

37. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2025. április 22–24.
Nemzeti Közsolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar

Kiberkockázatok a börtönbiztonságban

Jelige: *Kaptártűzfal*

Pályamunka lezárásának időpontja: 2024.05 hó

2025.



AZ INNOVÁCIÓS ÉS TECHNOLOGIAI MINISZTERIUM ÚNKP-22-2-II-NKE-45 KÓDSZÁMÚ ÚJ NEMZETI KIVÁLÓSÁG PROGRAMJÁNAK A NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS ALAPBÓL FINANSZÍROZOTT SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.

TARTALOMJEGYZÉK

1. RÖVIDÍTÉSEK JEGYZÉKE	5
2. BEVEZETÉS	6
2.1. A vizsgált téma bemutatása	7
2.2. Kutatási célok megfogalmazása	7
2.3. Hipotézisek	8
2.4. Módszertan	8
3. KIBERBIZTONSÁG, KIBERVÉDELEM, KIBERTÁMADÁS	9
3.1. A kibertér	9
3.2. A kiberbiztonság és a kibervédelem	10
3.3. A kibertér veszélyei	12
3.4. Állami szférát ért kibertámadások és hatásaik	15
4. A BV. SZERVEZETTŐL A BÖRTÖNBIZTONSÁGIG	16
4.1. A büntetés végrehajtási szervezet	16
4.2. A büntetés-végrehajtási biztonság	17
4.3. A dinamikus és statikus biztonság	18
5. NEMZETKÖZI TAPASZLATATOK	19
5.1. Port Philip Prison, Ausztrália (2022)	19
5.2. Metropolitan Detention Center, USA (2022)	21
5.3. Evin Prison, Irán (2021)	24
5.4. Idaho State Correctional Institution, USA (2018)	26
5.5. Összegzés	27
6. BV. INFORMATIKA	28
6.1. A rendvédelmi és a büntetés-végrehajtási informatika	28
6.2. A büntetés-végrehajtás informatikai infrastruktúrája	28
6.2.1 A hálózati rendszer	29
6.2.2 Szoftver környezet	30
6.2.3 Hardver környezet	32
7. HAZAI INCIDENSEK ÉS KOCKÁZATOK	34
7.1. Külső fenyegetések	34
7.1.1 E-mail fiókokra érkezett támadások	34
7.1.2 A bv. szervezet weboldalát ért támadás	36
7.2. Belső fenyegetések	36
7.2.1 Fogvatartotti mobiltelefon hardverének és szoftverének módosítása	37
7.2.2 Irrattanulmányozó számítógépek fogvatartotti használata	40
7.3. Összegzés	41
8. AZ ELEKTRONIKUS FOGVATARTOTTI ALAPNYILVÁNTARTÁS	42
8.1. A fogvatartotti alapnyilvántartó rendszer történetisége	42
8.1.1 Fogvatartotti Alrendszer (FAR)	43
8.1.2 A Főnix és a Fogvatartotti Alapnyilvántartás (FANY)	44
8.1.3 Főnix 2	46
8.1.4 Főnix 3	46
8.2. Kapcsolódó informatikai szakrendszerek	49
8.2.1 Navigator rendszer	49
8.2.2 Szolgálati Alkalmazás a Fogvatartás Elősegítésére (SAFE)	51
8.2.3 Előállítási Tevékenységet Támogató Rendszer (ETTR)	53
9. A KUTATÁS	55
9.1. A mintavétel	55
9.2. A kérdőívek eredményei	56

9.3.	Az interjúk eredményei.....	61
9.4.	Elemzés és hipotézis bizonyítás.....	62
9.5.	További elemzések	65
9.5.1	Összefüggések vizsgálata	65
9.5.2	Generációs különbségek megjelenése a vizsgálatban	66
9.5.3	Megengedett leállás.....	67
10.	JAVASLATOK.....	68
11.	ÖSSZEFOGLALÁS	71
12.	IRODALOMJEGYZÉK	72
13.	MELLÉKLETEK.....	77
1. sz.	melléklet.....	77
2. sz.	melléklet.....	83

1. RÖVIDÍTÉSEK JEGYZÉKE

APN	Access Point Name (hozzáférési pont név)
BGP	Border Gateway Protocol (határátkelő protokoll)
Bv.	Büntetés-végrehajtás
BvOP	Büntetés-végrehajtás Országos Parancsnoksága
CCTV	Closed-circuit television (zárt láncú televízió szolgáltatás)
EDR	Egységes Digitális Rádiórendszer
EIR	Elektronikus információs rendszer
EFANY	Elektronikus fogvatartotti alapnyilvántartás
EU	Európai Unió
FAR	Fogvatartotti Alrendszer
GSM	Global System for Mobile Communications (Mobil Távközlés Általános Rendszere)
IBK	Informatikai Biztonsági Kézikönyv
IBSZ	Informatikai Biztonsági Szabályzat
Ibtv.	2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
KEK KH	Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala
MDC	Metropolitan Detention Center
NBSZ	Nemzetbiztonsági Szakszolgálat
NFC	Near Field Communication (rövid hatótávú kommunikáció)
PC	Personal Computer (személyi számítógép)
PDF	Portable Document Format (hordozható dokumentum formátum)
RDP	Remote Desktop (távoli asztal protokoll)
RES	Rendkívüli esemény
SMS	Short Message Service (rövid üzenet-szolgáltatás)
SQL	Structured Query Language (strukturált lekérdezőnyelv)
SZMSZ	Szervezeti és Működési Szabályzat
VPN	Virtual Private Network (virtuális magánhálózat)
WiFi	Wireless Fidelity (vezeték nélküli mikrohullámú kommunikáció)

2. BEVEZETÉS

Digitális őrzés, okostelefonos bűnügyi nyilvántartás, információs „rabterminál”. Három, a közelmúltban megvalósult informatikai fejlesztés a büntetés-végrehajtási szervezet életéből és a lista koránt sem ér véget. Az elmúlt években a digitális technológiák egyre nagyobb teret nyertek a társadalom számos területén, és hasonlóképpen hódítottak a hazai börtönrendszerben is. A társadalomban futótűzként terjedő technológiai újdonságokkal bárhol találkozhatunk, de a börtönélet digitális innovációi sajátságosak, hiszen ezekre a megoldásokra jobbra csak a bástyafalakon belül van igény. Fontos megemlíteni, hogy a börtönbiztonságot szolgáló fizikai falak az eddigiekben jól szolgáltak, de a kibertéri fenyegetettségek elleni biztonság megteremtéséhez már új megközelítésekre van szükség. Ugyanis a kibertérbe áthelyezett büntetés-végrehajtási gyakorlatokkal nemcsak a kockázatok nőnek arányosan, hanem a kibertámadások fizikai végrehajtásra vonatkozó hatásai is.

A szabadságvesztés végrehajtásának helyszínén az utóbbi évtizedek során egyre növekedett az adatok elektronikus rögzítésére való igény, hiszen a szakmai munkát és a vezetői döntéshozatalt az elemző-értékelő tevékenység hatékonyan képes segíteni. Ezen igények kiszolgálását a büntetés-végrehajtási digitalizáció szolgáltatta. Manapság az informatikai rendszerek alkalmazása egyrészt a szerves része a börtönök biztonsági tevékenységének, másrészt közelebb helyezi a fogvatartottak életkörülményeit az információs társadalomhoz, így egyaránt szolgál több büntetés-végrehajtási célt is. Számos jelentős történetiséggel rendelkező szakmai tevékenység kerül át folyamatosan a kibertérbe, így felzárkózva az állami és társadalmi elvárásokhoz. A digitális fejlődéssel együtt ugyanakkor új, eddig ismeretlen veszélyek indukálódnak.

Ahhoz, hogy meghatározzuk ezeket a kockázatokat, elsőként azt szükséges felmérni, hogy milyen mértékben támaszkodik a börtön intézménye alapfeladatainak ellátása során az általa alkalmazott elektronikus információs rendszerekre, valamint, hogy adott esetben bekövetkező kibertámadás milyen mértékben képes akadályokat gördíteni a rendeltetésszerű működés elé.

Az elmúlt években több esetben ért külföldi börtönöket kiberbiztonsági incidens, és az elérhető nyilvános információk alapján olyan következményekkel jártak, amelyek a hazai szervezet képviselőit is gondolkodásra kell, hogy készítsék. Ahány ország, annyi féle szervezeti és végrehajtási forma, így nem lehet egyszerűen párhuzamot vonni a hazai büntetés-végrehajtási

szervezet és a külföldi példák között, helyette inkább önálló vizsgálatot érdemes folytatni. Az alábbi dolgozat erre kíván kísérletet tenni.

2.1. A vizsgált téma bemutatása

A dolgozattal szemben támasztott terjedelmi korlátok nem teszik lehetővé sem a büntetés-végrehajtási elektronikus információs rendszerek teljes körű bemutatását, sem azok minden elemre kiterjedő vizsgálatát. Egy magyar börtön esetében két alapvető terület azonosítható be komoly kockázati elemként. Az első a börtönök biztonságtechnikai rendszere, a második az elektronikus nyilvántartások rendszere. Az első téma feldolgozásának nemzetbiztonsági érintettsége jelentős, ennek okán utóbbi téma került kiválasztásra. Az elektronikus fogvatartotti alapnyilvántartás (a továbbiakban: EFANY) fundamentuma a büntetés-végrehajtás digitális kultúrájának, így kiberbiztonsági szempontú vizsgálata vitathatatlanul indokolt. Az elmúlt években végrehajtott informatikai innovációk az EFANY adatbázisának interfészeit alkalmazzák, így számos szaktevékenységet támogató egyéb informatikai rendszer támaszkodik az EFANY-ra. A rendszer bizalmassága, sértetlensége és rendelkezésre állása fontossá vált a szervezet számára, e három jellemző megsértése által kiváltott hatások vizsgálata érdekes vizsgálatnak ígérkezik.

2.2. Kutatási célok megfogalmazása

A dolgozat általános célja egy olyan rendészettudományi és kiberbiztonsági szempontú büntetés-végrehajtási ismeretanyag összeállítása, amely hiánypótló jelleget lát el a szakirodalmi bázisban. Bemutatni a külföldi börtönöket ért kibertámadásokat és a velük kapcsolatos hatásokat, valamint kitérni a hazai tapasztalásokra is. Szemeztetni az elmúlt évek újgenerációs bv. informatikai megoldásaiból, így betekintést adva a hazai börtönök informatikai életébe, ez által az olvasót részesévé tenni a honi végrehajtás innovációs sikerének.

A kutatás speciális célja felmérni a szervezet egyik legfőbb informatikai szakrendszeréhez, az elektronikus fogvatartotti nyilvántartáshoz (jelenlegi nevén: Főnix 3), valamint az azzal összefüggő büntetés-végrehajtási informatikai szakrendszerekhez köthető interdependencia mértékét. Vizsgálni a rendszer elérhetlensége esetén fellépő fizikai hatások mértékét, valamint, hogy egy kibertámadás milyen mértékig képes befolyásolni egy hazai börtön működését.

2.3. Hipotézisek

A tanulmány két hipotézist állított fel és kíván vizsgálni.

I. Egy bv. intézetet érintő kibertámadás képes jelentős zavarokat okozni a rendeltetésszerű működésben.

II. Egy elektronikus fogvatartotti alapnyilvántartást érintő kibertámadás hatásai érinthetik a fogvatartotti alapjogokat.

Az I. számú hipotézis a börtönt érintő kibertámadás kifelé (a szervezet felé) irányuló hatását vizsgálja. Azt, miszerint egy kiberincidens kezelhető-e bv. biztonsági szempontból rendkívüli eseményként (RES). Másképpen fogalmazva azt, hogy az információbiztonsági hatásokon felül egy kibertérben érkező incidens képes-e olyan mértékű hatásokat gyakorolni, amelyre a börtönnek biztonsági intézkedésekkel kell válaszolnia, hogy visszaállítsa a biztonság általános állapotát.

Az II. számú hipotézis a fogvatartotti elektronikus alapnyilvántartást érintő kibertámadás befelé irányuló hatását, vagyis a börtön legmélyebb rétegében megjelenő károkat kívánja vizsgálni. Azt, hogy a börtönben fogvatartott személyek alapjogai (pl.: tisztességes eljáráshoz való jog,¹ magánélethez és családhoz való jog,² stb.) sérülhetnek-e egy kibertámadás által. Amennyiben ez valós kockázatot jelent, úgy bekövetkezés esetén az alapot szolgáltat a fogvatartottnak a szervezettel szembeni kártalanítási eljárások megindítására, ezáltal pénzbeli kártérítések kifizetésére.³

2.4. Módszertan

Az alkalmazott módszertan egyaránt alkalmaz kvalitatív (dokumentumelemzés, történeti forráselemzés, interjú), valamint kvantitatív (kérdőív) eszközöket is. Forráselemzésként nemzetközi és hazai börtönöket ért kibertámadásokkal összefüggő információk kerülnek elemzésre. Dokumentumelemzésként jogszabályok, belső használatú dokumentumok (pl.: rendszertervek, módszertani útmutatók, kézikönyvek stb.) kerültek feldolgozásra a kívánt információbázis összeállítása érdekében. A kutatás módszertanának gerincét azonban a

¹ Magyarország Alaptörvénye XXVIII. cikk (1).

² Emberi Jogok Egyetemes Nyilatkozata 12. cikk.

³ Emberi Jogok Egyetemes Nyilatkozata 8. cikk.

büntetés-végrehajtás szervezetének személyi állományú tagjai által kitöltött kérdőívek és vezetői interjúk adják.

3. KIBERBIZTONSÁG, KIBERVÉDELEM, KIBERTÁMADÁS

A címben szereplő három fogalom definíciójáról a hazai és külföldi szakmai terminológia határozottan, de nem egységesen gondolkodik. A büntetés-végrehajtási kiberérintettség vizsgálata érdekében szükséges az alapvető meghatározások bemutatása, így a következő fejezet ezt kívánja teljesíteni.

3.1. A kibertér

Mi a kibertér? Hol helyezkedik el? Milyen jellemzőkkel írható le? E kérdésekre számos meghatározás létezik a szakirodalmi bázisban, azonban a különböző tudományos terminológiákból eredő definíciós kísérletek bemutatását a későbbiekre hagyva, először érdemes lehet a szót a maga egyszerűségében értelmezni. A „*kiber*” előtag jelentését számos forrás az 1940-es években a görög *kübernétész* (kormányos) szóból alkotott *kibernetika* kifejezésből származtatja, ⁴ amelyet egy komplex tudományos irányzat megjelölésére alkalmaznak manapság. A kibernetika a szabályozás, vezérlés, információfeldolgozás és továbbítás általános törvényszerűségeit kutatja.⁵ A „*kiber*” kifejezést tulajdonképpen a „*kibertér*” leegyszerűsített változata, ekként került be a hétköznapi szóhasználatba.⁶ Érdekes kísérletnek bizonyulhat egy innovatív, a „*kutyaharapást szőrével*” megközelítés alkalmazása, és lekérni „*kiber*” kifejezés jelentéstartalmát az emberi visszajelzésből származó, megerősítésen betanított, OpenAI⁷ elnevezésű mesterséges intelligencia laboratórium ChatGPT (Generative Pre-trained Transformer) elnevezésű mesterséges intelligencia chatbotjától. A lekérdezés az alábbi eredményt produkálta:

⁴ Wiener, Norbert (1948): *Cybernetics, or Communication and Control in the Animal and the Machine*, MIT Press, Cambridge.

⁵ Muha Lajos – Krasznay Csaba (2014): *Az elektronikus információs rendszerek biztonságának menedzselése*, Nemzeti Közszerológati Egyetem, Budapest. Online: <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/7135/Az%20elektronikus%20inform%C3%A1ci%C3%B3s%20rendszerek%20biztons%C3%A1g%C3%A1nak%20menedzsel%C3%A9sej%C3%B3.pdf?sequence=5&isAllowed=y>

⁶ Muha Lajos: *Kiberhadviselés – kiberbűnözés*, In: IDC IT Security Konferencia, Budapest, 2012.03.22.

⁷ Az OpenAI egy mesterséges intelligencia kutatólaboratórium, amely az OpenAI LP vállalatból és anyavállalatából, a nonprofit OpenAI Inc.-ből áll.

„A "kiber" szó a számítógépekkel és az információs technológiával (IT) kapcsolatos dolgokra utal. Gyakran használják az internethez, a digitális kommunikációhoz és az online biztonsághoz kapcsolódó fogalmak leírására.”⁸

Kovács (2018) megállapításában a kibertér a felhasználók, eszközök, szoftverek, folyamatok, tárolt vagy átvitel alatt lévő információk, szolgáltatások és rendszerek gyűjtőfogalma, amelyek közvetlenül vagy közvetett módon számítógép-hálózathoz vannak kapcsolva.⁹

Magyarország Nemzeti Kiberbiztonsági Stratégiája a kibertér megfogalmazásával együtt meghatározza a magyar kiberteret is. A stratégia alkotója szerint az a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint e 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.¹⁰

3.2. A kiberbiztonság és a kibervédelem

A biztonság szó jelentésének meghatározásával némiképpen könnyebb dolgunk van, hiszen ez az állapot Maslow¹¹ szerint az alapvető fiziológia szükségletek kielégítését követő szükséglet, saját tapasztalásunk alapján jó eséllyel ismerjük az általa hordozott jelentéstartalmat is.¹² Általános megközelítésben a biztonság tulajdonképpen a dolgoknak, életviszonyoknak olyan rendje, vagy állapota, amelyben kellemetlen meglepetésnek, zavarnak, veszélynek nincs vagy alig van lehetősége, amelyben ilyentől nem kell félni.¹³ Itt fontos megemlíteni, hogy az angol (amerikai) nyelv nem tesz különbséget a témában a védelem és a biztonság között. A kettő

⁸ Open AI Chat GPT mesterséges intelligenciával történő angol nyelvű lekérdezés. Online: <https://openai.com/blog/chatgpt/> Alkalmazva: 2022.12.29.

⁹ Kovács László (2018): A kibertér védelme, Dialóg Campus Kiadó, Budapest p. 18.

¹⁰ 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról 3.

¹¹ Abraham Maslow (1908-1970) amerikai pszichológus, a Maslow-piramis és a D-B motiváció elmélet kidolgozója.

¹² Paul W. King (2009): Climbing Maslow's Pyramid, Matador, Leicester. ISBN: 9781 8487 61124 Online: https://books.google.hu/books?id=bDJNJ53dFzSC&printsec=frontcover&hl=hu&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

¹³ A magyar nyelv értelmező szótára, első kiadás: 1959–1962, Akadémiai Kiadó, Online: <https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-a-magyar-nyelv-ertelmezo-szotara-1BE8B/> Utolsó letöltés: 2022.12.29.

közötti lényegi különbség a későbbiekben bemutatásra kerül. Az eddigiek értelmezéséből megállapíthatjuk, hogy a biztonság tulajdonképpen az a veszélyektől, károkozásoktól megóvó állapot, amelyet mindenkor el kívánunk érni annak fenntartására irányuló intézkedések alkalmazásával.

A kiberbiztonság mögött tehát a részdefiníciók alapján együttesen találjuk a felhasználó, a szolgáltatás, az informatika, az információs technológia együttes érintettségében létrejött, elérni kívánt állapotot.

Kovács (2018) szerint a kiberbiztonság a biztonságot meghatározó eszközök, politikák, koncepciók, technológiák, irányelvek, kockázatkezelési módszerek, tevékenységek, képzések, valamint a legjobb gyakorlatok összessége, amelyek arra irányulnak, hogy megvédjék a számítógépes környezetet, valamint az ezt használó szervezetek és felhasználók eszközeit, rendszereit.¹⁴

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) az általános rendelkezések között saját maga alkalmazásában az alábbiak szerint rögzíti a meghatározást: „*Kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kibertér megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.*”¹⁵

A törvényi megfogalmazásból egyértelműen értelmezhető a kiberbiztonság feladata és célja. A tevékenység feladata a kibertéri kockázatok kezelése annak érdekében, hogy a társadalmi és gazdasági folyamatoknak otthont adó kibertér célként, megbízható környezetté alakítsa.

A már kifejtett kiberbiztonság mellett ki kell térnünk a kibervédelem meghatározására is. A kibervédelem olyan tevékenységeket takar, amelyek a biztonság megteremtésére és fenntartására irányulnak.¹⁶ A fogalmat az Ibtv. is deklarálja, miszerint a kibervédelem: a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését.¹⁷ A védelem, mint tevékenység a legegyszerűbb modellezésben egy kétszereplős

¹⁴ Kovács László (2018): A kibertér védelme, Dialóg Campus Kiadó, Budapest p. 18.

¹⁵ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1.§. 26.

¹⁶ Kovács László (2018): A kibertér védelme. Dialóg Campus Kiadó, Budapest p. 18.

¹⁷ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1.§. 27.

tevékenység során valósul meg. A védelem az a tevékenység, amely során a védő a védett érték állapotát igyekszik megőrizni (védeni), míg a támadó a körülményektől függően különböző támadási útvonalon keresztül kívánja elérni (támadni), hogy a védendő értékkel kölcsönhatásba lépjen. A kibertérben a kibervédelem olyan komplex, aktív tevékenység, amely a kiberbiztonság elérése törekszik.

3.3. A kibertér veszélyei

Az eddigiekben bemutatásra került a kibertérben elérni kívánt állapot, a kiberbiztonság, valamint az annak elérésére irányuló védelmi tevékenység is. Azonban ahhoz, hogy megfelelő intézkedéseket tudjunk hozni, ismernünk kell azon tényezőket, melyek negatívan képesek hatni a kívánt állapotra. Kovács (2018) ezeket a tényezőket könyvében két részre bontja, a „Sérülékenységek, módszerek, eszközök”, valamint a „Támadók, avagy a kibertér (egyéni és csoportos) szereplői” csoportjára.¹⁸ Pontos listát felállítani a fenyegetésekről lehetetlen küldetés, hiszen azok száma napról napra nő. A terjedelmi korlátok tartása érdekében a fenyegetések teljes körű bemutatása helyett talán azok aktuális trendjeire és a velük kapcsolatos tapasztalatokra érdemes kitérni.

Népszerű támadási típusok

Az ENISA legfrissebb jelentése¹⁹ azonosította a legfontosabb fenyegetéseket a 2021. július és 2022. július közötti időszakban. Továbbá, vizsgálta a velük kapcsolatban megfigyelt fő trendeket, a fenyegetések szereplőit és támadási technikákat. Ezzel összefüggésben az alábbi fő fenyegetések kerültek beazonosításra.

1. Ransomware

Az első támadási forma az elmúlt években is főszereplő volt, azonban a vizsgált időszakban számos nagy horderejű és sajtónyilvánosságot kapott incidenssel került a fő fenyegetések körébe. A ransomware támadás egy olyan típusa a fenyegetéseknek, ahol a támadók átveszik az irányítást a célpont eszközei felett és váltságdíjat követelnek az eszközök rendelkezésre

¹⁸ Kovács László (2018): A kibertér védelme. Dialóg Campus Kiadó, Budapest p. 120.

¹⁹ European Union Agency for Cybersecurity (2022): Enisa Threat Landscape 2022 Online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

állításának visszaszolgáltatásáért. A támadás célja egyébként nem minden esetben az anyagi haszonszerzésre vonatkozik.²⁰

2. Malware

A rosszindulatú számítógépes programok köre. Ebbe a csoportba számos olyan szoftver vagy firmware tartozik, amelynek célja olyan jogosulatlan folyamatok végrehajtása, amelyek hátrányosan befolyásolják egy rendszer bizalmasságát, integritását és elérhetőségét. Hagyományosan ilyenek a vírusok, programférgek, trójai programok, valamint ide került besorolásra a kémprogramok és reklámprogramok bizonyos formái is.²¹

3. Social Engineering fenyegetések

Olyan tevékenységek széles köre, melyek a humán tényezőt használják ki annak érdekében, hogy információkat szerezzenek, vagy bizonyos szolgáltatásokhoz hozzáférjenek. A manipulációt, valamint eszközeit alkalmazva ráveszik a felhasználókat, hogy nyissanak meg bizonyos dokumentumokat, fájlokat, elektronikus üzeneteket stb., vagy illetéktelen személyeknek biztosítsanak hozzáférést.²²

4. Adatok elleni fenyegetések

Ezen fenyegetések körében azokat a módokat találjuk, amelyeknek az adatforrások a célpontjai, valamint céljuk, hogy ahhoz jogosulatlan hozzáférést szerezzenek. Ezt követően további céljuk az adatok nyilvánosságra hozatala vagy manipulálása. Technikailag az adatok elleni fenyegetések felbonthatóak adatsértésre és adatszivárgásra.²³

5. Szolgáltatásmegtagadás

Az elérhetőség számos fenyegetés célpontja, ezek közül kiemelkednek a DDoS támadások. A DDoS támadás a rendszert veszi célba, és az adatok rendelkezésre állását célozza. Nem egy új fenyegetéstípusról van szó, azonban manapság is jelentős szerepet kap a fenyegetések sorában.

²⁰ European Union Agency for Cybersecurity (2022): Enisa Threat Landscape 2022. p. 8. Online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

²¹ European Union Agency for Cybersecurity (2022): Enisa Threat Landscape 2022. p. 8. Online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

²² European Union Agency for Cybersecurity (2022): Enisa Threat Landscape 2022. p. 8. Online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

²³ European Union Agency for Cybersecurity (2022): Enisa Threat Landscape 2022. p. 8. Online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

A felhasználók nem férnek hozzá adataikhoz, vagy a szolgáltatáshoz. Ennek megvalósítása történhet a rendszer erőforrásinak kimerítésével vagy a hálózati infrastruktúra túlterhelésével.

6. Internetes fenyegetések

Az internet manapság már alapvető szolgáltatás a munkavégzéshez, a tanuláshoz és a társadalmi érintkezéshez egyaránt. Ebbe a csoportba azon fenyegetések tartoznak, amelyek az internet elérhetőségét befolyásolják, mint például a BGP (Border Gateway Protocol).²⁴ A protokoll ismert módon sérülékeny az eltérítési támadásokkal szemben (BGP hijacking), amelyek alkalmasak lehetnek az internetes kommunikáció átirányítására és megszerzésére, valamint egyes szolgáltatások elérésének ellehetetlenítésére.²⁵

7. Dezinformáció

A dezinformációs (félretájékoztatás) kampányok még mindig elterjedtek, a jelenségre a közösségi média is egyfajta katalizátorként hat. Manapság a közösségi oldalak, a hírek és sajtómédiumok, sőt még a keresőmotorok által szolgáltatott adatok is fő információforrássá váltak. Azonban számos nem hiteles információ is megjelenik ezeken a felületeken, melyek a felhasználókat félrevezetik, sőt az Orosz-Ukrán háború kifejezetten új módszereket hozott a dezinformációs műveletek körébe.²⁶

8. Ellátási lánc támadások

Az ellátási lánc támadások a szervezet és beszállítóik közötti kapcsolatot célozza. Az ilyen jellegű támadás akkor sorolható ide, ha legalább két támadás kombinációjából áll, valamint akkor, ha a szállító és a megrendelő egyaránt célpont. A szakmában kifejezetten ismert SolarWinds incidens volt az első ilyen eset, amely rávilágított az ellátási láncot ért támadások kiemelt következményeire.²⁷

²⁴ European Union Agency for Cybersecurity (2022): Enisa Threat Landscape 2022. p. 9. Online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

²⁵ Online: <https://nki.gov.hu/it-biztonsag/tanacsok/igy-ellenorizhetjuk-hogy-az-internet-szolgaltatonk-ved-e-minket-a-bgp-elteriteses-tamadasok-ellen/> Utolsó letöltés. 2023.01.17.

