HADMÉRNÖK

VII. Évfolyam 2. szám - 2012. június

Horvayné Fehér Judit
feherjenator@gmail.com

A RENDŐRSÉGI INFORMATIKAI HÁLÓZATOK FENYEGETÉSEI

Absztrakt

Minden olyan tevékenység mely az informatikai hálózati szolgáltatást, rendőrségi informatikai tevékenységének biztonsági szintjét alkotja és fenntartja, meghatározza az informatikai hálózat biztonság helyzetét, mely lehet személyi, szolgáltatási vagy tárgyi vonatkozású. Ezen tevékenységek ilyen sarkalatos szegmenseként értelmezem a veszélyhelyzeteket, az informatikai hálózatot érő fenyegetéseket, és azok elleni védekezések meghatározása érdekében megfogalmazott kérdések körét. Jelen publikáció összegzi a rendőrség informatikai hálózatának biztonságát veszélyeztető fenyegetéseket.

Every kind of activity, creating and supporting the it-network service and the security level of it-activity of police, is determining the situation of the it-network security, concerning to the personal, service or object level. I mean ont he cardinal segment of these activities the jeopardy, the threats againts the it-network and the conceive of the questions of the protection. Present publication is summarizing the expected threats, affecting the police information-technological (it) networks.

Kulcsszavak: *rendőrségi informatikai hálózat biztonsági veszélyhelyzet, informatikai hálózat fenyegetései ~ security jeopardy of police it-network, threats against it-network*

BEVEZETÉS

„A fenyegetettség olyan művelet, vagy esemény, illetve ezek hiánya, amely sértheti az információs rendszer védettségét, biztonságát.”[1]

A fenyegetettség tekintetében a rendőrség informatikai hálózatát a nagy vállalatok informatikai hálózatához hasonlónak tekintem. Ezért azt gondolom, hogy hasonló más, az Internetre csatlakozó informatikai hálózatokhoz. Kutatásokat végeztem mind nemzetközi területen mind hazai területeken a nagy hálózatok érő fenyegetések és támadások előfordulásainak- megjelenésük tekintetében. Ennek érdekében a 2012-es évi nemzetközi területeken megjelenő, informatikai biztonsági területet érintő jelentéseket vetettem össze. Megvizsgáltam a hazai nagyvállalati információbiztonságot veszélyeztető jelenségeket vizsgáló szervezetek jelentésekeit és összehasonlítottam egymással. A jelentések értékeléséből következtetéseket vontam le és megjelenési formáit kerestem a rendőrségi informatikai hálózatok fenyegetettségei tekintetében. Ahhoz, hogy ezen kérdésköröket és fenyegetéseket csoportosítani tudjam, továbbá jellemzőjüket határozzam meg, kockázatelemzéseket kell lefolytatnom.

„A kockázat a fenyegetettség mértéke, amely valamely fenyegető tényezőből ered. A kockázat mértéke, a kárnagyság és a bekövetkezési valószínűség (gyakoriság) szorzata.”[1]
„A kockázatelemzés olyan elemző és értékelő jellegű szakértői vizsgálat, amely az informatikai rendszerekben kezelt adatok és alkalmazások értékelése, gyenge pontjainak és fenyegetettségeinek elemzése útján meghatározza a potenciális kárértékeket és azok bekövetkezési gyakoriságát.”[1]

A kockázatelemzéshez elsődlegesen kockázatbecslést és fenyegetettség elemzést kell végezni, mely lépésinek és fontos mérföldköveinek meghatározásához felhasználtam a Magyar Informatikai Biztonsági Ajánlások közül, a KIB 25. számú Ajánlását a 25/1-3. kötet „Az Informatikai Biztonság Irányításának Vizsgálata”-át. A vizsgálat nyomán a kockázati tényezőket, szegmenseket, továbbá a feltételezhető károkat vettem sorra. Ezeket összevetve a hazai és nemzetközi jelentésekkel, meghatározom a rendőrség informatikai hálózatát várható fenyegetések sarkalatos pontjait, a feltételezhető támadásait, azok hatásait és az azokra történő reakciókat.

I. NEMZETKÖZI ÉS HAZAI TAPASZTALATOK INFORAMTIKAI HÁLÓZATOK FENYEGETETSÉG VIZSGÁLATA TERÜLETÉN

„Az internet alapú támadások sajátos jellegei önmaguk megmagyarázzák azoknak gyakoriságát és hatását. Az internet lehetővé teszi a nagy távolságokról történő támadásokat, amely magasabb fokú anonimitást és védelmet biztosít az elkövető számára. Ez a sajátosság csökkenti a jogszabályok hatékonyságát is. Számos esetben a támadásokat a nemzeti határokon túlról intézik … a bekövetkezett hatás nincs összefüggésben a támadó rendelkezésére álló erőforrásokkal. Figyelembe veendő, hogy az előre megírt, automatizált támadási eszközök egyre szélesebb körben elérhetőek az interneten, s olyan személyek által is használhatóvá válnak, akik nincsenek tisztában magával az eszközzel vagy a hatásukkal” [2; 220.o.]

Nemzetközi szakirodalmak közül megvizsgáltam a CSI és az FBI által készített jelentések Puskás Tivadar Alapítvány által készített kivonatait, és megállapítottam, hogy a támadások többsége a belső hálózatról származtatható. Elégedetlen alkalmazottak, belső kémek, látogatók, vendégek, hibás teszt szoftverek, hosztok, amelyek vírusokkal és férgekkel fertőzik a hálózatot, és képzetlen felhasználók alkotják az ilyen jellegű támadások potenciális forrását. A hálózatbiztonság tervezése során figyelembe kell venni a potenciális belső fenyegetéseket. [3; 26-29.o.]

A nemzetközi tapasztalatok összegzéseként elmondható, hogy a nyilvánosan címezhető hosztok, amelyek az Internetre vagy az extranet hálózatokon kapcsolódnak nagy valószínűséggel alkalmazás rétegbeli támadások várhatók, melyek privilegizált hozzáférés szerzésére irányulnak, vagy DoS támadáshoz vezetnek, melyek egyértelműen a rendszer üzembiztonságát fenyegetik. [3; 26-29.o.]

