HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

**Prisznyák Szabolcs**
prisznyak.szabolcs@bv.gov.hu

# A BVOP INFORMATIKAI KÖZPONTJÁNAK KOCKÁZATELEMZÉSE

***Absztrakt***

*A cikk bemutatja a büntetés-végrehajtási szervezetnél megvalósított informatikai fejlesztést. A centralizált rendszerek üzemeltetése során új kockázatok váltak ismertté. Ezt követően ismerteti a Büntetés-végrehajtás Országos Parancsnokságának informatikai központjára vonatkozó kockázatelemzést. Az elemzés az ISO/IEC 27005 (2008) szabvány előírásai szerint készült. A cikk végén összegzi a tapasztalatokat, továbbá ismerteti a szükséges fejlesztési lehetőségeket.*

*The article presents the IT-development at the Hungarian Prison Service. At the operational of centralized IT-system transpired several new risks. After then the author shows the risk analysis of headquarters of Hungarian prison system by ISO/IEC 27005 (2008) standard. The author concludes the article by summarising the experience gained and outlining the prospects for further development.*

***Kulcsszavak:*** *büntetés-végrehajtás, informatikai fejlesztés, információ-technológia, kockázatelemzés ~ prison service, IT-development, information technology, risk analysis*

## BEVEZETÉS

A büntetés-végrehajtási szervezet informatikai történetében mérföldkőnek számít a „Felelősen, felkészülten a büntetés-végrehajtásban” elnevezésű, EKOP-1.1.6-09-2009-0001 azonosítószámú, az Európai Unió támogatásával megvalósult informatikai fejlesztési projekt [1]. A projekt keretében közel 1,5 milliárd forint értékben megújult a büntetés-végrehajtási szervezet teljes informatikai rendszere. A fejlesztés azonban olyan rendszertechnológiai változásokat is magával hozott, amely újabb feladat elé állítja a szakembereket a nagy rendelkezésre állású központi informatikai üzemeltetés megvalósítása során.

Jelen publikációban bemutatom a megvalósított fejlesztés elemeit, illetve ismertetem, hogy ennek – és a változásokhoz illeszkedő logikai módosítások - eredményeként összességében milyen rendszertechnológiai, logikai változások következtek be [2]. Az erősen centralizálttá vált rendszer esetében kulcsfontosságú, hogy a Büntetés-végrehajtás Országos Parancsnokságának (BVOP) informatikai központja nagy rendelkezésre állással szolgálja ki a teljes szervezet információigényét. A rendelkezésre állás biztosításához szükséges felmérni a BVOP-n meglévő kockázatokat. A felmérés első lépéseként meghatároztam az informatikai rendszer működése szempontjából megvalósított funkció szerinti legmagasabb kockázatú helyiség, amely a BVOP központi gépterme. Ezt követően elvégezhető a helyiségre vonatkozó kockázatelemzés az IEC/ISO 27005 (2008) szabvány szerint. A kockázatelemzést jelen esetben kizárólag a központi gépterem esetében végzem el. A további helyiségek, helyiségcsoportok vizsgálata nem része jelen publikációnak.

Összképet adok a nagy rendelkezésre állást biztosító működés feltételeinek meglétéről, illetve ismertetem a szükséges fejlesztéseket.

A cikk elkészítéséhez feldolgoztam a témakörrel kapcsolatos tudományos publikációkat, valamint a kapcsolódó jogszabályokat. Az objektív kockázatelemzéshez figyelembe vettem Kerti András közleményében foglaltakat [3]. Tanulmányoztam a jelzett fejlesztés során keletkezett műszaki dokumentációkat. A több éves projektben, mint a BVOP informatikai fejlesztési osztályvezetője vettem részt. Ennek következtében munkám során fontosabb támasznak bizonyultak a megvalósítás és az üzemeltetés során szerzett személyes szakmai tapasztalatok.

