A MAGYAR TUDOMÁNY ÜNNEPE

Katasztrófák Csökkentésének Világnapja
Nemzetközi tudományos konferencia
2023. november 30.

Kritikus infrastruktúrák információs rendszereit ért támadásokat követő lehetséges lakosságvédelmi feladatok vizsgálata

VÁSÁRHELYI ÖRS,
DR. AMBRUSZ JÓZSEF, DR. HABIL. DOBOR JÓZSEF

MTA MAGYAR TUDOMÁNYOS AKADÉMIA

Bemutatkozás

Vásárhelyi Örs

- E-mail: vasarhelyi.ors@gmail.com
- Telefon: +36 -20-343-43-86
- NKE HHK KMDI doktorandusz
- ISO/IEC: 27001:2013 Lead Auditor
- Munkahely: Alverad Technology Focus Kft.
- Linkedin: linkedin.com/in/örs-vásárhelyi-769011174

Dr. habil. Dobor József tű. alez.

- Egyetemi docens
- E-mail: dobor.jozsef@uni-nke.hu
- Telefon: 06 1 432-9000/29-065

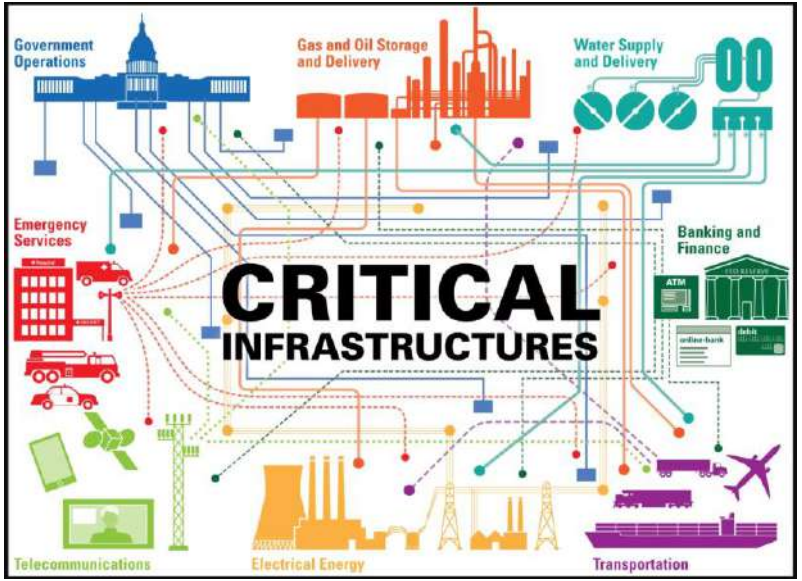
Dr. Ambrusz József tű. ezds.

- egyetemi docens, mb. intézetvezető-helyettes
- E-mail: ambrusz.jozsef@uni-nke.hu
- Telefon: 06 1 432-9000/29-657

Előadás bevezetése

A kritikus infrastruktúrák által biztosított szolgálatások nélkül a modern társadalmunk nem tartható fenn.

A kritikus infrastruktúrákat támogató vagy annak minősülő információs rendszerek kiemelt célpontjai a kibertámadásoknak



Kutatás során alkalmazott módszerek

Primer és szekunder adat és ismeretanyag gyűjtése;

Irodalmi forrásmunkák analitikai elemzése;

Empirikus kutatás;

Irányelvek, szabványok, hatályos jogszabályok megfigyelése, gyakorlatban történő megvalósulásuk elemzése, végrehajtás alatt jelentkező nehézségek keresése.

Kritikus infrastruktúra fogalma

„Magyarországon található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése, e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.”