További tapasztalatként elmondható, hogy egy hacker megpróbálhat ún. war-dialer alkalmazásokon keresztül hálózati hozzáférést szerezni, úgy hogy az adatkapcsolati telefonszámokat szerzi meg. A war-dialer alkalmazások vagy hardverek működésének alapja, hogy számos telefonszámot felhívnak és megállapítják az azok mögött található rendszerek típusát. A személyes felhasználásra szánt távfelügyelet szoftverek vannak leginkább kitéve az efféle támadásoknak, mivel ezek tipikusan nem túl biztonságosak. Mivel az ilyen eszközök általában tűzfal mögött helyezkednek el, amennyiben egy hacker hozzáférést szerez a betárcsázás során, belső felhasználó szerepkörében tud feltűnni a belső hálózaton.

A vezeték nélküli technológiák (WLAN) megjelenésével számos új fenyegetés típus jelent meg. Az ún. war-driving egyre népszerűbb a hackerek közt. Egy wireless kártya és egy sniffer alkalmazás segítségével a hacker könnyedén hozzáférhet a vállalati információkhoz, és belső jogosultságokat szerezhet.

A DSL technológia, és más nagy sávszélességű permanens kapcsolatok térhódításának köszönhetően a vállalati környezet a dolgozók távmunka környezetivel, otthoni irodai környezetekkel bővültek. Az ilyen helyszíneken található munkaállomások ugyanazon fenyegetéstípusoknak vannak kitéve, mint a vállalati hálózaton belüliek, viszont biztonsági szempontból azonos módon kezelendőek.

„A kibertámadások évről évre világszerte több százmilliárd dollárnyi kárt okoznak a szervezeteknek és magánszemélyeknek. A brit NCC csoport február elején közzétett kutatási eredményei szerint tavaly a legtöbb hackerakciót – az összes támadás 40%-át – az Egyesült Államokból és Kínából indították, s ezek összesen több mint 44 milliárd dollár kárt okoztak a világgazdaságban. Hollandia, Franciaország, Dánia és Németország követi a két éllovast a sorban. Ezekből az országokból összesen csaknem 200 millió támadás indult ki – a számított kárérték 16 milliárd dollár.”[3; 31.o.]

„Március végén az amerikai Szenátus illetékes szakmai bizottságának meghallgatásán James Peery, a Sandia National Laboratories információs rendszer-elemző központjának igazgatója így nyilatkozott: „Nem hinném, hogy a kémeket határainkon kívül tarthatjuk. Mostani kiber háborús modellünkben olyan rendszerben gondolkodunk, amelyet nem érhet támadás... Rossz megközelítés. ... Szerintem a modellnek abból a feltételezésből kell kiindulnia, hogy az ellenség bent van a hálózatunkban. Ott van a gépeinken, és nekünk ilyen körülmények között is dolgoznunk kell.” Az amerikai védelmi minisztérium 15 ezer hálózaton mintegy hétmillió számítástechnikai eszközt működtet. Egy ilyen komplex rendszert tökéletesen megvédeni gyakorlatilag lehetetlen – magyarázta hallgatóságának a szakember.”[3; 31.o.]

„Az amerikai Nemzetbiztonsági Hivatal (National Security Agency) igazgatója mégis Kínára mutatott, amikor a negyedév végén az egy esztendővel korábban az RSA ellen elkövetett, nagy port kavart kiber betörésről beszélt. (Mint emlékezetes, az RSA-tól elemelt biztonsági kóddal nem sokkal később a Lockheed Martin katonai óriás ellen kíséreltek meg támadást.) Január közepén pedig arról érkeztek hírek, hogy kínai hackerek egy trójai segítségével olyan chipkártyákat törtek fel, amelyeket számos amerikai kormányzati épület beleptető rendszerében alkalmaznak.” [3; 32.o.]

„Ugyancsak Kínából indult ki a jelek szerint az a jól szervezett, márciusi akció, amelynek tettesei hamis Facebook oldalt nyitottak James Stavridis tengernagynak, a NATO európai főparancsnokának nevében. A főtisztről közismert, hogy aktívan kommunikál a közösségi

hálózaton. A támadók nyílván abban bíztak, hogy az ál-oldallal lépre csalt látogatok révén további, kémkedésre felhasználható bizalmas információkhoz juthatnak." [3; 32o.]

„Állítólagos szaúdi hackerek azzal kérkedtek, hogy izraeli site-okról mintegy 400 ezer izraeli polgár személyi adatait, köztük bankkártya-információit emeltek el. Az illegális adatgyűjtés ténye beigazolódott, ám az áldozatok valós száma izraeli források szerint „csupán" 14 ezer volt. Utóbb az is felmerült, hogy esetleg nem is szaúdi csoport, hanem az Egyesült Arab Emirátusok egy Mexikóban elő ifjú állampolgára fejezte ki íly módon Izrael-ellenes érzelmeit. Mindenesetre a zsidó állam külügyminiszter-helyettese, Danny Ayalon terrorcselekménynek minősítette az arab akciót, s megtorlással fenyegette az elkövetőket. Ám az első válaszcsapást ő maga szenvedte el: személyes site-ját feltörték és rövid időre egy iszlám lapra irányították át. Nem kellett sokat várni az izraeli hackertársadalom bosszújára: Egy Hannibal fedőnevű kiberlovag azt állította, hogy 100 ezer arab Facebook belépőjét tette közzé." [3; 32o.]

A Magyarországi Nemzeti Hálózatbiztonsági Központ által készített jelentések alapján hazai eseményeket vizsgáltam meg a magyarországi informatikai fenyegetésekről. Összevetettem a Puskás Tivadar Alapítvány és a Virus Buster Kft. 2012-es évi első negyedéves jelentését az elmúlt évben jelentkező támadásokról és fenyegetésekről.

Két területet vizsgáltam, az Internet biztonsági incidenseket és a szoftver sérülékenységeket. „Internet biztonsági incidens minden olyan biztonsági esemény, amelynek célja az információs infrastruktúrák bizalmasságának, sértetlenségének vagy rendelkezésre állásának megsértése az Interneten, mint nyílt információs infrastruktúrán keresztül."[3; 5.o.]

A Puskás Tivadar Alapítvány jelentése szerint az első negyedévben 124 db incidens bejelentést regisztrált és kezelt, ebből 71 db alacsony és 53 db közepes kockázati besorolású volt.

