HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. június

KIBERBIZTONSÁGI ESEMÉNYKEZELŐ SZERVEZETEK RENDELTETÉSE, FELADATAI

PURPOSE, AND TASKS OF CYBERSECURITY CENTERS

MUNK Sándor

(OCID: 0000-0001-8576-308X)

munk.sandor@uni-nke.hu

Absztrakt

Napjaink társadalmi, gazdasági, és mindennapi tevékenysége egyre növekvő mértékben függ a kiberteret alkotó, globálisan összekapcsolt, decentralizált informatikai rendszerek és hálózatok által nyújtott szolgáltatásoktól.
A kiberbiztonság megteremtése és fenntartása a kiberbiztonsági szervezetek, az informatikai rendszereket, hálózatokat működtető szervezetek, az állampolgárok, és a média kiemelt jelentőségű közös feladata, amely több szereplőre kiterjedő és széleskörű együttműködést igényel.
Jelen publikáció – egy háromrészes sorozat első részeként – bemutatja a kiberbiztonsági szervezetek fogalmát, rendszerezi, elemzi főbb típusait, funkcióikat, feladataikat.
A publikáció a KÖFOP-2.1.2-VEKOP-15-2016-00001 'A jó kormányzást megalapozó közszolgálat-fejlesztés' projekt támogatásával, a Kiberbiztonsági Ludovika Kiemelt Kutató-műhely keretében készült.

Kulcsszavak: *kiberbiztonság, kiberbiztonsági szervezetek, kiberbiztonsági információcsere, interoperabilitás*

Abstract

Today's social, economic, and every-day activities are increasingly dependent on the services provided by globally interconnected, decentralized IT systems and networks, the cyberspace.
Ensuring cyber security is a common task of cybersecurity organisations, IT system-network operators, citizens, and media, which requires wide range, extensive cooperation of these actors.
Recent paper – as a first part of a three-part series - presents the concept of cyber security organisation, and analyses their main types, purpose, functions, and tasks.
The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in the Cyber Security Ludovika Workshop.

Keywords: *cybersecurity, cybersecurity organisations, cybersecurity information exchange, interoperability*

A kézirat benyújtásának dátuma (Date of the submission): (2018.03.26.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.02.

BEVEZETÉS

Napjaink társadalmi, gazdasági, és mindennapi tevékenysége egyre növekvő mértékben függ a kiberteret alkotó, globálisan összekapcsolt, decentralizált informatikai rendszerek és hálózatok által nyújtott szolgáltatásoktól. Az informatikai szolgáltatások egyre jelentősebb mértékben járulnak hozzá az állami működés hatékonyságának, a vállalkozások eredményességének és versenyképességének, valamint az állampolgárok életminőségének javításához. A növekvő függőség egyben növekvő kiszolgáltatottságot, kockázatot is jelent, mivel az informatikai rendszerek, hálózatok, és az általuk kezelt adatok, információk biztonságának (bizalmasságának, sértetlenségének, és rendelkezésre állásának) megsértése maga után vonja az informatikai szolgáltatásokra épülő rendszerek, folyamatok, szolgáltatások biztonságának sérülését is, ami jelentős kihatással lehet az átfogó biztonság politikai, katonai, gazdasági, pénzügyi, és társadalmi dimenzióira is.

A kibertérben világszerte növekvő mértékben jelentkező kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a nemzeti kritikus infrastruktúra működtetésének biztosítására minden államnak, így – Magyarország Nemzeti Biztonsági Stratégiájában megfogalmazottak szerint – hazánknak is készen kell állnia. A kiberbiztonság megteremtése és fenntartása nem csak a kiberbiztonsági (információbiztonsági, informatikai biztonsági) szervezetek, hanem az informatikai rendszereket, hálózatokat működtető szervezetek, az állampolgárok, és a média kiemelt jelentőségű feladata.

A kibertér informatikai rendszereinek, hálózatainak globális, szövevényes összekapcsolódása következtében az egyik rendszer biztonságának sérülése elvezethet egy másik (más országban, más ágazatban működő) rendszer biztonságának sérüléséhez. Egy magán vállalkozás által üzemeltetett informatikai infrastruktúra támadásával támadhatóvá válnak az infrastruktúra szolgáltatásait igénybevevő kormányzati, gazdasági, és más informatikai rendszerek is. Az Internet lényegében bárhonnan könnyű útvonalat biztosít kibertámadások, kiberbűncselekmények végrehajtásához. Mindebből következik, hogy a kiberbiztonság fenntartása több szereplőre kiterjedő és széleskörű együttműködést igényel.

