BODÓ ATTILA PÁL –
BOGNÁR BALÁZS

KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELME

Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2019

Nemzeti Közszolgálati Egyetem, Budapest

KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELME

Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2019

Szerkesztő:
Deák Veronika

Szerzők:
Dr. Bognár Balázs
Dr. Bodó Attila Pál

Szakmai lektor:
Dr. Vass Gyula

A kézirat lezárásának dátuma:
2019. november 18.

Kiadó:
Nemzeti Közszolgálati Egyetem
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert Rektorhelyettes
Címe: 1083 Budapest, Üllői út 82.

TARTALOM

1. BOGNÁR BALÁZS: KRITIKUS INFRASTRUKTÚRÁK ÉS KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK MAGYARORSZÁGON

1.1. Bevezető gondolatok

Mára már nyilvánvaló valamennyi társadalom számára, hogy az emberiség mindennapi életét kiszolgáló és támogató infrastruktúrák meghibásodása, működésképtelensége, zavara a társadalmak széles rétegeit érinthetik. Ezen rendszerek és létesítmények befolyásolják az emberek mindennapjait, hiszen olyannyira természetessé vált számunkra a létezésük, olyannyira beépültek a napi rutinokba, hogy az általuk nyújtott szolgáltatások folyamatosságát alapértelmezettnek vesszük és sokszor fel sem vagyunk készülve azok hiányára.

A bennünket körülvevő infrastruktúrák architektúrájának felvázolásával, a találkozási pontok beazonosításával, a hálózatszerű és egymásra épülő rendszerelemek összefüggéseivel éppen ezért kiemelten fontos foglalkozni, hiszen egy n számú rendszerben lehetnek olyan rendszerelemek, amelyek kiesése nem pótolható, illetőleg amelyek kiesése további dominóhatást indít be.

1.2. Mitől kritikus egy infrastruktúra [6]

Az alapvető jellemzők és tulajdonságok mellett kiemelkedő jelentőséggel bír az egyes infrastruktúrákat *veszélyeztető tényezők* köre. Olyan körülményeket értünk ezek alatt, amelyek az adott infrastruktúrára potenciálisan hatást gyakorló fenyegetés [2] jellege szerint különböztethetők meg. A XX. századra még jellemző, klasszikus háborús események és fegyveres konfliktusok a mai világ fejlett országaiban már kevésbé számottevőek. Egyre nagyobb jelentősége van azoknak a hadviselési módszereknek és egyéb eredetű kockázatoknak [2], amelyek nehezen azonosítható veszélyforrásból származnak, hatásuk az emberi életre és az anyagi javakra előre nem prognosztizálható.

Mind a természetes, mind az épített környezetre jelentős hatást gyakorolhatnak olyan kihívások [2], amelyeket az infrastruktúrák veszélyeztető tényezőiként azonosíthatunk. A hazai, modern értelemben vett kritikus infrastruktúra-védelmi folyamatok első mérföldköve volt a nemzeti kritikus infrastruktúra-védelemről szóló Zöld Könyv, amely a veszélyeztető tényezők egyes csoportjait bevezette a szakmai terminológiába.

Ezek alapján az infrastruktúrák potenciális veszélyeztető tényezőinek besorolása a következő [3]:

1. *Ártó szándékú cselekmények* – alapvetően a tudatos károkozás céljából végrehajtott cselekedetek, amelyeknek az okozott anyagi kár mellett főként a társadalomra gyakorolt pszichológiai hatása lehet rendkívül jelentős:
   - terrorcselekmény (például: 9/11. USA, 2004. Madrid, 2005. London, 2015. Párizs, 2016. Brüsszel),

- kibertámadások (például: 2007. észtországi támadások, 2017. Wannacry),
- társadalmi eredetű esemény (például: 2014. őszi zavargások Missouriban),
- fegyveres konfliktus előidézése (például: 2014. polgárháború Ukrajnában, Szíriában),
- gazdasági, politikai okkal elkövetett visszaélés.

2. *Katasztrófa jellegű események* – természeti, ipari vagy civilizációs eredettel bekövetkező események, amelyek bekövetkezési valószínűsége és gyakorisága csekély mértékben prognosztizálható, de jelentős következményekkel járhatnak:
   - természeti eredetű veszélyek (kiterjedést és anyagi kártételt figyelembe véve az egyik legsúlyosabb következménnyel járó eseménytípus, amely az elmúlt évtizedekben egyre szélsőségesebb formákat ölt)
   - hidrológiai események (például: ár- és belvíz, villámárvíz miatti korlátozások),
   - meteorológiai események (például: szélsőséges jelenségek miatti kiesések),
   - geológiai események (például: 2013. fonyódi partfalcsúszás miatti útlezárás),
   - kiterjedt vegetációs tűzesetek,
   - napkitörések (például: 1989. akadozások a kanadai távvezetékhálózaton),
   - ipari eredetű veszélyek (technológiai hiba, helytelen emberi beavatkozás vagy baleset miatt az ipari termelés létesítményeiben, illetve azokkal kapcsolatosan bekövetkező helyzetek),
   - veszélyes anyagokkal foglalkozó üzemben bekövetkező esemény (például: 2012. Bad Fallingbostel – Németország, Kraft foods),
   - közlekedési baleset veszélyes áru szállítása során (például: 2013. veszélyes anyagot szállító vonat balesete Baltimore-ban),
   - környezetkárosodással járó esemény (például: 2010. olajfúró platform elsüllyedése a Mexikói-öbölben),
   - egyéb ipari létesítményben bekövetkező esemény (például: hőerőmű-leállás),
   - nukleáris létesítményben bekövetkező esemény (például: 2011. fukusimai atomerőmű földrengést követő nukleáris üzemzavara),
   - civilizációs eredetű veszélyek (a modern társadalom sajátosságaiból eredő események, amelyek az alkalmazott rendszerek és a társadalom működőképességére egyaránt hatást gyakorolhatnak),
   - informatikai, kommunikációs vagy navigációs rendszerek károsodása (például: űrobjektum becsapódása),
   - humánegészségügyi és állategészségügyi járványok (például: H5N1 pandémia),
   - éhínség és vízkészletekért folyó harc (például: migráció erősödése),
   - infrastruktúrák teljesítőképességének kimerülése.

Napjaink fejlettsége, a társadalmi rétegek között tapasztalható különbségek, a szélsőséges vallási és politikai nézeteket valló csoportok elszaporodása és időszakos megerősödése, a világ terrorveszélyeztetettségének exponenciális növekedése mind okot szolgáltatnak arra, hogy a prevenciós szemlélet erősödjön.

1.2.1. A kritikus infrastruktúra definiálása

A kritikus infrastruktúra fogalmára többféle meghatározás létezik. A kritikus infrastruktúra kifejezés újként jelent meg Magyarország biztonságpolitikájában, a védelmi igazgatás komplex rendszerében, a hazai szabályozási környezetben, az iparbiztonsági hatósági és az információbiztonsági feladatrendszerben egyaránt. Európában is egyedülálló módon ezen feladatrendszer 2012-ben a hivatásos katasztrófavédelmi szervezeten belül kialakításra került iparbiztonsági hatóság részeként jelent meg,

olyan kiemelt szakterületek mellett, mint a veszélyes üzemek, veszélyes áruszállítás és a nukleáris-baleset-elhárítás.

Az új terminológia azonban tartalmát illetően a hazai vonatkozásban is köthető egyrészről a védelmi tervezéshez (például: Országvédelem Tervrendszere), másrészről a gazdasági szereplőknél alkalmazott nemzetközi szabványrendszereket is felölelő üzletmenet a folytonosság tervezéséhez (Business Continuity Planning). A fejlődő országok már a XX. században saját szempontrendszereket alkottak annak érdekében, hogy a számukra kritikusnak minősíthető infrastruktúrákat megfelelően tudják elsősorban fizikai értelemben véve védeni.

„Hazánkban, a kritikus infrastruktúrák azonosításáról és kijelöléséről szóló európai uniós irányelv alapján szintén kiemelt célkitűzés volt egy saját kritikus infrastruktúra-definíció megalkotása. A szupranacionális szinttől a nemzeti önállóság felé haladva, fokozatosan bővül a fogalom tartalma, ennek eredményeként egyre pontosabb és értelmezhetőbb lesz a meghatározás.

Hazánkban a jogharmonizáció során többféle definíciót is nevesítettek, legkorábban a már említett hazai Zöld Könyvben, majd később *a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtási rendeletében* (a továbbiakban: Kat. vhr.), illetve *a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényben* (a továbbiakban: Lrtv.) egyaránt.

A kritikus infrastruktúra magyar értelmezését a hazai Zöld Könyv által megfogalmazottak írják le a legpontosabban. Eszerint *„kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére”* [3].

A hatályos nemzeti szabályozás ennek megfelelően 10 ágazatba, azon belül 34 alágazatba sorolja mindazon infrastruktúrákat, akikre vonatkoztatva az azonosítási eljárást végre kell hajtani.

Az azonosítási és kijelölési eljárásokhoz kapcsolódóan az Lrtv. és annak végrehajtási rendelete kodexiális általános szabályozásokat tartalmaz, míg az ágazati specifikumokat, ágazati kritériumokat és különös szabályokat az egyes ágazati kormányrendeletek részletezik.

1. ábra: Lrtv. szerinti ágazati besorolás
(Forrás: Dr. Bognár Balázs NKE-előadása, 2019.09.19.)

Fontos kiemelni, hogy a hazai szabályozás a kritikus infrastruktúrák védelmével kapcsolatos feladatkört a hatósági felügyelet alatt tartás irányába tereli, ezáltal szigorúbb nemzeti keretszabályozást irányoz elő. Európai uniós szinten is példaértékű a rendkívüli események kezelésével kapcsolatos eljárásrendek, valamint a biztonsági összekötő személy kapcsán megállapított követelmények tudatos és szakmai jellege [7].

A kritikus infrastruktúra szempontjából legfontosabb jellemző a *függőség*, amely kettős eredetű lehet. Egyfelől az infrastruktúrák egymással való összekapcsolódását, *hálózatszerűségét,* másfelől a társadalom és az infrastruktúra kapcsolatát jellemezheti.

Az egymástól való függőség, más néven az egymásrautaltság, magában hordozza a lehetőségét annak, hogy mindkét érintett infrastruktúra megfeleljen a kritikusság feltételeinek. A mai fejlett, tudásalapú társadalom egyre több ilyen interdependenciát generál maga körül, amelyet az energetikai és informatikai rendszerektől való függőség határoz meg elsősorban.

A kölcsönös függőség miatt, a rendszer sérülése során tényleges valószínűsége van annak, hogy az esemény dominóhatásszerűen egyfajta láncreakciót generáljon és több infrastruktúra hálózatszerű működését, rendelkezésre állását befolyásolja.

A villamos energia iránti szükséglet például az élet minden terén jelentkezik, rendelkezésre állása nem csak az állami működés, hanem a lakossági fogyasztás szempontjából is kiemelkedő jelentőségű. Egy bekövetkező esemény rosszabb szcenáriója esetén egy lokális probléma akár regionális kiterjedésű rendkívüli eseményt vagy veszélyhelyzetet is eredményezhet.

A függőséget további kettő sajátosság súlyosbíthatja. Egyrészt az adott infrastruktúra *sajátos működéséből* fakadóan is különböző veszélyeztetettséggel bírhat, tehát az üzemeltetésből eredő kockázati szint eleve magasabb. Az ilyen infrastruktúrák önmagukban is veszélyeket hordoznak, amelynek eredményeként létesítésüktől kezdve veszélyforrásként tartják számon őket. Másrészt az adott infrastruktúra *kiterjedését és elhelyezkedését* vehetjük alapul, amelynek akkor van jelentősége, ha természeti eredetű kockázatok szempontjából nagyobb veszélynek van kitéve (például lemeztektonikai törésvonalak környékén, ár- és belvízzel veszélyeztetett területeken fekszik). Ez esetben az infrastruktúra normál működése alapvetően biztonságos, ugyanakkor a természetes környezetben bekövetkező, előre nem vagy ritkán prognosztizálható események következményei súlyosabb hatásokkal járhatnak.

A kritikus infrastruktúrák vonatkozásában külön specifikumnak tekintjük a fizikai védelemmel (létesítéssel, működéssel, üzletmenettel) kapcsolatos információk kezelési módját. Tekintettel arra, hogy egyes szolgáltatások – amelyeket kritikus infrastruktúrák biztosítanak – nélkülözhetetlenek a gördülékeny életvitelhez, kiemelt figyelmet kell szentelni a velük kapcsolatos *titokvédelemnek.* Az egyes infrastruktúrák azonosítási és a kijelölési eljárásában olyan információk alapján történik a döntéshozatal, amelyek érzékeny, minősített vagy titkos adatokat tartalmazhatnak.

Megismerésük emiatt csak korlátozott körben történhet, figyelembe véve, hogy az ilyen adatokkal történő visszaélés alapjaiban ingathatja meg az adott infrastruktúra működőképességét. Ugyanakkor a titokvédelemnek nem kell kiterjednie azokra az alapvető információkra, amelyek az adott kritikus infrastruktúra működési sajátosságait, kiesésének következményeit a lakosság tájékoztatása szempontjából tartalmazza, tehát hozzájárulhat az érintett fogyasztók megfelelő információkkal történő ellátásához.

Végül az információs társadalom sajátos jellemzője, vagyis az informatikai rendszerektől való nagyfokú függősége teszi szükségessé, hogy az *informatikai védelem* fogalma szintén specifikum legyen. Az információs társadalom sajátossága, hogy működőképességét alapjaiban meghatározzák a rendelkezésére álló információs infrastruktúrák, amelyek önmagukban és más rendszerek részeként is képesek működni. Figyelembe véve azokat a funkciókat, amelyeket az információs infrastruktúrák biztosítanak, definiálásuk megfelelő módon fejezi ki a XXI. századi függőség jelentőségét.

E szerint *„az információs társadalomnak […] szüksége van […] az információkat előállító, feldolgozó, továbbító stb. rendszerekre is, amelyeket gyűjtőnéven információs infrastruktúrának nevezünk. Ez a megkülönböztetés […] azt jelenti, hogy az általános infrastruktúra-halmazból*

kiemeltünk és kitüntetett szerepet adtunk egy olyan komplex infrastruktúra-részhalmaznak, amely az információs társadalom információellátásával és kezelésével foglalkozik" [4].

A definíció alapján az információs infrastruktúrák megkülönböztetésének oka, hogy védelmük sajátos megközelítést igényel. Működésük legfőbb célja az információs társadalomban szükséges adatok, információk biztosítása, az általános rendeltetésű infrastruktúrák informatikai jellegű működési feltételeinek folyamatos garantálása.

Emiatt legjellemzőbb tulajdonságuk a globális hálózatszerűség és függőség, az információs társadalom egyfajta létszükségleteként való működés. Mindez kellő alátámasztást ad az informatikai védelem kiemelt szerepének, amelyet mind az Európai Unióban, mind Magyarországon stratégiai szintű tervezési dokumentumokkal fejlesztenek. [6]

Az Európai Unió kiberbiztonsági stratégiája kiterjed a belső piacra, a bel- és igazságügyre, valamint a virtuális térrel kapcsolatos kérdések külpolitikai vetületeire. Magyarországon is a meglévő Nemzeti Biztonsági Stratégia és a Nemzeti Katonai Stratégia mellett, szükség volt egy olyan dokumentumra, amely magában foglalja a kibertérből érkező fenyegetésekkel kapcsolatos célkitűzéseket, alapelveket rögzítsen az információbiztonság vonatkozásában és tartalmazzon megfelelő válaszokat a védekezés megvalósítása érdekében. Magyarország Nemzeti Kiberbiztonsági Stratégiáját a Kormány a 1139/2013. (III. 21.) kormányhatározattal fogadta el.

1.3. A kritikus infrastruktúra-védelem kialakulásának fontosabb állomásai

Valamennyi kritikus infrastruktúra-üzemeltető (állami vagy magán egyaránt) folyamatosan törekszik arra, hogy az általa biztosított szolgáltatás folyamatosan, a lehető legnagyobb humán, fizikai és IT-biztonsági szinten működjön.

A XXI. században minden állam vitathatatlan érdeke, hogy a saját államigazgatásáról, hon- és rendvédelméről, nemzetgazdaságáról, belbiztonságáról, valamint az állampolgárai élet- és vagyonbiztonságáról folyamatosan gondoskodni legyen képes. A biztonság megítélésének kellett változnia ahhoz, hogy a kritikus infrastruktúrák védelmével ne csak nemzeti, hanem tagállami, szövetségi, globális szinten is foglalkozzanak a döntéshozók. A kockázatelemzésen alapuló összveszély-megközelítés folyamatában lehet beazonosítani a kritikus pontokat és megalkotni mindazon eljárásrendeket, melyeket alkalmazni kell egy váratlanul fellépő havaria esemény kezelése során.

A 2001. szeptember 11-i eseményeket követően rövid idő alatt elfogadásra került az új terrorellenes törvény *(Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. – USA PATRIOT ACT)*, amely már konkrétabban és szélesebb körben határozta meg a kritikus infrastruktúrákat.

A 2003-ban kiadott, majd többször módosított, a kritikus infrastruktúrák fizikai védelmére irányuló nemzeti stratégia *(The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets)* szektorokat és ágazatokat különített el, amelyek között az együttműködés koordinálását egy központi szövetségi kormányszerv, az Egyesült Államok Nemzeti Infrastruktúra-védelmi Központja *(National Infrasturcture Protection Center – NIPC)* végzi napjainkban is [5]. Még 1998-ban erre a feladatra hozták létre a Szövetségi Nyomozóiroda (Federal Bureau of Investigation – FBI) szervezetén belül működő Nemzeti Infrastruktúravédelmi Központot, amelynek feladatát 2004 óta a *Nemzeti Infrastruktúra-koordinációs Központ (National Infrastructure Coordinating Center – NICC)* látja el.

Az NICC a kritikus infrastruktúra-védelmi rendszer országos hálózatának információs és koordinációs központja, koordinálja a 2003-ban nevesített 16 szektor védelmi célú tevékenységét. A központ 24 órás ügyeleti rendben készenléti megfigyelést végez, amelynek keretében elsősorban a veszélyeztető tényezőkkel kapcsolatos információk megosztásáért felelős. Funkcióját tekintve egyszerre lát el megelőzési, felkészülési, információmegosztási, elemző és értékelő, valamint döntés-

támogató feladatokat. Az USA a kibertér biztonságára irányuló politikáját is fejlesztette, amelynek révén a költségvetés 2009-ben és 2010-ben 40 milliárd dollárt különített el hálózatbiztonsági célokra.

