HÍRVILLÁM

A NEMZETI KÖZSZOLGÁLATI EGYETEM
Híradó Tanszék szakmai tudományos kiadványa

SIGNAL Badge

Professional journal of Signal Departement
at the University of Public Service

2023

Infokommunikáció 2023

tudományos szakmai konferencia

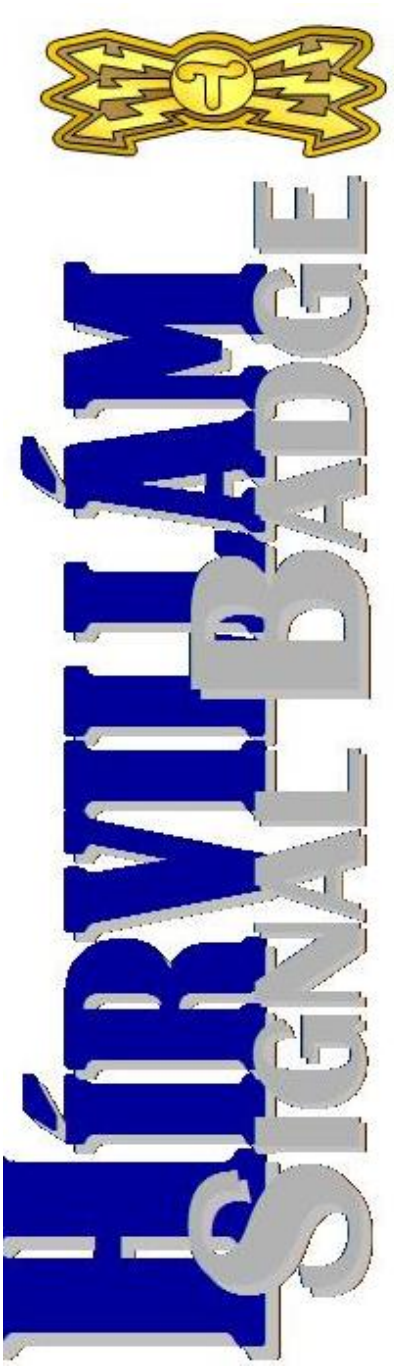
Konferencia kiadvány

2023. november 15.

HÍRVILLÁM
a Nemzeti Közszolgálati Egyetem, Híradó Tanszék tudományos időszaki kiadványa

SIGNAL BADGE
Professional Journal of the Signal Departement at the University of Public Service

Budapest, 2023



HU ISSN 2061-9499

NKE Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf.: 15
+36 1 432 9000 (29-407 mellék)

Tartalomjegyzék

Köszöntő

Tisztelettel köszöntjük Önt, Kedves Kolléga, Tisztelt Olvasó!

A Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Híradó Tanszéke, együttműködésben a Magyar Honvédség Honvéd Vezérkar Híradó és Informatikai Csoportfőnökségével, a Nemzeti Média- és Hírközlési Hatósággal, a Hírközlési és Informatikai Tudományos Egyesülettel, illetve a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Puskás Tivadar Műszaki Szakkollégiumával, 2023. november 15-én, idén 22. alkalommal rendezte meg nemzetközi tudományos-szakmai konferenciáját.

A konferencia szerves részét képezi a Magyar Tudományos Akadémia által fémjelzett, több évtizedes múltra visszatekintő, Magyar Tudomány Ünnepe rendezvénysorozatnak, amelyről az akadémia már 1997 óta megemlékezik, és 2003 óta hivatalosan is megünnepeljük minden év november 03-án. Ezzel emléket állítva, és tisztelegve azon momentumnak, amikor is Széchenyi István birtokai egy évi jövedelmét felajánlva hozzájárult a Magyar Tudós Társaság megalapításához, mely a későbbiekben lehetővé tette a Magyar Tudományos Akadémia megalapítását.

A konferencia - amely első alkalommal 2000-ben került megrendezésre - célja egy olyan tudományos-szakmai fórum biztosítása, amelynek keretében az infokommunikációban jártas, a professzionális- és a védelmi szférát képviselő hazai és nemzetközi

szakemberek, kutatók, egyetemi polgárok és hallgatók megoszthatják egymással ismereteiket, tapasztalataikat, bemutathatják kutatásaik eredményeit és kapcsolatokat építhetnek.

A konferencia során az infokommunikációval és az információbiztonsággal kapcsolatos kapcsolatos új trendeket és kihívásokat 12 színvonalas előadás keretében érdekesebbnél érdekesebb aspektusokból világították meg az előadók. Az érdekfeszítő előadások mellett, a rendezvény szakmai színvonalát emelte, az együttműködő partnereknek köszönhetően, egy látványos, a jelenkor technológiai-, technikai- és szolgáltatásszínvonalát felvonultató kiállítás is.

A rendezvény több mint 80 fő regisztrált résztvevőt számlált.

Jelen kiadványban a szerkesztőbizottság a szerzők hozzájárulásával az egyes előadásokból készített korreferátumokat gyűjtötte össze, amelynek eredményeképpen öt előadás került megjelentetésre, amelyeket nagyon nagy örömmel bocsájt rendelkezésre a Kedves Olvasóknak.

Budapest, 2023. november 15.

Dr. Tóth András
a Szerkesztőbizottság
elnöke

A HAZA SZOLGÁLATÁBAN

A MAGYAR TUDOMÁNY ÜNNEPE

TUDOMÁNY: VÁLASZOK A GLOBÁLIS KIHÍVÁSOKRA

MTA

Nemzeti Média- és Hírközlési Hatóság

INFOKOMMUNIKÁCIÓ 2023

Nemzetközi tudományos-szakmai konferencia programja

(2023. november 15.)

Fővédnök: **Dr. Gulyás Attila ezredes**

(Honvéd Vezérkar Híradó és Informatikai Csoportfőnökség csoportfőnök)

09:30-10:00	**REGISZTRÁCIÓ**
Levezető elnök: **Dr. Magyar Sándor** **Plenáris ülés I.**	
09:55-10:00	**MEGNYITÓ** **Dr. Tóth András**
10:00-10:20	**Dr. Orbán József (Nemzeti Média- és Hírközlési Hatóság):** A reziliens szervezet és a nem polgári infokommunikáció egyes kérdései
10:20-10:40	**Knerli Attila (Scorpio Kft.):** Komplex, gyorstelepítésű megoldások minden helyzetre
10:40-11:00	**Juhász László (Enterprise Communication Magyarország Kft.):** MH stacioner kommunikációs rendszerek fejlődése. „De mi a helyzet Paks II-vel, a Mentésirányítással, vagy a Nemzeti Bankkal?”
11:00-11:20	**Juricsky Endre (Nemzeti Média- és Hírközlési Hatóság):** 2023. évi Rádiótávközlési Világértekezlet katonai vonatkozásai
11:20-11:40	**KÁVÉSZÜNET**
Levezető elnök: **Dr. Tóth András** **Plenáris ülés II.**	
11:40-12:00	**Dr. Magyar Sándor (Nemzeti Közszolgálati Egyetem):** Miért fontos a felsővezetői információbiztonsági tudatosítás?
12:00-12:20	**Dr. Kucsera Erika (Nemzeti Közszolgálati Egyetem):** Kiberbiztonság aktualitásai eseménykezelési, sérülékenységvizsgálati kitekintéssel
12:20-12:40	**Répás József (Nemzeti Közszolgálati Egyetem):** Network Forensics módszertan alkalmazásának vizsgálata magas automatizáltságú járművek szakértői vizsgálatában
12:40-13:00	**Dr. Kassai Károly (Honvédelmi Minisztérium):** A kibertér keretrendszerének stratégiai szintű változásai, fontosabb hatások
13:00-14:00	**EBÉD**
Levezető elnök: **Dr. Jobbágy Szabolcs** **Plenáris ülés III.**	
14:00-14:20	**Oláh István (ÓE, Biztonságtudományi Doktori Iskola):** Hogyan érvényesülnek az információbiztonsági kontrollok egy publikus felhőben
14:20-14:40	**Busa Attila (ÓE, Biztonságtudományi Doktori Iskola):** Az egyes hacker generációk támadási szokásai és aktuális támadási trendek fejlődése a 2000-es évektől napjainkig
14:40-15:00	**Balogh Péter (NKE, Hadtudományi Doktori Iskola):** Az infokommunikációs szférát célzó műveletek a kibertérben - Összetett mintázatok az orosz-ukrán háború esetében
15:00-15:20	**Kiss Adrienn (NKE, Katonai Műszaki Doktori Iskola):** Az orosz-ukrán háború egyes kiberbiztonsági tanulságai az energiabiztonság aspektusából
15:20-15:30	**A KONFERENCIA ZÁRÁSA**

Knerli Attila: Komplex gyors telepítésű megoldások minden helyzetre

Számos olyan helyzet van, amikor a hagyományos megoldások alkalmazása sok időt és energiát igényel. Cégcsoportunk által ajánlott modern eszközök segítségével a megoldásokra lehet fókuszálni, igényeknek megfelelően teljes rendszer is kialakítható, de egyedileg is felhasználhatók az eszközök.

Rolatube árbócrendszerek

A ROLATUBE árbóc speciális, bi-kompozit alapú anyagból készült könnyű szerkezetű eszköz, mely tekercselt állapotban szállítható, kigöngyölt állapotában pedig merev csőhengerré alakítható. Alacsony súly, gyorsan összeállítható stabil, merev szerkezet jellemzi, ami 15 éve bizonyítottan megfelel mind a modern katonai, mind a civil felhasználói követelményeknek. A kompozit szerkezetbe

további technológiák is integrálhatók (pl. nagynyereségű dipólus antennák).

Norlense gyorstelepítésű sátor

A NorLense, norvég fegyveres erőkkel és polgári védelemmel közösen kifejlesztett nagynyomású levegővel felfújt merevítő rendszerű katonai sátrak teljes körű infrastruktúra megoldást kínálnak extrém körülmények között is. A folyamatos felhasználói visszajelzéseken alapuló fejlesztések eredménye a tartós, hatékony, felhasználóbarát, egyedi igényekre szabható és gyorsan telepíthető infrastruktúra, a SWIFT rendszer, amely széleskörűen használható katonai, rendőri, katasztrófavédelmi és egészségügyi feladatok ellátására is. Könnyű, nagyon gyors felállítást és leszerelést biztosít, minimálisan kiképzett személyzet is üzemeltetheti.

Mobil napelemes rendszer

A mobil napelemes rendszer lehetővé teszi, hogy ott termeljen villamos energiát, ahol arra szükség van, és ahol ez megéri. Az innovatív és mobil napelemes konténer 196 darab, legfeljebb 130 kWp névleges teljesítményű PV-modult tartalmaz, és megfelelő energiatároló rendszerekkel bővíthető. A könnyű, környezetbarát alumínium sínrendszer mobil megoldást garantál gyors rendelkezésre állással.

Összefoglalás

Az ismertetett rendszerek nagy előnyt biztosítanak azoknál a szervezeteknél, ahol a gyorsaság, és a felhasználó személyzet létszáma döntő fontosságú. A termékek kiegészítik egymást, együttesen alkalmazhatók a felhasználó szervezeteken belül.

Felhasznált irodalom

www.rolatube.com
www.norlense.no

ROLATUBE ÁRBOCRENDSZEREK

ROLATUBE TECHNOLOGY

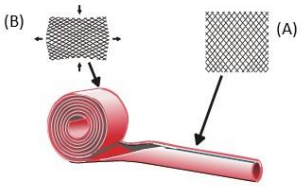
SCORPIO®

Rolatube: A technológia

Technikai neve – **"Bi-stable Reeled Composite"(Bi-stabil tekercselt kompozit)** – röviden "**BRC**"

- **Stabil** mind göngyölt, mind kiterjesztett állapotban.
- **Kis tárolási/szállítási térfogatúvá** göngyölhető.
- **Alacsony súly** a kompozit anyagnak köszönhetően.

- A kompozit szerkezetbe további technológiák is integrálhatók.
- **Gyors telepíthetőség** minimális személyzet alkalmazásával.



Rolatube: Az árbocrendszer piacai

- Az első célpont a védelmi piac volt, mivel nyilvánvaló előnyökkel jár a végfelhasználók számára
- Jól illeszkedik a jelenlegi katonai elvárásokhoz, mely a rendkívül mozgékony, kiváló kommunikációs és technológiai eszközökkel felszerelt harci erőket igényel

Rolatube: Áttekintés

System Group	Product Name	Description	Max Top Load	System Weight	Military Range	Civilian Range
System 100		101mm (4") diameter masts, integrated into a Rolacage.				
	System 100 8m	Mast of 8m (26.2') height, 101mm (4") diameter	15kg (33lb)	23kg (50lb)	Black	n/a
	System 100 10m	Mast of 10m (32.8') height, 101mm (4") diameter	12kg (26lb)	25kg (55lb)	Black	n/a
System 75		Mast systems using tubes of 76mm (3") diameter; single systems use one tube, double systems use two tubes, one inside the other, to provide additional strength.				
	System 75 3m single	Mast of 3m (9.8') height, 76mm (3") diameter	11kg (24lb)	4kg (8lb)	Black/Multicams	n/a
	System 75 4m single	Mast of 4m (13.1') height, 76mm (3") diameter	7kg (15lb)	4.5kg (9.9lb)	Black/Multicams	n/a
	System 75 5m single	Mast of 5m (16.4') height, 76mm (3") diameter	5kg (11lb)	5.25kg (11.5lb)	Black/Multicams	Black/blue/orange
	System 75 7m single	Mast of 7m (22.9') height, 76mm (3") diameter	2kg (4lb)	8.75kg (19lb)	Black/Multicams	Black/blue/orange
	System 75 2m double	Two masts of 2m (6.6') height, 76mm (3") diameter	25kg (55lb)	5kg (11lb)	Black/Multicams	n/a
	System 75 3m double	Two masts of 3m (9.8') height, 76mm (3") diameter	23kg (50lb)	6.5kg (14lb)	Black/Multicams	n/a
	System 75 4m double	Two masts of 4m (13.1') height, 76mm (3") diameter	20kg (44lb)	9kg (19lb)	Black/Multicams	n/a
	System 75 5m double	Two masts of 5m (16.4') height, 76mm (3") diameter	15kg (33lb)	10kg (22lb)	Black/Multicams	Black/blue/orange
	System 75 7m double	Two masts of 7m (22.9') height, 76mm (3") diameter	5kg (11lb)	14kg (30lb)	Black/Multicams	Black/blue/orange
System 50		Mast and tripod systems using tubes of 51mm (2") diameter.				
	System 50 2m	Mast of 2m (6.6') height, 51mm (2") diameter	10kg (22lb)	2.2kg (4.8lb)	Black/Multicams	n/a
	System 50 3m	Mast of 3m (9.8') height, 51mm (2") diameter	7kg (15lb)	2.6kg (5.7lb)	Black/Multicams	Black/blue/orange
	System 50 4m	Mast of 4m (13.1') height, 51mm (2") diameter	3kg (6lb)	3kg (6.6lb)	Black/Multicams	Black
	System 50 Tripod 1m	Tripod with legs of 1m (3.3') length, 51mm (2") diameter	30kg (66lb)	4kg (8lb)	Black/Multicams	Black/blue/orange
	System 50 Tripod 2m	Tripod with legs of 2m (6.6') length, 51mm (2") diameter	20kg (44lb)	5.3kg (11.6lb)	Black/Multicams	Black/blue/orange
	System 50 Tripod 3m	Tripod with legs of 3m (9.8') length, 51mm (2") diameter	10kg (22lb)	6kg (13.2lb)	Black/Multicams	Black/blue/orange
System IAM		Integrated Antenna Mast systems in UHF, VHF and DB.				
	System IAM 7m IAM-D	7m (22.9') 76mm (3") Integrated Antenna Mast @ VHF 30-88MHz & UHF 225-512MHz		7.9kg (17.4lb)	Black/Multicams	n/a
	System IAM 7m IAM-U	7m (22.9') 76mm (3") Integrated Antenna Mast @ UHF 225-512MHz		7.6kg (16.7lb)	Black/Multicams	n/a
	System IAM 7m IAM-V	7m (22.9') 76mm (3") Integrated Antenna Mast @ VHF 30-88MHz		7.6kg (16.7lb)	Black/Multicams	n/a
	System IAM 7m 'RESQ'	7m (22.9') 76mm (3") Integrated Antenna Mast @ VHF 136-175MHz		3.2kg (4.8lb)	n/a	Black/blue/orange
	System IAM 3.5m 'SQUAD'	3.5m (11.5') 51mm (2") Integrated Antenna Mast @ VHF 30-300MHz		2.2kg (4.8lb)	Black/Multicams	n/a
	System IAM 3.5m 'TEAM'	3.5m (11.5') 51mm (2") Integrated Antenna Mast @ 136-470MHz		2.2kg (4.8lb)	Black/Multicams	n/a
	System IAM 3.5m 'RESQ'	3.5m (11.5') 51mm (2") Integrated Antenna Mast @ VHF 136-175MHz		2.2kg (4.8lb)	n/a	Black/blue/orange

Rolatube: Az árbocrendszer

Páratlan előnyei:
- Könnyű súly
- kompakt
- Könnyű és gyors telepítés és helyreállítás

Az integrált antenna tartó rendszer egy teljesen új, forradalmi technológiát kínál a kezelő személyzet számára, egy úgynevezett „Plug & Play” megoldást.

"Gyorsabb, könnyebb, kisebb ... és jobb RF teljesítmény."

Rolatube: Az árbocrendszer

50-es és 75-ös árbocrendszer
- 50mm (2”) és 75mm (3”) átmérő
- 2m (6.6’) to 7m (22.9’)közötti hosszúságok
- Dupla csöves árbocrendszerek a nagyobb terhelhetőséghez
- A rendszer súlya: 2.2kg (4.8lb)

Rolatube: Az árbocrendszer

100-as árbocrendszer

- 8m (26.2’) és 10m (32.8’) változat
- Nagyobb felső terhelhetőség a
- nagyobb magasságban

Mast / Rolacage Systems	Maximum Top Load[1]	System Weight
System 100 8m (26.2')	15kg (33lb)	23.9kg (52.6lb)
System 100 10m (32.8')	12kg (26.4lb)	25.1kg (55.3lb)

1 Maximum weight only. Sail area should be discussed with Rolatube technical representative.




Rolatube: Integrált antenna tartó rendszerek

IAM rendszer

- Nagy nyereségű dipólus antenna mely teljesen az árboc kompozitba van integrálva.
- Egyedülálló ‘Plug & Play’ megoldás



Rolatube: Tripodok

30-as rendszer- Kompakt Taktikai Tripod rendszer

Kisebb méretű, mint bármely hasonló hagyományos változat

- MIL STD 810G szabványnak megfelelő
- Az árbócrendszer súlya 2,84 kg, de akár 40 kg-os felső terhelést is elbír.

Rolatube: Tripodok

50-es rendszer- Tripod rendszerek

Önálló termékként is használható érzékelők vagy kamerák állványzataként…

… vagy árbocok kiegészítő tartóállványaként, lehetővé téve a könnyű, stabil rögzítést nyugodt körülmények között feszítőkötelek vagy talajhoz rögzítés nélkül, állványként.

Rolatube: Gépjármű megoldások

- A Rolatube árbocrendszerek előnyei felbecsülhetetlen értékűnek bizonyulnak a taktikai járművek számára, ahol a helykihasználtság nagyon jelentős szempont
- Telepíthető közvetlen a gépjárműre, vagy a gépjárműbe
- A Rolatube árbocrendszerek segítségével hely- és súlymegtakarítást, és ezáltal megnövelt kényelmet és rugalmasságot érhetünk el

Rolatube: Kiegészítők

A Rolatube mint megoldás....

