Dr. Krasznay Csaba

krasznay.csaba@uni-nke.hu

A RENDVÉDELMI SZERVEK HELYE A KIBERVÉDELEMBEN

ROLE OF LAW ENFORCEMENT AGENCIES IN CYBER DEFENSE

Absztrakt

A kibervédelem megszervezése összetett, a kormányzat különböző szereplői közötti együttműködést igénylő feladat. Minden ország irányítási struktúrája különböző, de a belbiztonságért felelős minisztériumnak bizonyosan nagyon fontos szerepe van ebben a hierarchiában. Ezt erősítik meg az egyes nemzetközi szervezetek által kiadott ajánlások is, melyek egy ország kibervédelmi stratégiájának kialakítására mutatnak jó gyakorlatot. Jelen tanulmány célja áttekinteni Magyarország belügyi szerveinek kibervédelemben betöltött szerepét, illetve a nemzetközi ajánlásoknak való megfelelést.

Organizing cyberdefense in a country is a complex subject that needs interagency cooperation. All countries have a different governance structure, but it is a fact that the ministry responsible for internal security has a key role in this hierarchy. This is confirmed by recommendations from various international organizations that show best practices for the creation of national cyberdefense strategies. The goal of this study is to overview the role of Hungarian internal security organizations in cybersecurity and the compliance with international recommendations.

Kulcsszavak: *kiberbiztonság, kiberbűnözés, belügyi szervek, ITU, ENISA, NATO*

Keywords: *cybersecurity, cybercrime, internal security organization, ITU, ENISA, NATO*

Bevezetés

Egy ország kibervédelmi feladatait számos katonai, nemzetvédelmi, rendvédelmi és civil szervezet összehangolt munkájával kell megteremteni. Annak érdekében, hogy ez a rendkívül összetett feladat sikeres legyen, több mérvadó nemzetközi szervezet is ajánlásokat tett a felelősségekkel és szerepkörökkel kapcsolatban. Ugyan a szervezetrendszer felépítése országról országra változik, de a legfontosabb feladatokat ezek az ajánlások egyértelműen a belbiztonságért felelős minisztérium alárendeltségébe tartozó intézményekre szabták.

Nincsen ez másképp Magyarországon sem, ahol az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.) [1], valamint a Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat [2] rendelkezik az ország kibervédelmi szervezeti struktúrájáról. A teljes jogi környezet jelenleg kialakulóban van hazánkban, ezért érdemes áttekinteni, hogy az egyes Belügyminisztérium alá rendelt szervezetek törvényi kötelezettségei és a nemzetközi

ajánlások mennyiben vannak egymással összhangban, illetve milyen további jogszabály-alkotási feladatok állnak még a magyar kormány előtt a teljes lefedettség eléréséhez!

Jelen tanulmány az ITU National Cybersecurity Strategy Guide [3], az ENISA National Cyber Security Strategies [4] és a NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) National Cyber Security Framework Manual [5] alapján tekinti át azt, hogy 2013. közepén a magyar kibervédelem felépítése mennyiben felel meg a nemzetközi elvárásoknak, különösen a rendvédelmi szervek tekintetében. A központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény [6] 1. § (5) alapján a rendvédelmi szervek közé soroljuk a rendőrséget, a büntetés-végrehajtási szervezetet, a hivatásos katasztrófavédelmi szervet és a polgári nemzetbiztonsági szolgálatokat.

Nemzetközi ajánlások

International Telecommunication Union (ITU)

A távközléssel foglalkozó szervezeteket tömörítő ITU 2011-ben adta ki a National Cybersecurity Strategy Guide című ajánlását, melyben az elsők között kezdett azzal foglalkozni, hogyan kell egy nemzeti kibervédelmi rendszert felállítani. A publikáció 10 lépésben határozza meg a legfontosabb stratégiai lépéseket:

