Magyar Rendészet 2023/4. 17–43. DOI: 10.32577/mr.2023.4.1

A magyar büntetés-végrehajtási szervezet digitális kultúrájának kiberérzékenysége[1]

BOTTYÁN Sándor[2]

Az elmúlt időszakban a magyar büntetés-végrehajtási szervezetben lezajló digitális transzformáció során számos informatikai innovációt valósítottak meg. A szervezet működése egyre nagyobb mértékben kapcsolódik a digitális térhez, így fontossá vált a legújabb informatikai fejlesztések kiberbiztonsági szempontú vizsgálata. A tanulmány hiánypótló jelleggel, tudományos megközelítést alkalmazva vizsgálja a magyar büntetés-végrehajtási szervezet munkavállalóinak a kiberbiztonságról és a büntetés-végrehajtási kiberbiztonságról alkotott véleményét. Továbbá feltárja a börtönbeli feladatellátás és az elektronikus információs rendszerek között fellépő dependencia mértékét. Mindemellett a vizsgálat olyan nem várt tényezőket tár fel, amelyek egyaránt befolyásolhatják a magyar büntetés-végrehajtás kiberbiztonságának jelenét és jövőjét.

Kulcsszavak: *kiberincidens, kiberbiztonság, kibertámadás, börtön, információbiztonság*

Bevezetés

Az információs társadalom digitalizációjának folyamatában a prizonális környezet izolált közegnek tekinthető, a hazai börtönrendszer mégsem zárkózott el az informatikai megoldásokban rejlő lehetőségektől. A szabadságvesztés végrehajtásának helyszínén az utóbbi évtizedek során egyre növekedett az adatok rögzítésére való igény, a szakirányú tevékenységeket és a vezetői döntéshozatalt az adatokon lefolytatott elemző-értékelő tevékenység hatékonyan segítette. Manapság az elektronikus információs technológiák alkalmazása több büntetés-végrehajtási célt szolgál, hiszen egyrészről támogató szerepben szerves része a börtönök biztonságának, másrészről olyan eszköz, amelynek segítségével a fogvatartottak életkörülményeit és lehetőségeit közelíthetjük a társadalomban általánosan tapasztalhatókhoz, így az egyaránt hozzájárul a közrend, közbiztonság fenntartásához és az elítéltek társadalomba való reintegrációjához is.

[1] Az Innovációs és Technológiai Minisztérium ÚNKP-22-2-II-NKE-45 kódszámú Új Nemzeti Kiválóság Programjának a nemzeti kutatási, fejlesztési és innovációs alapból finanszírozott szakmai támogatásával készült.

[2] Bv. őrnagy, kiemelt főreferens, Büntetés-végrehajtás Országos Parancsnoksága Hivatal Titkársági Főosztály, e- mail: bottyan.sandor@gmail.com

Azonban a börtönök digitális innovációs irányai egyediek, hiszen az érvényesíteni kívánt célok és az implementációnak helyéül szolgáló közeg is speciálisnak mondhatók. Számos rendhagyó, saját fejlesztésű innovatív megoldás alkotja manapság a bv. szervezet által alkalmazható informatikai lehetőségek körét. Ilyenek az okostelefonon futtatott tevékenységtámogató alkalmazások, mint a SAFE (Szolgálati Alkalmazás a Fogvatartás Elősegítésére),[3] amelynek köszönhetően a felügyelők okoseszközeikkel a börtönön belül bárhol és bármikor elérhetik a fogvatartottakra vonatkozó legfontosabb adatokat és információkat, továbbá alapvető intézkedésekkel kapcsolatos információkat is rögzíthetnek. Vagy említhető még az ETTR (Előállítási Tevékenységet Támogató Rendszer),[4] amely szintén egy mobil alkalmazás, és célja a bv. szerven kívüli előállítási tevékenység szoftveres támogatása. Az elektronikus naplózást megvalósító Navigator rendszer szintén saját, a büntetés-végrehajtási szervezet igényei szerint fejlesztett informatikai rendszer, amely 2018 óta van alkalmazásban, és nagyban hozzájárul a papírmentes iroda elvhez. A KIOSZK a fogvatartottak büntetés-végrehajtási ügyeinek önálló intézésére szolgáló terminál, az azon futtatott Fogvatartotti Kezdeményezésű Kérelmek Modul olyan egyedi fejlesztésű büntetés-végrehajtási szakrendszer, amelyben az adatrögzítések és lekérdezések jelentős részét fogvatartottak végzik el. A közlekedőterületekre felszerelt konzol kialakításának célja, hogy a fogvatartottak közvetlenül hozzáférjenek a saját adataikhoz, irataikhoz, illetve ügyintézést tudjanak kezdeményezni a személyi állomány közreműködése nélkül. Az utóbbi években a már több évtizedes történelemmel rendelkező elektronikus fogvatartotti alapnyilvántartást is újraalkották. A Főnix 3 néven futó alkalmazásrendszer már a hivatali feladatok önálló elvégzésére is képessé vált.

Az utóbbi időszakban a bv. szervezetnél megvalósult informatikai fejlesztésekkel szemben alapvető elvárás volt, hogy csökkentsék a személyi állomány adminisztratív terheit, és segítsék az állományt a jogszerű és szakszerű feladatellátásban. Ezek a fejlesztések közvetlenül a fogvatartottal dolgozó személyi állomány részére készültek, és a gyakorlatba való integrálás következtében számos szakmai tevékenység adatkezelése kerül át folyamatosan a kibertérbe. Azonban ezzel a fejlődéssel együtt új veszélyek indukálódnak. A kibertérbe terjeszkedő büntetés-végrehajtási gyakorlatokkal gyarapodik a szervezethez köthető digitális adatok mértéke, amely folyamatban érintett a különleges és a bűnügyi személyes adatok köre is. A folyamat növeli a szervezet kiberkockázatait, befolyásolja annak kockázati profilját. A kockázatok mögötti veszélyek becsléséhez meg kell határoznunk azok valószínűségét és a bekövetkező hatások mértékét. Elsőként azt szükséges felmérni, hogy milyen mértékben támaszkodik a börtön intézménye alapfeladatainak ellátása során az általa alkalmazott elektronikus információs rendszerekre. Továbbá, hogy a vizsgált rendszerek esetében a főbb információbiztonsági jellemzőkben (rendelkezésre ál-

[3] BVOP 2021.
[4] 72/2020. (XII. 23.) BVOP utasítás.

lás,[5] sértetlenség,[6] bizalmasság[7]) beállt negatív irányú változások hogyan képesek korlátozni a rendeltetésszerű működést.

A kibertér és veszélyei

Mi a kibertér? Hol helyezkedik el? Milyen jellemzőkkel írható le? Ezekre a kérdésekre számos meghatározás létezik a szakirodalmi bázisban, azonban a különböző tudományos terminológiákból eredő definíciók bemutatása előtt először érdemes lehet a szót a maga egyszerűségében értelmezni. A *„kiber"* előtag jelentését számos szakirodalmi forrás az 1940-es években a görög *kübernétész* (kormányos) szóból alkotott *kibernetika* kifejezésből származtatja,[8] amelyet egy komplex tudományos irányzat megjelölésére alkalmaznak manapság is. A kibernetika a szabályozás, vezérlés, információfeldolgozás és -továbbítás általános törvényszerűségeit kutatja.[9] A „kiber" kifejezés tulajdonképpen a *„kibertér"* leegyszerűsített változata, ekként került be a hétköznapi szóhasználatba.[10]

Magyarország Nemzeti Kiberbiztonsági Stratégiája a kibertér megfogalmazásával együtt meghatározza a magyar kiberteret is. A stratégia alkotója szerint a kibertér 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, amely Magyarországon található, 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.[11]

Ahogy a fizikai világban fontos a biztonság, úgy az a kibertérben is az egyik alapvető szükségletként jelentkezik. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) az általános rendelkezések között saját maga alkalmazásában az alábbiak szerint rögzíti a kiberbiztonság meghatározását, miszerint az

---

5 Annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetők és az abban kezelt adatok felhasználhatók legyenek (2013. évi L. törvény).

6 Az adat azon tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható (2013. évi L. törvény).

7 Az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról (2013. évi L. törvény).

8 Wiener 1948.

9 Muha–Krasznay 2014: 17.

10 Muha 2012.

11 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról 3.

> „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 kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez".[12]

De melyek ezek a kockázatok, veszélyek, avagy fenyegetések? Pontos listát felállítani lehetetlen küldetés, hiszen azok száma napról napra nő. A terjedelmi korlátok betartása érdekében a fenyegetések teljes körű bemutatása helyett talán azok aktuális trendjeire és a velük kapcsolatos tapasztalatokra érdemes kitérni. Az ENISA legfrissebb jelentése[13] szerepelteti a legfontosabb fenyegetéseket a 2021. július és 2022. július közötti időszakban. Továbbá vizsgálta a velük kapcsolatban megfigyelt fő trendeket, szereplőket és támadási technikákat, ezek listája általánosságban az alábbiak szerint alakult.

