HÍRVILLÁM

A NEMZETI KÖZSZOLGÁLATI EGYETEM
Híradó Tanszék szakmai tudományos kiadványa

SIGNAL Badge

Professional journal of Signal Departement
at the University of Public Service

2023

Nemzetközi Katonai Információbiztonsági Konferencia

tudományos szakmai
konferencia

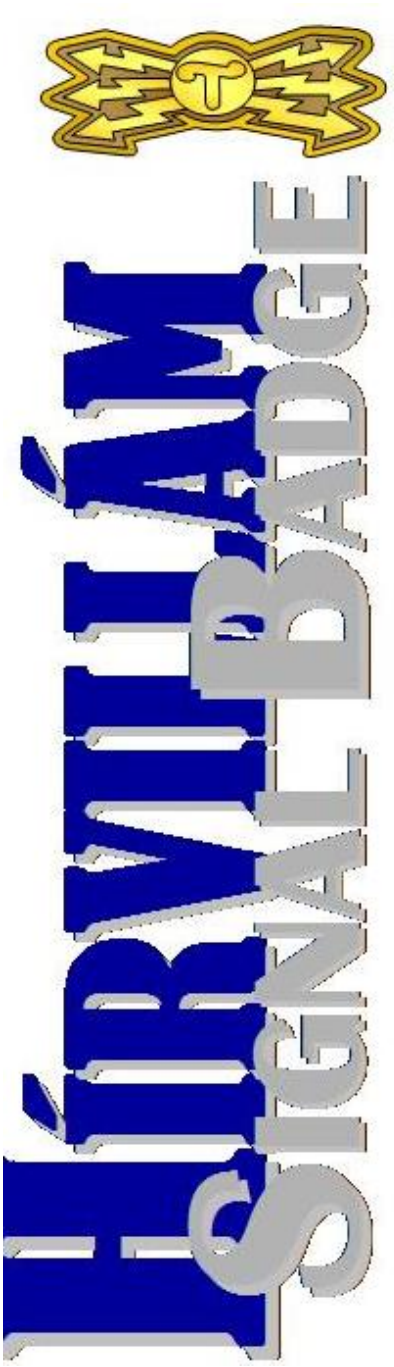
Konferencia kiadvány

2023. április 27.

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



Felelős kiadó/Editor in Chief
Dr. Tóth András

A konferencia szervezőbizottsága, illetve a kiadvány szerkesztőbizottsága/Editorial Board

A konferencia szervezőbizottságának társelnökei/ Co-chairs of the conference organising committee
Dr. Kerti András
Dr. Négyesi Imre
Dr. Tóth András

Főszerkesztő/Co-ordinating Editor
Dr. Tóth András

Tagok/Members
Busa Attila
Dr. habil. Farkas Tibor
Dr. Jobbágy Szabolcs
Knapp Gábor
Dr. Magyar Sándor
Megyeri Lajos
Oláh István
Prof. Dr. Rajnai Zoltán
Szűcs Attila

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!

Az NKE Hadtudományi és Honvédtisztképző Kar Híradó Tanszéke a Magyar Honvédség Parancsnoksága Infokommunikációs és Információvédelmi Csoportfőnökségével és a Hírközlési és Informatikai Tudományos Egyesület Információbiztonsági Szakosztályával együttműködve „Nemzetközi Katonai Információbiztonsági Konferencia" címmel szervezett tudományos konferenciát 2023. április 27-én a Magyar Honvédség Rekreációs Kiképzési és Konferencia Központban Balatonakarattyán.

A konferencia alapvető célja egy évente megrendezésre kerülő tudományos szakmai fórum biztosítása a kutatási eredmények bemutatása, ismeretterjesztés, valamint kapcsolatépítés céljából.

Jelen kiadványban a szerkesztőbizottság az egyes előadásokból készített korreferátumokat gyűjtötte össze, melyeket nagyon nagy örömmel bocsájt rendelkezésre a Kedves Olvasóknak.

Budapest, 2023. április 27.

Dr. habil. Kerti András
a Szerkesztőbizottság
elnöke

Kassai Károly[1]: Változások, fejlődési lépések a kibertérben (Átfogó jellegű gondolatok, 2023)

A „biztonságos kibertér" állapot elérése és megőrzése komplex[2] szemléletet, folyamatos tanulást, fejlesztést, koordinációt és információcserét igényel. Egy-egy szervezési elem, vagy történés kiemelése, megvilágítása, előtérbe helyezése hamis biztonságtudat kialakulás támogatására alkalmas.

Ennek megfelelően e gondolatok a legfontosabb, publikusan megismerhető információk mentén segítik annak megismerését és megértését, hogy milyen hatások érik napjainkban a katonai kibertérben zajló képességfejlesztést, melyek a közeljövő kihívásai.

Nemzetközi vektorok

A ***2022-es Madridi Csúcsértekezlet*** megállapította, hogy a Szövetség ellen irányuló fenyegetések erősödnek (kiber-, űr-, hibrid és egyéb aszimmetrikus fenyegetések), ami rendszer szintű versenyt jelent a nemzetközi rendre irányuló fenyegetésként. Emiatt a szövetségesek növelik a kiber- és hibrid fenyegetésekkel szembeni ellenálló képességet, erősítik az interoperabilitást.[3]

A ***2022-es NATO Stratégiai Koncepció*** szerint a szövetségesek tovább erősítik haderejük kollektív készenlétét, reagálóképességét,

[1] ORCID iD: 0009-0009-9398-6158

[2] A kibertérben szükséges fejlesztésekhez is használni kell az EU, NATO által is alkalmazott fejlesztési (un. DOTMLPF-I) keretrendszert.

[3] Madrid Summit Declaration in Madrid 29 June 2022, 6, 9. p.

bevethetőségét, integrációját és interoperabilitását. A hatékony elrettentés és védelem a kulcsa a világűr és a kibertér biztonságos használatának és a korlátlan hozzáférés biztosításának. A Szövetség *elismeri nemzetközi jog alkalmazhatóságát és előmozdítja a felelős magatartást a kibertérben és az űrben*.[4]

A 2022-es EU Kibervédelmi Politika szerint a támadások jelzik a fizikai és digitális infrastruktúrák kölcsönös függőségét. A tagállamoknak növelni kell a teljes spektrumú kibervédelmüket,[5] és képességekkel kell rendelkezni a támadások korai szakaszban történő felismerésére.[6] *Ki kell alakítani a katonai eseménykezelő központok műveleti hálózatát* (MICNET).[7]

Az EU-nak és a tagállamoknak erősíteni kell a katonai vezetési és irányítási struktúrákat (különösen a válságkezeléshez szükséges politikai-katonai konzultációkhoz). A kérdés megoldását célozza az *EU Nagytávolságú Műveleti Hálózat továbbfejlesztése*.[8]

[4] NATO 2022 Strategic Concept; 15, 20, 22, 24 és 25. p.

[5] Beleértve az „aktív védelmi képességet" is. A Politika nem ad fogalmi meghatározást az „aktív védelem" kifejezésre.

[6] A Politika nem világítja meg a „kiberbiztonság (cybersecurity)" és a „kibervédelem (cyber defence)" fogalmak tartalmát, így a szóhasználatot figyelve csak következtetni lehet arra, hogy az első esetben a polgári a második esetben katonai tartalmú fogalomról van szó.

[7] MICNET: milCERT Network. Ez egyben támogatja a fenyegetésekre történő erőteljes és összehangolt reagálást, a képzéseket és a hosszútávú igények azonosítását.

[8] EU Operation Wide Area Network (EU OpsWAN)

Kiemelt fontosságú az új technológiák alkalmazása (pl. mesterséges intelligencia, titkosítás, kvantum számítástechnika).[9]

A kiberbiztonság és kibervédelem kiemelt együttműködési terület a NATO és az EU között, ahol folytatódik a műveleti alkalmazással kapcsolatos eszmecsere, a koncepciók és doktrinák egyeztetése. *Mindkét fél törekszik az eseménykezelő szervezetek együttműködésének erősítésére*.

A Politika következtetésként az EU szervek felszólítják a tagállamokat, hogy *dolgozzák ki a kibervédelmi politika vonatkozó szempontjait.*[10]

2022 decemberi megjelenéssel az ***EU Hálózat és Információbiztonsági Irányelv*** (NIS2 Directive) [11] az elektronikus információbiztonság, míg az ***EU Kritikus Szervezetek Rezilienciája Irányelv*** (CER Directive)[12] a kritikus infrastruktúrák üzemeltetése területén képez megújított követelményeket.

[9] E mellett a poszt kvantum rejtjelzésbe történő beruházás is kiemelten fontos a védelmi rendszerek működőképessége érdekében.

[10] Az EU Kibervédelmi Politikája, JOIN(2022) 49 final p. 2, 4-7, 9-12, 15, 19, 21-22 és 24.

[11] DIRECTIVE (EU) 2022/2555

[12] DIRECTIVE (EU) 2022/2557

Nemzeti rezgések

Hazánk rendelkezik Nemzeti Biztonsági Stratégiával (2020)[13] és Nemzeti Katonai Stratégiával (2021),[14] melyeket a Nemzeti Kiberbiztonsági Stratégia (2013)[15] és a Nemzeti Hálózatbiztonsági Stratégia (2018)[16] valamint ennek végrehajtását szolgáló Intézkedési Terv (2019)[17] egészít ki szakpolitikai eszközként. *Nemzeti szinten várható a kibertér biztonsággal kapcsolatos kérdések legalább részbeni újragondolására*.

A 2023-ban hatályba lépett ***védelem és biztonság összehangolásáról szóló törvény***,[18] eredményeképpen új követelmények megjelenése várható, ami a válságkezelés területén vélhetően érinti a honvédelmi és katonai nemzetbiztonsági feladatokat is.

Honvédelmi szakmai mozzanatok

2022 decemberében hosszú előkészítés után megjelent ***a honvédelmi szervezetek általános elektronikus információbiztonsági követelményeinek meghatározásáról szóló miniszteri utasítás***[19] a honvédségi szervezetek egységes

[13] 1163/2020. (IV. 21.) Korm. határozat
[14] 1393/2021. (VI. 24.) Korm. határozat
[15] 1139/2013. (III. 21.) Korm. határozat
[16] 1838/2018. (XII. 28.) Korm. határozat
[17] A hálózati és információs rendszerek biztonságára vonatkozó Stratégia végrehajtásának 2020-2022. évekre vonatkozó intézkedési terve
[18] 2021. évi XCIII. törvény
[19] 53/2022. (XII. 28.) HM utasítás

szemléletű és teljeskörű biztonsági menedzsment feladatok támogatása érdekében.[20]

2023 elején az érintett szakmai szervezetek együttműködésének eredményeképpen megjelent a ***honvédelmi ágazat elektronikus információbiztonsági eseménykezelést szabályozó miniszteri utasítás***.[21]

Szintén 2023 elején jelent meg a ***kiberbiztonsági termékek tanúsításával kapcsolatos alapvető követelményeket tartalmazó honvédelmi szabályozás***.[22] A rendeletek az EU kiberbiztonság erősítését célzó terméktanúsítás végrehajtásaként hazánkban is megjelenő – polgári és honvédelmi területekre tagolt – tanúsítási követelmény honvédelmi területét szabályozzák.

2022-ben jelentős szervezeti változás a Magyar Honvédség Parancsnoksága helyett a Honvéd Vezérkar, alárendelt szervezetként az MH Kiberműveleti Parancsnokság megjelenése, alárendeltségben az MH Kiber és Információs Műveleti Központtal. A Honvéd Vezérkaron belül az információvédelmi kérdésekért az új szervezeti elemként megalakult Információ Védelmi Iroda felelős.

[20] Az utasítás a korábbi, a honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról szóló 3/2012. (I.13.) HM utasítást váltotta fel.

[21] 3/2023. (II. 24.) HM utasítás a honvédelmi ágazati elektronikus információbiztonsági eseménykezelés rendjéről

[22] 1/2023. (I. 12.) és 2/2023. (I. 12.) HM rendeletek

Irányok, várható kihívások

Szakmai szempontból kiemelt kérdés a Nemzeti Kiberbiztonsági Stratégia sürgősséggel történő rendezése, benne a polgári, honvédelmi és katonai nemzetbiztonsági szempontok összehangolása. Kiegészítő feladat lehet *a nemzetközi példákban már látható Kibervédelmi Stratégia kérdéseinek komplex vizsgálata*. A végrehajtást biztosító törvény és végrehajtási rendeletek felülvizsgálata során érdemes vizsgálni a jelenlegi, elektronikus információbiztonsági [23] fókuszú törvény mellé egy *kifejezetten „kibervédelmi" célú jogszabályi keretet.*

2023 júliusában esedékes a NATO Vilniusi Csúcstalálkozó, melyen várható a korábbi eredmények megerősítése, esetlegesen kiegészítésekkel. A NATO főtitkár 2022 decemberében a NATO Kibervédelmi Kötelezettségvállalás Konferencián Rómában kérte a nemzeteket a kibervédelmi képességek további erősítésére,[24] ami jelezheti a *Kötelezettségvállalás*[25] *áttekintését vagy átdolgozását*, ami egyben nemzeti szinten is feladatokat eredményezhet. A NATO Madridi Csúcstalálkozó egyik eredménye az önkéntes, nemzeti

[23] A törvény a közbeszédben gyakran „Kiberbiztonsági Törvényként" említett, minden tartalmi alap nélkül.

[24] Keynote address by NATO Secretary General Jens Stoltenberg at the NATO Cyber Defence Pledge Conference in Italy

[25] A NATO Kibervédelmi Kötelezettségvállalás (Cyber Pledge) hét kérdéskörre és e mellett évente megjelenő „fókusz területre" bontva éves gyakorisággal mutatja a nemzetek kiber képességeit, a változásokat és a tervezett célokat. (Cyber Defence Pledge, 2016. 07. 08.)

eszközök felhasználásával történő *virtuális gyorsreagálású kiber képesség*[26] kialakítása, ami további nemzeti feladatokat jelenthet.[27]

A fenti, stratégiai szintű feladatok mellett technikai szinten *további lépések szükségesek a honvédelmi célú elektronikus információs rendszerek kibervédelmének megerősítése érdekében* – kiemelten kezelve a beszállítói lánc biztonságot, a teljes életút szemléletet és az új technológiákban rejlő lehetőségeket és fenyegetéseket. Aktuális feladat a honvédelmi szervezetek számára az eseménykezelésre vonatkozó miniszteri utasítás végrehajtása, ami pontosítási, illetve szabályozási feladatokat jelent.