1. **A legmagasabb kormányzati szintű kiberbiztonsági felelősség meghatározása**. Magas rangú kormányzati felelőst neveznek ki, akinek feladata a nemzeti stratégia kidolgozása és a helyi, nemzeti és globális, szektorok közötti együttműködés elősegítése.
2. **Nemzeti kiberbiztonsági koordinátor kinevezése**. Olyan iroda vagy személy megbízása, aki vagy amely átlátja a kiberbiztonsági tevékenységeket az adott országban.
3. **Nemzeti kiberbiztonsági tanács létrehozása**. Olyan szervezet összehívása, mely a közigazgatás érintett szerveit tömöríti, és feladata azon tevékenységek összehangolása, mely a nemzeti kibertér védelmére irányul.
4. **Jogszabályalkotás**. Tipikusan az adott országban át kell tekinteni a létező jogszabályokat, és amennyiben szükséges, ki kell egészíteni a büntető-törvénykönyvet és a vonatkozó eljárásrendet a kiberbűnözés visszaszorítása érdekében.
5. **Nemzeti kiberbiztonsági keretrendszer kidolgozása**. Az ország létrehoz egy olyan keretrendszert, mely tartalmazza a minimális vagy kötelező biztonsági követelményeket olyan területeken, mint a kockázatkezelés és a megfelelőség.
6. **Computer Incident Response Team (CIRT) felállítása.** Az incidenskezelés nemzeti felelősség, melyet egy CERT[1]/CSIRT[2] képes megoldani. Ez a szervezet elemzi a kiberfenyegetések trendjeit, koordinálja a válaszadást és nyújt információt az érintett felek számára.
7. **Kiberbiztonsági tudatosság és oktatás megszervezése.** Nemzeti programot kell szervezni a kiberfenyegetésekkel kapcsolatos tudatosság erősítése érdekében.
8. **Köz- és magánegyüttműködés a kiberbiztonság területén**. A kormányzatnak szorosan együtt kell működnie a privát szféra szereplőivel.
9. **Humán képességek fejlesztése a kiberbiztonság területén**. Olyan oktatási rendszer kidolgozása, mely a kiberbiztonsággal foglalkozó szakértők tudását fejleszti.

[1] CERT: Computer Emergency Response Team
[2] CSIRT: Computer Security Incident Response Team

10. **Nemzetközi együttműködés**. Globális partnerség a mindenkit fenyegető kiberkockázat csökkentése érdekében.

Az ajánlás megnevezi azokat a kormányzati és civil szereplőket is, melyeknek szerepe van a fenti stratégiai feladatok végrehajtásában. Ezen szereplők a következők:

- Kormány, Magyarországon a Miniszterelnökség
- Parlament
- Kritikus infrastruktúrák tulajdonosai és üzemeltetői
- Bíróságok
- Bűnüldöző szervek
- Hírszerző szervezetek
- Információbiztonsági termékek gyártói
- Akadémiai szféra
- Nemzetközi partnerek
- Állampolgárok

A fenti szereplők közül Magyarországon a Belügyminisztérium szervezetei közé tartozik a kritikus infrastruktúrákat felügyelő Országos Katasztrófavédelmi Főigazgatóság, a bűnüldözéssel foglalkozó szervezetek (Rendőrség és a Terrorelhárítási Központ), a polgári titkosszolgálatok közül az Alkotmányvédelmi Hivatal és a Nemzetbiztonsági Szakszolgálat (ezen belül a kormányzati CERT) és részben a Nemzeti Közszolgálati Egyetem, mint akadémiai szereplő. A minisztérium kibervédelemben betöltött fontos szerepe tehát vitathatatlan.

European Network and Information Security Agency (ENISA)

Az Európai Unió kibervédelemmel foglalkozó szervezete, az ENISA 2012 decemberében publikálta a nemzeti kiberbiztonsági stratégiák létrehozását támogató National Cyber Security Strategies – Practical Guide on Development and Execution című kiadványát. Ebben 20 olyan lépést határozott meg, mely szükséges a nemzeti stratégia létrehozásához.