²⁶ European Union Agency for Cybersecurity (2022): Enisa Threat Landscape 2022. p. 9. Online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

²⁷ European Union Agency for Cybersecurity (2022): Enisa Threat Landscape 2022. p. 9. Online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

3.4. Állami szférát ért kibertámadások és hatásai

Kiemelt figyelemmel kell lenni az ENISA jelentésének – a kutatási témában kifejezetten releváns – azon megállapítására, amely szerint a vizsgált időszakban a közigazgatás, valamint a kormányzati szolgáltatók ellen elkövetett kibertámadások száma kiemelkedő (24,21 %) volt a többi mért adathoz képest (digitális szolgáltatók 13,09 %, általános közösségek 12,43 %, szolgáltatók 11,78 %, pénzügyi szektor 8,64 %).²⁸ Továbbá, kifejezetten érdekes a jelentésben megjelenített hatáselemzés, amely szerint a kibertámadás hírnévre gyakorolt hatása tekintetében, a közvélemény negatív megítélése legjobban a közigazgatási/kormányzati szektort érintette, melynek oka valószínűleg az állami szervbe vetett bizalom elvesztésének tudható be. A támadások hatásai (pl.: nem elérhető rendszerek, sérült adatfájlok) vonatkozásában is nagyszámban volt érintett a kormányzati szektor, melynek oka az állami szektort ért ransomware támadásokban rejlik. Ugyanerre (ransomware) vezethető vissza a gazdasági veszteségek köre, ahol a pénzügyi szektort a kormányzati szektor követi a hatásvizsgálat tekintetében. A társadalmi hatások okozásában is a kormányzati terület a legjelentősebb, hiszen a személyes adatok érintettsége számottevő. A fizikai hatásokkal – amelyek nehezen mérhetőek – összefüggésben a közzétett információk, illetve a megbízható adatok hiányának jelenségére visszavezethetően szintén a kormányzati szektor érintett legjobban.

²⁸ European Union Agency for Cybersecurity (2022): Enisa Threat Landscape 2022. p. 14. 4. ábra. Online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

4. A BV. SZERVEZETTŐL A BÖRTÖNBIZTONSÁGIG

Az alábbi fejezetben bemutatásra kerül a vizsgálati közeg, vagyis a büntetés-végrehajtási szervezet, a szervezet által irányított bv. szervek típusai, a szervek biztonságával összefüggő meghatározások, valamint a büntetés-végrehajtás statikus és dinamikus biztonságának jellemzői.

4.1. A büntetés végrehajtási szervezet



1. kép: A büntetés-végrehajtási szervezet logója²⁹

A büntetés-végrehajtási szervezet (a továbbiakban: bv. szervezet) a szabadságelvonással járó büntetéseket, intézkedéseket, büntetőeljárási kényszerintézkedéseket, a szabadságvesztésből szabadultak utógondozását, valamint a büntetés-végrehajtási pártfogó felügyelői feladatokat végrehajtó állami, fegyveres rendvédelmi szerv.³⁰ A bv. szervezet a feladatainak törvényes ellátásával járul hozzá a közrend és a közbiztonság erősítéséhez. A szervezetet a Kormány a büntetés-végrehajtásért felelős miniszter (jelenleg a Belügyminiszter) útján irányítja. A központi vezető szerve a Büntetés-végrehajtás Országos Parancsnoksága (a továbbiakban: BvOP), élén a szervezet országos parancsnokával.³¹ A szervezetben a BvOP irányítása alatt büntetés-végrehajtási intézetek (a köznyelvben: börtönök), intézmények (oktatási, rehabilitációs, egészségügyi), valamint a fogvatartottak foglalkoztatására létrehozott gazdasági társaságok és költségvetési szervek találhatóak. Ezeket együttesen bv. szerveknek nevezi a szervezeti törvény.³²

²⁹ A kép forrása: A BvOP belső használatú forrásából.

³⁰ 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről. 1. § (1).

³¹ 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről. 1. § (2).

³² 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről. 2. § (5).

Jelenleg az országban 32 bv. intézet, 10 bv. gazdasági társaság, illetve 2 bv. intézmény működik.³³ A szervezetben dolgozó személyi állomány száma több, mint 9000 fő,³⁴ a bv. intézetekben és intézményekben elhelyezett fogvatartottak létszáma meghaladja a 20 000 főt.³⁵

A bv. szervezet Szolgálati Szabályzata³⁶ a szervezet tevékenységeit biztonsági, egészségügyi, foglalkoztatási, nevelési és nyilvántartási szakfeladatra bontja. Továbbá kapcsolt szakfeladatokat is nevesít, amelyek az energetikai, a gazdasági (pénzügyi, anyagi, technikai, számviteli, beruházási), a hivatali (tájékoztatási, titkársági, ügykezelési), a humánpolitikai, az informatikai, a jogi, e mellett egyéb jogszabály alapján meghatározott egyéb feladat, mint a környezetvédelmi, munkavédelmi, tűzvédelmi és a védelmi szakfeladat.³⁷ A bv. szervezet szakfeladatai sokrétűek, azonban a börtönök mindennapi életében a biztonság jelenik meg elsődleges tevékenységként.

4.2. A büntetés-végrehajtási biztonság

A büntetés-végrehajtási biztonság a szervezeti munka alaptevékenysége, hiszen ez az állapot nélkülözhetetlen minden büntetés-végrehajtási szervben (a továbbiakban: bv. szerv). A biztonság köznyelvi értelmezése: „veszélyektől vagy bántódástól mentes (zavartalan) állapot”.³⁸ Ezzel összefüggésben természetesen helyén való Sztodola (2020) megállapítása, miszerint ezt az állapotot elérni lehetetlen,³⁹ azonban az arra való törekvés jelenik meg elsődleges célként. A biztonsági tevékenység egy olyan jellegű működés, amelynek egyes jelentős történetiséggel bíró fundamentumai örök érvényűek maradnak, ugyanakkor más részterületei folyamatosan igénylik az idomulást a jelenlegi korok új kihívásaihoz és fenyegetéseihez, így hát ezzel a kettősséggel terhelve igyekszik elérni a kívánt állapotot. A bv. szervek tekintetében amennyiben ez az állapot kielégítő, abban az esetben kaphatnak a további szakfeladatok teret és lehetőséget a működésre. Ha a biztonság aktuális állapota nem kielégítő, akkor minden rendelkezésre álló erőforrás a szükséges mértékben felhasználásra kerül a kívánt állapot elérése / visszaállítása érdekében.

³³ 6/2023. (I. 31.) BVOP utasítás a Büntetés-végrehajtás Országos Parancsnoksága Szervezeti és Működési Szabályzatáról 6. sz. melléklete

³⁴ Online: <https://www.bv.gov.hu> Utolsó letöltés 2022.12.12.

³⁵ 2023.03.08-ai adat, belső forrásból.

³⁶ 21/1997. IM rendelet a büntetés-végrehajtási szervezet Szolgálati Szabályzatáról.

³⁷ 21/1997. IM rendelet a büntetés-végrehajtási szervezet Szolgálati Szabályzatáról 2. § (3).

³⁸ A Magyar Értelmező Kéziszótár.

³⁹ Czenczer és Sztodola (2020): A biztonsági tiszti munka jogi és szakmai vonatkozásai, in Közbiztonság, Ludovika Egyetemi Kiadó, Budapest. p. 1078. Online: <http://hdl.handle.net/20.500.12944/16197>

4.3. A dinamikus és statikus biztonság

A bv. szervezet biztonsága tovább bontható dinamikus és statikus biztonságra. Statikus biztonság alatt azon tevékenységek, eljárások és eszközök körét kell érteni, melyek a fogvatartottak biztonságra veszélyes cselekményeinek megakadályozására, megszüntetésére irányulnak, azonban azok egyfajta fizikai akadályként jelennek meg, vagy a fizikai végrehajtást szabályozzák. Ezek az elemek a biztonsági tevékenységet szabályozó rendelkezések, hír és biztonságtechnikai berendezések, a kényszerítő és mozgáskorlátozó eszközök, a tűz-, és munkavédelmi eszközök, védőfelszerelések, valamint a biztonsági létesítmények (bástyafal, őrtorony stb.).⁴⁰

A dinamikus biztonság elemei azon tevékenységek köre, melyek a fogvatartottak megismerésén, társas viszonyainak befolyásán, életrendjük és életminőségük alakításán alapul. Ezek az eszközök a megfigyelés, az értékelés, a célorientált információs rendszer, a tájékoztatás, a napirend és házirend, a bánásmód, az alkalmazott fegyelmezési és jutalmazási gyakorlat, valamint a reagálás és a beavatkozás lehetősége. A statikus biztonság jelentős történetisége mellett a dinamikus terület elemei az utóbbi évszázadban, a szociológiai tudományok fejlődése okán kerültek integrálásra a büntetés-végrehajtási tevékenységbe. A fogalom már több mint 15 évvel ezelőtt megfogalmazásra került az Európa Bizottság ajánlása által is.⁴¹

A büntetés-végrehajtási kiberbiztonság elhelyezkedését valahol a statikus és dinamikus biztonság kötelékében kellene keresnünk, ám annak pontos meghatározása még nem került szakmai alkotó kezek közé. A már bemutatott definíciókat megismerve biztosak lehetünk abban, hogy a kiberbiztonság, mint állapot, vitathatatlanul része a büntetés-végrehajtási biztonság állapotának, a kérdés inkább az, hogy mekkora a betöltött szerep mértéke és annak zavara milyen valós hatásokat gyakorol a fizikai térre, ezáltal hogyan befolyásolja a biztonság elemeinek érvényesülését. Az esetek megismeréséhez megfelelő példa a nemzetközi tapasztalások megismerése, hiszen az utóbbi években több ilyen esemény is történt börtönöket érintően.

⁴⁰ Czenczer Orsolya és Pallo, József (2014) A büntetés-végrehajtási szervezet felsőszintű irányításának és vezetésének elvei, specifikumai. In: A rendészeti szervek vezetés- és szervezésmélete. Nemzeti Közszerzői Jogi Hivatal, Budapest, p. 185.

⁴¹ Európai Börtönszabályok - A Miniszteri Bizottság Európai Börtönszabályokról szóló R/2006/2 ajánlása a Tagállamok számára p. 19.

5. NEMZETKÖZI TAPASZLATATOK

Börtönöket ért kiberincidensekről szóló hivatalos közlemények, avagy konkrét esettanulmányok – nyilvános forrásként – nem igazán érhetőek el, így a témában a nemzetközi irodalomban történő dokumentum-kutatás csekély mértékben talált validált információkat. Ennek okai azok lehetnek, hogy egyrésztől nemzetbiztonsági érdekből nem kommunikálják az ilyen eseteket, valamint, hogy az ilyen incidens negatív hatást gyakorol az adott szervezet társadalmi megítélésére, tehát előnyös a szervezet számára, ha rejtve marad a nyilvánosság előtt az esemény. Azonban a börtönök kiberincidensei a társadalomra kifejtett hatásukról egyértelműen beazonosíthatóak. A következmények okozta megkeresésekre reagálva az érintett szervek az ilyen jellegű események megtörténtét több esetben elismerték sajtóorgánumnak, azonban a témában a kiadott tájékoztatások cseppet sem nevezhetők teljeskörűnek és nem szolgáltatnak transzparenciát. Az így fellelhető információkból – természetesen azok hitelességét helyén kezelve – megállapíthatjuk az események bekövetkezésének idejét, jellegét és az érintettség mértékét.

5.1. Port Philip Prison, Ausztrália (2022)



2. kép: Port Philip Prison, Truganina, Ausztrália⁴²

A G4S Correctional Services privát szolgáltatóként több börtön részére nyújt szolgáltatásokat. 1997 óta kezeli és üzemelteti a Melbourne nyugati külváros részében található Port Philip Prison elnevezésű maximális biztonságú börtönt, melynek fogvatartotti férőhelye 1087 fő.⁴³ A börtön alapfeladata ellátása mellett egészségügyi szolgáltatást is végez fogvatartottak részére.

⁴² A kép forrása: <https://www.forensicare.vic.gov.au/wp-content/uploads/2017/11/PPP.jpg>

⁴³ Online: <https://www.g4s.com/en-au/what-we-do/justice-services/custodial> Utolsó letöltés: 2022.12.20.

Az intézet üzemeltetése a magyar PPP programhoz⁴⁴ hasonlóan a magánszférával közösen valósul meg, tehát külső szolgáltatók végzik az üzemeltetési és karbantartási feladatokat. Azonban az említett magyar modelltől eltérve, itt a felügyeleti és egészségügyi szolgáltatásokat, valamint az oktatási szolgáltatásokat is a megbízott szolgáltatók végzik.⁴⁵

2022. július elejére tehető a Port Philip Prison elleni kibertámadás. Az incidenst követően a nyilvánosság felé közvetített információk nem nevezhetőek maradéktalannak, így a kutatás során fellelt írásos közlések is szükséztlenül közvetítették tovább az információt, egyértelműen megállapítható a teljes körű tájékoztatás hiánya. A 2022. szeptemberében megjelent sajtó értesülések szerint a fenti időszakban hackerek vették át az irányítást a börtön informatikai hálózata fölött, melynek okán közel 1000 fogvatartott személyes látogatási és videó alapú kommunikációs lehetőségét kellett felfüggeszteni több napra. A tájékoztatás szerint a börtön személyzete az incidenst követően értesítette Victoria Police⁴⁶ kiberincidens-elhárító csapatát a fejleményekről. Tájékoztatásukban közölték, hogy az incidensre válaszul az intézet vezetése biztonsági intézkedéseket hajtott végre a börtön alkalmazottjainak és a fogvatartottak biztonsága érdekében. Az incidens során a börtönt érintő telefonhívások is korlátozásra kerültek, azonban a szociális munkások és az ügyvédek továbbra is használhatták azt. A G4S szóvivőjének nyilatkozata szerint kiberbiztonsági incidens történt, de kiemelte, hogy a fogvatartottakat és a személyzetet nem érintette.⁴⁷

A Guardian Australia értesülései szerint az incidens okozója egy zsarolóvírus-támadás volt. 2022. szeptemberében a G4S értesült arról, hogy a támadás során megszerzett adatok egy része felkerült az internetre, azonban a vállalat a támadás mértékéről és az érintett adatokról lényegesen később, október elején tájékoztatta az érintetteket e-mailben. A tájékoztatás szerint a támadók hozzáfértek az alkalmazottak személyes, valamint a rendőrségi és orvosi szaktevékenységhez köthető adatokhoz. Továbbá nyugdíjkezeléssel kapcsolatos információkhoz és egészségügyi szolgáltatással összefüggő engedélyekhez. A G4S ezt követően sem nyújtott teljes transzparenciát a támadás tapasztalataival kapcsolatban, így nem

⁴⁴ A public-private partnership a feladatoknak a közszféra és a magántőke együttműködésében történő ellátását jelenti. A magyar büntetés-végrehajtás vonatkozásában a Tiszaölki Országos Büntetés-végrehajtási Intézet, valamint a Szombathelyi Országos Büntetés-végrehajtási Intézet megépítése és üzemeltetése valósult meg a programban.

⁴⁵ Online: <https://www.dtf.vic.gov.au/partnerships-victoria-ppp-projects/port-philip-prison-contract-extension-project> Utolsó letöltés: 2022.12.20.

⁴⁶ Az Ausztráliai Victoria állam elsődleges rendőrségi szerve.

⁴⁷ Online: <https://www.msn.com/en-au/news/australia/port-philip-prison-melbourne-jail-targeted-by-anonymous-hackers-in-cyber-attack/ar-AAZj25T> Utolsó letöltés: 2022.12.20.

tudni valójában hány személyt érintett a támadás, azonban tanácsolta a dolgozók személyazonossági okmányainak pótlását, de annak költségében nem vállalt részt. Feltárássra került az is, hogy bár a támadás a Port Phillip Prisont érintette, a támadó ezt kihasználva hozzáfért a vállalat teljes hálózatához egész Ausztráliában, amely így több börtönt és több ezer dolgozót és fogvatartottat érinthetett. Ennek ismeretében az esemény megítélése már nemzetbiztonsági megközelítésből is kritikus mértéket öltött.⁴⁸

5.2. Metropolitan Detention Center, USA (2022)



3. kép: Metropolitan Detention Center, Albuquerque, Új-mexikó, USA⁴⁹

A Bernalillo megyei szövetségi börtön egy nagy területű intézetnek mondható, közel 155 hektáron helyezkedik el. Az intézet öt objektumában elhelyezett fogvatartottak száma együttesen kb. 1200 fő, amely személyek között nagy arányban vannak jelen letartóztatott⁵⁰ személyek. Az intézet éves költségvetése közel 65 millió dollár, az itt dolgozó személyi állomány létszáma 551 fő volt a 2018-ban felmért adatok szerint.⁵¹

2022. január 5-én egy zsarolóvírus támadás érte a Bernalillo Megyei Hivatal informatikai rendszerét. A hivatali hálózatba bekapcsolt Metropolitan Detention Center (a továbbiakban: MDC) is érintetté vált, melyről elsőként az egyik helyi online média számolt be.⁵² Az MDC-t ért kibertámadás olyan súlyos károkat okozott, hogy az intézet teljes zárása mellett a vezetésnek

⁴⁸ Online: <https://www.theguardian.com/australia-news/2022/oct/05/staff-at-security-firm-g4s-on-alert-after-tax-numbers-and-bank-details-posted-online-following-hack> Utolsó letöltés: 2022.12.20

⁴⁹ A kép forrása: <https://www.abqjournal.com/2459954/cyber-attack-leads-to-jail-lockdown-settlement-violations.html>

⁵⁰ Ezen személyekkel összefüggésben még folyamatban van büntető eljárás, így azok sikeres lefolytatása miatt a fogvatartó intézet együttműködése szükséges az ügyekben eljáró bíróságokkal és ügyészségekkel.

⁵¹ Online: <https://www.bernco.gov/metropolitan-detention-center/frequently-asked-questions/> Utolsó letöltés: 2022.12.20.

⁵² Online: <https://sourcenm.com/2022/01/07/jails-inability-to-deal-with-cyberattack-could-violate-the-constitutional-rights-of-inmates/> Utolsó letöltés: 2022.12.20.

nyilvános, sürgősségi felhívást kellett kiadni a szövetségi bíróság részére, miszerint a rendkívüli helyzet miatt átmenetileg képtelenek lesznek betartani egy korábbi, 1995. évi peres ügyben létrejött egyezségi megállapodást, amely a börtönben biztosítandó alapvető körülményekre (túlzsúfoltság és egyéb körülményekre vonatkozó panaszokra) vonatkozott.

A MDC-t érintő kibertámadás megvalósítását 0:00 és 5:30 között⁵³ jelöli meg a nyilatkozat. Az incidenst egy ransomware támadásként azonosította a hivatalos felhívás is. A jelentés tájékoztatása alapján az informatikai szolgáltatások, köztük a kormányzati kezelésű adatbázisok és az e-mail címekhez való hozzáférés elérhetetlensége lépett fel. Nehezítette a helyreállítási intézkedések végrehajtását, hogy az intézet internethez való hozzáférése a kormányzati rendszeren keresztül nem volt kivitelezhető és az intézet helyi és építészeti sajátosságai miatt nem volt lehetséges mobil hálózat alkalmazása.⁵⁴

A támadás következtében az MDC nem tudta biztosítani a letartóztatott személyek büntetőeljárásokkal kapcsolatos videó-kommunikációs eszközön megvalósítandó tárgyalásait, amellyel megsértette a letartóztatott személyek tisztességes eljáráshoz való emberi jogát. Továbbá, a támadás az intézet biztonságtechnikai rendszerét is érintette, így az esemény reggelén az MDC automata ajtószervezetei használhatatlannak voltak.⁵⁵

Az ajtók működését csak délutánra sikerült visszaállítani, így addig a személyi állománynak fizikai kulcsokat kellett használnia. Az intézet lokális adatbázisait, saját szoftvereit, valamint az egészségügyi szolgáltatás során alkalmazott nyilvántartásokat nem érintette a támadás. Az intézet telefonjai és a zárkákban elhelyezett oda-vissza beszélő eszközök működtek, valamint a fogvatartottak birtokában található elítélt-táblagépek is alkalmazhatóak voltak.⁵⁶

⁵³ A szerző megjegyzése: a megjelölt időpont a legmegfelelőbb egy bv. intézet elleni kibertámadásra, hiszen az éjszaka szolgálatot teljesítő, biztonsági feladatokat ellátó személyi állományú tagok létszáma csökkentett a nappali létszámhoz képest, ugyanakkor az éppen váltásos (12,5 órás) munkarendben szolgálatot teljesítő állomány szolgálati idejének közel 2/3 letelt, így a fáradtság miatt a kognitív képességek sem teljes értékűek. Ugyanakkor az intézet informatikai üzemeltetési feladatokat ellátó munkavállalói a pihenő idejüket töltik, így nem tartózkodnak az intézet területén.

⁵⁴ Defendant's Notice Of Emergency Pursuant To Paragraph 14 Of The Settlement Agreement In The United States District Court for the district of New Mexico, 2022. Online: <https://www.documentcloud.org/documents/21176926-bernalillo-county-notice-of-emergency> Utolsó letöltés: 2022.12.20

⁵⁵ Defendant's Notice Of Emergency Pursuant To Paragraph 14 Of The Settlement Agreement In The United States District Court for the district of New Mexico, 2022. Online: <https://www.documentcloud.org/documents/21176926-bernalillo-county-notice-of-emergency> Utolsó letöltés: 2022.12.20.

⁵⁶ Defendant's Notice Of Emergency Pursuant To Paragraph 14 Of The Settlement Agreement In The United States District Court for the district of New Mexico, 2022. Online:

További káros következményként listázható, hogy nem voltak elérhetőek az intézet IP alapú kamerarendszerei, amely nagyon komoly aggodalmat jelentett a személyi és a fogvatartotti állomány biztonsága szempontjából. E kockázat csökkentésére rendkívüli biztonsági intézkedéseket kellett bevezetni, amelyek további fogvatartotti jogok korlátozásához vezettek. A fogvatartottak zárkájukat nem hagyhatták el, az összes hozzátartozói látogatást felfüggesztették. Internet hiányában a fogvatartotti kérelmeket és panaszokat nem lehetett rögzíteni, így papíralapú űrlapokat kellett biztosítani a fogvatartottak részére és a szolgálatban lévő személyi állomány tagjai is papíralapon rögzítették feljegyzéseiket. A fentiekén túl az intézet igyekezett számos alternatív megoldást megragadni a hivatali kötelességek teljesítése érdekében, melynek további részletezése már nem releváns.⁵⁷

Egy 2022. január 10-én kiadott sajtóközlemény szerint a megyei hivatal székhelyein ekkor még mindig nem sikerült visszaállítani a normális működési rendet.⁵⁸ További nem megerősített sajtóinformációk szerint a támadás háttere ismeretlen maradt, a gyanúsítottakat nem sikerült felderíteni, valamint a támadással összefüggő pénzkövetelést nem teljesítették.⁵⁹

Az incidens után a Bernalillo Megyei Bizottság döntése alapján új kiberbiztonsági politikát kívánnak bevezetni, amely magában foglalja a több faktoros⁶⁰ azonosítás alkalmazását a felhasználói fiókok tekintetében. Továbbá létrehoznak egy megyei hálózatok megfigyelését végző biztonsági műveleti központot, amely az alá tartozó hálózatokra kapcsolt számítógépek esetében riaszt a gyanús tevékenységek észlelésekor.⁶¹

<https://www.documentcloud.org/documents/21176926-bernalillo-county-notice-of-emergency> Utolsó letöltés: 2022.12.20

⁵⁷ Defendant's Notice Of Emergency Pursuant To Paragraph 14 Of The Settlement Agreement In The United States District Court for the district of New Mexico, 2022. Online: <https://www.documentcloud.org/documents/21176926-bernalillo-county-notice-of-emergency> Utolsó letöltés: 2022.12.20

⁵⁸ Online: <https://www.bernco.gov/blog/2022/01/10/alvarado-square-open-on-lobby-level-only/> Utolsó letöltés: 2022.12.20.

⁵⁹ Online: <https://statescoop.com/bernalillo-county-cybersecurity-policy-ransomware/> Utolsó letöltés: 2022.12.20.

⁶⁰ A többszörös hitelesítés egy olyan elektronikus hitelesítési módszer, amelyben a felhasználó csak akkor kap hozzáférést, ha két vagy több bizonyítékot sikeresen bemutatott egy hitelesítési mechanizmusnak.

⁶¹ Online: <https://www.cyansecurity.com/half-year-review-of-significant-cyberattacks-bernalillo-county/> Utolsó letöltés: 2022.12.20.