Oldalsó tartó a Cambium mikrohullámú antennához a 75-ös kettős rendszerekhez.

Cisco és Radwin antennához is elérhető.

Tripod adapterek az árboc állványhoz történő csatlakoztatásához.

A 25cm (10”) csap teszi lehetővé az antennák felszerelését a Rolatube rendszerek tetejére.

1.01m (40”) T-Bar kettős antenna tartó szerelvény

Szűkítő készlet 24mm (0.9”) és 17mm (0.6”)

Az egyedi szerelési segédeszközök a szállítás részét képezik.

Rolatube: Kiegészítők

Kiegészítő rendszerek a még könnyebb és gyorsabb telepítés érdekében...

Rolacage a 75-ös egyárbocos rendszerekhez kifejlesztve. Biztosítja a gyors telepítést, és állítható magasságot tesz lehetővé.

Central Guy Control (CGC) a szükséges kezelő személyzet csökkentése érdekében.

NORLENSE GYORSTELEPÍTÉSŰ SÁTOR

NorLense SHELTER SOLUTIONS

SCORPIO

Norlense: a kezdetek

A NorLense a világ egyik vezető vállalata az olajszennyezéssel kapcsolatos vészhelyzeti berendezések fejlesztése és gyártása terén. A termékeket a zord időjárási körülményekre fejlesztették ki, és rugalmas, tartós anyagokból, valamint innovatív technológiával készülnek.

Norlense: Nagynyomású felfújható merevítőjű sátor

Az új innováció alkalmazása gyorsan telepíthető sátrakba

- Az első sátort a norvég polgári védelemnek szállították 2001-ben.

Norlense: Nagynyomású felfújható merevítőjű sátor

Norlense: Nagynyomású felfújható merevítőjű sátor

SWIFT Sátor Rendszer - Telepítés

- Könnyű fel- és leszerelés, 2 személy által.
- Minimális képzéssel, nem műszaki szakemberek is működtethetik.

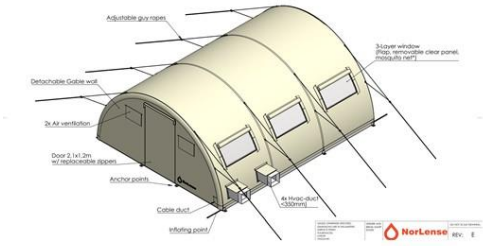





5-15 perc múlva kész

Norlense: Nagynyomású felfújható merevítőjű sátor

NorLense SWIFT sátrak



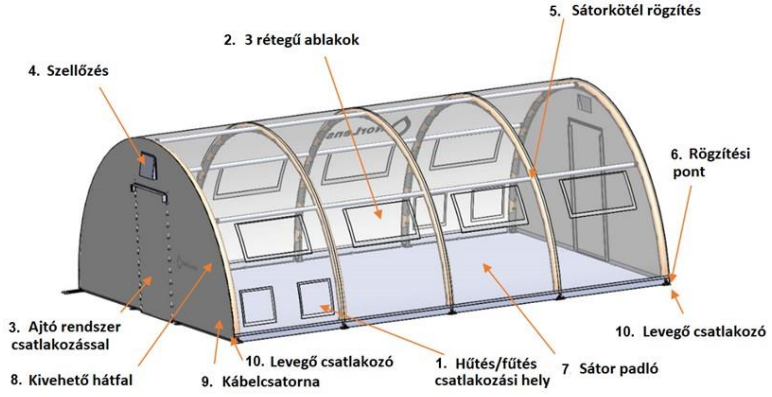
Szélesség:	3 méter	4 méter	5 méter	6 méter	8 méter	10 méter
Magasság:	2,1 m	2,4 m	2,5 m	3 m	4 m	4,65 m
Ø Légsugár szerkezet:	Ø75 mm	Ø102 mm	Ø 102 mm	Ø 125 mm	Ø 125 mm	Ø 150 mm
W x L (m)	3 x 2,5	4 x 4	5 x 4	6 x 6	8 x 6	10 x 6
	3 x 4	4 x 6	5 x 6	6 x 8	8 x 8	10 x 12,5*
			5 x 8	6 x 10	8 x 10	
			5 x 10	6 x 12	8 x 12,5*	
			5 x 5 Csatlakozó	6 x 6 Csatlakozó		

Műszaki jellemzők*:

- Egyrészes sátor egypontos felfújással és integrált padlóval
- Szélállóság: 120-145km/h
- Hóterhelés: 30 - 50 kg/m² (a sátor méretétől függően)
- Hő- és hidegállóság: - 45°C / + 70°C
- Nagynyomású légívek a sátor szerkezetében és hosszúságában
- Üzemi nyomás: 6-8 bar
- Légszerkezeti elemek közötti zárószelepek
- Cserélhető légszerkezeti elemek
- UV-álló, vízálló és lángálló PVC-ből készült.
- Felfújási idő) 10-30 perc a levegőforrástól függően
- A szerkezet 2,5 bar elérésekor magától megáll (5-15 perc)
- Felfújás után leválasztható levegőforrás - Nincs szükség állandó levegőellátásra
- A SWIFT sátrak számos konfigurációs lehetőséggel rendelkeznek az ügyfelek igényei szerint:
  - Az ajtók száma és mérete
  - Az ablakok száma és mérete
  - Kivehető/rögzített végfalak
  - Kivehető padló

Norlense: Nagynyomású felfújható merevítőjű sátor

SWIFT Sátor rendszer - modularitás és rugalmasság



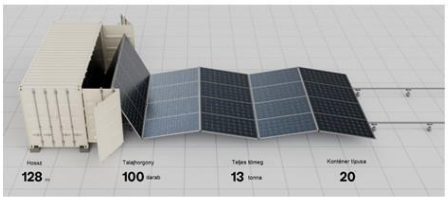

Norlense: Nagynyomású felfújható merevítőjű sátor
Miért válassza a SWIFT-et?
Merev vázas sátrak
Előnyök:
1: Erős tartószerkezet, amely kevés karbantartást igényel
2: Képes ellenállni a zord környezetnek
3: Kis tartószerkezet, amely kevés helyet foglal a sátorban
4: Felállításkor kevés felügyeletre van szükség.
Hátrányok:
1: Nehézkes logisztika
2: Több alkatrész/komponens, amelyet össze kell rakni.
3: Magas személyi és időigény a felállításhoz
4: A laza alkatrészek elvesznek, és utánpótlásra van szükségük.
NorLense SWIFT nagynyomású felfújható sátrak
Előnyök:
1: Erős szerkezet cserélhető alkatrészekkel
2: Nagyon alacsony karbantartási igény
2: Zord környezetnek való ellenállás, nagy hó- és szélterheléssel szembeni ellenállás.
3: Kis tartószerkezet, amely kevés helyet foglal a sátorban
4: Felállítás után nincs szükség levegőellátásra
5: Egyszerű logisztika
6: Gyors felállítási idő minimális személyzettel
7: Egy darabból álló integrált megoldás, nincsenek laza alkatrészek
8: Könnyű rendszer, kevés betanítás szükséges
=
Nagy teljesítmény és hatékonyság, hosszú élettartam és alacsony életciklusköltségek
Alacsony nyomású felfújható sátrak
Előnyök:
1: Egyszerű logisztika
2: Gyors felállítási idő kevés személyzettel
3: Egyszerű rendszer, kevés betanítás szükséges
Hátrányok:
1: Alacsony teljesítmény, gyenge hó- és szélterheléssel szembeni ellenállás
2: Hőmérséklet- és nyomásváltozások hatására
3: Gyakran állandó levegőellátást igényel
4: A szerkezeti keret könnyen kilyukad és gyakran karbantartásra szorul
5: Nagy pneumatikus szerkezet, kevesebb hely áll rendelkezésre a sátorban

SOLARFOLD
MOBIL NAPELEMES RENDSZER
Solarfold
MOBILE SOLAR CONTAINER
SCORPIO

Solarfold: Mobil napelemes rendszer

MOBIL NAPERŐMŰVES KONTÉNER

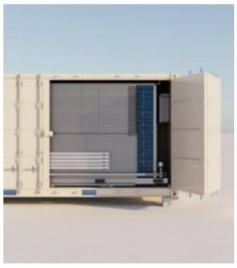
Az Off-Grid mobil konténer egy napelemes konténerből áll, amely egy megfelelő kiegészítő tárolóval kombinálva nem csatlakozik a közhálózathoz, és teljesen önellátóan működik. A rendszer akár 80 kW kisütési teljesítményt is biztosít, és akkor is ellátja a csatlakoztatott fogyasztókat, amikor az időjárási körülmények ezt nem teszik lehetővé.

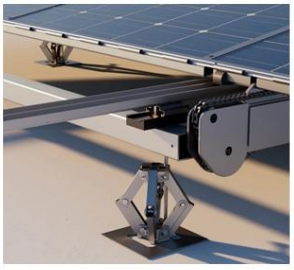


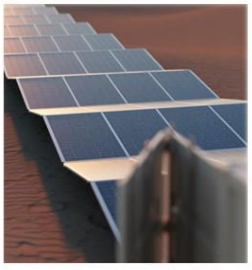
Annak érdekében, hogy a megtermelt energiát éjszaka is fel lehessen használni, ajánlott a nap konténert egy energiatárolóval bővíteni.

Solarfold: Mobil napelemes rendszer

- A Solarfold napelemes konténer bárhol használható, rugalmas és könnyű alépítmény jellemzi
- A félautomata elektromos meghajtás a mobil napelemes rendszert kb. 123 méter hosszúságban gyorsan és erőfeszítés nélkül, a lehető legrövidebb idő alatt üzemkész állapotba hozza
- Az összecsukható PV-generátorhoz nincs szükség kábelárkokra vagy nehézgépekre, és a terepfelület tömörítésére sem
- A Solarfold konténer a legapróbb részletekig lefedett plug-and-play rendszer számos alkalmazási területre







Solarfold: Mobil napelemes rendszer

MOBIL KONTÉNER ENERGIATÁROLÓ RENDSZER

- Biztosítja a megbízható, szünetmentes és minőségi áramellátás elérhetőségét
- Optimalizált költségek a szükséges generátorok számának csökkentése révén
- Egyenletes áramminőség a villamosenergia-rendszerek feszültség- és frekvenciaingadozással szembeni stabilizálása révén
- Biztonságos és fenntartható energiamix elérése az energiahatékonysággal együtt
- Robusztus környezetre és szélsőséges időjárási körülményekre tervezve, a szabvány konténerek szállítására kialakított gépjárművekkel a szállítási, telepítési feladatok gyorsan végrehajthatóak

Solarfold: Mobil napelemes rendszer

MOBIL KONTÉNER ENERGIATÁROLÓ RENDSZER

Az energia tároló konténer egy moduláris, rugalmas és költséghatékony MWh – méretű akkumulátoros rendszer. Több egység párhuzamosan csatlakoztatható.

- Költséghatékony, hosszú élettartam
- Folyékony hűtési technológia a cellahőmérsékletekhez az optimális üzemi hőmérsékleten belüli tartományban
- IP65 védettségű akkumulátorcsomag, por, nedvesség, és kondenzáció behatolással szemben
- Többlépcsős hőátadási technológia, mely hatékonyan megakadályozza az akkumulátor túlhevülését és javítja a biztonságot
- Többszintű tűzérzékelés, korai hőérzékelés a cellák túlmelegedésének megakadályozására
- Minden belső alkatrész (beleértve az akkumulátorokat is) a gyárban összeszerelve, ami csökkenti a helyszíni telepítési költségeket


SCORPIO
Köszönjük a figyelmet!
Forgalmazza:
Scorpio Kereskedelmi és Szolgáltató Kft.
Székhely: 1137 Budapest, Pomázi út 15.
Levelezési cím: 1137 Budapest, Pomázi út 15.
www.scorpio.hu
+36 (1) 320-2100
info@scorpio.hu
www.facebook.com/scorpiokft

Kucsera Erika: Kiberbiztonság aktualitásai eseménykezelési, sérülékenységvizsgálati kitekintéssel

Napjainkban számos befolyásoló tényező alakítja a kibertér aktuális fenyegetettségeit és ezzel együtt a védekezési stratégiákat, módokat. A sikeres védekezést támogatja a jól szervezett sérülékenységvizsgálati metodika, valamint az aktuális támadási trendekre felkészült eseménykezelési rendszer. Ezen szakterületek folyamatos fejlődése szilárd alapja a hatékony kibervédelmi tevékenységnek a honvédelmi ágazatban.

Befolyásoló tényezők

A kibervédelmi tevékenységek fókuszát, módszereit számos tényező befolyásolja.

A technológiai fejlődés hatásánál példaként kiemelhető az elmúlt években számos szakterületen tért nyerő és alkalmazott mesterséges intelligencia védelmi és támadó célú használata, a drónhasználat használatának széleskörű elterjedése, amely új kihívások elé állítja a kiberszakterületet.

A nemzetközi helyzet, az orosz-ukrán háború, a konfliktusok, az érdekek változása befolyásolja a kibertérben zajló műveletek, tevékenységek orientáltságát és számos kiberszakterületi támadási és védelmi tapasztalatot nyújt, melynek fenyegetettségelemző feldolgozása segíti a szakmai fejlődést az eseménykezelési és más védekezési szakterületeken.

Az orosz-ukrán háború kibertéri tapasztalatai sokrétűek voltak, melyben hangsúlyosan az információmanipuláció oly széles tárházát vonultatták fel, amely a védelmi irányvonalak kiegészítésére, újra strukturálására motiválta a kibertér szereplőit. A háború során tapasztalt támadási módokból az elosztott túlterheléses támadások, a weboldal tartalom megmásítása, az információs műveletek, a dezinformációs kampányok, a kártékony kódok terjesztése volt eddig jellemző, melyek célja a kormányzat tekintélyének aláásása, reputáció-rombolás, a kommunikáció és információmegosztás ellehetetlenítése, a haderő reagálóképességének csökkentése, valamint a támogató országoknál történő zavarkeltés volt.

Támadók aktuális motivációja, módszerei eltérőek, lehetnek pénzügyi-haszonszerzési, ideológiai, politikai motivációjúak. A honvédelmi ágazat ügyfélkörének sokszínűsége okán a támadások motivációjának különböző típusaira kell felkészülnie a védekező oldalnak.

A nemzetközi szabályzó környezet hatással van a nemzeti szabályzó környezetre. A jelenleg zajló NIS2 [1] jogharmonizációs folyamat végén a szakterületi követelmények jelentősen változni fognak, melyek átvezetése, alkalmazása kihívások elé állítja majd a kiberszakterület képviselőit. A mesterséges intelligencia részletes

[1] NIS2: Network and Information Systems Directive

szabályzása[2] várhatóan újabb szabályzási és eljárásrendkialakítási feladatot jelent majd a végrehajtó szakterületeknek is.

Tapasztalatok

Napjainkban nyílt forrásokból, információmegosztó platformokból, célzottan kialakított együttműködésekből hihetetlen mennyiségű fenyegetettségi adat gyűjthető össze folyamatosan. Napjainkban a kihívást emiatt az okozza, hogy megfelelő fókuszáltságú és mennyiségű információt gyűjtsünk és osszunk meg a kibertéri szereplőkkel, mivel így tudjuk elérni azt a célt, hogy hatékonyan reagáljanak erre. Ehhez fontos az ügyfélkör érdekeire, technológiájára, a fent felsorolt hatások szerinti aktuális kategorizálására szűrni az adatokat és ezeket a kiber- és IT szakterület által hasznosítható, feldolgozható módon megosztani. A honvédelmi ágazatban ennek érdekében célzott értesítések, riasztások, fenyegetettségi információk kerülnek kiküldésre.

A felhasználók biztonságtudatosságának folyamatos fejlesztése kiemelten fontos, tekintettel arra, hogy a kibertámadások jelentős részének sikerességét a humánsebezhetőség kihasználása teszi lehetővé. Eseménykezelési tapasztalatok alapján figyelemre méltó, hogy a magas biztonságtudatosságú felhasználó a korai észlelés fontos láncszeme lehet. Napjainkban megszaporodott a korai

[2] Az Európai Bizottság még 2021. évben tett javaslatot az első mesterséges intelligencia unió szabályozási keretrendszerére. Az Európai Parlament 2023 júniusában elfogadta Mesterséges Intelligencia Törvényt.

szakaszban bejelentés alapján felfedezett, azonban védelmi eszközparkok adatbázisaiban adott időszakban még nem szereplő és így automatikusan ki nem szűrt, a felhasználói fiókba így beérkező káros tartalmú levelek száma. Az ilyen típusú fenyegetettségekre, támadási kísérletekre történő gyors reagálás egyik leghatékonyabb forrása jelenleg a korai felhasználói észlelés, bejelentés. A jól felkészített felhasználó a káros tartalmú levelet késlekedés nélkül jelentve és rendelkezésre bocsájtva lehetővé teszi a káros tevékenység teljes lefutásának korai megismerését és ennek korlátázására, nyomainak keresésére lépések tételét, nemcsak az adott szervezetnél, hanem a teljes honvédelmi ágazatban is, még abban az időszakban, amikor ezen támadás technikailag automatizáltan még nem kerül kiszűrésre.

2023. év további tapasztalata, hogy a közép és nagyvállalati szinten a kiberbiztonság terén jelenleg is a mélységi védelem [3] a legelterjedtebb stratégia, azonban ez a tapasztalatok alapján magában nem elégséges a teljes körű védelemhez. A közép és nagyvállalatokat célzó felmérés [4] alapján a mélységi védekezés stratégiájának használata ellenére a válaszadók elismerték, hogy az elmúlt két évben közel 90%-át, az elmúlt 12 hónapban 45%-át érte kibertámadás.

[3] Defense In Depth (DiD)

[4] https://pentera.io/blog/the-state-of-pentesting-2023-global-trends-in-cybersecurity/

Eseménykezelési és sérülékenységvizsgálati tapasztalatok

Az eseménykezelési trendeknél a főbb támadási vektorok hatásuk, előfordulások alapján továbbra is a káros taralmú levelek, kártékony kódok, a Social engineering, az adatok elleni fenyegetések, a rendelkezésre állás elleni fenyegetések, az információmanipuláció és -zavarás, valamint az ellátási lánc elleni támadások voltak. A támadások egyre szofisztikáltabbak, mind nagyobb tért nyer a LOTL[5] támadási technika.

A sérülékenységvizsgálat a biztonsági események megelőzésének leghatékonyabb módja, a szervezet elektronikus információs rendszereinek, weboldalainak védelmét erősítve. Az utóbbi év tapasztalata az, hogy már nemcsak a jogszabályi megfelelés a legfőbb motivációja a sérülékenységvizsgálatoknak, hanem a szervezetek vezetőinek, elektronikus információs rendszer biztonságáért felelős személy azon szakmai motivációja, hogy a védelmi vonalaikat a lehető leghatékonyabban megerősítsék. Ezen folyamat viszont maga után vonja az igények számának jelentős növekedését, a szakterület terheltségének növekedését.

A sérülékenységvizsgálati-, eseménykezelési- és fenyegetettségelemző terület hatékony együttműködése biztosítja a már korábban leírt célzott figyelmeztetések, riasztások hatékony, célzott kiválasztását, ügyfélkörhöz juttatását.