1. A vízió, a hatókör, a célok és a prioritások meghatározása.
2. Nemzeti kockázatfelmérési szempontrendszer követése.
3. A létező jogszabályok, szabályozások és képességek számbavétele.
4. Tiszta irányítási struktúra felállítása.
5. A fontos szereplők azonosítása és bevonása.
6. Megbízható információátadási eljárások kidolgozása.
7. Kiberbiztonságot számba vevő folytonossági tervek kidolgozása.
8. Kibervédelmi gyakorlatok szervezése.
9. Alapvető biztonsági követelmények meghatározása.
10. Incidensjelentési eljárások kidolgozása.
11. Állampolgári tudatosság emelése.
12. Kutatás-fejlesztés támogatása.
13. Szakértői oktatások és tréningek indítása.
14. Incidenskezelési képességek kialakítása.
15. Kiberbűnözés visszaszorítása.
16. Részvétel a nemzetközi kapcsolatokban.
17. Köz- és magánegyüttműködés kialakítása.
18. A biztonság és az adatvédelem közötti összhang kialakítása.
19. A kibervédelem rendszerének értékelése.
20. A nemzeti kibervédelmi stratégia finomhangolása.

Az útmutató nem nevesíti az érintett szerveket, de a feladatokból és az ezekhez rendelt példákból több helyen is kimutatható, hogy a belügyi szervek természetesen kulcsfontosságúak a stratégia létrehozásában.

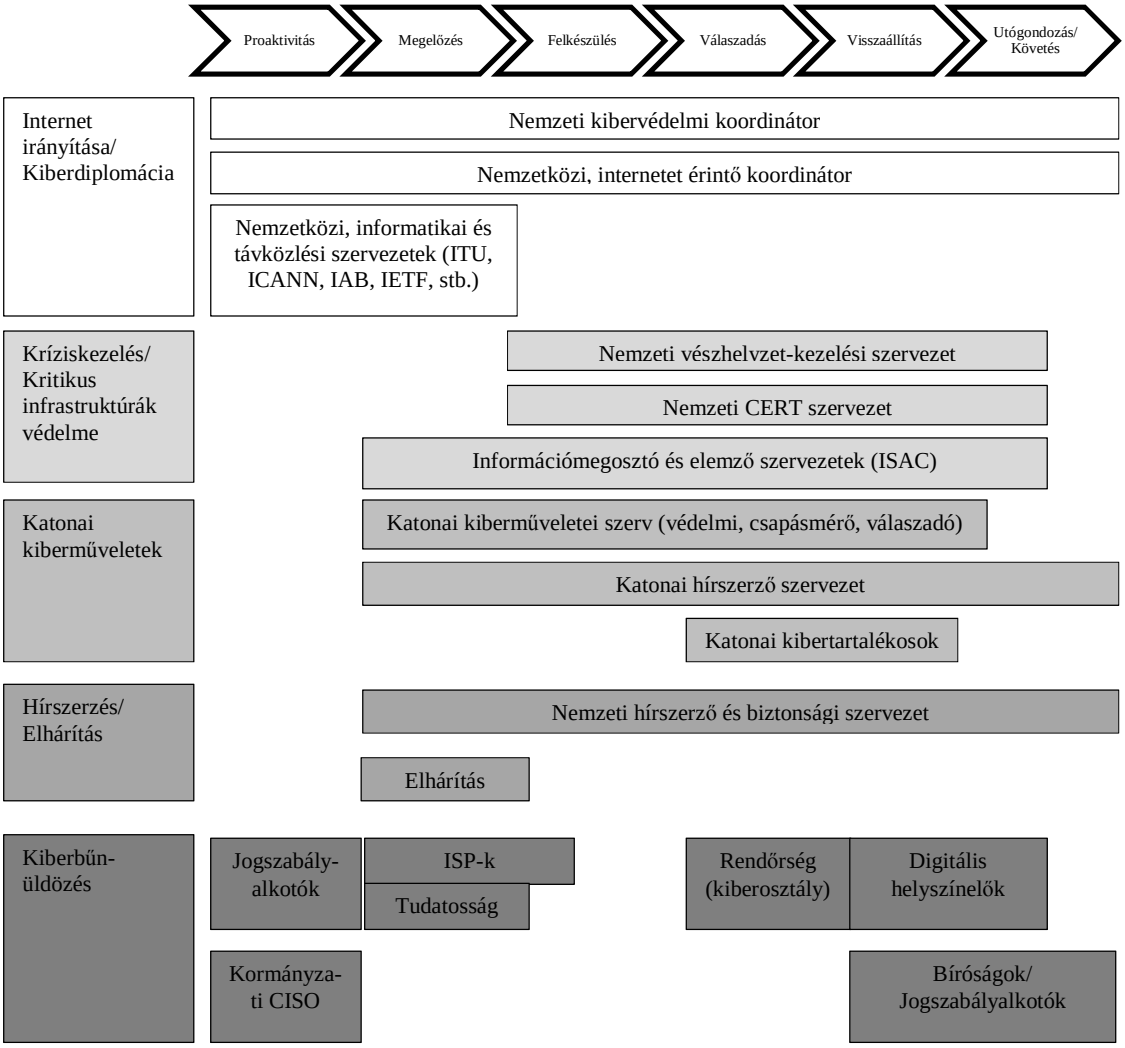
North Atlantic Treaty Organisation (NATO)