A bejelentések többnyire külföldi partner szervezetektől érkeztek és több mint 90%-ban hazai káros tevékenységgel vagy káros tartalommal voltak összefüggésben. Összesen 52 db szolgáltató került bevonásra az egyes incidensek kezelése során és összesen 542 db szálon folyt incidenskezelési koordináció.[3; 5.o.]

A 2012-es év első negyedéves incidens kimutatását közel 50%-os arányban a botnet hálózatok által megfertőzött számítógépek kapcsán fogadott bejelentések vezetik, még úgy is, hogy ezek az adatok nem tartalmazzák Shadowserver Foundationtől beérkező bejelentéseket. [3; 5.o.]

Továbbra is nagy számban érkeztek a felhasználók megtévesztésén alapuló, a banki és egyéb bejelentkezési adatok megszerzését célzó, adathalász tevékenységekkel kapcsolatos bejelentések, melyek az incidensek 25%-át teszik ki. A relatív számosságukat tekintve ezek ugyan nem kiemelkedőek, de egy-egy incidens kapcsán több száz kompromittált felhasználó adatairól is beszélhetünk egyszerre. Az ilyen jellegű incidensek nem csak az adatszivárgás szempontjából érdekesek, hanem olyan szempontból is, hogy a megszerzett információk, hogy jutottak a támadók birtokába. Ezért az ilyen esetek kapcsán számba kell, vennünk legalább egy esetleges sérülékeny szoftver vagy a felhasználó eszközeire települt káros szoftver jelentette kockázatokat is. [3; 3-4.o.]

A fennmaradó 25% főként a kártékony szoftverek, az elosztott szolgáltatás-megtagadásos támadások, valamint a kompromittált felhasználói adatok kapcsán érkezett incidens bejelentésekből tevődik össze. Ez utóbbi esetén érdemes megjegyezni, hogy bár ezek az incidensek a bejelentések mindössze 8%-át adják, az érintettek nagyszáma miatt ezen bejelentések kezelése az incidenskezelési koordináció közel 20%-át teszik ki. [3; 3-4.o.]

A Magyarországi Nemzeti Hálózatbiztonsági Központtól februárban megtudhattuk, hazánkban is 900 ezer körül jár azoknak a száma, akik elszenvedtek már valamilyen számítógépes bűncselekményt. A közvetlen anyagi kár 7 milliárd forint, és további 14 milliárd forintra becsülik a kiesett idő értéket. Természetesen a világon mindenhol vannak,

lehetnek pénzben ki nem fejezhető károk is. Ezen értékek felmérésében nyújt segítséget a Hétpecsét Információbiztonsági Egyesület, és 2008-óta a Budapesti Rendőr-főkapitányság számítógépes bűnözéssel foglalkozó alosztálya. [3; 31.o.]

A Magyarországi Nemzeti Hálózatbiztonsági Központ szerint szoftver sérülékenység tekintetében 454 db szoftver sérülékenységi információt publikáltak, amelyekből 210 db alacsony, 135 db közepes, 99 db magas és 10 db kritikus kockázati besorolású volt. [3; 31.o.]

KOCKÁZATBECSLÉS

A rendőrség informatikai hálózatainak fenyegetettség vizsgálatához szükségesnek tartottam a kockázat felmérést. Ehhez meg kellett vizsgálni a kockázatkezelési metódusaikat.

A kockázatkezelés sarokköve a kockázatok felmérése, becslése, mely folyamat során a szervezet meghatározza egy adott rendszerre, annak egész élettartamára vonatkozóan a kockázat szintjét. E folyamat eredménye a maradványkockázat és a döntés, hogy vajon ez a kockázati szint elfogadható-e, vagy további biztonsági óvintézkedéseket kell megvalósítani a kockázat további csökkentésére.

„A kockázat függvénye annak a valószínűségnek, hogy egy biztonsági esemény bekövetkezik, valamint annak a kihatásnak, melyet ez az esemény okoz a szervezet feladatainak megvalósítására. A valószínűség meghatározására a rendszert fenyegető veszélyeket elemezzük a meglévő sebezhetőségekkel összefüggésben. A kihatást az határozza meg, hogy milyen következményeket jelent a szervezet feladatait illetően.”[1]

E folyamat végig viteléhez a KIB 25. számú Ajánlását, a 25/1-3. kötetéből „Az Informatikai Biztonság Irányításának Vizsgálata”-át választottam, és az iránymutatások közül a kockázatkezelés eljárását.

A kockázatbecslés 9 lépésből áll, mely során, meg kell határozni az informatikai hálózat, mint rendszer leírását. A leírás során részletesen ki kell térni az informatikai hálózat határaira, valamint az informatikai hálózatot alkotó erőforrásokra, adatokra, az alábbi besorolás szerint:

- „információ infrastruktúra,
- hardver és szoftver,
- adatok és információ,
- emberek,
- informatikai hálózati interfészek és kapcsolatok.”[4; 176.o.]

Tekintettel arra, hogy a Rendőrség egy egyedi szervezet, így a specialitásaira is ki kell térni a kockázatkezelése során. Így szükségesnek tartottam a további információk vizsgálatát is a teljes kép megalkotásához:

- a szervezet feladatai,
- az informatikai hálózat által megvalósított folyamatok,
- az informatikai hálózat funkcionális követelményei,
- az informatikai hálózat felhasználói,
- az informatikai hálózatra vonatkozó minden biztonsági szabályzat (törvények, hazai és szervezeti jogszabályok),
- az informatikai hálózat biztonsági architektúrája,
- az informatikai hálózat működési környezete,
- az informatikai hálózatnak otthont adó épületek,
- az informatikai hálózatra vonatkozó információtárolási követelmények,
- az informatikai hálózat információáramlási folyamatai.