Ransomware

Az első támadási forma a korábbi években is a leggyakoribb 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 támadók átveszik az irányítást a célpont eszközei felett és váltságdíjat követelnek az eszközök rendelkezésre állásának visszaszolgáltatásáért. A támadás célja egyébként nem minden esetben az anyagi haszonszerzésre vonatkozik.[14]

Malware

A rosszindulatú számítógépes programok köre. Ebbe a csoportba számos olyan szoftver vagy firmware[15] 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 sorolják be a kémprogramokat és a reklámprogramok bizonyos formáit is.[16]

---

[12] 2013. évi L. törvény 1. §. 26.
[13] ENISA 2022.
[14] ENISA 2022: 8.
[15] A számítástechnika területén alkalmazott rögzített, kis méretű programok vagy adatstruktúrák, amelyek az elektronikai eszközök alapvető vezérlését hajtják végre.
[16] ENISA 2022: 8.

Social engineering fenyegetések

Olyan tevékenységek széles köre, amelyek a humán tényezőt használják ki annak érdekében, hogy információkat szerezzenek, vagy bizonyos szolgáltatásokhoz hozzáférjenek. A manipulációt, valamint annak eszközeit alkalmazva ráveszik a felhasználókat, hogy nyissanak meg bizonyos dokumentumokat, fájlokat, elektronikus üzeneteket stb., vagy illetéktelen személyeknek biztosítsanak hozzáférést.[17]

Adatok elleni fenyegetések

E fenyegetések célpontjai az adatforrások, valamint a céljuk, hogy azokhoz jogosulatlan hozzáférést szerezzenek. Ezt követően további céljuk az adatok nyilvánosságra hozatala vagy manipulálása. Technikailag az adatok elleni fenyegetések felbonthatók adatsértésre és adatszivárgásra.[18]

Szolgáltatásmegtagadás

Az elérhetőség számos fenyegetés célpontja, ezek közül kiemelkednek a DDoS-támadások. A DDoS-támadás a rendszert veszi célba, és az adatok rendelkezésre állását akadályozza. Nem új fenyegetéstípusról van szó, azonban manapság is jelentős szerepet kap az incidensek sorában. A támadás alatt a felhasználók nem férnek hozzá az adataikhoz vagy a szolgáltatáshoz. Ennek megvalósítása történhet a rendszer erőforrásainak kimerítésével vagy a hálózati infrastruktúra túlterhelésével.

Internetes fenyegetések

Manapság az internet a munkavégzés, a tanulás, a társadalmi érintkezés alapvető szolgáltatása, így az maga is erősen fenyegetett. Ebbe a csoportba azon fenyegetések tartoznak, amelyek az internet elérhetőségét befolyásolják, mint például a BGP *(Border Gateway Protocol).*[19] A protokoll ismert módon sérülékeny az eltérítéses támadásokkal szemben *(BGP hijacking),* amelyek alkalmasak lehetnek az internetes kommunikáció átirányítására és megszerzésére, valamint egyes szolgáltatások elérésének ellehetetlenítésére.[20]

[17] ENISA 2022: 8.
[18] ENISA 2022: 8.
[19] ENISA 2022: 9.
[20] ENISA 2022: 9.

Dezinformáció, avagy félretájékoztatás

A dezinformációs 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, amelyek a felhasználókat félrevezetik, sőt az orosz–ukrán háború kifejezetten új módszereket alkotott a dezinformációs műveletek körében.[21]

Ellátásilánc-támadások

Az ellátási lánc elleni támadások a szervezet és beszállítóik közötti kapcsolatot célozzák. Az ilyen jellegű támadások akkor sorolhatók ide, ha legalább két támadás kombinációjából állnak, valamint a szállítónak és a megrendelőnek is egyaránt célpontnak kell lennie. A szakmában kifejezetten ismert SolarWinds incidens volt az első ilyen eset, amely rávilágított az ellátási láncot ért támadások kiemelt következményeire.[22]

Állami intézményeket folyamatosan érnek kibertámadások, azonban az elmúlt években több külföldi büntetés-végrehajtási intézet is érintetté vált, és az elérhető információk alapján azok jelentős következményekkel jártak. Természetesen, a hazai gyakorlat nem tekinthető azonosnak a különféle nemzetközi büntetés-végrehajtási gyakorlatokkal, így nem lehet egyszerű párhuzamot vonni a hazai szervezet és a külföldi példák között. Azonban a külföldi történések eseményeit tapasztalásképpen érdemes részletesebben megismerni.

Nemzetközi tapasztalatok az államigazgatást érő kibertámadások és hatásaik terén

A kibertámadások növekvő mértéke és azok súlyos hatásai nemcsak egyes szervezetekre vagy vállalatokra, hanem egész nemzetekre nézve is komoly veszélyt jelentenek. Az államapparátusok kontra kibertámadások kontextusában a bizalom kérdése kiemelkedően kritikus aspektus. Az illetéktelen kezekbe jutott állampolgári személyes adatok nemcsak az adatok biztonságát veszélyeztetik, hanem ezek a támadások potenciálisan alááshatják az állami intézmények iránt tanúsított bizalom stabilitását. Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) utolsó jelentésének megállapítása szerint a 2021. július és 2022. július közötti időszakban a közigazgatás, valamint a kormányzati szolgáltatók ellen elkövetett kibertámadások száma kiemelkedő (24,21%) a többi mért adathoz képest (digitális szolgáltatók 13,09%, általános

[21] ENISA 2022: 9.
[22] ENISA 2022: 9.

közösségek 12,43%, szolgáltatók 11,78%, pénzügyi szektor 8,64%).[23] Az ENISA által végzett hatáselemzés szerint a kibertámadások hírnévre gyakorolt hatásai az igazgatási/kormányzati szektort érintették legjelentősebben, ennek oka az állami képviseletbe vetett bizalom elvesztésének tudható be. A támadások hatásai (nem elérhető rendszerek, sérült adatfájlok) vonatkozásában is nagy számban volt érintett a kormányzati szektor. A gazdasági veszteségek köre tekintetében a kormányzati szektor a pénzügyi szektort követi, hiszen a kibertámadásoknak jelentős gazdasági következményei is lehetnek. A támadások gyakran megbénítják a rendszereket és sérülést okoznak az adatfájlokban, aminek következtében jelentős anyagi veszteségek keletkezhetnek. A kormányzati szervek elleni kibertámadások ezért nemcsak a digitális infrastruktúrát veszélyeztetik, hanem az államgazdálkodást is.

Külföldi büntetés-végrehajtási intézetekben bekövetkezett kiberbiztonsági incidensek elemzése

Hivatalos minősítésben, börtönök kiberincidenseiről szóló közlemények nyilvános forrásként való megjelenése nem megszokott, a témában történő tartalom- és dokumentumkutatás csekély mértékben eredményezett hitelt érdemlő információfeltárást. A vizsgált esetek többségében nem történt nyilvános és részletes kommunikáció, mert ez negatívan hathat az adott szervezet társadalmi megítélésére, így ezen okokból előnyös a szervezetek számára, ha azok rejtve maradnak. A következményekkel kapcsolatos sajtómegkeresésekre reagálva az érintett szervek az ilyen események megtörténtét több esetben elismerték sajtóorgánumoknak, azonban a témában kiadott tájékoztatások nem szolgáltatnak teljes transzparenciát. Természetesen a külföldi büntetés-végrehajtási intézetek kiberincidensei a társadalomra kifejtett hatásukról – szervezeti kommunikáció hiányában is – egyértelműen beazonosíthatók. Az így fellelhető információkból – természetesen azok hitelességét helyén kezelve – megállapíthatjuk az események bekövetkezésének idejét és jellegét, az érintettség mértékét és az okozatok által fellépő hatásokat.

Port Phillip Prison, Ausztrália (2022): Az ausztráliai G4S Correctional Services privát szolgáltatóként több ausztrál büntetés-végrehajtási szerv részére nyújt szolgáltatásokat, 1997 óta kezeli és üzemelteti a Melbourne nyugati külvárosi részében található Port Phillip Prison elnevezésű maximális biztonságú börtönt.[24] A 2022 szeptemberében megjelent hírek szerint hackerek 2022. július elején átvették az irányítást a börtön informatikai hálózata fölött. Ennek okán közel 1000 fogvatartott személyes látogatási és videóalapú kommunikációs lehetőségét kellett felfüggeszteni több napra. Az incidenst követően a nyilvánosságot nem tájékoztatták az eset körülményeiről. A kiadott minimális tájékoztatás szerint a börtön személyzete az incidenst követően

[23] ENISA 2022: 9.
[24] Lásd: www.g4s.com/en-au/what-we-do/justice-services/custodial.