5.3. Evin Prison, Irán (2021)

A 2020 – 2021. évek során Irán több nagyobb volumenű kibertámadásban volt érintett, mint például az állami vasúti rendszert érintő incidens,⁶² vagy Bandar Abbas város kikötőjét célzó művelet.⁶³ Az Evin Prisont is ebben az időszakban érte kibertámadás, ám annak pontos időpontját a hatóságok nem hozták nyilvánosságra. A Teherán Evin városnegyedében található börtön 1972-óta üzemel. Az intézet nemzetközi viszonylatban hírhedtnek mondható a 70-80-as években ott zajlott kínzásokról és tömeges kivégzésekről. Napjainkban is erősen kritizálják működését az emberi jogokért és szabadságokért harcoló nemzetközi civil szervezetek.⁶⁴

2021. augusztus 22-én egyidejűleg számos, a börtön belső kamerarendszeréből kiszivárgott kamerafelvétel jelent meg több sajtóorgánum felületén. Az információkból egyértelműen megállapításra került, hogy a támadás egy Ali Adalat (Ali igazságszolgáltatása) nevű hacktivistá⁶⁵ csoporthoz köthető és videók időbélyegzőiből ítélve már jó ideje hozzáférést szereztek a börtön belső CCTV⁶⁶ kamerarendszeréhez. A felvételek között volt a börtön biztonságtechnikai-rendszer kezelő helyiségét megfigyelő kamera által – a behatolás közlése során – rögzített kamerafelvétel is, mely egyértelműen bizonyítja a személyzet általi észlelést. A nyilvánosságra hozott, 2020. és 2021. évi időbélyegzőkkel ellátott felvételek főként a börtön személyzetének fogvatartottakkal szembeni brutális, emberi jogokat sértő bántalmazásokat szolgáltatnak bizonyítani. A Tapandegan⁶⁷ elnevezésű, szintén hacktivistá csoport részt vett a videó anyagok népszerűsítésében, de a támadásban való részvételt tagadták. A nyilvánosságra kerülést követően az iráni tisztviselők elismerték a kibertámadás megtörténtét, ám további információkat nem osztottak meg, így a történések tisztázatlanok maradtak.⁶⁸

⁶² Online: <https://therecord.media/cyber-attack-disrupts-irans-national-railway-system/> Utolsó letöltés: 2022.12.21.

⁶³ Online: <https://www.zdnet.com/article/iran-reports-failed-cyber-attack-on-strait-of-hormuz-port/> Utolsó letöltés: 2022.12.21.

⁶⁴ Online: <https://www.dw.com/en/irans-evin-prison-experience-was-psychological-torture-says-former-prisoner/a-63509722> Utolsó letöltés 2022.12.21.

⁶⁵ A hacktivisták számítógépes hackelés felhasználásával promotálnak bizonyos politikai nézeteket, foglalnak állást politikai kérdésekben.

⁶⁶ Closed-circuit television, magyarul zártláncú televízió szolgáltatás.

⁶⁷ Egy iráni hackercsoport, amely 2018. május 24-én és 2018. június 6-án is feltörte az érkező és indulási monitorokat Irán két nagy nemzetközi repülőterén, majd azokon kormányellenes üzeneteket tett közzé.

⁶⁸ Online: <https://therecord.media/hacktivist-leak-videos-of-abuse-in-iran-evin-prison/> Utolsó letöltés: 2022.12.21.

A kiszivárgott felvételekből megállapítható, hogy a technikai rendszerkezelő szolgálati helyén elhelyezett monitorfal adását felülírták (4. kép) és egy politikai jellegű „Kibertámadás. Általános tiltakozás a politikai foglyok szabadságáig” szöveget osztottak meg perzsa nyelven.



4. kép: Az Ali Adalat hacktivista csoport üzenete⁶⁹

Az észlelő személyzet zavart viselkedésében mobiltelefonjával rögzíteni kezdte az eseményt (5. kép).⁷⁰



5. kép: Pillanatkép a technikai rendszer kezelő helységről, a támadás pillanatából, melyet a behatolók tettek közzé.⁷¹

Egyértelmű, hogy azon túl, hogy a börtön biztonságtechnikai rendszerében komoly zavarokat keltettek és megzavarták a rendeltetésszerű működést, nem az állami szervben történő károkozás volt a cél. Itt tulajdonképpen a börtön szimbolikáját, és az azzal összefüggő jelentéstartalmat és hírverést felhasználva igyekeztek minél nagyobb tömegekhez eljuttatni

⁶⁹ A kép forrása: <https://www.iran-emrooz.net/index.php/news2/more/93050>

⁷⁰ Online videó: <https://twitter.com/IranIntl/status/1429524913828900866?s=20> Utolsó letöltés: 2022.12.21.

⁷¹ A kép forrása: <https://old.iranintl.com/en/iran/hackers-release-security-footage-iran%E2%80%99s-evin-prison>

üzenetüket. A börtön azon felül, hogy alanya volt a kibertámadásnak, a politikai célok eszközüvé is vált egyúttal.

5.4. Idaho State Correctional Institution, USA (2018)

A 2018-ban történt incidens alapjaiban eltér az eddigiekben bemutatottaktól, hiszen nem egy börtönt érintő kibertámadásról van szó, hanem egy olyan jellegű informatikai incidensről, amelyben jelentős felelőssége van az érintett büntetés-végrehajtási szervezetnek. Az esetben érintett amerikai intézetek az Idaho State Correctional Institution, az Idaho State Correctional Center, az Idaho Correctional Institution-Orofino, valamint a South Idaho Correctional Institution and the Correctional Alternative Placement Plan Facility.

Az Amerikai Egyesült Államok több államában – többségében azonos feltételekkel – a fogvatartottaknak lehetőségük van tableteket használni. Ezek a készülékek speciális tervezésűek, célszerűen börtönhasználatra lettek fejlesztve, egyaránt szoftver és hardver tekintetben is.



6. kép: A JPay által szolgáltatott börtöntablet készülék.⁷²

A JPay szolgáltatása kifejezetten népszerű a fogvatartottak körében, hiszen a készülékkel e-maileket küldhetnek kapcsolattartóiknak, zenét vásárolhatnak és hallgathatnak, edukációs alkalmazásokat használhatnak, továbbá még játékokat is játszhatnak.⁷³ A készülékek elterjedését követően a fogvatartottaknak sikerült a készülék szoftverének egy sérülékenységet kihasználni, majd az alkalmazáshoz tartozó felhasználó számlájuk pénzösszegét megnövelni és számos vásárlást végrehajtani. Az eset kapcsán 364 fogvatartott összesen 225 000 \$ kárt okozott a szolgáltatónak. A JPay az esetet követően felfüggesztette a zenék és játékok letöltését a károk

⁷² A kép forrása: <https://www.jpays.com/education.aspx>

⁷³ Online: <https://www.jpays.com/education.aspx> Utolsó letöltés: 2022.12.24.

megtérítéséig, valamint a börtön fegyelmi eljárást kedvezményezett az érintett fogvatartottakkal szemben.

Az eset tanulsága, hogy a társadalom digitalizációja a börtönökben található fogvatartottakat is kikerülhetetlenül érinti és kell is érintenie, ugyanakkor a kiberbiztonságnak a bástyafalak között is érvényre kell jutnia. Az nem megoldás, hogy a digitalizációt a falakon kívül tartjuk, hiszen a büntetés-végrehajtási célokat számos alapelv mentén kell elérni. Ezek az alapelvek olyan erkölcsi értékek, melyek a végrehajtás teljes területét átszövik, hiszen segítik a jogalkotót, ezt követően a jogértelmezést végző szerveket, valamint természetesen a gyakorlati végrehajtást is. Az egyik ilyen alapelv a normalizáció elve, amely szerint a szabadságvesztés végrehajtási körülményeit a lehető legjobban kell közelíteni a szabad élet általános feltételeihez,⁷⁴ és ennek a digitalizáció bizonyosan szerves része napjainkban. Így elkerülhetetlen a digitális eszközök és a fogvatartottak egyre nagyobb fokú kapcsolata.

5.5. Összegzés

A fent bemutatott esetekből értelemszerűen – a maradéktalan tudományos megalapozottságot nélkülözve – következik, hogy nemzetközi viszonylatban a börtönök intézménye számos helyszínen és esetben rendelkezett olyan mértékű EIR interdependenciával, hogy a rendszerekben okozott korlátozások jelentős zavart okozzanak a mindennapi működésben. Továbbá felismerhető az a jelenség, miszerint egy EIR-t ért támadás követlen kihatással lehet a személyi állományi tagok biztonságának szavatosságára, valamint a fogvatartottak alapvető emberi jogainak garanciáira. Az alkalmazott biztonsági intézkedések napjainkig garantálták a rendeltetésszerű működést, de manapság már nem képesek teljes körű védelmet biztosítani, hiszen a digitalizáció folyamata egy új színteret, a kibernetikát nyitja meg a börtönöket érintő új kockázatok számára. Bár tökéletes védelem nem létezik, a büntetés-végrehajtási szervezetnek állami szervezet lévén garantálnia kell saját kibernetikájának biztonságát. Ennek hiánya esetén könnyűszerrel előfordulhatnak olyan események, amelyek akár a börtönben dolgozó személyi állomány, vagy az ott fogvatartottak biztonságát és alapjogait is érinthetik.

A tudományos kérdés az, hogy a magyar büntetés-végrehajtás börtöneit ért kibertámadás okozhat-e ilyen mértékű zavarokat? Hogyan áll hazánk börtöneinek kiberbiztonsága? A dolgozat ezen kérdésekre próbált válaszokat alkotni az általa vizsgált témák feldolgozásával.

⁷⁴ Juhász Zsuzsanna (2018): A büntetés-végrehajtás alapelvei). Magyar Rendészet 2018/5. Budapest. p. 15.

6. BV. INFORMATIKA

6.1. A rendvédelmi és a büntetés-végrehajtási informatika

A rendvédelmi informatika elméleti megközelítésben az információ gyűjtésével és tárolásával, feldolgozásával, továbbításával és szolgáltatásával foglalkozik. Gyakorlati megközelítésben a számítástechnikai, a vezetékes és vezeték nélküli híradó (távközlési) és biztonságtechnikai eszközök és szolgáltatások rendszere, amelyeknek alapvető szerepe van a jogszabályokban meghatározott rendvédelmi feladatok és ezeken keresztül a rendvédelmi szervezeti stratégiák megvalósításában. A rendvédelmi informatika része a rendvédelmi szervezet tevékenységét alapvetően meghatározó informatikai tevékenység tervezése, szervezése és irányítása.⁷⁵

A bv. szervezetnél informatikai szakfeladatokat egyaránt ellát az Országos Parancsnokság Informatikai Főosztálya, valamint a Büntetés-végrehajtás Gazdasági Ellátó Intézete (GEI)⁷⁶ is, utóbbi intézmény a bv. intézetekbe szervezett állománnyal helyben is ellátja feladatát, legfőképpen az üzemeltetési feladatokat.

6.2. A büntetés-végrehajtás informatikai infrastruktúrája

A büntetés-végrehajtás informatikai infrastruktúrája a korábbi évtizedekben jelentős fejlődésen ment keresztül, jelenleg az alap- és szaktevékenységek informatikai támogatását homogén, egységes és egyen szilárd informatikai rendszer valósítja meg. Ez a működési kialakítás biztosítja, hogy valamennyi helyi hálózatban azonos építőelemekből épüljön fel az informatikai rendszer, ez lényegi eleme a rendelkezésre állási követelmények teljesítésének. Az országosan azonos működési környezet hatékonyabbá teszi a hibadetektálás, a hibalokalizálás folyamatát és a hibajavítás időigényét, valamint a szolgáltatások minőségi javítását is egy időben képes biztosítani a teljes tartományban.⁷⁷ Az Informatikai Főosztály egy korábbi vezetőjének 2020-as felmérése alapján a szerverek száma 250 db, a munkaállomások száma 5000 db, az EDR

⁷⁵ Prisznyák Szabolcs (2020): A rendvédelmi informatikai egyes szervezési és oktatási kérdései c. Doktori (PhD) értekezés, Óbudai Egyetem, Biztonságtudományi Doktori Iskola. p. 31.

⁷⁶ Büntetés-végrehajtás Gazdasági Ellátó Intézetének Szervezeti és Működési Szabályzata I. fejezet 5. pont

⁷⁷ Rendészeti Alap – és Szakvizsga Bizottság (2022): Rendészeti Szakvizsga Tananyag – Büntetés-végrehajtási Igazgatás. p. 247-251. Online: http://bmkszf.hu/dokumentum/3411/buntetesvegrahajitasi_tananyag.pdf

rádióké több mint 1100 db, valamint a telefonvonalak száma 5000 db. A felhasználók száma körülbelül 8300 fő, az informatikai rendszert kb. 150 fő működteti.⁷⁸

6.2.1 A hálózati rendszer

A büntetés-végrehajtási szervezet helyi hálózatok összekapcsolásával jött létre, az összekapcsolást korábban az optikai gerincvezetékkel kialakított Elektronikus Kormányzati Gerinc (EKG) volt, ugyanezen a belső hálózaton üzemelt a telefonszolgáltatás is. A jelenlegi országos táv-adatátviteli hálózatot és az Internet elérését a kormányzati célú hálózatokról szóló 346/2010. (XII.28) Kormányrendelet szerint a kormányzati célú hírközlési szolgáltató, a Nemzeti Infokommunikációs Szolgáltató Zrt. biztosítja a Nemzeti Távközlési Gerinchálózat (NTG) alkalmazásával.⁷⁹ A NTG hálózatán logikai alhálózatok, úgynevezett virtuális magánhálózatok (VPN) működnek, ilyen alhálózat a szervezet által használt bv.gov.hu is. Ugyanezen a szolgáltatáson történik a telefonszolgáltatás is. A rendszernek része az intézeti GSM kijárat, amely a Telekomnál szerződött szolgálati célú, valamint dolgozói előfizetéseknek biztosítja az azonos hívócsoporthoz való elérést, amely így díjtalan.⁸⁰

A központi és az intézeti szerverek egy egységes logikai rendszerben működnek, a lokális rendszerek óránként szinkronizálnak központi irányba, illetve ugyan így a szinkronizált adatok továbbítása is megtörténik a telephelyek felé. A bv. szervek hálózati kialakítása csillag topológiájú, a telephelyeken belüli szerverek között optikai összeköttetés található. A címkiosztás DHCP szolgáltatását, a bejelentkezést, a jogosultság kiosztást intézetenként tartományvezérlő szerver (domain controller) végzi. A vékonykliensek távoli asztal kapcsolattal (RDP) jelentkeznek fel a terminál kiszolgálóra.⁸¹

A bv. hálózat internet irányú kijárása a BvOP irányában központosítva van. Az elérés rendszertechnológiai és személyi jogosultságkezeléssel biztosított. Internetelérés az alap felhasználó részére nem engedélyezett, annak engedélyeztetése külön jogosultságigénylő eljárás része. A szolgáltatás sávszélessége korlátozott (100 MB/s), továbbá tiltott a stream

⁷⁸ Prisznyák Szabolcs (2020): A rendvédelmi informatikai egyes szervezési és oktatási kérdései c. Doktori (PhD) értekezés, Óbudai Egyetem, Biztonságtudományi Doktori Iskola. p. 72.

⁷⁹ 346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról.

⁸⁰ Rendészeti Alap – és Szakvizsga Bizottság (2022): Rendészeti Szakvizsga Tananyag – Büntetés-végrehajtási Igazgatás. p. 247-251. Online: http://bmkszf.hu/dokumentum/3411/buntetesvegrahajitasi_tananyag.pdf

⁸¹ Tuba Kovács Béla (2019): Büntetés-végrehajtási informatikai ismeretek tananyag, Büntetés-végrehajtási Szervezet Oktatási, Továbbképzési és Rehabilitációs Központja, Budapest. p. 22.

szolgáltatások, valamint a közösségi oldalak elérése. Az internetforgalom az informatikai biztonsági szempontokat érvényesítve ellenőrzött, ennek érdekében kettős tűzfal rendszer működik (Cisco ASA eszköz, illetve Microsoft Forefront Threat Management Gateway 2010 – TMG). További védelmi megoldás a víruspajzs és SPAM szűrő rendszer, amely a virtuális Symantec Brigh Mail Gateway termék alkalmazásával történik. Valamennyi szerveren és munkaállomáson valós idejű vírusvédelem működik a Symantec End Point Protection termék használatával.⁸²

6.2.2 Szoftver környezet

A szervezet tartományában működő alkalmazás rendszerek három csoportba sorolhatóak, általános célú alkalmazások, szakrendszerekre és egyedi felhasználású alkalmazásokra.⁸³

Általános célú alkalmazások

A munkaállomások ellátására üzemeltetett szervereken rendszeresített operációs rendszer a Windows 2008 R2 Server 64 bites verziója. A kliens oldalon a PC-k Windows7, a vékony klienseken eLux linux operációs rendszerrel fut, amely távoli asztali kapcsolattal csatlakozik a szerverekre.⁸⁴

Irodai programcsomag a Microsoft Office 2010, amelyből a Word, Excel, Powerpoint és Outlook szoftverek kerülnek alkalmazásra. A belső intranetre, az internetre, illetve a fogvatartotti alapnyilvántartás elérésére több böngészőprogram elérhető, ezek a Google Chrome, Mozilla Firefox, Internet Explorer 9. Az állományok és mappák kezelésére egyaránt alkalmazható a Windows intéző, vagy Total Commander. A PDF⁸⁵ kiterjesztésű állományok megjelenítésére a Foxit Reader program lett rendszeresítve. Az elektronikus iratkezelésre az alább kifejtett RobotZsarú NEO integrált ügyviteli és ügyfeldolgozó rendszerét alkalmazzák.⁸⁶

⁸² Rendészeti Alap – és Szakvizsga Bizottság (2022): Rendészeti Szakvizsga Tananyag – Büntetés-végrehajtási Igazgatás. p. 251. Online: http://bmkszf.hu/dokumentum/3411/buntetesvegrahajitasi_tananyag.pdf

⁸³ Rendészeti Alap – és Szakvizsga Bizottság (2022): Rendészeti Szakvizsga Tananyag – Büntetés-végrehajtási Igazgatás. p. 247-251. Online: http://bmkszf.hu/dokumentum/3411/buntetesvegrahajitasi_tananyag.pdf

⁸⁴ Tuba Kovács Béla (2019): Büntetés-végrehajtási informatikai ismeretek tananyag, Büntetés-végrehajtási Szervezet Oktatási, Továbbképzési és Rehabilitációs Központja, Budapest.

⁸⁵ A Portable Document Format egy dokumentumok tárolására alkalmas fájlformátum, amelyet az Adobe Systems fejlesztett ki.

⁸⁶ Tuba Kovács Béla (2019): Büntetés-végrehajtási informatikai ismeretek tananyag, Büntetés-végrehajtási Szervezet Oktatási, Továbbképzési és Rehabilitációs Központja, Budapest.

Robotzsaru Neo

Az alkalmazás segítségével a szervezet adminisztratív tevékenységeit látja el, valamint a feladat ellátása során kezelt vagy keletkezett ügyiratok nyilvántartását, elektronikus kezelését és a munkafolyamatok követését. Az alkalmazás központi szervere a BvOP géptermében került elhelyezésre, azon operációs rendszerként Red Hat Linux és Oracle Database 11g Enterprise Server adatbáziskezelő fut.⁸⁷

Szakrendszerek

A szakrendszerek szűkebb körben, jellemzően egy adott tevékenységcsoport működésében meghatározott adatkör kezelését teszik lehetővé. A szervezet támogatásában betöltött szerepük szerint lehetnek alaptevékenységet támogató szakrendszerek, közigazgatási szakrendszerek, egészségügyi szakrendszerek stb.⁸⁸

Elektronikus fogvatartotti alapnyilvántartás

Alaptevékenységet támogató szakrendszernek tekinthető az elektronikus fogvatartotti alapnyilvántartás, valamint funkcionális bővítményeit kezelő alkalmazásrendszer. Jellemzője, hogy SQL szabványos adatbázis kezelőre épül, grafikus felületen működik, böngésző alapú elérést biztosít. A jelenleg alkalmazott elektronikus fogvatartotti alapnyilvántartás a dolgozat egyik fő vizsgálati eleme, így a későbbiekben részletesen bemutatásra kerül.⁸⁹

Egészségügyi szakrendszerek

Az egészségügyi nyilvántartás szintén egy böngésző alapú szolgáltatás, adatbázisa központosított Microsoft SQL Server 2008 Standard, a tevékenység releváns adatköre tárolásra kerül a fogvatartotti alapnyilvántartásban is. A gyógyszerkezelés nyilvántartása az intézeti központi gyógyszer-tár készletgazdálkodását és gyógyszer szakmai információinak kezelését

⁸⁷ Rendészeti Alap – és Szakvizsga Bizottság (2022): Rendészeti Szakvizsga Tananyag – Büntetés-végrehajtási Igazgatás. p. 247-251. Online: http://bmkszf.hu/dokumentum/3411/buntetesvegrahajitasi_tananyag.pdf

⁸⁸ Rendészeti Alap – és Szakvizsga Bizottság (2022): Rendészeti Szakvizsga Tananyag – Büntetés-végrehajtási Igazgatás. p. 247-251. Online: http://bmkszf.hu/dokumentum/3411/buntetesvegrahajitasi_tananyag.pdf

⁸⁹ Rendészeti Alap – és Szakvizsga Bizottság (2022): Rendészeti Szakvizsga Tananyag – Büntetés-végrehajtási Igazgatás. p. 247-251. Online: http://bmkszf.hu/dokumentum/3411/buntetesvegrahajitasi_tananyag.pdf

végző rendszerrel (Gyurika elnevezésű szoftver)⁹⁰ történik, valamint az osztályos gyógyszerelést és készletezését a Tobias szoftver⁹¹ támogatásával végzik.⁹²

Közigazgatási szakrendszerek

A közigazgatási rendszerek közül a QB-Élelem szoftver segíti az étkeztetési tevékenységeket, a Forrás DotNet felhő integrált ügyviteli rendszer pénzügyi és főkönyvi nyilvántartást, készlet és eszköznyilvántartást biztosít. A Központi Vagyon Kataszter program alkalmazásával történik a vagyontárgyak nyilvántartása, a Magyar Államkincstár által működtetett KIRA⁹³ rendszeren valósulnak meg a személyi állomány bérjellegű kifizetéseinek nyilvántartása.⁹⁴

Személyügyi szakrendszer:

A SENIOR alkalmazás a személyügyi nyilvántartásra kifejlesztett alkalmazásrendszer. A programrendszer jellemzője, hogy szabványos adatbázis kezelőre épül, grafikus felületen működik.

6.2.3 Hardver környezet

A központi szerverek – a BvOP és az intézeti infrastruktúra esetében is – szünetmentes tápellátása biztosított (az erősáramú szolgáltatás kiesést követő 15 perc áthidalási képességgel) annak érdekében, hogy az intézeti szükségáramforrás (aggregátor) indulásáig biztosítsa a szerverek elérhetőségét vagy biztonságos leállítását. Valamennyi szerverkiszolgálóhoz biztosított, több generációs mentést lehetővé tevő hálózati mentőeszköz lemezes, majd szalagos mentése (intézet esetében Network Attached Storage – NAS, a BvOP géptermben disk-to-disk és disk-to-tape egység Symantec Backup Exec programmal).⁹⁵

⁹⁰ Online: <http://www.skpont.hu/index.php/gyurika/> Utolsó letöltés: 2023.01.13.

⁹¹ Online: <http://www.skpont.hu/index.php/tobias/> Utolsó letöltés: 2023.01.13.

⁹² Rendészeti Alap – és Szakvizsga Bizottság (2022): Rendészeti Szakvizsga Tananyag – Büntetés-végrehajtási Igazgatás.p. 247-251. Online: http://bmkszf.hu/dokumentum/3411/buntetesvegrahajitasi_tananyag.pdf

⁹³ Központi Illetmény-számfejtési Rendszer (KIRA).

⁹⁴ Rendészeti Alap – és Szakvizsga Bizottság (2022): Rendészeti Szakvizsga Tananyag – Büntetés-végrehajtási Igazgatás.p. 247-251. Online: http://bmkszf.hu/dokumentum/3411/buntetesvegrahajitasi_tananyag.pdf

⁹⁵ Rendészeti Alap – és Szakvizsga Bizottság (2022): Rendészeti Szakvizsga Tananyag – Büntetés-végrehajtási Igazgatás. p. 251. Online: http://bmkszf.hu/dokumentum/3411/buntetesvegrahajitasi_tananyag.pdf

Munkaállomások:

A jelenleg alkalmazott munkaállomások nagy része a Belügyminisztérium Elektronikus Közigazgatás Operatív Programjának két ütemében került beszerzésre.⁹⁶ A két megvalósuló projektnek köszönhetően összesen 2400 db Fujitsu vékonykliens állt üzembe LCD monitorokkal, amelyek így biztosítják a homogenitást, interoperabilitást, a felcserélhetőséget és az átcsoportosíthatóságot.



7. kép A munkaállomásokon a Fujitsu S100 vékonykliens a jellemző.⁹⁷

A vékonykliensek mellett Fujitsu vastagkliensek, valamint notebookok is beszerzésre kerültek, ám csekélyebb darabszámuk miatt a munkaállomásokon a vékonykliensek alkalmazása a jellemző.

⁹⁶ Online: <https://bv.gov.hu/hu/ekop> Utolsó letöltés: 2023. 01.13.

⁹⁷ A kép forrása: https://www.heinzsoft-shop.de/images/product_images/info_images/vesa_mouting_kit_1.jpg

7. HAZAI INCIDENSEK ÉS KOCKÁZATOK

A magyar büntetés-végrehajtási szervezet történetiségében a nemzetközi kitekintés során bemutatott kiberincidensekhez hasonlókat nem találunk. Nyilvánvalóan ehhez hozzájárul, hogy állami szervként és minősített adatokat kezelő szervezet lévén, az adat- és információbiztonsági gyakorlata szigorú szabályozás mentén valósul meg. Természetes, ahogy minden szervezetben, az adatvédelmi felelősnek adott esetben itt is intézkednie szükséges, valamint az elektronikus információbiztonság területén is előfordulnak incidensek, azonban ezek nem érik el a kritikus mértéket.

A börtön világa sajátos, így specifikumokkal tűzdelt információbiztonsági politikát is igényel. A külső fenyegetések körében specifikáció nem igen van jelen, de a belső fenyegetések köre egyedülálló kiberfenyegetetési unikum. Minden szervezet helyén kezeli saját humán tényezői által okozott kockázatokat, azonban a bv. szervezet humán tényezőinek egy csoportja nem szokványos kockázatot képvisel. A fogvatartottak csoportja számos szempontból rejt egyedi, kiemelt kockázatokat. A következő fejezetben a külső és belső fenyegetések köréből származó esetek bemutatása történik. A bemutatott példák nem az általánosnak mondható incidensek sorából kerültek kiemelésre, hanem olyan esetek leíratai, amelyeknek egyik fő jellemzője, hogy „börtönre szabottak”, vagy börtön körülmények között jöttek létre.

