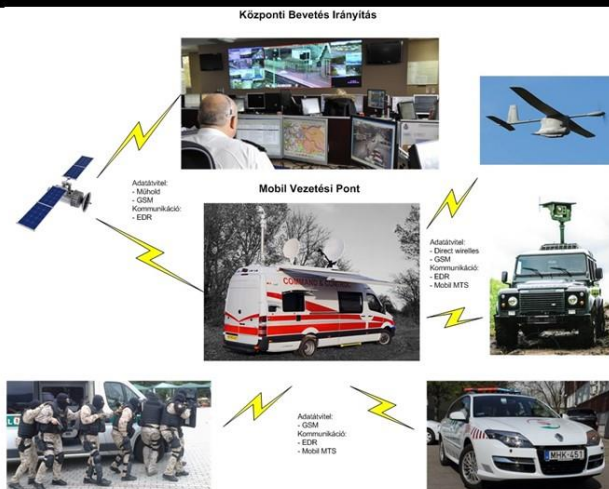
A biztos információ és kommunikáció szolgálatában



Cél:

- biztos információ szerzés
- Megfelelő kommunikáció

MOTOROLA
SOLUTIONS
DISTRIBUTION
PARTNER



Mobil vezetési pont



Általános leírás:

Mobil bevetési, irányítási rendszer önálló energiarendszerrel, beépített, biztonsági felszerelésekkel, kommunikációs kapcsolattal, megfigyelési és IT eszközökkel van ellátva. Mobilitás révén a kezelőszemélyzetek részére biztosítja mindazon szolgáltatásokat, amelyek gyorsabbá, hatékonyabbá teszi a feladatok végrehajtását. Lehetővé teszi, hogy olyan járműveket alkossunk, amelyek pontosan megfelelnek a megrendelő igényeinek.



Mobil vezetési képességek



- Helyszíni döntéshozatal és végrehajtás
- Saját központi adatbázisok és információs rendszerek elérése
- Felderítési információk gyűjtése
- Más információs rendszerek elérése
- Autonóm helyi kommunikáció támogatása



Belső tér elrendezése



- Infokommunikációs munkahelyek
- Vezetési munkahely
- „Tárgyaló”
- Technikai tér
- Tároló helyek

Klíma berendezés:

Hűtő-fűtő funkciójú klíma gondoskodik a megfelelő hőmérsékletről



Belső tér elrendezése



Belső tér:

Gépjármű felépítményébe kialakítható bármilyen speciális munkaállomás, videófal, projektor, labor. Kiépítésre kerül helyi LAN hálózat. A felépítményben és annak közvetlen közelében WIFI szolgáltatás építhető ki, illetve a bevetési központtal szélessávú műholdas internetkapcsolat áll rendelkezésre. A munkaállomásokon rázkódást tűrő számítógépek találhatók.



Beépíthető, hordozható kommunikációs eszközök

Vezeték nélküli adatátviteli megoldások

Műholdas internet:

- Gépjárműre szerelhető
- automatikusan műholdra álló antennarendszer.
- két tengelyes, motoros mozgatás;
- egy gombos, automatikus pozicionálás 2 percen belül;
- legfejlettebb antenna hangolási módszerek használata.

Előnyök:

- **Gyors**
 - Nagysebességű, folyamatos Internet kapcsolat
 - Akár 20 Mbps letöltés, 6 Mbps feltöltés
- **Egyszerű**
 - kis méretű parabola antenna
 - nem igényel külön telefonvonalat, illetve egyéb kiegészítő szolgáltatást
 - telepítés után azonnal használható
- **Bárhol elérhető**
 - teljes lefedettség Magyarországon
 - mindenhol azonos, kiváló minőség



Vezeték nélküli adatátviteli megoldások

Mikrohullámú adatátvitel:



Nagyobb távolságok áthidalására gyakran használják a mikrohullámú átvitelt frekvenciatartomány 2-40 GHz között lehet. A kiemelkedő antennatornyokon elhelyezkedő parabola adó és vevőantennák egymásnak sugárnyalábokat küldenek és akár száz kilométert is átfoghatnak. Sáv szélesség akár: > 100 Mbps

Motorola Cambium Networks:



Vezeték nélküli megoldások

EDR rádió kommunikáció:



Az Egységes Digitális Rádiótávközlő Rendszer (EDR) rendkívül magas rendelkezésre állást biztosító, zárt rádió-távközlő rendszer.

A felépítményben található munkaállomások számára kényelmesen elérhető és jól látható helyre kerül telepítésre a több kontrollfejes Motorola típusú EDR rádiók, melynek célja, hogy olyan professzionális összeköttetést valósítson meg a különféle készenléti és rendvédelmi szervek között, amely gyorsabbá, hatékonyabbá és biztonságosabbá teszi az egyes feladatok végrehajtását.

Autonóm rádió kommunikáció:

A Motorola MTS1 bázis állomásra építve, kialakítható lokális beszédkommunikáció a meglévő EDR készülékekkel.

Antenna rendszer:

A rádióberendezések antennái részére, beleértve a lokális pont-pont rendszereket, a jármű felszerelhető kitolható, forgatható antenna árbóccal, ami alkalmas körsugárzók és irányított antennák elhelyezésére is.



Vezeték nélküli megoldások

Motorola MTP6750 tetra kézi rádió



COMPREHENSIVE
PORTFOLIO FOR
2013



micro
S



MOTOROLA SOLUTIONS

Fercom

Vezeték nélküli megoldások

Motorola MTM5500 mobil tetra terminál



10W kimenő teljesítmény

Repeater és Gateway tulajdonságok

Többféle változat (asztali, távkezelős, motoros, stb)

1 illetve 2 kezelőfej egyidejűleg (hagyományos és/vagy telefon stílus)

MOTOROLA SOLUTIONS

Fercom

Vezeték nélküli megoldások Motorola MotoBridge



Bridge vagy gateway, összeköttetést biztosít

- Helyi vagy távoli diszpécserok
- Rádiós eszközök
 - Analóg
 - Konvencionális
 - Trónkölt
 - DMR
 - Tetra
 - APCO25
- Telefon
 - PSTN/PABX
 - GSM/GPRS
 - IP telefon
 - Android Smartphone



... eszközök között, korlátlan földrajzi területen.

Szabványos IP összeköttetések

Hálózaton belül is titkosított összeköttetések

Kommunikációs eszközök távkezelése,
beszédcsoport vagy csatorna váltás

Méretezhető rendszer, kettőtől akár több ezer
eszköz összeköttetését tudja biztosítani, akár
több ezer diszpécser csatlakozásával együtt

Távfelügyelet, a rendszer felügyelhető és
módosítható bármelyik bridge eszközhöz
csatlakozva

Hordozza a jelzéseket is, így pl. telefonszámok
vagy rádió azonosítók is megjelennek a
diszpécseroknél

Prioritások

Hangrögzítés

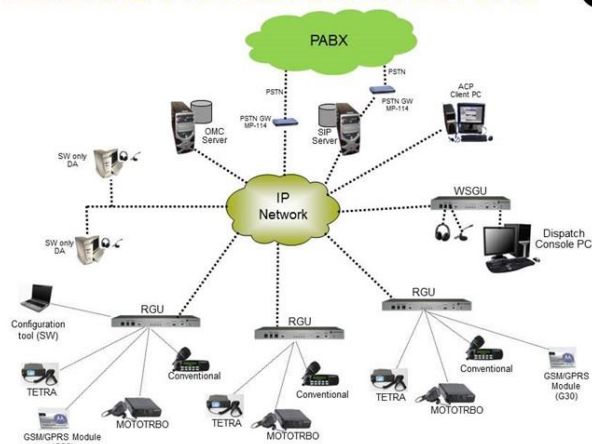


Motorola nap 2014. április 2.

Vezeték nélküli megoldások Motorola MotoBridge általános felépítés

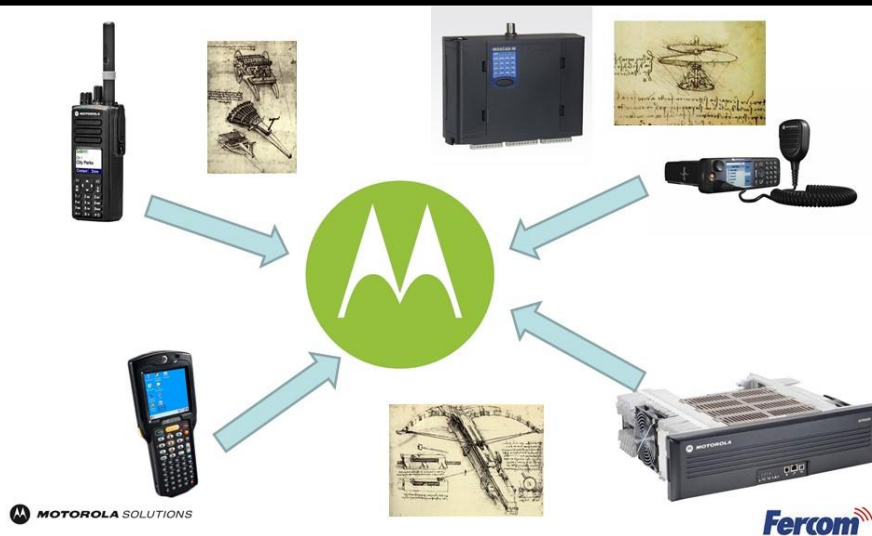


GENERAL SYSTEM ARCHITECTURE



Motorola nap 2014. április 2.

Vezeték nélküli megoldások Összefoglalás



Motorola nap 2014. április 2

Információ szerzés máshogyan!



„Látni és nem látszani”



Megfigyelő eszközök:

Hőkamerás alkalmazások



Megfigyelő eszközök:

Hőkamerás alkalmazások



Szárazföldi megfigyelés



Digitális zoom

2x és 4x digitális zoom. Ez lehetővé teszi, hogy közelebbi pillantást vessen a helyzetre, ha szükséges.

Hordozható és robusztus

Súlya alig haladja meg az 1000 grammot, elemekkel együtt, a FLIR BHS sorozat kompakt és rendkívül könnyű. IP 67-es besorolással rendelkezik, -20 ° C és +60 ° C között működik.

Könnyen működtethető

Ergonomikus és könnyen használható, a BHS sorozat teljes mértékben szabályozható mindössze 5 gombbal, amik a készülék tetején helyezkednek el.