értesítette a Victoria Police[25] kiberincidens-elhárító csapatát a fejleményekről. Az eset során korlátozni kellett a börtönbe érkező telefonhívásokat, azonban a szociális munkások és az ügyvédek továbbra is használhatták azt. A G4S szóvivőjének nyilatkozata szerint a kiberbiztonsági incidens a fogvatartottakat és a személyzetet nem érintette.[26] A *Guardian Australia* szerint a támadási forma zsarolóvírus-támadás volt. 2022 szeptemberében a G4S értesült arról, hogy a támadás során kiszivárgott adatok egy része felkerült az internetre. Ennek ellenére a cég ettől sokkal később, október elején tájékoztatta e-mailben a korábbi támadás mértékéről az érintetteket. A közlés szerint a támadók az eset során hozzáfértek az alkalmazottak személyes adataihoz, valamint további különleges (bűnügyi, egészségügyi) adatokhoz is, illetve nyugdíjkezeléssel kapcsolatos információkhoz és egészségügyi szolgáltatással összefüggő engedélyekhez. A G4S a mai napig nem nyújtott teljes tájékoztatást a támadásról, így azt sem tudni, pontosan hány személy adatait érinthette. A későbbiekben nyilvánosságra hozott információk szerint bár a támadást a Port Phillip Prisonban észlelték, azonban a támadó hozzáférhetett a cég teljes informatikai hálózatához, így az több ezer munkavállaló és fogvatartott lehetett érintett.[27]

Metropolitan Detention Center, USA (2022): Az amerikai Bernalillo megyei Metropolitan Detention Center (MDC) egy közel 155 hektár alapterületű, öt objektummal rendelkező szövetségi börtön. Az itt elhelyezett fogvatartottak száma együttesen meghaladja az 1200 főt, amelyek között nagy arányban vannak letartóztatott személyek.[28] 2022. január 5-én zsarolóvírus-támadás érte Bernalillo megye hivatali informatikai rendszerét. A hivatali hálózatban az MDC is érintetté vált, amelyről elsőként az egyik helyi online média számolt be.[29] A szervet ért kibertámadás olyan súlyos károkat okozott, hogy az intézet teljes zárása mellett a vezetésnek nyilvános, sürgősségi felhívást kellett kiadni a szövetségi bíróság részére, miszerint a rendkívüli körülmények miatt átmenetileg képtelenek betartani egy korábbi, 1995. évi peres ügyben létrejött megállapodást, amely a börtönben biztosítandó alapvető körülményekre (túlzsúfoltság és egyéb panaszokra) vonatkozott. A hivatalos nyilatkozat a kibertámadás megvalósítását 0:00 és 5:30 közötti időpontra jelöli. A támadás következtében az intézet nem tudta biztosítani a letartóztatott személyek büntetőeljárásokkal kapcsolatos, telekommunikációs eszközön megvalósítandó tárgyalásait, továbbá a támadás az intézet biztonságtechnikai rendszerét is érintette, így az esemény reggelén az automata ajtószerkezetek is használhatatlanok voltak. Az ajtók működését csak délutánra sikerült visszaállítani, így addig a személyi állománynak fizikai kulcsokat kellett használnia. Az intézet helyben kezelt adatbázisait, saját szoftvereit, valamint az egészségügyi szolgáltatás során alkalmazott nyilvántartásokat sikerült izolálni, így azt nem érintette a támadás. A telefonok

[25] Az ausztráliai Victoria állam elsődleges rendőrségi szerve.
[26] Day 2022.
[27] Taylor 2022.
[28] Lásd: www.bernco.gov/metropolitan-detention-center/frequently-asked-questions/
[29] Fisher 2022.

és a zárkákban elhelyezett oda-vissza beszélő eszközök működtek, valamint a fogvatartottak birtokában található táblagépek is alkalmazhatók voltak. További következményként listázható, hogy nem voltak elérhetők az intézet IP-alapú kamerarendszerei, ami komoly aggodalmat jelentett a személyi állomány és a fogvatartotti állomány biztonsága szempontjából. A fellépő kockázatok kezelése érdekében rendkívüli biztonsági intézkedéseket kellett bevezetni, ezek a fogvatartotti jogok korlátozásához vezettek. A fogvatartottak zárkájukat nem hagyhatták el, az összes hozzátartozói látogatást felfüggesztették. Internet-hozzáférés 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.[30] Az incidens után a Bernalillo Megyei Bizottság döntése alapján új kiberbiztonsági politikát kívánnak bevezetni, amely magában foglalja a felhasználók többfaktoros[31] azonosításának alkalmazását is. Továbbá létrehoznak egy megyei hálózatok megfigyelését végző biztonsági műveleti központot, amely az alá tartozó hálózatokra kapcsolt számítógépek esetében riaszt a gyanús tevékenységek észlelésekor.[32]

Evin Prison, Irán (2021): 2020–2021-ben Iránnak számos nagyobb kibertámadással kellett szembenéznie, ilyenek voltak az állami vasúti rendszert érintő incidens,[33] vagy a Bandar-Abbász város kikötőjét célzó művelet.[34] Az Evin Prisont is ebben az időszakban érte kibertámadás, ám annak pontos időpontját ebben az esetben sem hozták nyilvánosságra a hatóságok. Az 1972 óta üzemelő börtön Teherán Evin városnegyedében található, és az 1970–1980-as években ott zajlott kínzásokról és tömeges kivégzésekről nemzetközileg is ismertté vált, de napjainkban is erősen kritizálják működését az emberi jogokért és szabadságokért harcoló nemzetközi civil szervezetek.[35] 2021. augusztus 22-én több, a börtön belső kamerarendszeréből kiszivárgott kamerafelvétel jelent meg egyidejűleg különböző sajtóorgánumok felületén, amely információkból megállapítható volt, hogy a támadás egy Ali Adalat (Ali igazságszolgáltatása) nevű hacktivista[36] csoporthoz köthető. A 2020. és 2021. évi időbélyegzőkkel ellátott felvételek főként a börtön személyzetének a fogvatartottakkal szembeni brutális, emberi jogokat sértő bántalmazásait voltak hivatottak bizonyítani. A kiszivárgott felvételeken látható, hogy a technikai rendszerkezelő szolgálati helyén elhelyezett monitorfal adását is felülírták, és egy „Kibertámadás. Általános tiltakozás a politikai foglyok szabadságáig" üzenetet osztottak meg perzsa nyelven. Egyértelmű, hogy a börtön biztonságtechnikai rendszerében okozott zavarok

[30] 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.

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

[32] Lásd: www.cyansecurity.com/half-year-review-of-significant-cyberattacks-bernalillo-county/

[33] Cimpanu 2021.

[34] Cimpanu 2020.

[35] Gholami 2022.

[36] A hacktivisták számítógépes hackelés felhasználásával promotálnak bizonyos politikai nézeteket, foglalnak állást politikai kérdésekben.

és a rendeltetésszerű működés megzavarása mellett a hacktivista csoport célja nem az állami szervben való károkozás volt, hanem a börtön szimbolikáját és a hírverést felhasználva minél nagyobb tömegekhez igyekeztek politikai üzenetüket eljuttatni. A börtön, amely alanya volt a kibertámadásnak, egyúttal eszközzé vált a politikai célok elérésében.

Idaho State Correctional Institution, USA (2018): A következő incidens alapjaiban eltér az eddigiekben bemutatottaktól, hiszen nem egy börtönt érintő kibertámadásról van szó, hanem olyan jellegű informatikai incidensről, amelynek legfőbb kockázati tényezője a fogvatartotti populáció volt. 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 és a Correctional Alternative Placement Plan Facility. Az Egyesült Államok fogvatartottjainak már több államban van lehetőségük úgynevezett „börtöntableteket" használni. Ezek speciálisan börtönhasználatra tervezett készülékek, szoftver és hardver tekintetében is speciálisnak mondhatók. A JPay szolgáltatása kifejezetten népszerű a fogvatartottak körében, hiszen a készülékkel e-maileket küldhetnek kapcsolattartóiknak, zenéket vásárolhatnak és hallgathatnak, edukációs alkalmazásokat használhatnak, továbbá játékokat is játszhatnak.[37] A készülékek elterjedését követően a fogvatartottaknak sikerült a készülék szoftverének egy sérülékenységét kihasználni, majd felhasználói számláikon a pénzösszegeket megnövelni és vásárlásokat végrehajtani. Az eset során 364 fogvatartott összesen, átszámolva, közel 80 millió Ft értékű kárt okozott a szolgáltatónak. A JPay az esetet követően felfüggesztette a zenék és játékok letöltését a károk megtérítéséig, valamint a börtön fegyelmi eljárást kezdeményezett az érintett fogvatartottakkal szemben és magasabb biztonsági kockázatú csoportba helyezte őket.

A fent bemutatott esetekből értelemszerűen – a maradéktalan tudományos megalapozottságot nélkülözve – következik, hogy nemzetközi viszonylatban a börtönök olyan mértékű alapfeladat-ellátás – informatika dependenciával rendelkeztek, amelynek akadályoztatása erős zavarokat okozott az alapvető működési folyamatokban. Felismerhető az a jelenség, miszerint egy ilyen rendszert ért kibertéri támadás közvetlen kihatással lehet a személyi állomány biztonságára, de akár a fogvatartottak alapvető emberi jogainak garanciájára is. A magas bástyafalak, amelyek eddig fizikai akadályként szolgáltak és biztosították a rendeltetésszerű működést, már nem képesek teljes körű védelmet biztosítani, hiszen a digitalizáció folyamata egy új színteret, a kiberteret nyitja meg a börtönöket érintő új kockázatok számára. A tudományos kérdés az, hogy a hazai büntetés-végrehajtás börtöneit ért kibertámadás okozhat-e a nemzetközi kitekintésben részletezett eseményeket, zavarokat? A tanulmány e kérdésekre próbál válaszokat adni az általa vizsgált témák feldolgozásával.