A jogszabályok követelményeinek teljesítése mellett szükség van a kibervédelmi kérdéseken túlmutató képességfejlesztésre is, ami technikai szempontok mellett felveti a művelettervezési és irányítási kérdések részletes szabályozását, a kibertér műveleti szaktevékenységek katonai műveletekbe történő teljes integrálását. A NATO Kiberműveleti Doktrína[28] hároméves, ami jelzi egy várható felülvizsgálat kezdetét, melynek lehetnek nemzeti vonzatai is. Kifejezetten nemzeti katonai kihívásnak kell tekinteni a kibertér műveletekre vonatkozó pontos terminológia kialakítását, mert a tartalmi ismeretek nélküli megfogalmazások [29] használatával lehetetlen helyesen kommunikálni, folyamatokat kialakítani.

[26] virtual rapid response cyber capability
[27] Madrid Summit Declaration in Madrid 29 June 2022, 10. p.
[28] NATO AJP 3.20 Cyber Operations Doctrine
[29] Példa erre a kiberbiztonság, kibervédelem, offenzív műveletek, aktív védelem kifejezések pontatlan alkalmazása vagy az elrettentés kibertérre történő szűkítése.

Összefoglalás

A fentiek rámutatnak, hogy a kiber képességek fejlesztése összetett feladatrendszer, erős technikai alapokkal, illetve információs szükséglettel.

Az időprés, a fokozott elvárások mellett tudomásul kell venni a makacs tényt, hogy jogi megalapozás és szabályozás nélkül nem lehet működőképes, hiteles és jogilag elfogadható képességet kialakítani és fenntartani.

Mindezekhez pontos tervezés, türelem és a megfelelő kifutási idő szükséges – amennyiben hiteles képesség rendszerbe integrálása a végső célkitűzés.

Felhasznált irodalom

1/2023. (I. 12.) HM rendelet a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsítás keretében fizetendő igazgatási szolgáltatási díjról

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról

1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról; A hálózati és információs rendszerek biztonságára vonatkozó

Stratégia; https://nki.gov.hu/wp-content/uploads/2020/11/Stratégia-a-hálózati-és-információs-rendszerek-biztonságára.pdf

2/2023. (I. 12.) HM rendelet a hadiipari kutatás, fejlesztés, gyártás és kereskedelem területén megfelelőségértékelő szervezetek által teljesítendő követelményekről

2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról

3/2012. (I.13.) HM utasítás a honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról

3/2023. (II. 24.) HM utasítás a honvédelmi ágazati elektronikus információbiztonsági eseménykezelés rendjéről

53/2022. (XII. 28.) HM utasítás a honvédelmi szervezetek általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályokról

A hálózati és információs rendszerek biztonságára vonatkozó Stratégia végrehajtásának 2020-2022. évekre vonatkozó intézkedési terve; 2020- 1. 1. F - 2015-2019.kormany.hu

Cyber Defence Pledge, 2016. 07. 08. https://www.nato.int/cps/en/natohq/official_texts_133177.htm DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No

910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/ECKeynote address by NATO Secretary General Jens Stoltenberg at the NATO Cyber Defence Pledge Conference in Italy https://www.nato.int/cps/en/natohq/opinions_208925.htm

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

Madrid Summit Declaration Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022 https://www.nato.int/cps/en/natohq/official_texts_196951.htm

NATO 2022 Strategic Concept

Változások, fejlődési lépések a kibertérben

(Átfogó jellegű gondolatok, 2023)

B.akarattya, 2023. 04. 27.

Dr. Kassai Károly ezredes

Tartalom

- Nemzetközi jelenségek
- Nemzeti követelmények
- Honvédelmi helyzet, követelmények
- Várható terhelések

- A „biztonságos kibertér” állapot elérése és megőrzése komplex, DOTMLPF-I szemléletet, folyamatos tanulást, fejlesztést, koordinációt és információcserét igényel!
- Egy-egy elem kiemelése, megvilágítása, előtérbe helyezése hamis biztonságtudat kialakulás támogatására alkalmas!

Nemzetközi vektorok

- **NATO Stratégiai Koncepció** (2022), várható vilniusi fejlemények (2023)
  - NATO Cyber Pledge vitalizálása 7 év után (várható EU-s lépés is…)
  - NATO kezdeményezés (2022): Virtual Cyber Incident Support Capability - VCISC
  - NATO Defence Capability Survay (2023) feladat kezelése
- **EU NIS2 Directive** megjelenése (2022) és követelményei
  - Új Nemzeti Kiberbiztonsági Stratégia kiadása, + ideiglenes nemzeti Intézkedési Terv
  - Nemzeti szakpolitikák kiadása, jogszabályok harmonizálása
- **EU Critical Resilience Act** megjelenése (2022) és hatásai
  - Nemzeti ellenálló képesség kérdéskör kezelése (Vbö)
- **EU Cyber Defence Policy** megjelenése (2022) és hatásai
  - Miben szükséges a követelményeket átvezetni?

Nemzeti rezgések

- **NBS (2020) – NKS (2021) – NKBS (2013) háromszög feszülései**
  - Az új nemzetközi követelményekre reagálni kell
  - Biztonsági környezet radikális változásai (Nem csak a háború!)
- **Vbö tv. követelményei** szerint alakuló keretrendszer
  - Nemzeti Eseménykezelő Központ megalakulása
  - Nagy léptékű és mennyiségű követelmény várható megjelenése
- **Hjt megújított tartalmú megjelenése (2023 vége?)**
  - Kibertér, kiberműveletek, kiber erő (benne ügyeletes parancsnok), alkalmazási körülmények

Honvédelmi szakmai mozzanatok

- **Elektronikus információbiztonsági követelmények**
  - 53/2022 (XII. 28.) HM utasítás ☺ (a nemzeti követelmények végrehajtása érdekében…)
  - Megújul-e a HM Kibervédelmi Szakmai Koncepció (2013)?
- **Honvédelmi ágazati szintű eseménykezelés, sérülékenységvizsgálat és hatósági szakfeladatok**
  - A működési keretet leképező HM utasítás (15/2017) pontosított ☺
- **Honvédelmi ágazati eseménykezelés központi szabályozása**
  - 3/2023. HM utasítás ☺ >> aktuális feladat a HVK szintű szabályozás kiadás …
- **Kibertanúsítás követelményeinek lefektetése**
  - 1/2023 és 2/2023. Korm. rendeletek ☺
  - Várható törvény részletes követelményekkel (1-3 szintű termékek)

Szervezeti átalakulás

- **HM szervek irányító szerepe**
  - Védelempolitika, jog, nemzetközi együttműködés, védelemigazgatás, gazdasági tervezés
  - HM szintű szakfeladat koordinálás, irányítás
- **MHP >> HVK**
  - HVK HICSF és HVK IVI (elkülönült szervezeti és szakmai irányítási feladatok)
- **MH KIBP és MH KIMK**
  - Felkészülés az MH KIMK „IOC” állapotra
- **Példa nélküli működési struktúra**
  - új szituáció = a szakmai érettség tesztelése
- **Személyi változások kezelése**

Irányok

- **Nemzeti szintű szakfeladatokban részvétel**
  - Nemzeti stratégia, jogszabály változások menedzselése **(civil, katonai és katonai nemzetbiztonsági feladatok összehangolása, Nemzeti Kiberbiztonsági Koordinációs Tanács)**
    - Benne: HM **sportügyi** feladatrendszer kezelése
    - „Kibervédelmi Stratégia" és „Kibertörvény" kialakítás?
    - **„Position paper in cyberspace"** kiadása: nemzeti viselkedés deklarálása a kibertérben
  - Kritikus infrastruktúra fejleményekben való részvétel
    - Várható változások és honvédelmi érdekű létfontosságú infrastruktúra menedzselés
- **Elektronikus információvédelem/információbiztonság és kiberbiztonság/védelem és kibertér műveletek fogalmi és tartalmi tisztázása**
  - Műszaki, szervezeti, terminológiai és eljárásbeli kérdések megoldása
    - Kibertér művelet: pontosabban, mint „a katonai mozgásszabadság biztosítása a kibertérben"
  - Tapasztalat: offenzív művelet ≠ támadás megszakítás ☺

Irányok 2

- **Várható hadműveleti típusú feladatok**
  - Műveleti vezetési rend >> új a szervezeti struktúra + „kiber C2"
  - Művelettervezés és vezetés >>> COPD v3 NATO - nemzeti csatlakozó felület kialakítása
    - **= katonai művelettervezésbe és irányításba történő teljes integrálás**
  - CRMS és NIGY folyamatos fejlesztése >> benne kiber
  - Haderőnemi kérdés megoldása (szárazföld és légierő)
  - „Kiber elrettentés" kifejezés szükségességének tisztázása
- **Doktrinális kérdések:** NATO AJP 3.20 felülvizsgálat 2023-ban
  - MH Kibertér Műveleti Doktrína későbbi hangolása
  - + Magasabb szintű nemzeti doktrínákban a kibertér műveleti kérdések pontos, értelmezhető megjelenítése = *következetesség és láthatóság*!

Irányok 3

- **Technikai fejlesztési feladatok**
  - EU PESCO CTIRISP és CIDCC projektek, EU EDA MICNET projekt
  - MN MISP továbbfejlődés és NATO VCISC kezdeményezés kezelése
  - Korai előrejelző rendszer ágazati szintű kialakítása (jogi megalapozás és lépcsőzetes fejlesztés)
  - Nemzeti folyamatokban való részvétel (pl. **„nemzeti platform"** a kiberügyek összehangolására)
  - LS 23 TAFE
  - **ÁLTALÁNOSSÁGBAN: rendszerek kibervédelmének erősítése!**
    - Benne: **eseménykezelés, sérülékenységvizsgálat vagy hatósági eljárás miatti technikai feladatok…**
    - Külön figyelmet igényel a **beszállítói lánc biztonság**, az **életút** követő szemlélet és az **új technológiák alkalmazása** (AI, kvantum, OTrust)

Összefoglalva

- Jogi megalapozás és szabályozás nélkül nincs képesség!
- Összetett feladatrendszer, erős technikai alapokkal és információs igénnyel!
- Évek, türelem szükséges a hiteles kiber képességekhez!

Köszönöm a megtisztelő figyelmet!

Biztonságos Kiberteret!

Busa Attila József: A digitális információbiztonság alapja: A megfelelő kibertudatosság

1. ábra: Kibertudatossági alapismeretek

A kibervédelem helye, szerepe a honvédelemben

A kibervédelem egyre fontosabb szerepet tölt be a modern hadviselésben, és a honvédelem körében is egyre növekvő jelentőséggel bír. A digitális világban az információ gyűjtése, tárolása és átvitele kritikus fontosságú, és az online térben eltöltött idő számos veszélyforrást és fenyegetést jelent az államok és a katonai szervezetek számára.

A nemzeti kibervédelem célja az állam és a katonai szervezetek információs rendszereinek védelme a kiber-bűnözők, a hackerek és az idegen államok kémkedése ellen. A digitális világban az

információ olyan értékes eszköz, ami a hadviseléshez hasznos lehet az összes konfliktusban, belföldi vagy nemzetközi szinten egyaránt. A kibertámadások, adatlopások, vírusok és más ártalmas programok nagy károkat okozhatnak az államok és a katonai szervezetek, illetve a nemzetbiztonsági szervek számára, továbbá az innováció és a tudomány terén egyaránt.

Az egyre módszeresebb támadások, mint például az államilag szponzorált hackerek vagy a kiberterrorizmus, az államok védelmi rendszereinek állandó innovációjára kényszerítik a nemzeti és katonai szervezeteket és így a honvédelmi rendszereket is. A kibertámadások potenciálisan veszélyeztetik az ország gazdasági infrastruktúráját, erőforrásait, azokat az adatokat és folyamatokat, amelyek a nemzeti biztonság szempontjából kritikusak.
A kiberbiztonsági szakértők azon dolgoznak, hogy a katonai szervezetek és az állam igényeinek megfelelően kiberbiztonsági stratégiákat dolgozzanak ki (lásd a 2012/CLXVI. törvény), hogy megvédjék az ország létfontosságú rendszerelemeit. A kiberbiztonsági szakembereknek ellenőrzésük alatt kell tartaniuk az információ összes kulcsfontosságú pillérét, és meg kell védeniük a katonai és állami szervezetek információit.

Bevezető gondolatok

A biztonság hétköznapi értelemben a veszélyektől mentes, zavartalan állapotot jelenti. Az informatikai rendszerek esetében a legfontosabb a digitális adatok biztonságát megvalósítani. Ebben az esetben az informatikai rendszerelemek biztonságáról beszélünk,

ami nem egyezik az információbiztonság fogalmával. Tágabb értelemben az informatikai biztonság részelemét képezi az információbiztonságnak, amely magának az információnak (digitális vagy kézzel fogható) a védelmét jelenti. Az információbiztonság megvalósultnak tekinthető, ha teljesül a bizalmasság, sértetlenség és rendelkezésre állás elve.

A bizalmasság elve azt jelenti, hogy az információkat bizalmasan kell kezelni, és csak azoknak kell hozzáférést biztosítani, akiknek erre jogosultságuk van. A sértetlenség elve teljesül, ha az információk pontosnak, teljesek és megbízhatóak maradnak az adatkezelés során. A harmadik elv a rendelkezésre állás vagy más néven az elérhetőség elve. Az információknak és adatoknak elérhetőnek kell lenniük azok számára, akiknek megfelelő jogosultságuk van hozzá.

A mindennapokban az informatikai védelmet vagy IT védelmet egyre inkább felváltja a kibervédelem fogalma, ami valójában a kibertér védelmét jelenti.

„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információ rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül

azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett."[1]

Információbiztonsági alapfogalmak

Információbiztonság: Az információk emberi vagy gépi úton formalizált halmazának bizalmasságát, sértetlenségét és rendelkezésre állása.

Informatikai biztonság: Az információs rendszerekben tárolt adatok és a feldolgozáshoz használt hardveres és szoftveres erőforrások biztonsága.

Adatbiztonság: A számítógépes rendszerekben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megteremtése.

Adatvédelem: A személyes adatok jogszerű kezelésének, az érintett személyek védelmét biztosító alapelveknek és módszereknek az összessége.

Szakhatóságok

Az 531/2017. (XII. 29.) Korm. rendelet mellékletének 10. táblázat 44/A. pontja szerint Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (továbbiakban NKI) látja el Magyarországon a hatósági, biztonságirányítási, sérülékenység-vizsgálati feladatokat

[1] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

alapvetően az állami és önkormányzati szervek, valamint a létfontosságú rendszerek és rendszerelemek vonatkozásában.[2,3]

A honvédséget illetően jelenleg a Katonai Nemzetbiztonsági Szolgálat (KNBSZ) a felelős el a fent említett szakhatósági feladatokért (3/2016. (I. 22.) HM utasítás).

Személyes adatokat érintő incidensek

A kiberbiztonság szempontjából személyes adatokat érintő incidensnek számít bármely olyan eset, amelyben az egyénnek az interneten keresztül továbbított vagy tárolt személyes adatai veszélybe kerülnek vagy illetéktelenek számára elérhetővé válnak.