A fenti szempontrendszer alapján megállapítottam, hogy a rendőrség informatikai hálózata

- része a Nemzeti Távközlő Gerinchálózatnak,
- információ infrastruktúráját a zárt célú hálózat alkotja, a Zártkörű Rendészeti Hálózat,
- az informatikai hálózat hardver konfigurációja heterogén összetételű, a kornak és funkcionális követelményeknek megfelelőek,
- az informatikai hálózat szoftver konfigurációi legálisak, licenccel rendelkezőek, funkcionális feladatellátásra kerültek kiválasztása, továbbá egyedi rendőrségi akkreditált fejlesztéseket foglal magába,
- az informatikai hálózat funkcionálisan adat és hangátviteli feladatokat lát el,
- az informatikai hálózat kapcsolatai védettek, minden végponton tűzfallal védettek, így architektúrája is védettnek tekinthető,
- az informatikai hálózat felhasználói rendőrségi alkalmazottak, a biztonsági követelményeknek megfelelnek,
- az informatikai hálózatra vonatkozólag megállapításokat, és előírásokat fogalmaz meg árnyaltan a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzata,
- az informatikai hálózat működési környezete és a hálózatnak otthont adó épületek a 3. szintű információbiztonsági előírásoknak megfelelően ellátottak, mint fizikai, mint személyi védelem területén,
- az információtárolási követelmények tekintetében a Rendőrség Iratkezelési Szabályzata és Üzemeletetési Szabályzata tényszerűen rendelkezik.

A fenti szegmensek csak veszélyhelyzetben sérülhetnek. Egy veszélynek két tényezője van: a veszélyforrás és a sebezhetőség. „A veszély egy veszélyforrás lehetősége arra, hogy valamely sebezhetőséget kiváltson (véletlenül aktivizáljon vagy szándékosan kihasználjon).” [4; 177.o.]

A sebezhetőség gyakorlatilag egy olyan gyenge pont, melyet valaki véletlenül aktivizálhat, vagy szándékosan kihasználhat az informatikai hálózat elleni támadáskor. Ezek alapján a veszélyt annak a valószínűségnek a függvényeként fejezzük ki, hogy egy veszélyforrás sikeresen kihasznál egy adott sebezhetőséget.

Egyértelműen kijelenthetjük, hogy a kihasználható sebezhetőség nélkül egy veszélyforrás nem jelent kockázatot. Viszont a valószínűség meghatározásakor a veszélyforrásokon és a sebezhetőségeken kívül figyelembe kell venni a meglévő óvintézkedéseket is, melyek a sebezhetőség aktivizálását, szándékos kihasználását hivatottak megakadályozni, és megnehezíteni.

Hogy ezt a valószínűséget felállíthassam meg kell határoznom az informatikai hálózatot veszélyeztető forrásokat. Három veszélyforrást vetem számba:

- emberi,
- természeti,
- környezeti.

Veszélyforrás megjelenési formái szerint lehetnek:

- „szándék és módszer, mely egy sebezhetőség szándékos kihasználására irányul…, vagy rosszindulatú támadás a rendszer sértetlensége, bizalmassága, rendelkezésre állása ellen, jóindulatú, de ettől még célratörő kísérlet a biztonság csökkentésére,
- helyzet és módszer, mely véletlenül válthatja ki a sebezhetőséget.”[4; 178.o.]

A fent felsoroltakat tartom a legnagyobb kockázati tényezőknek. A kockázati tényezők meghatározásával készíthetjük elő a fenyegetettség elemzést.

FENYEGETETTSÉG-ELEMZÉS

A fenyegetettség-elemzésnél meg kell határozni az alapfenyegetettségeket. „Az informatikai rendszerek védelme a rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint a rendszer elemei sértetlenségének és rendelkezésre állásának.”[5]

A fenyegetettség-elemzés során fel kell tárni valamennyi elképzelhető fenyegető tényezőt, amelyek kárt okozhatnak az informatikai rendszerben, s ezzel az informatika-alkalmazásban vagy az adatokban. Ezért ismételten a kockázatkezelés lépéseihez fordultam. A fenyegetettség elemzés a kockázatkezelés kilenc lépése közül a következő három lépésből áll:

- Harmadik lépés: A fenyegetett rendszerelemek feltérképezése;
- Negyedik lépés: Az alapfenyegetettségek meghatározása;
- Ötödik lépés: A fenyegető tényezők meghatározása.

Célom a fenti három lépés segítségével az alábbi eredményeket elérni:

- „a rendszerelemek listája az alapfenyegetettségek megadásával,
- az informatika-alkalmazások és adatok más rendszerelemektől való függőségeinek leírása,
- rendszerelemenként a gyenge pontok leírása,
- az érvényes védelmi intézkedések leírása,
- az érvényes védelmi intézkedések kölcsönhatásainak leírása,
- a releváns fenyegető tényezők listája,
- a releváns fenyegető tényezők hozzárendelése a rendszerelemekhez és az alapfenyegetettségekhez.”[4; 229.o.]

Vizsgálataimat a feltérképezés során csak arra a rendszerelemekre szűkítem, amelyektől az informatika-alkalmazások és az információ-feldolgozás megvalósítása függ, és amelyekre a fenyegető tényezők hatással lehetnek.

3. lépés: A fenyegetett rendszerelemek feltérképezése: A vizsgálati lépés során adatfeldolgozási folyamatok személyi, dologi és környezeti elemei, valamint ezek egymástól való függősége kerül felmérésre és rögzítésre. A 3. lépés megvalósítása során a rendszerelemek feltérképezése, a rendszerelemek kölcsönös függőségeinek leírása a cél. Ehhez a leíráshoz rendszerelemek listáját kellett összegeznem.

- A rendőrség informatikai hálózata több alhálózatból áll, e rendszerelemek a lokális hálózatok (megyei rendőrségi hálózatok), mely egy zártkörű hálózatba a ZRH-ba tömörül, a kommunikációs eszközök listáját képezik a lokális (helyi) szerverek és a központi szerverek.
- A rendőrségi informatikai hálózatokat adat és hangátviteli hálózatokra osztom fel.
- A hálózatok infrastruktúrája jelenleg már állami tulajdont képeznek, nagymértékben a Nemzeti Infokommunikáció Szolgáltató Zrt-jé (NISZ) és csupán kis mértékben rendőrségi tulajdon. Minden esetben ellenőrzött adminisztratív zónán belül helyezkednek el.

A rendszerelemek feltérképezése: az első lépés eredményeiből kiindulva fel kell térképezni az informatikai rendszer minden elemét, majd azokat be kell sorolni a következő csoportokba:

- Minden rendőrségi informatikai hálózati végpont rendőrségi objektumban, őrzött területen végződik, a szervertermek, ahol a szerverekbe kerül bekötésre a hálózati végpontok, egyedileg ellenőrzöttek.
- A rendőrségi informatikai hálózatokat rendőrségi objektumon belül minden esetben rendőrségi alkalmazott üzemelteti és látja el karbantartását.
- A rendőrség informatikai hálózati rajzai jelenleg minősített dokumentumok, azok a minősített adatvédelmi törvénynek megfelelően védettek.

