ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY
A MAGYAR TUDOMÁNY ÜNNEPE
Az MTA programsorozata
Mérnöki Szimpózium a Bánkiban
(ESB 2025)
ESB

Az állami kritikus infrastruktúrák aktuális kiberbiztonsági kihívásai

Current cyber security challenges of state critical infrastructures

[1]Szabó Zsolt Mihály

[1]Óbudai Egyetem, Biztonságtudományi Doktori Iskola, Budapest, Magyarország, szabo.zsoltmihaly@uni-obuda.hu

Összefoglalás

Napjainkban az állam, annak minden szervezete, valamint polgára kiszolgáltatottá vált a többszörösen összetett elektronikus információs rendszereknek kiberterében, amelyek nélkül az állami működés, különböző szolgáltatások biztosítása és igénybevétele megvalósíthatatlanná válik. A kritikus infrastruktúra eszközei az életciklusuk bármely szakaszában – beleértve a tervezést, a terjesztést és az üzemeltetést – sebezhetők lehetnek a kiberfenyegetésekkel szemben. Ez azt jelenti, hogy még a legbiztonságosabb eszközök is veszélynek lehetnek kitéve, ezért gondoskodni kell védelmükről. A tanulmány elemzi a kritikus infrastruktúra védelem alapfogalmait, napjaink kihívásait jogszabályi keretrendszerét és ezeknek való megfelelés lehetséges lépéseit, legvégül kitér a kritikus infrastruktúrák biztonságát fenyegető jövőbeli kihívásokra.

Kulcsszavak: állami kritikus infrastruktúrák, kiberbiztonság, információbiztonság, informatikai biztonság, fenyegetettségek és kockázatok

Abstract

Nowadays, the state, all its organizations, and its citizens have become vulnerable in the cyberspace of multi-complex electronic information systems, without which state operation, provision and use of various services become impossible. Critical infrastructure assets can be vulnerable to cyber threats at any stage of their life cycle – including design, deployment and operation. This means that even the most secure devices can be at risk, so care must be taken to protect them. The study analyzes the basic concepts of critical infrastructure protection, the current challenges, the legal framework, and possible steps to comply with them, and finally addresses future challenges threatening the security of critical infrastructures.

Keywords: state critical infrastructures, cybersecurity, information security, IT security, threats and risks

1 Bevezető

A modern gazdasági berendezkedés mellett a társadalom nincs felkészülve arra, hogy a kiesett infrastruktúrák, eszközök vagy szolgáltatások nélkül működjön, így ezeket - egyértelműen - védeni kell, különös tekintettel arra, hogy azok működése során felhasznált és keletkező információk, továbbá az azokban kezelt adatok jelentős vagyont képviselnek.

A modern társadalmak működésének alapját képezik bizonyos létfontosságú rendszerek, amelyek biztosítják a gazdaság, a közszolgáltatások és a közbiztonság folyamatosságát. Ezeket az ágazatokat kritikus infrastruktúrának nevezzük. A kritikus infrastruktúra sérülése, működési zavarai vagy megsemmisülése komoly következményekkel járhat a társadalomra nézve, veszélyeztetve az emberek jólétét, a nemzetbiztonságot és a gazdaság stabilitását.

2 Kritikus infrastruktúrák

A kritikus infrastruktúrák azok az eszközök, létesítmények, hálózatok és rendszerek, amelyek létfontosságúak a társadalom működéséhez, beleértve az egészségügyet, a gazdaságot, a biztonságot és a közjavakat [1]. Ilyenek például az energiaellátás, a vízellátás, a távközlés, az egészségügyi intézmények, a közlekedési hálózatok, és az élelmiszer-ellátás. Ezeknek a rendszereknek a működése alapvető a lakosság jóléte és a nemzetbiztonság szempontjából, ezért védelmük kiemelt prioritás (lásd 1. táblázat).

Ezek az infrastruktúrák több ágazatot is érintenek, és összekapcsolódnak egymással, így ha sebezhetőek, dominóhatást válthatnak ki más ágazatokban is.