Adatlopás: az illetéktelenek kiberbűnözők vagy jogellenes adatgyűjtők által ellopott személyes adatok, például név, születési dátum, cím, e-mail cím, jelszó, bankkártya adatok, stb.

Adathalászat: olyan támadási módszer, amelyben az illetéktelenek hamis weboldalakon keresztül kérnek adatokat a felhasználóktól, például banki bejelentkezési adatokat vagy más személyes adatokat.

[2] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról 1. melléklet 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1. sz. melléklet I. / 3. bekezdés

[3] Dornfeld L., et.al: Kibervédelem a bűnügyi tudományokban, 2020.

Ransomware: az illetéktelenek által telepített rosszindulatú szoftverek, amelyek titkosítják a felhasználó fájljait és azok visszaállításáért váltságdíjat követelnek.

Adatvesztés: az adatok véletlen vagy szándékos törlése, amelyek között személyes adatok is lehetnek.

Identitáslopás: az illetéktelenek által megszerzett személyes adatok felhasználása azonosításra, például hamis banki tranzakciók végrehajtásához vagy hamis személyazonossággal történő vásárláshoz.

Ezek az esetek jelentős kockázatot jelentenek az egyének személyes adataira és pénzügyi biztonságára, és az ilyen incidensek megelőzése és kezelése kulcsfontosságú a kiberbiztonsági stratégiákban.

A közösségi média veszélyei

A közösségi média a mai társadalmunk egyik legnépszerűbb és legelterjedtebb kommunikációs formája, de sajnos sok veszélyt is hordoz magában, kibervédelmi szempontból. Ezek közé tartoznak:

Adatvédelmi problémák: A közösségi média platformok gyűjtik és tárolják a felhasználók személyes adatait, és a platformok általában nem mindig biztosítanak megfelelő adatvédelmet. Ezenkívül a felhasználók gyakran megosztanak olyan információkat, amelyek könnyen felhasználhatók azonosításra vagy személyes adatok lopására.

Hamis hírek és dezinformációk: A közösségi média platformokon könnyen terjednek a hamis hírek és dezinformációk, amelyek befolyásolhatják az emberek nézeteit és döntéseit.

Kiberbullying: A közösségi média platformokon keresztül az emberek könnyen és gyorsan megoszthatnak negatív kommenteket, fenyegetéseket és zaklató üzeneteket, amelyek súlyos hatással lehetnek a célpontok mentális egészségére és jóllétére.

Phishing: A közösségi média platformokon keresztül a kiberbűnözők hamis oldalakon keresztül kísérhetnek meg adathalász támadásokat, amelyeknek célja az érzékeny adatok megszerzése. Ezenkívül a kiberbűnözők megpróbálhatnak betörni a felhasználók fiókjába, hogy hozzáférjenek a személyes adatokhoz és információkhoz.

Identitáslopás: A közösségi média platformokon könnyű olyan személyes adatokat megosztani, amelyek azonosító adatokat tartalmaznak, például a teljes nevét vagy lakcímét. Ezek az adatok nagyon értékesek lehetnek az identitástolvajok számára, akik felhasználhatják azokat személyazonosságuk megszerzéséhez, valamint adathalász támadásokhoz és egyéb káros tevékenységekhez.

Fontos, hogy az emberek tudatában legyenek a közösségi média platformok veszélyeinek, és megfelelő lépéseket tegyenek az adataik és magánéletük védelme érdekében.

Figyelemgazdaság

A rendkívüli információbőség miatt a tartalmak versengenek egymással a felhasználók figyelméért, de a túl sok tartalom miatt az emberek figyelmének megragadása és megtartása szinte lehetetlenné vált. Az ingerküszöb is megnőtt, és a felhasználók szokásai gyorsan változnak. A figyelem fő típusai a tartós, szelektív és szórt figyelem, amelyek közül a szórt figyelem a leggyakoribb a mai digitális média környezetben. Az emberi figyelem határai végső pontjához érkeznek, és az influenszer-jelenség is rámutat erre a változásra. A figyelem megragadása egyre rövidebb időre korlátozódik, és a figyelemgazdaság már fenntarthatatlanul működik. A reklámoknak egyre nehezebb a figyelem megragadása, és a reklámvakság problémája is egyre nagyobb. Az emberek figyelmetlenebbekké válnak és nincsenek felkészülve a médiában zajló eseményekre. Az online média gyakran etikátlanul működik, és az álhírek különösen az időseket érintik negatívan. Az államnak és az oktatási intézményeknek nagyobb felelőssége van a szabályozásban és az oktatásban a médiatudatosság terén.

A felhasználók egyre inkább válogatnak a tartalmak között, és kritikusabbá válnak a reklámokkal szemben. Ezért a jövőben a tartalom-előállítókra (influenszerekre) és a kreatív megoldásokra helyeződik a hangsúly.

Az oktatás és az edukáció kulcsfontosságú szerepet fog játszani a jövőben. Az embereknek fel kell készülniük a média által kínált információk kritikus elemzésére és értékelésére. Az oktatási intézményeknek és a szülőknek kiemelt figyelmet kell fordítaniuk a digitális írástudásra, a médiahasználat etikájára és a manipuláció felismerésére.[4] [4]

Összességében az elmúlt években tapasztalt figyelemgazdasági változások hatással vannak mindennapi életünkre és társadalmi viselkedésünkre. Ahhoz, hogy sikeresen navigáljunk ebben az új média- és figyelemgazdaságban, kritikus gondolkodásra, figyelemkezelésre és tudatos médiahasználatra van szükségünk.

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.

Felhasznált irodalom

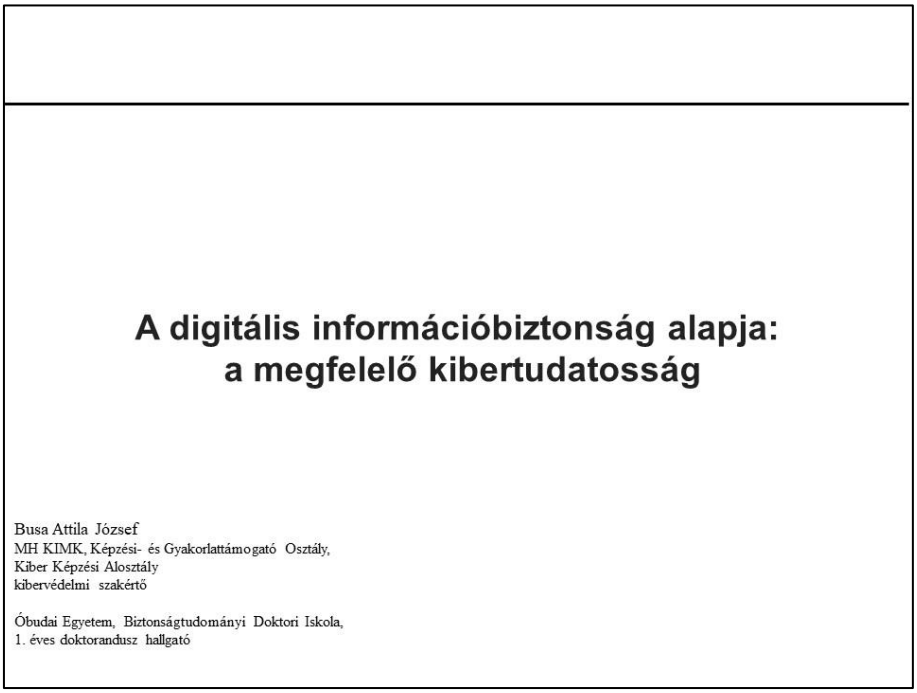
1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról 1. melléklet 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1. sz. melléklet I. / 3. bekezdés

[4] Bíró Veronika - A figyelemgazdaság átalakulása. Kitől kapjuk a kegyelemlökést?

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

Bíró Veronika - A figyelemgazdaság átalakulása. Kitől kapjuk a kegyelemlökést?, https://www.digitalhungary.hu/interjuk/A-figyelemgazdasag-atalakulasa-Kitol-kapjuk-a-kegyelemlokest/14003/ (letöltve: 2023.01.13.)

Dornfeld L., Gyaraki R., Kiss T., Kovács Z., Nagy Z., Simon B. – Kibervédelem a bűnügyi tudományokban, Szerkesztette: Kiss Tibor, Budapest, 2020.



VÁZLAT

- Információ-biztonság, kiber-biztonság
- Kiber támadások
- Személyes adatok biztonsága
- Kiberfenyegetettség
- Közösségi média veszélyei

MI JUT ESZÉBE A KIBERBIZTONSÁG SZÓRÓL?

www.menti.com

MI A BIZTONSÁG?

Hétköznapi értelemben a biztonság veszélyektől mentes, zavartalan állapotot jelent. Az informatikai rendszerek esetében a legfontosabb az adatok (információk) biztonságát megvalósítani.

INFORMÁCIÓ-BIZTONSÁG, KIBER-BIZTONSÁG

Információ-biztonság

Magának az információnak (digitális vagy kézzel fogható) a védelme.

Bizalmasság (**C**onfidentiality), sértetlenség (**I**ntegrity), elérhetőség (**A**vailablity) elve.

Védekezhetünk pl.:

- Digitális mentésekkel;
- Fizikai védelemmel (ajtók, kerítések, széfek);
- Biztonsági őrzéssel.

Kiber-biztonság

A kibertér használatának a védelme az esetleges támadásoktól.

„CIA" itt is.

Védekezhetünk pl.:

- Hálózati biztonsági beállításokkal;
- Web alkalmazások biztonsági beállításaival;
- Támadás elleni védekező és elemző szoftverekkel.

Teljes védelem **NINCS**!

C. I. A.

Három adatbiztonsági követelmény létezik:

- **Bizalmasság (Confidentiality):** valami, amit csak az arra jogosultak ismerhetnek meg, korlátozott a megismerésre jogosultak köre.
- **Sértetlenség (Integrity)** vagy integritás: valami, ami az eredeti állapotának megfelel és teljes.
- **Rendelkezésre állás (Availability)**: a szükséges infrastruktúrák, valamint adatok ott és akkor állnak a felhasználó rendelkezésére, amikor arra szükség van.

KIBERTÉR FOGALMA

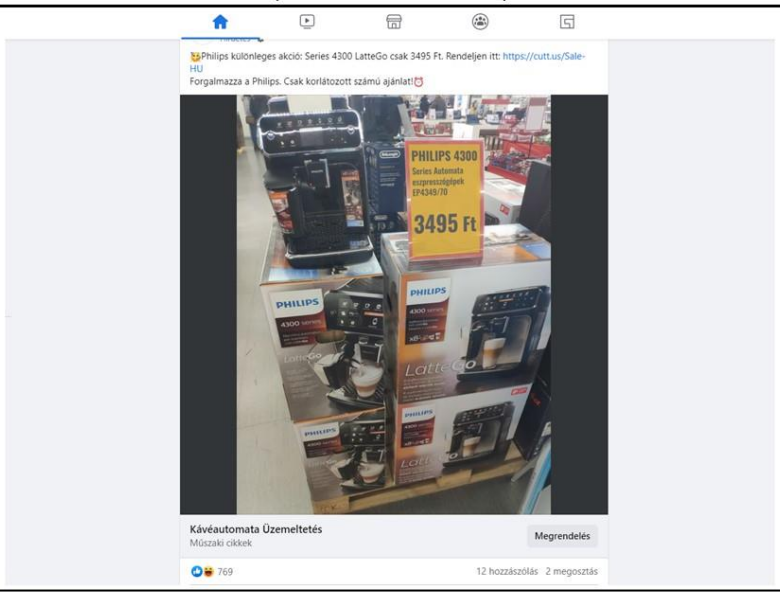
A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információ rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.

SZAKHATÓSÁGOK

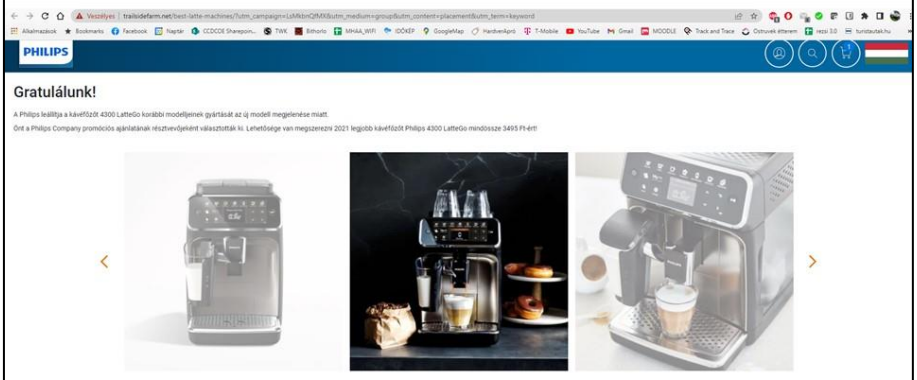
- A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (**NKI**) látja el Magyarországon a hatósági, biztonságirányítási, sérülékenység-vizsgálati feladatokat - alapvetően az állami és önkormányzati szervek, valamint a létfontosságú rendszerek és rendszerelemek vonatkozásában.

- A honvédséget illetően jelenleg a **KNBSZ** látja el a fent említett szakhatósági feladatokat.

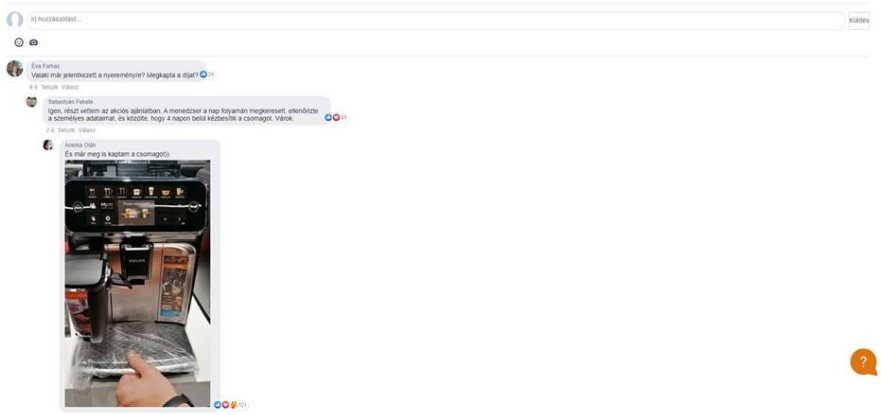
KÖZÖSSÉGI MÉDIA VESZÉLYEI
CSAK NEKED, CSAK MOST!
(SEMMI SINCS INGYEN!)