Jelen publikáció egy szélesebb körű, a kiberbiztonsági szervezetek információcsere igényeit, és az ehhez kapcsolódó interoperabilitási követelményeket vizsgáló kutatás első részét képezi. Ezt követi majd a szervezetek által kezelt, és köztük információk feltárása, végül a kapcsolódó interoperabilitási problémák és követelmények vizsgálata.

A kiberbiztonság fenntartásának alapvető feladatait angolul és magyarul is különböző megnevezésekkel jelölt biztonsági szervezetek (CERT, CSIRT, SOC, eseménykezelő/incidens kezelő, kiberbiztonsági műveleti központok[1]) valósítják meg, és további, speciális feladatokat ellátó, szolgáltatásokat nyújtó szervezetek támogatják. A kiberbiztonság fenntartásának minden szakértő, és minden szabályozó által alapvetőnek tartott feltétele ezen szervezetek eredményes és hatékony együttműködése.

Ennek megfelelően jelen publikáció célja a kiberbiztonsági szervezetek főbb típusainak, valamint ezen szervezetek funkcióinak és feladatainak rendszerezése. Ennek érdekében a következőkben:

- röviden összegezzük a kiberbiztonság alapvető fogalmait;
- áttekintjük és rendszerezzük a kiberbiztonsági szervezetek fogalmát és főbb típusait;
- valamint ezen szervezetek funkcióit és feladataikat.

[1] A rövidítések kifejtését, és a fogalmak értelmezését lásd később.

Köszönettel tartozok azon magyarországi kiberbiztonsági eseménykezelő központoknak, és az alábbiakban felsorolt vezetőiknek, munkatársaiknak, akik jelen publikáció kidolgozását személyes konzultációval és a kapcsolódó információk rendelkezésre bocsátásával segítették:
- a Kormányzati Eseménykezelő Központ részéről dr. Schmidt Miklós;
- a BM Országos Katasztrófavédelmi Főigazgatóság szervezetén belül működő Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja vezetője, dr. Gazdag Tibor tűzoltó alezredes, főosztályvezető helyettes;
- a MH Katonai Nemzetbiztonsági Szolgálat szervezetén belül működő Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ vezetője, dr. Kassai Károly ezredes;
- és az Internet Szolgáltatók Tanácsa által támogatott Hun-CERT vezetője, Rigó Ernő.

A KIBERBIZTONSÁG ALAPJAI

Kiberbiztonsági szervezetek alatt egyszerű nyelvtani értelmezés szerint is a kiberbiztonság fenntartásában érintett szervezeteket értünk. Ennek tényleges tartalma azonban értelemszerűen attól függ, hogy mit értünk kiberbiztonságon. A kiberbiztonság fogalmának azonban (mint oly sok fogalomnak) nincs egységesen értelmezett tartalma.

A biztonság (mint állapot) fogalom tartalmának meghatározása során mindenekelőtt azt kell megadnunk, hogy mi a biztonság alanya (minek a biztonságáról van szó) és melyek a biztonság összetevői (a biztonság alanyának fenntartandó tulajdonságai), amelyeket különböző hatások veszélyeztetnek.

A ***kiberbiztonság*** esetében a NATO Kibervédelmi Kiválósági Központ[2] kifejezés jegyzékében szereplő néhány kiemelt értelmezés szerint a biztonság alanya lehet:
- a kibertér[3] [1, 58. o.];
- a kibertérben található információk [2];
- a kiberkörnyezet, valamint a szervezeti és felhasználói erőforrások [3, 2. o.];
- az összekapcsolt hálózatok és az információs infrastruktúra, valamint a bennük található információk [4, 3. o.].

A fenti jelentős eltérésekkel szemben a biztonság összetevői közé viszonylag egységes értelmezés szerint a biztonság alanyának, annak összetevőinek bizalmassága (csak arra jogosultak számára hozzáférhetősége), sértetlensége, és rendelkezésre állása[4] tartoznak.