[37] Lásd: www.jpay.com/education.aspx

A vizsgált téma bemutatása

A nemzetközi kitekintésben feltárt események vizsgálatából megállapítható, hogy egy hazai bv. szerv[38] elektronikus információs rendszerei közül – azok rendelkezésre állásának megszűnése esetén – a rendeltetésszerű működésre gyakorolt hatások mértéke két rendszer vagy rendszercsoport esetében mondható jelentősnek. Az első a börtönök biztonságtechnikai rendszere, míg a második az elektronikus nyilvántartások csoportja. Előbbi rendelkezésre állásának megszűnése esetén a hatások vitán felül jelentősek és alapjaiban rengetik meg a működést, azonban biztonsági és/vagy korlátozó intézkedések meghozatalával, többlet személyi állomány bevonásával közel biztosítható a biztonságra gyakorolt védelmi hatás, amelyet a rendszer alapvető működése esetén szolgáltat (például elektronikus távfelügyeleti rendszer meghibásodása esetén járőr kiküldése, vagy a bv. intézet kamerarendszerének meghibásodása esetén az ajtók zárva tartásának elrendelése, felügyelet átcsoportosítása, belső járőrszolgálat indítása).

A másik csoport számos eleme közül az egyik, ha nem a legfontosabb az elektronikus fogvatartotti alapnyilvántartás rendszere, amely már több évtizede fundamentuma a büntetés-végrehajtás digitális kultúrájának. Az elektronikusan tárolt információk mennyisége folyamatosan gyarapodik, köszönhetően a munkafolyamatokba adaptált elektronikus adatkezelés és -feldolgozás folyamatainak. A BvOP[39] hatályos, belső szabályzói által nyilvántartásra előírt fogvatartotti adatok még helyi archív és aktuális személyenkénti papíralapú nyilvántartásokban is megtalálhatók, de a gazdasági és környezetbarát szempontok mentén érvényesülő papírmentes iroda elv megvalósulási folyamata hatással van a szervezeti kultúrára, és igazolja az informatikai nyilvántartások és a hozzá tartozó tevékenységtámogató rendszerek fontosságát. Mindazonáltal, ha az elektronikus fogvatartotti alapnyilvántartás elérhetetlenné válik, annak tevékenységtámogató funkciója nem pótolható, és az általa okozott negatív hatások nem csökkenthetők egyértelműen sem korlátozó, sem többletintézkedésekkel, vagy többlet személyi állomány bevonásával. Ezért a téma kiberbiztonsági szempontú vizsgálata vitathatatlanul indokolt, mindazonáltal érdemes kitérni a rendszer bemutatására.

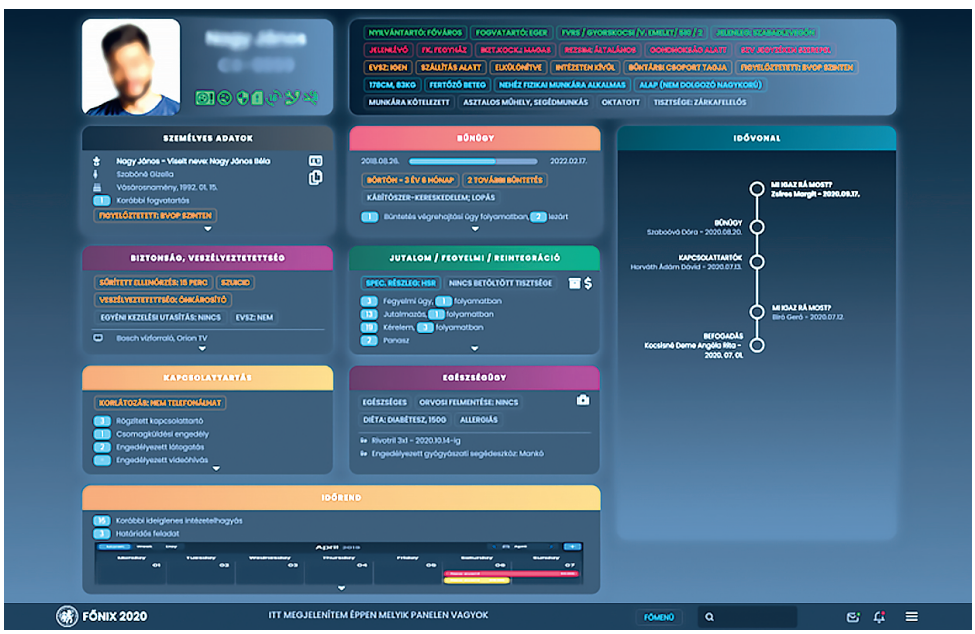
Az Elektronikus Fogvatartotti Alapnyilvántartás (Főnix3)

A büntetés-végrehajtási szervezet fogvatartotti alapnyilvántartásának kezdeti elvárásai a mai követelményekhez képest alacsonyak voltak. A 20. század elején a nyilvántartás csak a börtönökben elhelyezett fogvatartottak létszámára és személyes adataira terjedt ki. Egy erre a célra rendszeresített A/2-es méretű keményfedeles könyvben vezették az adatokat, és a nyilvántartásból kivezetést többnyire három élethelyzet in-

[38] Az Országos Parancsnokság, a büntetés-végrehajtási intézetek és intézmények, továbbá a fogvatartottak kötelező foglalkoztatására létrehozott gazdasági társaságok és költségvetési szervek (1995. évi CVII. törvény).

[39] Büntetés-végrehajtás Országos Parancsnoksága.

dokolta: szabadult, átszállították vagy elhalálozott.[40] Az évek során a nyilvántartások köre számos új adattal bővült, majd a rendelkezésre álló technológiák használatbavétele által exponenciálisan növekedett. Az informatika egyre nagyobb fokú elterjedésével a büntetés-végrehajtási szervezet sem kerülhette el azt a változást, hogy az általa kezelt adatokat digitális formában rögzítse. A jelenleg használt elektronikus fogvatartotti alapnyilvántartás (Főnix3) létrehozását az innováció tette lehetővé 2021-ben, hiszen a korábbi évek során alkalmazott Főnix2 rendszerben számos olyan informatikai modul[41] jött létre az elektronikus fogvatartotti alapnyilvántartás (FANY[42]) mellé, amely indokolta, hogy az így, szigetszerűen létrejött alkalmazásokat együttesen, egy új generációs informatikai megoldásba integrálják. Emellett 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, vagyis a munkafolyamatok támogatása és irányítása. A fejlesztés során a szakterületek legtapasztaltabb szakemberei dolgoztak együtt a Büntetés-végrehajtás Országos Parancsnokságának Informatikai Főosztályával és a külső fejlesztő partnerekkel. E közös munka eredményeként jött létre a Főnix.



1. ábra: A Főnix3 rendszer felhasználói felülete (mintaadatokkal)

Forrás: A BvOP belső forrásából

[40] Bogotyán–Veszeli 2011: 61.

[41] A Főnix2 rendszerben önálló informatikai modulok készültek a különböző szakterületek támogatására (pl. EÜ-rendszer, Élelmezés, OÉT-kezelés, Pénzügyi letétkezelés, Biometria stb.).

[42] Fogvatartotti Alap Nyilvántartás. A bv. szervezet korábbi, a FAR-t (Fogvatartotti Alrendszer) követő elektronikus SQL-alapú fogvatartotti alapnyilvántartása, amely webalapú grafikus felhasználói felülettel eleget tett a kor elvárásainak.

A rendszer webalapú, reszponzív megoldás, így a munkaállomásokon és tablet-készülékeken is könnyen alkalmazható felhasználói felületet biztosít. A felhasználói felület kialakítása során tudatos cél volt, hogy a felhasználó minél rövidebb idő alatt kapja meg a számára szükséges információt. Tartalmi szempontból fontos megemlíteni, hogy a büntetés-végrehajtási szervezet törvénye a fogvatartotti nyilvántartást a személyes adatok, lakcímadatok és kapcsolattartó személyekre vonatkozó adatok kivételével közhiteles nyilvántartásként ismeri el,[43] így számos jogszabályi előírásnak, legfőképpen a bűnügyi nyilvántartási rendszerről szóló törvény rendelkezésének kell megfelelnie.[44]

A rendszer négy fő részből áll, amelyek a következők: biztonság, bűnügyi nyilvántartás, fogvatartás és általános rész. Ez a tagoltság azért indokolt, mert a fogvatartotti alapnyilvántartást eltérő folyamatok támogatására alkalmazzák a különböző szakterületek, így a szaktevékenységeknek megfelelő tevékenységtámogató funkciókat fejlesztettek ki. A Főnix3 létrehozása során már szakmai elvárás volt, hogy a rendszer kezelje a digitális dokumentumokat, és segítse elő a papírmentes iroda megvalósulását, így a különböző felületeken dokumentumfeltöltési lehetőség is adott, amely funkció nagyban segíti a visszamenőleges iratok keresését. A legújabb technológiai újítás a rendszerben egy olyan interfészmegoldás, amely a bíróságokkal való adatkommunikációt segíti. Az igazságszolgáltatási szervek számos adatot szolgáltatnak a bv. szervek részére további feldolgozás céljából. A fejlesztést megelőzően a papíralapú dokumentumok elektronikus nyilvántartásba rögzítése jelentős adminisztratív teher volt, azonban a kialakított interfészkapcsolatnak köszönhetően ezek az adatok már digitálisan, újrarögzítés nélkül kerülnek be a fogvatartotti alapnyilvántartásba, így a bv. szervezetet érintő adminisztrációs terhek mértéke és az esetleges hibák kockázata és a rögzítésre szükséges időigény is csaknem megszűnt.

