XXII. Fiatal Műszakiak Tudományos Ülésszaka, 2017. Kolozsvár, 351–354. DOI: 10.33895/mtk-2017.07.80
http://hdl.handle.net/10598/29842

ÚJ ALAPOKON A MAGYARORSZÁGI KIBERVÉDELMI STRATÉGIA

NEW FUNDS OF THE CYBER SECURITY STRATEGY IN HUNGARY

Rajnai Zoltán[1], Fregan Beatrix[2]

[1]*Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar,*
Cím: 1081 Budapest, Népszínház u. 8., Tel: +36-1-666-5401,
rajnai.zoltan@bgk.uni-obuda.hu

[2]*Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar,*
fregan.beatrix@uni-nke.hu

Abstract

Hungary is focused on the role of national and international protection of cyberspace. The government's IT networks, the security of e-government has a high priority. The European Union Network and Information Security Directives givs a new foundations for the cyber security strategies. The authors present the legal foundations of the base of the Hungarian cyber security.

Keywords: *Information security, Cybersecurity, cybersecurity strategy*

Összefoglalás

Magyarország kiemelt szerepet szán a kibertér hazai és nemzetközi védelmére. A kormányzati informatikai hálózatok, az e-közigazgatás biztonsága kiemelt feladat. Az Európai Unió hálózatbiztonsági irányelvei új alapokra helyezi a kiberbiztonsági stratégiákat. A szerzők ennek megfelelően mutatják be a magyarországi kiberbiztonság jogi alapjait.

Kulcsszavak: *Információbiztonság, kibervédelem, kiberbiztonsági stratégia*

Magyarország 2013-ban nemzetközi téren is nagyot lépett előre az elktronikus információk biztonsága terén. Nemzetközi értékelési rendszerben világviszonylatban 6., az európai térségben a 3. helyre rangsorolták. Mindez annak volt köszönhető, hogy az Európai Unió tagállamai között is szinte elsőként alkotta meg nemzeti kiberbitztonsági stratégiáját, valamint az elektronikus információbiztonságról szóló törvényt (Ibtv.). Ezekhez természetesen hozzájárultak azok az ágazati törvények, rendeletek, amelyek az egyes szakterületekre részletesen fogalmazták meg a követelményeket és az azok teljesüléséhez szükséges feladatokat.

Az említett jogszabályok hatályba lépését követően megalakításra került a kormányzati eseménykezelő központ, a GovCERT. A Kormányzati Eseménykezelő Központ a magyar és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi szervezetek részére, mint az országon belüli koordinációs szervezet végzi az internetet támadási csatornaként felhasználó incidensek kezelését és elhárításának koordinálását, továbbá közzéteszi a felismert és publikált szoftver sérülékeny-

ségeket. A Központ a szolgáltatásait (preventív információ-megosztás és operatív incidens-kezelés) a kormányzati szervezetek és önkormányzatok részére nyújtja.[1]

A kormányzati eseménykezelő Központ szolgáltatásai lehetnek:

- **Preventív szolgáltatás:** Napi rendszerességű hálózatbiztonsági helyzet értékelések és elemzések készítése és jelentése, valamint azonnali figyelmeztetések a kritikus hálózatbiztonsági eseményekről.
- **Incidenskezelés és koordináció:** Folyamatos rendelkezésre állás: a Központ 7/24 órás ügyeletet működtet, ahol az ügyfeleket ért hálózatbiztonsági események, illetve támadások nemzetközi és hazai szintű kezelésére és az elhárítás koordinációjára.
- **Sérülékenység kezelési szolgáltatás:** Megbízható forrásokból (nemzetközi CERT közösség, szoftverszállítók, biztonsági szervezetek, stb.) származó szoftver sérülékenységi információk folyamatos értékelése, elemzése, magyarra fordítása, kockázati osztályba sorolása és jelentése az állami- és önkormányzati szervek részére.