A kiberbiztonságot érintő fenyegetésekhez kapcsolódó két alapfogalom az ***esemény és biztonsági esemény (incidens)***. Ezek értelmezésében is vannak eltérések. Jelen publikációban részletesebb indoklás nélkül arra az értelmezésre építünk, amely szerint az esemény a kiberbiztonság esetleges, elvileg lehetséges megsértését eredményező kibertéri esemény, míg a biztonsági esemény az előbbiek közül csak a működési folyamatokat, a biztonságot nagy valószínűséggel fenyegető esemény.

A kiberbiztonság eltérő tartalmú értelmezéseit ***az érintett technikai rendszerek eltérő megnevezései*** is tarkítják, amelyek egyes esetekben (részben) eltérő tartalmakat is jelölnek, a legtöbb esetben azonban csak az őket alkalmazó szakmai körök hagyományait, nézőpontját, ko-

[2] NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE).
[3] Jelen publikációban nem foglalkozunk azzal, hogy a kibertér értelmezése, tartalma sem egységes, ami tovább növeli a kiberbiztonság értelmezésének sokféleségét.
[4] A szakirodalomban gyakran használt megjelöléssel CIA (Confidentiality, Integrity, Availability), ezen kívül a sértetlenségbe beleértve, vagy önállóan szerepeltetve a hitelesség (Authenticity) és a letagadhatatlanság (Non-repudiation) tulajdonságokat is.

rábbi dokumentumainak szóhasználatát tükrözik. Ennek megfelelően ezen rendszerek megnevezésére többek között találkozhatunk az informatikai, infokommunikációs, információtechnológiai (IT), elektronikus információs, elektronikus adatkezelő, hálózati és információs jelzőkkel. A különböző megnevezések mindegyike olyan technikai rendszert takar, amely technikai eszközökkel információkat (pontosabban az azokat reprezentáló adatokat) kezel, és ezzel információs tevékenységeket támogat, vagy valósít meg.

A továbbiakban jelen publikációban a fenti rendszerek megnevezésére az informatikai rendszer kifejezést használom, és a kiberbiztonsági jelzőt az informatikai biztonsági, IT biztonsági, elektronikus információbiztonsági, hálózati és információbiztonsági, stb. jelzők szinonimájaként alkalmazom. Megítélésem szerint a felsorolt kifejezések közötti tartalmi eltérések – ha egyes értelmezések szerint vannak is – a publikáció témája szempontjából lényegtelenek, elhanyagolhatóak.

Összességében megállapíthatjuk, hogy a kiberbiztonsági szervezet fogalmának értelmezése a kiberbiztonság és annak alapfogalmai értelmezésére épül, ezektől függően ugyanazon meghatározások is eltérő tartalmat takarnak. A továbbiakban ezzel nem foglalkozunk, a vizsgálat tárgyát képező kérdések esetében arra törekszünk majd, hogy megállapításaink az alapot képező fogalmak különböző értelmezései mellett is érvényesek maradjanak.

KIBERBIZTONSÁGI SZERVEZETEK ÉS TÍPUSAIK

A kiberbiztonsági szervezetek fogalmának és típusainak áttekintését arra az általános megállapításra építhetjük, hogy alapvető rendeltetésük informatikai rendszerek, hálózatok védelme, kiberbiztonsági események (incidensek) megelőzése és elhárítása. Az ilyen szervezetek két nagy csoportba sorolhatóak, amelyek a következőek:

- egy védendő informatikai rendszert, hálózatot közvetlenül felügyelő szervezetek;
- több védendő informatikai rendszer, hálózat biztonságában közreműködő szervezetek.

A következőkben röviden összegezzük ezen szervezetek főbb jellemzőit, majd bemutatunk néhány más, a kiberbiztonságot támogató, témánk szempontjából fontos szervezettípust.

Egy adott szervezet által üzemeltetett informatikai infrastruktúrát (rendszert, hálózatot) közvetlenül felügyelő kiberbiztonsági szervezet (szervezeti egység) megnevezése napjainkban ***kiberbiztonsági műveleti központ*** (kiberbiztonsági központ), vagy csoport[5], amelynek alapvető sajátossága a felügyelt, védett informatikai rendszer, hálózat biztonsági állapotának közvetlen figyelemmel kísérése (monitorozása), és szükség esetén a működésbe történő beavatkozás lehetősége.