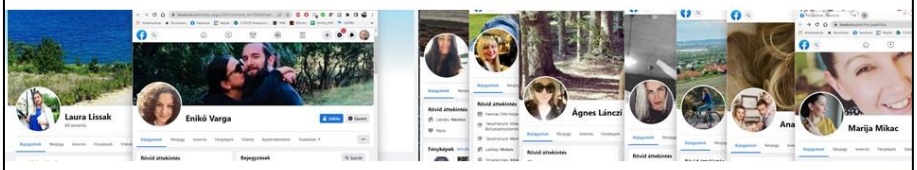
KÖZÖSSÉGI MÉDIA VESZÉLYEI
CSAK NEKED, CSAK MOST!
(SEMMI SINCS INGYEN!)



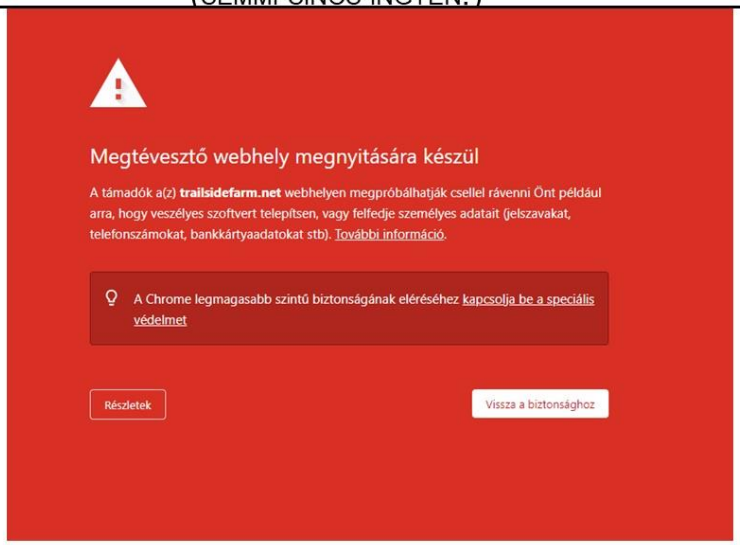
KÖZÖSSÉGI MÉDIA VESZÉLYEI
CSAK NEKED, CSAK MOST!
(SEMMI SINCS INGYEN!)



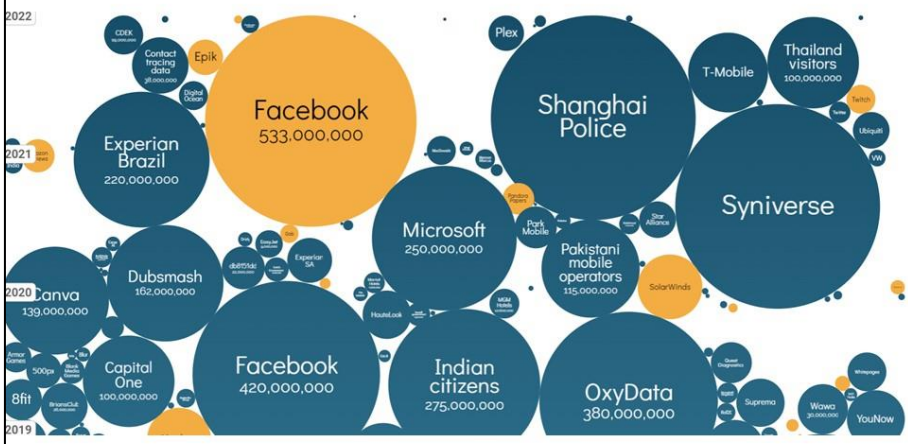
KÖZÖSSÉGI MÉDIA VESZÉLYEI
CSAK NEKED, CSAK MOST!
(SEMMI SINCS INGYEN!)



KÖZÖSSÉGI MÉDIA VESZÉLYEI
CSAK NEKED, CSAK MOST!
(SEMMI SINCS INGYEN!)



SZEMÉLYES ADATOKAT ÉRINTŐ INCIDENSEK



VERSENY A FIGYELMÜNKÉRT (A JÖVŐ?)

- Figyelemazdaság folyik (tavaly 12mp, idén már csak 8mp);
- A közelmúltban a kábel- és a műholdas televíziónak köszönhetően több száz csatorna vált elérhetővé, majd ezen még csavart egyet a digitális média megjelenése. Így már elképesztő mennyiségű csatorna és tartalom vált elérhetővé. Ebből kifolyólag a figyelem működése, a figyelemgazdaság teljesen átalakult. Korábban nem kellett küzdeni a fogyasztók figyelméért, mert azt nézték az emberek, ami volt, de ez többé nem igaz.
- A rendkívüli információbőséget mutatja az is, hogy ma már minden nap több tartalom kerül a digitális térbe, mint ahány ember él a Földön, és ezeknek a megosztásoknak a 60%-át senki sem látja a feltöltőn kívül. A tartalmak tehát versenyeznek is egymással, de ekkora mennyiségnél az emberek figyelmét megragadni és megtartani szinte lehetetlen.
- A figyelemgazdaság oda vezet majd, hogy a fogyasztók is kezdenek egyre tudatosabbá válni, ami a gazdaság részéről nem olyan jó hír, ugyanis nem a mennyiségre, hanem a minőségi tartalomfogyasztásra helyezik majd a hangsúlyt.

ÖSSZEFOGLALÁS

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.

MEGOLDÁS

„A józan észt semmilyen védelem nem tudja helyettesíteni!”

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.)
- 2012. évi CLXVI. törvény
- 1139. /2013. (III. 21.) Korm. Határozat
- 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.

Köszönöm a figyelmet!

Gábor Knapp: IoT, localization and threat, furthermore the defence sector – Thoughts on the margin of a future PhD research

In my presentation I introduced my thoughts that came up when I was applying to the University of Public Service, Faculty of Military Sciences and Officer Training, Doctoral School of Military. My research will be in the field of Engineering Defence electronics, IT and communication. I believe that the support of the Military National Security Service Scientific Council, and my supervisors will lead me to success.

In recent years, Internet connected devices (Internet of Things - IoT) have become increasingly popular. My research is based on the assumption that the possibilities are in connection with the capabilities of these devices, those emphasising the extraction of available data through the location determination, can cause a threat for the users of IoT devices. Since some of the devices available on the market can be easily integrated into the electronic information systems of the defence sector, and therefore the technical devices carrying these mentioned threats will also appear in governmental and national defence developments. The partial or complete integration of the threat containing IoT devices into military solutions initiates a necessary review of the defensive protection countermeasures based on the relevant requirements.

I assume that by examining the perspective from the defensive and

also from the offensive point of view of cyberspace as an operational domain, the vulnerabilities resulting from the location determination of IoT devices, I can also verify the involvement of the national defence sector. I think that the different approaches resulting from the originated threats will come with a similar outcome.

I believe that because of these involvement, this can contribute to the need to change the collective examination of operational planning and cyber security areas such as security awareness, development and also testing. The existence of this up-to-date knowledge can be integrated into the cyber security requirements of electronic information systems for national defence and can also provide a basis for the further, continuous formation of defence strategies.

As a result of my various positions, I constantly monitor the integration of cyber security and its growing importance in the national defence sector. At the operational, combat, and strategic level, I was confronted with the factors influencing threat operations, including operational planning. My previous presentations I held in these topics were based on the relationship between cyber security threats and operational planning, and the results of my initial research related to this, confirmed the topicality of the topic.

Therefore I will lie my research to the basis of the following hypothesis.

- The closed view management of defence purpose electronic

information systems is questionable in future terms, so the functions of Internet connections shall be protected with extended procedures, which can only be implemented with complex protection procedures with a full scale approach.

- Different extents and required integration of IoT systems can only be handled by taking into account other factors affecting the operations of the defence sector.
- It is necessary to examine and manage the threats of positioning in different phases, like manufacturing of positioning devices, development of defence purpose electronic information systems, the implementation of various technological solutions to varying degrees, and the application of ready-made products.
- Since, the connection models based on the technological background necessary for the operation of the industrial IoT or specially military IoT systems interpreted within the IoT systems differ from those used in traditional IT environments, from the point of view of my research, novel threat areas will be identifiable.

The "closed-handled" interpretation of national defence electronic systems needs to be reviewed due to the necessary - be it surveillance, security or even convenience - Internet connections. Artillery, infantry, air force troops are using a big amount of vehicles like tanks, APC's, fighters or helicopters that carry command and control, onboard and support systems in order to satisfy the

mission. Those elements are coming from different sources, manufacturers where the security maturity, requirements are also different. Hence the defence sector has a high level security approach, while integrating those elements into an existing system can harm the required CIA (continuity, integrity and availability) security requirements. Allowing for innovative developments, the development of procedures for the appropriate level of protection can only be started by presenting the threats and illuminating them in relation to current cases, based on drawing the attention of decision-makers.

During the entire research, my goal, based on individual results approached from a technical direction, is to verify the assumption that technical exposure can be effectively reduced through regulation.

With the answers to my hypotheses, with the help of recognizing the threats, the protection measures will be able to be developed, therefore, the reduction of the negative effects resulting from the revealed IoT threats will also appear as a goal in the management-level thinking for protection purposes. At the same time, since the examples of the operations can only prove effective protection if there is a real attacker's intent, I would like to point out the possible application of the related attack vectors, taking into account the defensive thinking, and thus the possibilities of these options that can be built into operational planning. At different levels and areas of operational planning, I would like to research the effects on

reconnaissance, operations, and – in the case of electronic information systems integrating IoT capabilities – on management and control, and present the positions of different levels of management in this context.

Allied (NATO and EU) directives, requirements, current and recently published legal documents that will be transposed into the national legal environment result in a regulatory environment different from the general one in the field of national defence. Taking them into account, for example, through the framework of cybersecurity certification, IoT regulation results in a different approach to integration.

I believe that the results of the research demonstrate the foundation of the need for full-scale development for defence purposes, the precise, all-encompassing formulation of the defence requirements during procurement and, prior to that, during planning. By proposing the regulation of the integration of IoT devices in different areas, limited to the appropriate level, I want to prove the acceptable level of residual risks, taking into account the probability of occurrence associated with the threats.

As an organisational response to the identified threats, I would like to research the connection, compliance, and opportunities for the organisational elements integrated into the cyber security task system, such as security awareness, requirement setting, and control enforcement.

During the research, after identifying the areas to be investigated,

I determine the necessary investigation aspects. In my opinion, IoT devices and cyberspace encompass a constantly changing field, the literature examination of which sheds light on the theoretical, and thus the practical, results realised from the strategic side through the threats approached from the technical side.

As a starting point, I set out to map the existing situation, which I can examine on the basis of the conclusions that can be drawn from the examples that can be found, based on the threatening effects. In order to investigate threats from positioning, I intend to achieve my own results with a methodology that reflects the specifics of the national defence industry. When choosing the methodology, I take into account that if they agree with the guidelines of other internal controls and organisational evaluations, then the results can be more easily implemented in the management's needs for change. The methodology must reflect the needs of the national defence sector, which uses a wide range of technical solutions, which can be determined by learning about electronic information systems. Threats can only be assessed by processing the approaches necessary to achieve different effects, thus by determining the individual, the organisation and the organisational goals and results, so examining them with different approaches should also be one of the goals of the research.

While covering all the mentioned topics I assume to receive a target that will adjust by the following research results:

- I can confirm that appropriate defence countermeasures does

not exclude the development needs arising in this area. The basis for creating a balance, and thus for leadership decision-making, can be the research of risk-proportionate measures.

- With a complex approach the recognizable threats related to the integration of IoT systems and influencing the operations of the national defence sector can be handled.
- It can be proven that threats resulting from positioning can be different due to the various phases of life cycle of the systems, which have unique characteristics for each phase, so it is possible to manage them.
- I can identify various threat areas based on the result of the research of the connection models of IoT systems.

Finally I kindly asked all the audience to support my research and also asked for inputs that can influence and open my thinking in these field.

IoT, localization and threat, furthermore the defence sector

Thoughts on the margin of a future PhD research

LtC Gábor KNAPP

1

Details of my research:

Application for study year 2023/24

MNSS Scientific Council

University of Public Service
Faculty of Military Sciences and Officer Training
Doctoral School of Military Engineering
Defence electronics, IT and communication

Dr. Krasznay Csaba, PhD
Dr. Tóth András, PhD

2

1. Hypothesis

The closed view management of defence purpose electronic information systems is questionable in future terms, so the functions of Internet connections shall protected with extended procedures, which can only be implemented with complex protection procedures with an full scale approach.

3

1. Target adjusted research result

I can confirm, that appropriate defence countermeasures does not exclude the development needs arising in this area. The basis for creating a balance, and thus for leadership decision-making, can be the research of risk-proportionate measures.

#INTERNET, #closed_purpose_network, #supervision, #centralising, #controll, #weakest_link

4

2. Hypothesis

Different extents and required integration of IoT systems can only be handled by taking into account other factors affecting the operations of the defense sector.

5

2. Target adjusted research result

With a complex approach the recognizable threats related to the integration of IoT systems and influencing the operations of the national defense sector can be handled.

#IoT, #integration, #exposure, #operation, #complexity

6

3. Hypothesis

It is necessary to examine and manage the threats of positioning in different phases, like manufacturing of positioning devices, development of defence purpose electronic information systems, the implementation of various technological solutions to varying degrees, and the application of ready-made products.

7

3. Target adjusted research result

It can be proven that threats resulting from positioning can be different due to the various phases of life cycle of the systems, which have unique characteristics for each phase, so it is possible to manage them.

#localisation, #threat, #development_phases, #implementation, #application, #defence

8

4. Hypothesis

Since, the connection models based on the technological background necessary for the operation of the industrial IoT or specially military IoT systems interpreted within the IoT systems differ from those used in traditional IT environment, from the point of view of my research, novel threat areas will be identifiable.

9

4. Target adjusted research result

I can identify various threat areas based on the result of the research of the connection models of IoT systems.

#industrial_IoT, #sector, #OSI_modell

10


THANK YOU FOR YOUR ATTENTION
Ideas, suggestions:
knapp.gabor@hm.gov.hu
11

István Oláh: Electronic Information Systems security – similarities and differences on the ground and in the public cloud

Introduction

More and more IT systems have been "moving" to the cloud, driven by the need to ensure continuous IT resources for accelerating innovation and a properly skilled operator workforce.

This has led to new requirements for service chains in EU legislation:
- CER[1] [1],
- NIS2[2] [2],
- DORA[3] [3].

Categorisation of cloud services

The first step in defining the security controls required for the use of cloud services is to answer the question "What cloud and for what purpose" will the organisation use? The definitions provided in NIST (National Institute of Standards and Technology) 800-145 [4] can help with this.