Napjainkban az USA nyomatékossá tette kritikus infrastruktúra-védelmi tevékenysége kapcsán az együttműködés jelentőségét. Ennek értelmében a működőképesség biztosításának felelőssége közös érdek, amely szövetségi, állami, területi és helyi szinten, állami és magánkézben lévő intézmények összehangolt tevékenységén alapul.

Emellett a Belbiztonsági Minisztérium (US Department of Homeland Security) fő feladata maradt, hogy a kritikus infrastruktúra-védelem tizenhat elkülönített szektora vonatkozásában a köz- és magánszféra részére stratégiai útmutatást nyújtson, illetve koordinálja a szövetségi szintű biztonsági intézkedések fejlesztését a kritikus infrastruktúrák ellenálló képességének növelése és biztonságuk szavatolása érdekében.

2006-ban a tagállamok megerősítették a kritikus infrastruktúra-védelemben betöltött szerepüket, hangsúlyozták, hogy az alapvető szolgáltatások folyamatos rendelkezésre állását érintő zavarok a Szövetség érdekeit is érinthetik. A NATO-nak tehát nem célja önálló szabályozás kialakítása, ugyanakkor természetesen nem hagyhatja figyelmen kívül a tagállamokban potenciálisan bekövetkezhető események határon átnyúló, akár szövetségi érdekeket is befolyásoló jellegét [1].

A kibervédelmi képességek egyik fő letéteményese ma a NATO. 2008 elejére körvonalazódott a NATO új kibervédelmi stratégiája, amely lefektette a szövetség kiberpolitikájának három alappillérét: a biztonság, a szubszidiaritás és a párhuzamosságok kiiktatása. A 2010-es lisszaboni döntés értelmében a kibervédelem kiépítése folyamatosan és önállóan napirenden lesz a NATO stratégiai célkitűzései között. Az új stratégiai célok kidolgozása mellett a NATO végrehajtja olyan már meglévő struktúrák szükséges megújítását, mint amilyen például a NATO Számítógépes Biztonsági Események Kezelése (Computer Incident Response Capability – CIRC). Fő cél egy továbbfejlesztett „Kibervédelem 2.0" kialakítása a teljes körű védelem érdekében. Érdemes megemlíteni azt is, hogy a válságövezetekben a NATO olyan „ernyőt" hozott létre, amely a kommunikáció biztonságát hivatott szavatolni.

Lényegében minden biztonsággal összefüggő uniós tevékenység az ENSZ-célkitűzésekhez kapcsolódik. Az ENSZ Európai Gazdasági Bizottsága (a továbbiakban: ENSZ EGB) 2006 februárjában tartott kerekasztal megbeszélésén foglalkozott első ízben, alapvetően a közlekedési infrastruktúra terrortámadások elleni védelmének kérdéseivel. Az ENSZ EGB egyetért az ENSZ Közgyűlésének 58/199. sz. határozatában foglalt felhívással, amely szerint szükséges *a kibervédelem globális kultúrájának megteremtése és a kritikus informatikai infrastruktúrák védelme*.

Tekintettel arra, hogy a kritikus informatikai infrastruktúrák biztonsága és ellenálló képessége szempontjából az országok kölcsönösen függnek egymástól – ahogyan egy lánc is csak annyira erős, amennyire a leggyengébb láncszeme –, aggodalomra adhat okot, hogy mindeddig csupán 9 tagállam alakított ki számítástechnikai eseménykezelő csoportot (Computer Emergency Response Team – CERT) és lépett be az Európai Kormányzati CERT-ek Csoportjába (EGC).

1.3.1. Terrortámadások és következményeik

A mai értelemben vett kritikus infrastruktúra-védelmi folyamatok megjelenését a XXI. század nagyobb terrortámadásaihoz vezethetjük vissza. Az új generációs terrorizmus egyik legmeghatározóbb eseménye, a *2001. szeptember 11-én* az USA ellen elkövetett támadássorozat volt, amely igazolta, hogy a terroristák is felismerték a társadalom mindennapjaira közvetlen hatással lévő rendszerek sebezhetőségét. A hajdani Világkereskedelmi Központ ikertornyai és a Védelmi Minisztérium székhelyeként működő Pentagon ellen intézett támadások több aspektusból alátámasztották, hogy a legnagyobb gazdasági és katonai potenciállal rendelkező ország sincs megfelelően felkészülve olyan eseményekre, amelyek egyik pillanatról a másikra, azonosítatlan eredettel következnek be és jelentős következményeket idéznek elő.

2004 tavaszán a terrorizmus globális jellegét alátámasztó robbantások rázták meg a világot, ezúttal európai földön, Madridban. A *spanyolországi terrorcselekmény* célkitűzése azonban túlmutatott az elrettentés szándékán és sokkal inkább a kormányba vetett bizalom megtörését célozta. A támadás elsősorban nem a nagyszámú emberáldozatra, hanem a minél jelentősebb károkozásra és pánikkeltésre irányult. E szándéknak kifejezetten megfelelt a madridi nagy kiterjedésű, stratégiailag fontos és fejlett főpályaudvar, amelynek hálózatszerűsége miatt a robbantások közvetett hatása országszerte érezhető volt. A robbantást követően oly mértékben megrendült a társadalom kormányba vetett bizalma, hogy az akkori spanyol kormányfő nyolcéves kormányzás után megbukott a terrortámadást követő héten tartott választásokon. Az új elnök első intézkedései között gondoskodott a spanyol katonai erők Irakból történő kivonásáról, amellyel jelezte Spanyolország közel-keleti konfliktusoktól való távolmaradási szándékát. Ebben az esetben konkrétabban látható, hogy a lakosságot kiszolgáló létesítmények sebezhetőségi indexe magas, így a védelmüket garantáló biztonsági intézkedéseket különösen magas prioritással kell kezelni.

A kulcsfontosságú események másfél év elteltével tovább bővültek, amikor *2005 júliusában* újabb robbantásos merényletek erősítették fel az európai nemzetek félelemérzetét. A *londoni* metróhálózat ellen intézett támadás több hasonlóságot mutatott a madridi eseményekkel. A *robbantás* időzítése egy jelentős nemzetközi-politikai döntéshez is köthető. A robbantások előtt egy nappal derült ki, hogy a brit főváros elnyerte a 2012. évi, nyári olimpiai játékok rendezési jogát. A támadás magas színvonalú szervezettségét támasztja alá, hogy a hat metróállomás felrobbantása után egy olyan buszon történt detonáció, amely a leállított metróforgalom pótlására indult.

A terroristák tehát azonosítottak egy olyan szolgáltatáscélú rendszert, amelynek sérülése jelentős káoszt, és a lakosság körében pánikot eredményezett. Mindezt tovább fokozta, hogy a túlterheltség miatt, a támadásokat követő órákban nem csak a közel tízmilliós lélekszámú Londonban, hanem a környéken is összeomlott a mobiltelefon-szolgáltatás. [6]

Ezek az események rövid idő alatt egyértelműsítették, hogy az állam biztonságát, a nemzetgazdaság működését, valamint az állampolgárok jólétét garantáló infrastruktúrák, illetve az azok által nyújtott szolgáltatások létfontosságúak, így azok védelmére különleges jogrendi szabályozás vagy sajátos intézkedések szükségesek.

1.4. Az infrastruktúra-védelem és az információbiztonság kapcsolata

Napjainkban a számítógépes rendszerek, kommunikációs eszközök működése rendkívül nagy hatást gyakorol a társadalom egészére, nélkülük az állam és gazdaság biztonságos üzemeltetése sem képzelhető el. Ezek az eszközök, rendszerek olyan mélyen beépültek a létfontosságú infrastruktúrákba, hogy kiesésük ellehetetleníthetné a különböző szolgáltatások igénybevételét, ami akár teljes szolgáltatások leállását, katasztrófahelyzetet is előidézhetne. A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti adatvagyon részét képező valamennyi adat, az ezeket kezelő információs rendszerek, illetve a létfontosságú rendszerek és rendszerelemek elektronikus információs rendszereinek biztonsága.

Az elektronikus információs rendszerek biztonsága alatt a bennük kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt (az egész rendszerre vonatkozó), teljes körű (minden veszélyeztető tényezőt figyelembe vevő), folytonos (megszakítás nélkül rendelkezésre álló) és a kockázatokkal arányos védelmét értjük. A bizalmasság alatt azt kell érteni, hogy egy rendszerben tárolt adatot, információt kizárólag az arra jogosult személy, a jogosultsága mértékéig ismerheti meg, használhatja fel vagy rendelkezhet felhasználásáról.

A sértetlenség az adat tulajdonsága, amely arra vonatkozik, hogy a tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. A rendelkezésre állás azt hivatott biztosítani, hogy az adott informatikai rendszer, a benne tárolt adat vagy információ az arra jogosult személyeknek a szükséges időben és időtartamban elérhető és használható legyen.

A nemzeti adatvagyon, valamint a kapcsolódó létfontosságú rendszerek és létesítmények információbiztonságának megteremtése érdekében 2013 márciusában a magyar Kormány 1139/2013. számú határozatával elfogadta Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló dokumentumot.

A Stratégia célja, hogy az Alaptörvény elveivel összhangban, a kibertér biztonsági környezetének elemzése alapján, meghatározza azon nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is. Mindezt egészíti ki a 1838/2018. (XII. 28.) kormányhatározattal elfogadott Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiája.

A kibertérből érkező fenyegetéseket már a 2001-es budapesti konvenció (Számítástechnikai Bűnözésről szóló Egyezmény) megfogalmazásakor felismerték a tagországok, de ezt követően, egy évtized elteltével került sor valódi védelmi célok megfogalmazására. A stratégiáink igazodnak az Európai Parlament által 2012. november 22-én elfogadott, *A kiberbiztonságról és védelemről szóló,* 2012/2096(INI) számú határozatában a tagállamok felé megfogalmazott ajánlásokhoz, valamint az Európai Bizottság és az Európai Unió közös kül- és biztonságpolitikájának főképviselője által 2013. február 7-én *Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér* címmel közzétett közös közleményhez. A hazai stratégiák illeszkednek továbbá a NATO 2010 novemberében elfogadott Stratégiai Koncepciójához, a Szövetség 2011 júniusában elfogadott Kibervédelmi Politikájához és ennek végrehajtási tervéhez, valamint a 2010. november 19–20-i lisszaboni és a 2012. május 20–21-i chicagói NATO-csúcs dokumentumaiban megfogalmazott szövetségi kibervédelmi elvekhez és célokhoz.

Az első igazán jelentős szakmai előrelépést az Európai Parlament, a Tanács és a Bizottság által 2016 júliusában elfogadott első, az egész Európai Unióra kiterjedő kiberbiztonsági direktíva jelentette. Az irányelv elfogadását hosszú tárgyalási szakasz előzte meg, ugyanis a Bizottság már 2013-ban előterjesztette a hálózat- és információbiztonságra vonatkozó javaslatát. Aktualitását a 21. század teremtette kihívások adják. Mai viszonyok között az egyre sűrűbben fellépő üzemzavarok és az informatikai sérülékenységek, károkozók, vírusok (együttesen: fenyegetések) elleni küzdelem egységes válaszlépéseket követel meg a biztonság fokozásának érdekében.

A NIS-irányelvként megismert direktíva minden uniós tagállam számára előírja a biztonságos és megbízható digitális környezetének kiberbiztonsági szempontú fejlesztését. Célja, hogy minden tagállam rendelkezzen minimális képességekkel, szükséges intézményekkel, szabályokkal, valamint a hálózat- és információbiztonság magas szintjét biztosító nemzeti szintű stratégiával. Első lépésként a tagállamok ennek érdekében azonosítják a területükön alapvető szolgáltatásokat nyújtó gazdasági szereplőket, illetve, ha a tagállami szabályozás előírja, a kiemelt szerepet játszó ún. digitális szolgáltatóikat, tekintettel arra, hogy az irányelv különböző megfelelési kritériumokat, valamint incidensbejelentési kötelezettséget fogalmaz meg rájuk vonatkozóan.

Az incidens bejelentése, mint kötelezettség, azért fontos, mert előfordulhat olyan biztonsági esemény vagy súlyos biztonsági esemény, amelyre egyedül nem képes egy szolgáltatásokat nyújtó üzemeltető reagálni, IT- vagy egyéb biztonsági szakember vagy eszköz és technológia hiányában. Az ún. eseménykezelő központok azonban segítséget nyújthatnak a probléma elhárításában, legyen az akár technikai, akár humán jellegű.

Az irányelv 2016. augusztus 8-i hatálybalépését követően a tagállamoknak 21 hónapjuk volt (2018. május 8.) a szükséges nemzeti intézkedések megtételére, jogszabályok megalkotására, és to-

vábbi 6 hónapot kaptak az alapvető szolgáltatásokat nyújtó szereplők azonosítására. Ennek megvalósítása érdekében ki kellett dolgozni a nemzeti hálózat- és információbiztonsági stratégiát; ki kellett jelölni a nemzeti hatóságot, amely felügyeli az átültetést és a végrehajtást; ki kellett jelölni egy vagy több „gyors reagálású kibervédelmi csoportot" (CSIRT/CERT); meg kellett határozni, hogy mely kritériumok alapján esik egy-egy szervezet az irányelv hatálya alá; és azonosítani kellett a konkrét érintetteket.

A NIS-ben megfogalmazott alapelvek és értékek mentén dolgozták ki és fogadták el az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) jelenleg is hatályos verzióját. Célja az állami és önkormányzati szervek, illetve a nemzeti elektronikus adatvagyon és az azt kezelő elektronikus információs rendszerek, valamint a létfontosságú rendszerek elektronikus információs rendszerei megfelelő szintű védelmének biztosítása. A törvény alapján az elektronikus információs rendszereket – a kockázatarányos védelem megvalósítása érdekében – biztonsági osztályba, míg magát a szervezeteket – a védelmi felkészültségük alapján – biztonsági szintbe kell sorolni. Az Ibtv. rendelkezik többek között a közvetlenül vagy közvetetten a hatálya alá tartozó szervezetek feladatairól és kötelezettségeiről, az elektronikus információs rendszer biztonsági osztályba sorolásáról és a megfelelés felméréséről, a szervezet biztonsági szintbe sorolásáról és a megfelelés felméréséről, cselekvési terv készítéséről, informatikai biztonsági incidensek bejelentéséről, illetve az elektronikus információs rendszer biztonságáért felelős személy feladatairól egyaránt.

Az információbiztonság témakörében jelenleg hatályos releváns jogszabályok a következők:

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról;
- 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól;
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról;
- 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről;
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről;
- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról.

Az Ibtv. 2. § (2) bekezdés c) pontja alapján a törvény (és végrehajtási rendeletei) előírásait kell alkalmazni az Lrtv. alapján kijelölt szervezetek elektronikus információs rendszereire is. Annak érdekében, hogy az e törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából, kockázatelemzés alapján.

A kockázatelemzés ki kell hogy terjedjen az elektronikus információs rendszerek vagyonelemeinek felmérésére, hogy meghatározható legyen a védelem tárgya (adatok). A különböző vagyonelemek tekintetében meg kell határozni, hogy milyen sebezhetőség jellemző rájuk, milyen fenyegetéseknek vannak kitéve IT, infrastrukturális, környezeti, humán, társadalmi, politikai, gazdasági stb.

szempontból. Ezt követően meg kell határozni, hogy melyek az elfogadható kockázatok, amelyekkel a rendszer „együtt tud élni", működését jelentős mértékben nem képesek befolyásolni, illetve melyek azok, amelyek nem elfogadhatók a szervezet számára, és intézkedéseket kell foganatosítani az adott kockázat csökkentésére. Ezen kockázatok mérséklésére alternatívákat kell felállítani, illetve fel kell tárni a maradványkockázatokat is, amelyek további értékelésre szorulnak.

Az elektronikus információs rendszerek osztályba sorolása a fenti szempontok alapján, ötfokozatú skálán történik, a rendszerben kezelt adatoktól és az elektronikus információs rendszer funkcióitól függően. Például minél több személyes vagy különleges (politikai hovatartozás, egészségügyi adat, szexuális beállítottság stb.) adatot, esetleg minősített adatot kezel az adott rendszerben egy szervezet, annál magasabb osztályba kell hogy kerüljön, mivel a kockázatok is magasabbak. Minél több érintettje van egy biztonsági eseménynek vagy minél szenzitívebb adata, annál magasabb szintű védelmet kell biztosítani a rendszer működése során.

Kritikus infrastruktúrák tekintetében – rendeltetésükből és létfontosságú jellegükből adódóan – a szabályozás a rendelkezésre állást követeli meg elsődlegesen a bizalmasság–sértetlenség–rendelkezésre állás hármas szempontrendszerét nézve, de természetesen nem zárható ki, hogy bizonyos – például az egészségügy ágazatba tartozó, nagy mennyiségű személyes adatot kezelő – rendszerek tekintetében hangsúlyosabb lesz a sértetlenség és a bizalmasság követelménye is. Az egyes biztonsági osztályokhoz meghatározott követelményrendszer társul, amelyet az adminisztratív, a fizikai és a logikai védelem terén kell a rendszereknek teljesíteniük. Az adminisztratív védelem körébe tartoznak például a szabályzatok, a biztonságért felelős személyek kinevezése, a nyilvántartások, kockázatelemzések, dokumentációk, eljárásrendek megléte, üzletmenet-folytonosság tervezése, oktatás, képzés stb.

A fizikai védelmi intézkedések között említhetők a rendszerhez és az eszközökhöz történő hozzáférés szabályozása, ellenőrzése, felügyelete, az áramellátás biztosítása, tűz-, víz-, egyéb károk elleni védelem, karbantartás. A logikai védelmi intézkedések közé tartoznak többek között a biztonsági elemzések, tesztelések, konfigurációkezelés, frissítések, naplózások, az adathordozók védelme, azonosítás, hitelesítés vagy a kommunikáció védelme. A jogszabályok alapján meghatározható az egyes rendszerek irányadó biztonsági osztálya, amelynek meg kell felelni és amelyhez társított követelményeket teljesíteni szükséges.

A biztonsági osztályba sorolást a kockázatelemzés elvégzését követően a szerv vezetője hagyja jóvá. A biztonsági osztályba sorolást háromévenként, vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni. A rendszer teljes életciklusában (működése minden időszakában és formájában) alapvető kötelezettség az irányadó osztálynak megfelelő biztonsági követelmények megvalósítása és fenntartása.