A kiberbiztonsági műveleti központ szorosan együttműködik, esetleg közös szervezeti egységet alkothat informatikai rendszerfelügyeleti, hálózatfelügyeleti központokkal, csoportokkal. A kiberbiztonsági műveleti központon belül a felügyelt rendszerösszetevő alapján elkülöníthető informatikai biztonsági műveleti központ/csoport és hálózatbiztonsági központ/csoport. Egy adott szervezet működtethet egyetlen kiberbiztonsági műveleti központot, de nagyméretű, összetett szervezet esetében lehet több, a szervezeti informatikai infrastruktúra meghatározott részéért felelős kiberbiztonsági műveleti központ is.

A több védendő informatikai rendszer, hálózat biztonságát támogató kiberbiztonsági szervezet megnevezése a mai magyar terminológiával ***[kiberbiztonsági] (számítógépes) eseményke-***

[5] Cyber Security Operations Center, Information Security Operations Center, Security Operations Center.

zelő központ, amely az információbiztonsági törvény meghatározása szerint "az Európai Hálózat- és Információbiztonsági Ügynökség[6] ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik."[7] [5, 1. § 42.]

Az ENISA meghatározása szerint az eseménykezelő központ informatikai biztonsági szakértők csoportja, amelynek fő feladata az informatikai biztonsági eseményekre reagálás, ehhez kapcsolódó szolgáltatások nyújtása egy meghatározott 'ügyfélkör'[8] számára. Szolgáltatásaik a biztonsági események megelőzését, kockázatának csökkentését, a biztonságsértés bekövetkezése esetén pedig annak kezelését, és a helyreállítást támogatják. [6, 8. o.]

Az eseménykezelő központok alapvető sajátossága, hogy tevékenységük közvetve, az ügyfélkörükbe tartozó szervezetek kiberbiztonsági szervezetein, azok támogatásán keresztül járul hozzá az ügyfeleik által üzemeltetett informatikai rendszerek, hálózatok védelméhez. Az ügyfélkör lehet nemzetközi, nemzeti, ágazati kiterjedésű, vagy más alapon szervezett.

A kiberbiztonsági eseménykezelő és műveleti központokat a katonai alkalmazás fogalomrendszerét kölcsönözve nevezhetjük harcászati és hadműveleti szintű szervezetnek is.

A kiberbiztonsági műveleti, és eseménykezelő központok mellett vannak ***további szervezetek*** is, amelyek – elsősorban kiberbiztonsági információk rendelkezésre bocsátásával – jelentős mértékben járulnak hozzá a kiberbiztonság fenntartásához. Ezek a kiberbiztonsági szervezetek nyilvánosan, vagy egy meghatározott kör számára elérhetően nyújtanak többek között:

- kiberbiztonsági fenyegetésekre vonatkozó nyers, vagy elemzett adatokat, információkat tartalmazó, rendszeresen frissülő hírcsatornákat9;
- kiberbiztonsági fenyegetéseket hordozó címeket (IP, e-mail, web, stb.) tartalmazó feketelistákat;
- kiberbiztonsági fenyegetésekre vonatkozó, azok azonosítását, besorolását elősegítő fogalomjegyzékeket, taxonómiákat,
- valamint bekövetkezett kiberbiztonsági eseményekre vonatkozó összegzéseket, elemzéseket, statisztikákat.

Ilyen információkat saját tevékenységi területükre vonatkozóan természetesen a kiberbiztonsági műveleti központok és eseménykezelő központok is gyűjtenek, kezelnek, azonban szélesebb körű, felhasználhatóbb információkat egyrészt a nagyobb kiberbiztonsági cégek, másrészt a speciálisan a kiberbiztonsági fenyegetések felderítésére, elemzésére[10] létrehozott cégek nyújtanak.

Végül a ***kiberbiztonsághoz kapcsolódó feladatokkal rendelkező szervezetek*** közé tartoznak a védelmi szféra egyes szervezetei, valamint az informatikai összetevőket fejlesztő, gyártó cégek. Az előbbiek közé tartoznak például, a katonai kiberhadviselési szervezetek, a kiberbűnözés ellen tevékenykedő rendőri szervezetek, valamint a nemzetbiztonsági szervezetek egyes szakterületi szervezetei. Az utóbbiak ellenőrzik a termékeikben felfedezett sérülékenységeket, megoldást dolgoznak ki rá, és hibajavító (sérülékenység kiküszöbölő, vagy csökkentő) csomagokat bocsátanak ki.