1. táblázat Kritikus infrastruktúrák [2], saját szerkesztés

Ágazat	Alapvető szolgáltatás
Energiaellátás	villamosenergia-hálózatok, földgáz- és üzemanyagrendszerek
Kommunikációs és informatikai rendszerek	távközlési hálózatok, internetkapcsolat, adatközpontok
Ivóvíz- és csatornahálózatok	vízellátó és -tisztító rendszerek
Egészségügy	kórházak, gyógyszerellátás, egészségügyi eszközök és rendszerek
Közlekedés	utak, vasutak, légi és vízi közlekedési infrastruktúrák
Pénzügyi rendszerek	bankok, biztosítótársaságok, tőzsdék működése
Élelmiszerellátás	élelmiszertermelés, -feldolgozás, -logisztika és -kereskedelem

A kritikus infrastruktúrák mindennapi életünk sarokkövei, ezért a társadalom elvárja tőlük, hogy maximális biztonságban működjenek. A különböző kritikus infrastruktúrák általában információs rendszerekből állnak, amelyek komoly jelentőséggel bírnak a különféle támadási felületek között.

A kiberbűnözés napjaink egyik legégetőbb biztonsági problémája, amely a kritikus infrastruktúrákat is fenyegeti. A kiberbiztonság fő célja a kiberbűnözés megelőzése és az elektronikus adatok jogosulatlan felhasználása elleni védelem biztosítása [3].

A kritikus infrastruktúrák elleni kibertámadások általában olyan online támadások, amelyek az alapvető szolgáltatásokat (pl. energiaellátás, vízellátás, közlekedés, kommunikáció) nyújtó rendszereket célozzák. Ezek a támadások jelentős gazdasági károkat és politikai instabilitást okozhatnak, és közvetlen hatással lehetnek az emberek mindennapi életére. A céljuk a működés megzavarása, leállítása, vagy akár a rendszerek irányításának átvétele.

A Microsoft 2025-ös digitális védelmi jelentése szerint a kiberbűnözők egyre nagyobb arányban

célozzák meg a kritikus infrastruktúrákat [4]. Ezeket a támadásokat általában pénzügyi haszon reményében kísérlik meg, vagy néha akár háborús célok is állnak mögöttük. A mesterséges intelligencia növekedése és alkalmazkodása mind a védők, mind a rendszereket fenyegetők számára előnyös, ami új kihívásokat teremt a kiberbiztonságban. A Microsoft jelentése továbbá kimutatta, hogy a kiberbűnözés gyakorisága és kifinomultsága is nőtt, amit a zsarolóvírus-támadások és a mesterséges intelligencia által fokozott taktikák jellemeztek.

3 Kritikus infrastruktúrák védelme

A kritikus infrastruktúrák védelme egyre nagyobb jelentőséggel bír nemcsak Magyarországon, hanem világszerte is.

A kritikus infrastruktúrák biztonsága elengedhetetlen a modern társadalmak működéséhez. A modern világban a kritikus infrastruktúrák védelme nemcsak a fizikai biztonsági intézkedésekre terjed ki, hanem a kiberbiztonságra is. A kritikus rendszerek, mint például az energiaellátás vagy a vízellátás, szorosan kapcsolódnak a digitális hálózatokhoz. Ezért sebezhetőbbek a kiberfenyegetésekkel szemben [5].

2. táblázat EU és hazai jogszabályok [2], saját szerkesztés

Jogszabály	Leírás
2008/114 (EU) irányelv	Ez az EU irányelv a kritikus infrastruktúrák azonosítására és kijelölésére vonatkozik, és alapot nyújt a védelmi intézkedések meghatározásához.
2012. évi CLXVI. törvény	A törvény célja a kritikus infrastruktúrák védelmével kapcsolatos követelmények és az érintett ágazatok felelősségének meghatározása.
2013. évi L. törvény	Magyarországon ez a törvény szabályozza a létfontosságú rendszerek és létesítmények, valamint az állami és helyi önkormányzati szervek információbiztonsági keretrendszerét, amelyeket a Nemzetbiztonsági Szakszolgálat felügyel.
2016/1148 irányelv (EU) (NIS)	Intézkedéseket határoz meg a hálózati és információs rendszerek egységesen magas biztonsági szintjének biztosítása érdekében az egész EU-ban.
2022/2555 irányelv (EU) (NIS2)	Ezen irányelv célja a hálózati és információs rendszerek biztonságának megerősítése, valamint az uniós tagállamok közötti együttműködés javítása.
2024. évi LXIX. törvény	Magyarország kiberbiztonságáról.
2024. évi LXXXIV. törvény	A kritikus szervezetek ellenálló képességéről.

Az Európai Unió irányelveivel összhangban Magyarország is kidolgozta a kritikus infrastruktúrával kapcsolatos saját szabályozási rendszerét (lásd 2. táblázat).