- A rendőrség informatikai hálózati hardverek heterogének, regionálisan azonosak, a rendőrség törekszik azonos típusok alkalmazására.
- A rendőrség informatikai hálózati szoftveri minden esetben azonosak, központi alkalmazások szoftverei, többnyire rendőrségi saját fejlesztések, vagy licence köteles irodai szoftverek.
- A rendőrség informatikai hálózati adathordozók, minden esetben az iratkezelési és a rendőrség Ideiglenes Informatikai Biztonsági Szabályzata által védett eljárások szerint kezelik.
- A rendőrség informatikai hálózati kommunikációja szabályozott üzemeltetési szabályok szerint történik, mely adat és hang alapú.
- Egyéb, az informatika-alkalmazás megvalósítását szolgáló elemként jelenítem meg az EDR rendszert és készülékeket, melyek funkcionálisan azonosak, mégis az eszköz típusok tekintetében heterogének.

Az informatikai rendszer műszaki behatárolása során fontos az izolált és a hálózatba kötött rendszerek megkülönböztetése. Ezrét jelen esetünkben a hálózatba kötött rendszerek a kommunikációs hálózat kapcsolódási pontjait az NTG hálózat képezi minden más kormányzati szervezethez.

A rendszerelemek kölcsönös függőségeinek leírása: a rendőrség informatikai hálózat informatika-alkalmazásai, szolgáltatásai, illetve adatok és a rendszerelemek közötti függőségek egyértelműen fellelhetőek. A rendőrség legfőbb alkalmazása a Robotzsaru Integrált Ügyfeldolgozó és Ügykezelő rendszer (a továbbiakban: RZS). AZ RZS minden megyei rendőrségi objektumban lokálisan kerül alkalmazásra. Az RZS tömörített és kivonatolt adattartama kerül a rendőrség informatikai hálózatán keresztül a központi alkalmazások közé az RZS NEO rendszerbe, mely minden rendőrségi informatikai lokális hálózaton keresztül elérthető. Így lehetőség nyílik minden adat megosztására a többi szervezettel.

4. lépés: Az alapfenyegetettség meghatározása: mely során az alapfenyegetettség felmérése történik meg valamennyi rendszerelemre kiterjedően. A 4. lépésben össze kell rendelni az alapfenyegetettségeket és a rendszerelemekkel.[4; 233.o.] Ezeket az alábbiakban összegzem:

- A bizalmasság elvesztése (a rendszerbe történő jogosulatlan belépéssel a munkaállomáson feldolgozott vagy kezelt minősített adat illetéktelen személy számára hozzáférhetővé vagy megismerhetővé válik).
- A sértetlenség elvesztése (a rendszer információinak jogosulatlan módosítása miatt a rendszer forrásainak hibás működése vagy a rendszeren kezelt információk valódiságának megszűnése).
- A rendelkezésre állás elvesztése (a jogosult bejelentkezés megtagadása vagy a rendszer szolgáltatásainak hozzáférhetetlenné tétele). [8; 22.o.]

5. lépés: A fenyegető tényezők meghatározása: Ebben lépésben a rendszerelemek gyenge pontjainak meghatározását, valamint a fenyegetı tényezőknek az alapfenyegetettség-rendszerelem párosokhoz való hozzárendelését végezhetjük el. Az 5. lépés során az informatikai rendszer gyenge pontjainak feltérképezése; és a fenyegető tényezők meghatározása az alap feladat. [3; 236.o.] A gyenge pontokat, kockázati tényezőket, hatásokat és reakciókat az 1. számú táblázat tartalmazza. Ezen gyenge pontokat tekintem fenyegetetteknek a támadások során.[3; 242.o.]

TÁMADÁSTÍPUSOK ÉS FELTÉTELEZETT MEGJELENÉSI HELYÜK ISMERTETÉSE A RENDŐRSÉG INFORMATIKAI HÁLÓZATÁN

„A támadás, valamilyen védett érték megszerzése, megsemmisítésére, károkozásra irányuló cselekmény. Támadás alatt nem csak a személyek, szervezetek által elkövetett támadásokat, de áttételesen a gondatlanságból, nem szándékosan kiváltott veszélyeztetéseket és a környezeti, természeti fenyegetéseket is értjük. A támadás legtöbbször nem közvetlenül éri a védett értéket, hanem a körülményektől függő támadási útvonalon zajlik le.”[1]

Léteznek belső felhasználók, akiknek kifelé irányú kapcsolatokra van szükségük, és léteznek külső felhasználók, akik befelé irányú kapcsolatokat szeretnének kezdeményezni.

A fenyegetés típusok, mint támadási lehetőségek vizsgálatánál figyelembe vettem a Virus Buster Kft. víruslaboratóriumának észlelései alapján készített Magyarországi Nemzeti Hálózatbiztonsági Központ 2012. első negyedév időszakáról készített jelentéseit. Ezeket megpróbáltam összevetetni a rendőrségi gyakorlattal. Tekintettel arra, hogy a Rendőrségnél semmilyen nyilvános felmérés sem statisztika nem áll rendelkezésre az informatikai hálózatot ért támadásokról, így csak személyes interjúk alapján és a Magyarországi Nemzeti Hálózatbiztonsági Központ jelentésére támaszkodva csoportosíthattam a leggyakrabban előforduló támadás típusokat. Ezek alapján az alábbiakban összegzem a támadás típusokat:

- Jogosulatlan hozzáférés,
- Alkalmazás szintű támadás,
- Jelszó megfejtés,
- Szolgáltatások blokkolása,
- IP címhamisítás,
- Csomagok vizsgálata,
- Hálózat feltérképezés,
- Trust kapcsolatok kihasználása,
- Port átirányítás,
- Root kit-ek, vírusok és trójai falovak,
- Zero-day jellegű támadások,
- Layer 2 támadások,
- URL és Content blocking támadások, kártékony kód futtatása.

A támadások megjelenési helye tekintetében a rendőrség informatikai hálózatait két részre osztottam. A menedzsmenti részre (mely gyakorlatilag az informatikai hálózatok teljes belső részét lefedi) és az internet felöli részre (mely az informatikai hálózatok határvonalait fedi le).