7.1. Külső fenyegetések

7.1.1 E-mail fiókokra érkezett támadások

A szervezet felhasználóinak e-mail címére számos esetben érkeznek olyan gyanús tartalmú csak szöveges, vagy gyanús mellékletet is tartalmazó elektronikus levelek, amelyekről első olvasatra is megállapítható azok rosszindulatú szándéka. Általános gyakorlatnak tekinthető az a jelenség, hogy a szervezeten belül – annak rendvédelmi jellegéből adódóan – a személyi állományú tagok közötti elektronikus csatornákon zajló kommunikáció során a nyelvezet a katonai alakítás szóbeliségét, valamint hivatalos megfogalmazás jegyeit egyaránt alkalmazza. Ezen íratlan szabályokat követő stílus elsajátításához és használatához gyakorlat szükséges, így az ilyen közlési formát nélkülöző elektronikus levelezés már eleve gyanút kelt a fogadó félben. Külön említésre méltó az a módszer, amely során a támadók egyértelműen észlelhető erőfeszítéseket tesznek annak érdekében, hogy átjussanak ezen a „szűrőn”. A 9. számú képen egy 2022.05.21-én, a szervezet egyik felhasználói e-mail fiókjára érkezett rosszindulatú e-mail szövegezése

látható, ahol az aláírásnál – ahogy ezt a hivatalos állomány is teszi –rendfokozati jelzést is alkalmaztak. Ez a formájú megvalósítás már egyértelműen rendvédelmi szervben dolgozó személyre célzott tevékenységként azonosítható.



8. kép: Rosszindulatú e-mail, melynek aláírásánál rendfokozati jelzés került alkalmazásra.⁹⁸

Hasonlóan célzott jelleget mutat a 2022. június 7-én érkezett e-mail a bv. szervezet egyik gazdasági társaságánál szolgálatot teljesítő, vezető beosztást gyakorló személyi állományú tag e-mail címére.



9. kép: Rosszindulatú e-mail, melynek egyértelmű célja a pénzügyi kiutalás.⁹⁹

A célzottság tulajdonsága itt is az aláírásban valósul meg, azonban az előző esettől eltérően nem egy rendfokozati jelzéssel látták el azt, hanem az aktuális, cégcsoportot összefogó holder szerepkörben eljáró társaság ügyvezető igazgatójának nevével.¹⁰⁰ Ez az információ természetesen nyilvános, az érintett gazdasági társaság, valamint a bv. szervezet honlapján is

⁹⁸ A kép forrása: A BvOP által szolgáltatott adat.

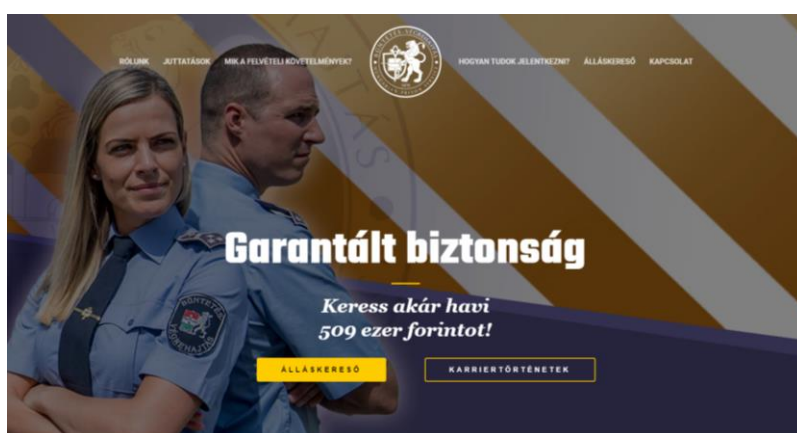
⁹⁹ A kép forrása: A BvOP által szolgáltatott adat.

¹⁰⁰ Cséri Zoltán bv. dandártábornok, bv. főtanácsos úr 2020-2022 között a bv. szervezet gazdasági társaságainak tevékenységét összefogó Bv. Holding Kft. ügyvezetőjeként látott el szolgáltatott.

elérhető bárki számára. Azonban a módszer, valamint az, hogy a szervezet gazdasági társaságát célozták meg, ez egyértelműen az előkészület jegyeit mutatja.

7.1.2 A bv. szervezet weboldalát ért támadás

A szervezet két nyilvános elérésű weboldalt adminisztrál. A kormányzati tájékoztatású www.bv.gov.hu cím a szervezet „main” weboldala, ahol a szervezettel kapcsolatos legfontosabb információk és hírek érhetőek el. E mellett a www.gyereahuvosre.hu címen is elérhető egy weboldal, amely újszerű, innovatív megközelítésben kívánja támogatni a szervezet toborzási tevékenységét.



10. kép: A szervezet toborzási weboldala.¹⁰¹

A BvOP 2021.05.17-én kiadott közleménye alapján utóbbi oldalt támadás érte, és az arra érkező látogatókat egy adathalász oldalra irányította a weboldal. Az oldal üzemeltetési feladatait a Nemzeti Infokommunikációs Szolgáltató Zrt. (NISZ Zrt.) látja el. A közlemény szerint a szakemberei vizsgálták a támadás körülményeit, valamint dolgoztak az oldal zavartalan működésének helyreállításán. A Büntetés-végrehajtás Országos Parancsnoksága büntetőfeljelentést tett az ügyben. Az oldal felhasználói adatokat nem tárol, így az esettel kapcsolatban további tájékoztatás nem történt.¹⁰²

7.2. Belső fenyegetések

A belső fenyegetések legfőbb köre a szervezet főtevékenységéből adódik. A fogvatartottak biztonságához való viszonya nem azonos az átlagos munkavállalók jellemzőivel. Fontos

¹⁰¹ A kép forrása: www.gyereahuvosre.hu

¹⁰² <https://bv.gov.hu/hu/intezetek/bvszervezet/hirek/4184> Utolsó letöltés: 2023.03.09.

megjegyezni, hogy a létszámadatok is a fogvatartotti csoport javára állnak, hiszen míg a bv. szervezet személyi állományi létszáma 9 ezer fő, addig a fogvatartottak létszáma meghaladja a 20 ezret, ebből következik, hogy a fogvatartotti csoportban rejlő kiberbiztonsági kockázat – annak sajátosságával együtt – jelentős.

A fogvatartottakkal közvetetten vagy közvetlenül, legálisan vagy illegális módon érintkezésbe lépő elektronikus információs rendszerek biztonsága a büntetés-végrehajtás felelőssége is, attól függetlenül, hogy annak üzemeltetését a bv. szerv, vagy külső szolgáltató végzi. Az elmúlt években megjelentek a zárkákban a televíziókészülékek, a kapcsolattartási célból biztosított fogvatartotti mobiltelefonok, a terminál kiszolgálók és a pandémiás helyzet magával hozta a videó alapú elektronikus kapcsolattartást megjelenését is. Ez a fajta átalakulás a végrehajtás számára eddig ismeretlen kockázatokat jelent, melyek által az alkalmazott rendszerek bizalmasságának, sértetlenségének és rendelkezésre állásának vesztesége jelentős hatással bírhat a bv. szervezet társadalmi megítélésére. Továbbá, jelentősen negatív a társadalmi megítélése annak a jelenségnek is, amennyiben egy, a börtön által a fogvatartottak részére biztosított EIR-t felhasználva követnek el bűncselekményeket a börtönből a társadalom irányába a szabadságvesztésüket töltő fogvatartottak.

Az alábbiakban bemutatott témakör egy kifejezetten büntetés-végrehajtási szempontú kockázatokat sorakoztat fel. Hiszen a börtön intézménye nemcsak „*kívülről*” támadható, hanem magából a börtönből is lehet támadásokat végrehajtani a társadalom felé, vagy akár a börtönnel szemben is.

7.2.1 Fogvatartotti mobiltelefon hardverének és szoftverének módosítása

A fogvatartotti mobiltelefonok a kapcsolattartás új típusú formáját valósítják meg. A fogvatartott részére mobiltelefon készülék kerül biztosításra, amelyen keresztül védőjével, hozzátartozóival tarthat kapcsolatot az előzetesen engedélyezett mértékben és gyakoriságban. Ezek a készülékek 2015 óta elérhetőek a hazai börtönökben, a kezdeti modellek a kínai gyártású ZTE R528 típusú készülékek voltak. A készülék háza összeragasztásra került, védőfólia lett elhelyezve az esetleges modifikációk észlelésére, valamint a készülékkel csak kimenő

hívásokat lehetett kezdeményezni, azok internetezésre, kép rögzítésére, SMS küldésére-fogadására alapesetben nem voltak alkalmasak.¹⁰³



11. kép: a ZTE R528 típusú fogvatartotti mobiltelefon készülék.¹⁰⁴

A telefonok bevezetését követő időszakban egyre több esetben fordult elő, hogy a telefonok szoftvereit, hardvereit börtön körülmények között módosították, valamint úgynevezett TurboSIM¹⁰⁵ (egy vékony fólia, amelyen egy mikrokontroller található) használatával SIM függetlenné tették azokat.



12. kép: SIM kártya TurboSIM mikrokontrollerrel.¹⁰⁶

¹⁰³ Online: <https://www.jogiforum.hu/cikk/2018/11/26/illegalis-bortontelefon-csalasra-hasznaljak-a-bortonoket-ellepo-mobilokat/> Utolsó letöltés: 2023.01.04.

¹⁰⁴ A kép forrása: <https://www.jogiforum.hu/cikk/2018/11/26/illegalis-bortontelefon-csalasra-hasznaljak-a-bortonoket-ellepo-mobilokat/>

¹⁰⁵ Online: https://mobilarena.hu/teszt/turbosim/mi_is_ez.html Utolsó letöltés 2023.01.04.

¹⁰⁶ A kép forrása: <https://www.jogiforum.hu/cikk/2018/11/26/illegalis-bortontelefon-csalasra-hasznaljak-a-bortonoket-ellepo-mobilokat/>

A modifikációval már egy – apró méretei miatt – bejuttatható¹⁰⁷ „civil” SIM kártya alkalmazásával a készülék már teljes értékű, korlátozás nélküli mobiltelefonként funkcionált, amivel fogvatartottak akár börtönön belül egymással, vagy akár a társadalom felé is ellenőrizetlen módon kommunikálhatnak. A módosított készülékeket a fogvatartottak elvesztettnek jelentették, ezt követően rejtve tartották, hiszen a védőfólián egyértelműen észlelhető volt a módosítás. A módosított készülék így már egy tiltott tárgyként funkcionál, birtoklása fegyelmi cselekmény. Egy ilyen telefonnal rendelkezve a fogvatartott akár további bűncselekményeket (csalás) követhet el fogvatartása alatt, ahogyan ez 2016-ban is történt a Budapesti Fegyház és Börtönben.¹⁰⁸ A módosított mobiltelefon jelenségre válaszul a börtönökben önálló kutató csoportok alakultak, akik nagy számban végezték a fogvatartotti zárkák biztonsági vizsgálatát, így csökkentve a módosított készülékek számát. Már a jelenség előtt, 2014 végén elindult az új fogvatartotti mobil rendszer (FMR) előkészítése, amelynek eredményeképpen egy kifejezetten erre a célra tervezett és kivitelezett, ütésálló, cseppálló, csökkentett funkciókkal rendelkező fogvatartotti mobil-rádiótelefon készülék lett rendszerbe állítva 2017-ben. Az azóta alkalmazott rendszer és a hozzá tartozó készülékek működése problémamentes. Az eszköz rongálására és eltűnésre volt már példa, de azzal összefüggésben hardveres vagy szoftveres (nem hagyományos telefon operációs rendszer) módosításra nem történt precedens.



13. kép: az új típusú FMR készülék.¹⁰⁹

¹⁰⁷ Egy SIM-kártya fémtartalma csekély, a kapukeretes és egyéb fémkereső készülékekkel nehezen felderíthető. Méretéből adódóan könnyen elrejtendő számtalan helyen. (pl.: a fogíny külső oldalához szorítva). A hozzátartozók látogató fogadása során több esetben megpróbálták átjuttatni a fogvatartottak részére SIM kártyákat. (pl: ölelkezéssel)

¹⁰⁸ Online: <https://www.jogiforum.hu/hir/2018/09/03/a-budapesti-fegyhaz-es-bortonbol-kovettek-le-rabok-unokazos-csalast-zarkajukbol-bonyolitottak-a-telefonhivasokat-a-sertettek-szama-35/> Utolsó letöltés: 2023.01.04.

¹⁰⁹ A kép forrása: www.bv.gov.hu

7.2.2 Irattanulmányozó számítógépek fogvatartotti használata

Az adatgyarapodás, a dokumentumok tömeges megjelenése szükségessé tette az adathordozók praktikus alkalmazását bírósági és ügyészségi eljárások során. A tisztességes eljáráshoz való jog alapvető emberi jog, amelyet a szabadságelvonás során is biztosítani kell a fogvatartottaknak. Ebből következik, hogy a fogvatartásban lévő személynek folyamatban lévő büntetőügyeivel összefüggésben ügyiratainak megismerését biztosítani kell. Amennyiben a fogvatartott büntetőeljárással kapcsolatos ügyiratait elektronikus adathordozón igényli és kapja meg,¹¹⁰ akkor az irattanulmányozási lehetőségre alkalmas számítástechnikai eszközt a bv. intézetnek biztosítani kell.¹¹¹

A beérkezett adathordozókat az informatikai szakterületnek tüzetesen át kell vizsgálnia. Egyrésztől vizsgálni kell az adathordozó feladójának hitelességét és azt, hogy valóban az engedélyezett tartalom került elhelyezésre az adathordozón. Vizsgálni szükséges a megtévesztő megoldások meglétét (pl: átnevezett formátumok, rejtett fájlok stb.), ugyanakkor fontos tudni azt, hogy a vizsgáló az adatok tartalmát nem, csak valid jellegét vizsgálhatja.

Kockázatot hordoz az engedélyezett irattanulmányozási helységben elhelyezett asztali számítógép alkalmazási módja. Az irattanulmányozási tevékenységet a fogvatartottak általánosságban önállóan végzik, amely tevékenységet a felügyelet közvetlenül személyesen vagy elektronikus megfigyelő eszközzel (kamerával) időszakosan ellenőriz. A tevékenység ellenőrzése során meg kell győződni arról, hogy a fogvatartott magatartása az engedélyezett tevékenységgel megegyező, hiszen számos lehetőség elérhető arra, hogy a fogvatartott az általa használt számítógépet hardveresen, vagy szoftveresen módosítja (pl: tiltott tárgyként bejuttatott bootolható pendrive alkalmazása, vagy mobil-stick alkalmazásával tiltott internet elérés). Továbbá nehezíti a helyzetet, hogy számos esetben specifikus szoftverigény is jelentkezik az eszközök kapcsán, hiszen az eljárásokkal összefüggésben biztosított adatok formátuma széleskörű (pl: csalás vádjával összefüggésben pénzügyi adatbázisok kezelését biztosító szoftver). Természetesen a fogvatartotti célra biztosított személyi számítógépeken alkalmazott védelmi megoldások nem teszik lehetővé az említett módosításokat, azonban mint tudjuk, tökéletes védelem nem létezik.

¹¹⁰ 2017. évi XC. törvény a büntetőeljárásról 159. § (1)

¹¹¹ 2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról 127. § (1)

7.3. Összegzés

Összefoglaló gondolatként fontos kihangsúlyozni, hogy a hazai bv. szervek esetében eddig még nem történt jelentős kibertámadás, ugyanakkor a digitalizáció a börtönön belüli térnyerésének köszönhetően a támadható felületek száma exponenciálisan nő. A fogvatartotti humán tényező olyan speciális sajátosság, amelynek kockázatkezelése nem maradhat ki a börtönök kiberbiztonsági politikájából. A börtönök elektronikus információs rendszereinek sértetlensége és bizalmassága egyértelműen szervezeti felelősség. A prizonális környezetben jelen lévő elektronikus információs rendszerek támadhatóságának kockázatait minimálisra kell redukálni, az esetleges megkerülési módok megszüntetésére haladéktalanul intézkedni kell, hiszen a rendszerek megsértésének következményei jelentős negatív hatást okozhatnak a szervezet társadalmi megítélésére.

8. AZ ELEKTRONIKUS FOGVATARTOTTI ALAPNYILVÁNTARTÁS

A jövőben egy állam sikeres csak úgy lehet, ha helyt ad az állami szintű digitalizációnak. E területen kifejezetten fontos az együtt gondolkodás, valamint az önálló állami cselekvés is.¹¹² Az EU-s iránymutatások hazai ratifikációjának eredménye a Nemzeti Digitalizációs Stratégia,¹¹³ amely 2030-ig rögzíti a célokat. A magyar rendvédelmi szervek esetében az adatok digitalizációjára irányuló törekvés már alapvető célkitűzésnek mondható. Ennek a fejlődésnek a történetisége joggal érdemelne ki akár önálló tanulmányt is, de ez a dolgozat – a terjedelmi korlátok okán – a teljes körű és maradéktalan bemutatást nélkülözve kíván betekintést adni a büntetés-végrehajtás szervezet informatikai kultúrájába.

8.1. A fogvatartotti alapnyilvántartó rendszer történetisége

A bv. szervezet bűnügyi nyilvántartásának hajnalán a fogvatartottak nyilvántartásával szemben megfogalmazott elvárások a mai korokhoz képest csekély mértékűek voltak. A XX. század elején ez a nyilvántartás csak a börtönökben elhelyezett fogvatartottak létszámára és személyes adataira terjedt ki. Az erre a célra rendszeresített A/2-es méretű kemény fedeles könyvben vezették az adatokat, és nyilvántartásból kivezetést többnyire három élethelyzet indokolta: szabadult, átszállításra került vagy meghalt.¹¹⁴ Az évek során a nyilvántartás adatköre számos új adattal bővült, majd a rendelkezésre álló technológiák megjelenésével exponenciálisan nőtt. Az informatika térnyerésével a büntetés-végrehajtási szervezet sem kerülhette el azt a következményt, hogy az általa kezelt adatok digitalizált formát öltsenek. A folyamatos átállásnak köszönhetően a büntetés-végrehajtás digitális adatainak mértéke jelentős növekedésnek indult az elmúlt évtizedekben, 2017-re már olyan mértéket öltött, amelyben már egyértelműen érvényesültek a Big Data megoldások, ahogy ezt Veszeli (2017) is megállapította.¹¹⁵

¹¹² Online: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_hu
Utolsó letöltés: 2022.12.25.

¹¹³ Online:
<https://cdn.kormany.hu/uploads/document/6/60/602/60242669c9f12756a2b104f8295b866a8bb8f684.pdf> Utolsó
letöltés: 2022.12.25.

¹¹⁴ Bogotyán Róbert – Veszeli Dániel (2011): Bűnügyi nyilvántartás a büntetés-végrehajtásban: a múlt örökségének és a jelen kihívásainak hatása a közeljövő terveire. Börtönügyi Szemle 2011/3.sz. BvOP, Budapest. p. 61.

¹¹⁵ Veszeli Dániel János (2017): A rendvédelmi szervek közötti automatizált információ megosztás és elérés, Belügyi Szemle, Budapest 2017/11-12. p. 93.

Az elektronikus fogvatartotti alapnyilvántartás történetisége azonban nem 2017-ben, hanem attól jóval korábban megkezdődött. A nyilvántartási rendszer mindenkor igyekezett megfelelni a jogszabályok által felállított követelményeknek, ennek köszönhetően több önálló fejlesztésű rendszer is napvilágra került az évek során. A bv. szervezet informatikai infrastruktúra fejlődése és az elektronikus fogvatartotti alapnyilvántartás új verziói kéz a kézben jártak, hiszen a továbblépés, a fejlődés lehetőségét a kettő közötti dependencia vagy akadályozta, avagy ellenkezőleg, éppen segítette. A következő részben egy rövid, kronológiai bemutatás következik a büntetés-végrehajtási szervezet egyik legfontosabb elektronikus információs rendszeréről, az elektronikus fogvatartotti alapnyilvántartásról.

8.1.1 Fogvatartotti Alrendszer (FAR)

A 90'-es évek elején megjelent az igény egy, az egész országot átfogó elektronikus fogvatartotti nyilvántartásra. A fejlesztés több szálon indult el, mert nem csak a nyilvántartást kezelő programot kellett kifejleszteni, hanem egy teljes hálózatot is ki kellett építeni. A rendszer végül 1994-ben indult el. Több büntetés-végrehajtási szakterület (bűnügyi nyilvántartás, nevelés, biztonság, befogadó bizottság, elhelyezés, egészségügy) részére tartalmazott lekérdező funkciókat.

KK_SZALJEL		SZÁLLÍTÁS JELENTÉS - VÉGLEG SZÁLLÍTANDÓK			
Szállítás dátuma: 2009.01.26		Fényes : Nem küldtük még a KNy-be		Aláhúzott : Nincs döntés	
Név	Azon.	Ut.szabad.	I n d o k l á s	Teru.	Jává. Áll.
HAÁM ÖDÖN	LC-3988	114	kérelem		E
HABOLI LAJOS	LC-4287		hhh		T
(kk_dbf)(Rek.sz.: 2) (2. Név)					
Megnézés: Return		Felvitel: F11	Módosítás: F12	Törlés: F14	
Nyomtatás: F10		Megőrzéses szállítás: Do		Küldés Kny-be: F20	

14. kép: A Fogvatartotti Alrendszer képernyőképe.¹¹⁶

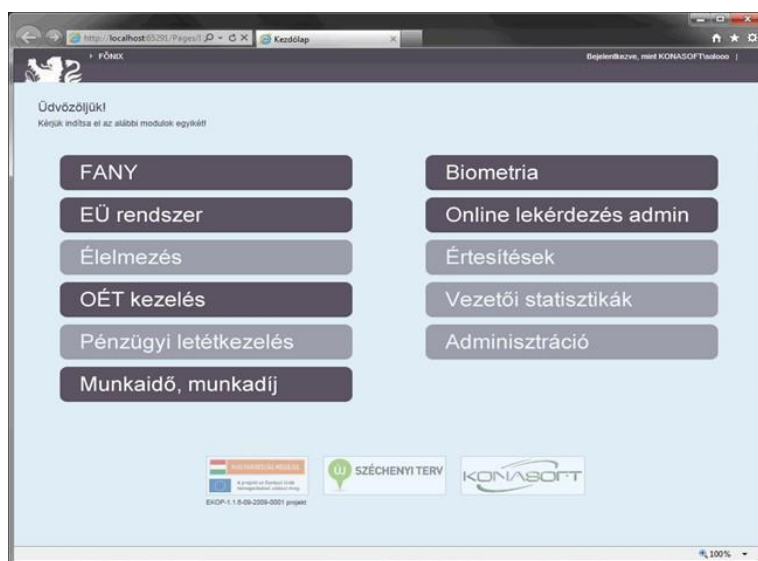
A lokális (bv. intézeti) helyszíneken elhelyezett PC-k terminálemulátor segítségével kommunikáltak a FAR adatbázisát futtató UNIX alapú központi szerverrel, az adatcsere

¹¹⁶ A kép forrása: Veszeli Dániel: A Fany Rendszer c. előadásanyaga. Online: <https://slideplayer.hu/slide/1953374/>

műholdas kommunikációs csatornákon keresztül történt.¹¹⁷ A rendszer eleinte kiszolgálta a felé támasztott elvárásokat, de a későbbiekben számos olyan igény keletkezett (pl: statisztikai lekérdezések) amelyek nem voltak elérhetőek, így egyértelműen megjelent az új rendszer fejlesztési igénye.¹¹⁸ Ezt tovább erősítette, hogy ebben az időszakban kezdte meg világuralmát a Microsoft Windows, amely kikényszerítette az irodai alkalmazáscsomagok használatát. Ennek a tényezőknek köszönhetően a grafikus felület iránti igény hozzájárult a fejlesztés sürgetéséhez.¹¹⁹

8.1.2 A Főnix és a Fogvatartotti Alapnyilvántartás (FANY)

Az informatikai fejlődésével a következő állomás a Főnix elnevezésű rendszer megjelenése volt. A Főnix már egy web alapú rendszerként, számos szaktevékenység támogatására tartalmazott önálló felületet. Ilyen önálló modul az egészségügy, az élelmezés, a tárgy és pénzügyi letétkezelés, munkaidő nyilvántartás, valamint a bűnügyi nyilvántartó biometri volt.



15. kép A Főnix rendszer kezdőlapja.¹²⁰

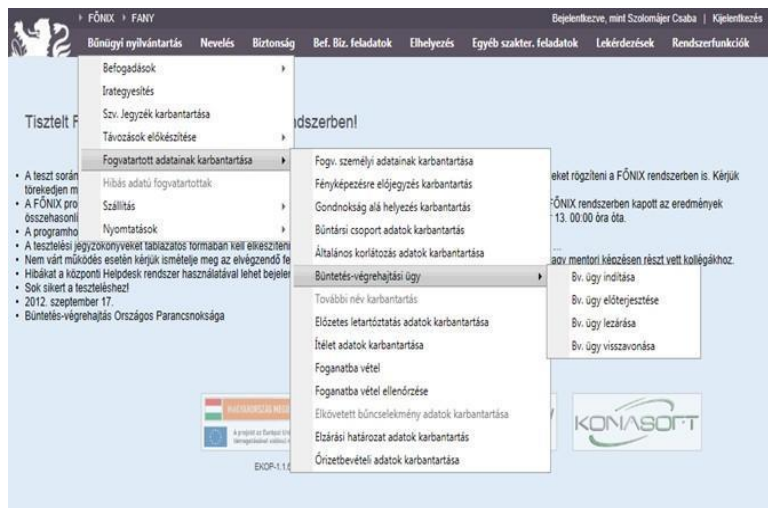
¹¹⁷ Soós Géza (2006): Az informatika szerepe a Büntetés-végrehajtási Szervezet fejlesztésében, Börtönügyi Szemle 2006/1. sz. BvOP, Budapest.

¹¹⁸ Horváth Mirtill Katalin (2022): Innovatív informatikai megoldások a büntetés-végrehajtásban, avagy a Főnix r bűnügyi nyilvántartási modulja c. TDK dolgozat, Nemzeti Közsolgálati Egyetem Rendészettudományi Kar, Büntetés-végrehajtási Tanszék. p. 6.

¹¹⁹ Kondás Katalin és Szűcs Endre (2017): informatikai korszakváltás egy büntetés-végrehajtási intézetben. Hadmérnök, XII. Évfolyam 2. szám. p. 273.

¹²⁰ A kép forrása: Veszeli Dániel: A FANY rendszer c. előadásanyaga. Online: <https://slideplayer.hu/slide/1953374/>

A Főnix fogvatartotti nyilvántartási modulja a Fogvatartotti Alapnyilvántartás (FANY) volt, amely még csak korlátozottan szolgálta ki az elemző-értékelő tevékenységeket, azonban már sokkal nagyobb adatbázist kezelt, mint elődje, így az adatbázisból már megfelelő informatikai támogatással (SQL lekérdezésekkel) manuálisan már lekérhetőek voltak a speciális adattáblák is további statisztikai célra.