Ideálisan alkalmazható a titkos műveletek alatt
Működésük során, a BHS sorozat teljesen csendes, a szemkátyó kialakításánál fokozottan figyeltek arra, hogy a felhasználó ne fedje fel pozícióját, maradjon észrevétlen a teljes sötétségben.

Egy gombos videó felvétel

Egy gomb lenyomásával elindítható a videó felvétel, a cserélhető SD kártyára.

Képtárolás

Hőképek tárolása SD kártyán jpeg formátumban

Hot shoe

A BHS sorozat alapfelszereltsége a „hot shoe”, amit könnyen lehet csatlakoztatni a hőkamerához. Ez lehetővé teszi, hogy töltsön a kamerát és csatlakoztathassa egy külső monitorhoz miközben a hőkamera egy állványhoz van rögzítve



Megfigyelő eszközök:

Hőkamerás alkalmazások



Vezetést segítő hőkamera



Megfigyelő eszközök:

Hőkamerás alkalmazások



Vezetést segítő hőkamera:

- A sofőr időben értesülhet a veszélyhelyzetről
- A fényviszonyok nem befolyásolják a képet
- MIL STD kialakítás
- Vízálló kivitel (IP67)
- Automatikus lencse jégtelenítés
- Látószög fix 19mm (36°x27°)
- 320x240 hűtetlen VOx mikrobolometer



Megfigyelő eszközök:

Hőkamerás alkalmazások



Megfigyelő eszközök:

Hőkamerás alkalmazások



Vezetést segítő hőkamera

Tökéletes megoldás katonai járművezetőknek



Főbb jellemzők:

- Hűtetlen hőkamera
- Kijelző és vezérlő egység
- Nappali kamera (opcionálisan optikai zoommal)
- MIL STD kialakítás

Megfigyelő eszközök:

Hőkamerás alkalmazások



Mobil hőkamera



Megfigyelő eszközök:

Hőkamerás alkalmazások



Mobil hőkamera

Rendszerezeszközök:

- Vezetésszűrőrendszer
- Rádió kommunikáció (EDR)
- Online kapcsolat
- Elektromos kiemelő egység
- Vezérelhető kameraegység
- Helyi video rögzítő
- DC tápellátás a hosszú üzemidő érdekében



Megfigyelő eszközök:

Hőkamerás alkalmazások



Mobil hőkamera fej egység

Forgató-billentőegység (nx360°
körbefordulás és $\pm 30^\circ$ billentési szög)

Elektronoptikai fej:

- GPS vevő
- Elektronikus iránytű
- Elektronoptikai egység (multiszenzor)
 - Hőkamera
 - Nappali kamera
 - Lézer távmérő



Megfigyelő eszközök:

Hőkamerás alkalmazások



Mobil hőkamera

Hőkamera:

- Jármű észlelési távolság: 5,2Km
- Jármű felismerési távolság: 2,5Km
- Ember észlelési távolság: 3Km
- Ember felismerési távolság: 1Km
- MIL STD 810 E

Nappali kamera:

- Jármű észlelési távolság: 15Km
- Jármű felismerési távolság: 7Km
- Ember észlelési távolság: 8Km
- Ember felismerési távolság: 2,7Km

Lézer távmérő:

- Hatótávolság: 5Km
- Max 15 célpont egyidejű mérése



Megfigyelő eszközök:

Hőkamerás alkalmazások



Mobil hőkamera



Kezelés:

- Funkciók gyors elérése
- Egyszerű kezelhetőség
- Klíma és állóhelyzeti fűtés
- Akkuidő visszajelzés
- MIL STD kivitel



Funkciók:

- Térkép (frissítési lehetőséggel)
- Élőkép (akár mindkét monitoron)
- Helymeghatározási adatok
- Rendszer állapotának kijelzése
- Rendszer és munka naplók rögzítése
- Automatikus célkövetés
- Lézeres távolságmérés, cél megjelenítése a térképen



Megfigyelő eszközök:

Mobil hőkamera automatikus célkövetés funkcióval



Megfigyelő eszközök:

Mobil hőkamera használat közben



2014-03-10 19:20:15



Megfigyelő eszközök:

Éjjellátó készülékek



NVLS ANVIS GOGGLE

Alacsony profilú felhajtható

Kompatibilis az összes ANVIS 9 sisak illeszkedéséhez

Ultrakompakt ANVIS
F1a vagy választható F1akusz
A, B osztály vagy szűrőgöngyölítő

Kiegészítők rendszere

Akkumulátor pack
2x AA 1.2 V - 3.6 V



Megfigyelő eszközök:

Éjjellátó készülékek



Megfigyelő eszközök:

Éjjellátó készülékek



Megfigyelő eszközök:

Éjjellátó készülékek



Digitális éjjellátó

Nagy felbontású digitális CMOS-érzékelő (1280 x 1024)
Súly: 85 g
Méret: 34,1 x 36,6 x 37,4 mm

- Nappali/Éjszakai digitális színes kamera, digitális zoom 4x
- Nagyfelbontású szenzor (1280 x 1024 pixel)
- Kis pixel méret: 9,2 µm
- Magas frissítési frekvencia: 100Hz
- Csatlakozás 5 másodpercen belül
- Analóg és digitális videó kimenet (10 bites)
- Kis fogyasztás (<1 BW) 5-15V
- Széles hőmérséklet tartomány -40°C és 60°C között
- Valós idejű videó átvitel rádión vagy kábelen keresztül
- Nem csak IIR alapú



Megfigyelő eszközök:

Éjjellátó készülékek



NVLS TWS THERMAL WEAPON SIGHTS

- Könnyű alumínium készülékhez
- Nagy érzékenységű-nagy felbontású hőkamera érzékelők (640 X 480)
- Kis Pixel távolság (PITCH): 17 µ
- Maximális képfrekvencia: 60 Hz
- Nincs amerikai alkatrész. Nincs szükség DOD engedélyre

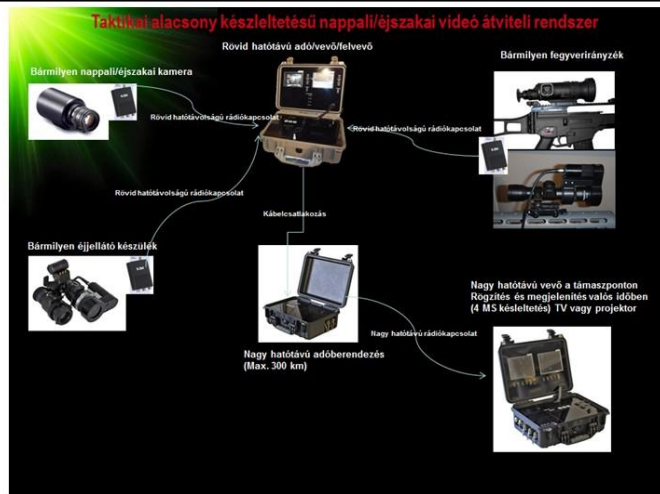
Rövid/Közepes hatótávú Hőkamerás irányzék

Nagy hatótávú hőkamerás irányzék és mesterlővész puskákhoz és nehézeppuskákhoz



Megfigyelő eszközök:

Éjjellátó készülékek



Megfigyelő eszközök:

Éjjellátó készülékek



Bármilyen fegyver átalakítása fejlett nappali/éjszakai rendszerre



A biztos információ és kommunikáció szolgálatában



Köszönjük a figyelmet!

Fercom Kommunikációs Kft., H-1037 Budapest, Pomázi út 15.

Telefon: +36(1)2507940, Fax: +36(1)250 7939 – info@fercom.hu – www.fercom.hu



BIG-DATA, BIG-BUMM

Kritikus infrastruktúrák új felfogású elemzése



Nyári László, NKE-KMDI/B7IOB2

Big Data, Big Bumm

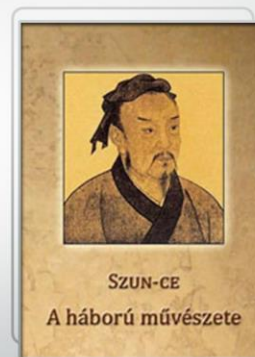
A gondolat Szun Ce (Kr.e. 561-496) az egyik legnagyobb kínai hadvezértől származik. Míg korábban csak a katonai teoretikusok szűk körében volt ismert, tanításait ma már az egyre agresszívabb tűzleti hadviseléshez is felhasználják.

„Korunkban úgy harcolnak a nagyvállalkozások, mint egykor a kis kínai háborúzó államocskák, és ma is az marad életben aki terjeszkedik, befolyása, uralma alá vonja vagy megsemmisíti a vetélytársakat.

Ehhez pedig hosszú távon jó stratégia, rövid távon kiterjedt információ szerzés – a cselekvések és dezinformációk indirekt módszere – szükséges.

Magyarra fordítva:

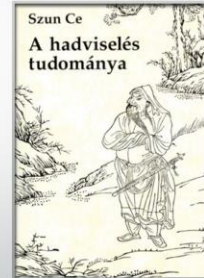
Minél több információ, annál biztosabb siker!



Big Data, Big Bumm

Az Észak-atlanti Szerződés Szervezete (NATO) Felsőszintű Polgári Veszélyhelyzeti Tervezési Bizottság 2002 novemberében meghatározta - a szövetség szempontjából meghatározó aspektusok alapján - a kritikus infrastruktúra definícióját.

Általánosságban kijelenthető, hogy kritikus infrastruktúrának mindazokat a létesítményeket és szolgáltatásokat tekintjük, amelyek sérülése, esetleges megsemmisülése súlyos következményekkel jár mind az emberek élete, mind a környezet szempontjából.



Big Data, Big Bumm

A XXI. század új típusú kihívásainak rendszerében a 2001. szeptember 11-i támadások következményeképpen Európában is erőteljesebben **megjelent a kritikus infrastruktúrák védelmének kérdésköre.**

Az uniós törekvések is felhívják az államok figyelmét arra, hogy a terror jelentette veszélyeken kívül számos más esemény is okot ad infrastruktúránk szervezett védelmének kialakítására.



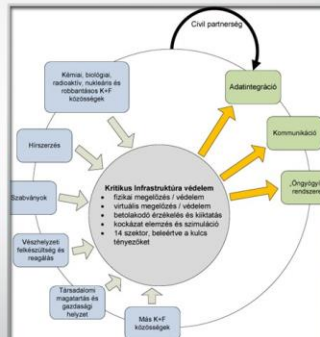
Big Data, Big Bumm

1249/2010. (XI. 19.) kormányhatározat 4. pontja alapján tárcaközi szakmai munkacsoportot alakítottak az irányelv végrehajtására. A kormányhatározat 8. a) pontja értelmében a nemzeti fejlesztési miniszter, a belügyminiszter és az érintett miniszterek részéről kijelölt vezetők részvételével, valamint az érintett infrastruktúra-tulajdonosok, üzemeltetők, érdekvédelmi szervezetek, tudományos testületek bevonásával

Kritikus Infrastruktúra Védelmi Konzultációs Fórumot hívott össze.