## A BÜNTETÉS-VÉGREHAJTÁS SZERVEZETI FELÉPÍTÉSE

A büntetés-végrehajtás állami, fegyveres, rendvédelmi szerv, amely külön jogszabályban meghatározott szabadságelvonással járó, büntetéseket, intézkedéseket, valamint büntetőeljárási kényszerintézkedéseket, továbbá elzárást hajt végre [4].

A büntetés-végrehajtási szervezet kormányzati irányítását a Belügyminisztérium végzi. A szervezet központi vezető szerve a Büntetés-végrehajtás Országos Parancsnoksága, amely főosztályai révén a büntetés-végrehajtási intézetekben folyó szakmai munka felügyeletét, ellenőrzését végzi. A büntetés-végrehajtási intézetek ellátják a büntetések és intézkedések végrehajtásával kapcsolatos feladatokat. A büntetés-végrehajtás a legtöbb magyarországi közigazgatási és rendvédelmi szervezettől eltérően nem három, hanem kétszintű szervezet. A központi (országos) szervezet alárendeltségébe közvetlenül a területi jogállású szervezetek tartoznak.

Magyarországon 28 önálló jogállású büntetés-végrehajtási intézet, 5 – egészségügyi és oktatási – intézmény, valamint 11 gazdasági társaság működik. Az informatikai szakterület kompetenciája a gazdasági társaságokra nem terjed ki, azok a büntetés-végrehajtási szervezet informatikai rendszerétől független önálló, elszigetelt rendszereket alakítottak ki.

## A FEJLESZTÉS MEGVALÓSÍTÁSA

Az EKOP-1.1.6-09-2009-0001 informatikai fejlesztési projekt a büntetés-végrehajtási szervezet eddigi legnagyobb és legátfogóbb informatikai beruházása. Ha hálózatokról beszélünk, külön kell választani a helyi hálózatokat (LAN), és a táv-adatátviteli hálózatot (WAN). Az EKOP-1.1.6 projekt keretében a helyi hálózatok fejlesztésére volt lehetőség. A táv-adatátviteli (WAN) hálózatot külső – kormányzati – szolgáltató üzemelteti, ugyanis a 346/2010 (XII.28.) Kormányrendelet 3.§ (1) bekezdés értelmében „…kormányzati célú hírközlési tevékenységet kizárólag a kormányzati célú hírközlési szolgáltató és az elkülönült hírközlési tevékenység végzésére jogosultak végezhetnek.” [5]. A hivatkozott kormányrendelet nevesíti a kormányzati célú hírközlési szolgáltatót, amely a Nemzeti Infokommunikációs Szolgáltató Zrt.

A helyi hálózatok fejlesztésénél elsődleges cél volt a homogén aktív eszköz park kialakítása. Ennek értelmében valamennyi switch cserére került, az új eszközök azonos gyártónak a termékei. Végeredményben modern, szabványos helyi hálózatok álltak rendelkezésre, amelyek kialakítása szakszerűen, igényesen történt.

A szerverpark kialakítása során a BVOP-n – a már meglévő gépteremben, amelynek kialakítására 2007-ben került sor - egy blade centerben 10 db új szerver üzembeállításával történt a központi infrastruktúra kialakítása. Az intézetek részére összesen 128 db rack szekrénybe helyezhető szerver került beszerzésre. Ez intézetenként 4 db szervert jelent (a pályázat benyújtásának időpontjában működő 32 intézettel számolva).

Munkaállomás oldalon szintén a szerverekkel azonos gyártótól kerültek beszerzésre az eszközök. A projekt keretében összesen 1200 db vékonykliens, 300 db asztali munkaállomás, valamint a működésükhöz szükséges 1500 db LCD monitor illetve 100 db notebook került beszerzésre.