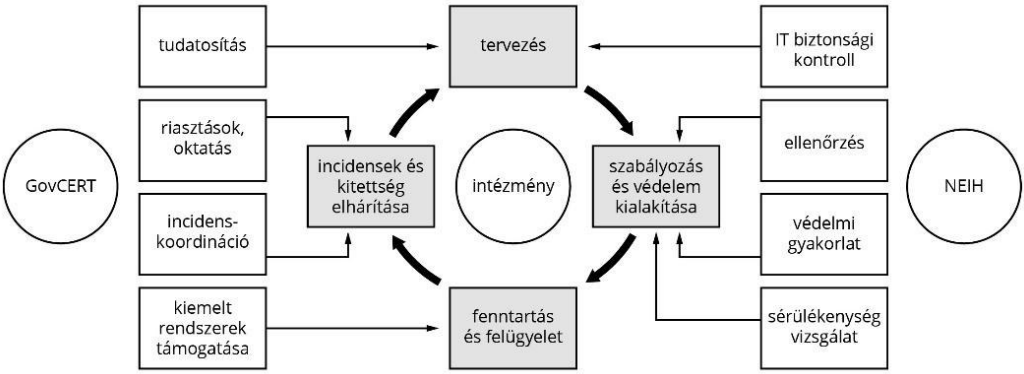
Magyarország esetében rendkívül fontos, hogy ezek a rendszerek megbízhatóan működjenek, mivel megbénulásuk súlyos károkat okozhat az ország működésében. Magyarországon a kritikus

infrastruktúrák védelmét jogszabályok szabályozzák (lásd 2. táblázat). Ezek a jogszabályok határozzák meg azokat az alapvető szabályokat és felelősségi köröket, amelyeket az infrastruktúra üzemeltetőinek be kell tartaniuk ezen rendszerek megbízható működésének biztosítása érdekében.

4 Jogszabályi megfelelés biztosítása

Az elmúlt években jelentős lépéseket tettek hazánkban a kritikus infrastruktúrák kiberbiztonságának megerősítése érdekében. A Nemzeti Kiberbiztonsági Stratégia kidolgozása és a Nemzeti Kiberbiztonsági Intézet létrehozásának a célja, hogy az ország ellenállóbbá váljon a kibertámadásokkal szemben.

Az Intézet felelős a kritikus infrastruktúra üzemeltetőivel való együttműködésért, a kiberbiztonsági kockázatok felméréséért és a megelőző intézkedések koordinálásáért. A kritikus infrastruktúrák üzemeltetői rendszeresen részt vesznek incidenskezelési gyakorlatokon, különböző forgatókönyvek alapján tesztelve a rendszerek ellenálló képességét.



1. ábra Az állami szervezetek IT biztonsági életciklus PDCA modellje [6] alapján, saját szerkesztés

Az Európai Unió és a magyar jogszabályok szigorú követelményeket támasztanak az érintett szervezetek számára (lásd 2. táblázat). Ezek azokat a kulcsfontosságú lépéseket (lásd 1. ábra) tartalmazzák, amelyeket az állami szervezeteknek és vállalatoknak meg kell tenniük a megfelelés érdekében [6]:

Első lépés: A szervezeteknek átfogó kiberbiztonsági stratégiát kell kidolgozniuk, amely kiterjed a hálózati és információs rendszerek biztonságára. Ez magában foglalja a potenciális kockázatok azonosítását, a megelőző intézkedések kidolgozását és a támadásokra adott válaszok meghatározását.

Második lépés: Az Európai Unió és a magyar jogszabályok minden szervezet számára előírják, hogy rendelkezzen incidenskezelési folyamattal. Ez a folyamat biztosítja, hogy a kiberbiztonsági támadásokat és incidenseket gyorsan és hatékonyan kezeljék.

Harmadik lépés: Az egyik alapvető követelmény a folyamatos kockázatelemzés és -értékelés. A vállalatoknak rendszeresen fel kell mérniük hálózati rendszereik biztonsági szintjét, és ennek megfelelően kell kidolgozniuk védelmi intézkedéseiket.

Negyedik lépés: A kiberbiztonság nemcsak technológiai kérdés, az emberi tényezőket is figyelembe kell venni. A rendszeres alkalmazotti képzés elengedhetetlen annak biztosításához, hogy

tisztában legyenek a legújabb fenyegetésekkel és biztonsági intézkedésekkel.

5 Jövőbeli kihívások

Napjaink kihívásai – covid járvány, háborús helyzet, terrorizmus és hibrid fenyegetés növekedése, klímaváltozás, hibrid technológiák, továbbá a kialakult és egyre szorosabbá váló kölcsönös függőségek –, megkövetelik az egyes országok biztonságának maximalizálását, az ellenálló képesség fejlesztését, az eddigi eljárások, gyakorlatok rendezettebb, összehangolását [7] [8].