A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet vagy szervezeti egységeket az elektronikus információs rendszerek védelmére való felkészültségük (biztonsági menedzsmentjük) alapján biztonsági szintbe kell sorolni a jogszabályban meghatározott szempontok szerint. Az elektronikus információs rendszerrel rendelkező szervezet/szervezeti egység biztonsági szintje a szervezet biztonsági menedzsmentjének fejlettségét, érettségét méri. A szintén ötfokozatú rendszerben a leggyengébb szint (1-es) azt jelenti, hogy a szervezetnél vannak az információbiztonságot érintő szabályozók, de a folyamatok ad hoc jellegűek, nem ellenőrzöttek. A szintek emelkedésével párhuzamosan a folyamatok szabályozottabbak, ellenőrzöttek, számonkérhetők, oktatottak, teszteltek, mérhetők, auditáltak lesznek. A rendszerek biztonsági osztálya és a használó szervezet biztonsági szintje között erős összefüggés van, hiszen szigorú védelmi intézkedéseket csak fejlett biztonsági kultúrával rendelkező szervezet tud biztosítható módon végrehajtatni.

A létfontosságú rendszerek, létesítmények elektronikus információs rendszereinek biztonsági osztályba sorolásához a 41/2015. (VII. 15.) BM rendelet ad segítséget. Az osztályba sorolásnál a rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint a rendszer sértetlenségének és rendelkezésre állásának követelményeit kell a funkciónak megfelelően érvényesíteni.

A rendelet 1. melléklete nem kötelező érvényű iránymutatást nyújt a biztonsági osztály megállapításához. Az egyes osztályoknál azt mérlegeli, hogy az elektronikus információs rendszereket érintő

sérülés okozta kár milyen nagyságrendű a kezelt adatok, az üzlet-, ügymenet akadályozása, valamint a további társadalmi, politikai hatások, esetleges személyi sérülések tekintetében.

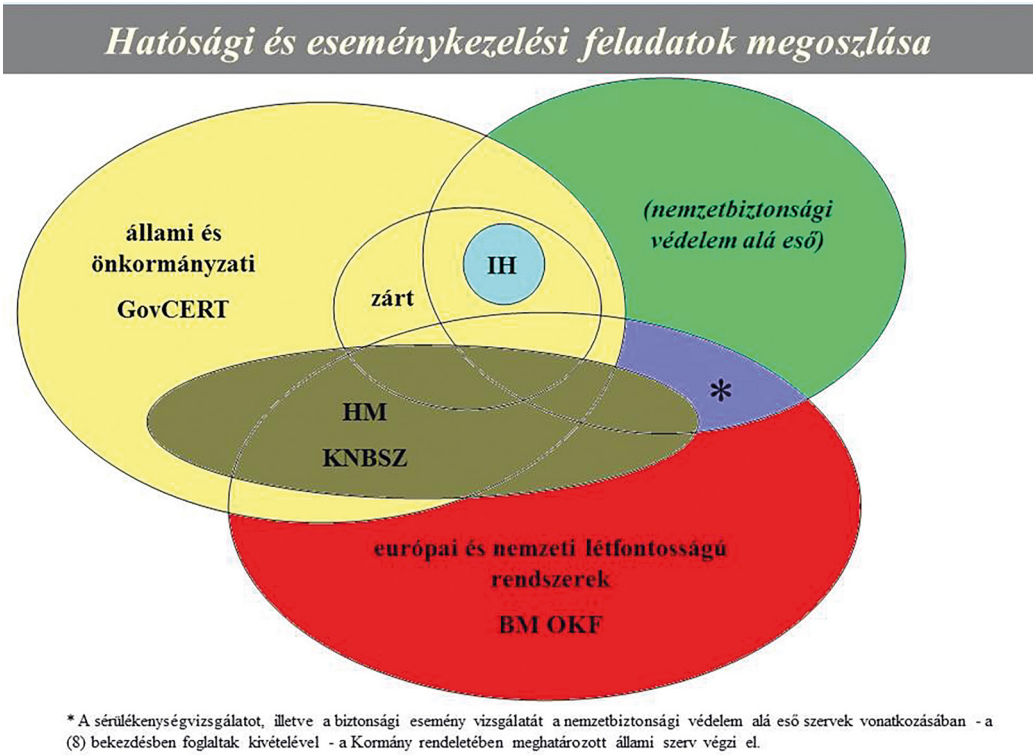
A biztonsági osztályokhoz és szintekhez tartozó követelményeket nem kell rögtön teljesíteni, a jogszabály lehetőséget ad a fokozatos elérésre. Amennyiben a szervezet vagy szervezeti egység nem éri el az 1-es biztonsági szintet, abban az esetben a vizsgálatot követően 6 év áll rendelkezésre, hogy az 1-es szinthez tartozó előírásoknak megfeleljen.

Ezt követően minden egyes szintet érintően, a következő magasabb szintre lépéshez 2 év áll rendelkezésre *(fokozatos elérés elve),* egészen addig, amíg el nem éri az irányadó fokozatot. A biztonsági osztályok tekintetében a vizsgálat elvégzését követően, minden egyes következő biztonsági osztály eléréséhez szintén 2 év áll rendelkezésre.

További kötelezettség a szervezetre nézve, hogy elektronikus információs rendszer biztonságáért felelős személyt nevezzen ki, a rendszer védelmével kapcsolatos felelősöket, feladatokat, hatásköröket az informatikai biztonsági szabályzatban vagy egyéb, az információbiztonságot érintő belső szabályozóban szabályozza.

Az elektronikus információs rendszerek biztonságának hatósági felügyelete több szervezet felelősségi körébe tartozik. A hatósági tevékenység két fő oszlopa a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) és a katasztrófavédelemnél működő információbiztonsági hatóság, de egyes speciális rendszerek tekintetében egyedi felelősségek lépnek érvénybe.

A különböző típusú elektronikus információs rendszerek hatósági felügyeletének megoszlása a következő ábrán látható:



2. ábra: Elektronikus információs rendszerek hatósági felügyelete (Forrás: BM OKF.)

A katasztrófavédelem szervezeti rendszerében kiemelt területként jelentkezik a *létfontosságú rendszerek és létesítmények* védelmével kapcsolatos feladatok ellátása, a potenciális kritikus infrastruktúra-elemek beazonosítása, valamint a kijelölt elemek hatósági felügyelet alatt tartása, nyilvántartása, ellenőrzése, ez által az ezekhez tartozó *információbiztonsági hatósági tevékenység hatékonyságának fokozása.*

1.4.1. Információbiztonsági hatósági tevékenység

Az Ibtv., illetve az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet alapján az *európai vagy nemzeti létfontosságú létesítmények, rendszerek elektronikus információs rendszerei* esetében a *BM OKF*-et nevesítették eljáró hatóságként.

Ugyanezen kormányrendelet az információbiztonsági hatósági feladatellátás másik legmeghatározóbb szerepet játszó hatóságaként (NEIH) a *Nemzetbiztonsági Szakszolgálatot* jelölte ki, amely *valamennyi állami és önkormányzati szerv* vonatkozásában eljárhat, a *nevesített kivételeken kívül* (például: polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei; honvédelmi célú elektronikus információs rendszerek; kritikus infrastruktúrák – amelyek üzemeltetője nem állami/önkormányzati szerv).

A BM OKF az Lrtv. alapján kijelölt létesítmények, rendszerek elektronikus információs rendszerei esetében látja el a hatósági feladatokat és a biztonsági felügyeletet a következő táblázatban ismertetett kivételekkel:

kivétel	**eljáró hatóság**
a rendészetért felelős miniszter alá tartozó szerveknél működő zárt célú elektronikus információs rendszer	rendszert működtető szerv vezetője
a honvédelmi célú elektronikus információs rendszerek és a honvédelemért felelős miniszter alá tartozó szervek, gazdasági társaságok zárt célú elektronikus információs rendszerei	Katonai Nemzetbiztonsági Szolgálat főigazgatója
a külpolitikáért felelős miniszter alá tartozó szerveknél működő zárt célú elektronikus információs rendszer	külpolitikáért felelős miniszter
polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei	rendszert működtető szerv vezetője

1. táblázat: Információbiztonsági hatósági feladatok megoszlása
(Forrás: Kritikus infrastruktúrák védelme I. [6].)

A katasztrófavédelem *információbiztonsági hatóságának* feladatkörébe a következő feladatok és jogosultságok tartoznak:

1. Biztonsági osztályba és szintbe sorolással, biztonsági események vizsgálatával kapcsolatos tevékenység során:
   – végzi az osztályba sorolás és a biztonsági szint megállapításának ellenőrzését és az ellenőrzés eredménye alapján *döntés* meghozatalát,
   – az osztályba sorolásra és – ehhez kapcsolódóan – a rendszert működtető szervek biztonsági szintjeire vonatkozó, jogszabályban meghatározott követelmények teljesülésének *ellenőrzését,*
   – az ellenőrzés során a feltárt vagy tudomására jutott *biztonsági hiányosságok elhárításának elrendelését* és eredményességének ellenőrzését,
   – a rendelkezésre álló információk alapján *kockázatelemzés* elvégzését,
   – a hozzá érkező biztonsági eseményekkel kapcsolatos bejelentések kivizsgálására irányuló *hatósági eljárás* megindítását (eljárás határideje 30 nap, logikai védelmi intézkedés teljesülésének vizsgálatára indított eljárás határideje 120 nap).

2. Nyilvántartás vezetésével kapcsolatos tevékenysége keretében kezeli:
   – a szervezet *azonosítás*ához szükséges adatokat (megküldés 60 napon belül),
   – a szervezet elektronikus információs rendszereinek *megnevezés*ét, *besorolás*ait, technikai adatait,
   – a szervezet elektronikus információs rendszereinek *biztonsági felelős*ére vonatkozó adatokat (megküldés 60 napon belül),
   – a szervezet *informatikai biztonsági szabályzat*át (megküldés 90 napon belül),
   – a biztonsági eseményekkel kapcsolatos, a kormányzati eseménykezelő központtól kapott *értesítések*et.
   – A nyilvántartásból adattovábbítás kizárólag az eseménykezelő központok részére történhet.
   – Az adatokat a tevékenység befejezésének bejelentését követő 5 év elteltével kell törölni.
3. Ellenőrzésekkel kapcsolatos tevékenység és szankcionálás:
   – a jogszabályokban foglalt *biztonsági követelmények* és az ezekhez kapcsolódó *eljárási szabályok* teljesülésének ellenőrzése,
   – a *követelményeknek való megfelelőség* alátámasztásához szükséges dokumentumok bekérése,
   – a központi költségvetési és az európai uniós forrásból megvalósuló *fejlesztési projektek* tervezési szakaszában az információbiztonsági követelmények megtartásának ellenőrzése, azokra ajánlások tétele,
   – a *fejlesztési projektek* tervezési szakaszában szakmai részvétel biztosítása és a biztonsági követelmények beépülésének ellenőrzésére irányuló tevékenység folytatása,
   – a sérülékenység megszüntetésére vonatkozó *intézkedési terv* készítése,
   – amennyiben a rendszert működtető szervezet a biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, akkor az érintett felszólítása a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére, vagy a körülmények mérlegelésével *bírság kiszabása*, amely további nem teljesülés esetén megismételhető.
4. Egyéb tevékenység:
   – az információs társadalom *biztonságtudatosság*ának *elősegítése* és támogatása,
   – a hazai és nemzetközi információbiztonsági, kibervédelmi, létfontosságú információs infrastruktúra védelmével kapcsolatos *gyakorlatok*on történő részvétel,
   – *kapcsolattartás és együttműködés* a hatóságokkal, valamint az eseménykezelő központokkal.

1.4.2. Informatikai biztonsági eseménykezelés

Az informatikai biztonsági események kezelésének egyre növekvő jelentőségét az a tény világítja meg leginkább, hogy a kritikus infrastruktúraként működő szolgáltatások egyre inkább informatikai rendszerek támogatásával vagy egyenesen informatikai rendszereken keresztül valósulnak meg, ezért az informatikai rendszerekkel kapcsolatos kockázatok, fenyegetettségek közvetlenül transzformálódnak a kapcsolódó infrastruktúrákra is. A létfontosságú rendszerelemek vizsgálata esetén látható, hogy a magyar gazdaság szinte minden szektora érintett valamilyen formában. Egy nem megfelelően kezelt informatikai incidens a továbbgyűrűző hatás (dominóhatás) miatt beláthatatlan károkat okozhat mind a termelésben, mind a szolgáltatások működésében, jelentős hatást gyakorolva a lakosság életére is. Gondoljunk bele, mi történne, ha egy hackercsoport átvenné az irányítást a magyar bankok vagy a víztisztító telepek informatikai rendszerei felett.

A jogszabály hatálya alá tartozó szervezet elektronikus információs rendszereit érintő súlyos biztonsági eseményekről tájékoztatnia kell a megfelelő eseménykezelő központot (GovCERT, MilCERT, IntCERT), ahol szükség esetén segítséget kap az esemény kezelésében és együtt kell működnie az incidens kivizsgálásában.

Az Ibtv. és végrehajtási rendeletei a kijelölt létfontosságú rendszerek és létesítmények elektronikus információs rendszerei tekintetében a kiberincidensek kezelését, vagyis az informatikai biztonsági eseménykezelő központ működtetését a Nemzetbiztonsági Szakszolgálat – azon belül a kormányzati eseménykezelő központ (GovCERT) – feladatkörébe helyezte.

Az eseménykezelő központ részletes feladatait, hatáskörét az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet szabályozza a következők szerint:

1. Biztonsági eseményekkel kapcsolatosan:
   - biztonsági események és kockázatok kezelésére vonatkozó *eljárások* meghatározása,
   - biztonsági események megelőzése céljából *tájékoztatási és tudatosítási tevékenység* végzése,
   - a biztonsági események nemzeti szintű *nyomon követés*e,
   - a tudomására jutott biztonsági eseményekről az érintettek haladéktalan értesítése,
   - *reagálás* a biztonsági eseményekre,
   - kockázatokkal és biztonsági eseményekkel kapcsolatos *tájékoztatás*, korai előrejelzés, riasztás, bejelentéstétel és *információterjesztés* az érdekeltek számára,
   - *sérülékenységvizsgálat* lefolytatása,
   - a biztonsági eseményekről *nyilvántartás* vezetése (megtett intézkedések és azok eredménye beleértendő).
2. Sérülékenységekkel és fenyegető kockázatokkal kapcsolatosan:
   - az elektronikus információs rendszerek biztonságáért felelős személyek *tájékoztatás*a,
   - a hatóságok és más eseménykezelő központok tájékoztatása,
   - a sérülékenységekről és fenyegetésekről, valamint a hozzájuk kapcsolódó, javasolt biztonsági intézkedésekről a honlapján rendszeres tájékoztatás biztosítása.
3. Nemzeti szintű, egyéb feladatai:
   - *elemzések, jelentések* készítése a magyar és a nemzetközi információbiztonsági irányokról,
   - *évente jelentés* készítése a tevékenységéről a polgári nemzetbiztonsági szolgálatokért felelős miniszter részére,
   - nem kötelező érvényű *állásfoglalások*, *ajánlások* kiadása,
   - a biztonsági események kezelésére irányuló *tájékoztatók* tartása, tudatosítási programokban, szakértői-oktatói tevékenységben részvétel,
   - kormányzati információtechnológiai és biztonságiesemény-kezelési *együttműködési fórum* működtetése,
   - részvétel az infokommunikációs biztonságra vonatkozó stratégiák és *szabályozás*ok előkészítésében.

Az alapvető és a bejelentésköteles szolgáltatást nyújtókkal kapcsolatos feladatok

A 2017. év egyik kiemelt feladata volt a tagállamok számára a NIS-irányelv nemzeti jogrendbe történő teljes körű átültetése, különös tekintettel az alapvető szolgáltatást nyújtó szereplőkkel, valamint a magyar terminológiában bejelentésköteles szolgáltatókkal (az irányelvben digitális szolgáltatók) kapcsolatos feladat- és intézményrendszer kialakítása.

A jogharmonizáció során elsődleges cél volt, hogy az új feladatrendszer ellátása a már meglévő, információbiztonsági területen hatáskörrel rendelkező szervek tapasztalataira és képességeire építve, azokat kiegészítve valósuljon meg.

A NIS-irányelv két szolgáltatói kört nevesít, az alapvető és a bejelentésköteles szolgáltatást nyújtókat, és az általuk nyújtott szolgáltatások folyamatosságának biztosítása, illetve az általuk kezelt adatok védelme érdekében biztonsági követelmények és bejelentési kötelezettség előírását várja el a tagállamoktól.

Az új szabályozás értelmében *alapvető szolgáltatást nyújtó szereplőnek minősül* a kritikus infrastruktúrák azon köre, amelyeket az irányelv által meghatározott – az Lrtv.-hez képest szűkített – ágazatokban (energia, pénzügy, egészségügy, ivóvízellátás, közlekedés, digitális infrastruktúrák) már kijelöltek létfontosságú rendszerré, létesítménnyé, valamint a működésük hálózati és információs rendszerektől függ és az ezeket érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában.

Ezen szolgáltatók beazonosítása a már meglévő jogszabályi háttér alapján, az abban foglalt kritériumrendszer kiegészítésével történik. Az új kijelölési eljárásokban a szokásos ágazati és horizontális kritériumokon túl a jövőben az alapvető szolgáltatásokra vonatkozó kritériumokat is vizsgálni kell.

Az új szabályozás hatálybalépésekor már létfontosságúnak kijelölt rendszerelemek tekintetében az üzemeltetőnek 60 napon belül kiegészítést kell benyújtania az azonosítási jelentéséhez a fenti kritériumoknak történő megfelelésről.

Mivel az irányelv szerinti alapvető szolgáltatást nyújtó szereplők a nemzeti szabályozás alapján létfontosságú rendszernek, létesítménynek kijelöltek egy szűkebb köre, így az elektronikus információbiztonsággal kapcsolatos felügyeletük, kötelezettségeik nem változnak.

A *bejelentésköteles szolgáltatást nyújtókkal* (online piacterek és keresőprogramok, felhőalapú számítástechnikai szolgáltatások) kapcsolatos hatósági és eseménykezelési feladatok meghatározása és végrehajtása a hatályos információbiztonsági jogszabályok mintájára, de teljesen új, különálló jogszabály alapján valósul meg, amely a Nemzetbiztonsági Szakszolgálathoz telepíti a kapcsolódó hatósági hatáskört és eseménykezelési feladatkört, ami által az eddigi információbiztonsági feladatrendszer kibővült.