A fejlesztéssel elértük, hogy egységes szerver infrastruktúra áll rendelkezésre, amely konszolidált módon, valamennyi helyszínen klimatizált gépteremben került elhelyezésre. A munkaállomások nagy része cserére került, így a karakteres Unix terminálok helyett megjelentek a grafikus operációs rendszerek és felhasználói programok futtatására is alkalmas eszközök. Az azonos gyártótól származó eszközök biztosítják a homogenitást, interoperabilitást, a felcserélhetőséget, átcsoportosíthatóságot.

A rendelkezésre állást biztosító eszközcsoport részeként beszerzésre került valamennyi szerverpark mellé 1 db szünetmentes tápegység, amely áramkimaradás esetén – terheléstől függően – 5-15 percig képes a folyamatos működést biztosítani. Ez elegendő lehet a pillanatnyi áramkimaradások áthidalására, illetve hosszabb áramkimaradás esetén elegendő áthidalási időt biztosít az áramfejlesztő készülék (aggregátor) indulásáig. Egységes platformra került az intézeti adatmentés is, egy jó minőségű hálózati mentőegység beszerzésével, és üzembeállításával. Ez az eszköz elegendő a teljes intézeti adatvagyont növekményes mentésére, szükség esetén visszaállítására.

A BVOP-n pedig egy nagy teljesítményű áramfejlesztő berendezés került telepítésre, amely áramkimaradás esetén a központi gépterem mellett a telefonközpont, valamint a 24 órában üzemelő ügyeleti helyiségek informatikai és biztonságtechnikai eszközeit is képes kiszolgálni.

A szoftver alapinfrastruktúrát tekintve a korábbi heterogén működés felszámolásra került. Kialakítottuk az országos címtárat, amelyet Microsoft Active Directoryval valósítottuk meg. Valamennyi szerveren Microsoft Windows Server 2008R2 operációs rendszer fut. Munkaállomás oldalon a vastag klienseken Windows 7 Professional operációs rendszer és Microsoft Office 2010 irodai programcsomag került telepítésre. A vékonyklienseken egy speciális Linux típusú operációs rendszer – eLux RL Lite – fut, amelynek alapfunkciója, hogy RDP kliensként képes terminal szerverhez kapcsolódni. Fontos eredmény, hogy valamennyi adat és program központi tárolásúvá vált, így lehetőség nyílt az adatvagyon képzésre, ennek

redundáns tárolására, mentésére. Az állománystruktúra a büntetés-végrehajtási szervezet Szervezeti Működési Szabályzatnak [6] megfelelő hierarchia szerint került kialakításra.

Az alkalmazásfejlesztések során megvalósult a FŐNIX rendszer, amely a korábbi fogvatartotti alrendszer korszerűsítése, rendszertechnológiai megújítása, funkcionális bővítése.

Szintén megvalósult a humán erőforrás adminisztrációt támogató alrendszer korszerűsítése, funkcionális bővítése. Ez a rendszer egy általános személyügyi rendszer követelményein túl megfelel a büntetés-végrehajtási szervezet – jogszabályból következő [7] - speciális igényeinek is, ennek alapján a következő modulokból épül fel: személyügyi modul, szolgálatszervezési modul, fegyelmi modul, egészségügyi-, fizikai-, pszichikai állapotfelmérés nyilvántartása modul.

Mindkét rendszer esetében azonos a központban történő programfuttatás, adattárolás, valamint a szerepkörök szerinti differenciált hozzáférés, amelynek alapja az Active Directory.