A NATO kibervédelemmel foglalkozó intézete, a Tallinban működő Cooperative Cyber Defence Centre of Excellence (CCD CoE) gondozásában megjelent National Cyber Security Framework Manual foglalkozik a legrészletesebben a kibervédelem szervezet- és feladatrendszerével. A 2012-ben kiadott kötet az előző ajánlásokkal szemben katonai szemszögből is elemzi a területet.

A nemzeti kibervédelem a tanulmány szerint öt különböző aspektusból vizsgálandó:

- **Katonai kibervédelem**. A hagyományos területekhez hasonlóan a kibertérben is ki kell építeni bizonyos katonai képességeket, így a saját hálózatok védelmét, a hálózatközpontú hadviselés képességeit, valamint a taktikai és stratégiai kiberhadviselés képességét.
- **Kiberbűnözés elleni harc**. Ebbe a körbe tartozik az egyént érintő kiberbűncselekmények üldözése mellett a kiberterrorizmus elleni lépések sora is.
- **Hírszerzés és elhárítás**. Az utóbbi években jelentősen nőtt az államok ellen a kibertérben elkövetett hírszerzési tevékenységek aktivitása, mely indokolttá teszi ezek körültekintő elhárítását, valamint az ország elleni esetleges kibertámadások mielőbbi, titkosszolgálati úton történő felderítését.
- **Kritikus infrastruktúra védelem és nemzeti krízismenedzsment**. Ez a terület lefedi a létfontosságú rendszerek védelmét, valamint az esetleges kibertámadás esetén az események informatikai és társadalmi kezelését is.
- **Kiberdiplomácia és az internet irányítása**. A kibervédelem nemzetközi rendszerének megalkotása esősorban a nemzetközi szervezeteken keresztül, részben bilaterális megállapodásokban lehetséges. Ezért fontos, hogy a kiberteret, és ennek közegét, az internetet irányító szervezetekben a kormányzat aktívan részt vegyen.

A keretrendszer ajánlást is tesz arra vonatkozóan, hogy a fenti feladatokat mely szerveknek kell ellátnia. Ezt egy összefoglaló ábrában tálalja, melyben a kibervédelem feladatrendszerét az egyes életciklus-elem függvényében osztja fel a kulcsszereplők között (ld. 1. ábra).



1. ábra: A kibervédelem életciklus modellje. Forrás: NATO CCDCOE National Cyber Security Framework Manual

A feladatokhoz rendelt szervezeti egységek jelentős részben a Belügyminisztérium alárendeltségébe tartoznak, megerősítve ezzel azt az előzetes feltételezést, hogy a kibervédelem elsősorban belbiztonsági feladat.

A teljes kibervédelmi struktúra kiépítéséhez a CCD COE keretrendszere 20 javaslatot, illetve tanulságot emel ki, melyet figyelembe kell venni!