A bejelentésköteles szolgáltatásokkal kapcsolatosan az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény is módosult, ugyanis értelmező rendelkezései között határozták meg magát a *bejelentésköteles szolgáltatást,* amely alatt olyan információs társadalommal összefüggő szolgáltatást értünk, amely: lehetővé teszi, hogy az online piactér weboldalán online adásvételi vagy szolgáltatási szerződéseket kössenek (= online piacterek, webáruházak); információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (= online keresőszolgáltatások); távoli hozzáférést tesz lehetővé a többek között hálózati funkciókat, adattárolást, alkalmazások, szolgáltatások futtatását biztosító számítástechnikai megoldásokhoz (= felhőalapú számítástechnikai szolgáltatások).

A fenti szolgáltatásokat nyújtó, *magyarországi székhellyel rendelkező* gazdasági társaságok körét a *NIS-irányelv III. melléklete szerint* kell *szűkíteni,* tehát azokra a szolgáltatókra terjed ki az új szabályozás személyi hatálya, amelyek a mellékletben meghatározott digitális szolgáltatást nyújtanak, és *nem tartoznak a mikro- és kisvállalkozások körébe.* A vonatkozó rendelkezéseket a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló a 2004. évi XXXIV. törvény 3. § (2)–(3) bekezdései szabályozzák.

Az így kialakuló ügyfélkörnek (bejelentésköteles szolgáltatók) regisztrálnia kell magát a hatóságnál, amely nyilvántartásba veszi. A működés során bekövetkező azon biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az általa az Európai Unión belül kínált bejelentésköteles szolgáltatás nyújtására, haladéktalanul be kell jelenteni az eseménykezelő központ részére. A szolgáltató mind a biztonsági események kezelése, mind a hatósági eljárások lebonyolítása tekintetében köteles a hatósággal együttműködni.

A szolgáltatók által bejelentett biztonsági események kezelése, kivizsgálása, az üzletmenet-folytonosság mielőbbi visszaállítása érdekében a *GovCERT* szintén eseménykezelési feladatkörében jár el.

Információbiztonsági hatáskörében a Nemzetbiztonsági Szakszolgálat a következő feladatok ellátására kötelezett.

1. Biztonsági események megelőzése/kivizsgálása/felszámolása és terjedésének korlátozása érdekében végezett tevékenysége keretében
   – regisztráció alapján nyilvántartást vezet,
   – tájékoztató kampányt szervez és végez,
   – kapcsolatot tart az érintett szolgáltatókkal, a bűnüldöző hatóságokkal, más tagállamok illetékes ágazati hatóságaival, az adatvédelmi hatósággal,
   – a nyilvánosságot szükség szerint tájékoztatja az egyes biztonsági eseményekről;
   – szükség szerint kötelezi a bejelentésköteles szolgáltatást nyújtót a nyilvánosság tájékoztatására;
   – hatósági ellenőrzést végez a bejelentésköteles szolgáltatást nyújtók kötelezettségeinek teljesítése céljából.
2. Bekövetkezett biztonsági eseménynél a GovCERT jelentése alapján *hivatalból indított hatósági eljárása* keretében vizsgálja
   – a szolgáltató által megtett megelőző és az adott eseményt kezelő tevékenységét,
   – a szolgáltató részére meghatározott követelmények teljesülését,
   – a biztonsági intézkedések megfelelőségét.
   – Helyszíni ellenőrzést folytathat és műszaki vizsgálatot végezhet.
   – A vizsgálat eredményeként hatósági döntést hoz, amelynek tartalma:
   – a biztonsági esemény bekövetkezése tényének megállapítása,
   – az elhárításra javasolt intézkedések,
   – a további károkozások megelőzése érdekében javasolt intézkedések.

Magyarországon, azzal, hogy a hivatásos katasztrófavédelem szervezetrendszerében alakították ki a kritikus infrastruktúrák védelmének átfogó felügyeletét, egy szervezetnél összpontosul a bekövetkező rendkívüli események kezelése, illetve a létfontosságú rendszerek és létesítmények hálózatbiztonsági szempontú, hatósági feladatrendszere is. Mindez szerves része annak a nemzeti rendszernek, amelyben a hazánk kiberterének biztonságára irányuló, védelmi célú, a kockázatok csökkentésére törekvő és az incidensek kezelésével kapcsolatos tevékenységek megvalósulnak.

Magyarország kiberbiztonságának letéteményeseiként a hatáskörrel rendelkező szervezetek, hatóságok, CERT-ek és CSIRT-ek folyamatos és szerteágazó együttműködése nélkülözhetetlen, feladatellátásukat érdemben és szakmai támogatás szempontjából a hatósági munka és az audit jellegű ellenőrzések teszik teljessé.

Ez a komplexitás, az összveszély-megközelítés, a kockázatelemzésen alapuló hatósági tevékenység, a gyorsreagálású incidenskezelés, a társadalom minden szintjén megjelenő tudatosítási kampányok garantálják a kiberbiztonság és az információbiztonság új, modern megközelítését, a kibertérből érkező veszélyek és a természeti és civilizációs katasztrófák egységes kezelését, amely nagymértékben hozzájárul Magyarországon a lakosság közbiztonsági szintjének, a biztonságkultúrának az emeléséhez.

1.5. Felhasznált irodalom

[1] Bonnyai Tünde: A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében. Doktori értekezés 2014. Nemzeti Közszolgálati Egyetem

[2] Bognár Balázs: A Magyar Köztársaság védelmi igazgatási rendszerének lehetséges korszerűsítése. Doktori értekezés, Budapest 2009. Zrínyi Miklós Nemzetvédelmi Egyetem

[3] Zöld Könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról. A Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) kormányhatározat 1. sz. melléklete.

[4] Várhegyi István, Makkay Imre: Információs korszak, információs háború, biztonságkultúra. Országos Műszaki Információs Központ és Könyvtár, Budapest 2000.

[5] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

[6] Bognár Balázs; Bonnyai Tünde; Vámosi Zoltán: Kritikus infrastruktúrák védelme I. Dialóg Campus Kiadó, Budapest 2019.

[7] Bognár Balázs, Bonnyai Tünde, Görög Katalin, Katai-Urban Lajos, Vass Gyula: Létfontosságú rendszerek és létesítmények védelme (kézikönyv a katasztrófavédelmi feladatok ellátására), NKE KVI, Budapest, 2015, ISBN 978-615-5057-52-6, ISBN 978-615-5057-49-6, ISBN 978-615-5057-50-2

[8] Bognár Balázs, Kátai-Urbán Lajos, Kossa György, Kozma Sándor, Szakál Béla, Vass Gyula: Iparbiztonságtan I: Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához. Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., 2013. 564 p. ISBN:978-615-5344-12-1

2. BODÓ ATTILA PÁL: ÚJDONSÁGOK A MAGYAR KIBERVÉDELMI SZABÁLYOZÁSBAN ÉS A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK SZABÁLYOZÁSA

2.1. Bevezető gondolatok

Az elmúlt években a kibervédelem szabályozása az Európai Unióban (a továbbiakban: Unió) és a nemzetállamokban egyaránt jelentős változáson ment keresztül. Az általános szabályozási keretek kezdeti megalkotását követően megjelentek a speciális, az egyes részterületekre összpontosító szabályozási elemek, amelyek hatása a végrehajtás szintjén is jelentkezik. Ugyanakkor egyre erőteljesebbé vált az a törekvés, hogy a szakterületi kidolgozottság mellett az egységes, komplex szabályok gyakorlati alkalmazása is érvényesüljön, és területi korlátok nélkül érvényesíthető legyen. Jelen jegyzetben a szabályozási környezetben bekövetkezett változásokat vizsgáljuk, alapvetően két szempontból. Az egyik az Unió stratégia- és jogalkotása területét érintő speciális szakkérdés, a hálózatbiztonság és az ebből eredő, nemzetállami szinten megjelenő kötelezettségek köre, a másik az önálló, szuverén államok által végzett jogalkotási tevékenység Magyarországra adaptálva. Ezen két megközelítés mellett jelen tananyag külön fejezetben ismerteti a kritikus infrastruktúrákkal kapcsolatos nemzeti szabályozási környezetet, figyelemmel arra, hogy az alapvető szolgáltatók kijelölése tekintetében kapcsolódik az uniós szabályozáshoz. Továbbá ezen témakör főbb elemeinek áttekintése a fent említett változások hatására szükségszerű ahhoz, hogy az információbiztonsággal foglalkozó szakember aktuális és rendszertani elméleti ismereteket szerezzen feladata szakszerű ellátásához és a jó gyakorlatok alkalmazásához.

2.2. Változások a kibervédelem stratégiai szintjén

A kibervédelem területére vonatkozó stratégiaalkotás uniós és nemzetállami szintje egymással szoros összefüggésben van. Az uniós irányok, adott esetben nemzetállami jogalkotási kötelezettségeket keletkeztető irányelvek, rendeletek, meghatározzák a kibervédelem aktuális mérföldköveit, biztosítva az egységes kereteket. Az Európát ért változó jellegű és mértékű kibertámadások hatására a sebezhetőség, az ellenálló és a reagáló képesség kérdésköre politikai szintre emelkedett, a kibervédelem aktualitása központi témává vált az Unió felsővezetői szintjén is. Ezzel összefügg, hogy az Európai Bizottság elnökének minden év szeptemberében az Európai Parlament előtt az Unió helyzetéről elmondott beszédében is megjelenik a kibervédelem témaköre, mivel az „évértékelés” tájékoztatást ad az elmúlt év eredményeiről és bemutatja a következő év kiemelt feladatait, kiemelve az Európai Bizottság és az Európai Unió előtt álló legfontosabb kihívásokat. Az évértékelő beszédeknek – különös tekintettel a 2017-es tallinni digitális csúcstalálkozó és az azzal párhuzamosan kiadott, *„Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése”* című Európai

Parlamenti és a Tanácsi közös közleményre – visszatérő eleme lett a kibervédelem kérdésköre, amely fókuszpontjában az együttműködésen alapuló és komplex kiberbiztonság kialakításának szorgalmazása áll. A 2018-as évértékelés részét képező szándéknyilatkozatban a kibervédelem korábbi beszédekből már ismert, több eleme ismételten megjelenik, így újból előkerül a főbb kezdeményezések között az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) megerősítésére vonatkozó javaslat (2. prioritás). Új elemként jelenik meg az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról szóló rendelet tervezetének (2. prioritás), valamint a kiberbiztonsági eseményekkel szembeni védelemről szóló bizottsági ajánlás (7. prioritas) tervezetének elfogadtatása. Ezen véglegesítés előtt álló szabályozási eszközök mellett az *„Erős kiberbiztonság kialakítása Európában”* című bizottsági bejelentés központi elemként jeleníti meg a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016. július 6-i 2016/1148/EU európai parlamenti és tanácsi irányelv (a továbbiakban: NIS-irányelv) hatékony végrehajtását és támogatását. A NIS-irányelv alapvetését és hatását – rendelkezéseinek részletes ismertetése nélkül – az alábbiakban tárgyaljuk.

2.2.1. A NIS-irányelv és hatása

Az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága 2013 februárjában közzétett közös közleménye, *„Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér”* című uniós stratégiában meghatározott priorításokhoz[1] kapcsolódóan került megalkotásra az első uniós kiberbiztonsági jogszabály, a NIS-irányelv[2]. Az irányelv mint uniós jogi norma sajátossága, hogy az elérendő célt tekintve valamennyi címzett tagállamot kötelezi a végrehajtásra úgy, hogy a nemzeti hatóságok szabadon dönthetnek arról, hogy az uniós szabályokat milyen módszerek és eszközök alkalmazásával teszik a nemzeti jog részévé. A NIS-irányelv a hatálybalépést követően az átültetési kötelezettség teljesítésére 21 hónapot írt elő[3], így minden tagállamnak a nemzeti jogi környezetének áttekintését és az irányelv előírásaival való összhang megteremtését ezen határidőig el kellett végeznie. Az irányelv rendelkezéseit 2018. május 10-től kezdve kötelező alkalmazni.

A NIS-irányelv alapvetése[4], hogy a hálózati és információs rendszerek és szolgáltatások megbízhatósága és biztonsága kiemelt jelentőségű a gazdaság és a társadalom működése szempontjából, mivel ezen információs rendszerek és szolgáltatások az Unió belső piacának működését tekintve létfontosságúnak minősülnek, alapvető szerepet játszanak az áruk, a szolgáltatások és a személyek határokon átnyúló mozgásának biztosításában. Ezért a működési zavarok, szélsőséges esetben részleges vagy teljes szolgáltatáskiesések az egyes tagállamok mellett akár az egész Unióra is kihatással lehetnek. Ennek megakadályozása érdekében az irányelv célja, hogy:

a. harmonizált szabályozás bevezetésével megteremtse a hálózati és információs rendszerek biztonságának általános szintjét az Unióban, továbbá

---

1 A stratégia prioritásai:
a) kibertámadásokkal szembeni ellenálló képesség megteremtése;
b) a számítástechnikai bűnözés és a kibertámadások visszaszorítása;
c) kibervédelmi politika kidolgozása és a kiberképességek fejlesztése;
d) a kiberbiztonsághoz szükséges ipari és technológiai erőforrások biztosítása;
e) a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozása, valamint az alapvető uniós értékek terjesztése;
f) számítógépes bűnözéssel foglalkozó nemzeti kiválósági központok hálózatának kialakítása és finanszírozása.

2 Hatálybalépés: 2016. augusztus 8.

3 NIS-irányelv 25. cikk (1) bekezdés.

4 NIS-irányelv bevezető (1)–(3) bekezdések.

b. a tagállamok kibervédelmi felkészültségének egyenszilárdságát támogassa és
c. a kiberbiztonság általános javítása érdekében valamennyi tagállam számára kötelezettségeket és konkrét intézkedéseket állapítson meg.

Fentiek érdekében – mintegy nemzeti keretként – a NIS-irányelv[5]:

a. a tagállamok számára előírja a hálózati és információs rendszerek biztonsága nemzeti stratégiájának kidolgozását és elfogadását azzal, hogy ezen nemzeti stratégiának a célkitűzések mellett a végrehajtandó konkrét szakpolitikai intézkedéseket is meg kell határoznia és rögzíti annak főbb tartalmi elemeit[6];
b. a tagállamok közötti stratégiai, illetve operatív együttműködés támogatása, a gyors és hatékony információcsere előmozdítása és elősegítése, valamint a közöttük lévő bizalom erősítése céljából:
   ba) együttműködési csoport létrehozását rendeli el a tagállamok, az Európai Bizottság és az ENISA képviselőivel a tagállamok közötti stratégiai együttműködés, tapasztalat- és információcsere támogatása és elősegítése céljából[7];
   bc) létrehozza a számítógép-biztonsági eseményekre reagáló csoportok hálózatát[8] (a továbbiakban: CSIRT-ek), amely a tagállamok CSIRT-jei és a CERT-EU képviselőiből áll és leírja a CSIRT-ek hálózatának feladatait[9];
c. biztonsági és bejelentési követelményeket állapít meg az alapvető szolgáltatásokat nyújtó szereplők[10] és a digitális szolgáltatók[11] számára;
d. a tagállamok részére kötelezettségként írja elő, hogy jelöljenek ki:
   da) a hálózati és információs rendszerek biztonságával kapcsolatos feladatok ellátására nemzeti illetékes hatóságokat[12], amelyek felügyelik a NIS-irányelv átültetését és végrehajtását;
   db) olyan, a hálózati és információs rendszerek biztonságáért felelős egyedüli kapcsolattartó pontokat, amelyek összekötő feladatokat látnak el a tagállami hatóságok és más tagállamok, továbbá az unió illetékes intézményei felé[13], valamint
   dc) CSIRT-eket[14].
e. előírja a tagállamok részére ágazatonként és alágazatonként az alapvető szolgáltatók azonosítását és kijelölését, az alapvető szolgáltatókról jegyzék összeállítását[15].

---

5 NIS-irányelv 1. cikk (2) bekezdés.
6 NIS-irányelv 7. cikk.
7 NIS-irányelv 11. cikk.
8 Computer Security Incident Response Teams.
9 NIS-irányelv 12. cikk.
10 Alapvető szolgáltatásokat nyújtó szereplőnek minősül az energia, a közlekedési, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, az ivóvízellátás és -elosztás, valamint a digitális infrastruktúra ágazatában működő – tagállami szinten kijelölt – közjogi vagy magánjogi szervezet, amely megfelel az alábbi kritériumoknak:
a) kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt;
b) az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ;
c) az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában.
NIS-irányelv 4. cikk 4 pont; 5. cikk 2. pont.
11 Digitális szolgáltatónak minősül a NIS-irányelv szempontjából az online piactér, az online keresőprogram és a felhőalapú számítástechnikai szolgáltatás. – NIS-irányelv 4. cikk, 6. pont, III. melléklet.
12 NIS-irányelv 8. cikk (1) bekezdés.
13 NIS-irányelv 8. cikk (3) bekezdés.
14 NIS-irányelv 9. cikk.
15 NIS-irányelv 5. cikk (1)–(3) bekezdései.

A NIS-irányelv előírja[16], hogy a tagállamoknak biztosítaniuk kell, hogy jól működő CSIRT-ekkel rendelkezzenek, amelyek megfelelnek a biztonsági események és kockázatok kezeléséhez szükséges hatékony és kompatibilis képességek garantálására, valamint az eredményes uniós szintű együttműködés biztosítására vonatkozó alapvető követelményeknek azzal, hogy az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók minden típusa tekintetében el kell végezni a CSIRT-ek kijelölését. Ezen előírás alapján Magyarországon nemzeti CSIRT-ként a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete került kijelölésre, aki egyben a nemzeti egyedüli kapcsolattartó pont is[17]. A CSIRT-ek kötelezettségeit és feladatait meghatározó azon alapvetéseket, melyeket a nemzeti szabályozásnak tartalmaznia kell, a NIS-irányelv 1. melléklete tartalmazza, amelyek az alábbiak.

A CSIRT-ek kötelezettsége:

a. biztosítani a hírközlési szolgáltatásaik magas szintű elérhetőségét a kritikus hibapontok kiküszöbölése által,
b. folyamatosan több eszközt fenntartani elérhetőségük és a kapcsolattartás céljára,
c. egyértelműen meghatározni a kommunikációs csatornákat a felhasználók és a partnerek megismertetésével együttesen,
d. hivatali helyiségei és a támogató információs rendszerei biztonságos helyszíneken történő elhelyezése,
e. az üzletmenet-folytonosság biztosítása, amely érdekében:
   ea) megfelelő rendszerrel kell rendelkeznie a megkeresések kezelésére és továbbítására,
   eb) feladatellátását elegendő létszámú személyi állománnyal kell elvégeznie a folyamatos készenlét biztosításához,
   ec) redundáns rendszereket és tartalék munkaterületet kell fenntartania.