A KIV Tárcaközi Szakmai Munkacsoport 2010. 12. 30-án megalakult a Belügyminisztérium (BM), Nemzetgazdasági Minisztérium (NGM), Honvédelmi Minisztérium (HM), BM OKF, Magyar Energia Hivatal (MEH), Alkotmányvédelmi Hivatal (AH), Nemzeti Közlekedési Hatóság (NKH), Nemzeti Biztonsági Felügyelet (NBH), Nemzeti Fejlesztési Minisztérium (NFM), Országos Rendőrfőkapitányság (ORFK), BM Terrorelhárítási Központ (TEK), Közigazgatási és Igazságügyi Minisztérium (KIM), Magyar Kereskedelmi Engedélyezési Hivatal (MKEH) részvételével, és határidős feladatot kapott az európai kritikus infrastruktúrák (ECI) beazonosításához szükséges kritériumok kidolgozására, a potenciális ECI-kre vonatkozó javaslatok kialakítására.

Több mint 15 szervezet összehangolása..... nem egyszerű feladat!!



Forrás: A szakterület elemzése | Kritikus infrastruktúra védelmi kutatások nik.uni-obuda.hu630 x 625 Keresés kép alapján

Big Data, Big Bumm

Az EPCIP* megvalósítására vonatkozóan végül 2008 decemberében született végleges döntés. Ekkor látott napvilágot az eljárási rend: a kritikus infrastruktúrák azonosításáról és kijelöléséről.

Sokáig a megelőzés, a detektálás és a visszacsatolás volt a védelem három legfontosabb alappillére, azonban napjainkban már érdemes egy lépéssel tovább haladni.

A hagyományos védelmi modellek egyre kevésbé hatékonyak a mindennapi használat során.

Új fenyegetések. Új kihívások. Új célok láttak napvilágot.

Válaszul, a fejlesztők folyamatosan új termékeket és technológiákat dolgoznak ki.



Forrás: BM Országos Katasztrófavédelmi Főigazgatóság www.katasztrofavedelem.hu406 x 303 Keresés kép alapján

*EPCIP eljárási rend, az európai kritikus infrastruktúrák azonosítására és kijelölésére.

Big Data, Big Bumm

Mitől lesz egy infrastruktúra (vagy annak eleme) kritikus?

Általánosságban már definiáltuk: hogy mindazokat a létesítményeket és szolgáltatásokat tekintjük, kritikus infrastruktúrának, amelyek sérülése, esetleges megsemmisülése súlyos következményekkel jár mind az emberek élete, mind a környezet szempontjából.

De gondoljuk csak tovább, (ÉRDEMES)!

Nem egy komplex elektromos ellátási rendszer a kritikus, hanem az, ha az ellátási rendszer meghibásodik és a szolgáltatását igénybe vevők helyzete negatívan, olyan (kritikusan) változik, melynek következtében,

szükségszerű esetben akár milliók életébe is kerülhet.



Forrás: [biztonsagpiac.hu/425 x 282/Keresés kép alapján](https://biztonsagpiac.hu/425-x-282/Kereses-k%C3%A9p-alapj%C3%A1n)

Big Data, Big Bumm



Hipotézis: A kritikus infrastruktúrák védelmével foglalkozó tanulmányok jelentős része abból a felfogásból indul ki a mely szerint a rendszerekre érő támadások - magára az adott vagy érintett infrastruktúra ellen, annak elpusztítására, tönkretételére irányulnak.

Szerintem: nagyságrendekkel fontosabb lenne az informatikai hálózatok védelme helyett (mellett) a forgalmazott információk, a feldolgozott, gyűjtött adatok/adatbázisok fokozott védelme!

A tönkretett vagy elpusztított struktúrákat helyreállítani vagy újraépíteni nem egyszerű de lehetséges,

az elveszett adatok információk pótlása lehetetlen!

Big Data, Big Bumm

Egy kis történelem (Inkák)

Az egyik legnagyobb (út)hálózat megtervezése, és kialakítása az Inkák nevéhez fűződik. A hálózatok építésének alkalmazott alapelvei – alternatív útvonalak, kijelölt csomópontok stb. - a mai napig is érvényesek. Eredménytelen lenne bármelyik vonalat lerombolni, hiszen a hálózat egy másik vonalát választva ugyanúgy el lehet érni a kijelölt helyre.

Az utak mentén 4 km-enként futárok részére kialakított állomáshelyek voltak. A futárok szóbeli vagy csomókkal zsinórokra rögzített üzeneteket vittek. A partvonalat egy a Királyi úttal párhuzamosan haladó 4000 km hosszú út követte.



Inka úthálózat. Forrás: Inkák.

online: <http://www.doksi.hu/news.php?order=ShowArticle&id=652>

Big Data, Big Bumm

Időzített bomba (napjaink története)

Védelmi hiba. Iránban valószínűleg az izraeliek sikeresen semmisítették meg egy szupertitkos nukleáris létesítményt. Az atomerőmű védelmi vezetője szerint a sokszorosan biztosított, több emelet mélyen kialakított létesítményben semmilyen külső támadás sem okozhat komolyabb károsodást. Az elektromos hálózat meghibásodása sem lehet gond, de a vészvilágítás tartalék hálózatába épített távirányítású bombaindító rendszer indítása ellen nincs orvosság.

Vince Flynn; azonos című regénye alapján



Big Data, Big Bumm

Szuper kritikus „Piszkos struktúrák”

Elképzelni is nehéz milyen súlyos következményekkel járma a különböző infrastruktúrák rosszindulatú „piszkos” fegyverként való alkalmazása. A különböző terrorista szervezetek pontosan tudják milyen - az atomfegyvernél is nagyobb, pusztítóbb - hatása lehet főleg a kritikus hálózatokon elindítható abnormalis akcióknak.

Elég csak néhány piszkos alkalmazást átgondolni,

elektromos hálózat: elég csak a földvezetéket egy másik fázisvezetékekkel felcserélni. Az eredmény katasztrofális lenne, minden 220V-ra tervezett készülék azonnal leég használhatatlenné válik,

vízközmű hálózat: szinte a levegőszűrőben támadhatól Megmérgezése az élő szervezetek azonnali pusztításával járhat,

gázmű-hálózat: mérges gázzal keverve kivédhetetlen fegyver, és ma már minden területen általánosan elterjedt.



Forrás: bitport.hu/630x350KeresesKep/alapjan

Veszélyben a kritikus infrastruktúrák!

* Haza szolgálatában

Big Data, Big Bumm



Összegezve:

- nagyságrendekkel fontosabb lenne az információs hálózatok védelme helyett (mellett) a forgalmazott információk, a feldolgozott, gyűjtött adatok/adatbázisok fokozott védelme!
- A tönkretett vagy elpusztított struktúrákat helyreállítani vagy újraépíteni nem egyszerű de lehetséges, az elveszett adatok információk pótlása lehetetlen!
- A kritikus infrastruktúrákat elsősorban nem támadásoktól kell megóvni, sokkal inkább a támadás eszközeként is használható piszkos fegyverként való alkalmazásuktól!

A kritikus infrastruktúrák védelme újragondolt ösznemzeti feladat kell hogy legyen. Sikeres végrehajtásához magas szinten koordinált védelmi vezetés, normál és válság-helyzetben is érvényes mindenre kiterjedő jogszabályi háttér, szakképzett

– struktúrákat felügyelő és védelmező - apparátus és megfelelő eszközrendszer biztosíthat.

Big Data, Big Bumm



Köszönöm a figyelmet

Nyári László, KDMI B710B2/2014

A MOBIL ESZKÖZÖK BIZTONSÁGI KÉRDÉSEI



A MOBIL ESZKÖZÖK BIZTONSÁGI KÉRDÉSEI

**AVAGY, HOGYAN HASZNÁLJUK A
NYILVÁNOS WI-FI HÁLÓZATOKAT**

Nyikes Zoltán

Bevezetés



- Minden elektronikai eszközünket **védenünk kell**, ezen belül is a mobileszközeinket.
- A „**mobilizáció**” megkönnyíti a mindennapjainkat.

A mobileszközök sérülékenységei



- Fizikai sérülések

- Gondoskodás, védelem, biztosítás.
- Elvesztés – ellopás, a telefon tartalmához hozzáférhetnek.
- Adatok titkosítása.

- Jelszóbiztonság

- Illetéktelen használat, a védelem feltörése.
- 3x3 mátrix grafikus kód, **389.112** kódkombináció.
- A feloldó minta **68%-ban** megfejezhető.

Nyikes Zoltán

3

A mobileszközök sérülékenységei



- Illetéktelen használat, a védelem feltörése

- **Zsarolás** a tartalmakkal, illetéktelen nyilvánosságra hozatal.
- A **felhőben** tárolt adatokhoz való illetéktelen hozzáférés.
- Az ismerőseink, munkahelyünk **kompromittálódása** a telefonon keresztül.

Nyikes Zoltán

4

A mobileszközök sérülékenységei



- Szoftver biztonság

- Rosszindulatú mobil alkalmazások, vírusok, malverek, szoftver csalások.

- **Mobil bankolás**

- *Kizárólag biztonságos csatornán keresztül.*

- Az átviteli út biztonsága

- A **GSM** hálózat gyenge védelme, a telefon követhetősége,
- A **Wi-Fi** hálózatok viszonylag gyenge védelme.

- Hardver biztonság

- USB port használatával a **BadUSB** hiba lehetősége.
- *Csak töltési célra alkalmas USB „szűrő” eszköz.*

Nyíkes Zoltán

5

A mobileszközök sérülékenységei



- Biztonsági szoftverek alkalmazásának hiánya

- **10 éve** jelent meg az első mobilvírus.
- **4 millió** rosszindulatú alkalmazás főleg Androidra.
- 2012-ben **40.059** mobilvírus, 2013-ban **145.000** mobilvírus ez **3x**-os növekedés.
- A 2013-ban észlelt mobilvírusok **98,1%** androidos.
- Adathalászat, bankkártya adatok lopása **20%-os** növekedés.
- Azonosított banki trójai programok 2013 elején **67 db**, 2013 végén **1321 db**.
- 2014 második negyedében **15 millió** fajta új kártevő jelent meg, napi szinten **160.000** új férget, vírust és kémprogramot jelent. Ebből **62,8 %** trójai program, **7%** kémprogram, **2,6-2,6 %** klasszikus vírus és féreg volt.