A rendszerben található a humoros szimbolika szerint elnevezett JARVIS[45] modul, amely kifejezetten érdekes, innovatív megoldás, és a Főnix3 automatizált funkcióinak körét jelenti. A funkció összefogja a nyilvántartásban található bv. ügyeket (például fogvatartotti kérelmeket), majd „intézi" azokat, és jelzést ad, ha szükséges a perszonális beavatkozás. Biztosítja a szervezetre vonatkozó szabályozókban meghatározott határidők betartását, az előírt eljárási útvonal betartását. Ezzel a megoldással a bv. ügyet automatizáltan a jogszabályi rendelkezések szerinti időpontban indítja, így az ügymenet e részén a hibafaktor nullára redukálódott. A fogvatartotti kérelmeknek tartalmi követelménye, hogy az adott kérelemben illetékes szakterületek véleményezzék azokat, hogy a döntési jogkör gyakorlója szakmai, adatok elemzésén és értékelésén nyugvó döntést tudjon hozni. A JARVIS modul az adatbázisból önállóan generálja ezeket a szakmai véleményeket, előre definiált sablonok alapján,

[43] Veszeli 2017: 94.

[44] 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.

[45] J.A.R.V.I.S. egy kitalált karakter a Marvel Cinematic Universe filmfranchise-ban, aki a Tony Stark szereplő által tervezett mesterséges intelligencián alapul.

ezáltal jelentősen tehermentesítve a felelős szakterületeket. Összességében elmondható, hogy a Főnix3 innovatív jellegű, korszerű és felhasználóbarát módon támogatja a szakterületi alapfolyamatokat, és képes kielégíteni a 21. századi igényeket.

A kutatás célja és eredményei

A kutatás általános célja egy kiberbiztonsági szempontú büntetés-végrehajtási ismeretanyag összeállítása volt, amely hiánypótló jelleget lát el a szakirodalmi bázisban, valamint bemutatja a büntetés-végrehajtási dolgozók vélekedését a kiberbiztonságról, valamint annak szakmai helyzetéről. Speciális célként felmérni a szervezet egyik legfőbb informatikai szakrendszeréhez, az elektronikus fogvatartotti nyilvántartáshoz, valamint az azzal összefüggő büntetés-végrehajtási informatikai szakrendszerekhez köthető dependencia mértékét. Vizsgálni a rendszer elérhetetlensége esetén fellépő fizikai hatások mértékét, valamint, hogy egy kibertámadás milyen mértékig képes befolyásolni egy hazai börtön működését.

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 fizikai hatásának egy adott mértékét vizsgálja. A II. számú hipotézis az kívánja vizsgálni, hogy a Főnix3 rendelkezésre állásának megszűnése esetén a fizikai hatások okozhatnak-e fogvatartotti alapjog-korlátozást (például tisztességes eljáráshoz való jog, magánélethez és családhoz való jog stb.). Amennyiben ez valós kockázatot jelent, úgy bekövetkezés esetén az eset alapot szolgáltathat a fogvatartottaknak a szervezettel szemben kártalanítási eljárások megindítására, ezáltal pénzbeli kártérítések kifizetésére.

Az általános jellemzők és a hipotézisek egyidejű vizsgálata kérdőívvel valósult meg, amelyet a bv. szervezetben aktív szolgálatot ellátó személyi állományi tagok töltöttek ki. A válaszadások elektronikusan, 2023. március 5. és 2023. március 20. között, több büntetés-végrehajtási intézet vonatkozásában valósultak meg, összesen 103 db kérdőív készült. Továbbá kvalitatív mintavételként hét, személyenként 45–75 perc időtartamú anonim interjú készült a Budapesti Fegyház és Börtön közép- és beosztott vezetői állományának (szakterületi vezetőinek) vonatkozásában 2023. március 20-án. Az interjúk esetében a célok azonosak voltak a kérdőívtől elvártakkal, azonban a hatások mértékén kívül azok módozatai is a vizsgálat tárgyát képezték. Az interjúk alapvetően strukturálisnak tekinthetők, három kivétellel a kérdések azonosak voltak a kérdőívben megfogalmazottakkal. Az eltérő kérdések a vizsgált Főnix3 rendszer sértetlenségére és bizalmasságára irányultak, a zárókérdés pedig a szervezet jövőbeli kiberbiztonsági fejlesztéseinek lehetőségeire terelte a figyelmet.

A kérdőívek eredményei

A 103 db kérdőív által szolgáltatott adatok közül érvénytelen nem volt. A válaszok számadatokká alakítását követően a kiértékelés az IBM SPSS Statistics szoftverrel történt. Az adatok ábrázolását a terjedelmi korlátok okán a helyigényes grafikonok helyett szöveges táblázatként jelenítjük meg.

A felmérésben részt vevők demográfiai adatai a következőképpen alakultak:

Az Ön neme?		
	Elemszám	**%**
Férfi	59	57
Nő	44	43
Összesen	103	100

Az Ön kora?		
	Elemszám	**%**
18–28 év	27	26
29–39 év	45	44
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 részt vevők bv. szervezethez való viszonyulásai a következőképpen alakultak:

Hány év szolgálati idővel rendelkezik a bv. szervezetnél?		
	Elemszám	**%**
0–5 év	30	29
5–10 év	38	37
10–15 év	21	20
15–20 év	9	9
21+ év	5	5
Összesen	103	100

Az Ön szolgálati helye:		
	Elemszám	**%**
Agglomerációs Központ	34	33
Egyobjektumos. bv. intézet	26	25
Intézmény (IMEI, BvEK)	6	6
Több obj. bv. intézet	37	36
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 érin-

tett olyan szervezeti specifikumokat, mint a Büntetés-végrehajtás Egészségügyi Központja (BvEK), vagy az Igazságügyi Megfigyelő és Elmegyógyintézet (IMEI) is.

A további kérdések:

Milyen beosztáscsoportban teljesít szolgálatot?		
	Elemszám	**%**
Végrehajtó	79	77
Középvezető	21	20
Vezető	3	3
Összesen	103	100

Melyik szakterületen teljesít szolgálatot?		
	Elemszám	**%**
Agglomerációs Osztály	5	5
Biztonsági Osztály	48	46
BvOP	1	1
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 értékeloszlása elfogadható, arányait tekintve a valóságot tükrözi. A szakterületekről érkező nyilatkozatok is megfelelnek az elvárt adatoknak. 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-végrehajtás személyi állományának véleménye a kiberbiztonságról:

Ön szerint mennyire fontos manapság a kiberbiztonság?		
	Elemszám	%
1	1	1
3	5	5
4	20	19
5	77	75
Összesen:	103	100

Ön szerint mennyire fontos a bv. szervek tekintetében a kiberbiztonság?		
	Elemszám	%
1	0	0
2	0	0
3	5	5
4	25	24
5	73	71
Összesen:	103	100

Ezzel a kérdéspárral a válaszadók értékelhették a kiberbiztonság fontosságát egy 1-től 5-ig terjedő skálán. Az 1 „Nem fontos”-t, míg az 5 „Kiemelten fontos”-t jelentett. A válaszok alapján a kiberbiztonság és különösen a büntetés-végrehajtási szervek kiberbiztonsága kiemelten fontos. A mindkét kérdésre adott értékelések szinte azonosak, ami azt jelenti, hogy a válaszadók szerint az „általános” kiberbiztonság és a büntetés-végrehajtási szervek kiberbiztonsága egyaránt fontos tényező manapság.

Ön szerint számítani lehet egy börtönt érintő kibertámadásra?		
	Elemszám	%
Igen	49	48
Talán	43	42
Nem	8	8
Nem tudom	3	2
Összesen:	103	100

A következő kérdés a börtönt érintő kibertámadás kockázatának személyi állomány általi érzékelését mérte. A kockázatok valódiságát igazolhatja, hogy a kitöltők 48%-a úgy gondolja, hogy egy börtönt érintő kibertámadásra számítani kell, valamint 42%-a úgy gondolja, hogy egy ilyen támadás eshetősége áll fenn.

Az elektronikus fogvatartotti nyilvántartásra vonatkozó kérdésekben a Főnix3 rendszer mellett szerepeltek az olyan interfészkapcsolatban álló tevékenységtámogató rendszerek is, mint a SAFE, ETTR és Navigator. Ennek célja az volt, hogy a válaszadók mérlegeljék az összes vizsgált rendszer esetleges leállásából adódó hatásokat egyidejűleg.