A CSIRT-ek feladata:

a. a biztonsági események nemzeti szintű monitoringja,
b. a kockázatokkal és biztonsági eseményekkel kapcsolatos korai előrejelzés, riasztás, bejelentéstétel és információterjesztés,
c. reagálás a biztonsági eseményekre,
d. dinamikus kockázat- és eseményelemzés, továbbá helyzetkép nyújtása,
e. a CSIRT-ek hálózatában való részvétel,
f. együttműködési kapcsolatok kialakítása a magánszférával,
g. közös vagy szabványosított gyakorlatok elfogadásának és alkalmazásának támogatása a biztonsági események és a kockázatok kezelésére vonatkozó eljárások, valamint a biztonsági események, kockázatok és információk osztályozására szolgáló rendszerek tekintetében.

A NIS-irányelv átültetését és végrehajtását felügyelő nemzeti illetékes hatóságnak az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóságát (a továbbiakban: BM OKF) jelöli ki[18].

---

16 NIS-irányelv bevezetés (34) bekezdés.

17 Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet (a továbbiakban: hatósági rendelet) 29/A. § (1) bekezdése.

18 Hatósági rendelet 25. § (5) bekezdés.

A NIS-irányelv szerint az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra vonatkozó biztonsági követelményeknek arányosaknak kell lenniük az adott hálózati és információs rendszert érintő kockázatokkal, ezért kötelező biztonsági és bejelentési követelményeket állapít meg[19]. Ezek a biztonsági követelmények az alapvető szolgáltatóknál magasabb szintűek, mivel működőképességük alapfeltétel a kritikus társadalmi és gazdasági tevékenységek fenntartásához.

A digitális szolgáltatók esetében a biztonsági követelmények az alábbiak[20]:

a. megfelelő és arányos műszaki és szervezési intézkedések meghatározása és megtétele azzal, hogy az intézkedéseknek biztosítaniuk kell a felmerülő kockázatoknak megfelelő biztonsági szintet és figyelembe kell venniük a következő tényezőket:
   aa) a rendszerek és a létesítmények biztonságát,
   ab) a biztonsági események kezelését,
   ac) az üzletmenet-folytonosság menedzsment követelményét,
   ad) a monitoring, az ellenőrzés és a vizsgálat követelményét,
   ae) a nemzetközi szabványoknak való megfelelést;
b. a digitális szolgáltatásaik folytonosságát biztosító intézkedések megtétele annak érdekében, hogy megelőzzék és csökkentsék a hálózati és információs rendszereik biztonságát érintő biztonsági eseményeknek a digitális szolgáltatásokra gyakorolt hatásait;
c. a digitális szolgáltatásaik folytonosságára jelentős hatást gyakorló biztonsági események indokolatlan késedelem nélküli bejelentése az illetékes hatóságnak vagy a CSIRT-nek. A jelentős hatás meghatározása során:
   ca) az érintett felhasználók számát, különös tekintettel azon felhasználókra, akik az érintett szolgáltatásra alapozzák a saját szolgáltatásaik nyújtását,
d. a biztonsági esemény időtartamát,
e. a biztonsági esemény által érintett terület földrajzi kiterjedését,
f. a szolgáltatás működésében támadt zavar mértékét és
g. a gazdasági és társadalmi tevékenységekre gyakorolt hatás mértékét

kell elsősorban figyelembe venni.

Az alapvető szolgáltatást nyújtó szereplőkre vonatkozó biztonsági követelmények az alábbiak[21]:

a. megfelelő és arányos műszaki és szervezési intézkedések megtétele a működés során használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében, azzal, hogy az intézkedéseknek biztosítaniuk kell a felmerülő kockázatok alapján azonosított biztonsági szintet;
b. az alapvető szolgáltatások folytonosságát biztosító intézkedések megtétele a szolgáltatásnyújtáshoz igénybe vett és alkalmazott hálózati és információs rendszerek biztonságát érintő biztonsági események megelőzésére és azok hatásainak csökkentésére;
c. az alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági események indokolatlan késedelem nélküli bejelentése az illetékes hatóságnak vagy a CSIRT-nek. A jelentős hatás meghatározása során:
   ca) az alapvető szolgáltatás zavara által érintett felhasználók számát,
   cb) a biztonsági esemény időtartamát és
   cc) a biztonsági esemény által érintett terület földrajzi kiterjedését kell elsősorban figyelembe venni.

[19] NIS-irányelv 14–17. cikkek.
[20] NIS-irányelv 16. cikk (1)–(4) bekezdés.
[21] NIS-irányelv 14. cikk (1)–(4) bekezdés.

A NIS-irányelv a digitális szolgáltatókra és az alapvető szolgáltatást nyújtó szereplőkre egyaránt elsődlegesen a jelentős zavart okozó biztonsági események bejelentési kötelezettségét írja elő azzal, hogy a zavar jelentőségének meghatározásához a tagállamoknak ágazatközi tényezőket kell figyelembe venniük. Ágazatközi tényezőknek minősülnek legalább az alábbiak:

a. a szolgáltatásokat igénybe vevő felhasználók száma (akár közvetlenül, akár közvetetten – pl. szolgáltatón mint közvetítőn keresztül – veszik igénybe az adott szolgáltatást),
b. az adott szolgáltatást nyújtó szereplők függelmi helyzete a jelentős zavart okozó biztonsági eseménnyel érintett más szervezet által nyújtott szolgáltatástól,
c. a biztonsági események hatása – mértéküket és időtartamukat tekintve – a gazdasági és társadalmi tevékenységekre vagy a közbiztonságra,
d. a jelentős zavart okozó biztonsági eseménnyel érintett szervezet piaci részesedése,
e. az adott biztonsági esemény által esetlegesen érintett terület földrajzi kiterjedése,
f. a jelentős zavart okozó biztonsági eseménnyel érintett szervezet jelentősége a szolgáltatás elégséges szintjének fenntartásában, figyelembe véve az adott szolgáltatás nyújtásához rendelkezésre álló egyéb lehetőségeket is[22].

Fentiekben felsorolt, a NIS-irányelv által előírt kötelezettségek közül a nemzeti stratégia készítésére és az alapvető szolgáltatók kijelölésére vonatkozó részletszabályok a következő fejezetekben kerülnek ismertetésre.

2.2.2. Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiája

A hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia (a továbbiakban: nemzeti stratégia) olyan keret, amelyben a hálózati és információs rendszerek biztonságára vonatkozóan nemzeti szinten stratégiai célkitűzéseket és prioritásokat állapít meg.[23] A NIS-irányelv[24] rendelkezik arról, hogy valamennyi tagállamnak kötelező elkészítenie és elfogadnia a nemzeti stratégiáját, amelyben az alapvető szolgáltatásként érintett ágazatokra (energia, közlekedés, banki szolgáltatások, pénzügyi piaci infrastruktúrák, egészségügy, ivóvízellátás és -elosztás, digitális infrastruktúra) és a digitális szolgáltatókra (online piactér, online keresőprogram, felhőalapú számítástechnikai szolgáltatás) vonatkozóan meg kell határozni:

a. a stratégiai célokat, valamint
b. a hálózati és információs rendszerek magas szintű biztonságának megteremtéséhez és fenntartásához szükséges szakpolitikai és szabályozási intézkedéseket.

A nemzeti stratégiának az alábbiakat kell tartalmaznia[25]:

a. a stratégiai célokat és prioritásokat, valamint ezek teljesítését szolgáló irányítási keretrendszert, ideértve a kormányzati szervek és egyéb érintett szereplők szerepkörét és felelősségét is,
b. a felkészültségre, a reagálásra és a helyreállításra vonatkozó intézkedések azonosítását, ideértve a köz- és a magánszféra közötti együttműködést is,
c. a kapcsolódó oktatási, tájékoztató és képzési programok, valamint a kutatási és fejlesztési tervek megjelölését,
d. a kockázatok feltárására szolgáló kockázatértékelési tervet,
e. a végrehajtásába bevont szereplők jegyzékét.

[22] NIS-irányelv 6. cikk (1) bekezdés.
[23] NIS-irányelv 4. cikk 3. pont.
[24] NIS-irányelv 7. cikk (1) bekezdés.
[25] NIS-irányelv 7. cikk (1) bekezdés.

A nemzeti stratégiát, annak elfogadást követő 3 hónapon belül, meg kell küldeni a Bizottságnak.

Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat (a továbbiakban: Korm. határozat) 1. pontja alapján, a Kormány elfogadta Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiáját (a továbbiakban: Stratégia).[26] A Stratégia célja[27]:

a. a szabad, biztonságos és innovatív kibertér megteremtése,
b. Magyarország versenyképességének növelése,
c. az innovációk, az új technológiai megoldások biztonságos módon történő bevezetése, illetve adaptálása,
d. a digitalizálódott államigazgatási, kormányzati és gazdasági területeken, a biztonságosabb elektronikus közigazgatási rendszer létrehozása, illetve az állami szolgáltatások innovatív fejlesztése, valamint
e. a kiberbiztonság, a tudatosság növelése, a felkészültség szintjének emelése a társadalom minden területén.

A Stratégia célkitűzései között 3 fő prioritás szerepel:

a. a digitális környezet iránti bizalom erősítése,
b. a digitális infrastruktúra-védelem és
c. a gazdasági szereplők támogatása.

Ezen fő prioritások 12 témakörben kerültek kibontásra, 56 darab intézkedés nevesítésével együtt, amelyek végrehajtásához külön intézkedési tervet kell kidolgoznia a nemzeti stratégia megalkotásáért felelős szervezetnek.

A *digitális környezet iránti bizalom erősítése* prioritáshoz tartozó témakörök és intézkedések az alábbiak[28]:

1. A szakmai együttműködés erősítése, különös tekintettel a biztonsági kérdésekkel, a biztonsági események kezelésének kérdéskörével kapcsolatban, mivel az érintettek közötti megfelelő kommunikáció és információcsere a záloga annak, hogy hatékony reagálásra és védelmi intézkedések meghozatalára kerüljön sor. A már meglévő együttműködési formák erősítése és új együttműködési csatornák kialakítása érdekében előírt intézkedések (7 darab) a következők:
   a. felül kell vizsgálni a kormányzati, piaci, oktatási és civil szereplők együttműködésének hatékonyságát;
   b. biztosítani kell azt a fórumot, ahol lehetőség nyílik a társadalmi párbeszédre és a széleskörű tájékoztatásra, az etikus hackerek szerepének, illetve a társadalom és az etikus hackerek viszonyának tisztázására;
   c. azonosítani kell, hogy mely területen szükséges javítani a meglévő együttműködésen;
   d. létre kell hozni a hatóságok, az állami és civil szervezetek, valamint az eseménykezelő központok közötti információmegosztás, illetve a kölcsönös segítségnyújtás érdekében az összehangolt megelőzési, feltárási, mérséklési és reagálási mechanizmusokat;
   e. ösztönözni kell a „Hibavadász" programok használatát az informatikai rendszerek gyengeségeinek feltárása és a biztonsági hibákra való figyelmeztetés érdekében;
   f. időszakos kiberbiztonsági gyakorlatokat kell tartani a reagáló és védekezési képesség továbbfejlesztése érdekében;
   g. támogatni és ösztönözni kell a köz- és magánszféra közös felelősségvállalásának tudatosítását.

[26] A nemzeti stratégia ismertetésére a www.kormany.hu oldalon található normaszöveg felhasználásával kerül sor, egyes esetekben információbiztonsági alapvetések kiegészítésével.

[27] Nemzeti stratégia 1. oldal.

[28] Nemzeti stratégia 11–13. oldalak.

2. A biztonságtudatosság növelése, az állampolgárok, szervezetek, a társadalom és a gazdaság szereplői irányába a kibertér és a digitális világ (digitális eszközök és elektronikus szolgáltatások) biztonságos használatával és kiberbiztonsággal összefüggésben. Az intézkedések (3 darab) kiemelt célja, hogy a lakosság és a gazdasági szereplők legyenek tudatában annak, hogy hol juthatnak hiteles információhoz és hova fordulhatnak segítségért, amellyel összefüggésben szükséges, hogy hiteles adatok álljanak rendelkezésre a lakosság és a gazdasági szereplők tájékozottságáról, tudatosságáról, felkészültségéről, fenyegetettségi helyzetéről. Előírás, hogy olyan ösztönzők kidolgozására kerüljön sor, melyek segítségével a kis- és középvállalkozási szektorban az információbiztonsági politikával rendelkező szervezetek aránya növekszik.
3. A kiberbűnüldözés fejlesztése, a felderítési hatékonyság növelésével, valamint a preventív intézkedések megtételével a károk mérséklésének érdekében, ideértve az elkövetők jövőbeni jogsértő magatartásának visszaszorítását. Ennek érdekében az intézkedések (2 darab) előírják, hogy:
    a. fejleszteni kell a rendvédelem és az igazságszolgáltatás kiberbűncselekmények elleni fellépési képességét,
    b. aktív együttműködés és információmegosztás szükséges a kiberbűncselekmények elleni hazai, valamint nemzetközi szervezetek között.
4. A szakmai irányító intézményrendszer fejlesztése, amely érdekében Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat (a továbbiakban: NKS) által létrehozott szakosított intézményrendszert, annak feladat- és hatásköre felülvizsgálatát kell elvégezni. Az előírt intézkedések (4 darab) a következők:
    a. ki kell jelölni a NIS-irányelvben megfogalmazott követelményeknek megfelelően a szükséges nemzeti szakosított intézményeket (CSIRT-ek és hatóságok);
    b. ki kell alakítani a nemzeti stratégiában megfogalmazott céloknak megfelelő szervezeti rendszert;
    c. fejleszteni kell a létfontosságú rendszerek, létesítmények és szolgáltatások információbiztonsági hatósági rendszerét az irányelvben megfogalmazott követelmények ágazatokon átívelő érvényesítése érdekében;
    d. létre kell hozni – a meglévő szabályozás figyelembevételével – a nemzeti eseménykezelő központot a nemzeti kibertér használóinak szélesebb köre számára elérhető kiberbiztonsági szolgáltatások nyújtása érdekében.

A *digitális infrastruktúra-védelem* prioritáshoz tartozó témakörök és intézkedések az alábbiak[29]:

1. Az informatikai fejlesztések minőségmenedzsmentjének kialakítása, amely során már a fejlesztés tervezési szakaszában meg kell határozni a kiberbiztonsági kritériumokat és azok mérési mutatóit. A minőségbiztosítási folyamat tervezéséhez előírt intézkedések (4 darab) rögzítik, hogy:
    a. kerüljön kialakításra egy könnyen elérhető, érthető és használható információs bázis,
    b. kerüljenek kidolgozásra a különböző komplexitású informatikai projektekhez, modulárisan felépülő módszertani útmutatók,
    c. kerüljenek kialakításra ingyenes segédletek a belső minőségbiztosítási folyamathoz,
    d. kerüljön kialakításra egy magyar–angol kétnyelvű, ingyenes, modulárisan felépülő, nyilvánosan elérhető kiberbiztonsági minőségmenedzsment tudástár.
2. A kormányzati elektronikus szolgáltatások biztonságának növelése, amely során tovább kell emelni a közigazgatás belső folyamatainak, illetve a közigazgatási szolgáltatásoknak elektronizálását, valamint az állami érdekkörbe tartozó információk és tartalmak digitalizációját és nyilvánosságát. Ezen törekvések végrehajtása során kiemelt figyelmet kell fordítani a hálózatok, rendszerek, folyamatok és felhasználói adatok biztonságára. A célok elérésére előírt intézkedések (7 darab) rögzítik, hogy:
    a. garantálni kell a kormányzati IT üzembiztos és biztonságos működését,

[29] Nemzeti stratégia 14–17. oldalak.

b. meg kell valósítani a nemzetbiztonsági szempontból, illetve a közigazgatás belső működése és az elektronikus közigazgatási szolgáltatások elérhetősége szempontjából létfontosságú információs infrastruktúrák, rendszerek és külső alkalmazások, valamint az ezekben tárolt és kezelt adatok maximális védelmét,
c. biztosítani kell a közigazgatás belső rendszereit és külső szolgáltatásait kiszolgáló hálózatok, informatikai infrastruktúra és alkalmazások maximális védelmét,
d. meg kell valósítani az ágazati sajátosságok figyelembevételével a közigazgatást átfogó, annak valamennyi alrendszerét érintő biztonsági felügyeletet,
e. elő kell írni, hogy a kormányzati támogatásban részesülő informatikai fejlesztések teljesülése a biztonsági előírások megvalósulásához legyen kötve,
f. el kell készíteni a meglévő e-közszolgáltatások esetében az előírt biztonsági szint eléréséhez szükséges intézkedési tervet,
g. szigorítani kell a meglévő szabályozást és gyakorlatot az informatikai fejlesztések egységes biztonsági követelményrendszerének kötelező előírásával.