A menedzsment modul elsődleges feladata, hogy biztonságos menedzsmentet nyújtson a rendőrségi informatikai hálózatban található eszközök és hosztok számára. Ez alá tartozik a loggolás és riportolás folyamata beleértve a hálózati eszközöket, tartalmakat, konfigurációkat és szoftvereket, valamint a menedzselés során alkalmazott adatátviteli módszereket és eljárásokat is. [8; 12.o.] Funkcionalitásának tekintetében az alábbiakban csoportosítom a modul részeit:

- SNMP menedzsment szerver – SNMP menedzsment szolgáltatásokat nyújt az eszközök számára,
- Riasztás kezelő szerver – Riasztás aggregálást végez az IDS/IPS rendszerek számára,
- Syslog szerverek – Tűzfalak és NIDS/NIPS rendszer információit aggregálja,
- Access Control szerver – Kéttényezős, OTP (lásd alább) authentikációs szolgáltatásokat nyújt a hálózati eszközök számára,
- One-time password (OTP) szerver – Időben nem ismétlődő jellegű információk autorizációját végző eszköz,
- Certficate Authority szerver – Tanúsítvány kezelő és kiosztó szerver,

- Rendszer adminisztrációs hoszt – Konfigurációs, szoftver és tartalomváltozások kiszolgálására fenntartott eszköz,
- NIDS/NIPS eszköz – Layer forgalmak monitorozását végző eszköz,
- Tűzfal – Részletes forgalomszabályzást végző eszköz a menedzselt eszközök és a menedzsment eszközök között,
- Layer 2 switch (Private VLAN támogatással) – Biztosítja, hogy a menedzselt eszközök felől érkező forgalom csak a tűzfalon keresztül léphessen a szegmensre.

A fenti eszközöket érő fenyegetések és azok elhárítására teendő intézkedéseket a következők szerint összegezem:

- Jogosulatlan hozzáférés – a tűzfalon történő szűrés minden irányban megakadályozza a jogosulatlan hozzáférést,
- IP spoofing – a szűrések alkalmazása meggátolja a spoofing hatékonyságát,
- Hálózat felderítés – az alkalmazott szűrések limitálják a bejutó nemkívánatos forgalmakat, és ez által limitálják egy támadó által végrehajtott hálózati felderítés hatékonyságát,
- Packet snifferek – a megfelelő módon konfigurált switchelt infrastruktúra limitálja a csomag lehallgatás hatékonyságát[8; 23.o.]

Az Internet modul, mely az Internet kapcsolatot biztosítja a belső felhasználók számára, illetve az Internet felől hozzáférést biztosít a publikus szerverekhez. A VPN végződtetésért felelős VPN and remote access modul forgalma is itt halad át. Ez a modul nem e-commerce alkalmazásokat szolgál ki. [8; 12-14.o.] Funkcionalitásának tekintetében az alábbiakban csoportosítom a modul részeit:

- SMTP szerver – relayként működik a belső és külső mail szerverek között, megvizsgálja a levelek átmenő tartalmát,
- DNS szerver – a vállalat megbízható külső DNS szervereként szolgál, illetve továbbítja az Internet felé irányuló belső névfeloldási kéréseket,
- FTP/HTTP szerver – publikus információkat nyújtanak a szervezetről,
- Tűzfal – hálózati rétegben védi az erőforrásokat, és stateful szűrést valósít meg,
- NIDS/NIPS – a modulban található hálózati szegmensek vizsgálatát látja el,
- URL filter szerver – a nem megengedett URL-ek alapján szűri a forgalmat,
- Content-aware Web proxy – blokkolja a befele jövő URL alapú támadásokat, cache-eli a weboldalakat a LAN forgalmának csökkentése végett. Az eszközök Internet Content Adaptation Protocol Version 1-et illetve Antivirus szervereket használnak annak érdekében, hogy a cache-élt web adatok vírusmentesek legyenek, továbbá szükség esetén authentikációt biztosít a kifele menő web kapcsolatoknak,
- Routerek – címhamisítás szűrés, bogon szűrés, routing protokollok authentikációja és szűrése, ACL-ek.

A fenti eszközöket érő fenyegetések és azok elhárítására teendő intézkedéseket a következők szerint összegezem:

- Jogosulatlan hozzáférés – elhárítva az ISP-nél, a routereken és a szervezet tűzfalán megvalósított szűréssel,
- Alkalmazásszintű támadások – a hálózati és hoszt szintű IDS/IPS megoldásokkal védhető ki,
- Vírusok és trójai alkalmazások – email tartalomelemzés, hoszt IDS/IPS, és Antivirus ellenőrzés által közömbösíthető,
- Jelszó elleni támadások – a brute force jellegű támadásnak csak korlátozott erőforrás tehetők ki, az operációs rendszer és az IDS/IPS rendszerek észlelni tudják a fenyegetést,

- DOS – rate limiting, és black-hole routing az ISP edge modulon, TCP SYN jellegű elárasztás elleni védelem a tűzfalon,
- IP spoofing –szűrés a modulokban,
- Packet snifferek – megfelelően tervezett, switch-elt hálózati architektúra, illetve hoszt IDS/IPS-ek csökkentik a veszélyt,
- Hálózat felderítés – az IDS/IPS rendszerek képesek felismeri a felderítési kísérleteket, a protokollok szűrése csökkenti a felderítési módszerek eredményességét,
- Trust alapú támadások– explicit trust modell és Private VLAN-ok alkalmazása korlátozzák az ilyen típusú támadások hatékonyságát,
- Port átirányítás – korlátozó szűrés és HIDS/HIPS alkalmazása csökkenti a veszélyt,
- Root kit, vírusok, férgek, zero-day támadások – hoszt alapú IDS/IPS alkalmazások és Antivirus szoftverek mérséklik az ilyen támadásokat,
- Nem engedélyezett URL hozzáférés – tűzfal és Content-aware Web proxy együttes használatával blokkolhatók a vállalati biztonsági politika szerint nem kívánatosnak ítélt weboldalak,
- URL alapú támadások – a terhelés megosztó rendszereken vagy web proxy cache rendszereken végzett URL szűrés segítségével blokkolható,
- Malicious code futtatás — HIDS/HIPS alkalmazása csökkenti a veszélyt [8; 23-27.o.].