Nyíkes Zoltán

6

A okos mobileszközök alkalmazása a közszférában



- Előnyei

- Az adatfeldolgozás **gyorsul**,
- **Csökkenthető** a hibás adatbevitel,
- A céges adatvagyon és erőforrások **biztonságos** elérése,
- A dolgozók mobilitása, **növekszik** a „termelékenység” és a dolgozó **elégedettség**.

- Hátrányai

- **Heterogén** eszközpark,
- Eszközök **elvesztése**,
- Az eszközök gyors **erkölcsi avulása**.

Nyikes Zoltán

7

A okos mobileszközök alkalmazása a közszférában



- Az MDM alkalmazása

- A **Mobile Device Management** a mobileszközök és a rajtuk tárolt információk, alkalmazások, illetve a kommunikációs folyamatok központi, távoli **védelme**, flottában történő **menedzselése** a beszerzéstől a kivonásig.

- A BYOD alkalmazása

- A **Bring Your Own Device**, azaz a saját eszköz vállalati célú alkalmazása.

Nyikes Zoltán

8

Egy mobil biztonság vizsgálata ál-Wi-Fi hotspot alkalmazásával.



- A **hotspot nyilvános** vezeték nélküli internet-hozzáférést biztosító szolgáltatás, általában **ingyenes**. Általában **nincs védve** jelszóval.
- A mobil eszközök az első csatlakozást követően a továbbiakban automatikusan **csatlakozik** a hotspothoz.

Nyíkes Zoltán

9

Egy mobil biztonság vizsgálata ál-Wi-Fi hotspot alkalmazásával.



- **A kísérlet (1. fázis)**
 - Egy dunántúli megyeszékhely belvárosában elérhető hotspotokhoz csatlakoztattam **5 mobil eszközt** (3 mobiltelefon, 2 tablet).
 - Az elérhető **10 hotspot** SSID-ját pontosan rögzítettem.
- **A kísérlet (2. fázis)**
 - A otthon, a **saját** Wi-Fi routerem SSID-ját a feljegyzett nyilvános hotspotokéra állítottam.
 - A mobil eszközeim **rövid időn belül**, kérdés nélkül csatlakoztak hozzá.
 - Ezt több SSID-val is végrehajtottam, az eredmény minden esetben ugyan az volt, **kérdés nélkül csatlakoztak!**

Nyíkes Zoltán

10

Egy mobil biztonság vizsgálata ál-Wi-Fi hotspot alkalmazásával.



• A kísérlet (3. fázis)

- A saját eszközeim Wi-Fi elérését lekapcsoltam, a router **bekapcsolva** maradt.
- Egy gyorsétterem-lánc helyi kirendeltségének az ál-SSID-jére **több idegen eszköz** is csatlakozott.
- Másik 3 SSID beállítása **kevésbé** volt népszerű az idegen eszközök esetében.

• A kísérlet (4. fázis)

- A kísérlet **leállítása**.
- A kísérlet **dokumentálása**, a nyert adatok kiértékelése.

Nyikes Zoltán

13

Egy mobil biztonság vizsgálata ál-Wi-Fi hotspot alkalmazásával.



ADVANCED SETUP

MAC	Name
08-00-27-1D-18-01	name=home-100
08-00-27-1D-18-02	name=android-cc
08-00-27-1D-18-03	name=android-20
08-00-27-1D-18-04	name=android-59
08-00-27-1D-18-05	name=android-eszuleke
08-00-27-1D-18-06	name=android-de
08-00-27-1D-18-07	name=android-e5
08-00-27-1D-18-08	name=android-d1

DHCP Client Log

View information on LAN (DHCP) clients currently linked to the wireless router.

2014-05-13 10:10:00 192.168.2.100 login success

2014-05-13 10:10:00 192.168.2.101 login success

2014-05-13 10:10:00 192.168.2.102 login success

2014-05-13 10:10:00 192.168.2.103 login success

2014-05-13 10:10:00 192.168.2.104 login success

2014-05-13 10:10:00 192.168.2.105 login success

2014-05-13 10:10:00 192.168.2.106 login success

2014-05-13 10:10:00 192.168.2.107 login success

Security Log

View any attempts that have been made to gain access to your network.

2014-05-13 10:10:00 192.168.2.100 login success

2014-05-13 10:10:00 192.168.2.101 login success

2014-05-13 10:10:00 192.168.2.102 login success

2014-05-13 10:10:00 192.168.2.103 login success

2014-05-13 10:10:00 192.168.2.104 login success

2014-05-13 10:10:00 192.168.2.105 login success

2014-05-13 10:10:00 192.168.2.106 login success

2014-05-13 10:10:00 192.168.2.107 login success

Az idegen eszközök csatlakozása (a szerző által készítve)

Nyikes Zoltán

14

Egy mobil biztonság vizsgálata ál-Wi-Fi hotspot alkalmazásával.



• Megállapítások

- A mobil eszközök minden esetben **megadták** a router részére a **MAC** azonosítójukat, - *ha be van állítva* - az **elnevezésüket**, Andorid esetében az **OP rendszerüket**.
- A MAC cím első **hat** karakteréből az **eszköz gyártója** beazonosítható.
- A megszerzett információk birtokában megállapítható adatelemző szoftverrel a **kommunikáció iránya**, a csomagok **mérete, típusa**.
- **Hozzá lehet férni** az eszközön tárolt, megosztott **adatokhoz**, **manipulálni** lehet azokat.
- Az eszköz rendszerének **feltörése**, rossz szándékú szoftver bejuttatása, **botnet** részévé lehet tenni.

Nyikes Zoltán

15

Egy mobil biztonság vizsgálata ál-Wi-Fi hotspot alkalmazásával.



MAC Address Lookup

Enter any MAC address, OUI, or IAB below to lookup the manufacturer, location, and more

Where can I find my MAC Address?

MAC Address Details

Company	Apple
Address	Cupertino CA 95014 UNITED STATES
Range	FDFA:1C:50:00:00 - FDFA:1C:5F:FF:FF
Type	IEEE 802.11

A MAC cím beazonosítása (a szerző által készítve)

<http://www.macvendorlookup.com/>

MAC Address Lookup

Enter any MAC address, OUI, or IAB below to lookup the manufacturer, location, and more

Where can I find my MAC Address?

MAC Address Details

Company	Sony Mobile Communications AB
Address	Lund SE-221 89 SWEDEN
Range	68:76:4F:00:00:00 - 68:76:4F:FF:FF:FF
Type	IEEE 802.11

Nyikes Zoltán

16

Egy mobil biztonság vizsgálata ál-Wi-Fi hotspot alkalmazásával.



• Megállapítások (2.)

- A MAC cím **klónozásával** vissza lehet élni, pl. egy kulcspozícióban lévő személy mobil adataihoz való hozzáféréssel, a **vállalati rendszerbe** is be lehet jutni.
- „**Wi-Fi szegény**” környezetben a mobil eszközök (bekapcsolt Wi-Fi-vel) könnyen csatlakoznak egy ál-Wi-Fi hotporthoz.

Nyikes Zoltán

17

Egy mobil biztonság vizsgálata ál-Wi-Fi hotspot alkalmazásával.



Ál-Wi-Fi hotspot működése „Wi-Fi szegény” környezetben (a szerző által készítve)

Nyikes Zoltán

18

Összegzés



- Okos mobileszközök fokozottan sérülékenyek.
- Szükséges olyan lehetőségek alkalmazása, amely a közigazgatásban bevezetendő okos eszközök távfelügyeletét biztosíthatja.
- A lefolytatott kísérlet is azt erősíti, hogy mennyire védtelen még mindig a vezeték nélküli technológia.

Nyikes Zoltán

19



Köszönöm a megtisztelő figyelmet!

Nyikes Zoltán százados

MH 54. Veszprém Radarezred, Információvédelmi központ, központparancsnok
Óbudai Egyetem, Biztonságtudományi Doktori Iskola, doktorandusz
nyikes.zoltan@mil.hu

Nyikes Zoltán

20

BITFÜGGÖNY



Bitfüggöny

Prisznyák Szabolcs bv. őrnagy
mb. főosztályvezető

BVOP Informatikai Főosztály

NKE HDI Phd hallgató

A vasfüggöny

- Jaltai konferencia (1945. február 4-11.)
- Winston Churchill fultoni beszéde 1946. március 5.
 - „A Balti-tenger melletti Stettintől az Adria- tenger mentén fekvő Triesztig vasfüggöny ereszkedik le a kontinensre.”
- A vasfüggöny lebontása: 1989



Határőrizet egykor és ma



Napjainkban a nyomozó hatóságok a bűncselekmények többségét a számítógép mellett ülve oldják meg.