[5] LOTL: Living off the land támadási technika.

A honvédelmi ágazati sérülékenységvizsgálat jogszabályilag körülhatárolt, melyet saját magasan képzett szakállomány hajtaj végre.

Támadó csoportok viselkedésváltozása

Tapasztalat, hogy a támadói csoportok a más által alkalmazott új technikákat gyorsan másolni és alkalmazni kezdik. A fenyegető szereplők már nem statikus, kiszámítható támadási láncolatokat használnak, hanem dinamikus, gyorsan változó technikákra támaszkodnak. A támadó oldalnál megfigyelhető az egyre erőteljesebb iparági jellegű működés a támadó szolgáltatások piaci értékesítésénél. Új trendként figyelhető meg a különböző, egymással összekapcsolt Crime-as-a-Service -piacok, amelyek már támadási terveket kínálnak. Ennek során több részszolgáltatásban kapcsolnak össze káros tevékenységeket és kompletten értékesítik. Ezek detektálása és a valós támadó felderítése nehézséget jelent a kibervédelmi szakterület képviselőinek.

Összegzés

A hatékonyabb védelmi felkészülés fontos része a sérülékenységek mielőbbi kiküszöbölése, az aktuális fenyegetettségi helyzetkép ismerete, a védelmi elvek megfelelő fókuszáltságú alkalmazása, valamint a jól szervezett eseménykezelés. Fontos a célzott szakterületi együttműködés, mivel napjainkban a hagyományos támadási elvek mellett a feltörekvő technológiák jelentette fenyegetettségekre is készülni kell.

Felhasznált irodalom

271/2018. (XII. 20.) Korm. Rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól;
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról;
A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. Törvény;
6/2020. (IV. 16.) HM rendelet a honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságok meghatározásáról;
AC/35-D/2005-REV3 Management Directive on CIS Security;
ENISA threats landscape 2023 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, 2023.11.11.
https://pentera.io/blog/the-state-of-pentesting-2023-global-trends-in-cybersecurity/, 2023.11.11.

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Kiberbiztonság aktualitásai eseménykezelési, sérülékenységvizsgálati kitekintéssel

Dr. Kucsera Erika ezredes
(kucsera.erika@uni-nke.hu)

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

ÁTTEKINTÉS

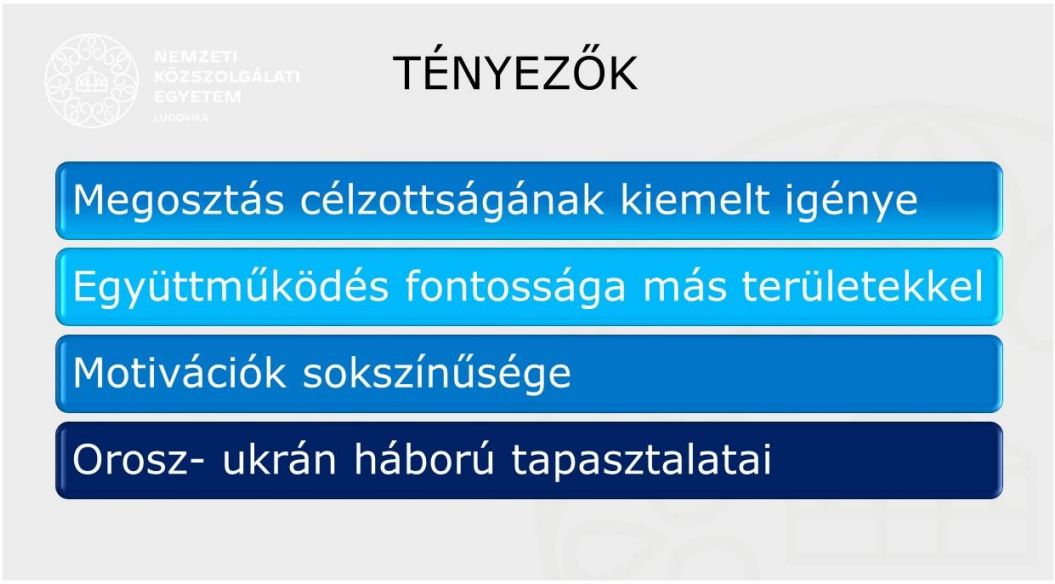
Befolyásoló tényezők

Fenyegetettségi trendek

Eseménykezelési tevékenység és tapasztalatai

Sérülékenységvizsgálat tapasztalatai


NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA
BEFOLYÁSOLÓ TÉNYEZŐK
Technológiai fejlődéshez kapcsolódó kihívások
Nemzetközi helyzet
Humánerő-forrás kihívások
Támadók aktuális motivációja, módszerei
Nemzetközi szabályzó környezet hatása
Nemzeti szabályzó környezet hatása


NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA
TÉNYEZŐK
Megosztás célzottságának kiemelt igénye
Együttműködés fontossága más területekkel
Motivációk sokszínűsége
Orosz- ukrán háború tapasztalatai

OROSZ-UKRÁN HÁBORÚ KIBERTÉRI TAPASZTALATAI

- Manipuláció
- Weboldal tartalom-módosítások
- Elosztott túlterheléses támadások
- Információs műveletek
- Dezinformációs kampányok
- Adathalász kampányok, kártékony kódok terjesztése

2023 ÉV TAPASZTALATAI

- Mélységi védelem (Defense In Depth) eredményességi kérdése
- Felhasználói tudatosság befolyása
- Honvédelmi ágazati fókuszált riasztás, tájékoztatás

ESEMÉNYKEZELÉSI TRENDEK VÁLTOZÁSA

- Malware
- Ransomware
- Social engineering
- Adatok elleni fenyegetések
- Rendelkezésre állás elleni fenyegetések
- Információmanipuláció és zavarás
- Ellátási lánc elleni támadások

TÁMADÓI OLDAL VÁLTOZÁSA

- Új támadó csoportok
- As-a-Service modell kiterjesztése--Crime-as-a-Service
- Támadó csoportok magatartásváltozása
- Iparág jellegű fejlődés felgyorsulása

SÉRÜLÉKENYSÉGVIZSGÁLAT

- Szigorúan szabályozott metodika
- Jogszabályi alapja szilárd
- Éves terv és külön elrendelés, igény alapján
- Feltárás, megoldási javaslat tétel, visszaellenőrzés
- Szervezet intézkedési terv kötelezettsége

SÉRÜLÉKENYSÉGVIZSGÁLAT AKTUALITÁSAI

Sérülékenységvizsgálat fontossága
Gyors hardver és szoftverháttér változás, sok aktuális sérülékenység
Nagy ágazati ügyfélkör
Megnövekedett igények
Riasztások, tájékoztatások aktualitásokkal támogatása

Tapasztalatok

- Sérülékenységek mielőbbi kiküszöbölésének fontossága
- Aktuális fenyegetettségi helyzetkép
- Destruktív mesterséges intelligencia használat vs. hagyományos támadási technikák
- Célzott szakterületi együttműködés fontossága

Felhasznált irodalom

271/2018. (XII. 20.) Korm. Rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól;

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról;

A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. Törvény;

6/2020. (IV. 16.) HM rendelet a honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságok meghatározásáról;

AC/35-D/2005-REV3 Management Directive on CIS Security;

ENISA threats landscape 2023 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, 2023.11.11.


NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA
KÖSZÖNÖM A FIGYELMET!
uni-nke.hu

Répás József: Network Forensics módszertan alkalmazásának vizsgálata magas automatizáltságú járművek szakértői vizsgálatában

A közúti közlekedés volumene, az infrastruktúra terheltsége, a közlekedési balesetek bár csökkenő tendenciájú, de továbbra is magas számai, a magas környezeti terhelés és a közlekedés nagy energiafelhasználása miatt fejlett közlekedési rendszerek tervezése és megvalósítása szükséges. Az Európa mozgásban – Fenntartható mobilitás Európában: biztonságos, összekapcsolt és tiszta közlekedés című program keretében olyan fejlesztési lehetőségekben látja a jövőt, mint a modern közlekedési rendszerek és az összekapcsolt és automatizált járművek széleskörű elterjedése. A közúti közlekedési járművekben egyre magasabb szintű vezetéstámogató rendszerek jelennek meg, az önvezető funkciók széleskörű elterjedése mind a polgári, mind a katonai felhasználásban megfigyelhetőek.

Modern közlekedési rendszerek

A modern, vagy intelligens közlekedési rendszerek (Intelligent Transport Systems - ITS) - melyek együttműködéssel, kooperatív intelligens közlekedési rendszerekként (Cooperative Intelligent Transport Systems – C-ITS) működni – alapja a kommunikáció, az összekapcsoltság. A rendszerek és rendszer elemek hálózati kapcsolatuk segítségével innovatív szolgáltatásokat nyújtanak, elősegítik a közlekedési hálózatok biztonságos, összehangolt

használatát, melyhez hozzájárul a jobb tájékoztatás is (EU, 2011), (EP, 2010).

Új kommunikációs megoldások szükségesek ezen innovatív megoldások támogatására, mind a járműveken belül, illetve azon kívül is. Az autóipar általánosan elfogadott főbb kommunikációs szabványai:

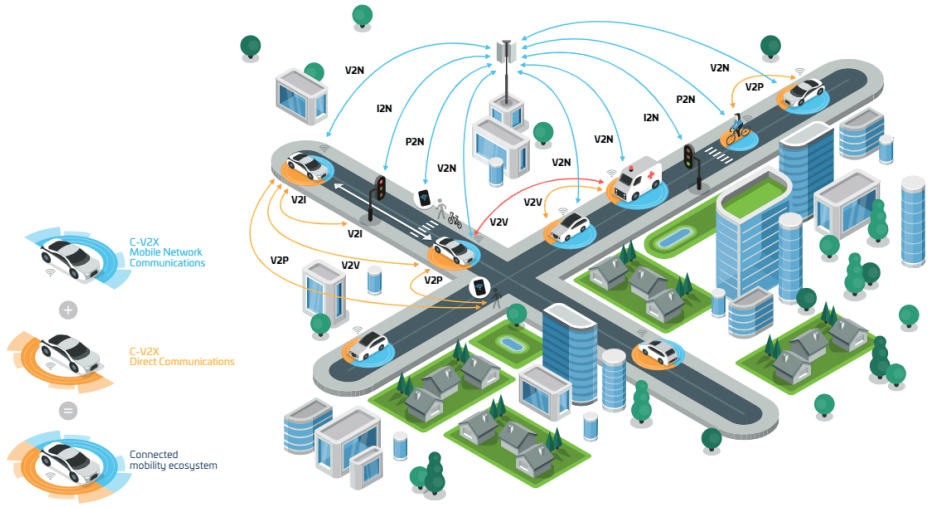
- CAN (Controller Area Network) protokoll,
- LIN (Local Interconnect Network),
- Flaxray,
- Automotive Ethernet,

lehetővé teszik az járműveken belüli nagy sebességű kommunikációt. A korábbi 10 Kbit/s-os sebességtől, napjainkra eljutottunk a gigabit/s-os nagyságrendig. A kommunikáció sebességének növekedési igényét a járművek kiterjedt érzékelő hálózata is indokolja. A kamerákkal, lézer és radar szenzorokkal, ultrahang érzékelőkkel felszerelt járművek nagy adatmennyiséget generálnak annak érdekében, hogy a jármű minél pontosabban fel tudja mérni környezetét, lokalizálni tudja magát. Ez akkor lehetséges, ha a szenzorok információit a lehető leggyorsabban képesek vagyunk eljuttatni a feldolgozási helyükre. Ahhoz, hogy az járművekben növelhető legyen a biztonság és a teljesítmény, csökkenthető a környezeti terhelés és fokozható legyen a kényelem, az elektronikus vezérlőegységek (electronic control unit - ECU) közötti kommunikáció sebességének, az adatátvitel mennyiségének és megbízhatóságának növekednie kell. A fejlett vezérlő- és biztonsági rendszerek - amelyek több érzékelőt, aktuátort és

elektronikus vezérlőegységet egyesítenek - megkövetelik a pontos szinkronizációt és a magas teljesítményt. Ez az igény már meghaladja a CAN (Controller Area Network) által biztosított lehetőségeket. A gyártókkal, az eszközök beszállítóival és a végfelhasználókkal való együttműködés eredményeként a FlexRay szabvány olyan járműfedélzeti kommunikációs megoldásként jelent meg, amely megfelel ezeknek az új kihívásoknak melyek a modern és önvezető járművek támasztanak. Bár megoldja a jelenlegi csúcskategóriás és a jövőbeni általános járműhálózati kihívásokat, nem helyettesíti, váltja ki a másik két domináns járműfedélzeti szabványt.

A jármű működése és biztonsága szempontjából kritikus információk a Flexray és Automotive Ethernet protokollokon kerülnek átvitelre a hibatűrés és időkövetelmények miatt (Luett, 2021), (SZE, 2020), (NI, 2022).

A gyors és biztonságos kommunikáció igénye a járművön kívül is megjelenik. A járművek egymással, környezetükkel, pálya elemekkel egyaránt kapcsolatot kell (fognak) tartani. A jármű- és minden lehetséges dolog közötti együttműködés, kommunikáció (Vehicle to Everything - V2X) lehetővé teszi, a járművek és az infrastrukturális rendszerek, összekapcsolását, megvalósítva a közlekedés kooperativitását (1. ábra). A V2X kommunikáció célja a jövő teljesen önvezető járműveinek kiszolgálása (Petkovics & Szabó, 2020), (Tokody et. al., 2018).



1. ábra Kooperatív intelligens közlekedési rendszer résztvevőinek V2X kommunikációi (5GAA, 2022)

A V2X-hez hasonló célok megvalósítására hozták létre a DSRC - Dedicated short-range communication szabványt, alacsony késleltetése, nagy megbízhatóság miatt biztonságos és támogatja az interoperabilitást, szélsőséges időjárási körülmények között is alkalmazható, azonban széleskörű Európai elterjedése a V2X térnyerése miatt nem várható.

Network forensics és a modern közlekedési járművek

A Network forensics, a hálózati kommunikáció forenzikus/szakértői vizsgálata, a digitális forenzikus vizsgálatok egyik területe, amely kommunikációs hálózatok mozgásban lévő adatainak (data in motion) azonosításához, vizsgálatához, értékeléséhez és elemzéséhez, illékony és dinamikus információkkal foglalkozik. A vizsgálatok célja a hálózaton keresztül átvitt adatok megértése és a

végpontok felé irányuló, vagy közötti interakciók és tevékenységek feltárása. A hálózati forgalom eseményeinek, naplóinak és kommunikációs mintáinak monitorozásával és elemzésével foglalkozik, annak érdekében, hogy biztosítsa a vizsgálati célok eléréséhez szükséges információkat.

Járművek esetén is szükség lehet a kommunikációs csatorna vizsgálatára, ami a network forensics eszközrendszerével történhet meg. Például olyan esetekben amikor a jármű a támadás célpontja, vagy eszköz a bűncselekmény elvégzéséhez, valamint tartalmazza az bizonyítékot az adott vizsgálathoz. Ilyen lehet a feltételezett visszaélés, jogosult vagy jogosulatlan hozzáférés, manipuláció, visszaélés, megtörtént esemény vizsgálata vagy terrorcselekmény, titkos információgyűjtés stb. a kiberműveletek, incidenskezelés, igazságszolgáltatás, csalásmegelőzés, hálózati teljesítmény optimalizálása vagy kutatás és fejlesztés érdekében. A példákból látható, hogy a hálózati kommunikáció szakértői vizsgálata jellemzően különböző hatóságok, katonai és állami szervezetek, vállalatok, egyetemek, kutató és kiberbiztonsági szervezetek feladata lehet.

Jelen tanulmány célja a hálózati forenzikus vizsgálatok főbb lépéseinek értékelése a modern közúti közlekedési járművek utólagos szakértői vizsgálatával kapcsolatban. Az információszerzés, mint kezdeti lépés mind a járművek, mind a hálózatok szakértői vizsgálata szempontjából fontos lépés. Ennek keretében a vizsgálati kérdésekhez kapcsolódóan előzetes információk gyűjtése történik a

vizsgálandó eseményről, a vizsgálati tárgyról, a környezetről. Ide tartozhatnak például az időpontok, érintettek (pl.: járművezető), a jármű típusa, kommunikációs csatornák. Az előzetes információk alapján lehetőség nyílik az adott vizsgálat megtervezésére, a vizsgálati stratégia kialakítására. Tervezési szempontok közé tartoznak a vizsgálati célok és kérdések, a nyomok forrása és megbízhatósága, az idővonal (nyomok összegyűjtési sorrendjének meghatározása) és a szükséges technikák, taktikák, módszerek és eszközök is.

Az adatgyűjtés lépésben két eljárást követnek a hálózatok vizsgálata során:

- Catch it as you can, - a teljes hálózati forgalom rögzítése,
- Stop, look and listen – a gyanúsnak tűnő forgalom rögzítése.

Catch it as you can eljárás során a teljes forgalom rögzítése biztosítja, hogy ne maradjanak ki fontos hálózati események. A rögzített forgalom időbélyeggel és HASH értékkel kerül kiegészítésre. Ennek a megoldásnak mind az idő, mind a tárkapacitás igénye rendkívül nagy. A Stop, look and listen eljárás során az adatforgalomnak csak a monitorozása történik meg és azok a forgalmak kerülnek rögzítésre, amelyek valamilyen szempontból gyanúsnak tartanak és további vizsgálatuk szükséges (Soundarya, 2023). Járművek esetén jellemzően utólagos vizsgálatok kerülnek elvégzésre, ezért ezek a megoldások nem, vagy csak kevés esetben végezhetőek el. A forgalmi adatok mellett, járművek vizsgálata során nagyobb szerepet kapnak a belső és külső kommunikációért

felelős vezérlő egységek, gateway-ek és ezek naplóállományai. Az elemzési fázisban a rögzített nyomok vizsgálata történik. Ide tartozik a hálózati keretek azonosítása és egymástól való elkülönítése, valamint a keretek belső szerkezetének és tartalmának feltárása, az adatok értelmezése. „A protokoll információk dekódolása, a hálózati protokoll hierarchia „visszafejtése” és az átvitt adatok […] összeállítása, a hálózati események időbeli sorrendjének rekonstruálása” (Illési, 2009). Az eredmények dokumentálása szakértői jelentés vagy szakvélemény formájában történik (Soundarya, 2023), (Illési, 2009), (Joshi 2016) (Répás, 2023), (Khan et. al., 2016), (Sudakar et. al., 2013), (Long, 2016), (Máté, 2018), (Kostadinov, 2020).

A modern járművek kommunikációjának szakértői vizsgálata több új és a Network forensics-ben is meglévő kihívással néz szembe. Az intelligens, napjainkban már mesterséges intelligenciával támogatott forenzikus eszközök, a speciális adatforrások és kommunikációs megoldások, a nagy sebességű adatátvitel, az hálózati kommunikációt lebonyolító eszközök/gateway-ek és ezek tárolt adatainak elérése, az adatokhoz, hozzáférési és eszköz azonosítókhoz való hozzáférés, vagy az adatok hitelességének, sértetlenségének biztosítása kihívást jelentenek a szakértőknek (Répás & Schmidt, 2023).