If the service defined by the NIST is a cloud, it is advisable to agree with the service provider on the type of service (IaaS, PaaS, SaaS) and the responsibilities involved, based on Recommendation 4/2019 of the National Bank of Hungary on the use of community and public cloud services [5], which is well understood by the role separation indicated in the diagram.
It is important to stress that in banking and insurance, the cloud service provider cannot be responsible for users, including customers, and data

[1] 2022/2557-EU
[2] 2022/2555-EU
[3] 2020/0266-EU

All this is presented in the second slide of the presentation.

Nowadays, you can use the cloud for any kind of service. These are summarised in the list on the third slide. On the fourth slide, we show some examples that are also available for criminal purposes.

Considerations before using cloud

Before concluding a contract for cloud use, it is recommended that the Confidentiality (C), Integrity (I), and Availability (A) aspects (CIA) are taken into account in the same way as for "on-premises" IT systems. In the cloud, identification, authorisation, and logging controls may be developed in a different way than usual and should be reconsidered. If an organisation has an internal policy on security requirements, the first step is to extend it to the cloud. Related topics are covered in slides five, six, seven, and eight.

If an organisation is subject to external and/or internal audit requirements, then services in the cloud can be performed on audited components and data managed in the same way. Examples of possible audits are given on slides nine and ten.

Legally, there is no fundamental obstacle to using cloud services. Each organisation needs to carry out a case-by-case legal analysis of whether:

- whether the data concerned can be transferred outside the EU,
- whether the data are part of the National Data Asset,
- whether the IT system is covered by restrictive legislation.

In practice, for example, when using a SaaS service, we are faced with a complete service chain in a way not foreseen in the offer and contract. Examples of this and other aspects are shown on slides eleven and fifteen. The security and other requirements of the organization apply to all IT elements. In order to explore the

elements of the chain, it is recommended that a complete data flow diagram be drawn up. It is necessary to define the expectations for all members of the chain in the contract in a uniform way and to make the diagram an annex to the contract. Individual contracts for data processing, outsourcing, etc. should be concluded with each role if the data handled justify it.

References

[1] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)

[2] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)

[3] Digital Operational Resilience Act (DORA)

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

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

Keywords: cloud, security, contract, controls

eivok

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Electronic Information Systems security - similarities and differences on the ground and in the public cloud

International Military Information Security Conference

27 April 2023.

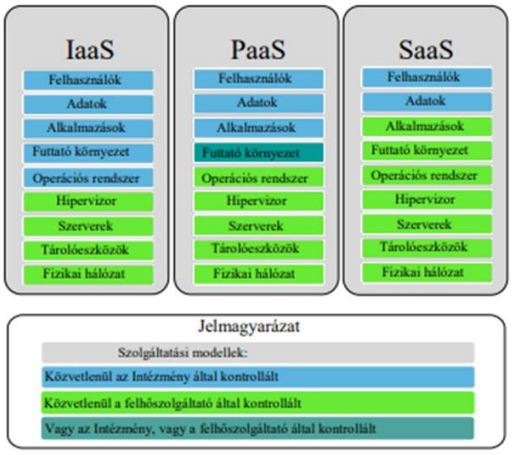
István Oláh

eivok

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

The concept of the cloud and liability issues?

- Private, Public, Community.
- Hybrid, Multi.
- The five essential characteristics of a public cloud service are:
  - on-demand, even self-service, access to the service,
  - universal network access,
  - shared resources,
  - fast tracking of changing capacity needs,
  - a measured service (usage-based usage charges)
- The NIST Definition of Cloud Computing (SP 800-145).



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

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

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**

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

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

As a Service?

- PhaaS Phishing as a service.
  - PhpaaS Phishing protection as a service.
- VaaS virus as a service.
  - VPaaS virus protection as a service.
- MaaS malware as a service.
  - MPaaS malware protection as a service.
- SaaS spam as a service.
  - SFaaS spam filter as a service.
- ..
- Any hacking as a service.

Can the cloud be used, and for what?

- **You can do anything! there are no legal restrictions outside the Ibtv,** but:
  - At the beginning of planning steps, it is also worth thinking about the exit strategy, which is more important than one might first think, in the case of Russia.
  - Need to back up IT platform configuration in the cloud, but where should the backed up file be? "e) Based on the risk analysis, in the case of critical functionality or systems, the institution shall also ensure that backups are stored independently from the cloud service provider; the regularity of independently stored backups shall be determined taking into account the risks and legal requirements."
  - Rethinking BCP, and DRP processes, what kind of "VAS" can be used if there is no own infrastructure?
  - Multi-Cloud? Hybrid-Cloud? Can our systems work like this and what does the economic model then show?
  - A DATA-DRiven risk analysis can help you decide what should and should not be stored in the cloud or stored exclusively with a cloud provider.
  - The BSR elements B and S are so far partly presented in the context of encryption procedures.
  - If possible, keys should not be trained on the serving device because residual information should be considered.

The Cloud „A" I.

- There is no single cloud service provider that is capable of 100% SLA, there are many professional articles published about the problems related to this, especially the daily problems related to mail.
- There is no 100% internet connection either, for very many reasons.
- Distance + BSR elements (e.g. encryption also takes time, it has a "cost" in time, i.e. if there is a process in the IT operation that needs backed up data, then an HLD, LLD design for the IT aspects of the processes is needed because latency needs to be modeled.
- The cloud and required Internet connectivity can significantly increase exposure risk, which in addition to the impact on user experience can cause problems in complex processes because of timeouts that can cause processes to fail stochastically.

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

The Cloud „A" II.

- QoS-enabled network devices may be required and may need to be purchased on a case-by-case basis.
- For the above reasons, it is recommended that contracts with cloud service providers include a reference measurement of times at different points in the overall signal stream.
- The importance of a "screen to data" back-and-forth design approach.
- The "Suppression Effect" of the Internet and TELECOM providers only gives any technical guarantees for X section, but cloud "infra" is beyond that...
  - High availability may require international leased data connections!
  - The cloud service provider is also "interesting...." scales its resources!

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

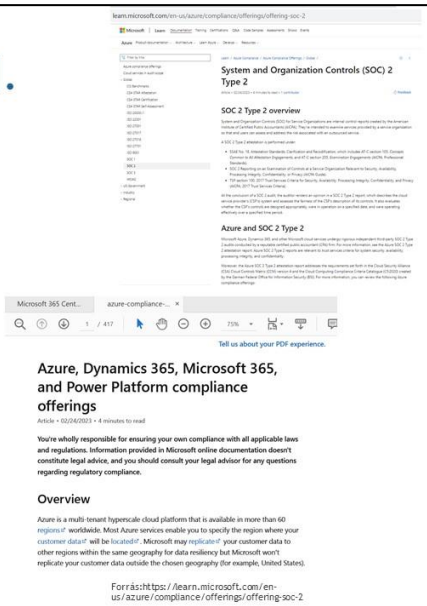
The Cloud „A", „C”

- Data from the cloud IT plant should be continuously processed in your management system by defining predictive and error levels.
- How is SIEM? Should we use a service provider's solution?
  - Preferably not only that, because who is guarding the guardians at this time?
  - If yes, it is recommended to save and process the relevant part of the logs elsewhere!
- In addition to the general availability, the expected time between the entry and exit point of the service provider should be legally treated as an SLA element in contracts.
- The effects of unavailability are not usually taken into account in economic calculations, I, therefore, propose to calculate and take into account this for other systems as well, as a non-EIR aspect of the additional costs caused by the cloud, which do not exist at present.
- This can be very diverse but a simple example, if on average invoices are sent out 2 days later due to the cloud (this is an empirical fact), then cash financing costs X HUF more (here the interest for the day is also taken into account), and many more examples could be given.....

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

The Cloud audit I.

- When procuring a cloud service provider, it is worth asking for documentation of the audits that have been carried out on each IT System.
- Those who have them typically publish the certificate on the Internet, but you can't really learn anything from them because you need to obtain the audit profile, methodology, and audit plan to interpret them. From there, you can see what and to what level the provider can offer which is not usually the level they advertise themselves!


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.

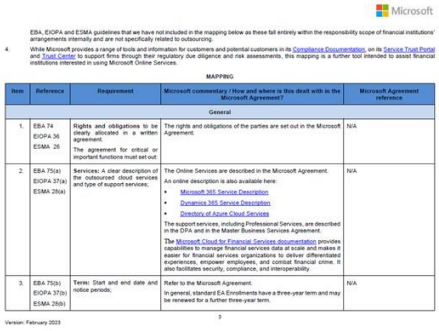
Overview

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

The Cloud audit II.

- Cloud provider documents are available.
- Thousands of pages with 10% URL.
- Documents are dynamic, and part of the contract!
- 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

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

The Cloud service chains

- We contract with a cloud service provider, but e.g. In the case of SaaS, multiple providers are involved:
  - In the case of SaaS, multiple providers are involved:
  - Service Provider.
  - Service.
  - Data Centres.
  - Service Level XaaS.
  - Contractual relationship direct, indirect.
  - Jurisdiction.
  - The procedural law of contracts!

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Other questions about the Cloud

- The role of a cloud service provider under GDPR because it is typically a data processor.
- The role of a cloud service provider is an outsourced activity because it is typically considered as such.
- The cloud service provider's solvency position, i.e. the extent to which it can recover potential direct and indirect damages arising from non-operation, if at all...
- The extent of default and non-performance penalties by solvency analysis. Analysis of the management and ownership structure of the service provider, because nothing is ever what it seems at first glance...., is there a political risk? In the case of Russia.
- Confidentiality issues.
- The eIDAS aspects if a process is involved where there is a commitment, digital signature/timestamping/organizational stamping.
- Are Cloud and TELKO operator colleagues a specific risk?
- ... and there are many more, but these are only worth analysing if there is a good answer to the above

eivok
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Thank you for your kind attention!

https://www.hte.hu/eivok
https://www.hte.hu/informaciobiztonsagi-szakosztaly-eivok/-/esemeny/1/4862605/eivok-35--informaciobiztonsagi-szakmai-forum
https://www.hte.hu/informaciobiztonsagi-szakosztaly-eivok/-/esemeny/1/4862408/eivok-36-hte-soc-minikonferencia

Magyar Sándor: Szoftverek biztonsági bevizsgálásának kérdései

Már nem kell bizonyítani az elektronikus információs rendszerek rohamos fejlődésének kérdését. Mindenki meg tudja ítélni, hogy mekkora a szerepük a mindennapi életben. Azonban a számítógépek, informatikai rendszerek egyik fő eleme maga a szoftver, amelyre mindig megfelelő hangsúlyt szükséges fordítani.

A növekvő számú elektronikus információs rendszerekkel együtt folyamatosan növekszik a szoftverek száma is. Egyre nagyobb nyomás kerül az informatikai fejlesztőkre, akiknek rövid határidőre, egyszerű használhatóságú, könnyű telepíthetőségű szoftvert kell kódolni. Az üzleti életben a piaci előny annál van, aki előbb hozza ki az adott terméket. A verseny ezen a területen növekszik, azonban ezek mellett nem szabad elfelejteni a kockázatokat sem.

Számos szervezet honlapján érhetők el információk a támadások típusairól, trendjeiről, a szoftverek sérülékenységéről (OWASP, CWE stb.), amelyek amellett, hogy információt szolgáltatnak, felhívják a figyelmet a terület fontosságára is.

Nemcsak a használatba vétel előtt szükséges a szoftverekre nagyobb figyelmet fordítani, hanem biztonság érdekében a szoftvereket a teljes életútjuk során nyomon kell követni. Legyen az bármely modell (vízesés, spirál, agilis stb.), amivel a szoftvereket tervezzük, már a kezdetekben első szempont kell, hogy legyen a sérülékenységek kiküszöbölése. Ez azért is fontos, mert a hatékonyság, találékonyság a fejlesztőknél az időkényszer miatt sajnos hibákat is eredményezhet, mint például a szoftver

komponensek újrahasznosítása, egyes kódrészletek letöltése esetleges szükségtelen többletszolgáltatásokkal stb. A hibás kódolás (konfigurációs hibák) ugyancsak rejthetnek kockázatokat (memória korrupciós sérülékenységek, SQL injection, cross-site scripting stb). A Zero Day (nulladik napi) sérülékenységek ennél sokkal komplexebb kérdéseket vetnek fel, amelyek megtalálása egyrészt komoly üzleti terület is, másrészt a kiberbűnözőknek ad jelentős előnyt a támadásaik végrehajtásánál. A szoftverek bevizsgálásánál azok nem rendeltetésszerű viselkedése is elemzésre kerül.

A szoftverek funkcionális tesztelése – amely során meggyőződünk, hogy a szoftver megfelel a felhasználói igényeknek – szükséges az igényeknek való megfelelés ellenőrzése szempontjából, azonban emellett hangsúlyos tevékenységként kell megjelennie a biztonsági szempontú vizsgálatoknak. Rendkívül fontos, hogy meggyőződjünk arról, hogy a szoftver mentes a sérülékenységektől. A szoftverek biztonsági bevizsgálását többféle módon lehet kategorizálni. Vizsgálat forma szerint lehet statikus vagy dinamikus. A szoftver típusa szerint megkülönböztethetők többek között webes szoftverek, mobil alkalmazások, PC-s szoftverek, adatbázis szoftverek, felhő, stb. A szoftver eredet szerint lehet „dobozos” vagy saját fejlesztésű, a vizsgálat típusa szerint pedig Black Box, Grey Box, White Box.

A szoftverek biztonsági bevizsgálásánál humán tényező nagy szerepet tölt be. A vizsgálatot végrehajtó személyeknek vagy szervezetnek az alábbi szempontoknak kell megfelelni az eredményes feladatvégrehajtáshoz:

- megfelelő számú szakember;

- megfelelő képzettségű szakember;
- korábbi fejlesztői tapasztalat előny;
- szükséges céltanfolyami végzettséggel rendelkezés.

A bevizsgálásnál kiemelt figyelmet kell fordítani szoftver futási környezetének megfelelő tesztkörnyezet létrehozására.

A már elérhető szoftverek esetében az információbiztonsági tudatosításnak is nagy szerepe van, mivel a frissítések szükségességét és elmaradásuk hiányának kockázatait itt hangsúlyozzák ki a használói, üzemeltetői részére.