Informatikai támogatás a magyar határőrizetben, történeti áttekintés a Schengeni csatlakozásig

- Az első számítógépek az 1980-as évek második felében
 - Késszámítógépes rendszer
- A rendszerváltozással új kihívások (szervezett bűnözés, illegális migráció, határon átnyúló bűnözés, ember-, kábítószer-, fegyvercsempészet)
- Az informatikai rendszerek folyamatos fejlődése
 - Foto Technikai Rendszer (FTR)
 - Határőrségi Automatikus Adattovábbító Rendszer (HAAR)
 - Solarium 2i
 - Kaktusz-1
 - Határregisztrációs rendszer (HRR)
 - Határellenőrzési és Regisztrációs Rendszer (HERR)
 - HERR I+



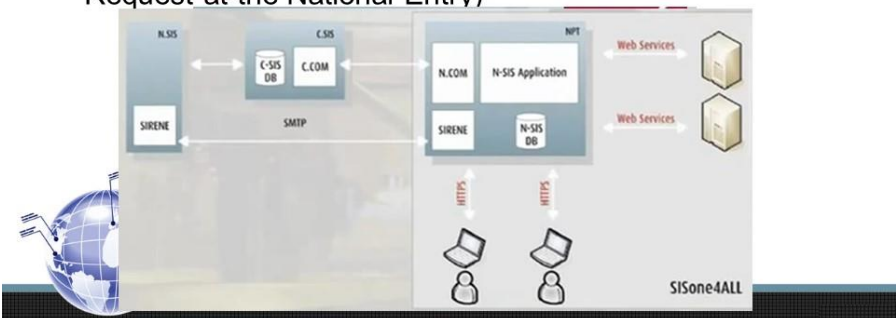
Schengen

- A Schengeni Végrehajtási Egyezmény
 - 1990. jún. 19. → közös információs rendszer
- Schengen Information System (SIS)
- Automatizált lekérdezések során a személyekre és tárgyakra vonatkozó információkhoz való hozzáférés
 - Bel- és igazságügyi együttműködés,
 - Vízumok és tartózkodási engedélyek kiadása,
 - Országhatáron és mélységben végzett ellenőrzések
- A rendszert később módosították → SIS I+

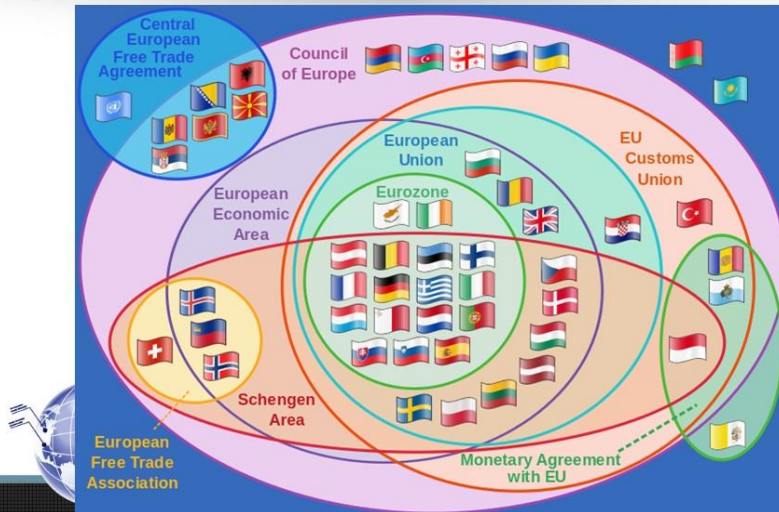


Schengen bővítése (2007)

- 2001-ben döntés a SIS II fejlesztéséről
- A fejlesztés folyamatosan csúszott
- Portugál megoldás: SISone4ALL (2006. dec.)
- ORFK NEBEK Sirene Iroda (Supplementary Information Request at the National Entry)



Európa napjainkban



SIS II

- Schengen Information System II (2013. április 9.)
 - beutazási és tartózkodási tilalom hatálya alatt álló személyek,
 - körözés információk (európai elfogatóparancs),
 - eltűnt személyek, különösen a kiskorúak,
 - gépjárművek, hajók, fegyverek, személyazonosító, okmányok (eltulajdonított vagy bűncselekményhez felhasznált),
 - személyazonosításhoz szükséges adatok; fényképek, biometrikus azonosítók,
 - figyelmeztető jelzések, végrehajtandó intézkedések



- Hozzáférés: nemzeti bűnüldöző, igazságügyi és közigazgatási hatóságok
- Szigorú adatvédelem



Változások a határrendészetben

- Határellenőrzés: határforgalom ellenőrzés + határőrizet
- Schengeni Határellenőrzési Kódex (2006)
- Négy lépcsős modell
 - Harmadik országban történő intézkedések
 - Szomszédos harmadik országgal történő együttműködés
 - Határellenőrzés (schengeni külső határ)
 - Szabad mozgás térségében végrehajtott ellenőrzés
- FRONTEX (2004. október 26.); székhelye: Varsó
 - Európai Unió Tagállamai Külső Határain Való Operatív Együttműködés Igazgatásáért Felelős Európai Ügynökség
 - Képzési szabványok, képzések, kockázatelemzés, ellenőrzés figyelemmel kísérése, technikai, operatív segítség, szervezi az Európai Határőrcsapatok bevetését, közös visszatérési műveletek.



További információs rendszerek

- **VIS:** Visum Information System
 - Egységes vízumpolitika, vízumkiadás
 - Csalások, hamisítások megakadályozása
 - Évi 20 millió igénylő személyes és biometrikus adatai (5 év tárolás)
- **EURODAC:** menekültkérők nyilvántartása
 - Menedékkérők azonosítása
 - Jogellenes határátlépők azonosítása
 - Személyes és biometrikus adatok
- **EUROSUR:** European Border Surveillance System - Európai Határőrizeti Rendszer (2013. dec. 2.)
 - Az integrált
 - Kockázatelemzés
 - Négyféle nemzeti szintű információ
 - Kame
 - alkalm



Elektronikus okmány nyilvántartások

Az Európai Unió
Tanácsa

PRADO

EREDETI SZEMÉLYAZONOSÍTÓ ÉS ÚTI OKMÁNYOK ONLINE NYILVÁNTARTÁSA

Magyar (hu) Q

[Főoldal](#)
[Keresés](#)
[Glosszárum](#)
[Szűrések](#)
[Okmányszám érvényességének ellenőrzése](#)
[Rólunk](#)
[GYIK](#)

Főoldal > BEL-PP-01003

<Előoldal (megszemélyesítéssel)> - <Hordozóanyag>



A jelen és a jövő

- **EES:** Entry Exit System; Határregisztrációs Rendszer
 - Ki-, és belépés elektronikus regisztrációja
 - Tartózkodási idő kiszámítását egyszerűsíti
- **RTP:** Registered Traveller Programme; Regisztrált Utas Program
 - Egyéniesítés: nem csak az országot vizsgáljuk, hanem a konkrét személyt is



- **EULISA:**
 - 2012. december 1-től.
 - Székhelye: Tallin; irányítás: Strasbourg; tartalék egység: Sankt Johann im Pongau (Ausztria); működési költsége: kb. 60 millió € / év
 - Az EULISA az alábbi rendszereket üzemelteti: **SIS II**; **VIS**; **EURODAC**



European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice



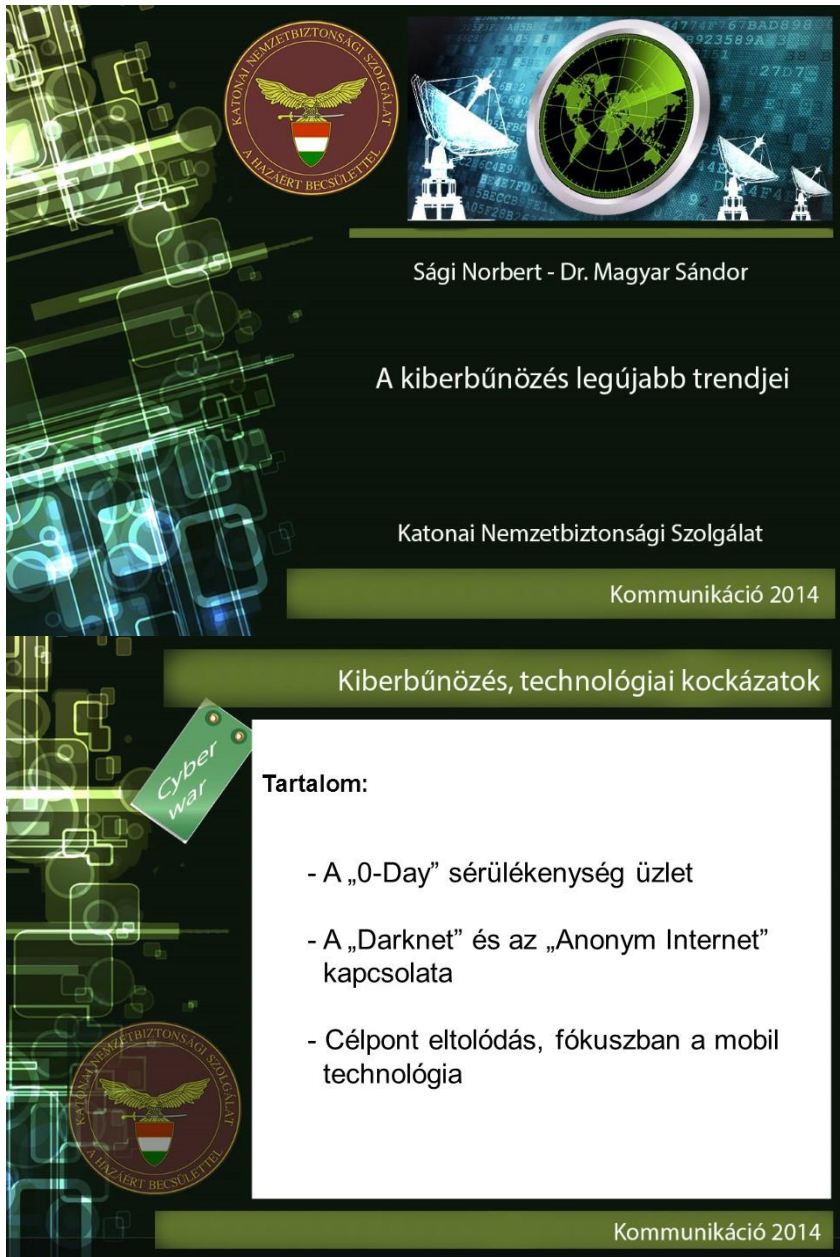
Köszönöm a megtisztelő figyelmet!

e-mail: prisznyak.szabolcs@bv.gov.hu



SÁGI Norbert – Dr. MAGYAR Sándor

A KIBERBŰNÖZÉS LEGÚJABB TRENDJEI



Sági Norbert - Dr. Magyar Sándor

A kiberbűnözés legújabb trendjei

Katonai Nemzetbiztonsági Szolgálat

Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

 Tartalom:

- A „0-Day” sérülékenység üzlet
- A „Darknet” és az „Anonym Internet” kapcsolata
- Célpont eltolódás, fókuszban a mobil technológia

 Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Cyber
war

A „0-Day” sérülékenységi üzenet:

Mit is takar az „Unspecified Vulnerability” fogalma?

Miért veszélyes ez a gyakorlat?

Hogyan üzletelnek a kiberbűnözők a „0-Day” sérülékenységekkel, mekkora piaca van?

Mit is ér valójában a frissítések telepítése, és kik ellen védekezünk egyáltalán?

Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Cyber
war

Hogyan üzletelnek a kiberbűnözők a „0-Day” sérülékenységekkel, mekkora piaca van?



- Anonym , védett és titkosított Internet vonal
- Védett Webáruház a DarkNet-en
- A cél: Pénz, Hatalom. (Siker – nem jellemző)

Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Hogyan csatlakoznak anonim módon a profi kiberbűnözők az Internetre?



Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Az igazi DarkNet Felhő: The Onion Router v 2.0

- VPN 3 rétegű RSA titkosítással, 3 különböző útvonalal.
- Minden titkosított adatcsomag 3 részre van vágva. Minden egyes szelet más útvonalon és más kódolási rétegekkel jut el a kilépő pontig. Az adatcsomag itt áll össze ismét.

RUNNING RINGS AROUND POLICE



Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Cyber
war

Mi a nyomozóhatóságok dilemmája a DarkNet-el?

- A kilépő pont IP címe nem azonos az elkövető valós IP címével, így nem határozható be a támadó kiléte.
- A **támadás idegen zászló** alatt vagy **zászló nélkül** zajlik.
- Egy „orosz” szó felfedezése az ártó kódban nem biztos hogy azonosítja a támadó országot, mert a kódokkal üzletelnek, bárhol átírhatják az eredetit és bevethetik.



Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Cyber
war

Mit találunk a „The Onion Router” felhőjében?

A DarkNet v. DeepNet:

- Silk Road Anonymus Webáruház *
- Hidden and Dark Wiki Webáruház



Silk Road

anonymous marketplace

- (2013. október 2-án az FBI lefoglalta a szervereket, azóta 2.0 néven újra nyílt.)

Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Cyber war

Mit vásárolhatunk itt illegálisan?



messages(0) | orders(0) | account(\$0.00) | settings | log out

SEARCH | 0

Shop by category:

Drugs(1462)
Benzos(153)
Cannabis(527)
Dissociatives(26)
Ecstasy(86)
Opioids(116)
Other(148)
Psychodelics(173)
Stimulants(137)
Apparel(4)
Art(26)
Books(118)
Computer equipment(1)
Digital goods(63)
Drug paraphernalia(26)
Electronics(10)
Food(1)
Forgery(17)
Home & Garden(1)
Lab Supplies(4)
Medical(7)
Money(85)
Services(34)
Weaponry(25)
XXX(43)



\$17.45



\$31.55



\$8.88



\$11.09



\$16.58



\$42.68



\$175.97



\$11.63



\$15.72

News:

- State of the Road Address
- Silk Road has a new URL
- Announcing the new wiki
- New shipping and display features

Rivort/Viclonopin 2 mg Roche Cinsanep x 100 | Largetto



Kábítószer; Fegyver; Pedofil videók; „0-Day” Sérülékenység
Kész és működő ártó kódok, Bank Kártya Adatok stb.

Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Cyber war

A Hidden Wiki – Dark Wikipedia

File Edit View History Bookmarks Tools Help

http://kpzv7ki2v5agwt35.onion/wiki/index.php/Main_Page#Marketplace

TorMarks Tor Directory Error

The Hidden Wiki

Marketplace

See also: [Marketplace Reviews](#) - Reviews of the marketplace experience. (ALL reviews go in this article, NOT in the listings below.)

Financial Services

Currencies, banks, money markets, clearing houses, exchangers.

- [BTC000](#) - Sells prepaid credit cards (Bitcoin). (Was: Mr. Brownstone which died on 2011-05-16) - DOWN 2011-08-07
- [Bank Bitcoin Transfers](#) - Laundry service, etc. Had source code. (Compromised) - Broken 2011-08-01
- [BitcoinATM cleared](#) - Converts your Bitcoins into a virtual VISA credit card instantly.
- [BitcoinCash cleared](#) - Buy Bitcoins with cash in the mail.
- [The Bitcoin Washing Machine](#) - Can launder large amounts of coins without same-coin contamination. 1% fee. (Link, FH)
- [Sell Your BTC](#) - Sell your Bitcoins for other currencies. (Link, FH) (Calculator returns 404) - Broken 2011-04-23
- [MyBitcoin cleared](#) - A web-based payment processor (Bitcoin). It has extensive Tor support. Free, ad supported. (Compromised) - Broken 2011-07
- [BTCLaundry](#) - For all your Bitcoin washing needs. (Link, FH)

Commercial Services

Buying and selling stuff, auction houses, sales forums, gaming.

See also: The separate [Drugs](#) and [Erotica](#) sections for those specific services.

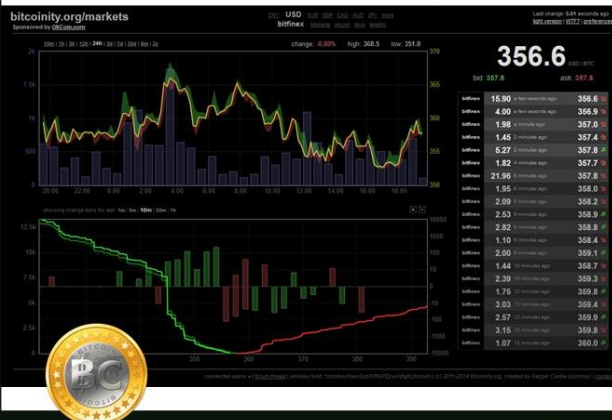
- [Contract Killer](#) - Kill your problem (snitch, paparazzo, rich husband, cop, judge, competition, etc). (Link, FH)
- [RePower v1.93](#) - Peaker (Bitcoin). (Link, FH)
- [Buttery Bootlegging](#) - Get any expensive item from major stores for a fraction of the price! (Link, FH)
- [Sell IDs](#) - Selling fake IDs.
- [ReCoin](#) - Like Ebay. We increase the gross national product. (Link, FH)
- [Video Poker](#) - A casino that features "jacks or better" video poker. - DOWN 2011-08-07
- [Cheap SWATTING Service](#) - Calls in raids as pranks. (Link, FH)
- [Data Buy](#) - Buy and sell files using digital currency.
- [The Last Bag](#) - Assassination Market (Bitcoin). - DOWN 2011-08-07
- [Prank Web DDoS](#) - Take out your enemies in seconds. (Link, FH)

Hacker Kézikönyv; Hacker bérlet; Bérgyilkos megbízása;
BotNet hálózat bérlet 2 layer DDoS támadásokhoz stb.

Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Hogyan adják-veszik a kiberbűnözők az illegális dolgait az Interneten?



Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Sokkoló kiberbűnözési adatok - Magyarország:

- 2465 Internet felhasználó válik áldozattá naponta
 - 102 károsult óránként
 - 1,7 károsult percenként
- (Norton CyberCrime Report 2013)

Sokkoló kiberbűnözési adatok - Globális:

- 556 millió áldozat évente
 - „Magasabb szám, mint az EU népessége”
 - A kiberbűnözés globális bevétele: 110 milliárd USD (2012)
 - „Ennyit költenek az USA-ban gyorsételekre”
 - 197 USD átlagos anyagi kár, károsultanként
- (Norton CyberCrime Report 2013)
- Egy felhasználható **JAVA „0-Day”** 100.000 USD a DarkNet-en.
- (TechWeek Europe 2013)

Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Cyber
war

Kiberbűnözési adatok változása - Globális:

- 91%-al növekedtek a célzott támadások
- 62%-al növekedett a kiber bűncselekmények száma
- 552 millió személyes adatot loptak el
- 23 „0” Day sebezhetőséget fedeztek fel
- 38%-al nőttek a mobil eszközök elleni támadások
- 66%-ra csökkent a Spam-ek száma össz. levél (69%)
- 1392 adathalász levél típust azonosítottak
- 23%-al nőttek a Web alapú támadások
- 8 népszerű Weboldalból 1 fertőzött - malware

(Norton 2014 Internet Security Threat Report – harmadik negyedévi összesített adat)

2013 YEAR OF THE
MEGA BREACH

Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Cyber
war

Mobil eszközök az új célpontok, miért is?

- 2010-re elmosódtak a határok a hagyományos PC-k és mobil eszközök között;
- Keverednek a technológiák: laptopon is használhatunk Android operációs rendszert, illetve egy mobil eszközön is lehetőség van Windows OS futtatására;
- A platform független programozási technológiák népszerűek, így az alkalmazás rétegben sincs különbség; (PERL, C#, Oracle Java, SQL, JQuery, HTML5, Adobe Flash)
- 2013-as esztendőben már egy nagyságrenddel több okos mobil eszközt vásároltak a világon, mint PC-t.

Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Cyber
war

Mobil eszközök az új célpontok, miért is?

- A mobil eszközöket gyártó cégek nem fektetnek kellő hangsúlyt a mobil eszközök védelmére;
- Sokáig csak mítosz volt egy mobiltelefonokon terjedő ártó kód;
- Egy átlagos iOS és Android program 12.000 soros programkódjában, átlagosan 1000 programozási hiba van.



Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Cyber
war

Mobil fenyegetések célkeresztben az Android

- 2013 évben 51447 támadás érte Android OS-t használó mobileszközöket; ebből:
- 2.2. (Froyo) verziót a kártékony szoftverek 4 százaléka célozza;
- 2.3. (Gingerbread) verziót pedig 52 százalékuk érinti
- 4.0. (Ice Cream Sandwich) verziót a kártékony szoftverek 38 százaléka célozza;



Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Cyber
war

Mobil fenyegetések célkeresztben az Android

- Az Android OS-t használó okos telefonok különösen sérülékenyek a káros szoftvertámadásokra;
- Sajnos, a felhasználók csak nagyon kis része telepít mobilkészülékére rootkit – malware – vírus és határvédelmi megoldásokat;
- A kiberbűnözők, viszonylag korán felismerték és kihasználták ezt a tényét, ezért a 2014-es évben 500%-al nőtt a **RansomWare** - un. „váltásdíj-támadás” és **RansomCrypt** – Cryptolocker támadás aránya az előző évhez képest, amihez ingyenes vírusirtó szoftvernek tűnő „ál-vírusirtó” alkalmazásokat töltenek fel az **iOS AppStore / Droid Google Play**-be.

Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Cyber
war

Megszűnik a telekommunikáció technológiai szegmentáltsága?

- A Szolgáltatók 3-5 éven belül átállnak tisztán IP alapú technológiára;
- Olcsóbb üzemeltetés és karbantartás, távoli menedzsment, erőforrás centralizáció, magasabb profit ... de mely országban kezelik az előfizetői adataimat?;
- Hátrány: Felteszünk mindent egy lapra ... csak egy technológiát kell támadni és digitálisan elsötétül az ország? Nemzeti érdekek védelme?