Összefoglalás

A magas automatizáltságú és egyre inkább önvezetővé váló járművek együttműködését a fejlett közlekedési rendszerekben a

gyors, megbízható és biztonságos kommunikáció teszi lehetővé. A járművek nem jogszerű és rendeltetésszerű használata, a folyamatos fejlesztési igények vagy egy baleset, incidens vizsgálata szükségessé teheti az új kommunikációs megoldások szakértői vizsgálatát. Mivel jelenleg nincs sztenderd eljárás, módszertan a modern járművek utólagos szakértői vizsgálatára, ezért a kutatásomban a digitális forenzik egyes területeit veszem górcső alá annak érdekében, hogy ezek egyes lépései, technikái alkalmazhatóak lesznek-e a járművek vizsgálata során, illetve mely lépések integrálhatóak a járművekhez készülő vizsgálati módszertanba. Jelen tanulmányban a Network forensics főbb lépései kerültek vizsgálatra a modern járművekhez kapcsolódóan és megállapítható, hogy a főbb vizsgálati lépések (pl.: adatgyűjtés, elemzés) alkalmazhatóak lesznek a járművek kommunikációjának vizsgálata során. Emellett megállapítható, hogy a vizsgálati kihívásokat is figyelembe véve, a Network forensics-ben használt vizsgálati stratégia lépés implementálása a készülő modern járművek szakértői vizsgálati módszertanába.

Köszönetnyilvánítás

A kutatás az Európai Unió támogatásával valósult meg, az RRF-2.3.1-21-2022-00004 azonosítójú, Mesterséges Intelligencia Nemzeti Laboratórium projekt keretében.

A szerzők külön szeretnének köszönetet mondani az Alverad Technology Focus Kft. Kutatás, fejlesztés és Innováció üzletágának a kutatási munkához nyújtott támogatásért.

Felhasznált irodalom

5G Automotive association, https://5gaa.org/content/uploads/2023/10/infographic-2023.png

AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2010/40/EU IRÁNYELVE (2010. július 7.) az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keretről, https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32010L0040

COM(2011) 144 Fehér Könyv - Útiterv az egységes európai közlekedési térség megvalósításához – Úton egy versenyképes és erőforrás-hatékony közlekedési rendszer felé, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0144:FIN:hu:PDF

Dimitar, K. (2020). Network forensics overview, https://resources.infosecinstitute.com/topics/digital-forensics/network-forensics-overview/

FlexRay Automotive Communication Bus Overview, https://www.ni.com/hu-hu/innovations/white-papers/06/flexray-automotive-communication-bus-overview.html

Illési, Zs. (2009). Számítógép hálózatok krimináltechnikai vizsgálata, Hadmérnök, IV évf. 4. szám.

Járműinformatika előadásvázlat (2020). http://www.sze.hu/~korosp/Jarmuinformatika_nappali/05%20-%20Jarmuinformatika%20FlexRay.pdf

Joshi R.C., Emmanuel, S. Pilli. (2016), Fundamentals of Network Forensics, Springer 2016. ISBN 978-1-4471-7297-0

Long, A. (2015)., What is FORENSICS? Why do we need Network Forensics?, https://slideplayer.com/slide/6938457/

Luett, M. (2021). How CAN-FD Light enables new car network architectures, Silica conference, 2021.10.20.

Máté, I. Zs. Informatikai rendszerek elleni támadások szakértõi vizsgálata – a digitális nyomok rögzítésének szerepe, http://real.mtak.hu/116025/1/MateIstvanZsoltBelugyiSzemle2018.evi7-8.szam36-54.pdf, DOI: 10.38146/BSZ.2018.7-8.3

Parate, S. Nirkhi, S. Nagpur S., Dharaskar R. (2013). Application of Network Forensics for Detection of Web Attack using Neural Network

Petkovics, Á. Szabó, Cs. A. Wippelhauser, A. Varga, N. Bokor, L. (2020). A V2X járműkommunikáció alapjai, Útügyi lapok 2020, 8. évfolyam, 14. szám, https://real.mtak.hu/117891/1/UL_14_01.pdf

Répás, J. Schmidt, M. (2023). Forensics tevékenységek kihívásai a modern közlekedési járművek fejlődésének tükrében, In: Gőcze, István; Padányi, József Húsz év a katonai műszaki tudományok szolgálatában : A katonai műszaki tudományok tudományág időszerű kérdései, aktuális tudományos kutatási eredményei -

Hallgatói kötet, Budapest, Magyarország : Ludovika Egyetemi Kiadó (2023) 295 p. pp. 181-194. , 14 p.

Répás, J. (2023). Definition of Forensic Methodologies for Autonomous Vehicles, HADMÉRNÖK 18 : 1 pp. 125-141. , 17 p. (2023)

Soundarya, J. (2023). What Is Network Forensics? Basics, Importance, And Tools, https://www.g2.com/articles/network-forensics

Suleman, K. Abdullah, G. Ainuddin, W.A.W. Muhammad, S. Iftikhar, A. (2016). Network forensics: Review, taxonomy, and open challenges, Journal of Network and Computer Applications, Volume 66, 2016, Pages 214-235, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2016.03.005

Tokody, D. Albini, A. Ady, L. Temesvári, Zs. M. Rajnai, Z. (2018). Kiberbiztonság az autóiparban. Connected and Automated Vehicles. http://bk.bgk.uni-obuda.hu/index.php/BK/article/view/79

Répás József – Nemzeti Közszolgálati Egyetem - KMDI

Alverad Technology Focus Kft.

- Független, integrált, szakmai partner
- Akkreditált kiberbiztonsági vizsgálólaboratórium
- Ipari rendszerek, informatikai rendszerek, szoftverek biztonsági vizsgálata

NAH-1-1829/2022
Vizsgálólaboratórium

Bevezető

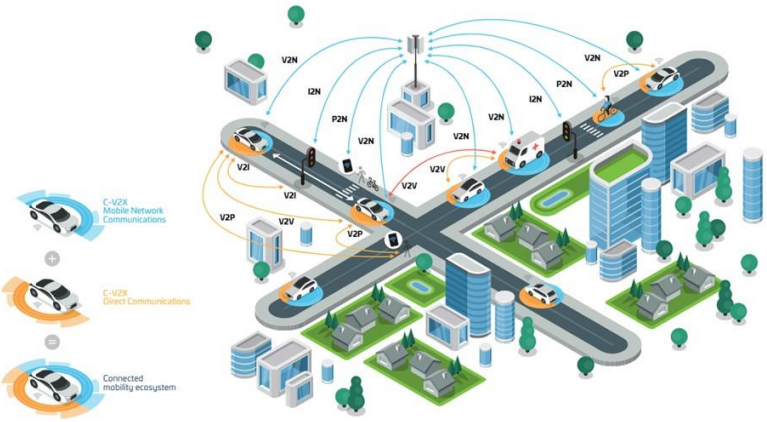
- A járműipar fejlődése
- Modern közúti közlekedési járművek megjelenése
- Hálózatba kapcsolt járművek
- Önvezető - emberi beavatkozás nélkül működő- járművek

- Közúti közlekedés balesetmentesítése
- Hatékony forgalomszervezés
- Károsanyag kibocsátás csökkentés
- Életmód változás

Aktualitás

- Új információs és kommunikációs technológiák
- Exponenciálisan növekszik a hálózatokban átvitt információk mennyisége
- Új szabályozási és vizsgálati környezet
- Járműgyártók elleni kibertámadások
- e-Call Segélyhívó Rendszer

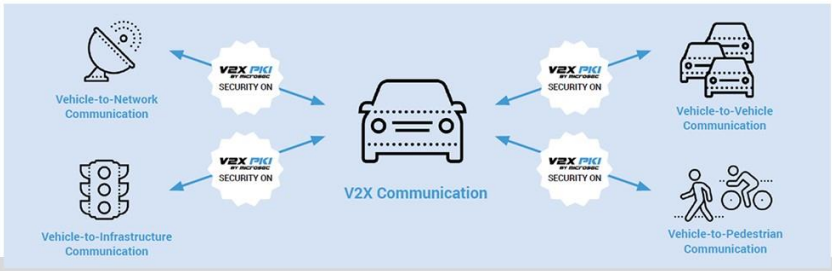
C-ITS



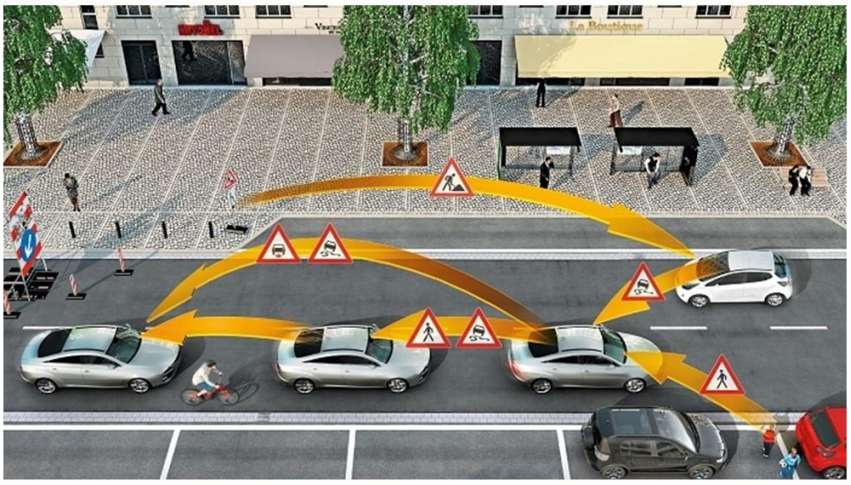
V2X

A jármű- és minden lehetséges dolog közötti együttműködés, kommunikáció lehetővé teszi, hogy összekapcsolja az összes járműtípust és a különféle infrastrukturális rendszereket.

Ez a kapcsolat magában foglalja az autókat, az autópályákat, a hajókat, a vonatokat, a repülőgépeket, valamint a gyalogosokat stb. is, ezáltal megvalósítva a teljes körű kooperativitást a közlekedésben



DSRC - Dedicated short-range communication



Jármű belső kommunikáció

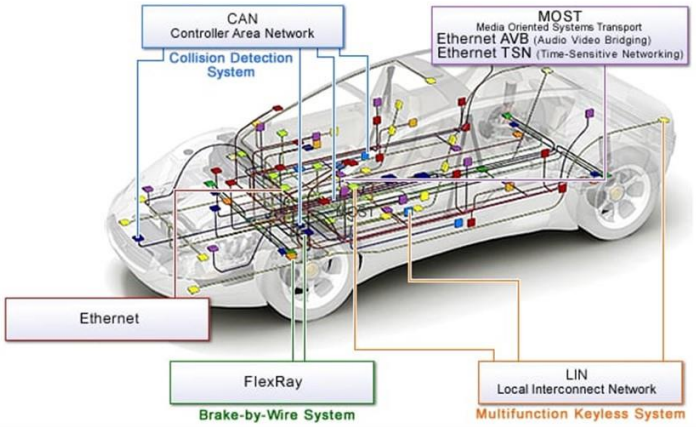
Az autóipar általánosan elfogadott kommunikációs szabványa:

- a CAN (Controller Area Network) protokoll,
- LIN (Local Interconnect Network),
- Flaxray,
- Automotive Ethernet.

Melyek szegmentált kialakítással, egyre gyorsabb és biztonságosabb kommunikációt hivatottak megvalósítani. Gateway-eken keresztül.

Jármű belső kommunikáció

A2B – Analog Devices‘ Automotive Audio Bus
MOST – Media Oriented System Transport



Jármű és nyomok

- Jármű a támadás célpontja,
- A jármű eszköz a bűncselekmény elvégzéséhez,
- Jármű tartalmazza az bizonyítékot.

- Európa Tanács Ajánlása a „Számítógépes-környezetben elkövetett bűncselekményekről”
  - Csalás, hamisítás, szabotázs,
  - Adatokban és programokban történő károkozás, ezek megváltoztatása,
  - Jogellenes behatolást
  - Jogellenes titokszerzést, kémkedés.

Forenzikus szakértői vizsgálat

- A vizsgálatok célja, a járművekben, járműrendszerekben bekövetkezett események hiteles, rekonstrukciója, felderítése. A releváns eseményekről bizonyítékok szolgáltatása, a későbbi, akár nyomozati és igazságszolgáltatási tevékenységekhez való felhasználáshoz.

Járművekhez kapcsolódó hálózati szakértői vizsgálatok célja

Járművekben található bizonyítékok

- Fellelése,
- Feltárása,
- Kinyerése,
- Vizsgálata,
- Megőrzése.

- Nyilvánvalóvá kell tenni, hogy mi történt, olyan esetekben is ami nem megismételhető.
- Live forensics kapcsolat + naplózás.

Vizsgálatok szükségessége

- Feltételezett visszaélés,
  - Jogosult vagy jogosulatlan hozzáférés,
  - Manipuláció,
  - Visszaélés vizsgálata.
- Megtörtént esemény vizsgálata,
- Root case elemzés
- Kártékony kód,
- Terrorcselekmény,
- Titkos információgyűjtés.

Network Forensics

A Network Forensics a Computer Forensics egyik ága, amely kommunikációs hálózatok mozgásban lévő adatainak (data in motion) azonosításához, vizsgálatához, értékeléséhez és elemzéséhez, illékony és dinamikus információkkal foglalkozik.

Célja annak biztosítása, hogy megértsük a hálózaton keresztül átvitt adatokat, valamint a végpontok felé irányuló, vagy közötti interakciók és tevékenységek feltárása.

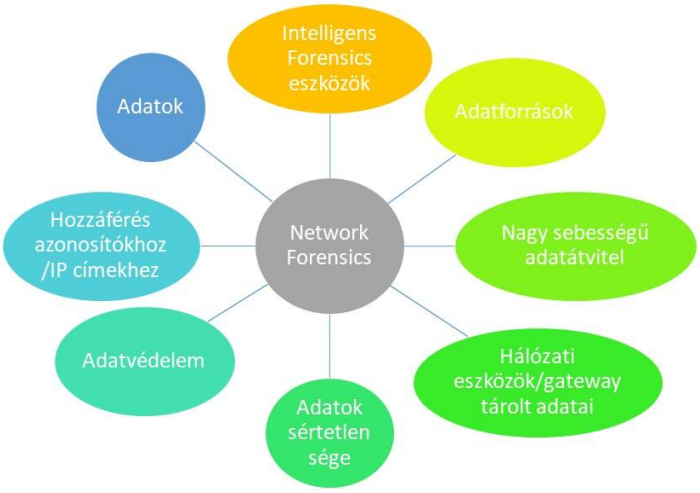
A hálózatokban megjelenő potenciális digitális bizonyítékokat a network forensics eszközrendszerével kell azonosítani és értékelni.

Network Forensics

- Hatóság,
- Katonai és állami szervezetek,
- Vállalatok,
- Egyetemek és kutató szervezetek,
- Kiberbiztonsági szervezetek.
- Kiberműveletek,
- Incidenskezelés,
- Igazságszolgáltatás,
- Csalásmegelőzés,
- Hálózati teljesítmény optimalizálás,
- Kutatás és fejlesztés.

Csatornák és kihívások

- Vezetékes
  - OBD-II
  - USB
- Vezeték nélküli
  - Wifi
  - Bluetooth
  - RFID



Jármű szakértői vizsgálat

Köszönöm a figyelmet!

ALVERAD TECHNOLOGY FOCUS

Kassai Károly:[1] A kibertér keretrendszerének stratégiai szintű változásai, fontosabb hatások (amelyek cselekvési irányokat mutatnak számunkra…)[2]

A kibertérben zajló történések a technológiai és társadalmi fejlődés számtalan oka miatt folyamatosan változó környezetet biztosítanak, benne pozitív és negatív jelenségekkel egyaránt. Emiatt a fenyegetések és sérülékenységek figyelemmel kísérése, a nemzetközi keretrendszer változásainak követése folyamatos kihívást jelent, de egyidejűleg támogatja a honvédelmi képességfejlesztésre vonatkozó gondolatok megfogalmazását, koncepciók és fejlesztési feladatok előkészítését.

Stratégiai irányok, a fenyegetések megvilágítása

Az EU és a NATO hasonló megfogalmazásokkal jellemzi napjaink biztonsági kihívásait.

Nemzetközi szinten stratégiai versenyhelyzet alakult ki (EU, 2022, old.: 5), összetett biztonsági fenyegetések fokozódó hatásokat váltanak ki. A nyílt tenger, légtér, világűr, kibertér[3] egyre inkább vitatott területekké vállnak.

A kihívások tengerében iránymutató a NATO stratégiai szintű megfogalmazás (NATO, 2022a, old.: 6), mely szerint a NATO elrettentés és védelem a nukleáris, a hagyományos és a

[1] ORCID: 0009-9398-6158
[2] Infokommunikáció 2023 Konferencia, Budapest, NKE, 2023. 11. 15.
[3] Más megfogalmazásban: globális közjavak (global commons).

rakétavédelmi képességek megfelelő összetételén alapul, amelyet űr- és kiberképességek egészítenek ki.[4]

A fenyegetések túlnyomó része hibrid formájú, amelyre az EU és NATO válasz az ellenálló képesség (resilience) fejlesztése komplex megközelítéssel, nemzeti szinten összkormányzati szemlélettel. A szükséges védelmi mechanizmusok kialakítása és fenntartása nem rövid távú feladat, amit a két forrásdokumentum perspektívája is szemléltet.[5]

A fenyegetések

Az EU a gazdaság biztonság területén 2023-ban fő kockázat típusokat azonosított (EU, 2023b, old.: 4-5):

- az ellátási láncok ellenállóképessége, beleértve az energiabiztonságot;
- a kritikus infrastruktúra fizikai és kiberbiztonságával kapcsolatos kockázatok;
- a technológiai biztonsággal és a technológia kiszivárgásával kapcsolatos kockázatok és
- a gazdasági függőségek és a gazdasági kényszerítés fegyverként való felhasználásának kockázata.

[4] A megfogalmazás tükrözi a Szövetség erejét képező összetevők rendjét és egyértelműen mutatja, hogy nem egy – egy elem (pl. nukleáris képesség vagy kiber erő) megléte, hanem az összes elem tudatosan összehangolt egysége nyújtja a reálisan értelmezett elrettentést, mint képességet.

[5] A NATO Stratégiai Koncepció a gyakorlatban egy évtizedre határozza meg az alapvető irányelveket, az EU Stratégiai Iránytű tervezetten a következő 5-10 évre határoz meg irányelveket, szempontokat a stratégiai és szakpolitikai tervezés számára.

Az EU Tanács a stratégia által azonosított fő kockázatok alapján több területen javaslatokat tett az EU szervezetek és a tagállamok felé kockázatelemzések végrehajtása érdekében (EU, 2023, old.: 3), négy területet kiemelve melyek vizsgálata sürgősen, már 2023-ban célszerű:

- fejlett félvezető technológiák;
- mesterséges intelligencia technológiák;
- kvantum technológiák;
- biotechnológiák.

A megfelelő védelmi eljárások kialakítása és felügyelhetősége érdekében a korábbinál lényegesen több, tizenegy EU-s kritikus szolgáltatás azonosítása történt 2022-ben a kritikus szervezetek rezilienciájára vonatkozó irányelv kiadásával (EU, 2022b, old.: 1-6, melléklet), illetve 2016-ban megkezdődött a NATO nemzeti ellenálló képességre vonatkozó követelmények megfogalmazása hét kritikus terület kijelölésével (NATO, 2023).