## A BVOP HELYISÉGEINEK BESOROLÁSA FUNKCIÓK ALAPJÁN

A fejlesztés eredményeként a büntetés-végrehajtási szervezet teljes informatikai környezete megváltozott. A korábbi decentralizált szigetszerű informatikai rendszerek helyett egy erősen központosított megoldás került kialakításra. Az új megoldás egységes, homogén rendszer, azonban üzemeltetési szempontból kulcsfontosságúvá vált a BVOP informatikai központjának elérése. A minél nagyobb rendelkezésre állás biztosításához szükséges a BVOP kockázatelemzése az informatikai rendszer vonatkozásában. A kockázatelemzés során legcélszerűbb az IEC/ISO 27005 (2008) szabvány előírásait alkalmazni. A kockázatelemzés megkezdése előtt a BVOP helyiségeit az informatikai üzemeltetés szempontjából betöltött funkcióik szerint fel kell mérni, majd a rendszerben betöltött szerepük szerint csoportokba kell sorolni. Az informatikai rendszer működése, rendelkezésre állása szempontjából a legkritikusabb helyiség a BVOP központi gépterme. A további helyiségek csoportokba sorolása jelen publikációnak nem része.

A központi gépteremben az informatikai működés központja található, kiesése a büntetés-végrehajtási szervezet informatikai működését rövid időn belül ellehetetleníti.

## A BVOP KÖZPONTI GÉPTEREM KOCKÁZATELEMZÉSE

A kockázatok elemzését az ISO/IEC 27005 (2008) szabvány C függelékében foglalt „Leggyakoribb fenyegetések” alapján végzem [8]. Az elemzés rendszer szintű kockázatelemzés, bizonyos esetekben – amennyiben az szükséges – részletes kockázatelemzésre is sor kerülhet. Az egyes fenyegetések bekövetkezésének valószínűségét 1-5 skálán sorolom be, ahol a bekövetkezés legkisebb valószínűsége 1. Ezt követően ismertetem a környezeti tényezőket és/vagy a tett intézkedéseket. Amennyiben szükséges ismertetem a kockázatok valószínűségének és/vagy hatásának csökkentéséhez esetlegesen szükséges további intézkedéseket.

### Fizikai károk

- *Tűzkár:* bekövetkezés valószínűsége: 2. A helyiségnek megtörtént a tűzveszélyességi besorolása, a helyiségben éghető anyagok tárolása nem történik, a helyiség tűzálló ajtóval védett. A helyiségben automatikus oltóberendezés működik. További intézkedés nem szükséges.
- *Vízkár:* bekövetkezés valószínűsége: 1. Sem a helyiségben, sem a közvetlen környezetében – alatta, fölötte, mellette – nincs vízvezeték. A helyiségben nincs központi fűtés. A helyiség vízszint érzékelővel felszerelt, amely – a padozaton víz jelenléte esetén – riasztást végez. További intézkedés nem szükséges.

- *Szennyezés okozta kár:* nem releváns esemény, bekövetkezés valószínűsége: 1.
- *Berendezések megrongálódása, elvesztése:* bekövetkezés valószínűsége: 3. Az informatikai berendezések használat során tönkremehetnek, ennek ellensúlyozására a rendszerek szinte valamennyi esetben megfelelő redundanciával kerültek kialakításra, továbbá tartalék eszközök állnak rendelkezésre. Szükséges intézkedés: redundancia kialakítása valamennyi rendszer esetén.
- Por, rozsda, fagyás okozta károk: bekövetkezés valószínűsége: 1. A por és rozsda okozta károk nem releváns események. A fagyás valószínűsége is rendkívül alacsony, szükség esetén a redundáns klímaberendezések fűtésre is alkalmasak. További intézkedés nem szükséges.

### Természeti esemény

- *Éghajlati jelenség*: Magyarország éghajlata kontinentális, szélsőséges éghajlati jelenségek előfordulása nem jellemző, így a kockázat nem releváns.
- *Szeizmikus jelenség:* Magyarországon a szeizmikus jelenségek (földrengések) nem jellemzőek, így a kockázat nem releváns.
- *Vulkanikus jelenség:* Magyarország területén nincs működő vulkán, a kockázat nem releváns.
- *Meteorológiai jelenség:* bekövetkezés valószínűsége: 1. A meteorológiai jelenségek közül a villámcsapás, amely lehetséges fenyegetés, ellene az épület villámvédelmének kiépítésével védekezünk, amely megfelelő műszaki színvonalon megoldott. További intézkedés nem szükséges.
- *Árvíz okozta károk:* bekövetkezés valószínűsége: kevesebb, mint 1. Az árvíz nem releváns fenyegetés, mert a BVOP épülete magasabban fekszik, mint a legmagasabb mért árvíz plusz egy méter, nagyon alacsony kockázati tényezőt jelent, hogy az épület a Dunától kb. 150 méter távolságra található, így esetleges kockázatot jelenthet egy árvíz másodlagos hatása. További intézkedés nem szükséges.