234/2011 (XI. 10.) Korm. rendelet

Hazai Kritikus Infrastruktúrák ágazatai

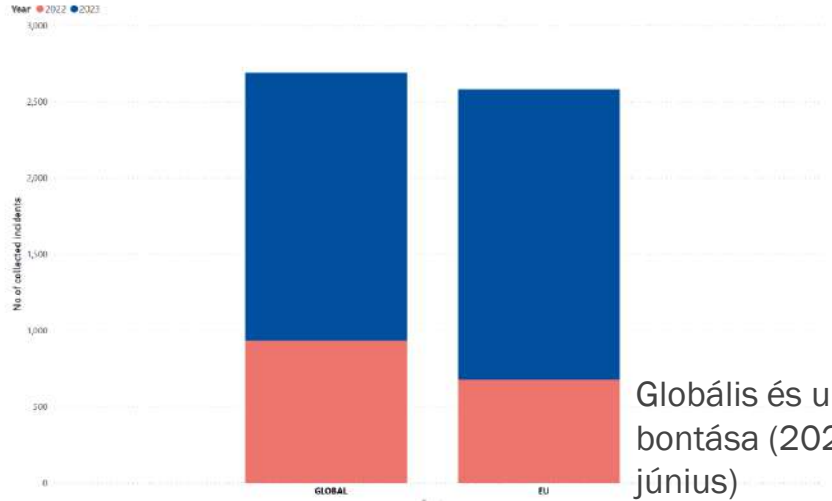
Vonatkozó jogszabályok

- **Tanács 2008/114/EK Irányelve** az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről;
- **2012. évi CLXVI. törvény** a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről;
- **65/2013. (III. 8.) Korm. rendelet** a 2012. évi CLXVI. törvény végrehajtási rendelete;
- **2013. évi L. törvény (Ibtv.)** az állami és önkormányzati szervek elektronikus információbiztonságáról;
- **41/2015. (VII. 15.) BM rendelet** az Ibtv.-ben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről;
- **187/2015. (VII. 13.) Korm. rendelet** az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról;
- **271/2018. (XII. 20.) Korm. rendelet** az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól.

Növekvő fenyegetettség

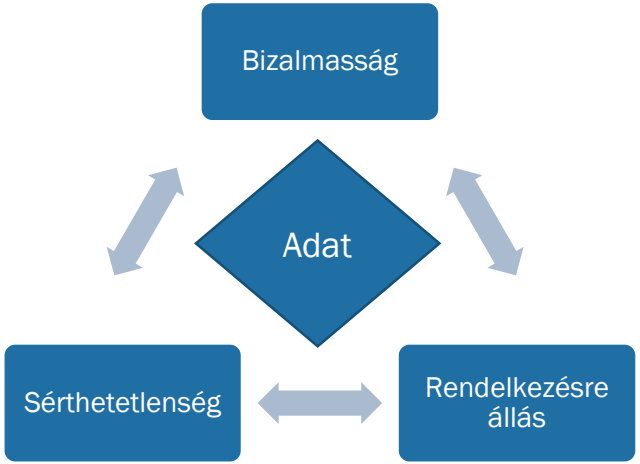
A kibertérből érkező támadások száma évről-évre növekvő tendenciát mutat;

A kritikus infrastruktúrák kiemelt célpontok lehetnek az ilyen jellegű támadásoknak.



Globális és uniós események bontása (2022. július – 2023. június)

Az információbiztonság



- 2013. évi L. törvény -*az állami és önkormányzati szervek elektronikus információbiztonságáról*
- 41/2015 BM rendelet (vhr.)
- ISO/IEC 27001:2022 – Szabvány
- NIST 800-53 rev 5.
- NIS 2 Direktíva – hamarosan…

INFORMÁCIÓ ≠ INFORMATIKA

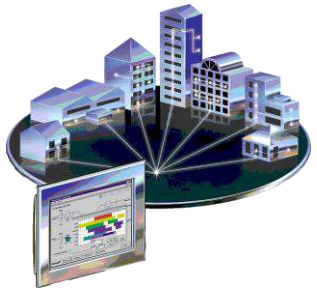
Információbiztonság hazai jogi környezete

A hazai jogszabályok a szervezetek által felmért és azonosított kockázatok csökkentése érdekében hozott információbiztonsági követelmények megvalósítását három nagy kategóriába sorolják:

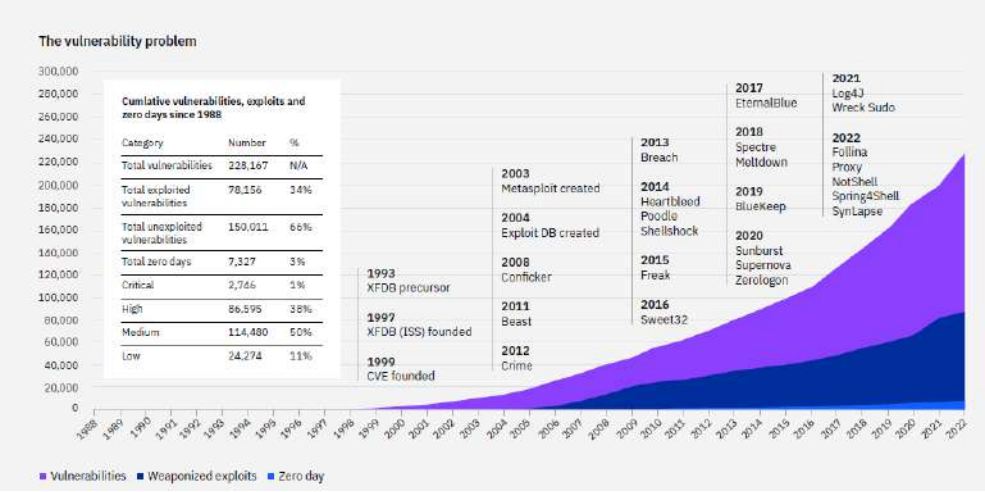
- Adminisztratív Védelmi Intézkedések
- Fizikai Védelmi Intézkedések
- Logikai Védelmi Intézkedések

Ezek elősegítik: a megelőzést és a korai figyelmeztetést, az észlelést, a reagálást, valamint a biztonsági események kezelését.

Kritikus infrastruktúrák OT-környezetének kitettsége



- Az IT hálózat mellett az OT (termelési technológia) hálózat is kiemelt veszélynek van kitéve ezen létfontosságú létesítmények esetén.
- Az ipari folyamatokat vezérlő ipari vezérlőrendszereket ért támadások az elmúlt években jelentős mértékben megnőttek.
- Az OT-t ért kibertámadásoknak valós, fizikai síkon bekövetkező káros következményei is lehetnek!



1988-tól a sebezhetőségek -, biztonsági rések kihasználási -, zero day-ek számának növekedését bemutató grafikon az OT-környezet esetén

NIS 2 direktíva és a kritikus infrastruktúrák

- EU valamennyi tagállamára kötelező érvényű;
- A kritikus infrastruktúrák kibervédelmi képességeinek fejlesztését is célul tűzte ki;
- Számos új ágazat került az irányelv hatálya alá (7+1);
- A kritikus infrastruktúrák üzemeltetői között gördülékenyebb információcsere;
- Nemzetközi kapcsolatok szorosabbra fonása;
- Elektronikus információs rendszerek ellenőrzéseinek megvalósítása tagállami szinten;
- Szankciók bevezetése – akár éves árbevétel 2%-nak megfelelő pénzbírság

CER (Critical Entities Resilience) Direktíva

- Uniós alapvető szolgáltatást nyújtó szervezetek rezilienciájának fokozása;
- Az Unióban egységes ágazatok és alágazatok létrehozása;
- Harmonizált minimumszabályok megteremtése;
- Átültetés a hazai jogszabályi környezetbe, legkésőbb 2024. október 17.;
- Új, visszatartó erejű szankciók kidolgozása;
- kritikus szervezetek rezilienciájával foglalkozó csoport munkaprogramot állít össze 2025 januárig;
- kritikus szervezetek rezilienciájának fokozására minden tagállam stratégiát hoz létre 2026 januárig;
- Minden tagállam az új ágazatoknak és alágazatoknak megfelelően azonosítja valamennyi kritikus infrastruktúráit 2026 júliusig.

Polgári Védelem jogszabály által meghatározott feladatai

gondoskodás a létfenntartáshoz szükséges anyagi javak (különösen víz-, élelmiszer-, takarmány- és gyógyszerkészletek, állatállomány) és a kritikus infrastruktúrák védelméről;

a kárterület felderítése, a mentés, az elsősegélynyújtás, a mentesítés és a fertőtlenítés, és az ezekkel összefüggő ideiglenes helyreállítás, (továbbá a halálos áldozatokkal kapcsolatos halaszthatatlan intézkedések),

közszolgáltatás ellátásának kiesésekor az, emberi életben, egészségben és az anyagi javakban esett kár megelőzése céljából a közszolgáltatás ideiglenes ellátásáról történő gondoskodás.

(2011. évi CXXVIII. tv.)

Polgári Védelmi beavatkozást igénylő esetek

A **víz** -, **energia** -, valamint az **egészségügyi** ágazatokat ért támadások következményeinek csökkentése érdekében szükség lehet a Polgári Védelem beavatkozására.