Az elektronikus információs rendszerek szintjén is megtörténik a fenyegetések trendek azonosítása. Az EU Kiberbiztonsági Ügynökség (ENISA)[6] 2023-as összefoglalásában az első kilenc fenyegetés között látható a zsarolóvírus, a pszichológiai megtévesztés és az ellátási lánc kockázat (ENISA, 2023, old.: 4), melyek káros hatásai a stratégiai szinten jelzett fenyegetett területeken is érzékelhetők.

[6] European Union Agency for Cybersecurity (korábban: EU Network and Information Security Agency)

Változások a fenyegetések ellensúlyozása érdekében

Lényegi lépés, hogy a már említett kritikus szervezetek ellenálló képességére vonatkozó irányelv 2024-ig nemzeti szakstratégiák kialakítását határozta meg.[7] Ugyanilyen határidővel az EU NIS2[8] Irányelv követelményeket határozott meg (EU, 2022a, old.: 22) a nemzeti kiberbiztonsági stratégiák felújítására (vagy újbóli kiadására).[9]

2023-ban megkezdődött az EU Kiberszolidaritásról szóló jogszabály megfogalmazása (EU, 2023d), melynek fő eleme a Kiber Pajzs (eseménykezelő képességek együttműködése), a Kiberbiztonsági Vészhelyzeti mechanizmus (közös felkészülés, EU szintű tartalék képzés, kölcsönös segítségnyújtás és a Kiberbiztonsági Eseményfelülvizsgálati Mechanizmus (nagyhatású események esetén ENISA műszaki felülvizsgálati eljárás).[10]

[7] Pl. „Nemzeti Ellenálló Képesség Stratégia” vagy más című, de hasonló tartalmú stratégia az alacsonyabb szintű jogszabályok összehangolása érdekében.
[8] Network and Information Security
[9] Az új nemzeti kiberbiztonsági stratégia várhatóan ki fogja váltani a jelenleg létező, a szakterületre vonatkozó két szakstratégiát. A kiberbiztonsági és kritikus infrastruktúra stratégiai szintű szabályozása további változásokat indukál. Jelentős változások várhatók a létfontosságú rendszerek védelmének törvényi szabályozásában (Lrtv.), az információbiztonsági törvényi szabályozásban (Ibtv.) illetve a törvényeket támogató végrehajtási rendeletek szintjén.
[10] A jogszabály tervezet három fő funkciójának (Cyber Shield, Cybersecurity Emergency Mechanism, Cybersecurity Incident Review Mechanism) tartalma, hatóköre és más képességekhez történő kapcsolódási pontjai kialakítás alatt állnak. A szabályozás célja a kiberbiztonság uniós szintű emelése, az együttműködési lehetőségek erősítése.

Technikai szintű változtatást vetít előre a 2019-es EU kiberbiztonsági jogszabály [11] tervezett módosítása. Az új kiberbiztonsági követelmények megjelenésének szempontjai felvetik az irányított biztonsági szolgáltatás [12] egyértelmű besorolását az egyéb elektronikus szolgáltatások közé, arra tanúsítására való kötelezettség bevezetését (EU, 2023c, old.: 2), új kiber tanúsítási kérdések megoldását igényli a tagállamoknál.[13]

2023-ban megjelent az EU Űr Stratégia a védelemért és biztonságért. A világűr kiemelt fontossága miatt szükség van a védelmi mechanizmusok, eljárások kiterjesztésére a világűrben lévő objektumokra, illetve a kapcsolódó infrastruktúrákra, a már említett kritikus szervezetekre és a hálózati és információbiztonságra vonatkozó irányelvek követelményeinek[14] megfelelően (EU, 2023a, old.: 3).

Katonai vonatkozások

A 2022-ben megjelent EU Kibervédelmi Politika megállapítja, hogy a katonai és polgári kibertér dimenziók közötti határ nem pontosan meghatározható; illetve a fizikai és digitális

[11] EU Cybersecurity Act
[12] managed security services - MSS
[13] Szakmai érdekesség, hogy a tervezet az „irányított biztonsági szolgáltatás” definiálására a NIS” Irányelv fogalmát (255/2555, Article 6, (40) kissé átalakította. A „kiberbiztonsági kockázatmenedzsment tevékenység (végrehajtása vagy annak támogatása)” kifejezéshez a „beleértve az incidensre adott választ, a behatolási tesztelést, a biztonsági auditokat és tanácsadást” értelmező jellegű kiegészítés történt. (Ez alapján érdemes lesz a végleges változat ellenőrzése.)
[14] Mindkét irányelv kritikus szegmensként azonosítja a világűrt.

infrastruktúrák közötti kölcsönös függőségek kiberbiztonsági incidensek forrásai lehetnek. Növelni kell a katonai – polgári együttműködést, a tagállamok teljes spektrumú kiberbiztonságát.[15] Az EDA[16] támogatásával ki kell alakítani a katonai eseménykezelő központok műveleti hálózatát (MICNET),[17] kiemelten a missziók és műveletek támogatása érdekében. A nagyhatású kiberbiztonsági események kezelése érdekében fokozni kell az együttműködést, illetve erősíteni kell a gyakorlatokat (EU, 2022, old.: 1, 3-4, 6).

A NATO Összhaderőnemi Doktrína 2023 decemberében megjelenítette a „multidomain” műveleti gondolkodást (NATO, 2022, old.: 3, 93, 98). Ez továbblépést jelent a NATO doktrinális gondolkodásban, műveletttervezésben és irányításban, ami Hazánk számára is végrehajtandó feladatokat jelent. Pontosítani kell a magyar műveletekre vonatkozó elveket, folyamatokat, a vezetésre és irányításra vonatkozó követelményeket, beleértve a kibertér műveletek katonai műveletekbe történő integrálásának kérdését is.

Az első NATO Kiber(tér) Műveleti Doktrína 2020-as kiadású (NATO, 2020). Az már említett új NATO Stratégiai Koncepció, az új műveleti (doktrinális) kérdések megjelenése, illetve az eltelt időszak tapasztalatainak hasznosítása szükségessé teszi a Doktrína felülvizsgálatát. Ezt a folyamatot a nemzeti doktrinális és műveleti területeken is át kell vezetni a NATO doktrínával történő

[15] A szakpolitika a „kiberbiztonság” és a „kibervédelem” kifejezést egyaránt alkalmazza, tartalmi magyarázat nélkül.
[16] EDA: European Defence Agency (Európai Védelmi Ügynökség)
[17] MICNET: milCERT Network

szinkronizálás, illetve nemzeti szabályozás korszerűsítése érdekében. A nemzeti szintű felső szintű szabályozás, a magyar kibertér műveletek alapvető kérdéseinek jogi megalapozása már megtörtént.

Az eltelt időszak alapján ugyanakkor jogos a kérdés, hogy a tapasztalatok szükség van a vonatkozó törvények (Nbtv, Hvtv. és Ibtv.)[18] változtatására (pl. felelősségek, folyamtok és feladatok), beleértve a szervezeti keretrendszert is (FARKAS, 2023). Az elméleti felvetés gyakorlati alapja egyszerű: pontos meghatározásra van szükség az elektronikus információbiztonság (és védelem),[19] a kiberbiztonság[20] és kibervédelem - vagy védelmi kibertér művelet - (beleértve a támadásmegszakítás kérdését is)[21] és az offenzív kibertér művelet[22] tevékenységekre (folyamatokra, feladatokra felelős szervezetekre és kapcsolódási pontokra) úgy, hogy a nemzeti és nemzetközi kapcsolódási pontok egyértelműen legyenek és feleljenek meg a nemzetközi normáknak, jogszabályoknak.

A kérdés a jogi és szabályozási értelmezés mellett a katonai képességek szempontjából sem mellőzhető. Az említett kibertér

[18] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról; 2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről; 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
[19] A magyar jogszabályok a nyílt, nem minősített adatok területén az „elektronikus információbiztonság” a minősített adatok területén az „elektronikus információvédelem” kifejezést alkalmazzák.
[20] Cyber Security
[21] Defence Cyber Operation - DCO
[22] Offensive Cyber Operations - OCO

tevékenységek nagy része azonos (vagy hasonló) elemeket tartalmaz.[23]

A működés alapvető kérdése annak egyértelmű megfogalmazása, hogy milyen műveletek milyen felelősségi körben történnek (folyamatok, feladatok és felelősök), milyen céllal, kinek a jóváhagyásával. A műveleti tervek (dokumentumok) elkészítésének és jóváhagyásának rendje, illetve a katonai műveletbe integrált vagy önálló kibertér művelet irányításával és más műveletekkel történő összehangolással kapcsolatos kérdések rögzítése nélkül reálisan nem képzelhető el kibertér művelet (önállóan, vagy összhaderőnemi, multidomain keretrendszeren belül értelmezetten). E kérdéseket nem csak alacsonyabb szintű (művelettervezési és irányítási) dokumentumokban, hanem a stratégiai szintű dokumentumokban (nemzeti stratégiai szint, jogszabályok és doktrínák) is részletesen ki kell dolgozni az átláthatóság, érthetőség, illetve az elszámoltathatóság érdekében.

Összefoglalás

Az egyre súlyosabb hatású fenyegetésekre adott NATO és EU válaszok a hatékonyabb reagálást, az ellenállóképesség és az együttműködés növelését, az elrettentés fenntartását célozzák. Az uniós, szövetséges és nemzeti szolgáltatások nagymértékben

[23] A teljesség igénye nélküli példák: a hálózati-, eszköz- vagy károskód elemzés egyaránt eszköze az elektronikus információbiztonságnak, kiberbiztonságnak vagy kibervédelemnek. A sérülékenységvizsgálat körébe tartozó technikák mind a négyfajta művelet esetében azonosítható, ugyanúgy, mint a fenyegetés felderítés (Cyber Threat Intelligence – CTI).

függenek a digitalizációtól (elektronikus szolgáltatásoktól), így kijelenthető, hogy a függőségeket (azok kezelését) is stratégia kérdésnek kell tekinteni.

A nemzetközi színtéren növekvő mértékben jelennek meg kibertér biztonságához köthető szabályozók, melyeket nemzeti szinten is követni kell, beleértve a katonai képességeket is.

Az EU és NATO katonai megfogalmazásokban erőteljesen azonosíthatók a kibertér biztonságára, illetve a kibertér műveleti képességekre vonatkozó igények, melyek rámutatnak az együttműködés fontosságára, a szakmai feladatok folyamatos fejlesztésére és a külső kapcsolódási pontok folyamatos pontosítására.

Felhasznált irodalom

ENISA. (2023). Threat Landscape 2023.

EU. (2022). A biztonság és a védelem területére vonatkozó stratégiai iránytű; Brüsszel, 2022. március 21, 7371/22.

EU. (2022). KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK Az EU kibervédelmi politikája, Brüsszel, 2022.11.10. JOIN(2022) 49 final.

EU. (2022a). AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáráról.

EU. (2022b). AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2557 IRÁNYELVE (2022. december 14.) a kritikus

szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről.

EU. (2023). COMMISSION RECOMMENDATION of 3.10.2023 on critical technology areas for the EU's economic security for further risk assessment with Member States, Strasbourg, 3.10.2023 C(2023) 6689 final.

EU. (2023a). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL European Union Space Strategy for Security and Defence; Brussels, 10.3.2023 JOIN(2023) 9 final.

EU. (2023b). KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK, AZ EURÓPAI TANÁCSNAK ÉS A TANÁCSNAK AZ EURÓPAI GAZDASÁGI BIZTONSÁGI STRATÉGIÁRÓL, Brüsszel, 2023.6.20. JOIN(2023) 20 final.

EU. (2023c). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services, COM(2023) 208 final.

EU. (2023d). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents COM/2023/209 final.

FARKAS, Á. (2023). *Az állami kiber képességek szervezésének és szabályozásának aktuális kérdései, előadás, Katonai Kibertér 2023 Konferencia, Budapest, 2023. 10. 25.*

NATO. (2020). Allied Joint Doctrine for Cyberspace Operations (AJP 3.20) Edition A Version 1.

NATO. (2022). Alllied Joint Doctrine (AJP 01) Edition F Version 1.

NATO. (2022a). NATO Stratégiai Koncepció 2022.

NATO. (2023). *Resilience, civil preparedness and Article 3*. Letöltés dátuma: 2023. 11 08, forrás: https://www.nato.int/cps/en/natohq/topics_132722.htm

A kibertér keretrendszerének stratégiai szintű változásai, fontosabb hatások
(amelyek cselekvési irányokat mutatnak számunkra…)

Infokommunikáció 2023 Konferencia

Budapest, NKE, 2023. 11. 15.

Dr. Kassai Károly

Tartalom

- **Fenyegetések, EU, NATO stratégiai irányok**
  - Összetett, bonyolult biztonsági helyzet

- **Változást jelentő folyamatok**
  - Rengeteg nemzetközi változás

- **Honvédelmi gondolatok**
  - A honvédelmi folyamatok, eljárások naprakészsége

Stratégiai irányok

- **Fenyegetések**
  - Stratégiai versenykörnyezet, fokozódó stratégiai verseny, összetett biztonsági fenyegetések
  - A nyílt tenger, a légtér, a világűr és a kibertér egyre inkább vitatott, műveleti terület
  - NATO elrettentés és védelem: a nukleáris, a hagyományos és a rakétavédelmi képességek megfelelő összetételén alapul, amelyet űr- és kiberképességek egészítenek ki
  - a világűr és a kibertér biztonságos használatának és korlátlan hozzáférésének biztosítása
- **2022-es reagálások a biztonsági helyzet változásaira**
  - NATO Stratégiai Koncepció (2022): biztonsági és katonai cselekvési irányok kijelölése
  - EU Stratégiai Iránytű (2022): iránymutatás a következő 5 - 10 évre a stratégiák, szakpolitikák számára
- **Hibrid szemlélet – ellenállóképesség fejlesztés**
  - Összkormányzati szemlélet – a komplex megközelítés szükségessége!

EU fejlett kockázatok 2023

EU Gazdasági Biztonsági Stratégia (2023), fő kockázattípusok

- Ellátási láncok ellenállóképessége, beleértve az energiabiztonságot
- Kritikus infrastruktúra fizikai és kiberbiztonságával kapcsolatos kockázatok
- Technológiai biztonsággal és a technológia kiszivárgásával kapcsolatos kockázatok
- Gazdasági függőségek és a gazdasági kényszerítés fegyverként való felhasználásának kockázata

EU Tanácsi javaslatok kockázatelemzésre (2023)

- Fejlett félvezető technológiák
- Mesterséges intelligencia technológiák
- Kvantum technológiák
- Biotechnológiák
- Fejlett kommunikációs, navigációs és digitális technológiák
- Fejlett szenzor technológiák
- Űr és hajtómű technológiák
- Energia technológiák
- korszerű anyagok, előállítási és újra-hasznosítási technológiák

ENISA Threat Landscape 2023

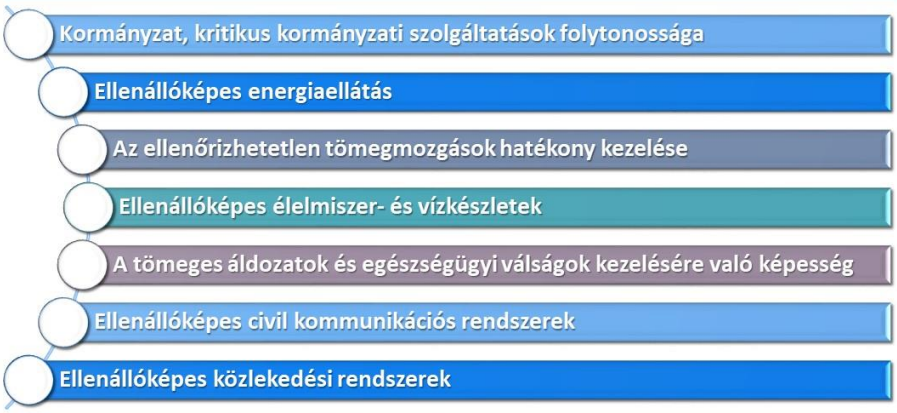
- Zsarolóvírus
- Káros kód
- Pszichológiai megtévesztés
- Adatfenyegetés
- Rendelkezésre állás veszélyeztetése (Denial of Service)
- Rendelkezésre állás veszélyeztetése (Internet threats)
- Információs manipulálás, befolyásolás
- Támogatói lánc fenyegetések

EU kritikus szolgáltatások (2022)

- Energia
  - Villamos energia
  - Távfűtés vagy távhűtés
  - Kőolaj
  - Földgáz
  - Hidrogén
- Közlekedés
  - Légi
  - Vasúti
  - Vizi
  - Közúti
  - Tömegközlekedés
- Banki szolgáltatások

- Pénzügyi piaci infrastruktúra
- Egészségügy
- Ivóvíz
- Szennyvíz
- Digitális infrastruktúra
- Közigazgatás
- Világűr
- Élelmiszer-előállítás, -feldolgozás és -forgalmazás

NATO: a nemzeti ellenálló képességre vonatkozó követelmények



Új követelmények >> új megoldások

- **EU kritikus infrastruktúra szolgáltatók, hálózatbiztonsági irányelv (2022)**
  - Az új irányelvek alapján >> 2024-től változó/új NKBS, Lrtv. és Ibtv. valamint a végrehajtási rendeletek, új „Nemzeti Ellenálló Képesség Stratégia”
- **EU Kiber Szolidaritási Rendelet (2023?)**
  - Új funkciók, folyamatok: Cyber Shield (SOC-ok hálózata), Cybersecurity Emergency Mechanism (felkészülés, EU tartalék, kölcsönös segítségnyújtás), Cybersecurity Incident Review Mechanism (ENISA műszaki felülvizsgálat)
- **EU Kiberbiztonsági Jogszabály (CSA) módosítás (2023?)**
  - NIS2 irányelv által bevezetett irányított biztonsági szolgáltatás (MSS) kerüljön tanúsítási kötelezettség alá>> új tanúsítási kérdések
- **EU digitális elemeket tartalmazó termékek kiberbiztonsági követelményei (2023?)**
  - Igazolt termékek igénye, gyártók bejelentési kötelezettsége >> növekedő CSIRT folyamatok, feladatok

Új követelmények >> új megoldások 2

- **EU Űr Stratégia a biztonságért és védelemért (2023?)**
  - Az űr infrastruktúrák kiemelt fontossága>> az új követelményeket át kell vezetni a kritikus infrastruktúra, NIS2 szabályokan (még nem készültek a nemezti végrehajtási elemek!)
- **EU Kibervédelmi Politika**
  - Együttes fellépés, uniós védelmi ökoszisztéma >> Szoros katonai – polgári együttműködés
- **NATO Összhaderőnemi Doktrína (AJP 01) (2022. 12.)**
  - Multidomain műveletek megjelenítése >> át kell vezetni a funkcionális doktrínákon az MDO gondolkodást >> ennek meg kell jelennie a magyar műveletnél is
- **NATO Kiber Műveleti Doktrína (AJP 3.20) (2020)**
  - Új Statégiai Koncepció/Új doktrinális elemek >> át kell vezetni a változásokat, értékelni kell a tapasztalatokat, a magyar kibertér műveleti kérdéseket célszerű felülvizsgálni…
- **Milyen változások szükségesek a Hvt-ben, Nbtv-ben, szervezeti keretrendszerben a kibertér műveletek sikere érdekében???** (Farkas Ádám, 2023 10. 27 konferencia)

A kiberműveletek rejtelmei…

Elektronikus információbiztonság(védelem) – kiberbiztonság

- Folyamatok, feladatok, felelősök (szereplők)

Kibervédelem (DCO) – benne támadás megszakítás

- Folyamatok-feladatok-felelősök (cél, jóváhagyó, határidő)

Offenzív kiberművelet (OCO)

- Folyamatok-feladatok-felelősök (cél, jóváhagyó, határidő)

- Biztonsági követelmények, audit (…)
- Oktatás és tudatosítás
- Sérülékenységvizsgálatok
- Eseménykezelés
- Műszaki elemzés (…)
- Kiber hírszerzés (CTI)

- Műveleti koncepció/terv dokumentumok (jóváhagyó, cél, határidő, felelősök, feladatok)
- Katonai műveletbe történő integrálás (önálló művelet vagy támogató feladat)
- Együttműködők …

Összefoglalás

- *(A mesterséges intelligencia tovább bonyolítja a helyzetet… ☺)*
- Egyre súlyosabb hatású fenyegetések >> az EU, NATO válaszoknak tükrözni kell a reagálást, mint elrettentés, ellenálló képesség és együttműködés
  - Alkalmazási, együttműködési és hozzájárulási kötelezettségeink vannak
  - Az uniós, szövetséges és nemzeti biztonsági szolgáltatások ezer szálon függenek az elektronikus szolgáltatásoktól >> nem csak a biztonság, a függőség is stratégiai kérdés!
- A szabályozási felületek fejlődnek, növekednek a kapcsolódási pontok (és szereplők, eljárások, feladatok)
  - Követni kell a szabályozási lépéseket >> nemzeti és katonai eljárok kompatibilitása!
  - Kommunikálni kell, hogy mi a nemzeti álláspont a kibertérben történő események megközelítéséről
- Az EU és a NATO katonai feladatokban markánsan azonosíthatók a kibertér műveleti igények
  - A fejlődésből nem lehet kimaradni >> a szakmai feladatokat, külső kapcsolódási pontokat folyamatosan fejleszteni kell

Köszönöm a megtisztelő figyelmet!