Az eseménykezelő központ feladatai mellett a hatósági jogköröket a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) látja el. **A hatóság feladatköre:**

1. Elbírálja az Ibtv. hatálya alá tartozó elektronikus információs rendszerek biztonsági osztályba sorolását;
2. Ellenőrzi az elektronikus információs rendszerek biztonsági osztályba és a szervezetek biztonsági szintbe sorolására vonatkozó jogszabályi követelmények teljesülését
3. A rendelkezésre álló információk alapján kockázatelemzést végez
4. Éves ellenőrzési terv alapján az érintett ügyfeleknél ellenőrzi az információbiztonsági követelményeknek való megfelelést
5. Elrendeli az ellenőrzés során feltárt, vagy más módon tudomására jutott biztonsági rések elhárítását, és ellenőrzi a helyreállító intézkedés eredményességét
6. Éves jelentést készít a Kormány részére az elektronikus információs rendszerek biztonságával, a létfontosságú információs rendszerelemek védelmével, és a kibervédelem helyzetével kapcsolatban
7. Együttműködik az Elektronikus Ügyintézési Felügyelettel a szabályozott elektronikus ügyintézési szolgáltatókra vonatkozó biztonsági követelmények biztosításában
8. Együttműködik a Kormányzati Eseménykezelő Központtal, valamint a Nemzeti Kiberbiztonsági Koordinációs Tanáccsal
9. Ügyfelei számára engedélyezi és felügyeli az elektronikus információs rendszerek EGT-államban való üzemeltetését
10. A központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában ellenőrzi az információbiztonsági követelmények megtartását
11. A Kormányzati Eseménykezelő Központtal együtt részt vesz a Nemzeti Kiberbiztonsági Koordinációs tanács által felügyelt információtechnológiai, hálózatbiztonsági, információmegosztási és incidenskezelési munkacsoportokban.

2015. október 1-jei hatállyal a Belügyminisztérium felügyelete alatt az említett két szervezet (GovCERT, NEIH) feladatrendszerével megalakult a Nemzeti Kibervédelmi Intézet, amely a felügyeleti munka mellett már a hatósági jogköröket is gyakorolja.

Nemzetközi kitekintés

2016 július 19-én az Európai Unió a hálózatbiztonság és információbiztonság területén egységes törekvéseként megjelentette az úgynevezett NIS irányelveket, amelyben a

tagállamok részére előírta, hogy rendelkezzenek az irányelvben bemutatott területeken kiberbiztonsági stratégiával.[3] Ennek megfelelően Magyarország előtt két lehetőség adódott. Vagy módosítja a már meglévő, 2013-ban kormányhatározattal elfogadott kiberbiztonsági sztratégiát, vagy az irányelveknek megfelelően új stratégiát alkot. A szakemberek egységes álláspontja egy új stratégia megalkotását célozta meg, így megkezdődött a jogszabály előkészítése. A NIS irányelv az első közösségi szintű szabályozás az információbiztonság területén, mely kötelezően és geopolitikai alapon határoz meg szabályokat és kötelező együttműködést egyes intézmények számára. Korábban is megfigyelhető volt a tagállamok információbiztonsággal foglalkozó szervei közötti együttműködés, viszont ez önkéntesen és bizalmi alapon valósult meg. Az irányelv célja, hogy megfogalmazzon egy közös intézmény és eszköztárat a tagállamok számára, illetve egy európai szintű együttműködés alapjait fogalmazza meg. Ennek megfelelően elkülöníthetünk nemzeti szinten végrehajtandó és közösségi szinten végrehajtandó feladatokat.

Nemzeti szintű feladatok

Az irányelv célja, hogy minden tagállam rendelkezzen minimális képességekkel, a szükséges intézményekkel, szabályokkal, valamint a hálózat- és információbiztonság magas szintjét biztosító nemzeti szintű stratégiával. Az irányelv hatályba lépését követően 21 hónap áll rendelkezésére a tagállamoknak ezen intézkedésekre, a jogszabályok létrehozására, módosítására.