Felhasznált irodalom

- Common Weakness Enumeration (CWE™), https://cwe.mitre.org/
- OpenText, What Is the SDLC? https://www.microfocus.com/en-us/what-is/sdlc
- Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2023 YTD, https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/
- OWASP Top Ten, https://owasp.org/www-project-top-ten/

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

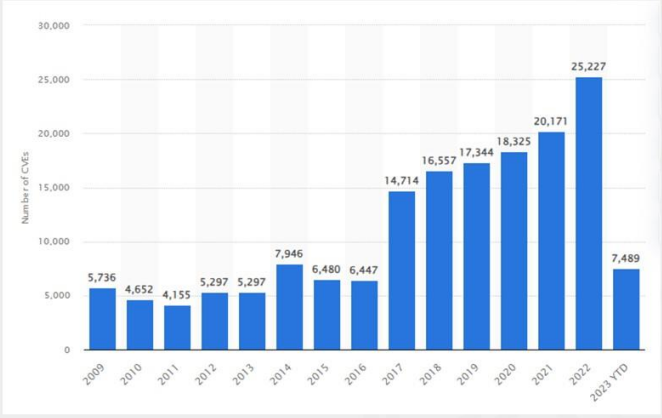
Szoftverek biztonsági bevizsgálásának kérdései

Magyar Sándor

Változó környezet

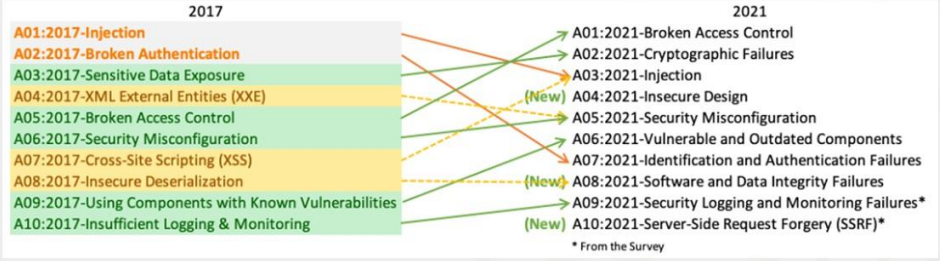
- Növekvő számú elektronikus információs rendszerek.
- Kikerülhetetlen okos rendszerek.
- Mindezekkel együtt a szoftverek száma növekszik, ezáltal a kockázatok is.
- Nyomás a fejlesztőkön:
  - Rövid határidőre.
  - Egyszerű használhatóság.
  - Könnyű telepíthetőség.
- Piaci előny annál, aki előbb kihozza a terméket.

A leggyakoribb informatikai biztonsági sebezhetőségek és kitettségek (CVE-k) száma világszerte



Forrás: https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/

OWASP top ten



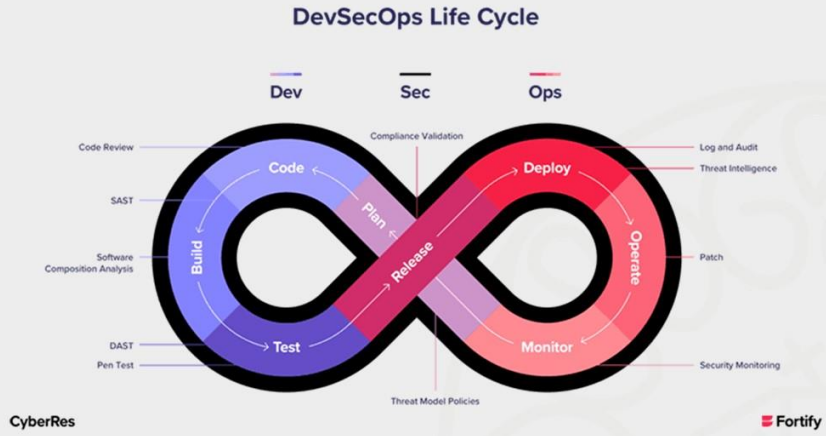
Forrás: Open Worldwide Application Security Project

Felhasználói gondolatok a szoftverekről Menyország helyett a pokolba

- Ami otthon jó, az a munkahelyen is!
- Engem nem zavarnak a reklámok!
- Hozzáférést kér a kamerához, tárhelyhez stb. de más alkalmazások is szoktak. Nem mindegy?
- Ezt nagyon sokan használják, ezzel nem lehet baj!
- A sógorom ajánlotta, mert a fia is ezt használja.
- Innen jobb letölteni és licenszkulcs sem kell…
- …
- Nekem otthon 2 perc alatt felment (next, next, next, finish), itt meg már egy hete nem történik semmi az informatikán.

Szoftverek biztonsági bevizsgálásának szerepe

- Hatékonyság, találékonyság a fejlesztőknél. Szoftver komponensek újrahasznosítása.
- Hibás kódolás (konfigurációs hibák).
  - Memória korrupciós sérülékenységek, SQL injection, cross-site scripting…
- Zero Day kérdése.
- A szoftverek nem rendeltetésszerű viselkedése.



Forrás: https://www.microfocus.com/en-us/what-is/sdlc

Szoftverek nyilvántartása

- Csak a szükséges szoftverek.
- Licensz menedzser

- Engedélyezett szoftverek listája:
  - Szoftver neve
  - Verziószáma

Szoftverek bevizsgálása

- Funkcionális
  - A szükséges funkcióival, támogatja a munkafolyamatot
  - UAT
- Biztonsági
  - Mentes a sérülékenységektől

Szükséges feltétek

- Humán
  - Megfelelő számú szakember
  - Megfelelő hozzáértésű szakember
    - Fejlesztői tapasztalat.
    - Céltanfolyamok.
- Tesztkörnyezet
  - Szoftver futási környezetének megfelelően.
- Szoftveres támogatás.

Kategorizálási lehetőségek

- Vizsgálat forma szerint
  - Statikus
    - Manuális
    - Szoftveres
  - Dinamikus
- Szoftver típus szerint:
  - Webes szoftverek
  - Mobil alkalmazások
  - PC-s szoftverek
  - Adatbázis szoftverek
  - Felhő
  - …
- Szoftver eredet szerint
  - „Dobozos”
  - Saját fejlesztés
- Vizsgálat típus szerint:
  - Black Box
  - Grey Box
  - White Box

Mesterséges intelligencia hatása

- Kód írása
- SW hibák felderítése
- SW tesztelése
- …
- …
- …
- Exploit írás

Felhasznált irodalom

- Common Weakness Enumeration (CWE™), https://cwe.mitre.org/
- OpenText, What Is the SDLC? https://www.microfocus.com/en-us/what-is/sdlc
- Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2023 YTD, https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/
- OWASP Top Ten, https://owasp.org/www-project-top-ten/

KÖSZÖNÖM A FIGYELMET!

uni-nke.hu

Szulcsányi Viktor: Támadó tevékenységek szerepe a kibervédelem fejlesztésében

A kiberbűnözők, vagy hackercsoportok által alkalmazott támadási technikák egyre inkább haladnak a digitális korral, és folyamatosan új kihívásokat jelentenek a valamennyi szervezet számára. A kibervédelem napjainkban nem csupán a meglévő védelmi intézkedések implementálásáról szól, hanem a támadók által alkalmazott módszerek megértéséről és az ezekkel szembeni hatékony védelem kiépítéséről is.

A múltban a kibervédelem fő fókuszában a reaktív védelmi képességek kialakítása állt, így a biztonságot elsősorban a tűzfalak, behatolás- és végpontvédelmi rendszerek, vírusvédelmi megoldások jelentették. Ezek az intézkedések ugyan továbbra is kulcsfontosságú szerepet játszanak az informatikai rendszerek védelmében, gyakran hamis biztonságérzetet keltenek, mivel a rendszerekben rejlő hibák, sebezhetőségek feltárása és kezelése elmarad.

Az eltérő szemléletmódok együttes alkalmazása jóval hatékonyabb megközelítést jelent, hiszen míg az eseménykezeléssel foglalkozó szakemberek általában az éppen zajló támadások és incidensek kezelésére összpontosítanak, a támadó tevékenységet végző szakemberek inkább proaktív módon, a vizsgált rendszer gyenge pontjainak, hiányosságainak feltárását tűzik ki célul.

A honvédelmi ágazatban a védelmi képességek fejlesztésére irányuló támadó tevékenységek végrehajtásának feltételei jogilag szabályozottak, így különböző korlátozások érvényesek a katonai

kibertér műveletekre és a honvédelmi célú elektronikus információs rendszerek sebezhetőségeinek feltárására is. A jogi korlátok azonban így is lehetőséget biztosítanak több, támadási technikán alapuló módszer alkalmazására.

Az egyik ilyen lehetőséget az IT biztonsági audit lefolytatása jelenti. Ez az infokommunikációs rendszerek biztonsági helyzetének felmérésére irányuló tevékenység, amely során az auditorok sérülékenységvizsgálatok során is alkalmazott, de annál jelentősen szűkebb eszközkészlettel végzik a munkájukat. Egy ilyen felmérés során áttekintik az adott szervezet informatikai rendszerét, hálózatát, adatvédelmi eljárásait, biztonsági gyakorlatait és egyéb releváns tényezőket.

A szoftverbiztonsági audit egy gyakran a szoftverfejlesztési folyamatba ágyazott biztonsági ellenőrzés, amely a programkód statikus és dinamikus módszerekkel történő vizsgálatát, valamint a szoftver architektúrájának és adatvédelmi mechanizmusainak ellenőrzését foglalja magában. Az audit során célzottan keresik a potenciális sebezhetőségeket, mint például sérülékenységeket a kód implementációjában, nem megfelelő adatkezelést, hibás jogosultság-kezelést vagy nem biztonságos kommunikációs protokollokat. A szoftverbiztonsági auditnak fontos szerepe van a biztonságos fejlesztési gyakorlatok előmozdításában és a szoftverek használatában rejlő esetleges kockázatok minimalizálásában. Az audit eredményeit felhasználva a szoftverfejlesztők képesek lehetnek kijavítani a felderített sebezhetőségeket, bevezetni

biztonsági javításokat és megerősíteni a szoftverek védelmi mechanizmusait.

Szintén ide kapcsolódó tevékenység a támadási felületek menedzsmentje is, amely egy szervezet interneten, publikusan elérhető szolgáltatásainak feltérképezését, biztonsági állapotuk felmérését, valamint az adott szolgáltatások kapcsán elérhető, esetlegesen érzékeny információk begyűjtését és feldolgozását jelenti. Ez az informatikai rendszerek IT biztonsági szempontú kockázatfelmérésének egy néhány éve elterjedő és azóta is növekvő népszerűségnek örvendő formája. A tevékenység képet adhat a szervezet kiberbiztonsági kitettségéről és ezáltal lehetőséget biztosíthat a kockázatok mitigálására is. Proaktív és stratégiai megközelítésen keresztül lehetőséget kínál a potenciális sebezhetőségek és támadási vektorok azonosítására és kezelésére.

A sérülékenységvizsgálat az informatikai rendszerek, hálózatok vagy alkalmazások sebezhetőségeinek, gyenge pontjainak azonosítására és lehetőség szerint megszüntetésére irányuló átfogó, széles spektrumú tevékenység. A sérülékenységvizsgálatot végző szakemberek számos technikát és eszközt alkalmazhatnak a rendszerek és alkalmazások ellenőrzésére. Ezek magukban foglalhatják az automatizált szoftvereket, manuális vizsgálatokat, forráskódelemzést, konfigurációs ellenőrzéseket és egyéb módszereket is. A tevékenység részét képezi a feltárt sérülékenységek javítására irányuló intézkedési javaslatok megtétele is, ezáltal az érintett szervezetek csökkenthetik az üzemeltetésből adódó biztonsági kockázatokat, felülvizsgálhatják az

érvényes biztonsági intézkedéseket és általánosságban javíthatják kibervédelmi képességüket.

A behatolás tesztelés általában a sérülékenységvizsgálatot követően vagy azzal együttesen történő, a feltárt hibák és sérülékenységek azonosítására és kihasználására irányuló támadó tevékenység. Amennyiben a folyamat során azonosításra kerültek sérülékenységek, a szakemberek megpróbálják kihasználni azt és ezáltal hozzáférést szerezni a vizsgálat hatáskörébe tartozó rendszerelemekhez, vagy érzékeny adatokhoz, esetlegesen parancsokat hajthatnak végre vagy módosításokat tehetnek a vizsgált rendszerben. A behatolás tesztelés lépései egy felügyelt rendszerben általában jól észlelhetők, ezáltal pedig a tevékenység alkalmas lehet az incidenskezelési képesség fejlesztésére is.

A red teaming talán a felsoroltak közül a legkomplexebb tevékenység, amely egy valós támadás végrehajtásán keresztül, gyakran időkorlát nélkül, folyamatos tevékenység formájában teszteli a szervezet informatikai rendszereinek biztonságát, az alkalmazott eljárásrendek megfelelőségét és a védelmi megoldások működőképességét. A red teaming során az általában külső szakértőkből álló „red team” olyan taktikákat, technikákat és eszközöket alkalmaz, amelyekkel egy szervezet egy valós támadás során is találkozhatna. Ez magában foglalhat a sérülékenységvizsgálati eszköztár alkalmazása és a támadó tevékenység elfedése mellett olyan rendszerspecifikus támadási módszereket is, mint például az úgynevezett „Living-off-the-Land” támadások, amelyek a rendszerekben, alkalmazásokban vagy

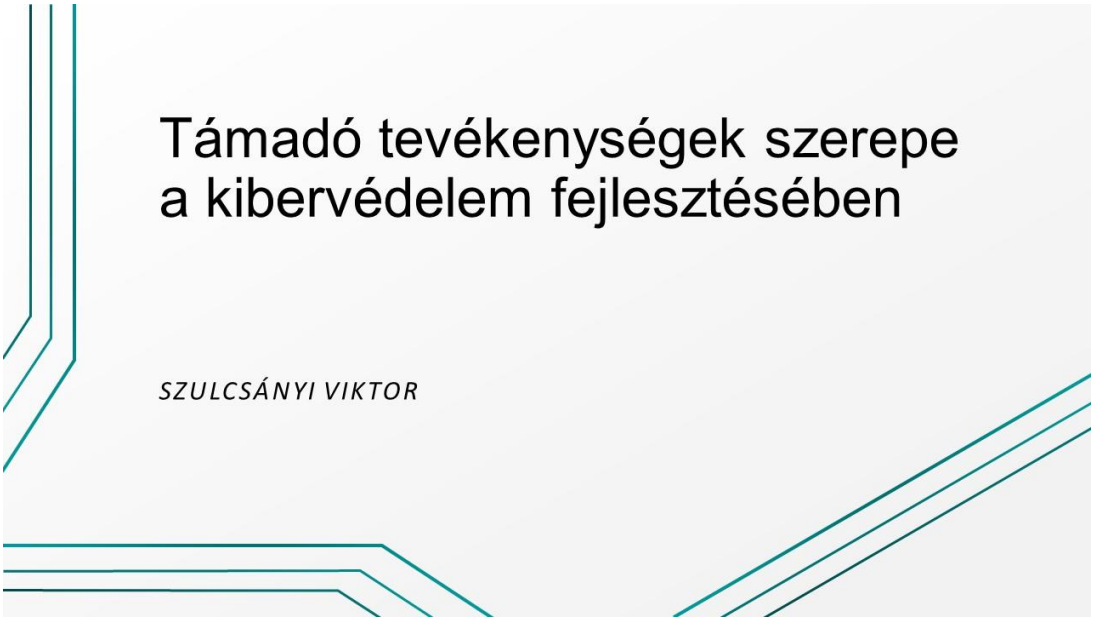
hálózatokban már meglévő, beépített funkciók és eszközök alkalmazására irányulnak a támadás nyomainak minimalizálása érdekében.