Biztonságos Kiberteret! ☺

Források

1) A biztonság és a védelem területére vonatkozó stratégiai iránytű; Brüsszel, 2022. március 21. 7371/22
2) AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/ 1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)
3) AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2557 IRÁNYELVE (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről
4) COMMISSION RECOMMENDATION of 3.10.2023 on critical technology areas for the EU's economic security for further risk assessment with Member States, Strasbourg, 3.10.2023 C(2023) 6689 final
5) ENISA Threat Landscape 2023

Források 2

6) Farkas Ádám: Az állami kiber képességek szervezésének és szabályozásának aktuális kérdései, Katonai Kibertér 2023 KOnferenccia, Budapest, 2023. 10. 25.
7) JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL European Union Space Strategy for Security and Defence; Brussels, 10.3.2023 JOIN(2023) 9 final
8) KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK, AZ EURÓPAI TANÁCSNAK ÉS A TANÁCSNAK AZ EURÓPAI GAZDASÁGI BIZTONSÁGI STRATÉGIÁRÓL, Brüsszel, 2023.6.20. JOIN(2023) 20 final
9) KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK Az EU kibervédelmi politikája, Brüsszel, 2022.11.10. JOIN(2022) 49 final
10) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents COM/2023/209 final

Források 3

11) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020
12) REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
13) NATO AJP 01 (2022)
14) NATO AJP 3.20 (2020)
15) NATO Stratégiai Koncepció 2022

Oláh István[1]: Hogyan érvényesülnek az Információbiztonsági kontrollok egy publikus felhőben.

Kulcsszavak:, felhő, biztonság, szerződés, technológia, kontrollok.

Bevezetés

A pulikus felhőszolgáltatásokkal kapcsolatos információbiztonsági kérdésekkel számos tudományos és szakmai konferencia foglalkozik. 2023-ban március 22-én a Hétpecsét Egyesület, "Információvédelem menedzselése CV. Szakmai Fórum" rendezvényén [2] , április 27-én egy Nemzetközi Katonai Információbiztonsági konferencián [3][4], szeptember 27-én az ICT Global Tech Leaders – Modellváltás konferencián[5] tartottam már előadásokat.

Az elmúlt időszakban egyre több informatikai rendszer költözik a felhőbe. Ennek oka az egyre gyorsuló innovációhoz szükséges folyamatos informatikai erőforrások, és a megfelelően képzett üzemeltetői állomány biztosítása.

[1]Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: olah.istvan@uni-obuda.hu
Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet, e-mail: olah.istvan.gyorgy@uni-nke.hu

[2]https://hetpecset.hu/site/events/index#w0-collapse4

[3]https://ludevent.uni-nke.hu/event/2860/

[4] https://comconf.hu/kiadvany/Nemzetk%C3%B6zi%20Katonai%20Inform%C3%A1ci%C3%B3biztons%C3%A1gi%20Konferencia_2023.pdf#page=55

[5] https://ictglobal.hu/iparagi-megoldasok/ict-global-tech-leaders-modellvaltas-konferencia/

Emiatt az Európai Uniós jogalkotásban is megjelentek az új előírások a szolgáltatói láncokra értelmezve: CER[6] [1], NIS2[7] [2], DORA[8] [3].

A felhőszolgáltátok csoportosítása

Amennyiben megkérdezünk szakembereket a mit jelent számukra a publikus felhő és abban az információbiztonsági kontrollok, számos eltérő választ kapunk. A felhőt kettős vetületben célszerű elemezni, mint technológia, és mint szolgálattatások. Erre a második dián tértem ki.

A felhőszolgáltatások igénybe vételéhez szükséges biztonsági kontrollok meghatározásakor első lépésként szükséges meghatározni a milyen felhőt, és mire fog a szervezet igénybe venni kérdésre a választ. Ebben nyújtanak segítséget a NIST (National Institute of Standards and Technology) 800-145-ben[9] [4] szereplő definíciók.

Amennyiben a NIST által meghatározott szolgáltatás felhőnek minősül, akkor célszerű a „Magyar Nemzeti Bank a közösségi és publikus felhőszolgálatatások igénybevételéről” szóló 4/2019 számú ajánlása[10] [5] alapján az egyes szolgáltatási fajtákat (IaaS, PaaS, SaaS), valamint a kapcsolatos felelősségeket a szolgálatóval egyeztetni, amely megértését jól segíti az ábrában jelzett szerepkör elválasztás.

---

[6]2022/2557-EU
[7]2022/2555-EU
[8]2020/0266-EU
[9]800-145-NIST
[10]4/2019-MNB

Fontos kihangsúlyozni, hogy egy munkaszervezet tevékenysége során a felhasználókért – beleértve az ügyfeleket is –, valamint az adatokért, a felhőszolgálató nem lehet felelős!

Mindezek az előadás harmadik diáján szerepelnek.

Manapság bármilyen szolgálatatásra lehet felhőt igénybe venni. Ezeket foglalja össze a negyedik dián szereplő felsorolás, amelyen mutatok pár olyan példát, amelyek a bűnözési célokra is elérhetők.

Egy felhő információbiztonsági auditja

Egy felhő használatra vonatkozó szerződés megkötése előtt a Bizalmasság (B), Sértetlenség, Rendelkezése (R) szempontokat (BSR) javasolt ugyanúgy figyelembe venni, mint a földi informatikai rendszerek esetén. A jogszabályokban, nemzetközi módszertanokban megfogalmazott információbiztonsági kontrollokat platform független célszerű alkalmazni, mert a megvédendő adat szempontjából érdektelen az, hogy az adat egy mobileszközön, egy fizikai serveren felhasználói eszközön, virtuális eszközön, konténerben, vagy a felhőben van-e. Az egyenszilárd védelem érdekében a felhőben is érvényesíteni szükséges az előírt információbiztonsági előírásokat. A felhőben a megszokott gyakorlattól eltérő mód lehet például az azonosítással, jogosultsággal, naplózással kapcsolatos kontrolokat kialakítani, ezért ezeket célszerű újra átgondolni. Amennyiben egy szervezet rendelkezik a biztonsági követelményeket előíró belső szabályozással, akkor első lépésként célszerű ezt kibővíteni a felhős esetekre is. A szolgálatóval történő szerződés megkötése előtt az

elérhető információbiztonsági és működésbiztonsági auditok dokumentációját szükséges elemezni. Erre az ötödik és hatodik dián térek ki.

Amennyiben egy szervezet létfontosságú feladatot lát el, mint kritikus infrastruktúra [11] és/vagy vonatkozik rá az Ibtv.[12], akkor az információbiztonsági kontrollok meghatározását célszerű a BM rendeletből kezdeni[13].

Az igénybe vett felhőszolgáltatást, a BM rendeleti információbiztonsági kontrollok alapján lehet végig elemezni több lépésben. Az előadásban a munkaszakasz zárolási kontrollokat[14] mutattam be lépésről lépésre a hetedik, nyolcadik és kilencedik dián. Az elemzések során nagyon fontos, hogy nem elégséges az információbiztonsági előírásoknak megfelelést dokumentáció alapon elemezni, mert a képesség meglétéből nem következik annak megléte is. Erre példát szintén a kilencedik dián mutatok be. A munkaszakasz zárolás, mint egy alapvető információbiztonsági előírás egy létfontosságú szervezetben működő elektronikus információs rendszerre példája alapján minden információbiztonsági

[11]A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló, 2012. évi CLXVI. törvény

[12]Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013, évi L. törvény

[13]az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet

[14]BM rendelt 3.3.10.10 munkaszakasz zárolása

kontroll kialakítható a felhőben is, ahogy a tizedik dia tartalmazza. A felhők egyéb kérdéseire a tizenegyedik dián tértem ki.

Irodalomjegyzék

[1] *AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2557 IRÁNYELVE a kritikus szervezetek rezilienciájáról, 2022. december 14.*

[2] *AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, 2022. december 14.*

[3] *AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2020/0266 RENDELETE a pénzügyi ágazat digitális működési rezilienciájáról, 2020. szeptember 24.*

[4] Peter Mall és Tim Grance, „U.S. Department of Commerce , National Institute of Standards and Technology,” szeptember 2011. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-145/final. [Hozzáférés dátuma: 10 május 2023].

[5] *A Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételéről,* 2019.

eivok

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Hogyan érvényesülnek az Információbiztonsági kontrollok egy publikus felhőben.

Infokommunikáció szakmai tudományos konferencia
2023.november 15.

Oláh István - EIVOK alelnök, Óbudai Egyetem BDI.
HTE Információbiztonsági Szakosztály - EIVOK
istvan.olah@hte.hu; olah.istvan.op@gmail.com;
olah.istvan.gyorgy@uni-nke.hu; olah.istvan@uni-obuda.hu

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

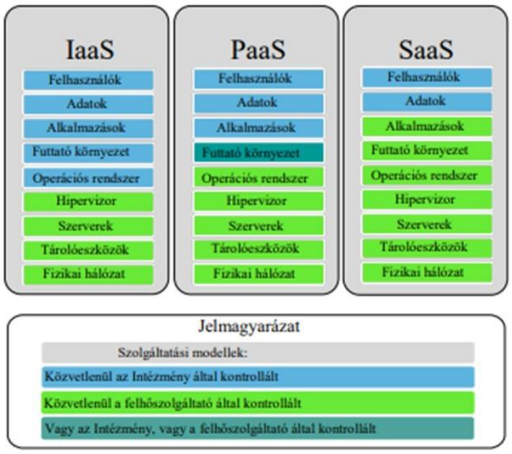
Mi a felhő ?

- Egy technológia,
- Erőforrás,
- Szolgáltatások,
- …
- A gyakorlatban sokan keverik ezeket a gondolkodásban
- A földön is lehet a felhő!

Forrás: https://www.usanotebook.hu/blog/mi-az-a-felho-es-miert-jo/467

A felhő fogalma, és felelősségi kérdései?

- Privát, Publikus, Közösségi.
- Hibrid, Multi.
- A publikus felhőszolgáltatás öt lényegi ismérve a következő:
  - a szolgáltatás igény szerinti, akár önkiszolgáló módon való igénybevétele,
  - általános hálózati elérés,
  - megosztottan használt erőforrások,
  - a változó kapacitás-igények gyors lekövetése,
  - mért szolgáltatás (felhasználással arányos használati díj),
- The NIST Definition of Cloud Computing (SP 800-145).



Forrás:
https://www.mnb.hu/letoltes/4-2019-felho.pdf

XaaS ?

+ Address Verification as a Service
+ Anything as a Service
+ API as a service (APIaaS) Application
+ Delivery as a Service
+ Application Platform as a Service
+ Architecture as a Service
+ Authentication as a Service
+ Backend as a Service
+ Backup as a Service
+ Big Data as a Service
+ Broker as a Service
+ Business as a Service
+ Business Process as a Service
+ Cloud Load Balancers as a Service
+ Cloud Search as a Service
+ Collaboration-as-a-Service
+ Commerce as a Service
+ Communication as a Service
+ Computing as a Service
+ Contact Center as a Service
+ Conversations as a Service
+ Data as a service
+ Database as a service
+ Desktop as a Service
+ Development as a Service
+ DevTest as a Service
+ Disaster Recovery as a Service
+ Drupal as a Service
+ Email as a Service
+ Encryption as a Service
+ Enterprise Resource Management as a Service
+ Ethernet as a Service
+ Everything as a Service
+ Firewall as a Service
+ Framework as a Service
+ Globalization as a Service
+ Hadoop as a Service
+ Hardware as a Service
+ High Performance Computing as a Service
+ Identity as a Service
+ (Infrastructure PaaS)
+ Insight as a Service
+ Integrated Development Environment as a Service
+ Integration as a Service Integration Platform as a Service
+ Integration Platform as a Service
+ IT as a Service
+ Java Platform as a Service
+ Knowledge as a Service
+ Light as a Service
+ Logon as a Service Management as a Service
+ Mashups as a Service
+ Message Queuing as a Service
+ Metal as a Service
+ Mobility as a Service
+ Mobility Backend as a Service
+ Monitoring as a Service
+ Network Access Control as a Service
+ Network as a Service
+ Operations as a Service
+ Optimization as a Service
+ Payment as a Service
+ Quality as a Service
+ Query as a Service
+ Recovery as a Service
+ Remote Backup as a Service
+ Risk Assessment as a Service
+ Robot as a Service
+ Security as a service
+ Service Desk as a Service
+ Solutions as a Service
+ Storage as a Service
+ Telepresence as a Service
+ Test environment as a Service
+ Testing as a Service
+ Transport as a Service
+ Unified Communications as a Service
+ User Interface as a Service
+ Video Conferencing as a Service
+ Video Surveillance as a Service
+ Voice as a Service
+ Website as a Service

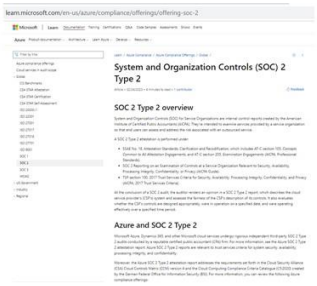
+ Mélytanulás
+ Kvantumszámítástechnika

Forrás: Koczka Ferenc, okosóra előadása az OTP Bank Nyrt-ben

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

A Felhő auditja I.

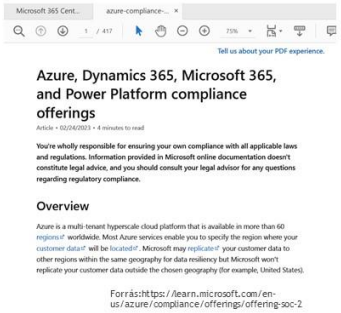
- Felhőszolgáltató igénybe vételével kapcsolatos beszerzéskor EIR-enként érdemes elkérni a szolgáltatást vizsgáló **auditok dokumentációját**.
- Akinek van, jellemzően a **tanúsítványt** publikálja az Interneten, de abból valójában semmit nem lehet megtudni, mert az értelmezésükhöz be kell szerezni a **vizsgálati profilt, módszertant és az audit tervet is.** Ezekből lehet látni a mit és milyen szinten tud nyújtani a szolgáltató ami általában nem az a szint amit hirdet magáról!


learn.microsoft.com/en-us/azure/compliance/offerings/offering-soc-2

System and Organization Controls (SOC) 2 Type 2

SOC 2 Type 2 overview

Azure and SOC 2 Type 2


Microsoft 365 Cent... azure-compliance-...

Tell us about your PDF experience.

Azure, Dynamics 365, Microsoft 365, and Power Platform compliance offerings

Article • 02/24/2023 • 4 minutes to read

You're wholly responsible for ensuring your own compliance with all applicable laws and regulations. Information provided in Microsoft online documentation doesn't constitute legal advice, and you should consult your legal advisor for any questions regarding regulatory compliance.

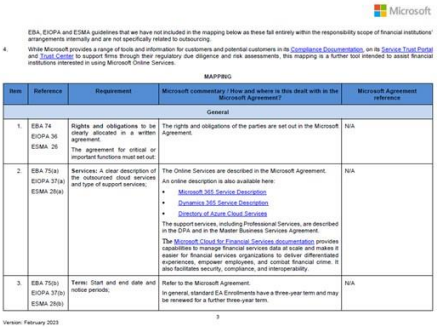
Overview

Azure is a multi-tenant hyperscale cloud platform that is available in more than 60 regions worldwide. Most Azure services enable you to specify the region where your customer data will be located. Microsoft may replicate your customer data to other regions within the same geography for data resiliency but Microsoft won't replicate your customer data outside the chosen geography (for example, United States).

Forrás:https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-soc-2

A Felhő auditja II.

- Felhőszolgáltató dokumentumai elérhetőek.
- Több ezer oldal 10% url.
- **A dokumentumok dinamikusak !**, de részei a szerződésnek!
- ISO 27017, 27018 (27015), SOC2-Type2,


Microsoft

EBA, EIOPA and ESMA guidelines that we have not included in the mapping below as these fall entirely within the responsibility scope of financial institutions' arrangements internally and are not specifically related to outsourcing.

4. While Microsoft provides a range of tools and information for customers and potential customers in its Compliance Documentation, on its Service Trust Portal and Trust Center to support firms through their regulatory due diligence and risk assessments, this mapping is a further tool intended to assist financial institutions interested in using Microsoft Online Services.

MAPPING

Item	Reference	Requirement	Microsoft commentary / How and where is this dealt with in the Microsoft Agreement?	Microsoft Agreement reference
		General		
1.	EBA 74 EIOPA 36 ESMA 26	Rights and obligations to be clearly allocated in a written agreement. The agreement for critical or important functions must set out	The rights and obligations of the parties are set out in the Microsoft Agreement.	N/A
2.	EBA 75(a) EIOPA 37(a) ESMA 28(a)	Services: A clear description of the outsourced cloud services and type of support services;	The Online Services are described in the Microsoft Agreement. An online description is also available here: • Microsoft 365 Service Description • Dynamics 365 Service Description • Directory of Azure Cloud Services The support services, including Professional Services, are described in the DPA and in the Master Business Services Agreement. The Microsoft Cloud for Financial Services documentation provides capabilities to manage financial services data at scale and makes it easier for financial services organizations to deliver differentiated experiences, empower employees, and combat financial crime. It also facilitates security, compliance, and interoperability.	N/A
3.	EBA 75(b) EIOPA 37(b) ESMA 28(b)	Term: Start and end date and notice periods;	Refer to the Microsoft Agreement. In general, standard EA Enrollments have a three-year term and may be renewed for a further three-year term.	N/A

Version: February 2023

3

Ibtv. Megfelelés kontroll szinten- I

- Az azpolicyadvertizer-semicolon lapon az Azure policydefiníciók összefoglalása található meg. Az Azure védelmi profilok egyes adatai innen kerülnek az Azureba.
- Első lépésként célszerű *„az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) **BM rendelet**”* **kontrolljait NIST azonosítóval összerendelni, pl:**

BM rendelet			NIST
3.3.10.10.	A munkaszakasz zárolása	3.3.10.10.1. Az érintett szervezet: 3.3.10.10.1.1. meghatározott időtartamú inaktivitás után, vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést; 3.3.10.10.1.2. megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.	AC-11

Ibtv. Megfelelés kontroll szinten-II

- Második lépésben a NIST kód alapján az audit dokumentumokban megkeresni az adott kontrollt:

NIST		
AC-11	Session Lock	The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

- *Harmadik lépésben a kontrollal kapcsolatos előírás értékelése következik megfelel, vagy nem felel meg lehetőség szinten:* ***IGEN!***
- Negyedik lépésben, az adott kontroll kialakítását szükséges előírni a biztonsági rendszertervben.