16. kép: A FANY menürendszere¹²¹

A FANY a szaktevékenységek támogatása mellett a modern informatikai környezetekkel való együttműködési feltételeknek is eleget tett. Az adatbázist lokálisan is elérhetővé tették, így adott esetben, ha a központi szerver bármilyen okból nem volt elérhető, a munkavégzést nem akadályozta, ezzel a rendelkezésre állás már elfogadható mértékű volt. A rendszer jogosultságkezelése is megfelelő volt, hiszen a felhasználó csakis a munkakörében ellátott feladatokhoz kapcsolódó funkciókhoz kapott elérést a rendszerben. A rendszer naplózta a felhasználói tevékenységeket is oly módon, hogy az utólagos ellenőrzési tevékenység egyszerűen elvégezhető legyen. Az alkalmazás életének végül az informatikai modernizáció vetett véget, hiszen a jegyzett időszakban a szervezetnél jelentős informatikai infrastruktúrafejlesztés történt, ami már lehetővé tette egy újabb fejlesztési tevékenység kezdetét.¹²²

¹²¹ A kép forrása: Veszeli Dániel: A FANY rendszer c. előadásanyaga. Online: <https://slideplayer.hu/slide/1953374/>

¹²² Horváth Mirtill Katalin (2022): Innovatív informatikai megoldások a büntetés-végrehajtásban, avagy a Főnix rendszer bűnügyi nyilvántartási modulja c. TDK dolgozat, Nemzeti Közszerületi Egyetem Rendészettudományi Kar, Büntetés-végrehajtási Tanszék. p. 7.

8.1.3 Főnix 2

A következő fejlesztési ciklust már külső erőforrások igénybevételével hajtotta végre a szervezet. A Konasoft Kft.-vel együttműködve nem új fogvatartotti rendszer került kialakításra, hanem a szaktevékenységek támogatását segítették önálló, elkülönült modulok létrehozásával.

A Főnix 2 önálló moduljai:

- panasz és kártalanítás (PKTTR),
- pártfogói tevékenység támogató rendszer (PTTR),
- vezetői információs rendszer (VIR),
- BV foglalkoztatás,
- BV Bank,
- kockázatelemzési modul (PME).

Ezzel a megoldással eltérő kialakítású, de a központi fogvatartotti adatbázissal szinkronban álló rendszerek jöttek létre, azonban összességében szigetszerűvé vált a fogvatartotti nyilvántartások rendszere.

8.1.4 Főnix 3

A FŐNIX3 programnak az innováció törte meg utat, hiszen számos olyan új megoldás¹²³ integrálódott a fogvatartotti alapnyilvántartás mellé, amely fókuszba helyezte annak fontosságát. Egy olyan rendszer igénye fogalmazódott meg, amely a büntetés-végrehajtási szervezet informatikai szükségletét nem tüneti kezelésként látja el, hanem amelynek elsődleges fejlesztési szempontja a gyakorlati alkalmazhatóság. A fejlesztési program támogatására a nyilvántartási szakterület legtapasztaltabb munkatársai működtek együtt a szervezet Informatikai Főosztályával, valamint a külső fejlesztő társaságokkal, ennek a munkának az eredményeként jött létre 2021-ben a Főnix 3.

¹²³ Ilyen például az amerikai modell szerint létrehozott PME modul (Prediktív Mérőeszköz), amely a fogvatartottak fogvatartásával összefüggő, várható kockázatainak elemzésére és meghatározására szolgál.



17. kép: A Főnix 3 rendszer felhasználói felülete egy minta fogvatartotti adatlap megnyitásakor.¹²⁴

A rendszer egy reszponzív, web alapú megoldás, így a munkaállomásokon és tablet készülékeken is megfelelő felhasználói felületet biztosít. A felület kialakításánál cél volt, hogy a felhasználó minél rövidebb idő alatt kapja meg a számára szükséges információt. Ennek legfőképpen az a magyarázata, hogy a börtönben történt RES¹²⁵ felszámolása során az idő múlása kiemelten fontos tényező, így az információk beszerzéséhez szükséges időigényt a fogvatartotti alapnyilvántartás a lehető legkisebb mértékűre redukálja. A tartalmi elemeket tekintve fontos megemlíteni, hogy a bv. szervezeti törvény a fogvatartotti nyilvántartást a személyes adatok, a lakcímadatok és a kapcsolattartó személyekre vonatkozó adatok kivételével közhiteles nyilvántartásnak ismeri el,¹²⁶ így számos jogszabályi előírásnak, legfőképpen a bűnügyi nyilvántartási rendszerről szóló törvény rendelkezésének kell megfelelnie.¹²⁷ A nyilvántartás működtetését a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (KEK KH) látja el. A rendszerrel kapcsolatos jogosultságkezelés a FANY rendszer óta még kifinomultabbá vált. A nyilvántartásban számos

¹²⁴ A kép forrása: A BvOP belső használatú dokumentumából.

¹²⁵ Rendkívüli esemény, mint például fogollyszökés, fogolyzandulás, terrorcselekmény, bv. szervet ért fegyveres támadás stb.

¹²⁶ Veszeli Dániel János (2017): A rendvédelmi szervek közötti automatizált információ megosztás és elérés, Belügyi Szemle, Budapest 2017/11-12. p. 94.

¹²⁷ 2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról.

munkavégzést támogató elem került megvalósításra, mint pl: felhasználói felület személyre szabása, telefonkönyv, gyorskereső¹²⁸, határidő figyelés stb.

A rendszer négy fő részre bontható, melyek a biztonság, a bűnügyi nyilvántartás, a fogvatartás, valamint az általános rész. A rendszerben észlelhetőek a szervezeti elemek önálló tagoltsága is, hiszen a fogvatartotti alapnyilvántartást más-más célra használják a szakterületek, így természetesen a különböző részekbe a szaktevékenységet megfelelően segítő önálló funkciók kerültek beépítésre. A rendszerben található egy chatszolgáltatás is, ahol a fejlesztőkkel történő kommunikáció során a support rövid időn belül képes megoldást nyújtani az esetlegesen felmerülő problémákra.

A Főnix3 fejlesztése során már egyértelmű szakmai elvárás volt, hogy a rendszer kezelje a digitális dokumentumokat és járja ki a papírmentes iroda eléréséhez szükséges utat, így a különböző felületeket dokumentumfeltöltési lehetőség is adott, amely funkció nagyban segíti a visszamenőleges iratok keresését.

A legújabb technológiai vívmány a rendszerrel kapcsolatban egy olyan interface megoldás kialakítása volt, mely a bíróságokkal történő kapcsolat kialakítást szolgálta. Az igazságszolgáltatási szervek számos adatot szolgáltatnak a bv. szervezet további feldolgozás céljából. A fejlesztést megelőzően a papír alapú dokumentumok elektronikus nyilvántartásba történő rögzítése jelentős adminisztratív teher volt, azonban a kapcsolatnak köszönhetően ezek az adatok már digitálisan, újra rögzítés nélkül kerülnek be a fogvatartotti alapnyilvántartásba, így a bv. szervezetet érintő adminisztrációs hibák kockázata és a rögzítésre szükséges időigény is csaknem megszűnt.

A rendszerben található egy humoros szimbolikával elnevezett JARVIS modul, amely egy kifejezetten innovatív megoldás. JARVIS a Főnix 3 automatizált funkcióinak körét jelenti. A funkció összefogja a nyilvántartásban található bv. ügyeket (pl: fogvatartotti kérelmek), majd „intézi” azokat és jelzést ad, ha szükséges a személyes beavatkozás. A JARVIS előtti időkben, a hivatalból indított kérelmeket a személyi állomány tagjai indították és irányították az illetékesekhez, de az új megoldással a kérelmek jogszerűen, időben indításra kerülnek. Az ilyen ügyiratoknak tartalmi követelménye, hogy az adott ügyben illetékes szakterületek véleményeket írjanak a fogvatartottal összefüggésben. Az így megadott információk alapján a

¹²⁸ A gyorskereső funkció képes a fogvatartotti nyilvántartásban keresni a fogvatartott alapadataira, vagy akár ismert becenévre, de gúnynevére is.

döntési jogkör gyakorlója szakmai, adatok elemzésén és értékelésén nyugvó döntést tud hozni. JARVIS ezeket a szakmai véleményeket előre definiált szakmai sablonok alapján az adatbázisból önállóan megírja, így nagymértékben tehermentesíti a szakterületeket. Összességében elmondható, hogy a Főnix 3 korszerű megoldásaira büszke lehet a szervezet, innovatív jellege vitathatatlan. Korszerű és felhasználóbarát, képes kiszolgálni a XXI. századi igényeket.

8.2. Kapcsolódó informatikai szakrendszerek

A Főnix 3 fejlesztési és bevezetési időszakával egyidejűleg olyan informatikai megoldások kerültek kialakításra, amelyek nem a fogvatartotti alapnyilvántartás funkcióit bővítették, hanem az abban rejlő lehetőségre építve a személyi állomány terheit igyekeztek csökkenteni. Az elmúlt években számos új informatikai megoldás került lefejlesztésre a szakmai munka hatékonyságának növelése érdekében, az alábbiakban – a teljesség igénye nélkül – azok bemutatására kerül sor, amelyek interface kapcsolatban állnak Főnix 3 rendszerrel.

8.2.1 Navigator rendszer

A Navigator rendszer szintén az egyik legmodernebb, saját igényekre tervezett web alapú informatikai rendszer. A Navigator tervezése során a legfőbb célkitűzés a BvOP főigyeleti, valamint a bv. szervek ügyeleti tevékenységét támogatása volt. A rendszerrel szemben további cél volt, hogy a szervezet különböző adatbázisait egy felületen kezelje, és a rendelkezésre álló adatokat egy modern formavilágban vigye közelebb a felhasználóknak. A szervezeti igények megvalósításra kerültek a fejlesztés során, valamint a rendszer fejlesztése jelenleg is folyamatos. Az aktuális verzióban jelenleg 5 modul került integrálásra.¹²⁹

A modulok között megtalálhatunk egy gyors adatlekérésre és továbbítási módokra fejlesztett felületet, amely például egy bekövetkezett rendkívüli esemény során (pl: fogvatartott szökése) a szükséges adatok rendkívüli gyorsasággal továbbíthatóak a felszámolásban részt vevők, valamint a társ rendvédelmi szervek részére. A „*Jelenlévők keresése*” funkcióval, rendkívüli

¹²⁹ Hinkel Tamás (2020): A mesterséges intelligencia térhódítása a büntetés-végrehajtásban, Börtönügyi Szemle 2020/4. Budapest. p.18.

gyorsasággal történhet az információközlés, amely növeli a hatékonyságot egy olyan folyamatban, ahol az idő múlása kritikus tényező.¹³⁰

További hatékony funkció a „*Szállítások követése*” modul, amely egy kiemelten kockázatos biztonsági szakfeladatot, a fogvatartottak kör- és célszállításait¹³¹ támogatja. A funkció alkalmazásával valós időben nyomon lehet követni a fogvatartotti szállítójárművek mozgását, hiszen e járművekbe telepített EDR készülékek GPS technológiája ezt lehetővé teszi. A pontos helymeghatározás mellett a rendszer megjeleníti a szállítmánnyal kapcsolatos fontos adatokat (fogvatartottak adatai és ülésrendje), valamint van lehetőség a feladatot végrehajtókkal történő kapcsolatfelvételre is. Fontos, hogy a rendszerbe építve megtalálható egy automatikus riasztás funkció, mely aktiválja magát, amennyiben egy szállítójármű helyzetében 10 perc után sem áll be változás. A funkció segíti a szállítójárművekkel kapcsolatos logisztikát, a valós időben történő esetleges átszervezéseket, továbbá nagymértékben hasznosul olyan rendkívüli esetekben, mint például a szállítójárművet ért közlekedési baleset követő esemény felszámolási feladatok. A jövőben tervezetten a modul kiegészül olyan funkcióval is, mely során a szállítótérben elhelyezett elektronikus megfigyelési eszközök (kamerák) élőképeit valós időben lehet majd megtekinteni.

A bv. szerv alapfeladatai során számos nyilvántartást vezet, e nyilvántartások digitális vezetésének lehetőségét szolgálja az „*E-naplók*” modul. A modulban történik a bv. szervek területére be- és kilépő személyek és gépjárművek nyilvántartásának, az ellenőrzési naplónak, az előállításokkal kapcsolatos nyilvántartásnak, valamint a jelentésköteles események naplójának rögzítése.

¹³⁰ Hinkel Tamás (2020): A mesterséges intelligencia térhódítása a büntetés-végrehajtásban, Börtönügyi Szemle 2020/4. Budapest. p.18.

¹³¹ A körszállítás központilag, a BvOP illetékes szakterülete által szervezett, rendszeres, a hét első munkanapján végrehajtott szállítás a bv. intézetek között.



18. kép: Több papír alapú nyilvántartás szűnt meg a Navigator E-napló moduljának létrejöttével.¹³²

A modul legfőbb célja az eddigiekben papír alapon vezetett nyilvántartások (szolgálati okmányok) digitális megoldással történő kiváltása, egyúttal a nyilvántartásokban való keresések, valamint az ezekkel összefüggő elemző-értékelő munka hatékonyságának növelése volt. Az adatok bevitele során létrejött adatbázisokban már nagy számban állnak rendelkezésre szűrési lehetőségek, így az adatkinyerés időigénye töredéke lett a papíralapú okmányvezetésből való kinyeréshez szükséges időnek.¹³³

8.2.2 Szolgálati Alkalmazás a Fogvatartás Elősegítésére (SAFE)

Már említésre került, hogy a fogvatartás egyre nagyobb mértékben indukálja a digitális adatokat. Ezek az adatok több folyamatban képesek hasznosulni, és közvetlenül a fogvatartottakkal foglalkozó személyi állomány feladatellátását is hatékonyan képesek támogatni. A szolgálati helyeken elhelyezett irodai munkaállomások helyhez kötöttek, így nem kínálnak lehetőséget az eltérő helyszíneken történő folyamatos (avagy dinamikus) támogatásra. Nagy szükség volt egy olyan megoldás kialakítására, amely a végrehajtás szintjén integrálódik, és kiszolgálja a feladatellátás során fellépő adatigényléseket, egyúttal csökkentve az adminisztratív terheket is. A Szolgálati Alkalmazás a Fogvatartás Elősegítésére (SAFE rendszer) egy erre a célra fejlesztett mobilalkalmazás.

¹³² A kép forrása: A BvOP belső használatú dokumentumából.

¹³³ Hinkel Tamás (2020): A mesterséges intelligencia térhódítása a büntetés-végrehajtásban, Börtönügyi Szemle 2020/4. Budapest. p.18.



19. kép: A SAFE rendszer felhasználói felülete.¹³⁴

A mobileszközön egy alkalmazás fut, amely adatkapcsolatban van az elektronikus fogvatartotti alapnyilvántartással. A tesztelés 2017-ben kezdődött meg, majd 2021-re valamennyi hazai bv. szervben is alkalmazásra került. A rendszer WiFi¹³⁵ vagy APN¹³⁶ technológiával csatlakozik a központi szerverhez, amelyről szinkronizálja a szükséges adatokat, majd a frissítést követően offline üzemel, így garantálva azt, hogy a különböző építészeti megoldások sem korlátozzák az eszköz hálózati elérését.¹³⁷

A rendszer újdonsága, hogy a fogvatartotti mozgatási folyamatok adminisztrációja automatizáltan történik, hiszen a fogvatartottak birtokában található NFC chipet tartalmazó azonosító kártyát a felügyelet a készülék alkalmazásával beolvassa, így a dokumentálási folyamat a másodperc törtrésze alatt megtörténik. Ugyanakkor nem csak a fogvatartottak kerültek ellátásra NFC kártyával, hanem azok elhelyezésére szolgáló zárak, körletrészek és körletek bejárata is, így az ajtók mellett elhelyezett NFC kártya beolvasásával összefüggő automatikus adatbázis lekérdezési funkcióval a felügyelet azonnali nyilvántartást kap a zárkában/körleten elhelyezett fogvatartottakról, valamint a velük kapcsolatos fontos adatról

¹³⁴ A kép forrása: a BvOP belső használatú anyagából.

¹³⁵ Vezeték nélküli mikrohullámú kommunikáció (wireless fidelity).

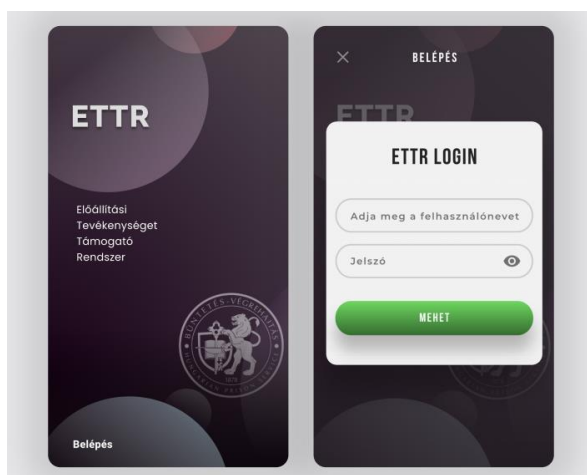
¹³⁶ Access Point Name, vagyis hozzáférési pont név.

¹³⁷ Hinkel Tamás (2020): A mesterséges intelligencia térhódítása a büntetés-végrehajtásban, Börtönügyi Szemle 2020/4. Budapest. p.18.

(létszám, biztonsági kockázat stb.). Ez az innovatív informatikai megoldás sikeresen hozzájárul a részlegen szolgáltatot teljesítők testi épségéhez és védelméhez is.¹³⁸

8.2.3 Előállítási Tevékenységet Támogató Rendszer (ETTR)

Az Előállítási Tevékenységet Támogató Rendszer (ETTR) a SAFE rendszerhez hasonlóan egy mobileszközre kifejlesztett alkalmazás. Amíg a SAFE rendszer a körleteken szolgáltatot teljesítő személyi állománynak szolgál támogatásul, addig az ETTR a börtön falain kívül megvalósuló kockázatos biztonsági tevékenységet, az előállítást kívánja támogatni. Az előállítás során a bv. szervet elhagyó felügyelő az előállítás teljes végrehajtási ideje alatt az ETTR rendszert alkalmazza. Az ETTR rendszer kölcsönösen segíti a végrehajtást végző felügyelőt az előállítás szakmai végrehajtásában, ugyanakkor valós időben adatot szolgáltat az előállítás aktuális állapotáról az ügyeleti központ részére.



20. kép: Az ETTR rendszer felhasználó felülete.¹³⁹

Az alkalmazás az előállítást végző felügyelő részére bocsájt minden fogvatartottal és annak előállításával kapcsolatos olyan információt, amelyből fel tud készülni a feladat biztonságos végrehajtására. Ez követően egy támogató rendszerként segítséget nyújt ahhoz, hogy a felügyelet a fogvatartott előállítási folyamatának szükséges lépéseit maradéktalanul végrehajtsa (személyi állomány eligazításának megtörténte, fogvatartott eligazítása stb.). Az alkalmazás biztosítja a hangfelvétel lehetőségét annak érdekében, hogy a fogvatartott eligazításának

¹³⁸ Hinkel Tamás (2020): A mesterséges intelligencia térhódítása a büntetés-végrehajtásban, Börtönügyi Szemle 2020/4. Budapest. p.18

¹³⁹ A kép forrása: a BvOP belső használatú dokumentumából.

megtörténtét, és fogvatartott általi tudomásulvételét a későbbiekben esetleges szükségesség céljából igazolni lehessen.

Az eligazítás végén a felügyelet elvégzi a fogvatartott magatartásának, a civil jelenlévő személyek biztonsági szempontú értékelését, valamint jelölheti a védő és a média jelenlétét is. Ezeket az adatokat a későbbi előállítások szervezésénél figyelembe veszik, és ez alapján hozzák meg az esetleges további szükséges biztonsági intézkedéseket. Fontos funkció a rendszerben, hogy az előállítás alkalmával bekövetkező RES során annak megtörténtét rögzíteni lehet a rendszerben, és ezt követően egy „*teendők listája*”-val szolgál az alkalmazás, így stresszhelyzetben jelentős segítséget nyújt a helyes intézkedések megtételében. Az ETTR alkalmazása az informatika előnyeivel hozzájárul az előállítási tevékenységek hatékonyabb végrehajtásához, és egyértelműen csökkenti az azzal kapcsolatos kockázatokat.

9. A KUTATÁS

9.1. A mintavétel

A kérdőíves mintavétel két csoportra bontva valósult meg. Annak érdekében, hogy a börtönökben szolgálatot teljesítő végrehajtói állomány ne kerüljön terhelésre a kérdőívekkel, első csoportként Nemzeti Közsolgálati Egyetem Rendészettudományi Kar Büntetés-végrehajtási Tanszékhez vezényelt nappali és levelező munkarendű hallgatóival kerültek felvételre. A levelező tanrendes hallgatók jelenleg az ország egész területén, különböző típusú intézetekben és szakterületeken teljesítenek szolgálatot különböző beosztásokban. A nappali tanrendes hallgatók úgynevezett kettős jogállású hallgatók, vagyis hivatásos és hallgatói jogviszonnyal is rendelkeznek. Tanulmányaik megkezdése előtt átlagosan több éves (de minimum 1 éves) gyakorlatot szereztek a végrehajtás területén, továbbá a hallgatói jogviszony alatt teljesítendő gyakorlati idő biztosítja számukra a tanulmányi évek alatt az aktuális szakmai tapasztalatot. A másik csoport nem célzottan került kiválasztásra, hanem a Szerző személyes kapcsolatainak köszönhetően kerültek felkeresésre a szervezetben aktív szolgálatot ellátó személyi állományi tagok. Mindkét csoport tekintetében a mintavétel 2023.03.05 – 2023.03.20. között, elektronikusan, a Google Űrlap szolgáltatásának alkalmazásával valósult meg. Együttesen 103 db kérdőív került felvételre. A kérdőív nyomtatott formában a dolgozat 1. számú mellékleteként megtalálható.

A kérdőívekben összeállított kérdéssor célja kettős volt. Elsődleges célként a büntetés-végrehajtási szervezet személyi állományának kiberbiztonsághoz való viszonyát tárja fel, különösen a bv. szervek vonatkozásában. Speciális célként az elektronikus fogvatartotti alapnyilvántartás rendelkezésre állásának fontosságát, és annak hiánya esetén felmerülő hatások mértékét kívánja mérni.

A kvalitatív mintavétel során egyéni, anonim interjúk készültek a Budapesti Fegyház és Börtön közép- és beosztott vezetői állománya vonatkozásában. A 7 darab vezetői interjú alanyai célirányosan lettek kiválasztva, parancsnokhelyetteseket, valamint szakterületei vezetőket érintett az alábbi területekről: Biztonsági Osztály, Nyilvántartási Osztály, Fogvatartási Ügyek Osztálya. Az interjúk alapvetően strukturálisnak tekinthetők, hiszen három kérdés kivételével a kérdések azonosak voltak a kérdőívben megtalálhatókkal. Az eltérő kérdések a vizsgált Főnix 3 rendszer sértetlenségére, és bizalmasságára irányultak, valamint a záró kérdés arra vonatkozott, hogy a jövőre nézve hogyan fejlesztenék a szervezeti kiberbiztonságot. Segítette

az interjúk lebonyolításának folyamatát, hogy az interjúztató (a Szerző) korábban Budapesti Fegyház és Börtön személyi állományába tartozott, így a kölcsönös bizalmi viszony adott volt, annak kialakításán nem kellett dolgozni. A lebonyolítás a már említett strukturált jelleg mellett rugalmasságot is tartalmazott, így a válaszadásokat helyenként együttes konstruktivitás kísérte. A vezetői interjúk lebonyolítására 2023.03.20-án került sor, átlagosan személyenként 45 perc időtartamban. Az interjúkban elhangzott válaszokról kondenzációs táblázat készült, amely a 2. számú mellékletként került elhelyezésre a dolgozatban.

9.2. A kérdőívek eredményei

A 103 db kérdőív által szolgáltatott adatok közül érvénytelen nem volt. A válaszok számadatokká való átalakítását követően a kiértékelés az IBM SPSS Statistics szoftverrel történt. Az adatok ábrázolása a terjedelmi korlátok okán a helyigényes grafikonok helyett szöveges táblázatként kerülnek megjelenítésre.

A felmérésben résztvevők demográfiai adatai a következőképpen alakultak:

Az Ön neme?			Az Ön kora?		
	Elemszám	%		Elemszám	%
Férfi	59	57	18-28 év	27	26
Nő	44	43	29-39 év	45	44
Összesen	103	100	40-50 év	26	25
			51+ év	5	5
			Összesen	103	100

A mért adatok egymáshoz való viszonyulása megfelelő, képes igazolni a kérdőív által szolgáltatott adatok validitását. A nemek és a korcsoportok mért eloszlása arányosnak tekinthető az egész populációra nézve.

A felmérésben résztvevők bv. szervezetéhez való viszonyulásai a következőképpen alakultak:

Hány év szolgálati idővel rendelkezik a bv. szervezetnél?			Az Ön szolgálati helye:		
	Elemsszám	%		Elemsszám	%
0 - 5 év	30	29	Agglomerációs Központ	34	33
5 - 10 év	38	37	Egyobjektumos. bv. intézet	26	25
10 - 15 év	21	20	Intézmény (IMEI, BvEK)	6	6
15 - 20 év	9	9	Több obj. bv. intézet	37	36
21 + év	5	5	Összesen	103	100
Összesen	103	100			

A mért adatok azonos arányokat mutatnak a szakmában tapasztalt eloszlással, így igazolhatja a mintavételben tett megállapítások teljes populációra való érvényességét. Tanúsítják továbbá a mintavétel sokszínűségét, valamint, hogy sikeresen érintett olyan szervezeti specifikumokat, mint a Büntetés-végrehajtás Egészségügyi Központja (BvEK), vagy az Igazságügyi Megfigyelő és Elmegyógy Intézet (IMEI) is.