A kritikus infrastruktúra védelme folyamatosan új kihívások elé állítja az Európai Unió tagállamait. A technológiai fejlődés és a nemzetközi terrorizmus mind olyan tényezők, amelyek befolyásolják a védelmi rendszerek hatékonyságát. Az alábbiakban felsoroljuk azokat a főbb kihívásokat, amelyekkel az elkövetkező években szembesülhetünk [9][10]:

A technológiai fejlődés és a kiberbiztonsági kockázatok, mint például a rendszerek növekvő digitalizációja, új kibervédelmi megoldásokat igényelnek. Továbbá fennáll az ellátási láncok elleni támadások, a DDoS támadások, a mesterséges intelligencia alkalmazása és a posztkvantum titkosítás kiberbiztonságban való alkalmazása veszélye.

A nemzetközi terrorizmus, például az infrastruktúrát érő terrortámadások kockázata továbbra is magas, különösen a közlekedési és energiarendszerek esetében.

6 Konklúzió

A kritikus infrastruktúrák védelme nem csupán nemzeti felelősség, hanem uniós szinten is kiemelt prioritás. A tagállamoknak együtt kell működniük a fenyegetések azonosítása és a rendszerek biztonságának megerősítése érdekében.

A kritikus infrastruktúra védelme folyamatos kihívások elé állítja az Európai Uniót és Magyarországot. Fontos az Európai Unió előírásainak és a magyar jogszabályoknak való megfelelés. A kritikus szervezeteknek intézkedéseket kell tenniük az Európai Unió és a magyar jogszabályok kritériumainak való megfelelés érdekében. A technológiai fejlődés és a nemzetközi terrorizmus mind hatással van a védelmi rendszerek hatékonyságára. Ide tartozik a megfelelő kiberbiztonsági rendszerek fejlesztése is.

7 Hivatkozások

[1] Ambrusz, J., Vásárhelyi, Ö. (2025). A kritikus szervezeti reziliencia és a lakosságfelkészítés nemzetbiztonsági jelentősége a modern fenyegetésekkel szemben. NEMZETBIZTONSÁGI SZEMLE 13. évfolyam (2025) 2. szám 74–93. DOI: 10.32561/nsz.2025.2.6, 1-20.

[2] 2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről. Netjogtár. https://net.jogtar.hu/jogszabaly?docid=a2400084.tv (2025.11.12.), 1-38.

[3] Kovács, L. (2018). A kibertér védelme. Dialóg Campus Kiadó, Budapest, 1-251.

[4] Microsoft Digital Defense Report 2025. Lighting the path to a secure future. https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/ (2025.11.115.), 1-85.

[5] Péter, H., Tibor, F. (2025). Az operatív technológia kiberbiztonsága kritikus infrastruktúrákban. BELÜGYI SZEMLE, 2025 1 Különszám. DOI:10.38146/BSZ-AJIA.2025.v73.SI1, 65-81.

[6] Bodó, A. P., Cser, O. A., Gyaraki, R. E., Kaczur, G.; Lattmann, T., Solymos, Á., Szabó, Zs. M., Tikos, A., Váczi, D., Zámbó, N. (2019). Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára. A hatályosított kiadvány a KÖFOP-2.1.1-VEKOP-15-2016-00001 „A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése" című projekt keretében jelent meg. Nemzeti Közszolgálati Egyetem, Budapest.

[7] Szenes, Z. (2021). A hibrid fenyegetések elleni szakpolitika Magyarországon. HADTUDOMÁNY 2021/4. DOI 10.17047/HADTUD.2021.31.4.39, 39-56.

[8] Ambrusz, J., Dobor, J., Vásárhelyi, Ö. (2024): Létfontosságú rendszerek,- rendszerelemek rezilienciájának fejlesztési lehetőségei az Európai Unió direktíváinak tükrében. Polgári VÉDELMI SZEMLE XVI. évfolyam. https://mpvsz.hu/pv_szemlek/pvszemle2024/index.html (2025.11.25.), 57–69.

[9] IDENTIFYING EMERGING CYBER SECURITY THREATS AND CHALLENGES FOR 2030. European Union Agency for Cybersecurity (ENISA), 2023. ISBN: 978-92-9204-634-7, DOI: 10.2824/117542, 1-60.

[10] ENISA NIS360 2024. ENISA Cybersecurity Maturity & Criticality Assessment of NIS2 sectors. FEBRUARY 2025. ISBN 978-92-9204-687-3, DOI: 10.2824/1378797, Catalogue nr. TP-01-25-002-EN-N, 1-61.