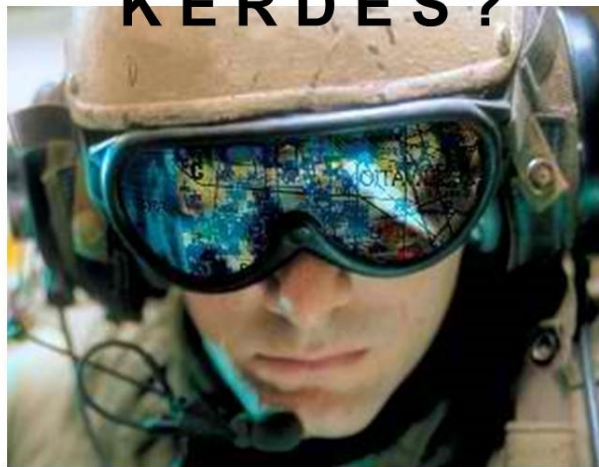


Kommunikáció 2014

Kiberbűnözés, technológiai kockázatok

Cyber
war

K É R D É S ?



Kommunikáció 2014

TÓTH András

A DÖNTÉSHOZATALI FOLYAMATOK HÁLÓZATKÖZPONTÚ TÁMOGATÁSI LEHETŐSÉGEI

A DÖNTÉSHOZATALI FOLYAMATOK HÁLÓZATKÖZPONTÚ TÁMOGATÁSI LEHETŐSÉGEI

Tóth András százados

PhD Hallgató

Nemzeti Közsolgálati Egyetem

KATONAI DÖNTÉSHOZATALI FOLYAMAT ELEMEI

FELADAT VÉTELE

FELADAT ELEMZÉSE

- A művelet céljának meghatározása
- A feladatok meghatározása
- A kritikus információigény meghatározása

Jelentés a Parancsnoknak

CSELEKVÉSI VÁLTOZATOK ELKÉSZÍTÉSE

Eligazítások

CSELEKVÉSI VÁLTOZATOK MODELLEZÉSE

CSELEKVÉSI VÁLTOZATOK ÖSSZEVETÉSE

Bemutatók

CSELEKVÉSI VÁLTOZAT KIVÁLASZTÁSA

- Cselekvési vázlat elfogadása
- A parancs és a végrehajtás meghatározása

Feladatszabó értekezlet

PARANCS ELKÉSZÍTÉSE

Parancs ismertetése

FELADAT VÉTELE

- Szükséges források összegyűjtése (például térkép a műveleti területről)
- A feladatelemzéshez szükséges főbb pontok meghatározása (szituáció, felelősségi körzetek, saját, ellenséges és baráti erők, támogatási követelmények)

FELADAT ELEMZÉSE

Az előljáró elgondolásának értékelése

A művelet céljának meghatározása

A feladatok meghatározása: előljáró által meghatározott, kikövetkeztetett és elengedhetetlen feladatok

A hadszíntér felderítő értékelése

A főerőkifejtés irányának meghatározása

A kritikus információigény meghatározása

A feladat-végrehajtás sikerét befolyásoló tényezők megállapítása

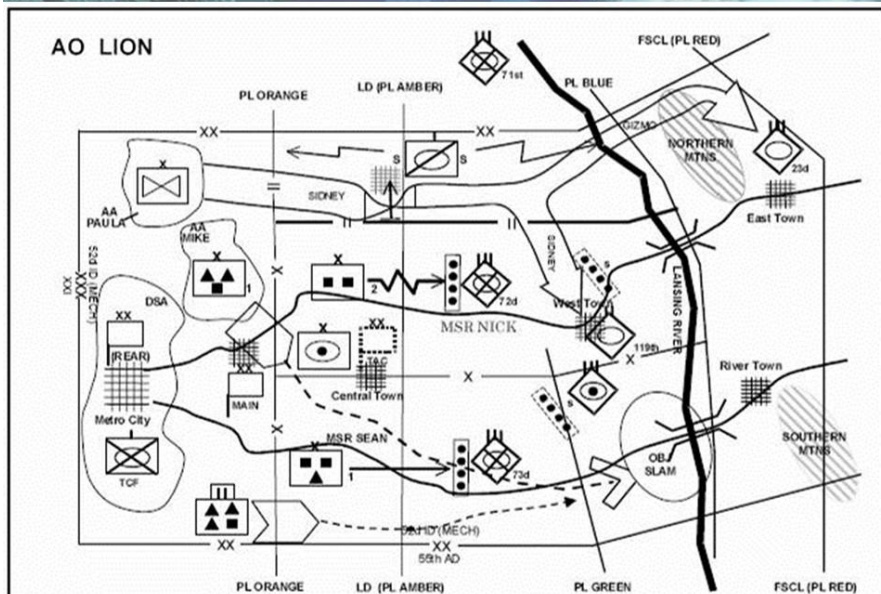
A korlátozó tényezők megállapítása és kiküszöbölése

Az előljárótól elvárt segítségnyújtás területeinek megállapítása

Törzseligazítás – feladatértékelés eredményének ismertetése.

Előzetes harcintézkedés kiadása az alárendeltnek felé

CSELEKVÉSI VÁLTOZATOK KIDOLGOZÁSA



CSELEKVÉSI VÁLTOZATOK MODELLEZÉSE

1. A SAJÁT CSELEKVÉSI VÁLTOZATOK HATÉKONYSÁGÁNAK ÉRTÉKELÉSE
2. AZ ELLENSÉG LEGVALÓSZÍNŰBB ÉS LEGVESZÉLYESEBB CSELEKVÉSI VÁLTOZATÁNAK MEGÁLLAPÍTÁSA
3. A SAJÁT CSELEKVÉSI VÁLTOZATOK GYENGE PONTJAINAK, A MŰVELET LEHETSÉGES FÁZISAINAK ÉS A KÖVETKEZMÉNYEKNEK MEGHATÁROZÁSA
4. A TEVÉKENYSÉGI VÁLTOZATOK ÖSSZEHASONLÍTÁSA ÉS JAVASLATTÉTEL A DÖNTÉS MEGHOZATALÁHOZ

CSELEKVÉSI VÁZLAT KIVÁLASZTÁSA

A PARANCSNOK:

- A KIVÁLASZTOTT CSELEKVÉSI VÁLTOZATOT MÓDOSÍTÁSOK NÉLKÜL FOGADHATJA EL.
- A MEGÁLLAPÍTOTT HÁTRÁNYOK KIKÜSZÖBÖLÉSE ÉRDEKÉBEN MÓDOSÍTÁSOKRA ADHAT UTASÍTÁST.
- KIALAKÍTHAT EGY TELJESEN ÚJ CSELEKVÉSI VÁLTOZATOT, FELHASZNÁLVA VALAMENNYI VÁLTOZAT ELŐNYOS ÖSSZETEVŐIT.
- ELRENDELHETI ÚJ CSELEKVÉSI VÁLTOZATOK KIALAKÍTÁSÁT VAGY A TELJES TERVEZÉSI FOLYAMAT ÚJRAKEZDÉSÉT.

PARANCS ELKÉSZÍTÉSE

1. HELYZET

1.1 ÁLTALÁNOS

1.2 RÉSZLETES

2. FELADAT

3. VÉGREHAJTÁS

3.1 A PARANCSNOK SZÁNDÉKA

3.2 A MŰVELET ELGONDOLÁSA

4. HARCIS KISZOLGÁLÓ TÁMOGATÁS

4.1 LOGISZTIKA

4.2 EGÉSZSÉGÜGY

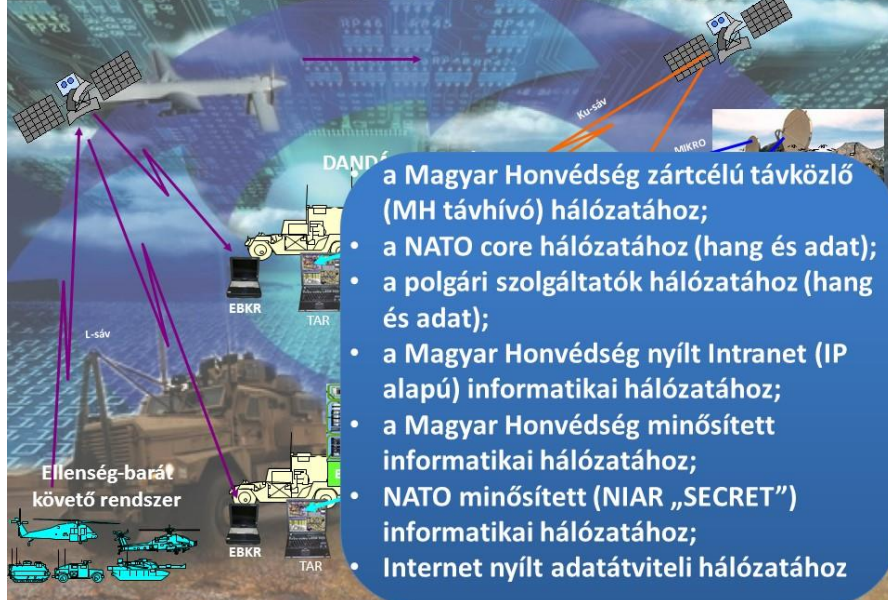
5. HÍRADÁS – VEZETÉS

6. MELLÉKLETEK

HÁLÓZATKÖZPONTÚ VEZETÉSI PONT



HARCÁSZATI KOMMUNIKÁCIÓ



MEGOSZTOTT HARCASZATI KOMMUNIKÁCIÓS RENDSZER

HÁLÓZATBA KAPCSOL

- BIZTONSÁGOS, MAGYAR HÁLÓZATBA KAPCSOL
- TÁMOGATJA A NAGY TÁVOLSÁGOK A MOZGÁS KÖZÖTT
- VALÓS IDEJŰ HELYZETBEÉPÍTETT HELYZET
- KÉPES KORLÁTLAN SÁVHÁZ
- INETOPERÁBILIS FÖLDKÖRNYEZETI HÁLÓZATOKKAL ÉS ESZKÖZÖKKEL
- HANG ÉS ADAT KOMMUNIKÁCIÓ PÁRHUZAMOS ALKALMAZHATÓSÁGA VÉDETT VONALON
- TÁMOGATJA A TÁVMENEDZSMENTET (PROGRAMOZÁS, IRÁNYÍTÁS, ÜZEMBENTARTÁS)

KÖSZÖNÖM A
FIGYELMET!

TURÁNYI Zoltán

**A KATASZTRÓFAVÉDELEM INFOKOMMUNIKÁCIÓS
RENDSZEREI**

**A katasztrófavédelem infokommunikációs
rendszerei**

Turányi Zoltán tű. alezredes

Térinformatikai és Távközlési osztályvezető

BM Országos Katasztrófavédelmi Főigazgatóság



Kommunikáció 2014
Budapest, 2014. november 12.