Az irányelv előírásai szerint minden tagállamnak ki kell jelölnie egy vagy több (akár szektoronként egy-egy) számítógépbiztonsági eseményekre reagáló csoportot (továbbiakban: CSIRT), amely legalább az adott szektor incidenskezelésért felelős.[4]

Az irányelv elsőként definiálja az ún. alapvető szolgáltatásokat nyújtó szolgáltatók csoportját, melybe a digitális infrastruktúrák, energetika, közlekedés, banki szolgáltatások, pénzügyi szolgáltatások, egészségügyi szektor tartozik.

A második alanyi kör a digitális szolgáltatásokat nyújtó szolgáltatók csoportja, melyek körébe pl. az online piactér, keresőmotorok, közösségi hálózatok, felhő szolgáltatók tartoznak.

Az irányelv különböző kijelölési szabályokat, megfelelési kritériumokat, valamint incidens bejelentési kötelezettségeket fogalmaz meg az alapvető szolgáltatásokat nyújtó szolgáltatókra vonatkozóan csakúgy, mint a digitális szolgáltatást nyújtó szolgáltatókra.

A fent felsorolt szektorokban a tagállamoknak ki kell jelölniük a meghatározott szempontok figyelembevételével a hatály alá eső vállalatokat, cégeket. Ehhez szektoronként pontosítani, specializálni kell az irányelv rendelkezéseiben megfogalmazott kijelölés kritériumait. A szolgáltatók kijelölésére az átültetési időszak (21 hónap) után 6 hónapja lesz a tagállamoknak.

EU szintű feladatok

Közösségi szintű együttműködéseket is megfogalmaz az irányelv, annak érdekében, hogy aktív, kiszámítható és hatékony képességekkel rendelkezzünk az egész EU területén. Ezen célból az irányelv létrehozta a hatóságok együttműködésére szolgáló Együttműködési Csoportot, valamint a CSIRT-ek együttműködését biztosító CSIRT hálózatot.

A szabályozás kitér a határon átnyúló események esetében a tagállamok által követendő eljárásra, együttműködésre is.

Az irányelv hatályba lépését követő 6. hónap végére EU szinten létrehozandó CSIRT-hálózat és az Együttműködési Csoport nemzeti résztvevőit (nemzeti CSIRT és kompetens hatóság) ki kell jelölnie a tagállamok döntéshozóinak.

Hálózat és Információbiztonsági irányelv számos végrehajtási aktus létrehozását írja elő (például: az Együttműködési Csoport működését biztosító eljárási szabályok, biztonsági és bejelentési követelmények a digitális szolgáltatást nyújtó szolgáltatók számára, valamint a digitális szolgáltatókra vonatkozó bejelentési köztelezettség formai és eljárási követelményei) a Bizottság számára. Ezen feladatok végrehajtására 2016. májusában létrehozta a Bizottság a NIS szakértői csoportot, melyben Magyarországot az NKI képviseli.

Következtetések

Magyarország a kiberbiztonság területét továbbra is kiemelt fontosságúnak tekinti. A hazai állami és kormányzati-önkormányzati rendszerek biztonsága mellett olyan új kihívások jelentek meg, mint a Digitális Jóléti Programból adódó feladatok, a biztonságtudatosítás és az euróai uniós elveknek való megfelelés. E területeken a Kormány minden tőle telhetőt megtesz a biztonságos informatikai hálózatok és az adatbiztonság érdekében.

Szakirodalmi hivatkozások

[1] www.cert-hungary.hu

[2] http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN&toc=OJ:L:2016:194:TOC

[3] Farkas Tibor, Sándor Miklós: *A honvédség állandó hírhálózatának fejlesztési kérdései*, Kard és toll: válogatás a hadtudomány doktorandu-szainak tanulmányaiból 1:(2) pp. 158-164. (2006).

[4] Farkas Tibor, Hronyecz Erika: *The infocommunication system requirements and analysis of the communication of the deployable rapid diagnostic laboratory support „sampling group" II.*, Academic and applied research in public management science XIV:(1) pp. 53-61. (2015) NKE