Ön szerint manapság a büntetés-végrehajtási feladatok jogszerű ellátásához nélkülözhetetlen a Főnix3, SAFE, ETTR, Navigator informatikai rendszerek alkalmazása?		
	Elemszám	%
Igen	83	81
Nem	13	12
Nem tudom	2	2
Talán	5	5
Összesen:	103	100

Ön szerint milyen mértékben támaszkodunk a feladatellátás során az alábbi informatikai rendszerekre: Főnix3, SAFE, ETTR, Navigator?		
Skálaérték	Elemszám	%
1	1	1
2	6	6
3	10	9
4	35	34
5	51	50
Összesen:	103	100

A speciális célokat szolgáló kérdéscsoport első kérdése a vizsgált rendszerek jogszerű feladatellátásához való nélkülözhetetlenségét kívánta felmérni. A kapott adatból egyértelműen megállapítható, hogy a válaszadók szerint a jogszerű feladatellátáshoz szükséges a megnevezett rendszerek alkalmazása. Továbbá, önálló kérdésben lett vizsgálva annak a mértéke, hogy a mindennapi feladatellátás érdekében milyen mértékben alkalmazzák a vizsgált rendszereket. A kérdés esetében a válaszadók 1-től 5-ig terjedő skálán értékelhették 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.

Ön szerint milyen mértékben zavarhatja meg a Főnix3, SAFE, ETTR, Navigator rendszerek leállása egy bv. intézet rendeltetésszerű működését?		
Skálaérték	Elemszám	%
1	4	4
2	9	9
3	9	9
4	31	30
5	50	48
Összesen:	103	100

Ön szerint a Főnix3, SAFE, ETTR, Navigator rendszerek elérhetetlensége okozhat rendkívüli eseményt?		
	Elemszám	%
Igen	54	52
Nem	19	18
Nem tudom	3	3
Talán	27	27
Összesen:	103	100

A következő két kérdés azt vizsgálta, milyen mértékű hatást gyakorol a vizsgált rendszerek leállása vagy elérhetetlensége. Az első kérdés a rendeltetésszerű működésre gyakorolt hatást mérte. A kérdés esetében a válaszadók 1-től 5-ig terjedő skálán értékelhették a választ, ahol az 1-es számhoz a „Csekély mértékben", míg az 5-ös számhoz a „Jelentős mértékben" jelentés társult. A kapott adathalmaz a je-

lentős mérték felé erősödő modellt mutat, így a válaszadók véleménye alapján a vizsgált rendszerek leállása képes megzavarni egy intézet rendeltetésszerű működését.

A másik kérdés az első megfogalmazásnál mélyebbre próbált hatolni. Azt kívánta vizsgálni, hogy a tanulmányozott rendszerek elérhetetlensége okozhat-e rendkívüli eseményt. A kérdés a válaszok alapján igazoltnak tekinthető, hiszen a válaszadók 52%-a igennel válaszolt, míg az eshetőséget 26% jelölte meg. Érdekes megfigyelés, hogy a feleletválasztós kérdések közül ebben a kérdésben érte el a „Nem" válasz a legnagyobb előfordulást. Ennek okát nem sikerült egyértelműen feltárni, azonban a szerző véleménye szerint leginkább az állhat a háttérben, hogy a szervezeti kultúra a rendkívüli esemény alatt leginkább a fogolyszökést, fogolyzendülést és a hasonló súlyos, közrendre és közbiztonságra veszélyes eseményeket érti, amely események létrejöttével összefüggésben informatikai dependenciát nehéz feltételezni vagy bizonyítani.

A kérdőív utolsó kérdése arra irányult, hogy a rendszer elérhetetlensége okozta negatív hatások között jelen van-e a fogvatartottak alapjogi érintettsége. Bár egy elektronikus fogvatartotti alapnyilvántartásra irányuló kiberincidens során a fogvatartottak adatainak (beleértve a személyes, különleges, egészségügyi és bűnügyi adatokat) biztonsága sérülhet, és ezzel egyidejűleg az alapjogi érintettség is megvalósulhat, ez a kérdés azt vizsgálta, hogyan befolyásolja a rendszer elérhetetlensége a fogvatartottak alapjogi érintettségét a kiváltott fizikai hatásokon keresztül. Ezt a fajta érintettséget legkönnyebben a kapcsolattartás funkciójának megvalósulásán keresztül mérhetjük fel.[46]

Ön szerint a Főnix3 rendszer elérhetetlensége akadályozhatja a fogvatartottak kapcsolattartási formáinak megvalósulását?		
	Elemszám	%
Igen	57	55
Nem	18	18
Nem tudom	2	2
Talán	26	25
Összesen	103	100

A kapott válaszokból megállapítható, hogy a feltételezés a válaszadók szerint helyénvaló, hiszen azok több mint fele gondolta úgy, hogy a rendszer elérhetetlensége képes akadályt gördíteni a fogvatartotti kapcsolattartás elé, ezáltal a vizsgált rendszer rendelkezésre állásának hiánya és a fogvatartotti alapjogok közötti érintkezés valóban észlelhető. Ugyanakkor a „Talán" válaszban értelmezhető eshetőség mértéke 25%, ami szintén jelentős mértéknek tekinthető. Érdekes adatként szolgálhat,

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

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 vizsgált közegbe, amelynek a megosztottsági mértéke már számottevő.

Az interjúk eredményei

A vezetői interjúk eredményei nagyrészt megerősítik a kérdőíves felmérés eredményeit, ugyanakkor új információkat is feltártak. A kiberbiztonságot és a bv. kiberbiztonságot megosztottság nélkül (7/7) fontos tényezőkként azonosították az interjúalanyok. Némi megosztottság jelent meg a bv. szerv kibertámadásának kockázatára irányuló kérdésnél, itt a 7 válaszadóból 2 nem gondolta számottevőnek a veszélyt. Azonban a rendszerek jogszerű feladatellátásban betöltött nélkülözhetetlenségéről alkotott vélemények erősen megosztottak voltak, ami nem igazolta a kérdőíves eredményeket. Ennek oka az lehet, hogy a vezetői gondolkodást befolyásolja az a múltbéli tapasztalás, hogy évekkel ezelőtt még az informatikai rendszerek nélkül is lehetséges volt a jogszerű feladatellátás. A szükséges feltételek (például papíralapú naplók és azok vezetéséhez szükséges szakmai ismeret) még manapság is rendelkezésre állnak, így véleményük szerint a jogszerűség biztosítható informatikai rendszerek nélkül is. A vizsgált rendszerekre való jelentős ráutaltságot a vezetői vélemények is megállapították (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 interjúalanyok véleményei alapján is (6/7). Az interjúban feltett három, kérdőívtől eltérő kérdésben kapott válaszokat az eredmények egybevetésével, valamint a további feltárt információk elemzésével együtt tüntetjük fel a következő fejezetben.

Megállapítások

A kérdőívek és a vezetői interjúk alapján a szervezet munkatársai kiemelten fontosnak tartják általában a kiberbiztonságot és a kiberbiztonságot a büntetés-végrehajtás területén, továbbá egy börtönt érintő kibertámadást komoly veszélyforrásként értékelnek. 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 önállóan is alátámasztják ezt, azonban az interjúalanyok válaszai, bár megosztottak voltak, összességében arra utaltak,

hogy a jogszerűséget biztosítani tudja egy bv. intézet akkor is, ha a ma már inkább alternatívaként számontartott papíralapú nyilvántartásokra és dokumentumokra támaszkodik.

Azzal a feltevéssel, hogy a vizsgált rendszerek leállása komoly zavarokat vagy akár rendkívüli eseményeket okozhat egy bv. intézet működésében, összességében egyetértettek a vizsgálat során, azonban a kérdőívek és az interjúk eredményeinek összevetése újabb részleteket hozott felszínre. 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 szolgáltak eszközül. A kérdéspár első kérdésével összefüggő interjúk rendkívüli esemény eshetőségére adott válaszaiban megjelenik megosztott polaritás, miszerint rendkívüli esemény okozójává igen, viszont súlyos rendkívüli esemény[47] okozójává nem válhatnak a vizsgált rendszerek leállásai.

A rendeltetésszerű működés megzavarására irányuló kérdésre adott vezetői válaszok egymáshoz viszonyítva, sőt még válaszokon belül is erősen megosztottak voltak, velük összefüggésben egyértelmű, önálló megállapítás nehezen tehető. Az interjúválaszok kérdőíveredményektől eltérő, valamint az egymáshoz viszonyított megosztott válaszait valószínűleg a „rendeltetésszerű működés" megfogalmazás körülötti fogalmi zavar okozhatta, hiszen ehhez a kifejezéshez egyesek a tágabb értelmezést, míg mások a sarkalatos, jogszabály jellegű megfogalmazást társítják. A kapott válaszokban azonban számszerű többségben van az a megállapítás, amely szerint a zavaró hatás egyértelműen, nagymértékben indukálódhat. Az elektronikus fogvatartotti alapnyilvántartás és az azzal összefüggő elektronikus információs tevékenységtámogató rendszerek elérhetetlensége jelentős mértékben megzavarja a bv. intézetek rendeltetésszerű működését, hatással van a biztonság állapotára, és adott esetben rendkívüli esemény forrása is lehet. Ezzel a megállapítással az I. számú hipotézis igaznak bizonyult.