Milyen beosztáscsoportban teljesít szolgálatot?			Melyik szakterületen teljesít szolgálatot?		
	Elemsszám	%		Elemsszám	%
Végrehajtó	79	77	Agglomerációs Osztály	5	5
Középvezető	21	20	Biztonsági Osztály	48	46
Vezető	3	3	BvOP	1	1
Összesen	103	100	Egészségügyi Osztály	4	4
			Egyéb	6	6
			Ellenőrzési Osztály	1	1
			Fogvatartási ügyek Osztálya	8	8
			Műszaki és Ellátási Osztály	4	4
			Műveleti Osztály	3	3
			Nyilvántartási Osztály	11	10
			Pszichológiai Osztály	4	4
			Személyügyi és Szociális Osztály	4	4
			Titkársági Osztály	1	1
			Vezetői Közvetlen	2	2
			Vezetői Törzs	1	1
			Összesen	103	100

A mintavételtől az egyik alapvető elvárás volt, hogy főként a végrehajtói állományból merítsen, és legfőképpen a Biztonság, a Fogvatartási Ügyek, a Nyilvántartás és az Egészségügy szakterületeiről, de egyúttal ne csak kizárólag ezeket a szakterületeket vizsgálja. Ennek oka, hogy a vizsgált informatikai rendszereket a felsorolt szakterületek alkalmazzák leginkább, az alkalmazott rendszerek hatásai legfőképpen e szakterületeket érinthetik. A beosztáscsoportok érték eloszlása elfogadható, arányait tekintve a valóságot tükrözik. A szakterületekről érkező nyilatkozatok is megfelelnek az elvárt adatokkal. Várható volt, hogy a legdominánsabb szakterület a biztonsági lesz, azonban a vártnál erősebben jelent meg a mintában, míg a többi kívánt szakterület alacsonyabb mintaszámot produkált, de összességében azt a valósággal azonos eloszlásnak tekinthetjük.

A büntetés-végrehajtási személyi állományának véleménye a kiberbiztonságról:

Ön szerint mennyire fontos manapság a kiberbiztonság?			Ön szerint, mennyire fontos a bv. szervek tekintetében a kiberbiztonság?		
	Elemszám	%		Elemszám	%
1	1	1	1	0	0
3	5	5	2	0	0
4	20	19	3	5	5
5	77	75	4	25	24
Összesen	103	100	5	73	71
			Összesen	103	100

Ennél a kérdéspárnál a válaszadók 1-től 5-ig terjedő skálán értékelhették a választ, ahol az 1-es számhoz a „*Nem fontos*”, míg az 5-ös számhoz a „*Kiemelten fontos*” jelentés társult. A hasonló típusú kérdéseknél megadott válaszok skála típusú változóként kerültek statisztikai feldolgozásra. A kérdőívek kitöltői szerint a kiberbiztonság, valamint a bv. szervek kiberbiztonsága kiemelten fontos. A mért értékek közel azonosak mindkét kérdés esetében, tehát a kitöltők szerint az „általános” kiberbiztonság és a bv. szervek esetében is egyaránt fontos tényező manapság.

Ön szerint számítani lehet egy börtönt érintő kibertámadásra?			Ön szerint milyen mértékben foglalkozik a bv. szervezet a kiberbiztonsággal?		
	Elemsszám	%	Skálaérték	Elemsszám	%
Igen	49	47	1	11	11
Nem	8	8	2	18	17
Nem tudom	3	3	3	43	42
Talán	43	42	4	19	18
Összesen	103	100	5	12	12
			Összesen	103	100

A következő kérdéspár a börtönt érintő kibertámadás kockázatának jelenlétét, valamint a szervezet kockázatokhoz való hozzáállásának kitöltők szerinti érezhető mértékét mérte. A kockázok valóságát igazolja, hogy a kitöltők 48%-a úgy gondolja, hogy egy börtönt érintő kibertámadásra számítani kell, valamint a 42%-a gondolja úgy, hogy egy ilyen támadás eshetősége áll fenn. A második kérdésnél a válaszadók 1-től 5-ig terjedő skálán értékelték a választ, ahol az 1-es számhoz a „Csekély”, míg az 5-ös számhoz a „Megfelelő” jelentés társult. A hasonló típusú kérdéseknél megadott válaszok skála típusú változóként kerültek statisztikai feldolgozásra. A válaszadók véleményei alapján a szervezet hozzáállása a kiberbiztonsághoz egy középértékű szimmetrikus modellt eredményezett, amely értékek mögött valószínűleg a közép szintű elégedettség vagy / és a határozott irányba tolódó válaszadás döntésképtelensége állhat.

Az elektronikus fogvatartotti nyilvántartással összefüggő kérdésekben egyaránt feltüntetésre került a Főnix 3 rendszer mellett az azzal kapcsolatban álló SAFE, az ETTR rendszerek is, hiszen a végrehajtási közegben ezeket a rendszereket alkalmazzák.

Ön szerint manapság a büntetés-végrehajtási feladatok jogszerű ellátásához nélkülözhetetlen a Főnix 3, SAFE, ETTR, Navigator informatikai rendszerek alkalmazása?			Ön szerint milyen mértékben támaszkodunk a feladatellátás során az alábbi informatikai rendszerekre: Főnix 3, SAFE, ETTR, Navigator?		
	Elemsszám	%	Skálaérték	Elemsszám	%
Igen	83	81	1	1	1
Nem	13	12	2	6	6
Nem tudom	2	2	3	10	10
Talán	5	5	4	35	34
Összesen	103	100	5	51	49
			Összesen	103	100

Az speciális kérdéscsoport első kérdése a vizsgált rendszerek jogszerű feladatellátáshoz való szükségességét kívánták felmérni, a kapott adatból egyértelműen megállapítható, hogy a válaszadók szerint a jogszerű feladatellátáshoz nélkülözhetetlen a megnevezett rendszerek alkalmazása. E mellett önálló kérdésben lett vizsgálva annak a mértéke, hogy a mindennapi feladatellátás érdekében milyen mértékben kell alkalmazni a vizsgált rendszereket. A kérdés esetében a válaszadók 1-től 5-ig terjedő skálán értékelték a választ, ahol az 1-es számhoz a „Csekély mértékben”, míg az 5-ös számhoz a „Jelentős mértékben” jelentés társult. A kapott adatok igazolják, hogy a válaszadók jelentős mértékben alkalmazzák ezeket a rendszereket, és a feladatellátás fundamentumaként is jellemezhetjük.

A következő kérdéspár azt vizsgálta, hogy a vizsgált rendszerek leállása / elérhetetlensége milyen mély hatásokkal jár a végrehajtásban. Az első kérdés a rendeltetésszerű működésre gyakorolt hatást vizsgálta. A kérdés esetében a válaszadók 1-től 5-ig terjedő skálán értékelték a választ, ahol az 1-es számhoz a „Csekély mértékben”, míg az 5-ös számhoz a „Jelentős mértékben” jelentés társult. A kapott adathalmaz a jelentős mérték felé erősödő modellt generált, így a válaszadók véleménye alapján igazolható az az állítás, hogy a vizsgált rendszerek leállása képes megzavarni egy intézet rendeltetésszerű működését.

Ön szerint milyen mértékben zavarhatja meg a Főnix 3, SAFE, ETTR, Navigator rendszerek leállása egy bv. intézet rendeltetésszerű működését?			Ön szerint a Főnix 3, SAFE, ETTR, Navigator rendszerek elérhetlensége okozhat rendkívüli eseményt?		
Skálaérték	Elemsszám	%		Elemsszám	%
1	4	4	Igen	54	52
2	9	9	Nem	19	18
3	9	9	Nem tudom	3	3
4	31	30	Talán	27	26
5	50	49	Összesen	103	100
Összesen	103	100			

A másik kérdés az első megfogalmazásnál mélyebbre próbált hatolni. Azt kívánta vizsgálni, hogy a vizsgált rendszerek elérhetetlensége okozhat-e rendkívüli eseményt. A kérdés a válaszok alapján igazoltnak tekinthető, hiszen a válaszadók 52%-a igennel válaszolt, míg az eshetőséget a 26%-a jelölte meg. Érdekes megfigyelésként szolgálhat, hogy a feleletválasztós kérdések közül ebben a kérdésben érte el a „Nem” válasz a legnagyobb előfordulást. Ennek oka több minden lehet. A Szerző véleménye szerint leginkább az, hogy a szervezeti kultúra a rendkívüli

esemény alatt leginkább a fogolyszökést és a hasonló volumenű súlyos rendkívüli eseményeket érti, amely eseményekkel összefüggésben informatikai dependenciát nehéz feltételezni/bizonyítani.

A kérdőív utolsó kérdése arra irányult, hogy a rendszer elérhetetlensége okozta hatások közül jelen van-e a fogvatartottak alapjogi érintettsége.

Ön szerint a Főnix 3 rendszer elérhetetlensége akadályozhatja a fogvatartottak kapcsolattartási formáinak megvalósulását?		
	Elemszám	%
Igen	57	55
Nem	18	17
Nem tudom	2	2
Talán	26	25
Összesen	103	100

A kapott válaszokból megállapítható, hogy a feltételezés helyénvaló, hiszen a válaszadók több mint fele gondolta úgy, hogy a rendszer elérhetetlensége képes akadályt gördíteni a fogvatartotti kapcsolattartás elé, ezáltal az alapjogi érintkezés bizonyítható. Ugyanakkor a „Talán” válaszban értelmezhető eshetőség mértéke 25%, ami szintén jelentős mérték. Érdekes adatként szolgálhat, hogy a feleletválasztós kérdések közül ebben a kérdésben érte el a „Nem” válasz közel a legnagyobb előfordulást. Ez a magas érték valószínűleg annak köszönhető, hogy a kérdés már olyan mélységig hatol be a végrehajtási közegbe, amely már megosztó.

9.3. Az interjúk eredményei

Az vezetői interjúk eredményei a legtöbb esetben alátámasztják a kérdőíves felmérés megállapításait, e mellett viszont számos többlet információt is felszínre tártak. A kérdésekre adott válaszokból táblázatos formájú kivonat készült, amely a dolgozat 2. számú mellékleteként érhető el. A táblázatban aláhúzással és félkövér jelzéssel kerültek kiemelésre azok a válaszok, melyek azonosnak tekinthetők a kérdőíves eredményekkel, míg az azzal ellentétes vélemények aláhúzással és dőlt betűstílussal kerültek jelölésre. Pár esetben a válaszadásban nem történt egyértelmű állásfoglalás, ezek a vélemények csak **félkövér** kiemeléssel lettek ellátva.

A kiberbiztonságot és a bv. kiberbiztonságot megosztottság nélkül (7/7) fontos tényezőkként azonosították az interjúalanyok. Némi megosztottság jelenik meg a bv. szerv kibertámadásának kockázatára irányuló kérdésnél, itt a 7 válaszadóból 2 nem gondolta számottevőnek a veszélyt. A szervezet kiberbiztonsági tevékenységének kérdőíves középértéke az interjúk során is hasonló átlageredményt adott (5/7 középérték, 1 alá és 1 fölé értékelés).

A rendszerek jogszerű feladatellátáshoz köthető nélkülözhetetlensége azonban erősen megosztott eredményt produkált, és nem erősítette meg a kérdőívek eredményeit. Ennek oka az lehet, hogy a vezetői gondolkodást befolyásolja az a múltbéli tapasztalat, hogy pár évvel ezelőtt még informatikai rendszerek nélkül is lehetséges volt a jogszerű feladatellátás. A szükséges feltételek (pl: papír alapú naplók és a vezetésükhöz szükséges szakmai ismeret) még manapság is a rendelkezésre állnak, így véleményük szerint a jogszerűség biztosítható informatikai rendszerek nélkül is.

A vizsgált rendszerekre való jelentős ráutaltság bizonyításra került a vezetői vélemények által is (6/7). Az interjúk igazolták a kérdőívek eredményeit abban a tekintetben is, hogy a vizsgált rendszerek leállása okozhat rendkívüli eseményt egy bv. intézet esetében. (6/7). A rendeltetésszerű működés megzavarásával összefüggésben megosztó vélemények születtek, egyértelmű következtetés nem vonható le a válaszokból, azonban, a vizsgált rendszerek elérhetetlensége akadályozhatja a fogvatartottak kapcsolattartásának megvalósulását az interjú alanyok vélemények alapján (6/7) is.

Az interjúban feltett három, kérdőívtől eltérő kérdésben adott válaszokat a mellékinformációk elemzésével együtt kerülnek feltüntetésre a következő fejezetben.

9.4. Elemzés és hipotézis bizonyítás

A kérdőíves mintavétel, valamint a vezetői interjúkból megállapítható, hogy a szervezetben dolgozók véleménye szerint a kiberbiztonság és a **büntetés végrehajtási kiberbiztonság kiemelkedően fontos terület**, valamint egy **börtönt érintő kibertámadás bekövetkezését valós veszélyként kell kezelni**. A szervezet kiberbiztonság-politikájának középértékű minősítése egyaránt meggyőzően észlelhető a kérdőívek és az interjúk eredményei között. Az eredmények igazolják, hogy **aktívabb szervezeti kiberstratégiai tevékenység szükséges** a

A bv. intézetek feladatellátásuk során az **elektronikus fogvatartotti nyilvántartásra bizonyítottan nagymértékben támaszkodnak**, azonban annak **nélkülözhetetlensége a**

jogszerű feladatellátáshoz nem állapítható meg minden kétséget kizáróan. A kérdőívek eredményei igazolnák azt, de az interjú alanyok által adott válaszok bár részben megosztóak voltak, összességében meggyőzőek voltak abban a tekintetben, hogy a jogszerűséget egy bv. intézet képes biztosítani a jelenleg már alternatív megoldásnak mondható papír alapú nyilvántartások, dokumentumok vezetésével.

Annak tekintetében, hogy a rendszerek leállása egy bv. intézet rendeltetésszerű működésében **komoly zavarokat és/vagy rendkívüli eseményt okozhat, összességében igazolást nyert,** de a kérdőívek és az interjúk által szolgáltatott eredmények összevetése **további jellemzőket tárt fel.** A kérdőívek eredményeit vizsgálva megállapítható, hogy mindkét kérdés esetében a válaszadók közel fele nyilatkozott egyértelműen igennel, míg 26% és 30% az eshetőséget jelölte meg. Az eredményeloszlás okának feltárásához az **interjúk eredményei szolgálhatnak eszközzel.** A kérdéspár első kérdésével összefüggő interjúk rendkívüli esemény eshetőségére adott válaszaiban megjelenik megosztott polaritás, miszerint **rendkívüli esemény okozójává igen, viszont súlyos rendkívüli esemény¹⁴⁰ okozójává nem** válhatnak vizsgált rendszerek leállásai.

A rendeltetésszerű működés megzavarására irányuló kérdésre adott **vezetői válaszok egymáshoz viszonyítva, sőt még válaszokon belül is erősen megosztottak,** velük összefüggésben egyértelmű, önálló megállapítás nehezen tehető. Az interjúválaszok kérdőív-eredményektől eltérő, valamint az egymáshoz viszonyított megosztott válaszait valószínűleg a „rendeltetésszerű működés” megfogalmazás körülötte fogalmi zavar okozhatta, hiszen ehhez a kifejezéshez egyesek a tágabb értelmezést, míg mások a sarkalatos, jogszabály jellegű megfogalmazást társítják. Az kapott válaszokban azonban számszerű többségben van az a megállapítás, amely szerint a **zavaró hatás egyértelműen nagy mértékben indukálódhat.** Így a kérdőívek eredményeivel együtt kiértékelve megállapítható, hogy **az I. számú hipotézist,** miszerint „*egy bv. intézetet érintő kibertámadás képes jelentős zavarokat okozni a rendeltetésszerű működésben*” **sikerült igazolni. Az elektronikus fogvatartotti alapnyilvántartás és az azzal összefüggő elektronikus információs rendszerek elérhetetlensége nagymértékben megzavarja a bv. intézetek rendeltetésszerű működését, hatással van a biztonság állapotára és adott esetben rendkívüli esemény forrása is lehet.**

¹⁴⁰ Olyan rendkívüli esemény, amely a közrendet, vagy közbiztonságot veszélyeztetné (pl: fogolyszökés)

A II. számú hipotézis kijelentésének (*Az elektronikus fogvatartotti alapnyilvántartást érintő kibertámadás hatásai fogvatartotti alapjogokat is érinthetnek*) vizsgálatára legfőképpen a kérdőív 15. kérdése irányult. A válaszadók véleménye szerint a Főnix 3 rendszer elérhetetlensége **akadályozhatja** (*levelezés, telefonbeszélgetés, látogatófogadás megjelenése, telekommunikációs a kapcsolattartási formák eszköz, csomagküldés, eltávozás, látogatófogadás intézetén kívül, kimaradás, reintegrációs eltávozás*) megvalósulását, ezáltal a fogvatartás alanyának **alapjogi érintettsége megvalósulhat**.¹⁴¹ A kérdőívek eredményeit a vezetői interjúk válaszai kimagasló arányban (6/7 eset) is igazolták. Az eredményeket összevetve megállapítható, hogy **egy kibertámadás hatása nem csak a börtön állapotát befolyásolja, hanem annak legmélyére hatolva a fogvatartottak alapjogaival is képes érintkezni. A kapott eredményeknek köszönhetően a II. számú hipotézis is igazoltnak tekinthető.**

A vizsgált rendszerek bizalmasságára irányuló vezetői interjú kérdések válaszaiban legfőképpen **a jogosultságkezelés fontossága** kerül felszínre. A vezetők fontosnak tartják, hogy a legérzékenyebb adatokhoz csak a szükséges mértékben, csak az arra jogosult személyek férjenek hozzá, ugyanakkor véleményük szerint a túl szigorú jogosultságkezelés akadálya is lehet a hatékony szakmai munkának. Az interjúk kivonatában a terjedelmi korlátok miatt nem került említésre, de a vezetők több esetben jelentették ki azon ellenőrzési tevékenység fontosságát, amely során a bizonyos jogosultságokkal rendelkező személyek által megtekintett adatok indokoltságát vizsgálja. Valamint nem ennél a kérdésnél került megfogalmazásra, de ide sorolható az a vezetői véleménynyilvánítás, amely a jogosultság felülvizsgálatának fontosságát említi abban az esetben, ha a személyi állományú tag más szakterületre kerül áthelyezésre.

A sértetlenséget minden vezető egyaránt fontosnak gondolja. Az állapot megsértését összességében komoly kockázatként jelölték meg, hiszen bármilyen rosszindulatú adاتمódosítás komoly, a fizikai életre kiterjedő hatásokkal járhat. Megfogalmazásra került az a bv. szervezeti sajátosság, hogy a sértetlenség állapotára a **fogvatartotti csoport is jelentős kockázati tényező**, így a védelmi intézkedésnek ezt a sajátosságot is figyelembe kell vennie. Továbbá, megfogalmazásra került szoftveres védelemnek a fontossága, amely biztosítja, hogy adott szakterület adatbázisában módosítani más szakterület dolgozója ne legyen képes.

¹⁴¹ A védővel, jogi képviselővel történő kapcsolattartás korlátozása – akár kibertámadás okozataként is – egyértelműen érinti a tisztességes eljáráshoz való alapjogot.

Az utolsó kérdés főként a további javaslatok és a vizsgálat során esetlegesen nem érintett kockázatok feltárása érdekében került megfogalmazásra. Az adott válaszokból megállapítható, hogy a **személyi állományi tagok információbiztonsági tudatosítása, képzése kiemelt helyet foglal el a vezetői elképzelések között**. Hasonló számban került megfogalmazásra az **informatikai infrastruktúrafejlesztés szükségessége**, de olyan elgondolkodtató vélemény is feltárásra került, amely a régi idők „zárt” **rendszereit** részesíti előnyben. Új és tovább gondolásra érett, nem vizsgált kockázatként került megfogalmazásra a különböző, a börtönökben szolgáltatásokat ellátó **külső cégek munkavállalóiban rejlő fenyegetettség**. Szintén szakmai vitára bocsájtható az a megfogalmazott vélemény, amely szerint indokolt egy **olyan szervezeti elem felállítása**, amely a különböző fogvatartottak részére elérhető elektronikus információs rendszerek büntetés-végrehajtási szakmai alapokon nyugvó, de elektronikus információbiztonsági ellenőrzési tevékenységét látja el.

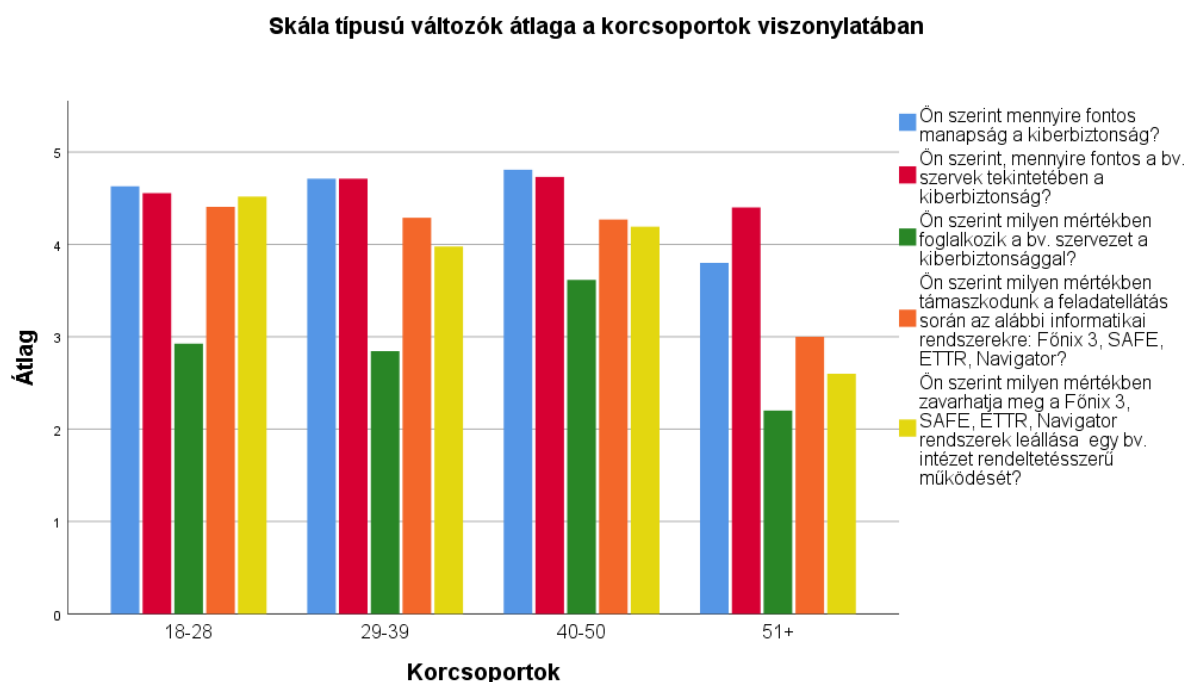
9.5. További elemzések

9.5.1 Összefüggések vizsgálata

A kérdőív azon válaszai esetében, amelyek skála típusú változóként kerültek rögzítésre, **Pearson típusú kétváltozós korrelációvizsgálat** került végrehajtásra. Az elemzés alapján megállapítható, hogy a kérdőívet kitöltő személyek **vélekedése a kiberbiztonság fontosságáról jelentős pozitív irányú szignifikanciát** mutat a soron következő kérdésekben adott válaszokkal. A többi válasz vonatkozásában a bv. szervek kiberbiztonságának fontosságánál a korreláció $r = .68$ $p < 0.01$., a rendszerek alkalmazására való hagyatkozást vizsgáló válaszokban $r = .44$ $p < 0.01$. A kibertámadás zavaró hatását vizsgáló válaszok elemzése esetében $r = .40$ $p < 0.01$. További jelentős, de **nem meglepetést okozó pozitív irányú összefüggés került feltárásra azon kérdéspár esetében, amely a rendszerekre való támaszkodást és azok leállása esetén fellépő zavaró hatások** mértékét mérte, itt az összefüggés mértéke $r = .68$ $p < 0.01$., amely értékek alapján itt is bizonyítható az az általános igazság, miszerint az informatikai rendszerek munkavégzésre való alkalmazásának mértéke egyenesen arányos a leállásuk okozta zavaró hatások mértékével.

9.5.2 Generációs különbségek megjelenése a vizsgálatban

Az interjúk alkalmával zajló beszélgetések során több esetben jelent meg egyfajta befolyásoló tényezőként az informatikai rendszerek használatának témájában a személyi állomány generációs különbségei. Például, hogy a **fiatalabb felügyelők szolgálati feladatuk ellátása során jobban függenek a vizsgált rendszerektől, míg az idősebbek kevésbé**. Az egyik interjúválaszban az is rögzítésre került, hogy a felügyelet idősebb tagjai még örülnek is neki, ha leállnak a rendszerek, mert újra elővehetik a már megszokott papír alapú naplózásokat. A fiatalabb generációk problémájával összefüggésben egyik vezető válaszában egy esettel példálózott, amely szerint egy nemrégiben felvett 18 év körüli munkavállalónak problémája akadt a nyomógombos mobiltelefon kezelésével, mert csak érintő képernyővel ellátott készülék-használatban volt eddig gyakorlata. Nyilvánvaló tény, hogy az idősebb generációk általánosságban nehezebben boldogulnak az informatikával, kevésbé érzik szükségesnek azt. Ez az általánosság a dolgozat által górcső alá vett környezetben is vizsgálható. Ennek bizonyítására a skálázható válaszok értékeinek átlaga került vizsgálatra a korcsoportok viszonylatában. Ennek során megállapítható, hogy **az idősebb korosztály (51 év felett) átlagban kevésbé gondolja fontosnak a kiberbiztonságot, valamint átlag alá helyezték a szervezeti kiberbiztonsági politikát. Az átlagnál alacsonyabbnak gondolják a vizsgált rendszerek alkalmazásának szintjét és annak zavaró mértékét egy bv. intézetre nézve**.



Érdekes eredmény, hogy **a fiatalabb korosztályba tartozó személyek válaszaikban nem produkáltak az idősebbekhez viszonyított aszimmetriás értékeket, inkább a 40-50 év közötti korosztály átlag feletti értékelései kompenzálták a legidősebb korosztály alulértékelését.**

9.5.3 Megengedett leállás

A feltett kérdésekben több esetben megjelent egy nem várt tényező, amely utólag értékelve – ha előzetesen beépítés kerül – fontos vizsgálati elemként is szolgálhatott volna a kutatásnak. Ez a tényező nem más, mint a vizsgált **informatikai rendszerek leállításának időtartalma**. Több válaszadó bontotta fel válaszát két részre, miszerint eltérő a véleményük, ha a leállás „*rövid*” (kb. 1-3 óra), vagy „*hosszabb*” (minimum több nap) időtartamú. A válaszokból megállapítható, **hogy a rendelkezésre állás szünetelésének időtartalma befolyásolja az okozott károk mértékét. A rövid időtartalmú (1-3 óra) leállás esetén fellépő nehézségeket képesek áthidalni a dolgozók, mert több esetben volt ilyen időtartalmú informatikai leállásban részük, így a nehézségek áthidalására már megvannak a gyakorlataik. A hosszabb időtartalom során jelölték meg a kockázatok megjelenését, azonban az is feltárásra került, hogy körülbelül 3-7 nap után képesek lennének visszatérni a teljes a papír alapú munkavégzésre.** Az így kapott intervallumból megállapítható, hogy **a fogvatartotti alapnyilvántartás esetében a megengedett leállás mértéke megközelítőleg 3 óra lehet.** Az ezt követő időszakban a fellépő kockázatok már károkat okozhatnak.