Ibtv. Megfelelés kontroll szinten-III.

- Ötödik lépésben az Azure-ban az adott rendszere az érvényesítő paramétereket hangolni szükséges, azaz az alapbeállításokat kontrollonként végig kell gondolni, és a hangolást elvégezni.
- Az előíró jellegű lépések a forráshelyről pl. excel exportot alkalmazva úgy végezhetők el könnyedén, hogy egy „üres OVI” táblába az összerendelési logikát bevisszük, azaz az ovi táblát egy felhős + „*füllel*” látjuk el.
- Az adott rendszer biztonsági előírásait a kibővített „ovi” fájlban ugyanúgy lehet kezelni mint a többi kontrollt.
- Az előírt kontrollok paramétereit sem szükséges egyenként konfigurálni, mert a "M" (Mandatory), és az "O" (Optional) értékeket fileból be lehet olvasni, és az értékek benne lehetnek egy egy rendszer biztonsági leíró adatbázisában, akár az ovi táblájában is.
- A biztonságos környezet egyszerűen és gyorsan alakítható így ki, sőt a változásokra riasztás állítható be (Sentinel)

Hol lehet a kontrollokat kialakítani?

MINDENHOL !

mert egy, egy kontroll nem szolgáltató és technologai függő!

A Felhő egyéb kérdései

- Ki birtokolja az adatokat?
- KULCSOK KEZELÉSE!
- Késleltetés!
- Elnyomási hatás!
- Szerződési feltételek.
- A szolgáltató menedzsment és tulajdonosi szerkezet elemzése, **mert sosem az semmi aminek elsőre látszik**….,
- Politikai kockázat van-e? Oroszország esete!
- A Felhő és a TELKO **üzemeltetői kollegái egyedi kockázatot jelentenek-e?**
- … és….

Köszönöm a megtisztelő jelenlétet és figyelmet!

https://www.hte.hu/eivok
https://www.hte.hu/esemenyek/-/esemeny/1/4876226/eivok-40--szakmai-est

Busa Attila József[1]: Az egyes hacker generációk támadási szokásai és aktuális támadási trendek fejlődése a 2000-es évektől napjainkig

Az első generáció, a „hacker-lét”, mint életforma

A „hackerek” első generációja a 2000-es évek elején jelent meg és a közhiedelemben úgy váltak ismertté, mint tinédzserek, akik sötét, nyirkos pincékben vírusokat írnak, hogy hírnevet szerezzenek, és megmutassák a világnak, hogy mire képesek. Az emberek átverése, segítőkészségük kihasználása nem újkeletű dolog, hiszen a „Social engineering” már a kezdetektől jelen volt és a telefonos csalásokkal (vishing, smishing) kezdődött, de manapság is nagyon gyakoriak. Megjelenik a „script kiddie” elnevezés, ami egy olyan kifejezés, amelyet a számítógépes világban használnak, hogy leírják azokat a személyeket, akik nem rendelkeznek mély szakmai tudással vagy készségekkel a számítógépes biztonság területén, de mégis megpróbálkoznak az illegális vagy kártékony tevékenységekkel vagy más informatikai támadásokkal. [1]

White Hat: A fehér sapkás hackerek vagy más nevükön etikus hackerek olyan számítástechnikai szakemberek, akik főként biztonsági problémákkal foglalkoznak, és munkájuk segítségével a felhasználók biztonságosabban használhatják számítógépieket. A jó etikus hacker vagy másnéven biztonsági tesztelő tudása nem

[1] ORCID iD: 0009-0009-6167-2154

szabad, hogy eltérjen feketesapkás társaitól. Akkor tud megfelelően védekezni egy támadás ellen, ha a támadási folyamatokkal is tisztában van. Egy adott szervezet kiberbiztonsági tesztelésére általában egy szerződés keretein belül kérik fel, amivel igazolhatja, hogy legálisan támadja az adott infrastruktúrát. A támadások sikerességéről egyesével jelentéseket készít és javaslatokat tesz az esetlegesen feltárt sérülékenységek kijavítására.

Black Hat: A feketesapkás hackerek számítástechnikai tudásukat egyértelműen etikátlan módon használják fel. Azért hatolnak be különböző rendszerekbe, hogy azok adatállományát ellopják, megváltoztassák vagy töröljék. A motiváció lehet anyagi érdek, politikai elfogultság, de gyakran a szórakozás is.

Gray Hat: A szürke sapkás hacker a két véglet, a fehér és a fekete között helyezkedik el. Tevékenysége nem mindig törvényes, de általában nem is káros. Úgy hatolnak be különféle rendszerekbe, hogy azok adatállományát nem semmisítik meg, sőt általában a feltörés nyomait is eltüntetik, így a rendszergazda nem is észleli, hogy hálózatát feltörték. Tevékenységük többnyire jószándékú, mégis a törvény szempontjából illegálisnak tekinthető. Általában igyekeznek felhívni egy rendszer gyengeségére a figyelmet. [2]

A második generáció, avagy a kiváló programozó

A 2000-es évek közepétől azonosítható a hackerek második generációja. Fejlett férgeket kezdtek alkalmazni, amelyekkel adathordozók és e-mailek segítségével képesek voltak megfertőzni munkaállomásokat.

Pl.:

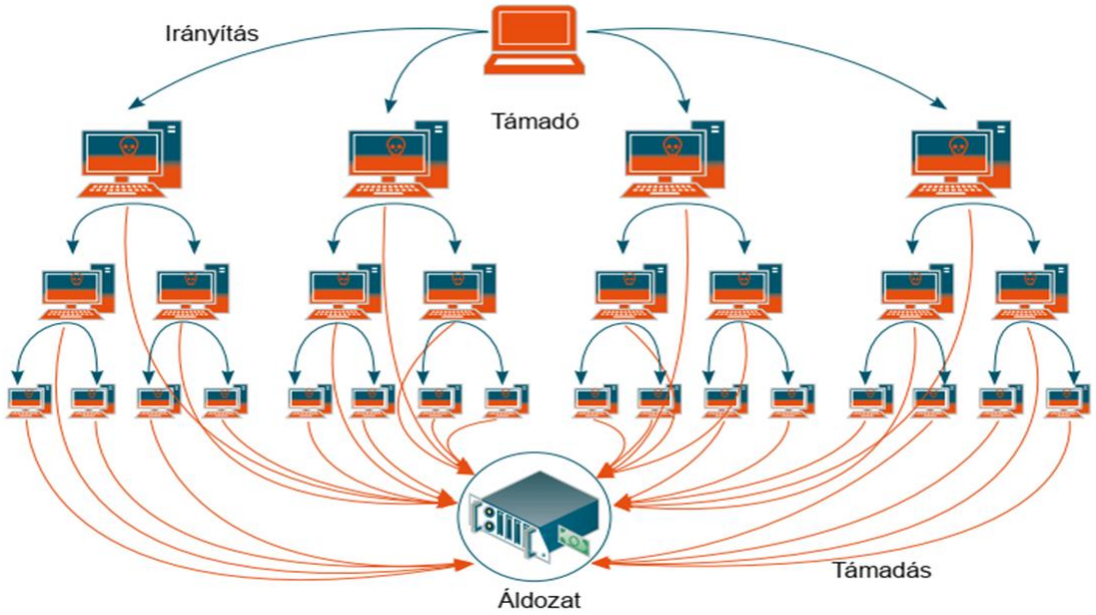
- Sasser (2004) – Olykor a PC-k leállítását, újraindítását blokkolta Ms. Windows XP és Ms. Windows 2000-es gépeken. A fertőzött számítógépeken a Sasser megakadályozta a rendszer leállítását, és a számítógép újraindításával ismét megjelent. Ez a folyamat akadályozta a számítógép használatát, és a fertőzött rendszer instabillá válhatott. A Sasser féreg fejlesztőjét, Sven Jaschan-t 2004 májusában tartóztatták le Németországban. Jaschan egy fiatal programozó volt, aki a fertőzött rendszerekkel okozott kárt, a Sasser féreg elterjedésével vált híressé és széles körű figyelmet kapott a sajtóban és a számítógépes biztonsági szakemberek körében. Ő volt a Blaster nevű féreg készítője is.
- NetSky (2000-es évek) – Tömeges e-mailekben küldte szét magát az áldozatoknak valamint a szükségtelen hálózati forgalommal lassították vagy blokkálták a kommunikációt.

A támadók célja többnyire káresemény okozás vagy az infokommunikáció hátráltatása volt.

A harmadik generáció, összefűzött rendszerek előnyei

A 2010-es évek végén megjelent harmadik generációnál már a motiváció az elismerésről a díjazás felé mozdult el. Megjelentek a botnetek (2. ábra), amelyeket már DDOS támadásokra is alkalmaztak. A bevetett programkódok már jóval fejlettebbek voltak, mint a korábbi generációk által használt programsorok, azonban

még mindig könnyen beazonosíthatónak és kivédhetőnek számítottak.



2. ábra: Botnet működése [3]

A negyedik generáció, az árulkodó nyomok eltüntetése

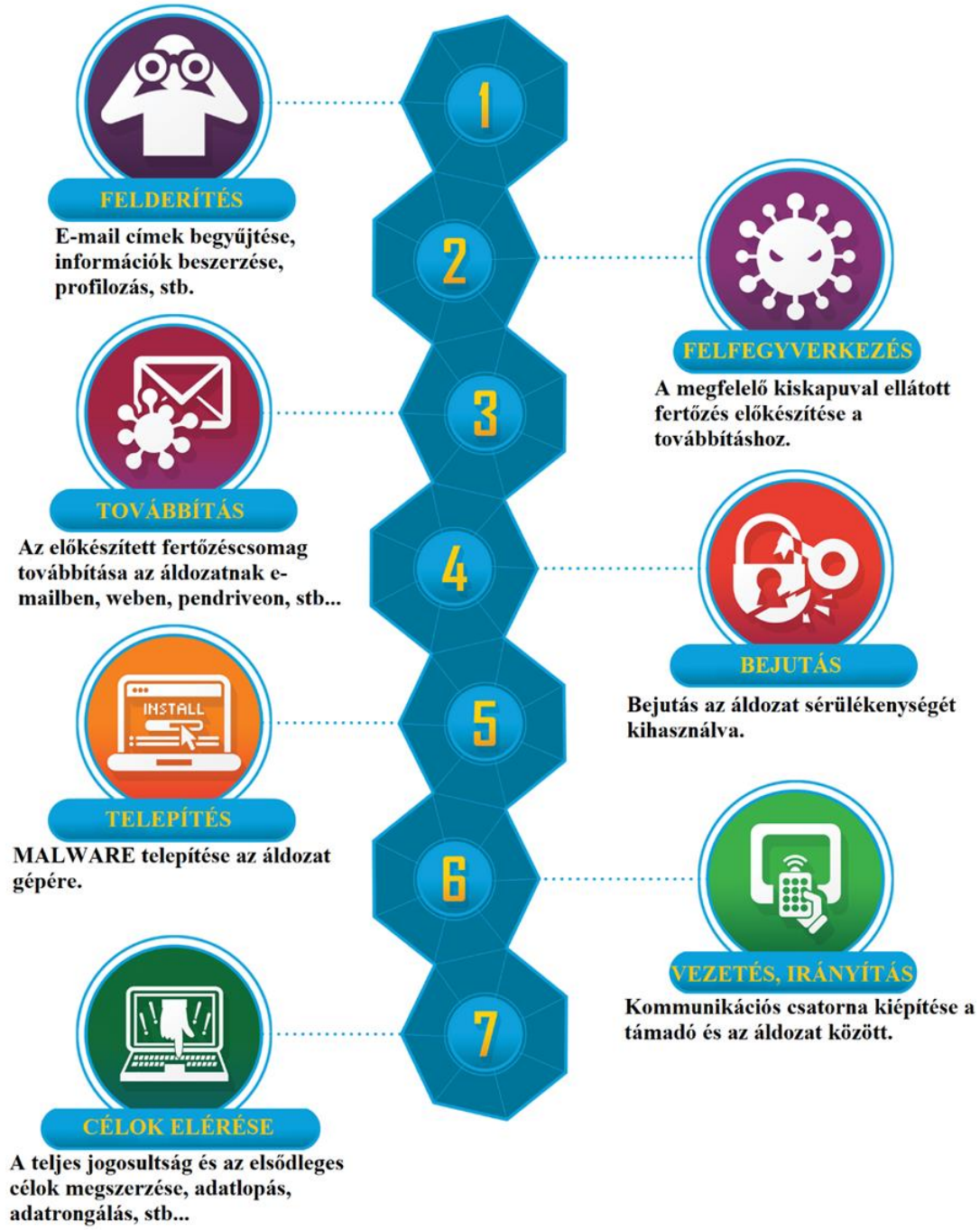
A 2010-es évek utolsó negyedévében a kiberbűnözés professzionális szintre lépett. A kiberűnözők a rosszindulatú szoftvereket elkezdték elrejteni, és egyre jobban megszervezték csoportjaikat. Tapasztalt programozói tudással rendelkeztek, ami sokkal jobb minőségű malware-eket eredményezett. A támadók többnyire saját maguk módosították egyedivé a payload-ot, pontosan tudták, hogy a támadást elősegítő programkód hogyan épül fel és hogyan működik. Egyre nagyobb célpontokat vettek célba, ahonnan több pénzt lehet ellopni. Ez az időszak, amikor a hagyományos maffiák is bekapcsolódtak a játékba.

Az ötödik generáció, elkezdődik a rootkitek világa

Az ötödik és jelenlegi generáció gyakran előre elkészített eszközöket (toolokat) használ a kibertámadásokhoz azért, mert ezek könnyen használhatók, idő- és erőforrástakarékosak, lehetővé teszik gyors támadásokat és tömeges célpontokat, valamint lehetővé teszik a specializációt az adott területeken. Programozói tudásuk nem olyan fejlett, mint a 4. és az azt megelőző generációnak. Minden támadás típusra megvannak a kifinomult eszközcsomagjuk. Az ilyen előre elkészített eszközök elterjedése és nagy hatóereje miatt kiemelten fontos a számítógépes rendszerek hatékony védelme a kibertámadások ellen. Ha valami nem működik, nehezebben rögtönöznek.

Lokheed Martin féle kibertámadási lánc

A támadásokra teljes egészében nem lehet egy általános sémát ráhúzni, azonban a kiberbiztonsági szakmában a legismertebb a Lockheed Martin által kidolgozott kibertámadási folyamat, amely a fentiekhez hasonló részegységekkel rendelkezik (3. ábra).



3. ábra: : Lockheed Martin féle kibertámadási lánc (cyber killchain) [4]

Egy átgondolt kibertámadás felépítése tehát egy összetett folyamat, amely a támadók részéről kitartó erőfeszítést igényel, és egyre nehezebbé válik a technológiai fejlődésnek köszönhetően. Azonban a megelőzés, a védekezés és a legjobb eljárásmódok betartása segíthet a kibertámadások elleni küzdelemben. Fontos továbbá, ha nemcsak a kibertámadás folyamatát, hanem annak a lehetséges taktikáit és technikáit (pl.: MITRE ATT&CK® Matrix) is megismerjük, ugyanis az egyes kibervédelmi célszoftverek ezek alapján tudják beazonosítani az esetleges támadásokat. A biztonsági incidensek dokumentálása kiemelkedően fontos a későbbi tapasztalatfeldolgozás érdekében.

Védelmi intézkedések

Egy általános szervezet infokommunikációs felépítése általában minimum két, jól elkülöníthető szektorra bontható. Ezen szektorokhoz javaslok néhány egyszerű védelmi megoldást az alábbiakban.

1. szektor: Azok a szerverek, amik az internetről láthatóak

Az egyes szerverek egy alhálózatban vannak és kommunikálnak egymással. A bejutás többnyire egy létező rendszersérülékenység segítségével történik.

Javasolt megoldások:

- biztonsági dokumentációk elkészítése és betartatása;
- hálózati szegmentálás (nincs új a nap alatt);
- hardveres illetve szoftveres biztonsági megoldások (IDS, IPS, Firewall);

- ellenőrzött operációs rendszer frissítések alkalmazása;
- képzett személyzet (ahol nem üzemeltetés a cél!!!).

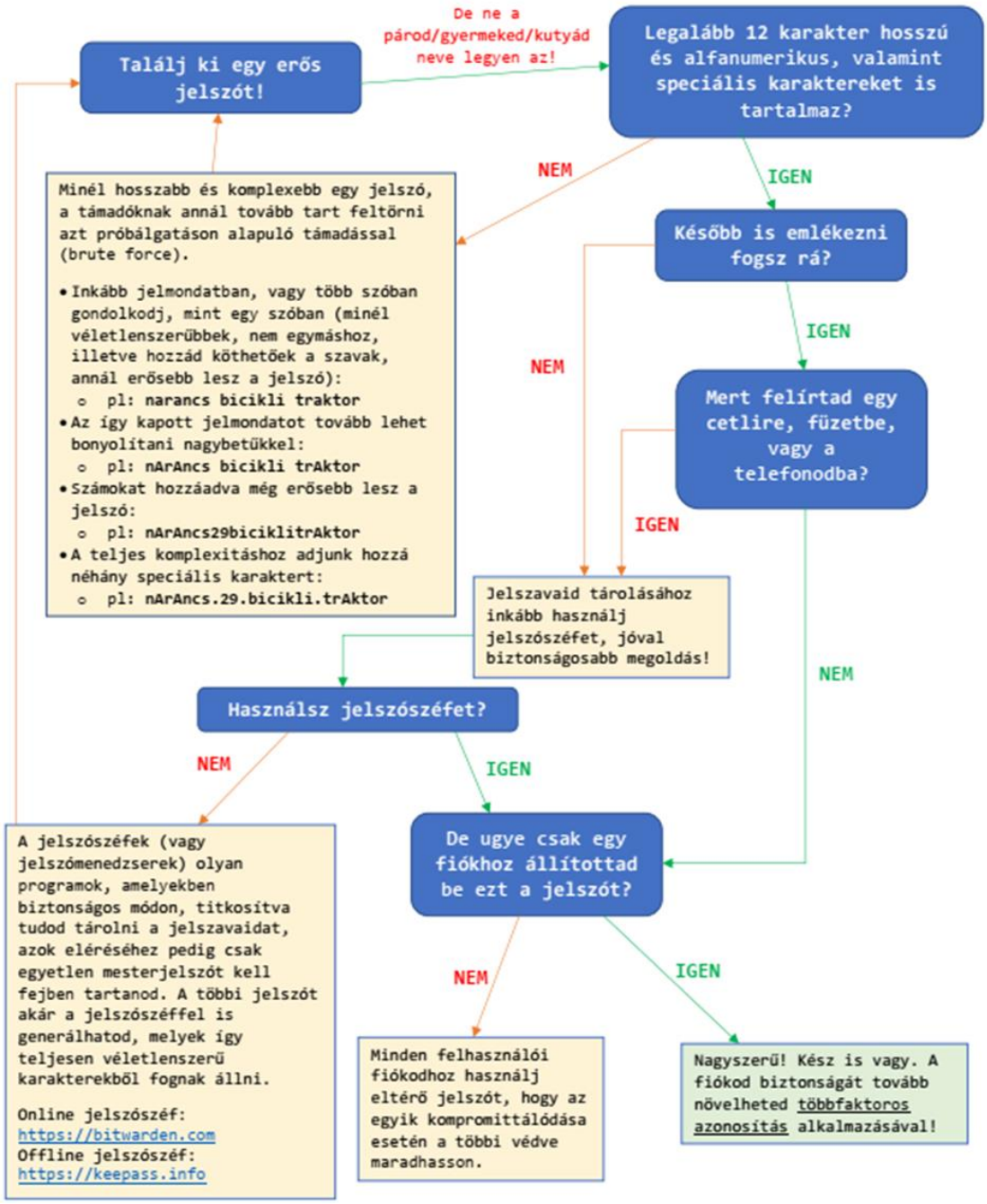
2. szektor: Felhasználói szféra vagy üzemi terület

Általában külön alhálózatot képeznek a szerver szekcióval. A bejutás többnyire phising kampánnyal kezdődik. Ebben az esetben a támadónak mindenképpen el kell érnie, hogy a felhasználó hibázzon. Javasolt megoldások:

- biztonsági dokumentációk elkészítése és betartatása;
- „erős jelszó” használata;
- kiberbiztonsági tudatosító oktatások megtartása (védekezni kell a social engineering ellen).