A kérdőívek válaszai és az interjúalanyok együttes véleménye alapján a Főnix3 rendszer elérhetetlensége akadályozhatja a fogvatartottak kapcsolattartási formáinak (levelezés, telefonbeszélgetés, látogatófogadás megjelenése, telekommunikációs eszköz, csomagküldés, eltávozás, látogatófogadás intézeten kívül, kimaradás, reintegrációs eltávozás) megvalósulását, ezáltal a fogva tartás alanyának alapjogi érintettsége létrejöhet. Az interjúalanyok szerint a rendszer leállása eshetőlegesen vezethet a felsorolt kapcsolattartások elmaradásához vagy korlátozásához. Az eshetőség oka, hogy a rendszer leállása esetén az eljárások alternatív biztosításához a személyi és papíralapú nyilvántartásokból szükséges feltárni az adatokat, amely tevékenységnek az idő- és humánerőforrás-igénye jelentős, így tömeges érintettség esetén a folyamatok megvalósítása akadályba ütközhet. Az eredményeket összevetve megállapítható, hogy egy elektronikus fogvatartotti alapnyilvántartást

[47] Olyan rendkívüli esemény, amely a közrendet vagy közbiztonságot veszélyeztetné (pl. fogolyszökés).

érintő kibertámadás hatása nemcsak a börtön állapotát befolyásolja, hanem annak legmélyére hatolva a fogvatartottak alapjogaival is képes érintkezni. Ezzel a megállapítással a II. számú hipotézis is igaznak bizonyult.

A vezetők az interjúk során adott válaszaikban különös hangsúlyt helyeztek az informatikai rendszerek jogosultságkezelésének fontosságára. A vezetők fontosnak tartják, hogy a legérzékenyebb adatokhoz csak a szükséges mértékben, csak az arra jogosult személyek férjenek hozzá, ugyanakkor egyes vélemények szerint a túl szigorú jogosultságkezelés akadálya is lehet a hatékony szakmai munkának. Az interjúk során a vezetők több esetben jelentették ki azon ellenőrzési tevékenység fontosságát, amely a bizonyos jogosultságokkal rendelkező személyek által megtekintett adatok vonatkozásában a megtekintés indokoltságát vizsgálja.

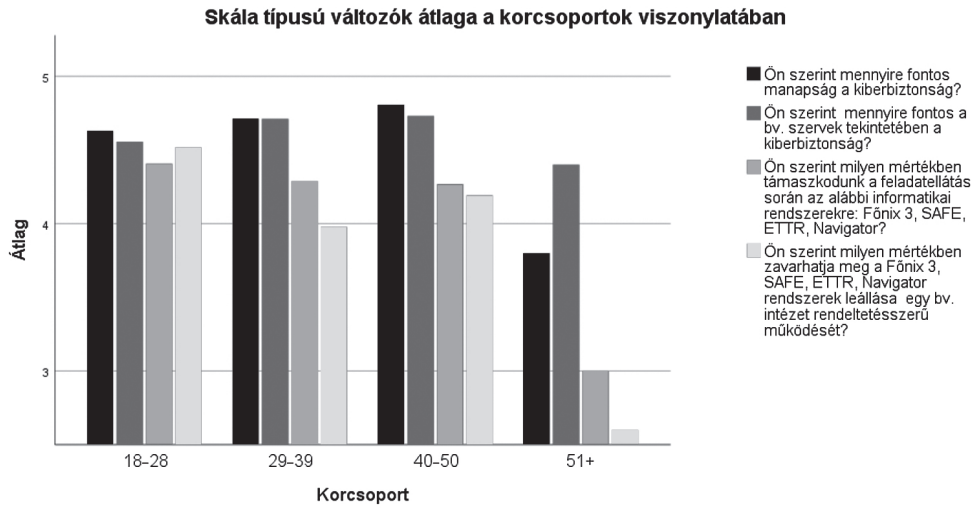
Minden vezető egyöntetűen nagy jelentőséget tulajdonít a vizsgált rendszerek sértetlenségének. Az állapot megsértését összességében komoly kockázatként jelölték meg, hiszen egy rosszindulatú adatmódosítás komoly, a szakmai munkára veszélyes hatásokkal járhat. Megfogalmazták azt a bv. szervezeti sajátosságot, hogy a sértetlenség állapotára a fogvatartotti csoport is jelentős kockázati tényező, így a védelmi intézkedéseknek ezt a sajátosságot is figyelembe kell vennie.

Az interjúk záró kérdése arra irányult, hogy felkutassa a további javaslatokat és az esetlegesen figyelmen kívül hagyott kockázatokat. Az adott válaszokból megállapítható, hogy a személyi állományi tagok információbiztonsági tudatosítása, képzése kiemelt helyet foglal el a vezetői elképzelések között. Hasonló mértékben fogalmazódott meg az informatikai infrastruktúra-fejlesztés szükségessége, de olyan elgondolkodtató véleményt is sikerült feltárni, amely a régi idők „zárt" biztonságtechnikai rendszerek előnyeire utalt vissza. Új és továbbgondolásra érett, nem vizsgált kockázatként fogalmazták meg a különböző, a börtönökben szolgáltatásokat ellátó külső cégek munkavállalóiban rejlő információbiztonsági fenyegetettséget.

Generációs különbségek megjelenése a vizsgálatban

A személyi állomány generációs különbségei az interjúkban több alkalommal befolyásoló tényezőként kerültek elő, az informatika alkalmazásával összefüggésben. Megállapítottuk, hogy a büntetés-végrehajtási szervezet elektronikus információbiztonságát és digitális kultúráját, valamint az informatikai dependenciát jelentősen befolyásolja a korosztályok átalakulása. Ismert tény, hogy az idősebb generációk általánosságban nehezebben boldogulnak az informatikával, kevésbé érzik szükségesnek azt. Ez az általános jelenség szintén vizsgálható a kutatás során gyűjtött adatokon. A korcsoportok viszonylatában a skálázott válaszok értékeinek átlagát vizsgáltuk a bizonyításhoz. Ez alapján megállapítható, hogy az idősebb korosztály (51 év felett) bár alacsony arányban van jelen a mintában (4%), a csoportba tartozó személyek átlagosan kevésbé gondolják fontosnak az általános kiberbiztonságot, így a bv. szervek kiberbiztonságát is. Az átlagnál alacsonyabbnak gondolják a vizs-

gált rendszerek alkalmazásának szintjét és annak zavaró mértékét egy bv. intézetre nézve (2. ábra).



2. ábra: Generációs különbségek

Forrás: a szerző szerkesztése

Megengedett leállás

Az interjúk során végrehajtott beszélgetésekben megjelent egy nem várt tényező, amely utólag értékelve – ha előzetesen beépítik – fontos vizsgálati elemként is szolgálhatott volna a kutatásban. Ez a tényező nem más, mint a vizsgált informatikai rendszerek leállásának időtartama. Számos válaszadó két részre osztotta válaszát, különbséget téve a „rövid" (körülbelül 1–3 óra) és „hosszabb" (minimum több nap) időtartamú leállás között. Az interjúválaszokból megállapítható, hogy a rendelkezésre állás szünetelésének időtartama befolyásolja az okozott hatások/károk mértékét. A dolgozók a rövid időtartamú (1–3 óra) leállás során fellépő nehézségeket képesek áthidalni, hiszen többször szembesültek már ilyen időtartamú informatikai leállással, így már van gyakorlatuk a nehézségek kezelésében. A hosszabb időtartam során jelölték meg a kockázatok megjelenését, azonban az is kiderült, hogy körülbelül 3–7 nap után képesek lennének visszatérni a teljes papíralapú munkavégzésre. Az így kapott intervallumból megállapítható, hogy az elektronikus fogvatartotti alapnyilvántartás esetében a megengedett leállás mértéke megközelítőleg 3 óra. Az ezt követő időszakban a fellépő kockázatok már károkat okozhatnak.

Összefoglalás és javaslatok

A kiberbiztonság a mai világban nélkülözhetetlenné vált, és annak valódi fontosságát leginkább azok ismerik fel, akik már személyesen megtapasztalták a kiberincidensek hatásait és az ezekkel járó kihívásokat. A kutatás legfőbb tanúsága, hogy a büntetés-végrehajtási dolgozók is érzik ezt a fontosságot, valamint a kiberbiztonság szerepét a börtönbiztonságban. Minden állami szervnek alaposan meg kell vizsgálnia és figyelembe kell vennie a kibertere jelentőségét, hiszen számos kockázatot kell kezelni ezen a téren. Minden intézménynek, ideértve a büntetés-végrehajtási szerveket is, kötelessége megvédeni az állampolgárok „kiberbizalmát". A digitális átalakulás hatással van a börtönök folyamataira, elkerülhetetlenül növekszik a digitális eszközök kapcsolata a személyi állománnyal, valamint a fogvatartottakkal is. A modernizáció következtében a börtönök biztonsága már a kibertéren keresztül is veszélyeztetetté vált, ami külföldi esetekkel és a feltárt eredmények tükrében igazolást nyert. Magyarországon a hazai börtönök történetében nem találunk olyan jelentős kibereseményeket, mint a külföldi példákban, de a tanulmány eredményei rámutatnak arra, hogy egy kibertámadás komoly zavarokat okozhat a hazai börtönökben. A büntetés-végrehajtási intézetek legfontosabb informatikai nyilvántartásának, az elektronikus fogvatartotti alapnyilvántartás bizalmasságának, rendelkezésre állásának és sértetlenségének megőrzése létfontosságú. Amennyiben ezek a jellemzők sérülnek, a fogvatartottak alapjogi érintettsége is előfordulhat, és ez akár kártalanítási eljárások alapjául is szolgálhat. Az információbiztonság és kiberbiztonság területén végzett kutatások és fejlesztések elengedhetetlenek ahhoz, hogy a büntetés-végrehajtási intézetek megfelelő védelmet érjenek el a kiberfenyegetésekkel szemben. A kiberbiztonság a börtönök stabilitásának és működésének alapvető elemévé vált, annak védelme hozzájárul a bv. szervek integritásához, így a társadalom védelméhez is.