3. A nemzetközi együttműködés erősítése a stratégiai és operatív szintű regionális és nemzetközi kibervédelmi gyakorlatok tervezésében és végrehajtásában, kiváltképp az Unió, a NATO és a közép-kelet-európai régió keretein belül történő kiberbiztonsági együttműködésekben, a kapcsolódó nemzetközi elvárások és szabályozások megfogalmazásában. Emellett aktív részvétel szükséges a szektorális együttműködést biztosító közösségekkel és központokkal (ISAC-ok, szektorális CSIRT-ek). A kölcsönös bizalmon alapuló együttműködés kialakítása érdekében előírt intézkedések (4 darab) előírják, hogy:
   a. erősíteni kell az együttműködést a NIS-irányelvben meghatározott uniós és a kijelölt hazai intézmények között,
   b. összehangolni és fokozni kell a hazai intézmények nemzetközi együttműködését,
   c. részt kell venni nemzetközi szintű kiberbiztonsági gyakorlatokon a nemzetközi együttműködés előmozdítása és a nemzetközi szintű reagáló és védekezési képesség továbbfejlesztése érdekében,
   d. hangsúlyosan kell képviselni Magyarország érdekeit és értékeit a kibertérrel kapcsolatos külkapcsolati tevékenység során.
4. Az alapvető szolgáltatások, valamint a létfontosságú infrastruktúrák és szolgáltatásaik védelme, amely kiemelt célja, hogy azon alapvető szolgáltatást nyújtó szereplők, valamint a digitális szolgáltatók, amelyek kijelölt létfontosságú rendszerek és létesítmények, üzemeltető szinten kiemelten kezeljék a hálózati és információs rendszereik kockázatokkal arányos, zárt, teljes körű és folytonos védelmének megteremtését és fenntartását. A célok eléréshez előír intézkedések (7 darab) között rögzítésre került, hogy ki kell alakítani egy olyan kockázatértékelési, elemzési módszertant, amely lehetővé teszi az adatok korrelált gyűjtését, a szolgáltatáskiesés hatásainak dinamikus becslését és a kötelező évenkénti jelentést a szervezetek számára. Mindezt ágazati szinten kell megvalósítani. A további intézkedések rögzítik, hogy:
   a. hozzáférhetővé kell tenni a biztonsági célok elérésére vonatkozóan az ágazatközi, illetve ágazatspecifikus ajánlásokat és jó gyakorlatokat,
   b. elő kell mozdítani az állami intézmények és a magánszektor szereplőinek kölcsönös bizalmon alapuló együttműködésének kialakítását és fenntartását,
   c. hozzáférhetővé kell tenni a kritikus infrastruktúrák üzemeltetői részére a védelmet kiegészíteni képes, egységes szolgáltatáscsomagot,
   d. biztosítani szükséges a célzott pályázati lehetőségeket az üzemeltetők, a szolgáltatást nyújtók, az érintett hatóságok és az eseménykezelő központok működésének fejlesztésére a létfontosságú rendszerek, létesítmények és szolgáltatások fizikai és kiberbiztonsága területén a hatékony megelőzés és gyors reagáló képesség fejlesztésére,

e. fokozni kell a létfontosságú rendszerek, létesítmények és szolgáltatások üzemeltetőinek irányába az információbiztonsági tudatosítási tevékenységet az érintett hatóságok és szervezetek részvételével,
f. be kell vonni a nemzeti és nemzetközi védelmi gyakorlatokba a létfontosságú infrastruktúrák üzemeltetőit.

5. A védekező, elhárító és reagáló kiberképességek fejlesztése, amely során alapvető célként került meghatározásra, a meglévő infrastruktúra passzív és aktív eszközeinek széleskörű kialakítása és alkalmazása. Az intézkedések (5 darab) rögzítik, hogy:
   a. fejleszteni kell azon észlelési, feldolgozási (elemzés) és felderítési képességeket, amelyek lehetővé teszik a fenyegetések és támadások felismerését, osztályozását és forrásának megállapítását,
   b. meg kell teremteni az ágazati szinten egységes és ágazatok közötti koordináción alapuló irányítást és menedzsmentet,
   c. ki kell alakítani a gyors helyzetfelismerés, az értékelés és a kockázatelemzés rendszerét,
   d. ki kell fejleszteni a különböző fokozatú reagálás eszközrendszerét,
   e. meg kell teremteni a lehetőségét annak, hogy különleges esetekben civil, polgári területen dolgozó szakemberek is részt tudjanak venni a nemzeti kibervédelemben.

A *gazdasági szereplők támogatása* prioritáshoz tartozó témakörök és intézkedések az alábbiak[30]:

1. A kutatóközpontokkal való együttműködés, valamint a kutatás és fejlesztés szerepének erősítése, amely során szükséges a felsőoktatási és tudományos kutatóműhelyekkel a stratégiai együttműködés kialakítása, valamint az ilyen irányú K+F feladatok és források kutatóbázisokhoz történő összpontosítása. A célok elérésére előírt intézkedések (5 darab) rögzítik, hogy:
   a. biztosítani kell a mérnökök, kutatók képzéséhez és a kiemelkedő tehetségek gondozásához, illetve magyarországi tevékenységükhöz szükséges feltételeket,
   b. létre kell hozni egy kiberbiztonsági szakterületet érintő kutatási stratégiát, melynek célja a magyar fejlesztésű kiberbiztonsági eszközök, szoftverek és termékek alkalmazásának fokozása, amely stratégiának kiemelten kell kezelnie az Unió 2021–2027 között meghirdetésre kerülő Kutatás+Fejlesztés+Innováció felhívásainak témáit, a magyar szervezetek nemzetközi projektekben való részvétele céljából,
   c. azonosítani kell a kapcsolódó kutatás-fejlesztési témaköröket azzal, hogy meg kell teremteni az ehhez szükséges állami ösztönzési lehetőségeket, beleértve a magyar korai fázisú vállalkozások ösztönzését is,
   d. támogatni kell a gazdaságdiplomáciai tevékenységek során a kiberbiztonsággal foglalkozó magyar szolgáltató- és fejlesztőközpontok megjelenését.
2. A hazai digitális innováció támogatása, támogatási konstrukciók kialakítása, koordinációs feladatok ellátása, amelyhez kapcsolódóan előírt intézkedések (2 darab) rögzítik, hogy:
   a. ki kell alakítani az államilag támogatott kibervédelmi szolgáltatáscsomagokat a szektor vállalkozásainak a nehezen elérhető, drága megoldások beszerzésének és bevezetésének elősegítése érdekében,
   b. biztosítani kell a vállalkozások számára a támogatott formában elérhető oktatási, képzési programokat biztonsági üzemeltetési, biztonsági megfelelőségi és audit témában.
3. A versenyképes hazai tudásbázis létrehozása, amely érdekében a kiberbiztonsági oktatás, képzés, valamint a kutatási és fejlesztési lehetőségek fejlesztése mellett a digitális kompetenciák, a tudatosság és tájékozottság, illetve az információbiztonságot elősegítő oktatási és szakképzési szakterületek fejlesztését kell elvégezni. Ezzel összefüggésben az előírt intézkedések (6 darab) rögzítik:

[30] Nemzeti stratégia 18–20. oldalak.

a. át kell tekinteni az aktuális problémákat és meg kell fogalmazni az azonosított problémák kezelésére vonatkozó javaslatokat a kiberbiztonsági munkacsoportnak,
b. biztosítani kell, hogy az érintett oktatási és szakképzési végzettségek adjanak megbízható alapot a munkaerőpiaci versenyben,
c. meg kell teremteni és hozzáférést kell biztosítani az érintetteknek egy közös informatikai tudásbázishoz,
d. biztosítani kell az információbiztonsági képzéshez való hozzájutást és a képesítés szerzésének lehetőségét a társadalom széles köre számára,
e. ki kell dolgozni az alapvető szolgáltatók személyi állományát érintően az információbiztonságra vonatkozó képzettségi követelményeket és a képzési programokat,
f. támogatni kell azokat az egységes minőségi követelmények mellett megtartott helyi és országos kiberbiztonsági gyakorlatokat és versenyeket, melyek a közép- és felsőoktatásban tanuló fiatalok bevonását és tudásnövelését célozzák meg.

A kormányhatározat 2. pontja felhívja a belügyminisztert, hogy az érintett miniszterek bevonásával, a Stratégiában szereplő 56 darab intézkedés végrehajtása érdekében 2019. március 31-ig intézkedési tervet készítsen. (Az intézkedési terv elkészítése jelen jegyzet kéziratának lezárásánál még folyamatban volt a kijelölt szerv által.)

2.3. Főbb változások a magyar kibervédelmi szabályozásban

A 2018. évben a nemzeti szabályozás főáramát a NIS-irányelvből eredő átültetési kötelezettség határozta meg. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és végrehajtási rendeletei tekintetében minden esetben sor került a jogharmonizációs klauzula beépítésére, amely átültetési kötelezettségből eredő szabályváltozások főként 2019. január 1-vel kerültek hatálybaléptetésre. További számottevő változás a törvényi szintet nem érintette, de új végrehajtási rendeletek megalkotására vonatkozó felhatalmazó szabályok megalkotására sor került. Mindemellett a lassan „iskolaérett", hatéves Ibtv. novelláris felülvizsgálata továbbra is várat magára.

2.3.1. Az Ibtv. változásai

Az Ibtv.-nek az Ákr.[31] hatálybalépésével összefüggő és az E-ügyintézési tv.[32] végrehajtásához kapcsolódó módosításai mellett – a NIS-irányelv szerinti jogharmonizációs klauzula beépítésén kívül – a 2018. évben érdemi módosítása csak a biztonsági szintbe sorolást érintően volt. A módosítás azt a kiegészítő szabályt[33] érintette, amely szerint, ha a szervezet vagy szervezeti egység biztonsági szintje az 1. szintet nem éri el, az 1. szint eléréséhez szükséges intézkedéseket 6 éven belül meg kell valósítani. Ezt a kiegészítő szabályt a törvény hatálybalépése óta 2018-ig négy alkalommal[34] módosították, azonban a szabály újabb módosítására 2019-ben is sor került, amely következtében a „türelmi időt" 6 évről 8 évre emelték.

31 Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény.
32 Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény
33 Ibtv. 10. § (3) bekezdés.
34 2015-ben 1 évről 2 évre, 2016-ban 2 évről 4 évre, 2017-ben 4 évről 5 évre, 2018-ban 5 évről 6 évre.

2019-ben az Ibtv. módosításának első lépéseként az értelmező rendelkezések január 1-jei kiegészítésére került sor. Meghatározásra került a NIS-irányelvvel összhangban az alapvető szolgáltatásokat nyújtó szereplő és a bejelentésköteles szolgáltatás[35] fogalma, mindkét esetben utaló szabály alkalmazásával az ágazati jogszabályra. Alapvető szolgáltatásokat nyújtó szereplőnek a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 2/A. §-a alapján kijelölt szolgáltató minősül[36] (ezen törvény a 4. fejezetben kerül ismertetésre). Bejelentésköteles szolgáltatásnak[37] minősülnek az információs társadalommal összefüggő szolgáltatások – ide nem értve az Ibtv. személyi hatálya alá tartozó szervek[38] számára adatkezelést végzők és a nemzeti adatvagyon körébe tartozó nyilvántartások adatfeldolgozói által nyújtott szolgáltatásokat – közül:

a. az online piactér[39],
b. a keresőszolgáltatás[40] és
c. a felhőalapú számítástechnikai szolgáltatás[41].

Változott továbbá az elektronikus információs rendszer fogalma[42] is, amely igazodik a NIS-irányelv hálózati és információs rendszer fogalmához[43]. Az új meghatározás alapján elektronikus információs rendszernek minősül:

a. az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat[44];
b. minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi vagy
c. az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

A létfontosságú rendszerelemek ágazati szabályozásával összefüggően rögzítésre került a honvédelmi célú elektronikus információs rendszer fogalma[45], valamint az Unió Általános Adatvédelmi Ren-

35 Ibtv. 1. § (1) bekezdés 7a. pont.

36 Ibtv. 1. § (1) bekezdés 6a. pont.

37 Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2. § j) pontjában meghatározott szolgáltatások.

38 Ibtv. 2. § (1) bekezdés.

39 Olyan szolgáltatás, amely a fogyasztói jogviták alternatív rendezéséről, valamint a 2006/2004/EK rendelet és a 2009/22/EK irányelv módosításáról szóló, 2013. május 21-i 2013/11/EU európai parlamenti és tanácsi irányelv szerinti fogyasztók, illetve kereskedők számára lehetővé teszi, hogy az online piactér weboldalán vagy valamely kereskedőnek az online piactér által nyújtott számítástechnikai szolgáltatásokat felhasználó weboldalán keresztül online adásvételi vagy szolgáltatási szerződéseket kössenek.

40 Olyan szolgáltatás, amely információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára.

41 Olyan szolgáltatás, amely távoli hozzáférést tesz lehetővé a többek között hálózati funkciókat, adattárolást, alkalmazások, szolgáltatások futtatását biztosító számítástechnikai megoldásokhoz.

42 Ibtv. 1. § (1) bekezdés 14a. pont.

43 NIS-irányelv 4. cikk 1. pont.

44 Elektronikus hírközlő hálózat: átviteli rendszerek és – ahol ez értelmezhető – a hálózatban jelek irányítására szolgáló berendezések, továbbá más erőforrások – beleértve a nem aktív hálózati elemeket is –, amelyek jelek továbbítását teszik lehetővé meghatározott végpontok között vezetéken, rádiós, optikai vagy egyéb elektromágneses úton, beleértve a műholdas hálózatokat, a helyhez kötött és a mobil földfelszíni hálózatokat, az energiaellátó kábelrendszereket, olyan mértékben, amennyiben azt a jelek továbbítására használják, a műsorszórásra használt hálózatokat és a kábeltelevíziós hálózatokat, tekintet nélkül a továbbított információ fajtájára. – 2003. évi C. törvény).

45 Ibtv. 1. § (1) bekezdés 23 pont: honvédelmi célú elektronikus információs rendszer: a honvédelmért felelős miniszter vezetése, irányítása alatt álló szervek zárt célú elektronikus információs rendszereinek, valamint egyéb – funkciója, rendeltetése, feladatellátása szerint – nyílt elektronikus információs rendszereinek összessége, amely ágazatspecifikus módon támogatja a honvédelmi ágazaton belüli és ágazatok közötti működést.

delete[46] és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) módosítása miatt a kritikus adat fogalma[47].

Az Ibtv. személyi hatálya alá tartozó szervek esetében alaprendelkezés, hogy az általuk kezelt adatok csak a Magyarország területén üzemeltetett és tárolt elektronikus információs rendszerekben, valamint honvédelmi, diplomáciai információs célokra használt zárt célú elektronikus információs rendszerben kezelhetők. Ez alól kivételt képez a Magyar Nemzeti Bank által a monetáris politika végrehajtásával és a devizatartalék kezelésével kapcsolatos kockázatértékelési és portfoliókezelési tevékenysége keretében kezelt adatok köre. Ez a kivétel vonatkozik az EGT-államok területén belül üzemeltetett elektronikus információs rendszerekben történő, hatósági engedélyen alapuló rendelkezésre is[48].

Kiegészítésre került továbbá a Nemzetbiztonsági Szakszolgálat, mint az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóság (a továbbiakban: Hatóság)[49], jogköre az elektronikus információs rendszer védelmére vonatkozó intézkedések terén. Ez alapján a Hatóság jogosult az eljárása során független, képesített ellenőrt igénybe venni és az általa végzett ellenőrzés eredményét megállapításainál figyelembe venni[50].

2019. január 1-től új hatósági jogkör a költségvetési szervek esetében történő – a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat megsértése esetén – a bírság kiszabása[51], amely részletszabályait az Ibtv. végrehajtási rendelete tartalmazza (lásd: 3.2 fejezet).

Európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemek szervezetei tekintetében a Hatóság előzetes engedélyezési jogköre megszűnt az adott szervezetre irányadó besorolási szintnél alacsonyabb szintű besorolás megállapítása esetén, az indokolási kötelezettség azonban megmaradt[52].

Kiegészült az Eseménykezelő Központ jogköre a sérülékenységvizsgálatok elvégzésével kapcsolatban, mivel már saját hatáskörben a Központ is indíthat és lefolytathat sérülékenységvizsgálatot regisztrált felhasználói jogosultság birtokában vagy ennek hiányában, ha erre külön jogszabály felhatalmazza[53].

A NIS-irányelvből adódó kötelezettségek végrehajtása érdekében az Ibtv. eseménykezelő központokra vonatkozó rendelkezései szintén módosultak. A kormány által kijelölt eseménykezelő központ (a továbbiakban: Központ)[54]:

a. az alapvető szolgáltatást nyújtó szolgáltatók, valamint a bejelentésköteles szolgáltatást nyújtó szolgáltatók elektronikus információs rendszereit (kivéve a honvédelmi célú elektronikus információs rendszereket és a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit), valamint
b. az európai vagy nemzeti létfontosságú rendszerelemmé törvény[55] alapján kijelölt rendszerelemek elektronikus információs rendszereit

érintően a Nemzetbiztonsági Szakszolgálat irányítása alatt működő Nemzeti Kibervédelmi Központ lett. A Központ feladatai kiegészültek az azonnali figyelmeztetések közzétételével a

[46] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről.

[47] Ibtv. 1. § (1) bekezdés 32a. pont – kritikus adat: a személyes adat vagy valamely jogszabállyal védett adat.

[48] Ibtv. 3. §. (1) és (3) bekezdései, hatályosak 2019. január 1-től.

[49] Hatósági rendelet 2. §-a.

[50] Ibtv. 4. §-a és 16. §. (1) bekezdés h) pont, hatályosak 2019. január 1-től.

[51] Ibtv. 16. §. (1) bekezdés h) pont, hatályos 2019. január 1-től.

[52] Ibtv. 9. §. (6) bekezdés.

[53] Ibtv. 18. §. (2a) bekezdés, hatályos 2019. január 1-től.

[54] Ibtv. 19. §. (1) bekezdés, hatályos 2019. január 1-től.

[55] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (a továbbiakban: Lrtv.).

kritikus hálózatbiztonsági fenyegetettségekről és ezek magyar nyelvű megjelenítésével, valamint a nemzetközileg publikált sérülékenységek honlapján történő hozzáférhetővé tételével[56].

Módosult az Ibtv. adatvédelmi rendelkezése is. A Hatóság és az eseménykezelő központok a hatósági döntés véglegessé válását, a sérülékenységvizsgálat lezárását, valamint a biztonsági esemény vizsgálatának lefolytatását követő öt évig jogosultak adatkezelésre, amely lejártát követően kötelesek az elektronikus információs rendszereikből és adathordozóikról az adatokat törölni. Módosult továbbá a munkatársakra vonatkozó titoktartási kötelezettség szabálya is, amely a minősített adatok tekintetében azok érvényességi idejének végéig, személyes adatok tekintetében időkorlát nélkül fennmarad.[57]

2.3.2. A végrehajtási rendeletek változásai

2018-ban – figyelemmel a NIS-irányelvben meghatározott határidőre – sor került az Ibtv. végrehajtási rendeletei vonatkozásában a NIS-irányelvnek való megfelelés céljából a jogharmonizációs klauzula beépítésére. Jelen tananyag a végrehajtási rendeletek közül kizárólag a kormányrendeletek változását tárgyalja, a miniszteri rendeleti szintű háttérszabályok ismertetésére nem tér ki, mivel azok módosítására 2019-ben nem került sor. A kormányrendeletek közül a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet módosítására nem került sor. A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendelet 2019. január 1-től hatályos minimális szövegcserés módosítására az Ibtv. Hatóság és Központ elnevezésének és feladatkörének változása miatt került sor, kodifikációs pontosítások átvezetése mellett.