1. Minden ország más, ezért egyéni kibervédelmi stratégiát kell kidolgozni!
2. A stratégia csatlakozzon más nemzetek stratégiájához és a nemzetközi szervezetek ajánlásaihoz!
3. Legyen kidolgozva egy olyan frissítési és ellenőrzési eljárás, melynek segítségével a szabályozás mindig a valós kockázatokra adhat választ!
4. Legyen felsőszintű, kormányzati és középszintű, szervezeti koordinációs csoport!
5. Legyenek beazonosítva a kritikus szolgáltatások és infrastruktúrák!
6. Meg kell teremteni a kibertudatosságot, elsősorban a jogszabályalkotók szintjén!
7. Biztosítani kell az információk formális és informális áramlását a szereplők között!
8. Ki kell dolgozni a közös fogalmi rendszert!

9. Olyan jogszabályi rendszert kell létrehozni, mely az alapelveket magas szinten, az operatív munkához szükséges szabályokat rugalmasan változtatható, alacsony szintű rendeletekben szabályozza!
10. A kulcsfontosságú szervezeteknek rugalmasnak kell lenniük az operatív munkában!
11. Ne legyenek lyukak a jogszabályi rendszerben!
12. A szervezeten belüli információáramlást elő kell segíteni!
13. A fenyegetési környezet folyamatosan változik, ezt figyelembe kell venni a jogszabályalkotásban! Ne legyenek elavult szabályozások!
14. Az operatív műveletek esetén a szervezetek között rugalmas együttműködést kell kialakítani!
15. Tisztázni kell az információátadás és az adatvédelem közötti egyensúlyt!
16. Küzdeni kell a digitális írástudatlanság ellen!
17. A nemzetközi kötelezettségvállalásokat a helyükön kell kezelni!
18. Az alapvető információbiztonsági követelmények megvalósítását meg kell követelni!
19. Törekedni kell a nemzetközi interoperabilitásra (műszaki és szervezeti értelemben is)!
20. Tanulni kell más országok tapasztalatából!

Belbiztonsági feladatok Magyarországon

Jogszabályi környezet

A rendvédelmi szervek kibervédelemmel kapcsolatos feladatait számos különböző jogszabály rendezi. A tanulmány írásának időpontjában ezek nem alkotnak egységes, összefüggő, minden feladatot teljesen lefedő rendszert, de a 2012-ben megindult kibervédelmi szabályozás egy későbbi fázisában, a tapasztalatok alapján ezeket a hiányokat pótolni lehet. A legfelsőbb szintű jogszabályok lehetőséget adnak arra, hogy az alsóbb szintű jogszabályok rugalmasan alkalmazkodjanak a változó körülményekhez.

Polgári titkosszolgálatok

A nemzetbiztonsági szolgálatok működését szabályozó 1995. évi CXXV. törvény [7] a kibervédelem tekintetében kizárólag a Katonai Nemzetbiztonsági Szolgálatnak ad feladatokat. A polgári titkosszolgálatok tevékenységében a kibervédelem, illetve az informatikai jellegű tevékenység nem nevesített, közvetett cél. A kibervédelmi stratégia azonban nevesíti ezt a célt: „A kiberbiztonsággal összefüggő feladatok ellátását a specifikus szakértelemmel és hatáskörrel rendelkező szervezetekhez szükséges telepíteni, amely szervezetek nem csak egymással, hanem az adat- és titokvédelem területén hatósági feladatokat ellátó más szervezetekkel is együttműködnek. A feladatellátás érinti a nemzetbiztonsági, honvédelmi, bűnüldözési, katasztrófavédelmi és létfontosságú intézmények és létesítmények védelmével kapcsolatos feladatokat ellátó szervezeteket, valamint az elektronikus információbiztonság területén hatósági jogosítványokkal rendelkező intézményeket.”