### Kulcsfontosságú szolgáltatás kiesése

- *Légkondicionáló vagy a vízvezeték rendszer meghibásodása okozta kár:* bekövetkezés valószínűsége: 2. A vízvezetékrendszer meghibásodása nem releváns az informatikai rendszer működése szempontjából. A gépterembe 2013-ban új légkondicionáló berendezések kerültek telepítésre. A berendezések rendszeresen ellenőrzöttek karbantartottak. Két berendezés működik párhuzamosan, egyik kiesése esetén a tovább működő egység képes biztosítani a megfelelő működési hőmérsékletet. További intézkedés nem szükséges.
- *Áramellátás hibája (áramszünet):* bekövetkezés valószínűsége: 3. A BVOP épülete a múlt század elején épült, villamosítása az 1940-es, 1950-es években történhetett, azóta csak egyes szakaszok újjáépítése, javítása, bővítése történt meg. Az épület teljes elektromos felújítására évtizedek óta nem került sor. A kockázatot tovább növeli, hogy a belvárosban az épület környékén több nagy volumenű ingatlanfejlesztés is zajlik, és az építkezések során több esetben előfordul figyelmetlenségből vagy a megfelelő műszaki dokumentumok hiányából adódó vétlen nagyfeszültségű vezetékrongálás, amely áramkimaradást eredményezhet. A kockázatot csökkenti, hogy az informatikai központ teljes nagyfeszültségű kábelrendszere megújításra került, a BVOP épületének további rendszeritől függetlenítve. Beszerzésre került egy szünetmentes tápegység, amely a központi géptermet ellátja. Szintén beszerzésre került egy nagy teljesítményű áramfejlesztő berendezés (aggregátor), amely áramkimaradás esetén is biztosítja a központi gépterem áramellátását. További szükséges intézkedések: szünetmentes tápegység kapacitásának növelése.

- *Telekommunikációs berendezések meghibásodása:* bekövetkezés valószínűsége: 3. A telekommunikációs berendezések a BVOP telefonközpont rendellenes működéséből következhetnek. A telefonközpont redundáns. Meghibásodás esetén a tartalékegység (amely egy büntetés-végrehajtási intézetben található) automatikusan átveszi a vezérlést. További szükséges intézkedések: a telefonközpont teljes és alapos felülvizsgálata az üzemeltető NISZ Zrt. által a hibás működés esetszámának csökkentése érdekében. A redundancia logikájának felülvizsgálata, az automatikus folyamatok üzembiztos működésének kialakítása érdekében (jelenleg a rendellenes működést követő helyreállítás legtöbb esetben manuális beavatkozást igényel).

### Sugárzás miatti zavar

- *Elektromágneses sugárzás okozta kár:* a kockázat nem releváns.
- *Hő sugárzás okozta kár:* a kockázat nem releváns.
- *Elektromágneses impulzus okozta kár:* nem releváns.