10. JAVASLATOK

A hierarchikus rendszerek és az innováció kapcsolatára kitűnő szemléltetés Niall Ferguson „*Torony és tér*” modellje. Ebben az értelmezésben a torony a hierarchiát képviselő csoportosulás, jelen esetben a büntetés-végrehajtási szervezet, míg a tornyot körülvevő tér a kreatív és ötleteket gyártó társadalmat és az innovációt képviseli. A torony és a tér alapvetően ellentétei egymásnak, ugyanakkor nem tudnak létezni egymás nélkül. A torony alá-fölé rendeltsége biztosítja a stabilitás és védelmezi a teret, de ugyanakkor nehezen integrálhatóak közé az új ötletek, a hierarchia elnyomja azokat, hiszen akár romba is döntheti a gyakorlatias végrehajtást segítő modellt. Azonban, ha a torony egy külső hatástól vagy kihívástól megrendül, akkor egyfajta szerveződésként „kibújik” és a tértől kér segítséget innováció formájában, majd az újító hatással tér vissza.¹⁴²

A büntetés-végrehajtási szervezet informatikai fejlesztéseit egyértelműen ilyen kibújásként azonosíthatjuk, hiszen megjelent a belső modellben az igény az újításra, majd a fentebb taglalt elmélet szerint végbe is ment. Azonban a kiberbiztonsági megrendülést még nem tapasztalt a szervezet. A témában a várt megrendülést jobb esetben a vezetők felismerése hozhatja el, rosszabb esetben a szervezetet érintő kibertámadás, vagy elektronikus információbiztonságot érintő incidens lehet a kiváltó ok. Mindkét **esetre egy megoldás adott, egy szakmai alapokon nyugvó kiberbiztonsági politika.** A bőrtönök informatikai rendszerei megállíthatatlanul fejlődnek, folyamatos a térnyerés, így a kockázatok kezelésére az alábbi javaslatok fogalmazhatóak meg.

Szabványosítás

A kutatás bizonyította, hogy a szervezet bv. szerveiben a feladatellátás alapvetésévé váltak az adatok és információk. Jelentős kockázatot jelent végrehajtásra az, ha zavar keletkezik az elektronikus információs rendszerek sértetlenségében, bizalmasságában, rendelkezésre állásában. A kockázatok kezelésére, menedzsmentjére hatékony megoldás az **ISO/IEC 27000** szabványcsalád szerinti releváns tanúsítások, legfőképpen az Információbiztonsági Irányítási Rendszer (IBIR) alkalmazása. A szabványcsalád alkalmazásának igényét támasztja alá, hogy Prisznyák (2014) is alkalmazta már a bv. szervezet informatikai központjának

¹⁴² Kozma Tamás (2022): Innováció és tanulás. Gondolat Kiadó, Budapest. p. 25-26. Online: <https://mek.oszk.hu/23100/23194/23194.pdf>

kockázatelemzése során.¹⁴³ A kívánt állapot eléréséhez hatékonyan hozzájárulhat még az **ISO 22301** üzletmenet-folytonossági irányítási rendszer szabvány szerinti tanúsítás, amelyet már Böszörményi-Halász (2022)¹⁴⁴ is javasolt a bv. szervezet részére.

Törzsfoglalkozás

Az bv. szervek éves törzsfoglalkozására¹⁴⁵ kibertámadás témájú tematika kidolgozása. A kutatási eredmények alapján valószínűsíthető, hogy egy kibertámadás képes lehet a büntetés-végrehajtás rendjét sérteni, így alapját szolgáltathatja az éves törzsfoglalkozásoknak.¹⁴⁶ Egy összeállított tematikájú esemény gyakorlatozása felkészítheti a személyi állományú tagokat azokra a helyzetekre, amelyekre egy valós helyzetben számíthatnak. Tesztelhetik saját tudásukat és képességeiket egy olyan modellezett rendkívüli esemény során, amely összefüggésben van az eseményt megelőző kibertámadással.

Személyi állomány tudatosítása

Szinte minden információbiztonsági incidensben megtaláljuk a humán tényező szerepét, így a személyi állomány tudatosítása a témában, képzések és oktatások tartása kiemelt feladat. A „sablon” jellegű információbiztonsági képzési és oktatási formák bizonyosan hozzájárulnak a tudatosítás sikerességéhez, azonban hatékonyabbá válthat, ha bv. szervezetre vonatkozó specifikumokkal látjuk el ezeket a képzéseket, hogy a részt vevők érdekelté váljanak benne (pl: a közösségi platformok „büntetés-végrehajtási” tudatos használata, miszerint a fogvatartottak okozta kockázatok csökkentése a megfelelő biztonsági javaslatok alkalmazásával).

Ajánlatos az idősebb generáció képviselőinek az új technológiák megismerésére, azokhoz való alkalmazkodást elősegítő képzéseket szervezni, ugyanakkor ezzel párhuzamosan a teljes személyi állomány részére a meglévő információbiztonsági, kiberbiztonsági képzések számát növelni, **azoknak speciális, büntetés-végrehajtási jellegű adni**. Fontos figyelembe vennünk azt a tényezőt, hogy az alapvető feladat végrehajtás informatikai függőségének mértéke

¹⁴³ Prisznyák Szabolcs (2014): A BvOP Informatikai központjának kockázatelemzése, Hadmérnök, IX. Évfolyam 1. szám. p. 231-239.

¹⁴⁴ Böszörményi-Halász Bence (2022): Az elektronikus információbiztonság alapvetései, valamint a büntetés-végrehajtási szervezet információbiztonsági tudatosságának fejlesztési lehetőségei, Börtönügyi Szemle 2022/1. BvOP, Budapest. p. 122.

¹⁴⁵ A törzsfoglalkozás végrehajtása a büntetés-végrehajtás rendjét, biztonságát súlyosan sértő vagy veszélyeztető cselekmények, események, rendkívüli események, katasztrófhelyzetek megelőzése, felszámolása érdekében végrehajtandó intézkedések gyakorlását biztosítja annak érdekében, hogy a bv. szerv felkészültsége magas színvonalú, összehangolt és begyakorolt legyen.

¹⁴⁶ 21/2022. (IX. 14.) BVOP utasítás a törzsfoglalkozás végrehajtásáról 3. pont

nővekedhet a személyzet generációváltása következtében. A jövő börtönőrei, akik már az informatikai eszközök korszakában nőnek fel, **kevésbé lesznek jártasak a hagyományos gyakorlatokban**, ami jelentős kihívásokat jelenthet a jövőbeli kiberincidens káros hatásainak csökkentése terén. Ajánlatos lehet, hogy a személyi állományi tagok következő generációi ne távolodjanak el a hagyományos, technológia nélküli gyakorlatok ismeretétől.

Önálló szervezeti elem létrehozása

Jelenleg a bv. szervezet a lbtv. szerinti elektronikus információ biztonsági felelősi feladatait egy fő (kiberbiztos) látja el. A szervezeti specifikumok (informatikai függés, fogvatartotti kockázatok) miatt indokolt lehet egy önálló, vezetői közvetlen szervezeti elem (pl: kiberbiztonsági osztály) létrehozása. Az itt szolgálatot teljesítő személyek alapfeladatként bv. kiberbiztonsági politikát alkotnak, részt vesznek a fejlesztésekben és a szabályozások alkotásában, ellátják a személyi állomány képzését, az elektronikus információ biztonsági felelősség gyakorlását, a speciális eszközök bv. kiberbiztonsági tesztelését, valamint a szervezetben jelentkező kockázatok elemzését és kezelését. Adott esetben social engineering technikát alkalmaznak a személyi állományi tagok tesztelésére, valamint ellenőrizhetik az adatbetekintéseket a jogosultságok és adekvátság viszonylatában.

11. ÖSSZEFOGLALÁS

Manapság a kiberbiztonság már fontosabb tényező az életünkben, mint azt elsőre gondolnánk. Természetesen legtöbbünk elismeri és hangoztatja jelentőségét, de főként azok ismerik a súlyát, akik már érintettek voltak kiberincidensekben. Az államigazgatás valamennyi szereplőjének ajánlatos figyelembe venni és vizsgálni az általa használt kibertér hangsúlyosságát, mivel számos fenyegetéssel szemben kell a kockázatkezelést gyakorolni. A magyar államba vetett „kiberbizalmat” minden szervnek kötelessége védelmezni, ez alól a büntetés-végrehajtási szervezet sem kivétel. A digitalizáció a börtönben is átalakítja a folyamatokat, sőt megkerülhetetlen a digitális eszközök és a fogvatartottak egyre nagyobb fokú kapcsolata. Sajnos a modernizációnak köszönhetően a börtönök biztonsága már a kibertéren keresztül is befolyásolható, erre több külföldi eset szolgál például. A magyar bv. szervezet is számos fenyegetettséggel néz szembe, azonban a külföldi példákhoz hasonló eseményt nem találunk a hazai börtönök történetiségében. A dolgozatban bemutatott kutatás eredményei alapján kijelenthetjük, hogy a kockázat itthon is jelen van. Megállapításra került az is, hogy egy kibertámadás képes komoly zavarokat okozni börtöneinkben. Az intézetek legfőbb informatikai szakrendszere, az elektronikus fogvatartotti nyilvántartás bizalmasságának, rendelkezésre állásának és sértetlenségének fenntartása nélkülözhetetlen. E jellemzők sérülése esetén akár a fogvatartott személyek alapjogi érintettségének eshetőségével is számolni kell, amely akár kártalanítási eljárások alapjául is szolgálhat. Fontos szem előtt tartanunk azt a feltárt tényezőt, hogy a börtönök személyi állományának generációváltása hátrányokkal is jár, hiszen a jövő börtönőrei nem fogják ismerni a régi gyakorlatokat, így az informatika és a feladat-végrehajtás közötti interdependencia mértéke nőni fog. A jövő vitán felül nagyobb „kiberfigyelmet” vár el a szervezettől, így valószínűleg a kiberbiztonság hamarosan önálló, szakmai szükségleten alapuló státuszt fog kiérdemelni magának.

12. IRODALOMJEGYZÉK

Monográfiák:

Czenczer és Sztodola (2020): A biztonsági tiszt munkája jogi és szakmai vonatkozásai, in Közbiztonság, Ludovika Egyetemi Kiadó, Budapest <http://hdl.handle.net/20.500.12944/16197>

Czenczer Orsolya és Pallo, József (2014) A büntetés-végrehajtási szervezet felsőszintű irányításának és vezetésének elvei, specifikumai. In: A rendészeti szervek vezetés- és szervezésmélete. Nemzeti Közszerológati Egyetem Rendészettudományi Kar, Budapest. Online: <http://real.mtak.hu/106851/>

Horváth Mirtill Katalin (2022): Innovatív informatikai megoldások a büntetés-végrehajtásban, avagy a Főnix rendszer bűnügyi nyilvántartási modulja c. TDK dolgozat, Nemzeti Közszerológati Egyetem Rendészettudományi Kar, Büntetés-végrehajtási Tanszék.

Kovács László (2018): A kibertér védelme, Dialóg Campus Kiadó, Budapest. Online: <http://hdl.handle.net/20.500.12944/12603>

Muha Lajos – Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése, Nemzeti Közszerológati Egyetem, Budapest. Online: <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/7135/Az%20elektronikus%20inform%C3%A1ci%C3%B3s%20rendszerek%20biztons%C3%A1g%C3%A1nak%20menedzsel%C3%A9sej%C3%B3.pdf?sequence=5&isAllowed=y>

Paul W. King (2009): Climbing Maslow's Pyramid, Matador, Leicester. ISBN: 9781 8487 61124 Online: https://books.google.hu/books?id=bDJNJ53dFzC&printsec=frontcover&hl=hu&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Prisznay Szabolcs (2020): A rendvédelmi informatikai egyes szervezési és oktatási kérdései c. Doktori (PhD) értekezés, Óbudai Egyetem, Biztonságtudományi Doktori Iskola. Online: http://lib.uni-obuda.hu/sites/lib.uni-obuda.hu/files/Prisznay_Szabolcs_ertekezes.pdf

Norbert Wiener (1948): Cybernetics, or Communication and Control in the Animal and the Machine, MIT Press, Cambridge.

Folyóiratcikkek:

Bogotyán Róbert – Veszeli Dániel (2011): Bűnügyi nyilvántartás a büntetés-végrehajtásban: a múlt örökségének és a jelen kihívásainak hatása a közeljövő terveire. Börtönügyi Szemle 2011/3.sz. BvOP, Budapest.

Böszörményi-Halász Bence (2022): Az elektronikus információbiztonság alapvetései, valamint a büntetés-végrehajtási szervezet információbiztonsági tudatosságának fejlesztési lehetőségei, Börtönügyi Szemle 2022/1. BvOP, Budapest.

Hinkel Tamás (2020): A mesterséges intelligencia térhódítása a büntetés-végrehajtásban, Börtönügyi Szemle 2020/4., BvOP, Budapest.

Juhász Zsuzsanna (2018): A büntetés-végrehajtás alapelvei. Magyar Rendészet 2018/5. Budapest.

Kondás Katalin és Szűcs Endre (2017): Informatikai korszakváltás egy büntetés-végrehajtási intézetben, Hadmérnök, XII. Évfolyam 2. szám.

Kozma Tamás (2022): Innováció és tanulás, Gondolat Kiadó, Budapest. Online: <https://mek.oszk.hu/23100/23194/23194.pdf>

Prisznyák Szabolcs (2014): A BvOP Informatikai központjának kockázatelemzése, Hadmérnök, IX. Évfolyam 1. szám. p. 231-239

Soós Géza (2006): Az informatika szerepe a Büntetés-végrehajtási Szervezet fejlesztésében, Börtönügyi Szemle 2006/1. sz. BvOP, Budapest.

Veszeli Dániel János (2017): A rendvédelmi szervek közötti automatizált információ megosztás és elérés, Belügyi Szemle, Budapest 2017/11-12.

Jogszabályok:

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

1995. évi CVII. törvény a büntetés-végrehajtási szervezetről.

2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról.

2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról.

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

2017. évi XC. törvény a büntetőeljárásról.

21/1997. IM rendelet a büntetés-végrehajtási szervezet Szolgálati Szabályzatáról.

21/2022. (IX. 14.) BVOP utasítás a törzsfoglalkozás végrehajtásáról.

346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról.

6/2023. (I. 31.) BVOP utasítás a Büntetés-végrehajtás Országos Parancsnoksága Szervezeti és Működési Szabályzatáról.

Emberi Jogok Egyetemes Nyilatkozata.

Európai Börtönszabályok - A Miniszteri Bizottság Európai Börtönszabályokról szóló R/2006/2 ajánlása a Tagállamok számára.

Magyarország Alaptörvénye.

Belső szabályozók:

Egyéb kiadványok:

A magyar nyelv értelmező szótára, első kiadás: 1959–1962, Akadémiai Kiadó, Online: <https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-a-magyar-nyelv-ertelmezo-szotara-1BE8B/> Utolsó letöltés: 2022.12.29.

Defendant's Notice Of Emergency Pursuant To Paragraph 14 Of The Settlement Agreement In The United States District Court for the district of New Mexico, 2022. Online: <https://www.documentcloud.org/documents/21176926-bernalillo-county-notice-of-emergency> Utolsó letöltés: 2022.12.20

Muha Lajos: Kiberhadviselés – kiberbűnözés, In: IDC IT Security Konferencia, Budapest, 2012.03.22.

Open AI Chat GPT mesterséges intelligenciával történő angol nyelvű lekérdezés. Online: <https://openai.com/blog/chatgpt/> Alkalmazva: 2022.12.29.

Rendészeti Alap – és Szakvizsga Bizottság (2022): Rendészeti Szakvizsga Tananyag – Büntetés-végrehajtási Igazgatás. Online: http://bmkszf.hu/dokumentum/3411/buntetesvegrahajitasi_tananyag.pdf

Tuba Kovács Béla (2019): Büntetés-végrehajtási informatikai ismeretek tananyag, Büntetés-végrehajtási Szervezet Oktatási, Továbbképzési és Rehabilitációs Központja, Budapest. p. 22.

Internetes hivatkozások:

European Union Agency for Cybersecurity (2022): Enisa Threat Landscape 2022 Online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

<http://www.skpont.hu/index.php/tobias/> Utolsó letöltés: 2023.01.13.

<https://bv.gov.hu/hu/ekop> Utolsó letöltés: 2023. 01.13.

<https://bv.gov.hu/hu/intezetek/bvszervezet/hirek/4184> Utolsó letöltés: 2023.03.09.

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_hu Utolsó letöltés: 2022.12.25.
<https://cdn.kormany.hu/uploads/document/6/60/602/60242669c9f12756a2b104f8295b866a8bb8f684.pdf> Utolsó letöltés: 2022.12.25.

https://mobilarena.hu/teszt/turbosim/mi_is_ez.html Utolsó letöltés 2023.01.04.

<https://nki.gov.hu/it-biztonsag/tanacsok/igy-ellenorizhetjuk-hogy-az-internet-szolgaltatonk-ved-e-minket-a-bgp-elteriteses-tamadasok-ellen/> Utolsó letöltés. 2023.01.17.

<https://old.iranintl.com/en/iran/hackers-release-security-footage-iran%E2%80%99s-evin-prison> Utolsó letöltés: 2022.12.21.

<https://slideplayer.hu/slide/1953374/> Utolsó letöltés: 2022.12.25.

<https://sourcenm.com/2022/01/07/jails-inability-to-deal-with-cyberattack-could-violate-the-constitutional-rights-of-inmates/> Utolsó letöltés: 2022.12.20.

<https://statescoop.com/bernalillo-county-cybersecurity-policy-ransomware/> Utolsó letöltés: 2022.12.20.

<https://therecord.media/cyber-attack-disrupts-irans-national-railway-system/> Utolsó letöltés: 2022.12.21.

<https://therecord.media/hacktivists-leak-videos-of-abuse-in-iran-evin-prison/> Utolsó letöltés: 2022.12.21.

<https://twitter.com/IranIntl/status/1429524913828900866?s=20> Utolsó letöltés: 2022.12.21.

<https://www.bernco.gov/blog/2022/01/10/alvarado-square-open-on-lobby-level-only/> Utolsó letöltés: 2022.12.20.

<https://www.bernco.gov/metropolitan-detention-center/frequently-asked-questions/> Utolsó letöltés: 2022.12.20.

<https://www.cyansecurity.com/half-year-review-of-significant-cyberattacks-bernalillo-county/> Utolsó letöltés: 2022.12.20.

<https://www.dtf.vic.gov.au/partnerships-victoria-ppp-projects/port-phillip-prison-contract-extension-project> Utolsó letöltés: 2022.12.20.

<https://www.dw.com/en/irans-evin-prison-experience-was-psychological-torture-says-former-prisoner/a-63509722> Utolsó letöltés: 2022.12.21.

<https://www.easytechjunkie.com/what-is-a-kiosk-terminal.htm> Utolsó letöltés: 2023.01.12.

<https://www.g4s.com/en-au/what-we-do/justice-services/custodial> Utolsó letöltés: 2022.12.20.

https://www.heinzsoft-shop.de/images/product_images/info_images/vesa_mouting_kit_1.jpg Utolsó letöltés: 2022.12.24.

<https://www.iran-emrooz.net/index.php/news2/more/93050/> Utolsó letöltés: 2022.12.21.

<https://www.jogiforum.hu/cikk/2018/11/26/illegalis-bortontelefon-csalasra-hasznaljak-a-bortonoket-ellepo-mobilokat/> Utolsó letöltés: 2023.01.04.

<https://www.jogiforum.hu/hir/2018/09/03/a-budapesti-fegyhazi-es-bortonbol-kovettek-le-rabok-unokazos-csalast-zarkajukbol-bonyolitottak-a-telefonhivasokat-a-sertettek-szama-35/> Utolsó letöltés: 2023.01.04.

<https://www.jpay.com/education.aspx> Utolsó letöltés: 2022.12.24.

<https://www.msn.com/en-au/news/australia/port-phillip-prison-melbourne-jail-targeted-by-anonymous-hackers-in-cyber-attack/ar-AAZj25T> Utolsó letöltés: 2022.12.20.

<https://www.theguardian.com/australia-news/2022/oct/05/staff-at-security-firm-g4s-on-alert-after-tax-numbers-and-bank-details-posted-online-following-hack> Utolsó letöltés: 2022.12.20

<https://www.zdnet.com/article/iran-reports-failed-cyber-attack-on-strait-of-hormuz-port/>
Utolsó letöltés: 2022.12.21.

13. MELLÉKLETEK

1. sz. melléklet

Kutatási kérdőív

Tisztelt Kitöltő!

Kedves Kolléga!

A *"Bástyafalak kiberbiztonsága, avagy a büntetés-végrehajtás digitális kultúrájának kiberérintettsége"* című kutatásban szeretném a segítségét kérni. A kutatás témája a hazai büntetés-végrehajtási szervezet végrehajtási közegében igyekszik felfedni azt, hogy manapság mennyire függünk munkavégzésünk során a szakmai informatikai rendszerektől, továbbá, hogy egy börtönt ért kibertámadás milyen hatásokkal járhat. Az elmúlt években nagymértékben megnőtt az állami szervek ellen intézett kibertámadások száma, továbbá kiberincidens több ország (*USA, Ausztrália, Irán*) börtönei esetében okozott komoly zavarokat a rendeltetésszerű működésében. A magyar bv. szervezet az elmúlt időszakban számos informatikai fejlesztést hajtott végre, ezért kiemelten fontos, hogy vizsgáljuk az új fenyegetések sorát.

A kérdőív anonim, kitöltés ideje kb. 3-4 perc.

Kérem, legyen a segítségemre!

Válaszaival nagymértékben hozzájárul a kutatás eredményességéhez.

Segítő együttműködését ezúton köszönöm!

Tisztelettel:

Bottyán Sándor

*Kötelező

Demográfiai kérdések

1. Az Ön neme? *

Soronként csak egy oválist jelöljön be.

☐ Férfi

☐ Nő

2. Az Ön kora? *

Soronként csak egy oválist jelöljön be.

- ☐ 18-28
- ☐ 29-39
- ☐ 40-50
- ☐ 51+

3. Hány év szolgálati idővel rendelkezik a bv. szervezetnél? *

Soronként csak egy oválist jelöljön be.

- ☐ 0 - 5 év
- ☐ 5 - 10 év
- ☐ 10 - 15 év
- ☐ 15 - 20 év
- ☐ 21 + év

4. Az Ön szolgálati helye: *

(nappali munkarendes hallgatók esetében a volt szolg. hely)

Soronként csak egy oválist jelöljön be.

- ☐ Agglomerációs Központ
- ☐ Egy objektumos bv. intézet
- ☐ Több objektumos bv. intézet
- ☐ Intézmény (IMEI, BVKK)

5. Milyen beosztáscsoportban teljesít szolgálatot?*

(nappali munkarendes hallgatók esetében az utolsó beosztás)

Soronként csak egy oválist jelöljön be.

- ☐ Végrehajtó
- ☐ Középvezető
- ☐ Vezető

6. Melyik szakterületen teljesít szolgálatot? *

(nappali munkarendes hallgatók esetében a volt szakterület)

Soronként csak egy oválist jelöljön be.

- ☐ Agglomerációs Osztály
- ☐ Biztonsági Osztály
- ☐ Egészségügyi Osztály
- ☐ Ellenőrzési Osztály
- ☐ Fogvatartási ügyek Osztálya
- ☐ Informatikai Osztály
- ☐ Közgazdasági Osztály
- ☐ Műszaki és Ellátási Osztály
- ☐ Műveleti Osztály
- ☐ Nyilvántartási Osztály
- ☐ Pártfogó felügyelet
- ☐ Pszichológiai Osztály
- ☐ Személyügyi és Szociális
- ☐ OsztályTitkársági Osztály
- ☐ Vezetői Közvetlen
- ☐ Vezetői Törzs Egyéb
- ☐ BvOP

Kiberbiztonsági témájú kérdések

7. Ön szerint mennyire fontos manapság a kiberbiztonság? *

(Állítsa be a skálán a gondolt mértékben)

Soronként csak egy oválist jelöljön be.

Nem fontos

☐ ☐ ☐ ☐ ☐

Kiemelten fontos

8. Ön szerint, mennyire fontos a bv. szervek tekintetében a kiberbiztonság? *

(Állítsa be a skálán a gondolt mértékben)

Soronként csak egy oválist jelöljön be.

Nem fontos

☐ ☐ ☐ ☐ ☐

Kiemelten fontos

9. Ön szerint számítani lehet egy börtönt érintő kibertámadásra? *

Soronként csak egy oválist jelöljön be.

☐ Igen

☐ Nem

☐ Talán

☐ Nem tudom

10. Ön szerint milyen mértékben foglalkozik a bv. szervezet a kiberbiztonsággal? *

(Állítsa be a skálán a gondolt mértékben)

Soronként csak egy oválist jelöljön be.

Csekély

☐☐☐☐☐

Megfelelő

Az alábbi kérdések az Ön munkavégzése során alkalmazott **elektronikus fogvatartotti alapnyilvántartással (Főnix 3)** és az azzal összefüggő informatikai rendszerekkel összefüggésben kerültek megfogalmazásra.

11. Ön szerint manapság a büntetés-végrehajtási feladatok jogszerű ellátásához nélkülözhetetlen a Főnix 3, SAFE, ETTR, Navigator informatikai rendszerek alkalmazása? *

Soronként csak egy oválist jelöljön be.

☐

Igen

☐

Nem

☐

Talán

☐

Nem tudom

12. Ön szerint milyen mértékben támaszkodunk a feladatellátás során az alábbi informatikai rendszerekre: Főnix 3, SAFE, ETTR, Navigator? *

(Állítsa be a skálán a gondolt mértékben)

Soronként csak egy oválist jelöljön be.

Csekély

☐☐☐☐☐

Jelentős

13. Ön szerint milyen mértékben zavarhatja meg a *Főnix 3*, *SAFE*, *ETTR*, *Navigator* rendszerek leállása egy bv. intézet rendeltetésszerű működését? *

(Állítsa be a skálán a gondolt mértékben)

Soranként csak egy oválist jelöljön be.

Csekély

☐☐☐☐☐

Jelentős

14. Ön szerint a *Főnix 3*, *SAFE*, *ETTR*, *Navigator* rendszerek elérhetetlensége okozhat rendkívüli eseményt? *

Soranként csak egy oválist jelöljön be.

☐

Igen

☐

Nem

☐

Talán

☐

Nem tudom

15. Ön szerint a *Főnix 3* rendszer elérhetlensége akadályozhatja a fogvatartottak kapcsolattartási formáinak megvalósulását? *

Soranként csak egy oválist jelöljön be.