Kibervédelmi feladatot a jogszabályok alapján egyedül a Nemzetbiztonsági Szakszolgálat kap. A szervezet tevékenysége kettős. Egyrészt az Ibtv., illetve annak az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről szóló 233/2013. (VI. 30.) Korm. rendelete [8] alapján kormányzati eseménykezelő központként működik. Másrészt a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról szóló 36/2013. (VII. 17.) BM rendelet (továbbiakban: BM rendelet) [9] ezt a szervezetet jelölte ki a belügyi szervek vonatkozásában a sérülékenységvizsgálattal összefüggő feladatok ellátására.

Katasztrófavédelmi szervezet

Az Országos Katasztrófavédelmi Főigazgatóság a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény [10] alapján felelős számos kritikus információs infrastruktúra védelmének felügyeletéért. Az Ibtv. ennek a feladatnak a kibervédelmi aspektusait nem részletezi, de több helyen is megerősíti azt, hogy a létfontosságú rendszerelemeket informatikai szempontból is védeni szükséges, ezért az OKF-et és a törvényben nevesített szervezeteket együttműködésre utasítja.

Az OKF emellett eseménykezelő központot működtet Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (LRLIBEK) elnevezéssel. Ezt a feladatot a BM rendelet határozza meg számára.

Rendőrség

A rendőrségi és terrorelhárító szervek feladata a kibervédelem egészében rendkívül fontos, de Magyarországon nem pontosan szabályozott. Annak ellenére, hogy az informatikai bűnözés területén mérvadó nemzetközi egyezmény Budapest nevét viseli, a magyar jogrend pedig részletesen foglalkozik a kiberbűncselekményekkel és azok szankcionálásával, a szóba jöhető szervezetek feladatkiosztásánál ez a terület rendkívül alulreprezentált.

Gyömbér Béla gyűjtése szerint [11] a Rendőrségen belül a területtel foglalkozik a Készenléti Rendőrség Nemzeti Nyomozó Iroda Csúcstechnológiai Bűnözés Elleni Osztály, a Budapesti Rendőr-főkapitányság, Gazdaságvédelmi Osztály, Számítógépes Bűnözés Elleni Alosztály, valamint a Terrorelhárítási Központ, Terrorizmus és Számítógépes Bűnözés Elleni Monitoring Egység.

Egyéb belügyi szervek

A törvényben nevesített rendvédelmi szervek mellett az Ibtv. alapján további szervezetek kaptak feladatokat a kibervédelemben. Egyrészt a BM rendelet szerint a belügyi szervek zárt célú elektronikus információs rendszerei biztonságának központi felügyeletéről a belügyminiszter a Belügyminisztérium Miniszteri Kabinet útján gondoskodik. Másrészt a részben a BM felelősségébe tartozó Nemzeti Közszolgálati Egyetemnek kell bizonyos oktatási és kutatási tevékenységet ellátni. Az Egyetem felelős elsősorban a kibervédelmi szakemberek képzéséért is.

Megfelelés a nemzetközi ajánlásoknak

A nemzetközi szervezetek által kidolgozott ajánlások és keretrendszerek körvonalazzák azt, hogy milyen feladatokat kell ellátnia a belbiztonsági szerveknek a kibervédelmi területen. Az 1. táblázat felsorolja azokat a követelményeket, melyek az ajánlásokból származnak, egyben jelzi azt, hogy jelenleg hatályos magyar jogszabályok szerint melyik intézmény foglalkozik ezekkel a követelményekkel.

Feladatok	Titkosszolgálatok	OKF	Rendőrség	Egyéb
Jogszabályalkotás				X (BM)
Részvétel a nemzeti kiberbiztonsági tanács munkájában				X (BM)
Nemzetközi együttműködés	X	X	X	X
Köz- és magánegyüttműködés a kiberbiztonság területén		X		
Nemzeti kockázati szempontrendszer meghatározása, kritikus szolgáltatások és infrastruktúrák beazonosítása	X	X		
Nemzeti CERT működtetése	X			

Incidensjelentési eljárások kidolgozása	X			
Kibervédelmi gyakorlatok szervezése	X			
Humán képességek fejlesztése, kutatás-fejlesztés támogatása				X (NKE)
Kiberbűnözés visszaszorítása			X	
A biztonság és az adatvédelem közötti összhang kialakítása	X		X	
Információáramlás elősegítése				X (BM)

1. táblázat: Belbiztonsági szervezetek feladatai a kibervédelem területén

Az ajánlásokból eredő feladatok mindegyike lefedésre került, ám ezek különböző érettségi szinten vannak. Az egyes teendők állapota a nyilvánosan elérhető információk alapján a következőképp alakul.