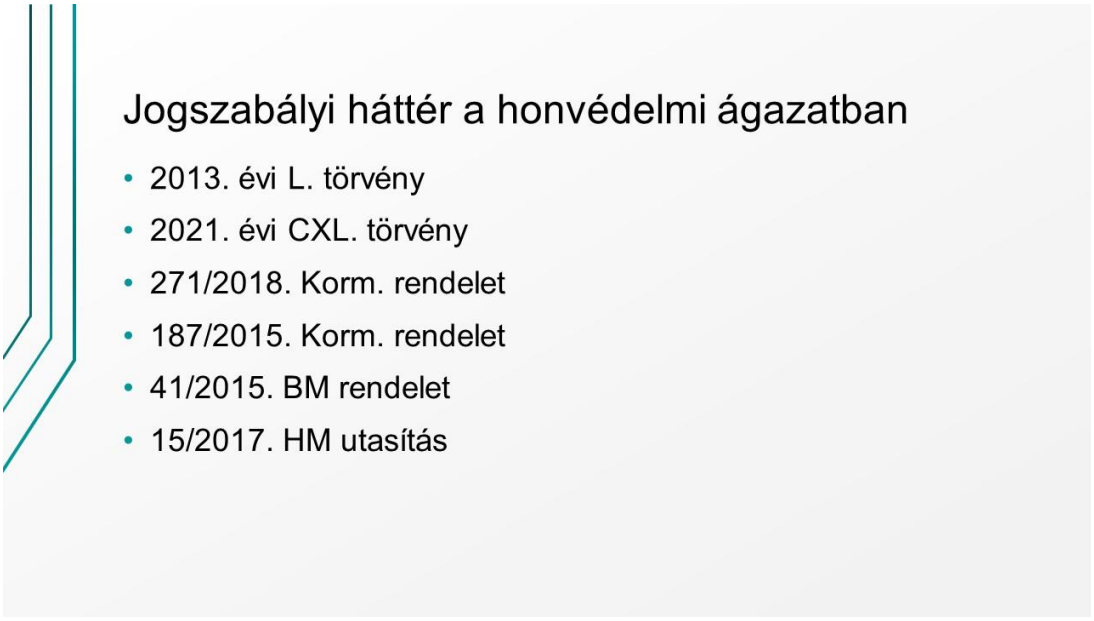
A red teaming tevékenység által lehetővé válik újabb, nehezen észlelhető vagy kihasználható sérülékenységek azonosítása, valamint a meglévő védelmi megoldások és a biztonsági eseményekre történő reagálás hatékonyságának tesztelése, fejlesztése is. Egy red team gyakorlat tapasztalatai segíthetnek a kiberbiztonsági fejlesztési irányok kijelölésében, a szakértői állomány tudásának és alkalmazkodóképességének fejlesztésében, valamint vezetői, beszerzési döntések előkészítésében is támpontul szolgálhat, hiszen rávilágíthat azokra a hiányzó védelmi képességekre, amelyek alkalmazásával a sérülékenységek kihasználása és a jogosulatlan hozzáférés ténye észlelhetővé válhat vagy akár meg is előzhető a későbbiekben.

A tevékenység azonban elég könnyen egy kétélű karddá válhat, ha a végrehajtásának feltételei nem állnak rendelkezésre az érintett szervezet esetében. Ilyen követelmények lehetnek a SIEM, határvédelmi és végpontvédelmi megoldások, valamint a SOC képesség megléte, az eseménykezelést és threat hunting-ot végző állomány megfelelő szintű felkészültsége, valamint a célok és vizsgálati feltételek tisztázása.

Összegzésként elmondható, hogy a fent felsorolt valamennyi támadó tevékenység hatékonyan alkalmazható az adott informatikai rendszerhez kapcsolódó kibervédelmi képességek emelése, továbbá a kiberbiztonsági kockázatok csökkentése során.

Bármely szervezetnek, így különösen a honvédelmi ágazati szereplőknek képessé kell válnia a támadási trendekhez történő folyamatos alkalmazkodásra, fejlődésre és megújulásra.





Támadó jellegű tevékenységek

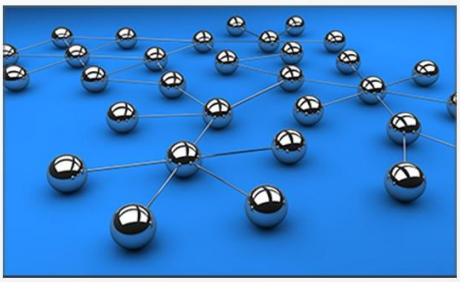
- IT biztonsági auditok
- Szoftverbiztonsági auditok
- Támadási felületek menedzsmentje
- Sérülékenységvizsgálat
- Behatolás tesztelés
- Red Teaming

Red Teaming lehetséges hatásai

- Új, nehezen észlelhető sérülékenységek azonosítása
- A biztonsági eseményekre történő reagálás tesztelése, fejlesztése
- A védelmi megoldások hatékonyságának tesztelése, fejlesztése
- A kiberbiztonsági fejlesztési irányok kijelölésének támogatása
- A szakértői állomány tudásának, alkalmazkodóképességének fejlesztése

Mi befolyásolhatja a Red Teaming hatékonyságát?

- SOC képesség,
- SIEM, XDR, határvédelmi és végpontvédelmi megoldások,
- Mélységi védelem,
- Állomány felkészültsége,
- Kommunikáció



Mik egy sikeres Red Team tevékenység feltételei?

- Meglévő, működő informatikai rendszer,
- Egyértelmű, tisztázott célok és vizsgálati feltételek,
- Magas szintű kibervédelmi képesség megléte,
- Kellő létszámú, képzett állomány megléte,
- Mindkét fél részéről biztosított erőforrások a tevékenység ideje alatt.


Köszönöm a figyelmet!

Tóth András[1]: C2-biztonság katonai szemszögből

Az orosz-ukrán konfliktus jelentősen befolyásolta a katonai elveket, ami a szimmetrikus hadviselésre való felkészültség hiányához vezetett. A hangsúly a békefenntartó műveletekről az aszimmetrikus vonásokra helyeződött át, ami a vezetés és irányítás (command and control – C2) végrehajtásában is változást eredményezett. A NATO Összhaderőnemi Doktrínája hangsúlyozza a parancsnokság és az irányítás mint kapcsolódó fogalmak fontosságát. [2] E kérdés kezelése érdekében elengedhetetlen a jelenlegi C2-stratégiák újraértékelése és a hagyományos többdimenziós műveletekhez (multi-domain operation – MDO) való igazítása. Ez magában foglalhatja az új technológiák, eljárásrendek, a jobb kommunikáció és a különböző katonai szakterületek közötti koordináció beépítését. Emellett új hangsúlyt kell fektetni a szimmetrikus hadviselésre való kiképzésre és felkészülésre, beleértve a hagyományos és aszimmetrikus fenyegetéseket egyaránt magában foglaló forgatókönyveket is.

Az amerikai hadsereg három magas rangú vezetője elismerte, hogy a hadviselés új korszakában a vezetési pontok újragondolására van szükség. A hadseregeknek át kell alakítaniuk a vezetési és irányítási rendszereiket, hogy a nagyszabású katonai műveletekben való sikerek és a győzelem érdekében beépítsék azokba a többdimenziós

[1] ORCID iD: 0000-0001-6098-3262
[2] Czeglédi Mihály: Gondolatok a vezetés-irányítás jelenéről, jövőjéről. 2018.

műveletek elveit. A katonai műveletek jövője összetett és sokrétű lesz, az űrhadviselés, az információs és a kiberműveletek megjelenésével a csatatéren való navigálás még nagyobb kihívást jelent.[3] A nagy mennyiségű adat valós idejű gyűjtésének és elemzésének képessége kritikus fontosságú lesz a harctéri sikerhez. Az olyan fejlett technológiák, mint a mesterséges intelligencia, az autonóm rendszerek és a robotika egyre fontosabb szerepet fognak játszani a jövő katonai műveleteiben.

A vezetési pontok optimalizálására vonatkozó követelmények

A többdimenziós művelet alapvető követelménye a mozgékonyság, az összehangoltság, a rugalmasság és a vezetési pontok mélysége. A vezetési pontok optimalizálásához elengedhetetlen a fizikai eszközökre való támaszkodás csökkentése, az információs tér használatának növelése és a parancsnokok közötti interakció maximalizálása. A nagyszabású műveletekben a hatékony és túlélőképes vezetési pontok kialakításához négy kulcsfontosságú alapelv elengedhetetlen: a mobilitás, a fejlett technológiák integrálása, az egyértelmű kommunikáció, valamint az olyan emberi tényezők, mint a vezetés, a képzés és a morál.

A mobilitás alapvető fontosságú a műveleti hatékonyság és eredményesség fenntartásához. Ennek megoldása érdekében a hadseregek új megközelítéseket vizsgálnak a vezetési pontok

[3] Hegedűs Ernő, Hennel Sándor: Többdimenziós (multidomain) hadműveletek. 2020.

kialakítására és telepítésére, mint például a moduláris, előre gyártott szerkezetek, amelyek könnyen össze- és szétszerelhetők. Ezek a szerkezetek testre szabhatók, hogy megfeleljenek a konkrét műveleti követelményeknek, és könnyen szállíthatóak légi vagy földi úton.

Az összehangoltság elengedhetetlen a hatékony vezetés és irányításhoz, mivel a jelenlegi rendszerek és helyszíni szerverek nem képesek a folyamatos adatáramlást támogatni. Ennek megoldásához a felhőbe való átmenetre, az adatkiszolgálók fejlesztésére és az adatszövet koncepciókra van szükség. Az érzékelők, a fegyverrendszerek és a döntéshozók integrációja a gépi tanulás és a mesterséges intelligencia révén javíthatja a hatékonyságot, gyorsabb döntéshozatalt és hatékonyabb reagálást tesz lehetővé a dinamikus helyzetekre. A felhőalapú számítástechnika és az elosztott rendszerek tovább javíthatják az információs infrastruktúra skálázhatóságát és rugalmasságát, biztosítva, hogy a művelteben részt vevő erők a lehető legpontosabb információkkal rendelkezzenek és optimális teljesítményt érjenek el.

Az ellenállóképesség a modern hadviselés kulcsfontosságú eleme, mivel lehetővé teszi az egységek számára, hogy a jelkibocsátás elfedésével és a parancsnoki pontok csökkentésével hosszabb ideig is fennmaradjanak a műveleti környezetben. Ez a megközelítés lehetővé teszi az álcázott hadviselést, megnehezítve az ellenség számára a konkrét célpontok meghatározását.

A hadműveletek mélysége kiterjeszti a műveleteket időben, térben vagy kognitív szempontból, maximalizálva a hatékonyságot az emberi, fizikai és információs dimenziókban. A mélységi és többdimenziós műveletek elfogadásával a hadseregek nagyobb rugalmasságot, ellenállóképességet és hatékonyságot érhetnek el a küldetési célok elérésében.

Az adatközpontú vezetési pontok felváltják a hálózatközpontúakat, az adatfeldolgozásra, a biztonságra és a műveleti szakemberekre támaszkodva. Az as-a-service (aaS) modell kiszervezi a karbantartást, lehetővé téve az új technológiák és a mobilitás gyors átvételét. A katonai szervezetek a felhőszolgáltatásokat kihasználva javíthatják a műveleti képességeket, általuk globális hozzáférést nyerhetnek a kritikus információkhoz és alkalmazásokhoz, csökkenthetik a költségeket és hatékonyabban működhetnek együtt. A technológia fejlődésével az aaS-modell várhatóan egyre inkább elterjed a katonai műveletekben, lehetővé téve a hadseregek számára, hogy a felmerülő fenyegetések előtt járjanak, és megőrizzék információs fölényüket a harctéren.[4]

Összefoglalás

[4] Lt. Gen. Milford "Beags" Beagle, Brig. Gen. Jason C. Slider, Lt. Col. Matthew R. Arrol: The Graveyard of Command Posts. 2023.

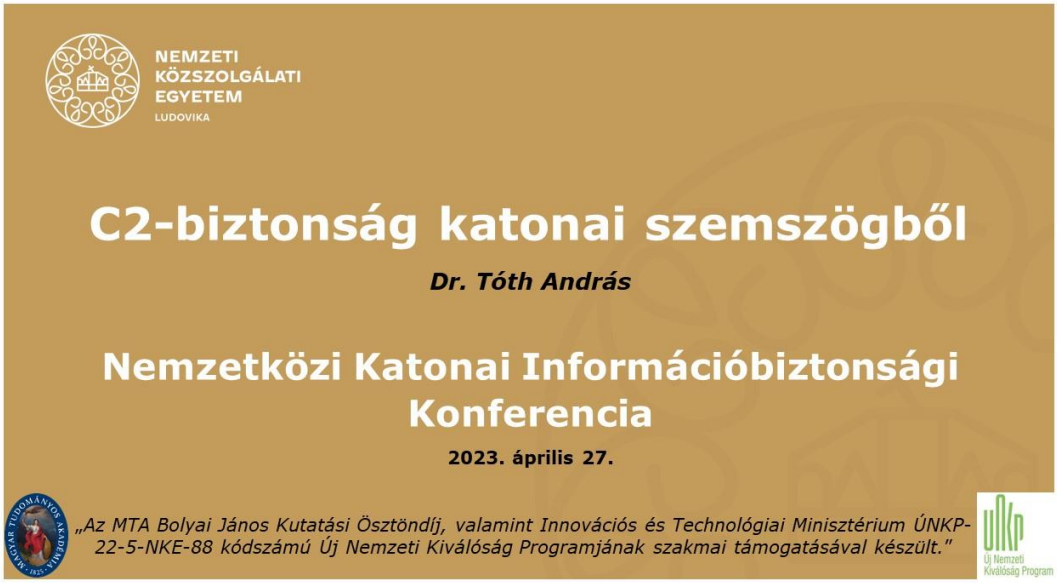
A sikeres műveletekhez elengedhetetlenek a nagy sebességű, biztonságos adatátvitelt és -megosztást támogató infokommunikációs megoldások. A felhőtechnológia a legoptimálisabb megoldás a tárolásra, elemzésre és megosztásra, mivel integrálja az összes adatgyűjtési elemet. A a katonai egységes felhőalapú eszközrendszer (KEFE) egy olyan rendszer példája, amely a hálózatba kapcsolt harci és katonai eszközöket egy közös felhőkörnyezetbe integrálja.[5] Ez a rendszer valós idejű műveleti helyzetfelismerést biztosít, lehetővé téve a döntéshozók számára, hogy megalapozott döntéseket hozzanak. Annak biztosítása, hogy a rendszer biztonságos legyen, és csak az arra jogosult felhasználók férjenek hozzá, megfelelően védett hálózatokat igényel, mint például a szövetségesi missziós hálózati modell (Federated Mission Network – FMN).[6] Megbízható adatelemző eszközök segítik a döntéshozókat a hatalmas mennyiségű adat megértésében, és olyan minták és tendenciák azonosításában, amelyek esetleg észrevétlenek maradnának.[7]

„Az MTA Bolyai János Kutatási Ösztöndíj, valamint Innovációs és Technológiai Minisztérium ÚNKP-22-5-NKE-88 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült.”