### Információ kompromittálódás

- *Kompromittáló kisugárzott jelek elfogása*: a bekövetkezés valószínűsége: 1. A BVOP nem alkalmaz vezeték nélküli eszközöket. A gépterem az épület belső részén helyezkedik el. Az ingatlan területére ellenőrzötten, dokumentáltan történik a beléptetés. A múlt századi építészeti megoldások következtében a 80-100 cm-es falvastagság is csökkenti a jelfelderítés valószínűségét. További intézkedés nem szükséges.
- *Távoli kémkedés okozta kár*: a bekövetkezés valószínűsége: 1. A BVOP a kormányzati hálózat része, amelyet a NISZ Zrt. üzemeltet. A hálózat a távoli behatolás ellen több szintű logikai és fizikai védelemmel ellátott. További intézkedés nem szükséges.
- *Lehallgatás okozta kár:* a bekövetkezés valószínűsége: 1. A lehallgatáshoz a hálózatra fizikailag kell rácsatlakozni. Az épület fent ismertetett védelme jelentősen csökkenti a kockázatot. További intézkedés nem szükséges.
- *Média (adathordozó) vagy dokumentumok ellopása:* a bekövetkezés valószínűsége: 2. A kockázatot elsősorban a saját dolgozók jelentik. Az épületbe, az informatikai helyiségekbe a belépés korlátozott. Az adathordozók biztonságosan tároltak (lemezszekrény, páncélszekrény). A dolgozók tájékoztatása, oktatása megtörtént. További szükséges intézkedések: Az informatikai biztonsági oktatások számának növelése, rendszeressé tétele, a megszerzett ismeretek ellenőrzése. A dolgozókban a felelősségtudat kialakítása.
- *Berendezések ellopása: a bekövetkezés valószínűsége: 2*. A tett és a szükséges intézkedések azonosak a fenti pontban megfogalmazottakkal.
- *Kidobott, újrafelhasznált média (adathordozó) helyreállítása:* a bekövetkezés valószínűsége: kevesebb, mint 1. Minden használatból kivont adathordozó esetében adat helyreállítást lehetetlenné tevő roncsolásra kerül sor. További intézkedés nem szükséges.
- *Árulás, információk közzététele:* a bekövetkezés valószínűsége: 2. A dolgozók felkészítése, oktatása megtörtént. További szükséges intézkedés: további rendszeres oktatások a dolgozók részére, a tudatos magatartás kialakítása.
- *Megbízhatatlan forrásból származó adat:* a bekövetkezés valószínűsége: 2. A rendszerbe kerülő adatok ellenőrzöttek, hiteles forrásból származnak. Nem megfelelő adat csak tévedésből vagy szándékosan kerülhet a rendszerbe. További szükséges intézkedések: tudatos magatartás kialakítása oktatással.

- *Hardverek működésének befolyásolása*: a bekövetkezés valószínűsége: 2. A központi gépteremben található hardverekhez csak a kijelölt állomány férhet hozzá. További szükséges intézkedések: tudatos magatartás kialakítása oktatással.
- *Szoftverek működésének befolyásolása:* a bekövetkezés valószínűsége: 2. A központi rendszeren futó szoftverek logikailag és fizikailag is védettek. A szoftverekhez csak a kijelölt állomány férhet hozzá. A BVOP megfelelő vírusvédelemi rendszerrel rendelkezik, a vírusinformációs állomány frissítése rendszeres és automatikus. Minden szoftverelem csak előzetes tesztelés után kerül telepítésre. Problémát jelenthetnek a nem a BVOP állománya által felügyelt szoftverek.További szükséges intézkedések: tudatos magatartás kialakítása oktatással. A vírusvédelmi rendszer rendszeres ellenőrzése. A külső – szoftvereket telepítő, üzemeltető – partnerek esetében a megfelelő együttműködés kialakítása.
- *Pozíció (hely) kinyomozása*: a bekövetkezés valószínűsége: 1. A BVOP elhelyezkedése ismert, nyilvános információ, de ebből nem következik egyenesen a központi gépterem elhelyezkedése. A kockázatot csökkenti az épület védelme, a ki- és beléptetés szabályrendszere, annak betartása. További intézkedés nem szükséges.