- **Jogszabályalkotás**: Az Ibtv. és annak végrehajtási rendeletei jó alapot teremtenek a kibervédelem teljes rendszerének kiépítéséhez. Egy magas szintű törvény időtálló keretet ad, a kormányrendeletek kijelölik az intézményrendszert, a miniszteri szintű rendeletek pedig elég rugalmasak a folyamatosan változó körülmények követéséhez. A tapasztalatok alapján erre a rendszerre építhető fel a minősített időszakok kibervédelmi tevékenysége. Szintén jól körülhatárolt a kritikus információs infrastruktúrákkal kapcsolatos feladatrendszer. Hiányzik azonban jogszabályokból a titkosszolgálatok adott területen követendő tevékenységeinek nevesítése, illetve a kiberbűnözés elleni tevékenység kiemelt támogatása.
- **Részvétel a nemzeti kiberbiztonsági tanács munkájában**: A Nemzeti Kiberbiztonsági Koordinációs Tanács munkájában a Belügyminisztérium magas rangú képviselővel vesz részt, képviseli a tárca alá tartozó szervezeteket.
- **Nemzetközi együttműködés**: Mind a BM, mind az egyes szervezetek részvétele kiemelten fontos a nemzetközi együttműködések és szervezetek munkájában. Ennek koordinációja minisztériumi szintet követel meg. Ki kell emelni a Nemzetbiztonsági Szakszolgálaton belül működő CERT nemzetközi kapcsolatokban való részvételének fontosságát, illetve meg kell említeni az Interpol/Europol kiberbűnüldözési kezdeményezéseit, melyben a magyar részvétel hasznos tapasztalatokat hozhat!
- **Köz- és magánegyüttműködés**: Elsősorban a kritikus információs infrastruktúrák védelmében kulcsfontosságú a sokszor privát kézben levő rendszerelemek üzemeltetőivel való aktív együttműködés. Ez a jelenleg hatósági megközelítésű kapcsolat lényegesen hatékonyabb akkor, ha valamilyen kötetlenebb, pl. egyesületi együttműködés is párosul hozzá. Ilyen kezdeményezés az Önkéntes Kibervédelmi Összefogás (KIBEV) is, melynek célja az érintett szervezetek kibervédelemért felelős személyeinek megszólítása állami és civil oldalról is.
- **Nemzeti kockázati szempontrendszer meghatározása, kritikus szolgáltatások és infrastruktúrák beazonosítása**: Az Ibtv. rendelkezéseinek értelmében az érintett szervezetek elektronikus információs rendszereit és magát a szervezetet is kockázatalapon be kell sorolni. A kritikus információs infrastruktúrák esetében a rendszerelemeket és ezek kockázati szempontjait az OKF-nek, illetve részben az Alkotmányvédelmi Hivatalnak kellene meghatározni! Ennek állapotára vonatkozóan nem áll rendelkezésre nyilvános információ.
- **Nemzeti CERT működtetése**: A Nemzetbiztonsági Szakszolgálat keretében a nemzeti CERT megkezdte működését, a CERT-Hungary korábbi infrastruktúrájára és kapcsolatrendszerére építve. A működés hatékonysága és az esetleges problémák később válnak értékelhetővé.