1. 2019-ben az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról 187/2015. (VII. 13.) Korm. rendelet (a továbbiakban: hatósági rendelet) változásait a Hatóság feladatellátásával összefüggő módosítások alkották. Alapvetésként bekerült a szabályozásba a Hatóság függetlenségét deklaráló rendelkezés, amely szerint hatósági eljárása során és hatósági döntéseinek tartalmával összefüggésben – a feladat elvégzésére vagy a mulasztás pótlására irányuló utasítás kivételével – nem utasítható[58].

Az Ibtv. változásával összhangban, amely szerint a Hatóság jogosult az eljárása során független, képesített ellenőrt igénybe venni és az általa végzett ellenőrzés eredményét megállapításainál figyelembe venni, a hatósági rendelet is módosításra került. Az ellenőrzési jogosultság kiterjed minden olyan, az elektronikus információs rendszer védelmére vonatkozó intézkedésre, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek[59].

A Hatóság feladatai közül – az Ibtv. fent említett változásaival való összhang megteremtése érdekében – néhány törlésre került[60], illetve új feladatként jelentek meg az alábbiak[61]:

a. hatósági ellenőrzés keretében lefolytatja a fizikai, logikai és adminisztratív védelmi ellenőrzéseket,

[56] Ibtv. 20. §. (1) bekezdés, hatályos 2019. január 1-től.
[57] Ibtv. 22. §. (2)–(3) bekezdései, hatályosak 2019. január 1-től.
[58] Hatósági rendelet 2. § (2) bekezdése.
[59] Hatósági rendelet 5/A. §.
[60] Hatósági rendelet 6. § (1) bekezdés i)–n) pontok, hatályos 2019. január 1-től.
[61] Hatósági rendelet 6. § (1) bekezdés f)–h) pontok, hatályos 2019. január 1-től.

b. a Központtól kapott, biztonsági eseményekkel kapcsolatos értesítéseket nyilvántartja és honlapján közzéteszi azokat,
c. az elektronikus információs rendszerek biztonságáért felelős nemzetközi szervezetekben ellátja Magyarország képviseletét.

A NIS-irányelv átültetésének és végrehajtásának felügyeletére kijelölt nemzeti hatóság a BM OKF, amely egyben ellátja az alapvető szolgáltatásokat nyújtó szolgáltatók hálózati és információs rendszerei biztonságának felügyeletét is. Szükség szerint konzultációt folytat és együttműködik a bűnüldöző szervekkel, illetve a Nemzeti Adatvédelmi és Információszabadság Hatósággal (a továbbiakban: NAIH), valamint tájékoztatja a NIS-irányelv szerint kijelölt, az elektronikus információs rendszerek biztonságáért felelős nemzeti egyedüli kapcsolattartó pontot[62] (a továbbiakban: egyedüli kapcsolattartó pont).

A Hatóság, mint egyedüli kapcsolattartó pont, feladatai az alábbiak:

a. biztosítja a hatóságok és az érintett EGT-tagállamok hatóságai között folytatott együttműködést,
b. együttműködik a NIS-irányelvnek való megfelelés vizsgálata érdekében a Központtal, a BM OKF-fel, valamint a Hatósággal[63],
c. az azonosított alapvető szolgáltatásokat nyújtó szolgáltatók elektronikus információs rendszerei esetében a megfelelés vizsgálatával összefüggő adatokat[64], valamint a vizsgálat eredményét megküldi az Európai Bizottság részére,
d. tájékoztatja az érintett tagállamokat az azonosított alapvető szolgáltatásokat nyújtó és a bejelentésköteles szolgáltatást nyújtó szolgáltatók elektronikus információs rendszereiben bekövetkezett biztonsági eseményről, ha az jelentős zavart okozott a szolgáltatás nyújtásában,
e. az Unió e feladatra létrehozott Együttműködési csoportja részére összefoglaló jelentést küld a d) pont szerinti biztonsági eseményekről,
f. együttműködik a magyar és a nemzetközi hálózatbiztonsági szervekkel, különösen az Együttműködési csoporttal és a NIS-irányelv által létrehozott CSIRT-ek hálózatával,
g. szükség szerint konzultációt folytat és együttműködik a rendvédelmi szervekkel, illetve a NAIH-val[65].

Az Ibtv. módosításához igazodva változtak a Hatóság által alkalmazható jogkövetkezményekre vonatkozó szabályok. A bírság kiszabása, mint szankció, már költségvetési szerv esetén is alkalmazható. Az új eljárási lépések az alábbiak[66].

a. A Hatóság vagy a Központ értesítése esetén megfelelő határidő tűzése mellett a Hatóság felszólítja az érintett szervezetet a jogszabálysértő tevékenység vagy a jogsértő állapot megszüntetésére, ennek keretében különösen bejelentési, adatszolgáltatási, együttműködési kötelezettségének teljesítésére.

---

62 Hatósági rendelet 25. § (5)–(7) bekezdései, hatályosak 2019. január 1-től.

63 Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 6/B. § (3) bekezdése szerinti hatóság.

64 A megküldött adatok köre:
a) az alapvető szolgáltatásokat nyújtó szereplők azonosítását lehetővé tevő nemzeti intézkedések,
b) a kritikus társadalmi, gazdasági tevékenységek fenntartásához nyújtott alapvető szolgáltatások jegyzéke,
c) az alapvető szolgáltatásokat nyújtó szereplők száma, valamint az érintett ágazat szempontja szerinti jelentőségük,
d) az adott szolgáltatásra támaszkodó felhasználók száma vagy az alapvető szolgáltatásokat nyújtó gazdasági szereplő ellátási szintje,
e) az eseménykezelő központok hatásköréről és a biztonsági események kezelésére szolgáló eljárásról szóló tájékoztatás.
Hatósági rendelet 29/A. § (2) bekezdés, hatályos 2019. január 1-től.

65 Hatósági rendelet 29/A. § (1) bekezdés, hatályos 2019. január 1-től

66 Hatósági rendelet 13. § (3)–(6) bekezdései, hatályosak 2019. január 13-tól.

b. Ha a költségvetési szerv a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be – a jogkövető magatartás betartására vonatkozó eredménytelen felszólítás, illetve a felügyelő szerv eredménytelen közreműködése esetén –, az eset összes körülményeinek mérlegelésével, bírságot szabhat ki. A kiszabható bírság ötvenezer forinttól ötmillió forintig terjedhet, amelyet a határozat véglegessé válását követő 8 napon belül kell befizetni a Hatóság Magyar Államkincstárnál vezetett számlájára.
c. Az eljárás akadályozása, illetve az adatszolgáltatás nem vagy nem megfelelő teljesítése esetén a Hatóság hárommillió forintig terjedő bírsággal sújthatja – ismételt jogsértés esetén sújtani köteles – a jogsértő vezető tisztségviselőjét is.

	A jogszabálysértés megnevezése	**Legkisebb mérték**	**Legnagyobb mérték**
1.	Regisztráció elmulasztása	50 000 Ft	100 000 Ft
2.	Adatváltozás bejelentésének elmulasztása	50 000 Ft	500 000 Ft
3.	Kockázatelemzés készítésének elmulasztása	200 000 Ft	500 000 Ft
4.	Kockázatokkal arányos biztonsági intézkedések bevezetésének és alkalmazásának elmulasztása	300 000 Ft	5 000 000 Ft
5.	Kockázatelemzés és a szükséges biztonsági intézkedések biztonsági eseményt követő haladéktalan, egyéb esetben évente dokumentált felülvizsgálatának elmulasztása, a felülvizsgálat során feltárt hiányosságok alapján a szükséges módosítások végrehajtásának elmulasztása	200 000 Ft	2 000 000 Ft
6.	Biztonsági esemény bejelentésének elmulasztása	300 000 Ft	5 000 000 Ft
7.	Hatóság végleges, végrehajtandó határozatában foglalt kötelezésének nem teljesítése	400 000 Ft	5 000 000 Ft

2. táblázat: Az egyes jogszabálysértések esetén kiszabható bírság mértéke (Forrás: Hatósági rendelet 1. melléklet.)

2. Főbb változást az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet (a továbbiakban: Rendelet) hozott, amely 2019. január 1-jén lépett hatályba. A Rendelet hatályon kívül helyezte a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) Korm. rendeletet [a továbbiakban: 185/2015. (VII. 13.) Korm. rendelet], amely a NIS-irányelvvel való összhang megteremtésére vonatkozó, átfogó módosítására még 2018. május 10-ei határnappal sor került. A Rendelet normaszövege a 185/2015. (VII. 13.) Korm. rendelet korábbi felépítésén és normaszövegén alapul, az Ibtv. fent említett változásai és a NIS-irányelv, valamint a végrehajtásához szükséges rendelkezéseket megállapító bizottsági rendelet[67] miatt abba új részek is bevezetésre kerültek.

[67] A hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok meghatározásáról szóló, 2018. január 30-i (EU) 2018/151 bizottsági végrehajtási rendelet.

Az értelmező rendelkezések között meghatározásra került az alapvető szolgáltatást nyújtó szolgáltató[68] és a bejelentésköteles szolgáltatást nyújtó fogalma[69], amely összhangban áll a NIS-irányelv és az Ibtv. vonatkozó rendelkezéseivel. Új fogalomként került rögzítésre a CSIRT-ek hálózata, mint a NIS-irányelv által létrehozott hálózat[70], valamint a közvetítő szolgáltató[71] meghatározása. Közvetítő szolgáltató olyan, az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató, amely:

a. egyszerű adatátvitel és hozzáférés-biztosítást,
b. gyorsítótárolást,
c. tárhelyszolgáltatást,
d. keresőszolgáltatást,
e. alkalmazásszolgáltatást
biztosít.

Új sérülékenység vizsgálati módszerként került meghatározásra a pszichológiai manipuláció[72] és fogalma[73], amely olyan tevékenységi forma, technikák és módszerek összessége, amely az emberek befolyásolására alapozva teszi lehetővé bizalmas információk megszerzését vagy kártékony program terjedését és működését. A vizsgálat lefolytatásának határideje 90 nap[74].

A Központ feladatai jelentősen átalakultak. Az új, megváltozott feladatokat a Rendelet az alábbiak szerint határozza meg[75]. A Központ kezeli

a. az Ibtv. hatálya alá tartozó szervek[76] – kivéve a honvédelmi célú és a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit – nyílt,
b. a bejelentésköteles szolgáltatók,
c. az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők (kivéve honvédelmi célú rendszerelemek),
d. a központosított informatikai és elektronikus hírközlési szolgáltató elektronikus információs rendszereit érintő biztonsági eseményeket és fenyegetéseket.

Az eseménykezelés céljából a Központot együttműködési kötelezettség terheli:

a. az elektronikus információs rendszerek felügyeletére kijelölt hatóságokkal,
b. a honvédelmi célú és a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereinek eseménykezelő központjaival,
c. a rendvédelmi szervekkel,
d. a Nemzeti Média- és Hírközlési Hatósággal és az általa működtetett Országos Informatikai és Hírközlési Főügyelettel,

---

68 Alapvető szolgáltatást nyújtó szolgáltató: a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény alapján alapvető szolgáltatást nyújtóként azonosított szolgáltató. – Rendelet 1. § 2. pont.

69 Bejelentésköteles szolgáltatást nyújtó: az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) 2. § j) pontja szerinti szolgáltatást nyújtó szolgáltató. – Rendelet 1. § 4. pont.

70 Rendelet 1. § 8. pont.

71 Rendelet 1. § 11. pont – Közvetítő szolgáltató: az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2. § l) pontja szerint Rendelet 1. § 11. pont.

72 Rendelet 24. § (1) bekezdés d) pont.

73 Rendelet 1. § 15. pont.

74 Rendelet 24. § (3) bekezdés c) pont.

75 Rendelet 3. § (1)–(7) bekezdései.

76 Ibtv. 2. §.

e. az elektronikus hírközlési szolgáltatókkal, a központosított informatikai és elektronikus hírközlési szolgáltatóval,
f. az Lrtv.[77] szerinti üzemeltetőkkel, kijelölő és javaslattevő hatóságokkal, valamint
g. a NAIH-val.

A Központ a biztonsági eseményre vagy fenyegetésre utaló tevékenységek kivizsgálását követően, szükség esetén figyelmeztetést ad ki:

a. a felhasználók,
b. az eseménykezelő központok,
c. az elektronikus információs rendszerek felügyeletét ellátó hatóságok,
d. a Hatóság mint egyedüli kapcsolattartó pont (akit tájékoztat a biztonsági események kezelésére vonatkozó, jogszabályban nem részletezett eljárásrendjéről),
e. az Ibtv. hatálya alá tartozó szervek,
f. a bejelentésköteles szolgáltatók,
g. az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők, valamint
h. a központosított informatikai és elektronikus hírközlési szolgáltatók felé.

A Központ feladatellátása során:

a. végzi a biztonsági események nemzeti szintű nyomon követését,
b. ellátja a kockázatokkal és biztonsági eseményekkel kapcsolatos tájékoztatást az érdekeltek számára,
c. végzi a korai előrejelzéssel, a riasztással, a bejelentéstétellel és az információterjesztéssel kapcsolatos feladatokat,
d. reagál a biztonsági eseményekre,
e. dinamikus kockázat- és eseményelemzéseket, valamint a biztonsági eseményekkel kapcsolatos helyzetképet készít,
f. sérülékenységvizsgálatot végez,
g. a hatáskörébe tartozó elektronikus információs rendszerek tekintetében részt vesz a CSIRT-ek hálózatának tevékenységében,
h. meghatározza a biztonsági események és kockázatok kezelésére vonatkozó eljárásokat, valamint a biztonsági események, kockázatok és információk osztályozására szolgáló eljárásokat és szabályokat.

Változtak a biztonsági események bejelentésére vonatkozó előírások. A Rendelet 8. §-a szerint a Központ felé bejelentési kötelezettség terheli az Ibtv. hatálya alá tartozó szerveket[78] – kivéve a honvédelmi célú és a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit – nyílt rendszereiket ért biztonsági események tekintetében, valamint a közvetítő szolgáltatókat. A honvédelmi célú elektronikus információs rendszert érintő biztonsági eseményt és fenyegetést a Katonai Nemzetbiztonsági Szolgálat felé kell bejelenteni.

A Rendelet szerint a bejelentésnek tartalmaznia kell legalább[79]:

a. a biztonsági esemény rövid leírását és státuszát,
b. a szolgáltatás működésében támadt zavar mértékét,
c. az esemény kezelésére az üzemeltető által kijelölt kapcsolattartó személy és szervezet elérhetőségeit,

[77] Lrtv.
[78] Ibtv. 2. §.
[79] Rendelet 11. §.

d. a biztonsági esemény hatását meghatározó szempontokat, valamint
e. közvetítő szolgáltató igénybevétele esetén a közvetítő szolgáltató megnevezését, elérhetőségét.

A biztonsági események bejelentése elsődlegesen elektronikus úton történik, ha azonban az elektronikus információs rendszer oly mértékben sérül, hogy az nem lehetséges, a bejelentés bármely más módon megvalósítható[80].

Az alapvető szolgáltatást nyújtó szolgáltatókra további külön szabályok vonatkoznak[81]. A szolgáltatás folytonosságára jelentős hatást gyakorló biztonsági eseményeket indokolatlan késedelem nélkül kötelesek bejelenteni a Központnak. A jelentős hatás meghatározása érdekében a bejelentésnek az alábbi adatokat kell tartalmaznia:

a. az alapvető szolgáltatás zavara által érintett felhasználók száma,
b. a biztonsági esemény időtartama,
c. a biztonsági esemény által érintett terület földrajzi kiterjedése.

Ha az alapvető szolgáltatás nyújtása harmadik fél bejelentésköteles szolgáltatóra alapozott, akkor ezen szolgáltatónak is be kell jelentenie minden olyan esetet, amikor a bejelentésköteles szolgáltatót érintő biztonsági esemény jelentős hatást gyakorol az alapvető szolgáltatások folytonosságára.

További kiegészítő szabályok vonatkoznak a bejelentésköteles szolgáltatást nyújtóra is, akinek haladéktalanul be kell jelentenie a Központ részére az elektronikus információs rendszerein bekövetkezett azon biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az általa az Unión belül kínált, bejelentésköteles szolgáltatás nyújtására. A jelentős hatás meghatározása érdekében a bejelentésnek az alábbi – külön jogszabályban meghatározott – adatokat kell tartalmaznia[82]:

a. a biztonsági esemény által érintett felhasználók számát, különös tekintettel azon felhasználókra, akik az érintett szolgáltatásra alapozzák a saját szolgáltatásaik nyújtását,
b. a biztonsági esemény időtartamát,
c. a biztonsági esemény által érintett terület földrajzi kiterjedését,
d. a szolgáltatás működésében támadt zavar mértékét,
e. a gazdasági és társadalmi tevékenységekre gyakorolt hatás mértékét.

A Központ az alapvető szolgáltatást, valamint a bejelentésköteles szolgáltatást nyújtók bejelentései alapján vizsgálja a jelentős hatást gyakorló biztonsági események határon átnyúló hatását, és közvetlenül vagy az egyedüli kapcsolattartó pont útján indokolt esetben tájékoztatja az Unió érintett tagállamait. A tájékoztatás során gondoskodnia kell arról, hogy ne sérüljenek a szolgáltatók kereskedelmi érdekei és a bejelentésben foglalt információk bizalmassága[83].

Új szabályozási elemként megjelent a biztonsági események kezelése tekintetében az önkéntes bejelentés[84] lehetősége az alapvető szolgáltatónak nem minősülő ágazati szereplők részére, kivéve azon rendszerelemeket, amelyek létfontosságú rendszerelemként kijelölésre kerültek. A Központ felé történő bejelentést olyan biztonsági események esetében alkalmazhatják, amelyek jelentős hatást gyakorolnak az általuk nyújtott szolgáltatások folytonosságára. Az online piactért, a keresőszolgáltatást és a felhőalapú számítástechnikai szolgáltatást biztosító bejelentésköteles szolgáltató önkéntes alapon bejelenthet minden olyan eseményt, amelyek számára addig ismeretlen jellemzőkkel bírnak,

80 Rendelet 11. §.
81 Rendelet 9. §.
82 Az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018. (XII. 20.) Korm. rendelet 6. §-a.
83 Rendelet 12. §.
84 Rendelet 13. §.

ideértve különösen a sérülékenységet kihasználó új módszereket, a kihasználásra vonatkozó adatokat, sebezhető pontokat vagy fenyegetéseket. A Központnak ezeket a bejelentéseket csak akkor kell feldolgoznia, ha az nem jelent aránytalan vagy indokolatlan terhet.