☐

Igen

☐

Nem

☐

Talán

☐

Nem tudom

Ezt a tartalmat nem a Google hozta létre, és nem is hagyta azt jóvá.

Google Úrlapok

2. sz. melléklet

	1. sz. interjú alany	2. sz. interjú alany	3. sz. interjú alany	4. sz. interjú alany	5. sz. interjú alany	6. sz. interjú alany	7. sz. interjú alany
Ön szerint mennyire fontos manapság a kiberbiztonság?	<u>Fontos, elengedhetetlenül fontos. Magas prioritású.</u>	<u>Egyre fontosabb.</u> Ha abból indulok ki, hogy az én telefonomon is jelszavak, bankkártya adatok vannak, így elég fontos.	<u>Lehető legfontosabb</u> manapság. A gyermekek is rengeteg időt töltenek online.	A XXI. században vagyunk, minden digitális színté. <u>1-5 közötti skálán 4-es.</u> Technikai fejlődés begyűrűzik a hétköznapiakba, sok területet megkönnyít, de a veszélyei is megvannak.	<u>Elsődleges fontosságú.</u> nagyon e felé megy a világ. Már a céges e-maileket otthonról is meg tudom tekinteni, így ezt is egy jelentős kockázatnak gondolom.	<u>Nagyon fontos.</u> Ahogy fejlődik a technológia, egyre több személyes adatunk kerül digitalizálásra, felkerülnek felhőkhöz például. Régebben nem volt EESZT, Webkincstár stb., papíralapon volt minden. Manapság ezeket meg kell védenünk a kibertérben.	<u>Rendkívül fontos.</u> A híradásokból is ez folyik mostanában. Manapság már egy teljes életet tönkre lehet tenni ezzel, értem ez alatt az kiberpénzügyi bűncselekményeket.
Ön szerint, mennyire fontos a bv. szervek tekintetében a kiberbiztonság?	<u>Ugyanaz az álláspontom,</u> mint az előző kérdésnél. Itt annyival másabb, hogy személyi állományi tagok, vagy fogvatartottak személyiségi jogai érintetté válhatnak. Manapság mindent informatikai rendszerek alkalmazásával hajtunk végre, előállításokat is, de még a fogvatartotti élelmezést is.	Nyilván <u>fontos</u> itt is. Abban biztos vagyok, ha az intézettel történne kiberincidens, lennének problémák.	<u>Nagyon fontos.</u> Az elektronikusan tárolt információk kijutásának megakadályozása fontos feladat.	Megmaradok <u>itt is a 4-es értékelésnél.</u> Erősítik itt is a digitalizációt, mesterséges intelligenciáról is szó van már, elektronikus naplót vezetünk, indokolt, hogy foglalkozzunk a kiberbiztonsággal is.	<u>Eléggé az.</u> Manapság már a fogvatartottak adatai, sőt a mi adataink is fent vannak a rendszerekben. Vannak papíralapú akták, de már minden digitalizálva van. Sőt a biztonságtechnikai rendszer, amikor külső szakemberek jönnek be a szolgáltatótól, ez is komoly kockázatot jelent szerintem.	Ugyanúgy <u>nagyon fontos.</u> Visszakanyarodva a társadalomhoz, ott is, itt is egyre több alkalmazás van, egyre több adat van szervereken. Azt gondolom, a biztonságna ezel arányban kellene lennie.	Itt még inkább <u>fontosabb.</u> A személyiségi jogok tekintetében, a fogvatartás biztonsága szempontjából is rendkívül fontos. Ha az elektronikus nyilvántartáshoz, a kamerafelvételekhez ha hozzájutnak, ott bármit csinálhatnak. Támadáshoz, túszejtéshez, szabadításához felhasználhatják ezt a hozzáférést.

Ön szerint számítani kell egy börtönt érintő kibertámadásra?	<u>Bármikor megtörténhet.</u> Annyira globalizáltak vagyunk, hogy magánemberként is rengeteg adathalász e-mailt kapunk naponta. Az ilyen jellegű veszélyeknek a szervezet is erősen ki van téve.	Szerintem Magyarországon ennek <i>kicsi az esélye</i>. Inkább arra látok esélyt, hogy bizonyos fogvatartottak esetében olyan adatokat tartunk nyilván, ami ellen intézhetnek támadást.	Szerintem igen. Elég <u>nagy mértékűnek</u> gondolom ezt a kockázatot.	10 éven belül <u>erre számítani kell.</u> Nyilvánvalóan a médiában nem jelennek meg a kormányzati, állami szerveket ért kibertámadások, de ez elkerülhetetlen.	<u>Azt hiszem igen.</u> Eléggé komollyá vált a fogvatartotti populáció, komoly bűncselekményekkel kerülnek be, milliárdok lehetnek a háttérben. A fenyegetés komolyodik, és ez a kibertérre is érvényes. A ftt. adataihoz való hozzáférésből egyaránt előnyt is szerezhetnek a fogvatartottak, és ugyanakkor veszélyes is lehet. Értem ez alatt, hogy megismerik a hozzátartozók, kapcsolattartók adatait, megismerik hova és mikor fogjuk előállítani a fogvatartottat, fel tudnak készülni bármilyen támadásra is akár	<i><u>Rövid távon azt gondolom nem.</u></i> Ha hackerek támadják hazánkat, nem a büntetés-végrehajtás lesz az első célpontjuk. Ugyanakkor rajta vagyunk a kormányzati hálózaton, azon keresztül bennünket is érhet támadás bármikor.	<u>Nem tartom kizártnak.</u> Szerintem vannak már ilyesmire specializálódott emberek, akikről még nincs tudomásunk.
Ön szerint milyen mértékben foglalkozik a bv. szervezet a kiberbiztonsággal?	Olyan <u>középtértékben.</u> Kapunk értesítéseket a veszélyes e-mailekről, látszik, hogy van ilyen tevékenység.	Szerintem <u>középtértékben.</u> Azért annyi, mert nem igazán látok bele, de azt sem tudom mondani, hogy nagyon jól. Azt gondolom, hogy a napi szolgálatellátáshoz, a biztonságos fogvatartás biztosításához megfelelő. Biztos, hogy lehetne jobb, de rosszabb is.	<u>1-5 közötti skálán</u> <u>hármasnak</u> mondanám. Ezt azzal indoklom, hogy szinte állandóan fejlesztjük a technikát, hogy nehezebb legyen a bejutás.	<i><u>1-5 közötti skálán 1,5.</u></i> Lehet ettől több, de hozzánk nem igazán jut el. Amilyen technikai eszközöket használunk, azt gondolom az informatikai háttérünk nem mondható fejlettnak, ebben van némi kockázat azért.	<u>Nem tudom.</u> Én annyit tapasztaltam, hogy párszor kaptam egy e-mailt, hogy ne nyissak meg bizonyos e-maileket, mert veszélyesek. Azt gondolom, hogy az informatikai eszközeink terén nagyon szükség lenne újírtásra, ez is hozzá járulna a biztonsághoz.	Erre nehéz válaszolni. <u>Olyan közép-re helyezném el.</u> Vannak kezdeményezések. Pár éve jött ki tájékoztató a zsarolóvírusokról. Folyamatosan látok szervezeti címekre érkezett e-maileket, amelyek egyértelműen adathalász üzenetek, és kiszűrtük őket. Vannak megfelelő megoldásaink, mint a SAFE telefonon a Samsung Knox alkalmazás, vagy ugyebár van IBSZ-ünk. De azt gondolom, a valós veszély kívülről érkezik, nem onnan, hogy oda engedek egy kollégát a számítógépemhez. E mellett azt gondolom, a különböző szolgáltatókra, akik fejlesztenek, vagy üzemeltetnek nekünk, nagyobb kontroll kellene.	Biztosan nem tudom. De egyszer-kétszer szoktunk kapni e-mailt, hogy ha bizonyos tartalmakat kapunk ne nyissuk meg. Ebből azt vonom le, hogy odafigyelnek erre, de hogy ezt milyen mértékben teszik arra nem látok rá. Hozzánk általában ezek a figyelmeztetések hamarabb elérnek, mint a fenyegetés, ezért <i><u>1 és 5 közötti skálán én a maximumot adnám.</u></i>

Ön szerint manapság a büntetés-végrehajtási feladatok jogszerű ellátásához nélkülözhetetlen a Főnix 3, SAFE, ETTR, Navigator informatikai rendszerek alkalmazása?	<u>Nem nélkülözhetetlen.</u> abszolút nem az. Más rendszerrel bármikor helyettesíthetőek. Manapság még mindig ott tartunk, hogy van egy elektronikus iratunk, amit egyébként ki is nyomtatunk és lefűzünk. Az egészségügyi, nyilvántartási, nevelési anyagaink papír alapon is megvannak. Többletfeladattal, de el tudjuk teljesíteni jogszerűséget.	Természetesen. A jogszerű végrehajtáshoz elengedhetetlenek.	<u>Nyilván tudunk lenni jogszerűek nélkülük.</u> de ezekkel a rendszerekkel könnyebben, hatékonyabban tudunk dolgozni. A Főnix 3 azért elég fontos a jogszerűséghez, minden nyilvántartásunk abban van.	Annak tartom. Nem tudjuk, és nem is akarjuk megakadályozni a fejlődést, egyre több feladatunk van, számos szakterület dolgozik ezekből a rendszerekből. Ha ezt a rendszert elveszítenénk, elő tudjuk venni a régi naplókat, de az már lehet kevés lesz a jogszerűséghez.	Vissza lehet térni a papír alapú munkára. Nem vagyunk messze '97-től, amikor még papír alapon ment minden. Régebben is működött ez a dolog. Manapság sok az adat, ezt már papíron nem lehetne vezetni, kellenek a rendszerek. <u>Nem nélkülözhetetlen.</u> volt már, hogy kifagytak a rendszerek, újra elő kellett vennünk a naplókat, és ment minden jogszerűen. A mellékletek a szabályzatokban benne vannak, csak másolunk belőlük és megy minden papíralapon.	SAFE, ETTR <u>nem szükséges.</u> ezek munkateher csökkentő intézkedésre kiadott digitalizációs megoldások. A módszertani útmutatójukba benne van, hogy ha nem működik elő kell venni a naplókat. A Főnix 3 már másabb terület, minden dokumentumot az generál. Ha nem elérhető, kell egy kis idő, amíg át tudunk állni a papír alapra. Rövid távon lehet zavarná a jogszerű feladatellátást, de hosszú távon meg tudnánk oldani. Azt gondolom, minden intézetnél papír alapon megvannak azok az adatok, amelyek kellenek a feladat-végrehajtáshoz. Sokkal körülményesebb lenne, de működhet a dolog.	Ha minden kötél szakadna, <u>meg tudnánk oldani a feladatokat elektronikus nyilvántartási rendszer nélkül is,</u> ideig-óráig. Ha probléma merülne fel, megoldanánk pár óráig, mint ahogy már nélkülöztük is leállások alkalmával. De hosszú távon másabb a helyzet, előre szoktunk dolgozni papír alapú nyilvántartások esetében, de abban már nem vagyok biztos, hogy hibamentes lenne a működés csak ebből hosszabb távon.
Ön szerint milyen mértékben támaszkodunk a feladatellátás során az alábbi informatikai rendszerekre: Főnix 3, SAFE, ETTR, Navigator?	A munkánkban 60 %-ban erre támaszkodunk.	<u>Minden a Főnix 3 rendszeren keresztül megy.</u> A papír alapú dokumentumokat is ez a rendszer generálja le. Az ETTR-rel kapcsolatban vannak még problémák, de teljes mértékben szerepet kap az előállítások során.	A Főnix 3-ra <u>teljes mértékben.</u>	<u>80-85%-ban támaszkodunk,</u> viszont majdnem mindent ki kell nyomtatnunk. Duplikáljuk a feladatokat, elektronikusan és kinyomtatva is vezetjük. Ami néha nem hátrány, mert nem minden személyi állományú tag az újabb generációk tagja, az idősebbek nehezebben boldogulnak az informatikai rendszerek kezelésével.	Mivel megszüntették a papír alapú naplókat, szinte <u>100%-ban ezeket használjuk.</u> Akik jelenleg érkeznek a szervezethez, ők egy új generáció tagjai, egy fél év múlva nem fogják tudni, hogy kell naplózni papíralapon. A rendszer nélkül nem fogják tudni, hogy kell dolgozni, <u>a ráutaltság teljes lesz.</u>	Sajnos <u>nagyon nagy mértékben.</u> Gyakorlatilag, mivel <u>minden adatunk a Főnix 3-ban van,</u> erős függésben vagyunk vele. Ez egyébként attól függ, kit kérdezzük meg. Ha megkérdezel egy idősebb felügyelőt, ő abszolút nincs függőségben az informatikai rendszerekkel, mert a kulcs ugyan úgy az oldalán csörög, ha működik a SAFE, ha nem. Függ a korosztálytól. A fiatalabb felügyelők nyilvánvalóan jobban függenek ettől.	<u>A Főnix 3-ra nyilvántartási szakterület nagyon.</u> Minden adatunk itt van, egy-két kattintással könnyen kinyerjük a szükséges adatokat, így sokat használjuk.

Ön szerint a Főnix 3, SAFE, ETTR, Navigator rendszerek elérhetetlensége okozhat rendkívüli eseményt?	Súlyos RES-t, ami a közbiztonságot veszélyeztetné, <u>ha rövid távú ez a leállás akkor nem.</u> Ha a biztonságtechnikai rendszert érintené, akkor bajban lennénk, mert élő erővel kellene pótolni.	<u>Persze. Biztos, hogy okozhat.</u> A súlyosságot nem egyszerű meghatározni. De, ha érkezik egy 20 fős szállítás és a rendszer elérhetetlen, én nem tudom megmondani kit-ivel helyezhetek el. Ha összeférhetetlen fogvatartottakat helyezek el egy zárkában és verekedés tör ki, az elég komoly rendkívüli esemény.	<u>Szerintem igen.</u> Előállítás elmaradást például. De az egészségügyben is, vagy a fogvatartotti pénzmozgásban, szabadításban, kapcsolattartásban <u>esély van rá.</u>	<i>Súlyos rendkívüli eseményt nem, mert ilyen rendszer leállás esetén, ha jelentős kockázatok lépnek fel, a vezetés inkább ezen kockázatok megszüntetésére intézkedne leginkább.</i> <u>De kisebb súlyú rendkívüli eseményt, mint egy jogtalan fogvatartás igen, okozhat.</u>	A nyilvántartást nem tudom, a biztonságot annyira érintené, hogy nincs aktuális információnk a fogvatartottáról, mert aktuálisat csak <u>ott látunk, így egyértelműen okozhat.</u>	Attól függ milyen rendkívüli eseményt. <u>A szállítást elmaradást például okozhat, de súlyos rendkívüli eseményt nem.</u> Téves szabadítást is okozhat, azt gondolom.	<u>Egyértelműen igen.</u> Napokra történő leállás esetén igen. Egyébként elég nagy százalékban le vagyunk védve egyébként a papír alapú nyilvántartásokkal, de megeshet.
Ön szerint milyen mértékben zavarhatja meg a Főnix 3, SAFE, ETTR, Navigator rendszerek leállása egy bv. intézet rendeltetésszerű működését?	Két részre kellene ezt bontani. <u>0,5-1 napos leállás nem vezetne súlyos RES-hez, de nagyon befolyásolná az intézet működését.</u> Hosszú távon viszont kb. egy hét alatt visszatérnénk azokra a megoldásokra, amikor még nem voltak számítógépek. A SAFE, ETTR rendszerek támogató rendszerek, <u>nélkülük is el tudjuk végezni a feladatokat.</u>	Függ attól, hogy mikor állnak le ezek a rendszerek. Ha ez egy hétköznapra esne, amikor több a végrehajtandó feladat, <u>okozna tanácsstalanságot.</u> Akut feladatokat el tudnánk látni, de a biztonsági kockázatokat egyértelműen növelné.	Szerintem, mondhatni, hogy <u>összeomlana itt minden. Biztos, hogy nagyon nagy mértékben. 90 %-ban.</u> Minden egyes adat, információ a fogvatartottakról ott van fent. Leállás esetén nehéz lenne minden dolognak utána nézni egyéb nyilvántartásokban.	Ez egy <u>1-5 közötti skálán 6-os. Minden téren.</u> Nagyon összetett problémához vezetne, ha ezek a rendszerek leállnának.	A nyilvántartási szakterület nem tudom mennyire van rá utalva, de én azt gondolom <u>olyan 1-5 között skálán 3.</u> Még rendben vagyunk ha leáll a rendszer, meg utána kell dolgozni ha feláll, de simán elmegy a börtön ezek nélkül is, mert olyan kollégák vannak, akik elő tudják venni a naplókat, és tudják kezelni. Ha leáll a rendszer, néhányan még örülnek is neki, hogy visszatérhetnek a hagyományos naplózáshoz, mert nekik ezek a rendszerek még újak, szokatlanok.	A jogszabály azt írja, hogy a bv. a rendeltetésszerű feladatainak végrehajtása során szolgálja a közbiztonság és a közrend fenntartását. Tág értelemben ez azt jelenti, hogy a bíróság által kiszabott szabadságvesztés végrehajtása, ez az alapfeladatunk. Ha ezt nézem, <u>nem zavarja meg, mert a fogvatartottat nem fogjuk kiengedni,</u> mert nem működnek a rendszerek. Nagyobb probléma lenne, ha a biztonságtechnikai rendszer állna le. A Főnix 3 is hangsúlyos egyébként, mert a kollégák nagymértékben alkalmazzák. Leállás esetén tudjuk pótolni, de jelentős többletfeladattal. Abban biztos vagyok, hogy <u>nem lehetetlenítené el.</u>	Attól függ mennyi időre. <u>Ha például 3 óra, ezt megoldjuk könnyedén papír alapon. Ha napokra állna le, ott már komoly gondok lehetne számítani.</u>

Ön szerint a Főnix 3 rendszer elérhetetlensége akadályozhatja a fogvatartottak kapcsolattartási formáinak megvalósulását?	<u>Egyértelműen. Rövid távon egyértelműen, biztosan.</u> Ha ez ma megtörténne, nem tudnánk megmondani, hogy ma kinek van látogatófogadása. <u>Hosszú távon nem, mert visszatérnénk a papír alapú működésre.</u>	<u>Persze. Biztos, hogy akadályozhatja.</u> Akár a rendszer elérhetetlensége esetén megtörténhet egy olyan hozzátartozó látogatásának megtagadása, ami egyébként jogszerű lenne. Látogatófogadás, Skype-beszélő során előfordulhat.	<u>Nagy mértékben.</u> Nem tudnánk ellenőrizni a fogvatartottak kapcsolattartását, a korlátozásokat legfőképpen, az nincs benne a papír alapú nyilvántartásokban. Elérhetetlenség esetén nem tudnánk biztosítani ezeket.	<u>Akadályozhatja.</u> Például látogatófogadás, Skype, távtárgyalás. Egy letartóztatott személy esetében ez még kritikusabban felléphet. Kártalanítási eljárások is felléphetnek az eset bekövetkezésével összefüggésben.	<u>Akadályozhatja mindenképpen,</u> de az gondolom, hogy alternatívan meg tudnánk valósítani a telefonhívásokat is például, körülményesen, de megoldanánk. A papír alapú nyilvántartásból megoldanák, persze többszörös energia befektetéssel.	1100 fogvatartott van, ha mindenkinél 10 kapcsolattartó van, az 11 000 kapcsolattartó. Nincs ember aki ezt tudná zökkenőmentesen kezelni rendszer nélkül. <u>Egyértelműen akadályozhatja,</u> például a védő esetében alapjogi érintettség is felmerülhet.	<i><u>Azt gondolom nem.</u></i> A védővel, hozzátartozókkal való kapcsolattartást megoldanánk a nyilvántartási, nevelési anyagokból.
Ön szerint mennyire fontos a Főnix 3, SAFE, ETTR, Navigator rendszerek bizalmasságának biztosítása?	Az IBSZ érvényesülése teljesen egyértelmű, magas prioritás. Egyrészt fontos, hogy ki milyen szenzitív adatokhoz fér hozzá, másrészt, hogy mire akarja felhasználni.	A jogosultság szintek beállítása kiemelten fontos, mindenkinek a megfelelő jogosultságokkal kell rendelkeznie. Ugyanakkor a vezetőknek is fontos, hogy meglegyenek azok a jogosultságok, mint az alárendeltjeiknek, hogy tudják ellenőrizni azt, hogy készságszinten alkalmazzák a rendszereket.	Ez is nagyon fontos. Ezeket a rendszereket csak azok ismerhetik meg, és módosíthatnak benne, akiknek ebben feladata van és jogosultsággal rendelkeznek.	Fontos. De ezzel összefüggésben azt gondolom, hogy nem lehet túl szigorú a jogosultságkezelés. A legalapvetőbb szinteken, legfőképpen a körleten is biztosítani kell egy adott szintű jogosultságot. Az ott dolgozóknak szükség esetén bele kell tekinteniük bizonyos nyilvántartásokba. Ők dolgoznak a fogvatartottakkal, ha bármit észlelnek, vagy egy megérzésük támad egy kockázatról, a nyilvántartásban meg tudnak győződni arról, hogy valós-e a veszély.	Fontos, megfelelő szűrés kell a hozzáférések engedélyezéséhez. A fogvatartotti adatbázisban történő "szűrőlést" meg kell akadályozni, de erre van is ellenőrzési tevékenység.	Olyan rendszerről van szó, ahol nagyon szenzitív adatok vannak. Például, ha orvos vagy, olyan jogosultságokkal rendelkez az amivel a különös védelmet igénylő adatokat is megtekinthetsz. Nagyon fontos, hogy csak az a kör tudja használni, amelynek szükséges. Egyébként ez jól van kezelve a rendszerünkben, de fontos, hogy folyamatosan karban legyen tartva a jogosultság kiosztás.	Aki bv-n belül dolgozik, és fogvatartottakkal dolgozik annak kellenek alapvető hozzáférések, és így sajnos ez nehezen kategorizálható, mármint, hogy ki mihez fér hozzá. Az alapjogosultság is rengeteg dologra enged rátekinteni, de ez szükséges is valahol.

Ön szerint mennyire fontos a Főnix 3, SAFE, ETTR, Navigator rendszerek sértetlenségének biztosítása?	Ezt egy példán keresztül tudnám levezetni. Ha én egy hacker lennék, és ártani kívánnék a bv-nek, pont azt csinálnám, hogy hozzáférek a rendszerhez és átírnám a szabadulási időket. Így közép- és hosszú távon sokkal komolyabb károkat lehet okozni. Egy zsarolóvírus támadás után pár nap után felállnánk. De ezek a támadások rejtve is maradhatnak.	A közhiteles rendszereknek olyan információkat kell tartalmaznia, amelyek relevánsak.	Ezt a védett állapotot is meg kell őrizni. Ha belegondolok, elég ha valaki egy telefonszámot átír, az is nagy mértékben megváltoztatná a folyamatok biztonságát. De ez bármilyen adatmódosításra igaz.	Fontos fenntartani ezt az állapotot. Kellene egy nagy piros lámpa ami villog, ha valaki joggalansul módosított valamit, mert lehet észre sem vesszük. Nagyon fontos az is, hogy ha valaki egyik szakterületről átkerül egy másikra, a jogosultságait azonnal felül kell vizsgálni.	Mivel erre támaszkodunk, ilyen mértékben nagyon fontos. Bárki bármit módosítani, nagyon komoly következményei lehetnek.	Ugyanazt tudnám elmondani, mint a bizalmasság esetében. A sértetlenség védelme fontos a külső és belső veszélyek ellen is a megfelelő védelem kell.	Fontos. A sértetlenséget nem csak a kívülről kell biztosítani, hanem a szervezeten belül is. Például az én szakterületi adataim legyenek védve más szakterületektől.
Milyen tanácsai vannak a szervezeti kiberbiztonság területén? Hol kellene/lehetne fejlődünk?	A kiberbiztonság elengedhetetlen, nem kérdés, hogy többet kellene vele foglalkozni, előrébb kellene sorolni. Gondoljunk bele, mi történne, ha valaki hozzá férne a szervezet pénzügyi rendszeréhez. Azt gondolom, hogy hihetetlen jók a jelenlegi fejlesztések, de vissza kellene kanyarodni egy kicsit a múltba. Régebben a rendszerek zártak voltak, kívülről elérhetetlenek. A biztonságtechnikai rendszerhez kívülről nem lehetett hozzáférni, aki hozzáakart, annak be kellett jönni az intézetbe. Régen ez az első fogvatartotti elektronikus nyilvántartási rendszereknél is így volt, a zárt rendszereket kellene visszahozni. Másrészt jelenleg 4-5 külső szolgáltatónak korlátlan hozzáférése van bizonyos rendszerekhez. Harmadrésztől a bíróságok is hozzáférnek már a nyilvántartásunkhoz, ami azért szintén biztonsági kockázat.	Nem igazán vagyok informatikai fejlesztő. Az informatikai infrastruktúrát bizonyosan fejleszteni, újítani kellene. Arra tudok itt gondolni, hogy például az ETTR telefonokon a feloldó kulcs csak egy minta, és mögötte ott van a teljes fogvatartotti nyilvántartás, itt is jelen van egyfajta kockázat, amire megoldás lenne, a névre szóló eszközök kiadása, amelyek például biometrikus azonosítással oldhatóak fel.	A személyi állomány képzésében javulnunk kellene. Kellenének személyek, akik ezzel foglalkoznak, és képzik az állományt. Ez a legfontosabb szerintem.	Az állománynak vannak hiányosságai az informatika terén. Felzárkóztató, és szinten tartó képzések kellenének. Az informatikai infrastruktúra is fejlesztésre szorul, de legfőképpen a képzést gondolom elsődlegesnek.	Szerintem az informatikai infrastruktúrát kellene fejleszteni, idős a géppark, így munkaállomások, szerverek kellenének első körben. Fejlődnek a börtön-technológiák, egyre több mindent vezérlünk technológiákkal, csökken az emberi tényező. Azt gondolom, ezzel egyidejűleg fejleszteni kellene a kiberbiztonságot is.	Először is a tudatosság fokozása. Interaktív képzési felületen képzés kialakítása. A programok hatékonyabb védelme. Az előzetes tesztelés nagyon fontos, hogy olyan alkalmazások kerüljenek rendszerbe, amelyek teljes mértékben tesztelésre kerültek, és nincsenek kiskapuk vagy véletlenül bent maradt funkciók	Hát, ehhez nem igazán tudok véleményt hozzáfűzni, nem vagyok ebben igazán jártas. Nekem a számítógép olyan mint ha egy kávédaráló lenne, így inkább az ilyen javaslatok megfogalmazását meghagyom másnak.