A technológia folyamatos fejlődése és a kiberfenyegetések növekvő száma miatt a bv. szervezetnek fel kell készülnie az új kihívásokra, és folyamatosan frissítenie kell védelmi mechanizmusait. A korszerű informatikai infrastruktúra kiépítése, a szabályozási tevékenység fenntartása, a kibervédelmi felkészültség növelése, a személyzet információbiztonsági képzése és tudatosságának növelése is szükségletként fog jelentkezni a szervezeti kibervédelemben. Ezen túlmenően a bv. szervezetben a kiberbiztonságnak önálló, szervezeti szükségleten alapuló kiemelt prioritást kell kapnia, ezzel egyidejűleg speciálisan képzett, információbiztonsági és büntetés-végrehajtási szakismeretekkel egyaránt rendelkező szakemberek bevonása válhat szükségessé. A szabványosítás alkalmazása, mint az ISO 27000,[48] különösen az ISO 27001 és ISO 27002, kiváló alapot nyújtanak a büntetés-végrehajtási szervek számára az információbiztonsági irányítási rendszer (IBR) bevezetésére és fenntartására. Az ISO

[48] Az ISO (International Organization for Standardization) egy nemzetközi szervezet, amely világszerte elfogadott ipari és kereskedelmi szabványokat hoz létre.

27000 sorozat alkalmazása növeli a büntetés-végrehajtási szervek kibervédelmi képességeit, így hatékonyabban tudják védeni az általuk kezelt információkat és rendszereket a kibertámadások ellen. A jövőben esetlegesen bekövetkező kiberincidens okozta káros hatások minimalizálása, valamint a tevékenységfolytonosság biztosítása érdekében ajánlatos intézeti vagy agglomerációs szintű törzsfoglalkozás keretében kiberincidens témában szimulációs gyakorlatot végrehajtani, amely nagymértékben hozzájárulhat a vezetői és beosztott vezetői állomány incidenskezelési gondolkodásának kialakításához.

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, kiberbiztonági képzések számát növelni, azoknak speciális, büntetés-végrehajtási jelleget adni.[49] Fontos figyelembe vennünk azt a tényezőt, hogy az alapvető feladat-végrehajtás informatikai függőségének mértéke növekedhet a személyzet generációváltása következtében. A jövő börtönőrei, akik már az informatikai eszközök korszakában nőnek fel, kevésbé lesznek jártasak a hagyományos gyakorlatokban, ami komoly kihívásokat jelenthet a jövőbeli kiberincidensek hatásainak csökkentése terén. Ajánlatos lehet, hogy a személyi állományi tagok következő generációi ne távolodjanak el a hagyományos, technológia nélküli gyakorlatok ismeretétől. Ennek érdekében érdemes továbbra is oktatni a képzési tematikákban a hagyományos, papíralapú dokumentációk és gyakorlatok megismerését.

A bv. szervezetnek ajánlatos tovább növelnie kapcsolatát a releváns szervezetekkel, intézményekkel és szakmai közösségekkel, a megszerzett ismereteket felhasználva továbbra is naprakészen kell tartania aktuális szervezeti kiberpolitikáját. Ez magában foglalja a „börtönspecifikus" kibergondolkodás művelését, az ezzel összefüggő eljárások kidolgozását és végrehajtását. Az információbiztonság területe komplex és folyamatosan változó, ezért a szervezetnek dinamikusan kell reagálnia a világban tapasztalt kiberfenyegetési trendekre, továbbá a folyamatos, állandó felülvizsgálati tevékenység mellett, prediktív és proaktív szemlélettel úgy kell alakítania a sajátos jellemzőkkel tűzdelt digitális börtönbiztonságot, hogy az megszolgálja a társadalom kiberbizalmát.

[49] A büntetés-végrehajtási jelleg alatt az olyan speciális információbiztonsági kockázat tudatosítási tevékenységet kell érteni, amely kitér a személyi állományi tagok online adatkezelésének (pl. közösségi profilok) kiemelt kockázataira. A fogvatartottak vagy más személyek hozzáférhetnek a személyes adatokhoz, amelyeket felhasználhatnak arra, hogy nyomást gyakoroljanak a személyi állomány tagjára, valamint fenyegethetik annak családját, közeli perszonális kapcsolatait. Ellophatják a munkavállalók digitális személyazonosságát, és felhasználhatják arra, hogy másokat megtévesszenek, hamis információt terjesszenek, vagy akár bűncselekményeket is elkövethetnek.

Irodalomjegyzék

Bogotyán Róbert – Veszeli Dániel (2011): Bűnügyi nyilvántartás a büntetés-végrehajtásban: a múlt örökségének és a jelen kihívásainak hatása a közeljövő terveire. *Börtönügyi Szemle,* 30(3), 61–74.

BVOP (2021): *Soha nem látott mértékű fejlesztések a magyar börtönökben.* 2021. június 18. Online: https://bv.gov.hu/hu/intezetek/bvszervezet/hirek/4246

Cimpanu, Catalin (2020): Iran Reports Failed Cyber-Attack on Strait of Hormuz Port. *ZDNET,* 2020. május 11. www.zdnet.com/article/iran-reports-failed-cyber-attack-on-strait-of-hormuz-port/

Cimpanu, Catalin (2021): Cyber-Attack Disrupts Iran's National Railway System. *The Record,* 2021. július 10. Online: https://therecord.media/cyber-attack-disrupts-irans-national-railway-system/

Day, Olivia (2022): Port Phillip Prison: Melbourne Jail Targeted by Anonymous Hackers in Cyber Attack. *Daily Mail,* 2022. július 7. Online: www.dailymail.co.uk/news/article-10990551/Port-Phillip-Prison-Melbourne-jail-targeted-anonymous-hackers-sophisticated-cyber-attack.html

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. január 6. Online: www.documentcloud.org/documents/21176926-bernalillo-county-notice-of-emergency

ENISA (2022): *ENISA Threat Landscape 2022.* European Union Agency for Cybersecurity, 2022. november 3. Online: www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Fisher, Austin (2022): Jail's Inability to Deal with Cyberattack could Violate the Constitutional Rights of Inmates. *Source NM,* 2022. január 7. Online: https://sourcenm.com/2022/01/07/jails-inability-to-deal-with-cyberattack-could-violate-the-constitutional-rights-of-inmates/

Gholami, Niloofar (2022): A Look Inside Iran's Notorious Evin Prison. *DW,* 2022. október 22. Online: www.dw.com/en/irans-evin-prison-experience-was-psychological-torture-says-former-prisoner/a-63509722

Muha Lajos (2012): Kiberhadviselés – kiberbűnözés. In *IDC IT Security Konferencia.* Budapest, 2012. március 22.

Muha Lajos – Krasznay Csaba (2014): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/7135/Az%20elektronikus%20információs%20rendszerek%20biztonságának%20menedzselésejó.pdf?sequence=5&isAllowed=y

Taylor, Josh (2022): Staff at Security Firm G4S on Alert after Tax Numbers and Bank Details Posted Online Following Hack. *The Guardian,* 2022. október 4. Online: 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

Veszeli Dániel János (2017): A rendvédelmi szervek közötti automatizált információmegosztás és -elérés. *Belügyi Szemle,* 65(11–12), 93–117. Online: https://doi.org/10.38146/BSZ.2017.11-12.5

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

Jogforrások

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 L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
72/2020. (XII. 23.) BVOP utasítás a büntetés-végrehajtási szervezet Biztonsági Szabályzatáról

ABSTRACT

Cyber-Sensitivity of the Digital Culture of Hungarian Prison Service

Sándor BOTTYÁN

During the digital transformation that has been taking place in the Hungarian correctional service in recent times, lots of IT innovations have been implemented. The operation of the organization is increasingly linked to the digital space, so it has become important to examine the latest IT developments from a cybersecurity perspective. The study, in a ground-breaking manner, uses a scientific approach to examine the opinions of the employees of the Hungarian correctional service about cybersecurity and correctional cybersecurity. Furthermore, it reveals the extent of dependency between prison task performance and electronic information systems. In addition, the study reveals unexpected factors that may influence both the present and future of cybersecurity in Hungarian correctional services.

Keywords: *cyber-incident, cybersecurity, cyberattack, prison, information security*