Infokommunikációs szakterület

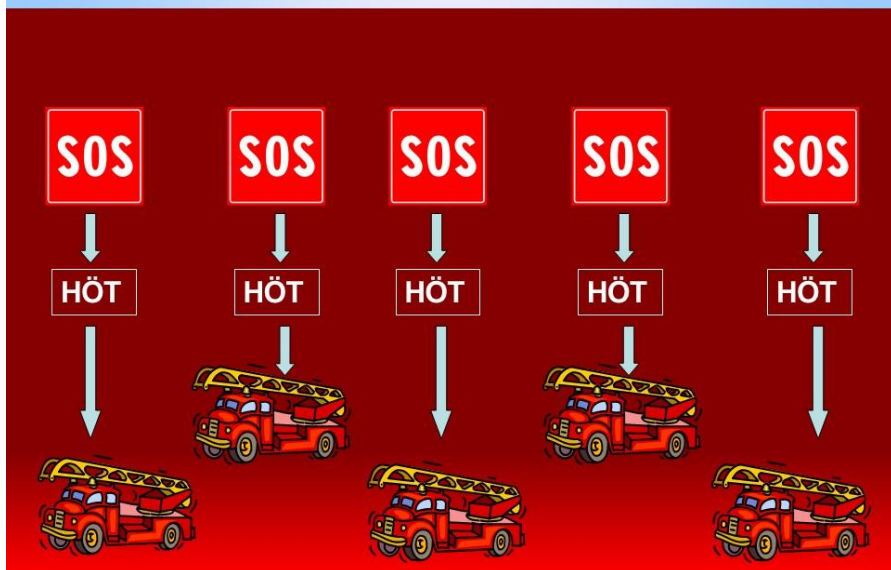
- Segélyhívás fogadás, távbeszélő rendszer,
- Viharjelző rendszerek,
- Lakosságtájékoztatási és riasztó rendszerek,
- Pályázati lehetőségek,
- Térinformatikai támogatás,
- Informatikai hálózatok, szolgáltatások.

2012. évi távközlési fejlesztés

- 18 új telefonközpont
- 18 digitális hangrögzítő
- Fax szerver
- 76 db rendszerkészülék
- 1180db IP telefonkészülék
- 18db telefonközpont upgrade

~ 150 mFt

Segélyhívás fogadás 2012 előtt



Segélyhívás fogadás 2012 után



MoLaRi rendszer elvi vázlata



Ipari baleset



A veszélyes anyag
érzékelése

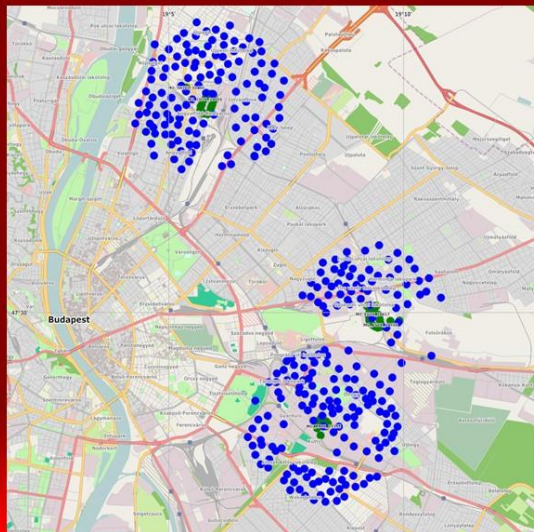


Jelzés feldolgozása



Lakosság riasztása,
tájékoztatása

A MoLaRi budapesti szegmensei



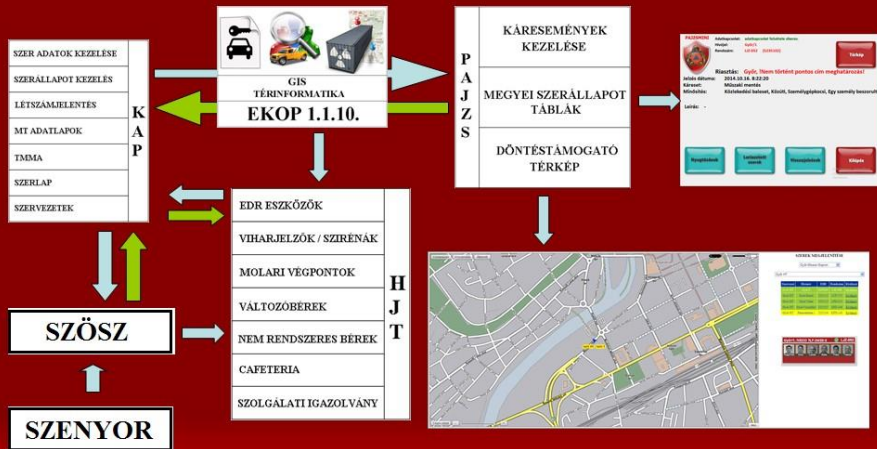
Pályázatok

- Megyei, regionális pályázatok,
- EKOP-1.A.1-08/B-2009-0004 ,
- Közös kockázatbecslés és felkészülés a Duna makrorégióban ,
- Pályázatok az Önkéntes Tűzoltó Egyesületek támogatására,
- EKOP-1.1.10 A katasztrófa-védelmi informatikai rendszerek döntéstámogató szerepének és biztonságának növelése.

Térinformatikával támogatott rendszerek

- Tűzoltósági műveletirányítás,
- Polgári védelmi műveletirányítás,
- Veszélyes áruszállítás,
- Gépjárműnyilvántartás,

Adatok átjárhatósága



Köszönöm a figyelmet!

Turányi Zoltán tő. alezredes
Térinformatikai és Távközlési osztályvezető

BM Országos Katasztrófavédelmi Főigazgatóság



Kommunikáció 2014
Budapest, 2014. november 12.

Gábor VANDERER

SECURITY AWARENESS AND SOCIAL RESPONSIBILITY

Security Awareness and Social Responsibility

Gábor VANDERER
Óbudai University
Doctoral School on Safety and Security
Sciences

Information Society

- Electronic administration
- NEPTUN, e-files
- National Consultation

Broad sections of society use internet-based channels, but a significant number of users are not aware of the dangers.



Information Security

- 20 years ago – problem of professionals
- Later – problem of employers
- Today – everyone's problem. We either ignore it or not.

Not just IT technologies are a part of our life but the Internet as well.



Security Awareness

- Laptop
 - Sensitive data can get out of the workplace
- SmartPhone
 - Common platform for internet access
 - Stored password
 - Access codes and IDs
 - Photos



Non-Secure Environment

- It was evident 20 years ago that we do NOT store sensitive data in non-secure environment
 - Encryption, Document-management systems, etc.
- The SmartPhone is typically non-secure
 - Could be lost
 - Could be stolen



In case of a loss...

- What is the percentage of SmartPhone users who are able to put together their compromised access codes?
- „My laptop has been stolen with irreplaceable documents on the hard drive...”
 - Backup?
If you are already aware of the criticality of data, handle it accordingly!



Credit cards and PIN codes

- Banks spent more than 10 years on educating their customers
 - Do not write the PIN on the card
 - Do not store the PIN in the same wallet
 - Do not write the PIN anywhere
- Today they move toward policy enforcement
 - Tokens generating single-use passwords
 - Codes sent via SMS



The lesson of the banks

- Banks protect their users' data - because they themselves also have an interest in it.
- A new generation has grown up. Using Internet technology is more natural for them, but with the loss of aversion also a healthy sense of fear is lost



Generation Z

- Born after 1996
- They live on the Internet
 - They gatehr information from the Internet
 - Source criticism!
 - „Heard from friends” is considered more authentic than mainstream media messages



Source Criticism

- Incredible amount of information could be accessed at any time
 - You can find **anything** on the Internet and also the opposite
 - Source criticism have to be learnt and used
- What makes a source authentic?
 - What makes an Internet-based source authentic?



Financial literacy and crisis

- In connection with the credit crisis, it has been mentioned several times how low the financial literacy of our country is.
 - Indeed
- Same with information security - and it becomes more and more important.

Should not wait until a crisis breaks out.



Threats

- More or less unregulated area
 - Tallin Protocol
- 4th Generation warfare
- Perfect weapon for terrorists

Do not be the weakest link!



Development opportunities

- Banks can give up, but the society can not
 - We use technology to work around structural problems
- Adult Education - ECDL
 - IT Security module since 15 Oct. 2013
- Graduation
 - Informatics (not mandatory)
- Source criticism

Hivatkozások

- ⁱ Miklós Hóka: The Tactical Internet, Overview of a new type communications system for command and controls, AARMS, Vol. 2, No. 2 (2003), ZMNE, p.: 272
- ⁱⁱ AEDP2 - NATO Intelligence, Surveillance, Reconnaissance (ISR) Interoperability Architecture
- ⁱⁱⁱ <http://www.zmne.hu/tanszekek/ehc/konferencia/may/szalai.htm> (Letöltve: 2014. április 15.)
- ^{iv} NC3 Common Operating Environment and Transformation to the NATO Network Enabled Capability”, NATO C3 Technical Architecture, Volume 5, Version 7.0
- ^v ACT Transformation Network Portal:
<https://transnet.act.nato.int/WISE/Information>
- ^{vi} Magyar Sándor mk. őrnagy: Katonai kommunikációs igények, lehetőségek a békefenntartás vezetésének támogatásában, Doktori (PhD) értekezés, Budapest 2008, p.: 71
- ^{vii} Farkas Tibor főhadnagy: A válságreagáló műveletek vezetését és irányítását támogató híradó- és informatikai rendszer megszervezése a Magyar Honvédség többnemzeti műveleteinek tükrében, Doktori (PhD) értekezés, Budapest 2010, p.: 87
- ^{viii} Kassai Károly mk. alezredes: A Magyar Honvédség Információvédelmének – mint a biztonság részének – feladatrendszere, Doktori (PhD) értekezés, Budapest 2007, p.: 51
- ^{ix} Field Manual (FM) 3-0, *Operations*, Chapter 3
- ^x http://www.biztonsagpolitika.hu/documents/1276888013_dr_szenes_zoltan_a_nato_jovoje_uj_strategiai_koncepciora_van_szukseg_-_biztonsagpolitika.hu.pdf (Letöltve: 2014. március 18.)