A felhasználókkal szemben elkövetett csalások jelentős kockázatot jelentenek az egyének személyes adataira és pénzügyi biztonságára, és az ilyen incidensek megelőzése és kezelése kulcsfontosságú a kiberbiztonsági stratégiákban.

Előfordulhat, hogy e-mail címünk, felhasználói nevünk, telefonszámunk vagy jelszavaink is tudtunk nélkül adatszivárgás áldozatává válnak. Ez a legtöbbször úgy lehetséges, hogy az adatbázist, ahol egy adott webhely tárolta a személyes adatainkat, feltörik és az információkat eladják a feketepiacon vagy személyesen élnek vissza vele, ezért javasolt a jelszavainkat gyakorta, akár 30 naponta megváltoztatni. Az „erős jelszó” megválasztásában a 4. ábra nyújthat segítséget. [2]



4. ábra: Erős jelszó [2]

Teljes védelem nincs, a nemzetközi kibergyakorlatok szerepe

A nemzetközi kibervédelmi gyakorlatok rendkívül fontosak az informatikai biztonság és az online védelem szempontjából. Az információs technológiák robbanásszerű fejlődése miatt egyre több személyes és üzleti adatot kezelünk az interneten, így a kibertámadások és a kibertámadók által okozott kár is egyre nagyobb.

A gyakorlatokon szimulálni tudják a különböző kibertámadásokat, a vírusok, férgek, trójaik, adathalász támadások hatásait a teljes infrastruktúrára. Az ilyen támadások következményei súlyosak lehetnek, például adatvesztés, személyazonosság lopás, pénzügyi csalás, vagy akár az egész szervezet megbénulását is okozhatják.

A nemzetközi kibervédelmi gyakorlatok és együttműködések különböző országok, iparágak, vállalkozások és intézmények között segíthetnek az ilyen támadások elhárításában és a károk minimalizálásában. Ezek gyakorlatok általában magukban foglalják a biztonsági szabályok és eljárások kidolgozását és betartását, a biztonsági eszközök telepítését és frissítését, valamint a személyzet oktatását és felkészítését. [5]

Az együttműködés fontos szerepet játszik az online biztonság és a kibervédelem terén, mivel ezek lehetővé teszik az információk és a szakértelem megosztását a különböző szervezetek között, és segítik a megfelelő védelmi eszközök és eljárások kidolgozását és alkalmazását. Az online tér egyre fontosabbá válik az életünkben,

mert számos olyan tevékenységet végzünk az interneten, amelyekben hozzáférünk személyes vagy üzleti információkhoz. Ezért fontos, hogy az online védelemmel kapcsolatos gyakorlatok hatékonyak legyenek, hogy megtanuljuk megvédeni az adatokat a kibertámadásokkal szemben.

Az online világ globális jellegét tekintve a kibervédelmi kihívások nem ismernek határokat, ezért a nemzetközi együttműködés lehetővé teszi az információk és a szakértelem megosztását, valamint a különböző országok és szervezetek közötti erőforrások hatékony felhasználását.

A NATO országain belül a legtöbb kibervédelmi gyakorlatot az észtországi NATO Kibervédelmi Kiválósági Központ (NATO CCDCOE) szervezi, melynek Magyarország is állandó résztvevője. [2]

Számos éles helyzetet szimuláló nemzetközi kibervédelmi gyakorlat van, amik segítenek felkészülni egy esetleges kibertámadásra mind védekezési (blue team), mind támadási (red team) oldalról.

<u>Blue team gyakorlatok:</u>

Pl.: Locked Shields, Cyber Coalition, EDA MilCert… stb.

<u>Red team gyakorlatok:</u>

pl.: Crossed Swords

Összefoglalás

A felnövekvő hacker generációkkal nagyon nehéz tartani a lépést a védelem oldalán, mert ez mindig egy macska-egér harc lesz a jövőben is. Azonban mindig nagyon hasznos megismerni hogyan épülhet fel egy valós kibertámadás, hogy felkészülhessünk az ellene való védelemre.

A kibervédelem szerepe nemzetközi és hazai szinten is kimagaslóan fontos. A védelmet azonban nem szabad csupán a szakemberekre hárítani. Minden felhasználónak tudatában kell lennie az őt érintő esetleges kiberfenyegetettségekkel és meg kell tennie mindent a tudatos kibertér használatának érdekében.

Hivatkozott irodalom

[1] Kibervédelem a bűnügyi tudományokban (Dornfeld L., Gyaraki R., Kiss T., Kovács Z., Nagy Z., Simon B.) Szerk.: Kiss Tibor, Budapest, 2020.

[2] Honvédelmi alapismeretek tankönyv (Almási L., Balog P., Berkecz G., Busa Attila József, Drót L., dr. Eleki Z., Fekete A., dr. Kállai A., Kalmár I., Mihályi L., Nyulászi T., Szűcs P., dr. Tálas P. H., Tóth G., Zentai K.), Zrínyi Kiadó, Budapest, 2023.

[3] MH KIMK – Cyber Academy: I. modul tananyag (Busa A. J., Rácz O., Umhauser B.), Szerk.: Busa Attila József, Szentendre, 2022.

[4] Cyber killchain - https://www.lockheedmartin.com/ (fordította a Szerző), (Letöltve: 2023.03.28.)

[5] Snoj Péter – Katonáink a kibertér biztonságáért, Honvédelem.hu, 2022. március 18.

Ábrajegyzék

Infokommunikáció 2023

Az egyes hacker generációk támadási szokásai és aktuális támadási trendek fejlődése a 2000-es évektől napjainkig

Busa Attila József
MH KIMK, Képzési- és Gyakorlattámogató Osztály,
Kiber Képzési Alosztály
kibervédelmi tanácsos

BRU Infosec Kft.
alapító tag, ügyvezető

Óbudai Egyetem, Biztonságtudományi Doktori Iskola,
1.éves doktorandusz hallgató

2023.12.12.

Vázlat

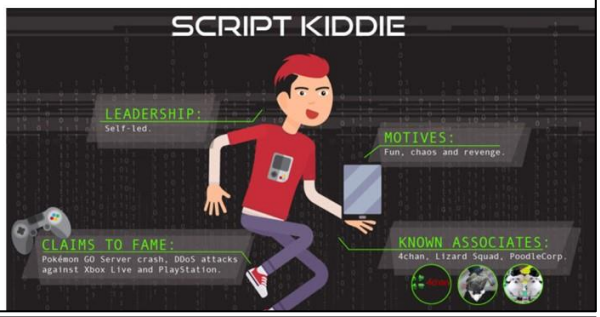
- hacker generációk fejlődésének bemutatása;
- a kialakult kibertámadási lánc;
- ajánlott védekezési javaslatok;
- összegzés;
- kérdések / válaszok

1. Generáció avagy a „hackerek” megjelenése

A 2000-es évek elején a közhiedelemben ők úgy jelentek meg, mint tinédzserek, akik sötét, nyirkos pincékben vírusokat írnak, hogy hírnevet szerezzenek, és megmutassák a világnak, hogy képesek rá.

„Social engineering” már az alapoktól jelen volt és a telefonos csalásokkal (vishing) kezdtek, amik a manapság is nagyon elterjedtek.

„Script kiddie”-k megjelenése.



2. Generáció (2000-es évek közepe)

Olyan férgeket kezdtek alkalmazni, amelyekkel adathordozók és e-mailek segítségével képesek voltak megfertőzni munkaállomásokat.

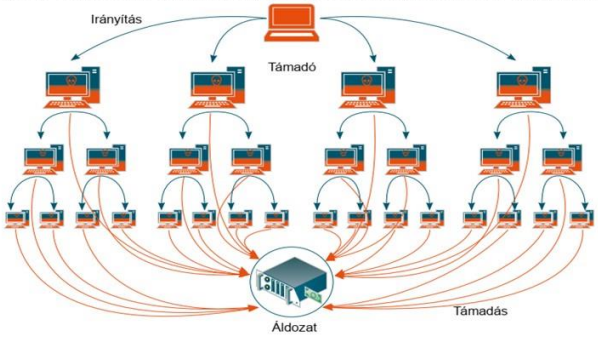
Pl.:

- Sasser (2004) – Olykor a PC-k leállítását, újraindítását blokkolta Ms. Windows XP és Ms. Windows 2000-es gépeken.
- NetSky (2000-es évek) – Tömeges e-mailekben küldte szét magát az áldozatoknak valamint a szükségtelen hálózati forgalommal lassították vagy blokkálták a kommunikációt.

Cél: többnyire káresemény okozás, infokommunikáció hátráltatása.

3. Generáció (2010-s évek eleje)

Ennél a generációnál már a motiváció az elismerésről a díjazás felé mozdult el. Megjelentek a botnetek, melyeket már DDOS támadásokra is alkalmaztak. A bevetett programkódok már jóval fejlettebbek voltak, mint a korábbi generációk által használt programsorok, azonban még mindig könnyen beazonosíthatónak és kivédhetőnek számítottak.

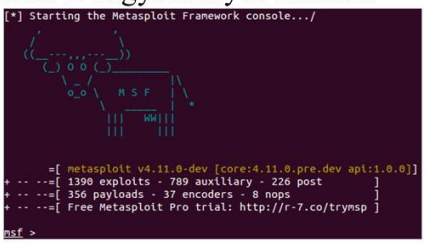


4. Generáció (2010-es évek közepe)

A kiberbűnözés professzionális szintre lépett. A kiberűnözők a rosszindulatú szoftvereket elkezdték elrejteni, és egyre jobban megszervezték csoportjaikat. Tapasztalt programozói tudással rendelkeztek, ami sokkal jobb minőségű malware-eket eredményezett. A támadók többnyire saját maguk módosították egyedivé a payload-ot, pontosan tudták, hogy a támadást elősegítő programkód hogyan épül fel és hogyan működik. Egyre nagyobb célpontokat vettek célba, ahonnan több pénzt lehet ellopni. Ez az időszak, amikor a hagyományos maffiák is bekapcsolódtak a játékba.

CYBER KILL CHAIN

MIMIKATZ



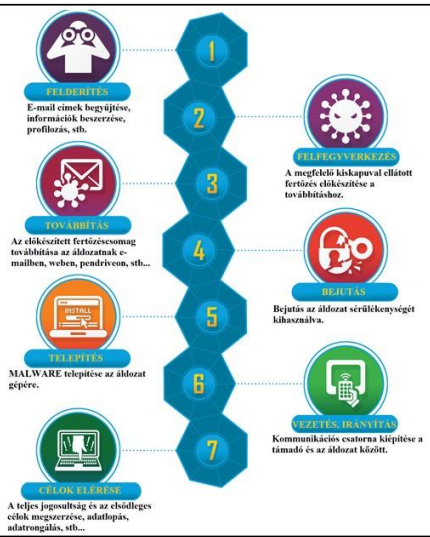
5. Generáció (2010-es évek végétől napjainkig)

Az ötödik és jelenlegi generáció gyakran előre elkészített eszközöket (toolokat) használ a kibertámadásokhoz azért, mert ezek könnyen használhatók, idő- és erőforrástakarékosak, lehetővé teszik gyors támadásokat és tömeges célpontokat, valamint lehetővé teszik a specializációt az adott területeken. Programozói tudásuk nem olyan fejlett, mint a 4. generációnak. Minden támadás típusra megvannak a kifinomult eszközcsomagjuk. Ha valami nem működik, nehezebben rögtönöznek.

Az ilyen előre elkészített eszközök elterjedése és nagy hatóereje miatt kiemelten fontos a számítógépes rendszerek hatékony védelme a kibertámadások ellen.

COBALT STRIKE ADVANCED THREAT TACTICS FOR PENETRATION TESTERS VPNTUNNEL EXPLOIT DATABASE

Lokheed Martin féle kibertámadási lánc



Védekezési javaslatok I.

1. szektor: Szerverek, amik az internetről láthatóak.

Az egyes szerverek egy alhálózatban vannak és kommunikálnak egymással. A bejutás többnyire egy létező rendszersérülékenység segítségével történik.

Javasolt megoldások:

- biztonsági dokumentációk elkészítése és betartatása;
- hálózati szegmentálás (nincs új a nap alatt);
- ellenőrzött operációs rendszer frissítések alkalmazása;
- logolás;
- képzett, személyzet (nem üzemeltetés a cél!!!);
- stb...

Védekezési javaslatok II.

2. szektor: Felhasználói szféra vagy üzemi terület

Külön alhálózatot képeznek a szerver szekcióval. A bejutás többnyire phising kampánnyal kezdődik. Ebben az esetben a támadónak mindenképpen el kell érnie, hogy a felhasználó hibázzon.

Javasolt megoldások:

- biztonsági dokumentációk elkészítése és betartatása;
- kiberbiztonsági tudatosító oktatások megtartása;
- stb...

Teljes biztonság nincs

Számos éles helyzetet szimuláló nemzetközi kibervédelmi gyakorlat van, amik segítenek felkészülni egy esetleges kibertámadásra.

blue side:

Pl.: Locked Shields, Cyber Coalition, EDA MilCert… stb.

red side:

pl.: Crossed Swords

Összefoglalás

A felnövekvő hacker generációkkal nagyon nehéz tartani a lépést a védelem oldalán, mert ez mindig egy macska-egér harc lesz a jövőben is. Azonban mindig nagyon hasznos megismerni hogyan épülhet fel egy valós kibertámadás, hogy felkészülhessünk az ellene való védelemre.

A kibervédelem szerepe nemzetközi és hazai szinten is kimagaslóan fontos. A védelmet azonban nem szabad csupán a szakemberekre hárítani. Minden felhasználónak tudatában kell lennie az őt érintő esetleges kiberfenyegetettségekkel és meg kell tennie mindent a tudatos kibertér használatának érdekében.

Források

- https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (letöltve: 2023.01.13.)
- A figyelemgazdaság átalakulása. Kitől kapjuk a kegyelemlökést? (Bíró Veronika), DigitalHungary, 2022. https://www.digitalhungary.hu/interjuk/A-figyelemgazdasag-atalakulasa-Kitol-kapjuk-a-kegyelemlokest/14003/ (letöltve: 2023.01.13.)
- Kibervédelem a bűnügyi tudományokban (Dornfeld L., Gyaraki R., Kiss T., Kovács Z., Nagy Z., Simon B.) Szerk.: Kiss Tibor, Budapest, 2020.
- MH KIMK – Cyber Academy: I. modul tananyag (Busa A. J., Rácz O., Umhauser B.), Szerk.: Busa A. J., Szentendre, 2022.
- Honvédelmi alapismeretek tankönyv (Almási L., Balog P., Berkecz G., Busa A. J., Drót L., dr. Eleki Z., Fekete A., dr. Kállai A., Kalmár I., Mihályi L., Nyulászi T., Szűcs P., dr. Tálas P. H., Tóth G., Zentai K.), Zrínyi Kiadó, Budapest, 2023.

Kérdések?

Köszönöm a figyelmet!

Szerzőink figyelmébe

Kiadványunk lehetőséget biztosít max. 40 ezer leütés (egy szerzői ív) terjedelemben – *elsősorban: távközlés, híradás, informatika, információvédelem, illetőleg hadtudományi és természettudományi témakörökben* – tanulmányok, szakcikkek magyar és idegen nyelvű megjelentetésére.

A cikknek tartalmaznia kell egy 2-5 soros absztraktot magyar és/vagy idegen nyelven.

A cikkek beküldése e-mailen a hhk_hirado_szakcsoport@uni-nke.hu címre lehetséges. A cikkek leadási határideje: folyamatos (megjelenés évente kétszer).

A megjelentetésre szánt cikkek csak a szerző(k) eddig máshol még meg nem jelent, saját önálló (társszerzők esetében közös) írásműve(i) lehetnek. Az írásművekben lévő idézeteknek meg kell felelniük a szerzői jogról szóló hatályos jogszabályoknak. A megjelentetésre szánt írásművek csak nyílt (nem minősített) információkat és adatokat tartalmazhatnak. Ezek minősített voltát a szerkesztőbizottság nem vizsgálja, ennek felelőssége a cikk szerzőjét terheli.

A szerkesztőbizottság a megjelentetésre szánt írásműveket lektoráltatja. A szerkesztőbizottság fenntartja a jogot, hogy a megjelentetésre szánt és megküldött írásművet – *külön indoklás*

nélkül - megjelenésre alkalmatlannak ítélje. Az ilyen cikkeket nem küldi vissza, és nem őrzi meg.

A kiadványban lehetőség van idegen nyelvű cikkek megjelentetésére. Az idegen nyelven megjelentetésre szánt írásművek nyelvi lektorálása a szerzőt terheli.

Minden kézirathoz elektronikusan is mellékelni kell egy kitöltött "Kéziratbeküldési űrlap"-ot, és egy "Copyright átruházási űrlap"-ot. Mindkét űrlapot ki kell nyomtatni és alá kell írni (többszerzős cikk esetében minden szerzőnek!), majd a kinyomtatott és aláírt űrlapokat faxon (fax szám: +36-1-432-9025), vagy postai úton levélben (levélcím: Hírvillám Szerkesztőség, 1581. Budapest Pf.: 15.) is meg kell küldeni a szerkesztőségnek. Ezek hiányában a cikkeket a szerkesztőség nem lektoráltatja és nem jelenteti meg!

Az űrlapok a szerkesztőségnél szerezhetők be.

Megjelent az NKE HHK Híradó Tanszék gondozásában

www.comconf.hu
www.puskashirbaje.hu

HU ISSN 2061-9499

***

NKE HHK Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf. 15.
+36 1 432 9000 (29-407 mellék)