Felhasznált irodalom

[5] Tóth András: A Katonai Egységes Felhőalapú Eszközrendszer fogalmi rendszerének meghatározása. 2022.
[6] Gulyás Attila: Networks Enabling the Alliance’s Command and Control. 2023.
[7] Szeleczki Szilveszter, Farkas Tibor: A Magyar Honvédség harcászati infokommunikációs hálózatainak korszerűsítési irányelvei. 2022.

Czeglédi Mihály: Gondolatok a vezetés-irányítás jelenéről, jövőjéről. 2018.
Gulyás Attila: Networks Enabling the Alliance's Command and Control. 2023.
Hegedűs Ernő, Hennel Sándor: Többdimenziós (multidomain) hadműveletek. 2020.
Lt. Gen. Milford "Beags" Beagle, Brig. Gen. Jason C. Slider, Lt. Col. Matthew R. Arrol: The Graveyard of Command Posts. 2023.
Szeleczki Szilveszter, Farkas Tibor: A Magyar Honvédség harcászati infokommunikációs hálózatainak korszerűsítési irányelvei. 2022.
Tóth András: A Katonai Egységes Felhőalapú Eszközrendszer fogalmi rendszerének meghatározása. 2022.


NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA
C2-biztonság katonai szemszögből
Dr. Tóth András
Nemzetközi Katonai Információbiztonsági Konferencia
2023. április 27.
„Az MTA Bolyai János Kutatási Ösztöndíj, valamint Innovációs és Technológiai Minisztérium ÚNKP-22-5-NKE-88 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült."
Új Nemzeti Kiválóság Program


Tartalom
I • Témaválasztás
II • Vezetés-irányítás
III • Vezetési pont
IV • A vezetési és irányítási követelmények egyensúlyhiánya
V • A vezetési pontok optimalizálásának négy követelménye
VI • Következtetések

I. Témaválasztás

Lt. Gen. Milford "Beags" Beagle, Brig. Gen. Jason C. Slider, Lt. Col. Matthew R. Arrol: *The Graveyard of Command Posts*. Army University Press (2023)

Gulyás Attila: *Networks Enabling the Alliance's Command and Control*. AARMS (2023)

Tóth András: A Katonai Egységes Felhőalapú Eszközrendszer fogalmi rendszerének meghatározása (2022)

II/1. Vezetés-irányítás

- A „C2" rövidítés egyaránt jelenti a vezetés-irányítás koncepcionális oldalát, a **vezetési**, **együttműködési**, **koordinációs** rendet, de alkalmazható az **összeköttetést biztosító** fizikai **összetevőkre** is.
- A NATO Összhaderőnemi Doktrínája kiemeli, hogy a vezetés (command) és az irányítás (control) egymáshoz közeli fogalmak, általában együtt használatosak, de nem szinonimák. A katonai vezető, a **parancsnok** minden szinten a döntéshozatal művésze, **motivál** és **utasít** annak érdekében, hogy az adott feladatot teljesítse. Fő feladata a **személyes vezetés** (leadership) és a **döntéshozatal**, miközben elszámoltatható és **irányító-szabályzó tevékenységében osztozik törzsével**.

Forrás: Czeglédi Mihály: Gondolatok a vezetés-irányítás jelenéről, jövőjéről, Hadtudományi Szemle 2018/3, pp. 75-76.

II/2. Vezetési pont

A vezetési feladatok sajátosságainak megfelelően berendezett, elektronizált és informatizált vezetéstechnikai eszközökkel felszerelt olyan objektum, ahonnan a **vezető szervek** (a parancsnokok és a törzsek), a híradó-kiszolgáló és biztosító alegységek közreműködésével **megvalósítják az alárendeltek vezetését**, a katonai műveletek előkészítése és megvívása során.

II/3. Vezetési pont

Lt. Gen. Milford "Beags" Beagle, U.S. Army

&

Brig. Gen. Jason C. Slider, U.S. Army

&

Lt. Col. Matthew R. Arrol, U.S. Army

„a vezetési pontjaink olyan helyek lesznek, ahová a parancsnokaink **meghalni** mennek."

II/4. Vezetési pont

Csornobajevka a vezetés és irányítás elleni könyörtelen támadás, amelyet az orosz parancsnoki állások elleni szisztematikus támadás jellemzett minden műveleti szintre kiterjedően.

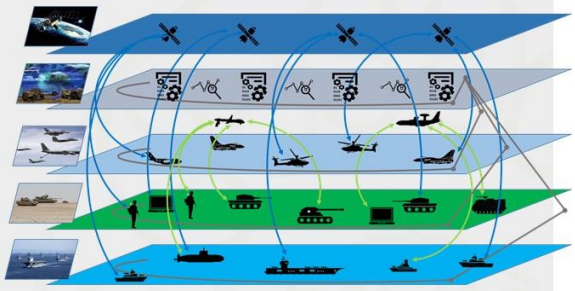
Több mint 1500 tiszt halt meg Oroszország Ukrajna elleni háborújában, köztük tíz tábornok, 152 ezredes és alezredes (2022 novemberéig)

II/4. Vezetési pont

A hadseregeknek át kell alakítaniuk a vezetés-irányítási rendszerüket, hogy a **többdimenziós műveletek** (multi-domain operations – MDO) **alapelvei beépüljenek**, ahogy átállnak erre az új működési koncepcióra az összes hadviselési szinten.

A parancsnokságoknak **rugalmasabbá**, **mozgékonyabbá** és **ellenállóbbá** (rezíliensebbé) kell válniuk, miközben nem szabad feláldozniuk a hatékonyságot.

Jobb megközelítésre van szükség a többdimenziós vezetés és irányítás elősegítésére, rövid távú célokkal és egy objektív, a nagyszabású harci műveletekre optimalizált végállapottal.



A vezetési és irányítási követelmények egyensúlyhiánya

A jelenlegi vezetési és irányítási dilemma a vezetési pontok funkcionális követelményeinek **egyensúlyhiány**át tükrözi, hogy egyszerre legyenek **hatékonyak** és **túlélőképesek**.

A vezetési pontok az idők során úgy alakultak ki, hogy a háború káoszában a **legjobb eszközt nyújtsák az egységek és alegységek irányítására**, **az ellenségnél gyorsabban hozzanak jó döntéseket**, és a parancsnok tapasztalatának és vezetői képességének kihasználásával **növeljék a hatékonyságot**.

A helyzetfelismerést és a parancsnoki vizualizációt lehetővé tevő, döntéstámogató **információk iránti** kielégíthetetlen **igény** azonban az idők során csak **nőtt**, ami a funkcionális követelmények egyensúlytalanságát eredményezte.

A vezetési és irányítási követelmények egyensúlyhiánya

A parancsnokok a túlélőképesség növelésére törekedtek a **méretcsökkentés**, a **megerősítés**, a **felosztás**, az **álcázás**, a **mobilitás növelése** és a fenyegetések elleni aktív védekezés révén.

A fejlődő technológia kommunikációs, automatizálási és informatikai eszközöket biztosított a parancsnokságok struktúrájának egyszerűsítése és hatékonyabbá tétele érdekében.

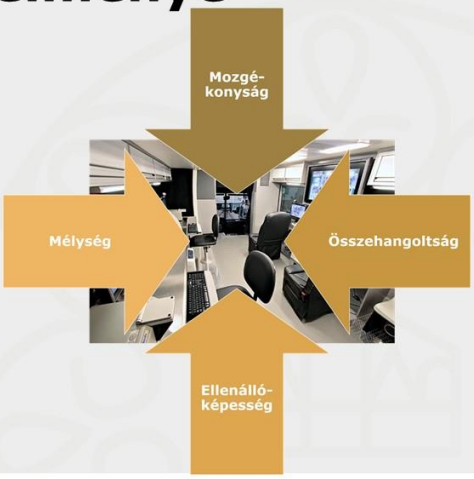
A technológiai fejlődések egyben további funkciókat és képességeket hoztak, ezzel a túlélőképességgel ellentétes méretűvé és szerkezetűvé téve a vezetési pontokat.

A vezetési pontok optimalizálásának négy követelménye

A jelenlegi környezet kihívásait felismerve az MDO hangsúlyozza, hogy a vezetési pontoknak, mint a vezetési és irányítási rendszer elemének, a **mozgékonyság**, az **összehangoltság**, az **ellenállóképesség** és a **mélység** alapelveit kell követniük.

A vezetési pontok optimalizálásához **csökkenteni kell a fizikai dimenzióra** (az eszközállományra) **való támaszkodást**, **növelni kell az információs dimenzió** (az adatok) **kihasználását**, és **maximalizálni kell az emberi dimenzióval** (a vezetőinkkel) **való kapcsolattartás képességét**.

Ennek a négy alapelvnek a vizsgálata segít meghatározni, hogy mi az, ami valóban egy **elfogadható**, **megbízható** és **átfogó** vezetési pont kialakítását jelenti, amely hatékony és túlélőképes a nagyszabású harci műveletek során egy ütőképes ellenféllel szemben.



Mozgékonyság

Jelenleg a vezetési pontok végtelen ciklusba vannak zárva a telepítés, a bontás, az áttelepítés és az újratelepítés munkájának végtelen ciklusába, hogy túlélőképesek maradjanak és lépést tartsanak a műveletekkel. Ez önmagában megzavarja a műveleti tempót, és még ellenséges beavatkozás nélkül is csökkenti a döntési előnyt.

A mozgékonyság növelése a sátrak leépítésével és a **járművekre szerelt rendszerekre való áttéréssel segít**, de nem szünteti meg ezt a problémát.

A mozgékonyság növelése nem változtat azon a tényen, hogy amikor a vezetési pontok megérkeznek új helyükre, nem lesznek többek, mint amilyenek korábban voltak.

Összehangoltság

Az elavult, egymásra épülő rendszerek és a helyszíni szerverek nem képesek támogatni a hatékony vezetés-irányításhoz szükséges, döntési minőségű adatok folyamatos áramlását.

Az érzékelők, a fegyverrendszerek és a döntéshozók integrálása a gépi tanulás és a mesterséges intelligencia segítségével.

Az adatkezelési koncepciók alkalmazása elősegíti a parancsnokságok megbízhatóságának és rugalmasságának növelését, ezáltal csökkentve az egyes platformoktól vagy adattáraktól való függőséget, amelyek ellenséges tevékenységek miatt sebezhetővé és elszigeteltté válhatnak. Az információs dimenzióra való áttérés újszerű módszertanokat és kompetenciákat tesz szükségessé a hatékony működés eléréséhez.

Ehelyett a felhőbe való áttérésre, valamint az adatháló és az adatszövet koncepciók kialakítására van szükség.

- Az adatháló egy decentralizált adatarchitektúra, amely az adatok előállítását, kezelését és megosztását a tartományokon belül és a tartományok között egyesíti.
- Az adatszövet egy olyan tartomány az adathálózaton belül, amely automatizálja az adatintegrációt, és lehetővé teszi a kapcsolódást és a hozzáférést az adattermékek megtalálása, létrehozása és széles körű megosztása érdekében.

Ellenállóképesség

„Minden hadviselés a megtévesztésen alapul”

Az a képesség, amely biztosítja, hogy egy műveletet végrehajtó egység/alegység egy működési környezetben hosszabb ideig fenn tudjon maradni.

A vezetési pontoknak képesnek kell lenniük arra, hogy **elrejtsék a „jelüket”**, hogy megnehezítsék az ellenfél célzását a vizuális, termikus, elektronikus és akusztikus jelkibocsátásuk elrejtésével.

A vezetési pontok méretének és szerkezetének minden szinten **néhány taktikai páncélozott járműre történő csökkentésével** a magas műveleti parancsnokságok rendkívüli jellegzetességei elhalványulnak a normalizált elektromágneses spektrumban és a háttérben lévő zavaró tényezők között egy olyan harctéren, ahol a páncélozott járművek mindenütt jelen vannak.

Ily módon megfoszthatjuk az ellenséget attól a képességtől, hogy megkülönböztesse a kiemelt és nagy értékű célpontokat, ami értékes képesség a precíziós fegyverek és fegyverrendszerek világában.

Mélység

A mélység a parancsnokságok azon képessége, hogy időben, térben vagy kognitív céllal kiterjesszék a műveleteket.

A teljes spektrumú műveletekben a csapatok integrációja lehetővé teszi a hatékonyság maximalizálását az **emberi**, a **fizikai** és az **információs dimenziókban**.

Az MDO ehhez megfelelő alapot nyújt.

Adatközpontú vezetési pontok

- Az adatközpontú vezetési pontok felváltják a hálózatközpontú vezetési pontokat, és az **adatfejlesztési, -biztonsági és -üzemeltetési mérnökök**re támaszkodnak.
- Ez a megközelítés **rugalmasságot biztosít** a parancsnokok számára, hogy a vezetési és irányítási rendszerüket az **egyedi műveleti követelmények és a vezetői preferenciák alapján finomhangolják**.
- Ahhoz, hogy a vezetési pontok túlélőképesek maradjanak, **meg kell szabadulni**uk minden olyan **dolog fizikai elhelyezésétől**, amelyet "szolgáltatásként" (aaS) nyújtanak.
- Az aaS-megközelítés kiszervezi a tulajdonosi fenntartás terhét, és lehetővé teszi az új technológiák és a mobilitás gyors átvételét.
- Az információs dimenzióra való támaszkodásból adódóan a személyzet egy helyen történő összevonásának szükségességének csökkentése növeli a túlélőképességet.


Következtetések
Katonai Egységes Felhőalapú Eszközrendszer (KEFE)
Többfaktoros azonosítás és hozzáférés-kezelés
Megosztott katonai szolgáltatások
Fejlesztett hálózati kapacitás
Összevont egységes adatközpontok
Megosztott műveleti környezet
Kiterjesztett kiberbiztonság
Alkalmazás migráció
MIMO Troposzféra Műhold
HEFE
4G/5G MIMO WiMAX Harcászati rádió
Helymeghatározók Kamerák Szenzorok
Érzékelők Radarok Szonárok


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

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)