---

[6] European Network and Information Security Agency (ENISA).

[7] A törvény kiegészítő megjegyzésével: európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team).

[8] Constituency, constituents.

[9] Cyber security feeds, cyber threat intelligence feeds.

[10] Cyber Threat Intelligence.

KIBERBIZTONSÁGI SZERVEZETEK FUNKCIÓI, FELADATAI

A kiberbiztonsági szervezetek feladatainak áttekintéséhez a legjobb alapot az első CERT-et létrehozó Carnegie Mellon University Szoftvermérnöki Intézete CERT részlegének a kiberbiztonsági eseménykezelő központok szolgáltatásaira vonatkozó anyagai [elsősorban 7] biztosítják. Nagyrészt ez képezte, képezi alapját az ENISA kapcsolódó dokumentumainak [8, 9] is. A kiberbiztonsági műveleti központok az eseménykezelő központokhoz hasonló feladatokat látnak el, kiegészítve ezeket a felügyelt informatikai rendszerekbe történő beavatkozások feladataival. Ez utóbbiakkal jelen publikációban nem foglalkozunk, mert nem kapcsolódnak a kiberbiztonsági szervezetek közötti információcsere kérdéseihez.

A kiberbiztonsági eseménykezelő szervezetek feladatai között, rendeltetésükből következően kiemelt szerepet az ügyfélkörükbe tartozó szervezeteknek nyújtott szolgáltatások töltenek be. Ezek a szervezetek ezen kívül természetesen számos további belső funkciót is megvalósítanak, azonban mivel kutatási témánkhoz közvetlenül ezek sem kapcsolódnak, a továbbiakban ezekkel sem foglalkozunk.

A ***kiberbiztonsági eseménykezelő szervezetek által nyújtott szolgáltatások*** három nagy csoportba – a reagáló (reaktív), a megelőző (proaktív), valamint a további biztonsági szolgáltatások[11] közé – sorolhatóak. A reagáló szolgáltatások a biztonsági események bekövetkezését követően a támogatott szervezetektől érkező kérésekre, jelentésekre adott válaszok, amelyek az eseménykezelő szervezet alapvető feladatai közé tartoznak. A megelőző szolgáltatások segítséget és információkat nyújtanak a támogatott szervezetek infrastruktúrájának és biztonsági folyamatainak fejlesztéséhez, a biztonsági események észlelése előtt, azok megelőzése, hatásuk és hatókörük csökkentése érdekében. A további biztonsági szolgáltatások nem közvetlenül a biztonsági esemény kezeléshez kapcsolódnak, a szervezetek átfogó biztonságát növelik.[12] [8, 4. o.]

A ***kiberbiztonsági szervezetek reagáló szolgáltatásai*** közé a riasztások és értesítések, a biztonsági események (incidensek) kezelése, a sérülékenységek kezelése, valamint a tárgyi leletek kezelése tartoznak. [7, 25. o.] A *riasztások és értesítések* bekövetkezett biztonsági eseményekre, új sérülékenységekre, várható fenyegetésekre, stb. vonatkozó információk, valamint a jelzett problémák kezelésére vonatkozó rövidtávú feladatok közreadása. Ezek származhatnak a kiberbiztonsági szervezettől, vagy érkezhetnek külső forrásokból.

A *biztonsági esemény (incidens) kezelő szolgáltatások* valamennyi kiberbiztonsági szervezet feladatrendszerének központi, kötelező összetevőjét képezik. A szolgáltatás összetevői közé az detektálás, az osztályozás, az elemzés, és a reagálás (ellenintézkedések) tartoznak. A detektálás az esemény bekövetkezésének érzékelését, vagy az erre vonatkozó bejelentés fogadását; az osztályozás az értékelést, kategorizálást, fontossági besorolást, és nyilvántartásba vételt; az elemzés az esemény tartalmának, érintettjeinek meghatározását; végül a reagálás a káros következmények felszámolásához, a működés helyreállításához szükséges tevékenységeket foglalja magában. Az eseménykezelő központok feladatai közé ezek közül elsősorban az elemzés, a reagálás koordinálása, támogatása, esetleg helyi segítése tartozik. [7, 26-27. o.]