### Technikai meghibásodás

- *Eszközök, berendezések meghibásodása*: a bekövetkezés valószínűsége: 2. Az informatikai eszközök, berendezések használatuk során meghibásodhatnak, ennek kezelésére a központi rendszer elemei szinte valamennyi esetben megfelelő redundanciával kerültek kialakításra, továbbá tartalék eszközök állnak rendelkezésre. Szükséges intézkedés: redundancia kialakítása valamennyi rendszer esetén, a rendelkezésre állás további növelése.
- *Üzemzavar, hibás működés:* a bekövetkezés valószínűsége: 2. A fenti pontban megfogalmazottakkal azonos intézkedések történtek és szükségesek.
- *Információs rendszer telítettsége:* a bekövetkezés valószínűsége: 1. A rendszer folyamatosan ellenőrzött, mind automatikusan, mind humán erőforrás bevonásával. Szükség esetén a rendszerek automatikus megelőző figyelmeztetést küldenek. További intézkedés nem szükséges.
- *Szoftverek hibás működése:* a bekövetkezés valószínűsége: 2. A központi rendszeren futó szoftverek logikailag és fizikailag is védettek. A BVOP megfelelő vírusvédelemi rendszerrel rendelkezik, a vírusinformációs állomány frissítése rendszeres és automatikus. Minden szoftverelem csak előzetes tesztelés után kerül telepítésre. Problémát jelenthetnek a nem a BVOP állománya által felügyelt szoftverek. További szükséges intézkedések: A vírusvédelmi rendszer rendszeres ellenőrzése. A külső – szoftvereket telepítő, üzemeltető – partnerek esetében a megfelelő együttműködés kialakítása.
- *Az információs rendszer helyreállíthatóságának megsértése:* a bekövetkezés valószínűsége: 2. Az adatbázisokról, adatállományokról rendszeres, automatikus, több generációs mentéssel rendelkezünk. A mentések megfelelő helyen őrzöttek. Szükséges intézkedések: mentési rendszer kialakítása távoli telephelyre.

### Illetéktelen cselekedetek

- *Illetéktelen eszközhasználat*: a bekövetkezés valószínűsége: 2. Az eszközök be- és kivitele az épületbe történő be- és kiléptetés során ellenőrzésre kerülnek. A gépterembe történő belépés korlátozott. Az eszközök hálózatra csatlakoztatása sem lehetséges a fizikai címre (MAC address) történő szűrés alapján. Egyes esetekben kockázatot jelenthet az USB alapú eszközök használata. Szükséges intézkedések: az USB alapú

eszközök egyedi azonosító alapján személyekhez rendelt módon történő központi felügyeletének kialakítása.

- *Szoftverek illegális másolása*: nem releváns esemény, bekövetkezés valószínűsége: 1

- *Hamis szoftverek használata*: nem releváns esemény, bekövetkezés valószínűsége: 1
- *Adatok elrontása (meghamisítása):* a bekövetkezés valószínűsége: 2. A rendszerbe kerülő adatok ellenőrzöttek, hiteles forrásból származnak. Nem megfelelő adat csak tévedésből vagy szándékosan kerülhet a rendszerbe. További szükséges intézkedések: tudatos magatartás kialakítása oktatással.
- *Illegális adathasználat (adatfeldolgozás)*: fentivel azonos.

### Funkció kompromittálódása

- *Használat közbeni hiba*: a bekövetkezés valószínűsége: 3. A központi rendszer elemei szinte valamennyi funkciót tekintve redundánsak, illetve szükség esetére tartalék eszköz, alkatrész áll rendelkezésre. További szükséges intézkedések: újabb redundáns megoldások kialakításának folyamatos vizsgálata.
- *Jogokkal való visszaélés*: a bekövetkezés valószínűsége: 2. A jogosultsági rendszer úgy került kialakításra, hogy minden felhasználó csak a munkavégzéséhez szükséges jogosultsággal rendelkezik. További szükséges intézkedések: tudatos, felelősségteljes magatartás kialakítása oktatással, ellenőrzéssel.
- *Jogokról való megfeledkezés*: a bekövetkezés valószínűsége: 2. Fentivel azonos kockázat és intézkedések.
- *Tevékenység megtagadás*: a bekövetkezés valószínűsége: 1. A szervezet jellegéből adódóan nem releváns kockázat. További intézkedés nem szükséges.
- *Személyes hozzáférés megakadályozása*: a bekövetkezés valószínűsége: 1. Több személy is rendelkezik rendszerfelügyeletet és rendszerkonfigurációt biztosító jogosultságokkal. A rendszerek jól dokumentáltak. Amennyiben fizikai hozzáférési probléma történik (pl. elromlik a központi gépterem ajtajának zárja és az nem nyitható), annak kijavításáig távoli adminisztrációval biztosítható a rendelkezésre állás. További intézkedés nem szükséges.