A fenti felsorolásban igyekeztem a rendőrség informatikai hálózatait általánosságban vizsgálni a támadások tekintetében. Megállapítottam, hogy számos olyan fenyegetés és támadás létezik, amelyek a kezdeti kompromittálás által egy hacker behatolása leegyszerűsödik, és másodlagos támadásokat kezdeményezhet többek között, vagy az eredeti célnál megmarad a támadó. Rendkívül szerteágazó és széleskörű lehet a támadások köre. [8; 11.o.] A fenti felsorolás csak az alapvető típusokat öleli fel, a speciális irányúakat jelen elemzés során, figyelmen kívül hagytam.

ÖSSZEGZÉS

Ahhoz, hogy a rendőrség informatikai hálózatait érő fenyegetés típusokat meg tudjam határozni kutatásokat folytattam mind a nemzetközi mind a hazai CERT dokumentációkban. Tekintettel arra, hogy a Magyarországi Nemzeti Hálózatbiztonsági Központ szakirányítása és szakmai tapasztalat cseréje egyelőre még csak egyirányú, és a kapcsolódó hazai szervezetek, mint a rendőrség is csak fogadja a tájékoztatásokat, viszont tájékoztatást az incidens kezelésekről nem ad. Így rendkívül kevés információval rendelkezünk az informatikai hálózatokat ért támadásokról. Sajnos a rendőrség tekintetben semmilyen nyílt statisztika nem állt rendelkezésemre. Csak a szakmai tapasztalatokra, dokumentációkra és riportokra tudtam kutatásom során támaszkodni.

A rendelkezésre álló szakmai dokumentációk és ajánlások alapján kockázatelemzést folytattam le. Az elemzés segítségével, a támadás típusok meghatározásával rá kívántam mutatni, hogy mely biztonsági követelmények meglétével védhetőek ki a támadások. A követelmények meglétének hiányát feltételezve, taglalni kívántam a gyenge pontok felsorolásával létrehozott sérülékenységi mátrixszal, hogy milyen eredményeket okozhatnak az általam meghatározott támadások az informatikai hálózat biztonsági állapotában.

Megállapítottam, hogy a „védelemnek biztosítania kell az informatikai rendszer megbízható üzemét fenyegető káresemények elhárítását, illetve hatásuk minimalizálását a megadott biztonsági követelmények szintjén.”[7; 8501.o.] „Olyan védelmi eljárásokat kell alkalmazni, amelyek garantálják, hogy az államigazgatás még akkor is hatékonyan működjön, ha akár egy szervezetét (tárca, intézmény, az országos hatáskörű szerv) is katasztrófa ér. Az

informatikai biztonság rendszere olyan legyen, hogy minimális adminisztratív terhet jelentsen, az alkalmazottaktól ne igényeljen aránytalanul nagy erőfeszítést, csak amelyet a helyes munkavégzés gyakorlata során elvárhatunk. Elsősorban abban nyújtson támogatást, hogy állapítsa meg a kivételes eseteket és biztosítsa a normálállapotra való visszatérést a kivételes esemény leküzdése után." [9; 1.o.]

Tekintettel arra, hogy jelenleg a rendőrség csak az Ideiglenes Informatikai Biztonsági Szabályzatával rendelkezik, és speciális hálózatbiztonsági szabályzási rendszerrel nem rendelkezik. Ezért szükségesnek tartom, olyan egységes a szervezet egészét érintő informatikai biztonsági dokumentáció megalkotását, mely egyértelműen meghatározná a rendőrség informatikai hálózatának védelmével kapcsolatos konkrét ilyen irányú elgondolásait. Véleményem szerint az informatikai biztonság politikájának, a rendőrségnek a már megfogalmazott informatikai biztonság filozófiára kellene épülnie, és megfelelő alapot kell majd teremtenie az informatikai biztonsági célkitűzések meghatározásához. Ehhez jó kiindulópontnak tekintem az alapfenyegetettségben meghatározott elveket. Véleményem szerint, ha a jelenlegi gyakorlatot, melyet az interjúk eredménye is mutatott, szakszerűen szabályokba öntve sikerülne szervezet szinten elfogadtatni, kimagasló eredményeket mutatna a biztonság terültén, és rendkívülien magas lenne az elrettentő ereje. Ezért azt gondolom, hogy minden lehetséges esetben a megelőzésre törekvő magatartást kell előnyben részesítenie a követő magatartással szemben, elvégre alapozó dokumentumot kell létrehozni a védelem érdekében, melynek az informatikai biztonsággal összefüggő szabályoknak, intézkedéseknek egységes értelmezését kell elősegítenie. Ezen szabályozó rendszer kialakításához fontosnak tartom az ISO/IEC 27001:2005-ös szabvány „A" mellékletének 10.6 fejezetének felhasználását, meg követelményeket fogalmaz meg a hálózatbiztonság kezelésére.

„A hálózatok biztonságos kezelése, amely átívelhet a szervezeti határokon, gondos megfontolást kíván az adatfolyamatra, a jogi követelményekre, figyelemmel kísérésre és védelemre vonatkozóan. A szabályozás kialakításánál ügyelni kell arra, hogy minden hálózati szolgáltatás biztonsági jellemzőit, szolgáltatás szintjeit és irányítási követelményeit azonosítsák és foglalják bele a szolgáltatási megállapodásokba, legyen akár belső, akár külső (kiszervezett) szolgáltatásról is szó." [6; 39.o.]

Felhasznált irodalom

[1] MUHA LAJOS: *Fogalmak és definíciók*, Az informatikai biztonság kézikönyve (szerk.: Muha Lajos) – Verlag Dashöfer Szakkiadó, Budapest, (2004.) ISBN 963 9313 12 2

[2] MUHA LAJOS: *Infokommunikációs biztonsági stratégia*, Hadmérnök IV:1, (2009) pp. 214-224.

[3] PUSKÁS TIVADAR KÖZALAPÍTVÁNY CERT-Hungary: *Nemzeti Hálózatbiztonsági Központ 2012. I. negyedéves jelentése*, (2012.) pp.1-42.2012.

[4] *Az Informatikai Biztonság Irányításának Vizsgálata (IBIV)* – Magyar Informatikai Biztonsági Ajánlások (MIBA) 25/1-3. kötet, Budapest, (2008.) pp.175-179.