A *sérülékenység kezelő szolgáltatások* tárgyát a hardver és szoftver összetevők sérülékenységei képezik. Ezek olyan hibák, vagy gyengeségek, amelyeket egy támadó kihasználhat egy rendszer, hálózat biztonságának megsértése során. A szolgáltatások rendeltetése ezen sérülé-

[11] Reactive services, proactive services, security quality management services. [7, 25. o.]

[12] Kockázatelemzés, üzletmenet folytonosság és katasztrófa utáni helyreállítás tervezés, biztonsági tanácsadás, biztonságtudatosság növelés, felkészítés/kiképzés, termék minősítés és tanúsítás. [7, 32-34. o.]

kenységek jellegének, működésmódjának, és hatásainak elemzése, valamint felkutatásuk és kiküszöbölésük (kijavításuk) eszközeinek, módszereinek meghatározása. Ez utóbbiak lehetnek javítócsomagok, javítások, vagy megkerülő megoldások. [7, 28. o.]

A *tárgyi leleteket kezelő szolgáltatások* tárgyát olyan, az informatikai rendszerekben található objektumok, egy behatolás maradványai (fájlok, naplófájl bejegyzések, rosszindulatú programok, stb.)[13] képezik, amelyek szerepet játszhattak, játszhatnak a rendszer biztonsági rendszerének támadó általi felderítésében, tesztelésében, vagy a rendszer támadásában. A szolgáltatások rendeltetése a tárgyi leletek begyűjtése, jellegének, működésmódjának, verziójának és felhasználásának elemzése, valamint észlelésük, eltávolításuk, és az ellenük való védelem eszközeinek, módszereinek meghatározása. [7, 28-29. o.]

A ***kiberbiztonsági szervezetek megelőző szolgáltatásai*** közé többek között a következők tartozhatnak:

- közlemények közreadása behatolásokról, sérülékenységekről, biztonsági tanácsadókról;
- technikai fejlesztések, új megoldások, kialakult trendek figyelemmel kísérése;
- kiberbiztonsági ellenőrzések és értékelések;
- biztonsági beállítások, karbantartási feladatok meghatározása, közreadása;
- támogatott szervezet specifikus biztonsági eszközök létrehozása;
- behatolás jelző/érzékelő szolgáltatások;
- biztonsági jellegű információk közreadása. [7, 29-32. o.]

KIBERBIZTONSÁGI SZERVEZETEK MAGYARORSZÁGON

Az első ***hálózatbiztonsági eseménykezelő központok Magyarországon*** az 1990-es évek végén jöttek létre. A *Hungary-CERT (ma Hun-CERT)* csoport a Magyarországon működő Internet kapcsolattal rendelkező számítógép-hálózatokkal összefüggő biztonságtechnikai problémák kezelésének, illetve azok megelőzésének céljából, az internetszolgáltatóknak nyújtott szolgáltatásokra jött létre a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága, a Magyarországi Vezető Informatikusok Szövetsége és a MTA Számítástechnikai és Automatizálási Kutató Intézet (SZTAKI) támogatásával. A Nemzeti Információs Infrastruktúra Fejlesztési Intézet keretében a szervezet által nyújtott Internet szolgáltatást igénybevevő felsőoktatási, kutatási, és közgyűjteményi szervezetek számítógépes és hálózati incidenseinek kezelésére, koordinációjára alakult meg a *NIIF-CSIRT,* HUNGARNET CERT munkacsoport (2016-tól Kormányzati Informatikai Fejlesztési Intézet, *KIFÜ CSIRT*).

A Puskás Tivadar Közalapítvány 2005-ben hozta létre a kritikus információs infrastruktúrák védelmére specializálódott CERT-Hungary Központot, amely egy 2009-es kormányrendelet alapján a magyar kritikus információs infrastruktúrák védelmét, valamint az elektronikus közszolgáltatásokat biztosító központi rendszeren megvalósuló kommunikáció biztonságát, a vírus- és más támadások káros hatásainak korlátozását szolgáló *Nemzeti Hálózatbiztonsági Központtá (CERT-Hungary)* alakult.[14]

A 2013-ban elfogadott Nemzeti Kiberbiztonsági Stratégiában foglaltakra is épülő 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, szervezeti átalakulással, a Nemzeti Kibervédelmi Intézet részeként hozta létre a *Kormányzati Eseménykezelő Központot (GovCERT-Hungary),* valamint határozta meg három ágazati eseménykezelő központ működtetését.