A veszélyeztetett települések esetén a veszélyelhárítási tervek a beavatkozó állomány döntési mechanizmusainak hatékonyságát segíti.

A lakosság alapvető létfenntartásához szükséges ellátás biztosítása

Amennyiben szükséges az átmeneti kitelepítés és befogadás végrehajtása, társszervek bevonásával.

Polgári Védelem felépítése

62/2011. BM. Rendelet:

A polgári védelmi feladatok ellátására létrehozott egységek típusai különösen:

a) infokommunikációs egység,

b) lakosságvédelmi egység,

c) egészségügyi egység,

d) logisztikai egység,

Megoldási javaslataink

- Kritikus infrastruktúrák elektronikus információs rendszerei esetén információbiztonsági követelmények megerősítése;
- Hazai ICS védelem érdekében egy alkalmazható keretrendszer létrehozása nemzetközi ajánlások mentén és az OT környezettel rendelkező kritikus infrastruktúrák esetén ennek a keretrendszernek alkalmazása fokozottan szükséges.
- A Kritikus infrastruktúra üzemeltetését végző személyzet fokozott IT- és OT biztonságtudatossági képzéseken való részvételének erősítése, megfelelő és naprakész információkat tartalmazó oktatási anyagokkal.
- CISA mintára veszélyhelyzeti forgatókönyvek létrehozása valamennyi ágazat tekintetében – stressztesztek - a kritikus infrastruktúrákat érintő biztonsági eseményekre és válságokra vonatkozó terv
- Folyamatos lépéstartás a technológia fejlődésével (blockchain technológia), hatósági szervek közti szoros együttműködés fejlesztése (NBSZ NKI, BM OKF).
- CER és NIS2 irányelvek sikeres implementációja valamennyi tagállam esetén

Felhasznált Irodalom

- Európai Bizottság: Kritikus infrastruktúrák: a Bizottság felgyorsítja az európai reziliencia kiépítésére irányuló munkát, 2022.10.18., https://ec.europa.eu/commission/presscorner/detail/hu/ip_22_6238
- Az Európai Parlament és a Tanács (EU) 2022/2557 Irányelv: a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről, 2022.12.14., https://eur-lex.europa.eu/legalcontent/HU/TXT/PDF/?uri=CELEX:32022L2557
- Az Európai Parlament és a Tanács (EU) 2022/2557 Irányelv: az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/ 1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv), https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32022L2555&qid=1700772235586
- Kátai-Urbán, M. (2021), Managing the Environmental Risks of Dangerous Goods Warehouses. *Hadmérnök, 15 (4)*, 89-96. https://doi.org/10.32567/hm.2020.4.6
- Pók László: Megjelent a magas szintű uniós kiberbiztonságot biztosító intézkedésekről szóló irányelv (NIS 2), 2023.01.02., https://gdpr.blog.hu/2023/01/02/megjelent_a_nis_2_iranyelv
- Kátai-Urbán Lajos, Vass Gyula. Safety of Hungarian Dangerous Establishments - Review of the Industrial Safety's Authority. (2014) HADMÉRNÖK 1788-1919 IX. 1 88-95.
- Horváth Hermina, Kátai-Urbán Lajos. Assessment of the Implementation Practice of Emergency Planning Regulations Dedicated to the Rail Transportation of Dangerous Goods. (2013) ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 1588-8789 1788-0017 12 1 73-82, 2450737
- Cimer Zsolt; Varga Ferenc: Application of Special Risk Reduction Protective Measures in Combiterminals for Dangerous Goods. *AARMS* : 14. 2. pp 209-218 (2015)
- Ambrusz József, Dobor József, Vásárhelyi Örs: Veszélyes üzemek XXI. századi fenyegetettségekkel szembeni védelmi képességeinek fejlesztési lehetőségei, in XV. évfolyam DAREnet projekt Különszám 2023, https://mpvsz.hu/pv_szemlek/pvszemle2023/index.html
- Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban, *Hadmérnök, 7 (4),* 142-151. (2012), https://hadmernok.hu/2012_4_krasznay.pdf

KÖSZÖNÖM A FIGYELMET!

mta.hu

A MAGYAR TUDOMÁNY ÜNNEPE

MTA MAGYAR TUDOMÁNYOS AKADÉMIA