[5] MUHA LAJOS: Az informatikai biztonság egy lehetséges rendszertana, Bolyai Szemle XVII:4, (2008) pp. 137-156.

[6] DR. KÖDMÖN ISTVÁN: *Információbiztonság az ISO27001 tükrében*, Hétpecsétes Történetek, – Hétpecsét Információbiztonsági Egyesület, Budapest, (2008.), pp.39. MSZ ISO/IEC 27001:2006,

[7] *21/2011. (VIII. 11.) BM utasítás a Belügyminisztérium Informatikai Biztonság Politikájáról,* Hivatalos Értesítő 44. számában 2011. augusztus 11., Budapest. (2011.) pp 8498-8504.

[8] *60/2008. (OT 32.) ORFK utasítás a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatának kiadásáról,* (5-1/60/2008. TÜK iktatószám – Országos Rendőr-főkapitányságí Tájékoztató 32. száma, Budapest, (2008.) pp 2-63.

[9] INFORMATIKAI TÁRCAKÖZI BIZOTTSÁG AJÁNLÁSAI: *Informatikai rendszerek biztonsági követelményei* 12. sz. ajánlás 1.0, Miniszterelnöki Hivatal Informatikai Koordinációs Iroda Budapest, (1996.) pp.1-26. (http://www.itb.hu/ajanlasok/a12/html/a12_2.htm)

Megnevezés /kockázati tényező	meghibásodás	kárérték	előfordulási gyakoriság	kritikusság	hatás	reagálás	időinter-vallum
Szerver hardveres meghibásodása	A meghibásodás olyan elemet érint, mely nem redundáns.	3	1	4	A rendszer működésképtelenné válik.	A szerver javítását / cseréjét haladéktalanul el kell végezni.	1 nap
	A meghibásodás olyan elemet érint, mely redundáns. A szerver kapacitása csökken.	2	1	3	A rendszer működőképes marad, de a használhatósága csökken, a szerver meghibásodott alkatrésze a továbbiakban nem redundáns.	A szerver javítását / cseréjét haladéktalanul el kell végezni.	3 nap
	A meghibásodás olyan elemet érint, mely redundáns.	1	1	2	A rendszer működőképes marad, a szerver meghibásodott alkatrésze a továbbiakban nem redundáns.	A szerver javítását / cseréjét haladéktalanul el kell végezni.	1 hét
Szerver szoftveres meghibásodása	A meghibásodás következményeként a rendszer használható marad	0	2	2	A rendszer működőképes marad.	A szoftver javítását haladéktalanul el kell végezni	3 nap
	A meghibásodás következményeként a rendszer nem marad használható	2	1	3	A rendszer, vagy egyes moduljai működésképtelenné válnak.	A szoftver javítását haladéktalanul el kell végezni	1 nap
Kliens hardveres meghibásodása	A meghibásodás következményeként a kliens használható marad	0	2	2	A rendszer működőképes marad.	A kliens javítását el kell végezni	3 nap
	A meghibásodás következményeként a kliens nem marad használható	1	1	2	Az adott kliens használhatatlanná válik, de a rendszer többi eleme használható marad. A munka elvégezhető másik kliensről.	A kliens javítását el kell végezni	2 nap
Kliens szoftveres meghibásodása	A meghibásodás következményeként a rendszer használható marad	0	2	2	A rendszer működőképes marad.	A kliens javítását el kell végezni	3 nap
	A meghibásodás következményeként a rendszer nem marad használható	1	1	2	Az adott kliens használhatatlanná válik, de a rendszer többi eleme használható marad. A munka elvégezhető másik kliensről.	A kliens javítását el kell végezni	2 nap

Hálózat meghibásodása	A probléma csak egy kliens gépet érint	1	2	3	Az adott kliens használhatatlanná válik, de a rendszer többi eleme használható marad. A munka elvégezhető másik kliensről.	A hálózati elem javítását el kell végezni.	3 nap
	A probléma minden kliens gépet érinti	3	1	4	A rendszer használhatatlanná válik.	A hálózati elem javítását haladéktalanul el kell végezni.	1 nap
	A probléma a szervert érinti	4	1	5	A rendszer használhatatlanná válik.	A hálózati elem javítását haladéktalanul el kell végezni.	1 nap
	Átviteli út fizikai meghibásodása	4	1	5	A rendszer használhatatlanná válik.	A hálózati elem javítását haladéktalanul el kell végezni.	1 nap
Erősáramú betáplálási problémák	Rövid idejű áramszünet a területen (max. 1-2 perc)	1	2	3	A kliensgépek leállnak, de a munkamenetek nem vesznek el, az áramszünet után a munka folytatható		
	Közepes idejű áramszünet a területen (max 15. perc)	2	1	3	A kliensgépek leállnak, de a munkamenetek nem vesznek el, az áramszünet után a munka folytatható	Amennyiben az áramszünet 5 percnél tovább tart fel kell készülni a rendszer biztonságos leállítására	5 perc
	Hosszú idejű áramszünet a területen (több mint 15 perc)	3	1	4	A teljes rendszer működő képtelenné válik	Amennyiben az áramszünet 15 percnél tovább tart meg kell kezdeni a rendszer biztonságos leállítását.	15 perc
Szerverterem klimatizálási probléma	A klíma teljesítménye lecsökken	0	2	2	A szerverterem hőmérséklete megnövekszik, de még a kritikus szintet nem éri el.	A klíma berendezést meg kell javítani, a szerverterem hőmérsékletét napi 3x ellenőrizni kell.	2 óra
	A klíma működésképtelenné válik.	3	1	4	A szerverterem hőmérséklete megnövekszik, beavatkozás nélkül átlépheti a kritikus pontot, ami a rendszer meghibásodásával jár.	A klíma berendezést haladéktalanul meg kell javíttatni. Ha a szerverterem hőmérséklete átlépi a kritikus szintet (35C), meg kell kezdeni a rendszer biztonságos leállítását.	2 óra
Természeti katasztrófa	a teljes körlet megsemmisül	3	1	4	A rendszer működésképtelenné válik. Az adatok archívumból visszaállíthatóak.	Az archív anyagok felhasználásával a rendszert újra kell építeni.	1 hónap

	a teljes épület megsemmisül	4	1	5	A rendszer működésképtelenné válik. Az adatok archívumból sem állíthatóak vissza.		

1. táblázat.