- **Incidensjelentési eljárások kidolgozása**: Az Ibtv. által megszabott egyik legfontosabb feladat a kiberbiztonsági incidensek jelentése. Ennek eljárásrendjére nemzetközi ajánlások állnak rendelkezésre, de Magyarországon nem egyértelmű ezek használata.
- **Kibervédelmi gyakorlatok szervezése**: A CERT-Hungary évek óta szervez kibervédelmi gyakorlatokat, illetve részt vesz ilyen nemzetközi rendezvényeken. Ezek folytatása, illetve kiterjesztése kiemelt fontosságú az elkövetkező időszakban.
- **Humán képességek fejlesztése, kutatás-fejlesztés támogatása**: Az Ibtv. az információvédelemért felelős személyek képzését kötelezően írja elő, ami fontos lépés a széleskörű tudatosság elterjesztésében. Vannak azonban hiányterületek, elsősorban a szakirányú műszaki felkészítés területén. Ezt, valamint a műszaki és társadalomtudományi irányú kibervédelmi K+F tevékenység támogatását erőteljesen kell támogatni!
- **Kiberbűnözés visszaszorítása**: Az intézményrendszer szétaprózott, a képességek fejlesztése esetleges, pedig mind az oktatási bázis, mind a nemzetközi kapcsolatrendszer adott ahhoz, hogy Magyarország hatékonyan vehessen részt a kiberbűnözés visszaszorítását célzó együttműködésekben.
- **A biztonság és az adatvédelem közötti összhang kialakítása:** Az információtechnológia elterjedése lehetőséget kínál arra, hogy az állam érdekeit és törvényeit sértő tevékenységeket célzottan és minden korábbinál hatékonyabban lehessen visszaszorítani. Ez azonban sértheti a magánszemélyek privát szféráját. Meg kell találni a hatékony egyensúlyt a bűnüldözés és az adatvédelem között, hangsúlyozva azt a nemzetközi gyakorlatot, hogy a személyes adatok védelmét érintő csekély jogszabályi lazítás is képes jelentősen növelni a nyomozati cselekmények hatékonyságát.
- **Információáramlás elősegítése:** A Belügyminisztérium szervezetein belül a kibervédelem feladatainak jelentős része összpontosul. Ez lehetővé teszi azt, hogy a minisztériumon belül olyan szakirányú koordináció épüljön ki, melynek segítségével a szervezetek közötti információáramlás akadálymentessé válik. Nem áll rendelkezésre nyilvános információ arról, hogy ezt a minisztérium hogyan kívánja megoldani, illetve a hatékonyság értékelését is csak később célszerű megtenni.

Összefoglalás

Magyarországon a nemzetközi ajánlásoknak megfelelően épül fel a kibervédelem belbiztonsági struktúrája. Számos területen nemzetközi viszonylatban is élenjáró együttműködések születtek a kormányzaton belül. Az Ibtv. olyan keretet ad, melyen belül hatékonyan oldható meg az ország kibervédelme. Az Ibtv.-t és annak végrehajtási rendeleteit, valamint a korábban elkészült, kibervédelmet érintő jogszabályok tapasztalatait azonban még korai lenne értékelni.

A kibervédelmi szabályozás az operatív feladatok döntő többségét a Belügyminisztériumhoz rendelte. Ennek megfelelően a minisztérium felelőssége és lehetősége is hatalmas. Belbiztonsági területen a kiberbűnözés és kiberterrorizmus elleni tevékenység esetében lehet lemaradást megállapítani. Amennyiben a Belügyminisztériumon belüli kibervédelmi koordináció sikeres lesz, és jól használják ki a rendelkezésre álló tudásbázist és erőforrásokat, ez a lemaradás gyorsan felszámolható.

Irodalomjegyzék

[1] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

[2] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

[3] Wamala, F.: *The ITU National Cybersecurity Strategy Guide.* International Telecommunication Union, 2011.

[4] *National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace*. European Network and Information Security Agency (ENISA), 2012.

[5] Klimburg, A. (ed): *National Cyber Security Framework Manual*. NATO CCD COE Publication, Tallinn 2012

[6] 2010. évi XLIII. törvény a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról

[7] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatok működéséről

[8] 233/2013. (VI. 30.) Korm. rendelet az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről

[9] 36/2013. (VII. 17.) BM rendelet a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról

[10] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

[11] Gyömbér, B.: *Reszkessetek betörők.* Szerzői jog a XXI. században blog, http://copyrightinthexxicentury.blogspot.hu/2012/10/reszkessetek-betorok.html