## ÖSSZEGZÉS

Az EKOP-1.1.6-09-2009-0001 informatikai fejlesztési projekt a büntetés-végrehajtás történetének eddigi legnagyobb informatikai fejlesztése. Ebből következően – mivel az informatika szinte valamennyi munkafolyamat támogatásában érintett – döntően befolyásolja a szervezet működését. A fejlesztés rendszertechnológiai változásokat is magával hozott, amelynek következtében megváltoztak az informatikai rendszer működésének, elérésnek feltételei is.

Az új – erősen centralizált – környezetben kulcsfontosságú, hogy a központi rendszer a lehető legnagyobb rendelkezésre állású legyen. A rendelkezésre állás biztosításához, növeléséhez elengedhetetlen a teljes rendszer, illetve annak egyes elemeinek a felülvizsgálata. Az egyes kockázatok elemzéséhez, a kockázatok bekövetkezési valószínűségének csökkentéséhez, illetve a bekövetkezett események hatásának csökkentéséhez megtett és a jövőben szükséges intézkedések meghatározásához a nemzetközileg elfogadott ISO/IEC 27005 (2008) szabványt választottam.

Bízom benn, hogy elemzésem eredményeként rávilágítottam a fejlesztendő területekre, és felszínre kerültek olyan problémák is, amelyek a szabvány következetes – pontról pontra – történő alkalmazása nélkül csak egy már bekövetkezett esemény után derültek volna ki.

Véleményem szerint a kockázatelemzés eredményét és módszerét célszerű figyelembe venni más rendvédelmi (és/vagy közigazgatási) szervezet hasonló volumenű informatikai fejlesztése, vagy a meglévő rendszerek vizsgálata során. A szabványban meghatározott elvek és módszerek alkalmazásával magasabb rendelkezésre állású, biztonságosabban üzemeltethető informatikai infrastruktúrák alakíthatók ki.

## Felhasznált irodalom


[1] SEBESTYÉN Attila: Büntetés-végrehajtás informatikai fejlesztési projekt. = Kommunikáció 2009, 2009 Zrínyi Miklós Nemzetvédelmi Egyetemi Kiadó - ISBN 978-963-7060-70-0

[2] A büntetés-végrehajtás országos parancsnokának 1-1/13/2011.(III. 22.) OP intézkedése a büntetés-végrehajtási szervezet informatikai biztonsági szabályainak kiadásáról

[3] KERTI András: Az információbiztonsági kockázatkezelés oktatásának buktatói = Kommunikáció 2013: Communications 2013, 2013 Nemzeti Közszolgálati Egyetem, pp. 53-60. - ISBN:978-615-5305-16-0

[4] 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről

[5] 346/2010 (XII.28.) Kormányrendelet a kormányzati célú hálózatokról 3.§ (1)

[6] A büntetés-végrehajtás országos parancsnokának 1/2011. (V.6.) BVOP utasítása a Büntetés-végrehajtás Országos Parancsnoksága Szervezeti és Működési Szabályzatának kiadásáról

[7] 1996. évi XLIII. törvény a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról

[8] International Standard ISO/IEC 27005 Information technology – Securtity techniques – Information security risk management