[13] A szakterület szóhasználatában: artifacts.

[14] Nem tartozott a Nemzeti Hálózatbiztonsági Központ tevékenységi körébe a kormányzati célú elkülönült hírközlő (nemzetbiztonsági, honvédelmi, diplomáciai) hálózatok biztonsága.

A ***magyar kiberbiztonsági eseménykezelő szervezetek körét*** és az általuk felügyelt informatikai rendszereket, hálózatokat napjainkban a következő lista tartalmazza[15]:

- Kormányzati Eseménykezelő Központ: állami és önkormányzati nyílt informatikai rendszerek;
- Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja: nemzeti létfontosságú rendszerek és létesítmények (előző pontba nem tartozó) informatikai rendszerei;
- Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ: honvédelmi célú informatikai rendszerek, és a katonai nemzetbiztonsági műveleti hálózat, valamint a MH Kormányzati Célú Elkülönült Hírközlő Hálózat;
- az Információs Hivatal Eseménykezelő Központja: a polgári hírszerzés informatikai rendszerei, és a polgári nemzetbiztonsági műveleti hálózat;
- SZTAKI Hun-CERT munkacsoport: az Internet Szolgáltatók Tanácsa tagszervezetei által üzemeltetett informatikai rendszerek, hálózatok;
- KIFÜ CSIRT csoport: az NIIF program hálózata, és az ahhoz csatlakozó informatikai rendszerek.

A felsoroltakon kívül természetesen informatikai rendszerei, és hálózatai kiberbiztonságának fenntartására számos szervezet működtet szervezeti szintű kiberbiztonsági eseménykezelő központokat, vagy kiberbiztonsági műveleti központokat.

A *Kormányzati Eseménykezelő Központ (GovCERT-Hungary)* a magyar kormányzat központi információ-megosztó és incidenskezelő szervezete, amely a nemzetközi és magyar hálózatbiztonsági és kritikus információs infrastruktúra védelmi szervezetek felé, mint az országon belüli koordinációs szervezet végzi az internetet támadási csatornaként felhasználó, állami és önkormányzati nyílt informatikai rendszereket érintő incidensek kezelését, elhárításának koordinálását, valamint a felismert és publikált szoftver sérülékenységek közzétételét.

A *Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja* (LRL IBEK) a BM Országos Katasztrófavédelmi Főigazgatóság szervezetében[16] 2013-ban megalakult ágazati szervezet. Rendeltetése – az állam és az önkormányzatok által üzemeltetett létfontosságú rendszerek és létesítmények kivételével – a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenység ellátása.

A *Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ (HÁEI-BEK)*[17] a Katonai Nemzetbiztonsági Szolgálat (KNBSZ) szervezetében működő ágazati szervezet, amelynek rendeltetése a honvédelmi célú informatikai rendszerek biztonságának támogatása, a rendszerek működése során bekövetkező biztonsági események ágazati szintű kezelése, a sérülékenység vizsgálatok végrehajtása és a fenyegetettségek kezelése. Szakmai irányítása alatt a MH informatikai hálózatait ért támadások felderítésére, vizsgálatára, a károk hatásainak minimalizálására további, szakfeladat szerint elkülönült eseménykezelő központokat működnek.

A polgári hírszerzés informatikai rendszereit érintő biztonsági események és fenyegetések kezelésére az Információs Hivatal keretében ágazati szintű *Eseménykezelő Központ (IntCERT)* működik.

---

[15] A kidolgozásnál nem volt információm a terrorizmust elhárító szerv által használt, valamint a diplomáciai információs célokra használt hálózatok eseménykezelő központjairól.

[16] Az LRL IBEK az Iparbiztonsági Főfelügyelőség Kritikus Infrastruktúra Koordinációs Főosztály Információ- és Hálózatbiztonsági Osztály bázisán működik.

[17] A honvédelmi szervezetek 2016. évi fő célkitűzéseit és fő feladatait, valamint a 2017-2018. évi tevékenység fő irányait meghatározó HM utasításban még MilCERT.

A SZTAKI által működtetett, és az Internet Szolgáltatók Tanácsa (ISZT) által támogatott *Hun-CERT* munkacsoport rendeltetése a segítségnyújtás az ISZT tagszervezeteinél előforduló hálózati incidensek felderítéséhez, elemzéséhez és kezeléséhez. Más eseménykezelő központokkal ellentétben a Hun-CERT nem rendelkezik jogosítványokkal a támogatott hálózatok üzemeltetői felé, szükségesnek ítélt biztonsági intézkedéseit csak az ISZT-n keresztül érvényesíti.

Végül a *Kormányzati Informatikai Fejlesztési Ügynökség CSIRT (KIFÜ CSIRT)* a NIIF Program hazai felsőoktatást, közoktatást, kutatás-fejlesztést, könyvtárakat és közgyűjteményeket, valamint számos egyéb közintézményt kiszolgáló hálózatához (HBONE) csatlakozó szervezeteket támogató számítógép biztonsági és incidenskezelő csoport.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Összegzésképpen megállapíthatjuk, hogy a kiberbiztonság, a kiberteret alkotó, hálózatba kapcsolódó informatikai rendszerek és szolgáltatásaik biztonsága napjaink egyik legfontosabb szervezeti, nemzeti, regionális, és globális biztonsági kihívása. A kibertér informatikai rendszereinek, hálózatainak szövevényes összekapcsolódása a kiberbiztonság fenntartását csak számos különböző szereplő együttműködésére épülve teszi lehetővé.

A kiberbiztonságban érintett szervezetek közé különböző típusú szervezetek sorolhatóak. A két legfontosabb csoportot az egy védendő informatikai rendszert, hálózatot közvetlenül felügyelő szervezetek (kiberbiztonsági műveleti központok, csoportok), valamint a több védendő informatikai rendszer, hálózat biztonságában közreműködő szervezetek (kiberbiztonsági eseménykezelő központok) képezik. Emellett az együttműködésben érintettek más típusú szervezetek (védelmi szféra egyes szervezetei, szoftver, hardver gyártók, stb.) is.

A kiberbiztonsági eseménykezelő szervezetek által nyújtott szolgáltatások három nagy csoportba – a reagáló (reaktív), a megelőző (proaktív), valamint a további biztonsági szolgáltatások közé – sorolhatóak. Az első csoportba a riasztások és értesítések, a biztonsági események (incidensek) kezelése, a sérülékenységek kezelése, valamint a tárgyi leletek kezelése tartoznak. A második csoport főbb összetevői az új megoldások, kialakult trendek figyelemmel kísérése, tájékoztatások, valamint az ellenőrzések és értékelések.

Magyarországon az első hálózatbiztonsági eseménykezelő központok az 1990-es évek végén jöttek létre (Hungary-CERT, MIIF CSIRT). 2005-ben alakult meg a kritikus információs infrastruktúrák védelmére specializálódott CERT-Hungary Központ, amely 2009-ben Nemzeti Hálózatbiztonsági Központtá (CERT-Hungary) alakult. Ennek bázisán került kialakításra 2013-ban a Nemzeti Kibervédelmi Intézet részeként a Kormányzati Eseménykezelő Központ *(*GovCERT-Hungary*)*, és jöttek létre az ágazati eseménykezelő központok.

FELHASZNÁLT IRODALOM

[1] KISSEL, R. (szerk.): *NISTIR 7298, Glossary of Key Information Security Terms, Revision 2* – National Institute of Standards and Technology, 2013 május.

[2] *ISO/IEC 27032:2012, Information technology — Security techniques — Guidelines for cybersecurity.* – International Organization for Standardization, International Electrotechnical Commission, Genf, 2012.

[3] *ITU-T X.1205, Series X: Data Networks, Open System Communications and security. Telecommunication Security. Overview of cybersecurity.* – International Telecommunication Union, Genf, 2008 április.

[4] *JOIN(2013), Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* – European Commission, Brussels, 2013 február.

[5] *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)*

[6] *Baseline capabilities for national / governmental CERTs. v1.0* – European Network and Information Security Agency, 2009 december.

[7] WEST-BROWN, M. J. et. al.: *Handbook for Computer Security Response Teams (CSIRTs). 2nd Edition.* – Carnegie Mellon University, Software Engineering Institute, Pittsburgh, 2003 április.

[8] *National/governmental CERTs. ENISA's recommendations on baseline capabilities.* – European Union Agency for Network and Information Security, Heraklion, 2014 december.

[9] *Strategies for Incident Response and Cyber Crisis Cooperation. Version 1.1* – European Union Agency for Network and Information Security, Heraklion, 2016 augusztus.