A biztonsági eseménnyel érintett szervezet a biztonsági esemény kivizsgálása során köteles együttműködni a Központtal, amely együttműködés kiterjed:

a. a bejelentéssel kapcsolatos információk átadására,
b. a biztonsági eseményben érintettek (támadó/támadott) beazonosításához szükséges műszaki, technikai adatok átadására,
c. a Központ szakembereit illetően:
   ca) a biztonsági esemény következményei elhárítása érdekében tett intézkedésekről, illetve a biztonsági esemény vizsgálata során, az infrastruktúrával kapcsolatos beállításokról történő tájékoztatásra,
   cb) az incidensben érintett infrastruktúrához való hozzáférés biztosítására, valamint
   cc) az általuk végzett kockázatelemzés alapján szükségesnek ítélt korai figyelmeztető- vagy csapdarendszerek, szenzorok telepítésére,
   cd) alapvető szolgáltatást nyújtó szolgáltatók esetében az incidensben érintett infrastruktúrával kapcsolatos, speciális, ágazati sajátosságok megosztására.[85]

A biztonsági eseményekkel érintett szerv – a bejelentésköteles szolgáltató kivételével – köteles a vizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat a Központ rendelkezésére bocsátani[86].

Kiegészítő szabály, hogy a bejelentésköteles szolgáltatók, valamint az alapvető szolgáltatást nyújtó internet szolgáltatók az incidensben érintett előfizetőkkel kapcsolatban a Központ kérésére kötelesek szükség szerint tiltásokat bevezetni, illetve (felhasználói, előfizetői) hozzáféréseket korlátozni, felfüggeszteni vagy megszüntetni.[87]

A bejelentésköteles szolgáltatóra vonatkozóan további kiegészítő szabályok kerültek megalkotásra az alábbiak szerint[88]:

a. Ha a Központtal való együttműködéshez szükséges adatok összegyűjtésére bármely okból nem képes a Központ képviselője helyszíni tanácsadás keretein belül, az érintett szervezet szakértőinek bevonásával javaslatot tesz a szükséges adatok összegyűjtésének és biztosításának módjára, azzal, hogy a szolgáltatást nyújtó köteles gondoskodni az adatokhoz való hozzáférés biztosításáról.
b. Kötelezettsége a vizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat tartalmazó, bitazonos másolatokat a Központ rendelkezésére bocsátani.
c. A biztonsági esemény felszámolásához szükséges intézkedéseket a Központ támogatásával ki kell dolgoznia és haladéktalanul végre kell hajtania.
d. Az esemény felszámolását követően felül kell vizsgálja az elektronikus információs rendszerei kockázatelemzésének, kockázatkezelésének teljeskörűségét, és a szükséges módosításokat végre kell hajtania.

A közvetítő szolgáltatókra[89] vonatkozó kiegészítő szabályok[90]:

85 Rendelet 16. § (1)-(2) bekezdései.
86 Rendelet 17. § (4) bekezdés.
87 Rendelet 16. § (3) bekezdés.
88 Rendelet 17. § (3) és (5) bekezdése, valamint (7)–(8) bekezdései.
89 Vö. 28–29. oldalak fogalommeghatározása.
90 Rendelet 19. § (1)–(4) bekezdések.

a. A biztonsági események kivizsgálása során a Központnak jogosultsága van szükség szerint megismerni a különböző szolgáltatás- vagy üzletmenet-folytonosságot biztosító szabályzókat, eljárásrendeket, ideértve különösen az üzletfolytonossági tervet és a katasztrófa-helyreállítási tervet.
b. A konkrét biztonsági esemény kezelése érdekében a Központ kérésére:
   ba) a biztonsági eseményben érintettek, a támadó és a támadott beazonosításához szükséges, adatait átadja,
   bb) az incidensben érintett előfizetőkkel kapcsolatban szükség szerint tiltásokat vezet be, felhasználói, illetve előfizetői hozzáféréseket korlátoz, függeszt fel vagy szüntet meg.
c. Veszélyesnek vagy károsnak ítélt szolgáltatás biztosítása esetén a Központ kötelezést adhat ki az adott szolgáltatás tiltására.

Kiegészítő szabály került megalkotásra a nyilvántartásba felvett, sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetre[91] vonatkozóan, amely szerint a gazdálkodó szervezetnek a felvételt követő minden második évben ismételten meg kell küldenie[92] az Alkotmányvédelmi Hivatal részére – a feltételek teljesülésének ismételt ellenőrzése céljából – a tevékenyég végzéséhez szükséges okiratokat[93]. A kötelezettség elmulasztása a nyilvántartásból való törlést eredményezi.

A Központ részére a Központ által saját hatáskörében indított sérülékenységvizsgálat végrehajtása érdekében, az érintett szervezetek[94] kötelesek bejelenteni a webes szolgáltatások, weboldalak és webszerverek elérhetőségére vonatkozó egyedi technikai adatokat azzal, hogy a bekövetkezett változásokat 3 napon belül be kell jelenteni. A Központ tájékoztatja az érintett szervezetet a vizsgálathoz használt IP-címről vagy más egyedi technikai azonosítóról, amelyet az érintett szervezet nem tilthat ki a webes szolgáltatás eléréséből.[95]

3. Az Ibtv. felhatalmazó rendelkezései[96] között 2019. január 1-től megjelent három új szabály, amely az alábbi rendeletek megalkotását írja elő a Kormány részére:
   a. a korai figyelmeztetés részletes szabályairól, így különösen annak rendszerét, a rendszer üzemeltetőjének kijelölését, valamint a kapcsolódó korai figyelmeztető szolgáltatás igénybevételének rendjét előíró rendelet (ennek működtetése a Központ feladat- és hatáskörébe került[97]),
   b. az Ibtv. 16. § (1) bekezdése szerinti független, képesített ellenőr igénybevételével kapcsolatos eljárásrendet tartalmazó rendelet,
   c. a honvédelmi célú elektronikus információs rendszerre vonatkozóan a korai figyelmeztetés részletes szabályait, így különösen annak rendszerét, a rendszer üzemeltetőjének kijelölését, valamint a kapcsolódó korai figyelmeztető szolgáltatás igénybevételének rendjét előíró rendelet.

(Ezen rendeletek megalkotására a kézirat lezárásáig nem került sor.)

---

91 Rendelet 22. § (5) bekezdés.
92 Rendelet 22. § (11)–(13) bekezdései.
93 Rendelet 22. § (4) és (7) bekezdései.
94 Rendelet 22. § (1) bekezdése alapján a nemzetbiztonsági védelem alá eső állami és önkormányzati szervek elektronikus információs rendszerei, az Ibtv. 2. § (1) bekezdése szerinti szervezetek létfontosságú rendszerelemmé kijelölt elektronikus információs rendszerek, valamint a zárt célú elektronikus információs rendszerek. A Katonai Nemzetbiztonsági Szolgálatot és az Információs Hivatalt a bejelentési kötelezettség saját illetékes eseménykezelő központja felé terheli.
95 Rendelet 27. § (1)–(2) bekezdése. A Katonai Nemzetbiztonsági Szolgálatot és az Információs Hivatalt a bejelentési kötelezettség saját illetékes eseménykezelő központja felé terheli.
96 Ibtv. 24. § (1) bekezdés d), l), m) pontok.
97 Rendelet 4. § c) pont.

2.4. A kritikus infrastruktúrával kapcsolatos nemzeti szabályozás

Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelv (a továbbiakban: EKI-irányelv) volt az Unió részéről az első olyan szabályozás, amely intézkedéseket tartalmazott az európai kritikus infrastruktúrák védelmére vonatkozóan és rögzítette, hogy a védelmi intézkedések kialakítása során figyelembe kell venni az ember által okozott technológiai veszélyeket, a természeti katasztrófákat és a fokozott terrorveszélyt. Az EKI-irányelv megállapította, hogy az európai kritikus infrastruktúrák védelmének felelőssége a tagállamokat és az infrastruktúrák tulajdonosait/üzemeltetőit terheli, akiknek valamennyi kijelölt kritikus infrastruktúra esetében gondoskodni kell arról, hogy rendelkezzenek üzemeltetői biztonsági tervvel, vagy ezzel egyenértékű olyan intézkedések kerüljenek bevezetésre, amelyek magukban foglalják a jelentős eszközök meghatározását, a kockázatértékelést, valamint az ellenintézkedések és -eljárások meghatározását, kiválasztását és rangsorolását. Az EKI-irányelv kimondja, hogy valamennyi kijelölt kritikus infrastruktúra tekintetében gondoskodni kell biztonsági összekötő tisztviselő kijelöléséről a kritikus infrastruktúrák védelméért felelős nemzeti hatóságokkal való együttműködés és kapcsolattartás megkönnyítése érdekében. Rögzíti továbbá, hogy a tagállamoknak az európai kritikus infrastruktúrák védelmével foglalkozó kapcsolattartó pontot kell kialakítaniuk a koordináció és a végrehajtás érdekében. Az EKI-irányelvnek való megfelelés érdekében a tagállamoknak 2011. január 12-ig kellett meghozni a szükséges intézkedéseket. Az EKI-irányelvnek való megfelelést Magyarország a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (a továbbiakban: Lrtv.), valamint a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet (a továbbiakban: Lrtv. vhr.) magalkotásával biztosította, amelyek NIS-irányelv szerinti megfeleltetésére is sor került 2018-ban. Jelen fejezet az Lrtv. és az Lrtv. vhr. 2019. január 1-től hatályos főbb rendelkezéseit rögzíti és a főbb rendelkezések tekintetében utal a kapcsolódó ágazati szabályokra is.

2.4.1. Az Lrtv. szerinti ágazatok és alágazatok

Az Lrtv., mint a nemzeti jogrendbe átültetett létfontosságú rendszerelemekre vonatkozó szabályozás, meghatározza a nemzeti és az európai létfontosságú rendszerelemmé történő kijelölés főbb eljárási lépéseit, a kijelöléssel érintett ágazatokat és alágazatokat, valamint a NIS-irányelvvel összhangban az alapvető szolgáltatásokat nyújtó szereplők kijelölésére és nyilvántartására vonatkozó rendelkezéseket.

Létfontosságú rendszerelemnek az eszköz, létesítmény vagy rendszer olyan rendszereleme tekinthető, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna és az Lrtv. mellékletében felsorolt ágazatok és alágazatok valamelyikébe tartozik[98]. A kijelölt rendszerelem üzemeltetője egyben – a NIS-irányelvvel összhangban – alapvető szolgáltatásokat nyújtó szereplőnek is minősül, ha az alágazat megfeleltethető a NIS-irányelv szerinti ágazatnak vagy alágazatnak, a szolgáltatás nyújtása elektronikus információs rendszerektől függ és a bekövetkezett biztonsági esemény jelentős zavart okozna a szolgáltatás biztosításában.[99]

[98] Lrtv 1. § f) pont.
[99] Lrtv 2/A. § (2) bekezdés.

Az Lrtv. szerinti, valamint a NIS-irányelv szerinti megfeleltetés alapján azonosított ágazatokat és alágazatokat az alábbi felsorolás tartalmazza[100]:

a. Energia ágazat és alágazatai, melyek mindegyike a NIS-irányelv szerinti megfeleltetés alapján azonosításra került, az alábbiak:
   aa) a villamosenergia-rendszer létesítményei (kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek),
   ab) a kőolajipar és
   ac) a földgázipar.
b. Közlekedési ágazat és alágazatai, melyek a logisztikai központok kivételével a NIS-irányelv szerinti megfeleltetés alapján azonosításra kerültek, az alábbiak:
   ba) a közúti közlekedés,
   bb) a vasúti közlekedés,
   bc) a légi közlekedés,
   bd) a vízi közlekedés és
   be) a logisztikai központok.
c. Agrárgazdasági ágazat alágazatai (NIS-irányelv szerinti megfeleltetésükre nem került sor):
   ca) a mezőgazdaság,
   cb) az élelmiszeripar és
   cc) az elosztó hálózatok.
d. Egészségügyi ágazat és alágazatai, melyek a laborok és a gyógyszer-nagykereskedelem kivételével a NIS-irányelv szerinti megfeleltetés alapján, mint egészségügyi ellátó létesítmények (beleértve a kórházakat és a magánklinikákat is) azonosításra kerültek, az alábbiak:
   da) az aktív fekvőbeteg-ellátás,
   db) a mentésirányítás,
   dc) az egészségügyi tartalékok és vérkészletek,
   dd) a magas biztonsági szintű biológiai laboratóriumok és
   de) a gyógyszer-nagykereskedelem.
e. Társadalombiztosítási ágazat, azon belül a társadalombiztosítási ellátások igénybevételéhez kapcsolódó informatikai rendszerek és nyilvántartások. NIS-irányelv szerinti megfeleltetésére nem került sor.
f. Pénzügyi ágazat és alágazatai, melyek a készpénzellátás kivételével a NIS-irányelv szerinti megfeleltetés alapján azonosításra kerültek, az alábbiak:
   fa) a pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei (NIS-irányelv szerint pénzügyi piaci infrastruktúrák),
   fb) a bank- és hitelintézeti biztonság (NIS-irányelv szerint banki szolgáltatások) és
   fc) a készpénzellátás.
g. Infokommunikációs technológiák ágazata és alágazatai, melyek közül egy került a NIS-irányelv szerinti megfeleltetés alapján azonosításra, az alábbiak:
   ga) az internet-infrastruktúra és internet hozzáférés szolgáltatás (NIS-irányelv szerint digitális infrastruktúra),
   gb) a vezetékes és vezeték nélküli elektronikus hírközlési szolgáltatások, vezetékes és vezeték nélküli hírközlő hálózatok,
   gc) a rádiós távközlés,
   gd) az űrtávközlés,
   ge) a műsorszórás,
   gf) a postai szolgáltatások és
   gg) a kormányzati elektronikus információs rendszerek.

[100] Lrtv 1. § f) pont és az Lrtv. 1–4. mellékletei.

h. Víz ágazata és alágazatai, melyek közül egy került a NIS-irányelv szerinti megfeleltetés alapján azonosításra, az alábbiak:
   ha) az ivóvíz-szolgáltatás (NIS-irányelv szerint ivóvízellátás és -elosztás),
   hb) a felszíni és felszín alatti vizek minőségének ellenőrzése,
   hc) a szennyvízelvezetés és -tisztítás,
   hd) a vízbázisok védelme és
   he) az árvízi védművek és gátak.
i. A közbiztonság és védelem ágazata, azon belül a rendvédelmi szervek infrastruktúrái (NIS-irányelv szerinti megfeleltetésükre nem került sor).
j. A honvédelem ágazata, azon belül a honvédelmi rendszerek és létesítmények (NIS-irányelv szerinti megfeleltetésükre nem került sor).

2.4.2. A javaslattevő és a kijelölő hatóságok

A létfontosságú rendszerelem kijelölésére vonatkozó eljárás során javaslattevő hatóságként jár el:

a. a BM OKF, a közrend, a közbiztonság, a lakosságvédelem, az alkotmányvédelem, a nemzetbiztonság és a terrorelhárítás szempontjai esetében[101],
b. a BM OKF, a Büntetés-végrehajtás Országos Parancsnoksága, az Országos Rendőrfőkapitányság azon rendvédelmi rendszer, létesítmény vonatkozásában, melynek üzemeltetőjét irányítja, felügyeli[102],
c. az élelmiszerlánc-biztonsági és állategészségügyi hatósági hatáskörében, illetve a növény- és talajvédelmi hatósági hatáskörében eljáró megyei kormányhivatal az agrárgazdasági ágazat tekintetében[103],
d. az ivóvíz-szolgáltatás, a szennyvízelvezetés és -tisztítás, valamint az árvízvédelmi létesítmény vonatkozásában a területi vízügyi igazgatóság a víz ágazat tekintetében[104],
e. az egészségügyi ágazatot érintően
   ea) az aktív fekvőbeteg-ellátás esetében az Állami Egészségügyi Ellátó Központ,
   eb) a mentésirányítás esetében az Országos Mentőszolgálat,
   ec) az egészségügyi tartalékok vonatkozásában az Állami Egészségügyi Ellátó Központ,
   ed) a vérkészletek vonatkozásában az Országos Vérellátó Szolgálat,
   ee) a magas biztonsági szintű biológiai laboratóriumok esetében az országos tisztifőorvos,
   ef) a gyógyszer-nagykereskedelem esetében az Országos Gyógyszerészeti és Élelmezés-egészségügyi Intézet[105],
f. a pénzügyi közvetítőrendszer felügyeletével kapcsolatos feladatkörében eljáró Magyar Nemzeti Bank a pénzügyi ágazat tekintetében[106],

---

101 Lrtv. vhr. 3. §.

102 Az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról szóló 512/2013. (XII. 29.) Korm. rendelet (a továbbiakban: Rendvédelmi vhr.) 1. § (3) bekezdés.

103 A létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 540/2013. (XII. 30.) Korm. rendelet (a továbbiakban: Agrár vhr.) 1. § (1) bekezdés.

104 A létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről szóló 541/2013. (XII. 30.) Korm. rendelet (a továbbiakban: Víz vhr.) 1. § (1) bekezdése.

105 Az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendelet (a továbbiakban: Eü. vhr.) 2. §-a.

106 A pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 330/2015. (XI. 10.) Korm. rendelet (a továbbiakban: Pénzügy vhr.) 2. §-a.

g. a Honvédelmi Minisztérium a honvédelmi ágazat tekintetében[107],
h. a postai szolgáltatások tekintetében a postaügyért felelős miniszter[108].

A létfontosságú rendszerelem kijelölésére vonatkozó eljárás során ágazati kijelölő hatósági feladatokat lát el:

a. Az energia ágazat vonatkozásában[109]:
   aa) a villamosenergia-rendszer tekintetében a Magyar Energetikai és Közműszabályozási Hivatal,
   ab) a kőolaj-feldolgozás és kőolajtermék-tárolás kivételével a kőolajipar és a földgázipar tekintetében a bányafelügyelet,
   ac) a kőolaj-feldolgozás és kőolajtermék-tárolás tekintetében első fokon a fővárosi és megyei kormányhivatal mérésügyi feladatkörében eljáró megyeszékhely szerinti járási (fővárosi kerületi) hivatala.
b. A rendvédelmi ágazat vonatkozásában[110]:
   ba) az Alkotmányvédelmi Hivatal, a Nemzetbiztonsági Szakszolgálat, a Terrorelhárítási Információs és Bűnügyi Elemző Központ, a Büntetés-végrehajtás Országos Parancsnoksága és szervei, a Nemzeti Védelmi Szolgálat, az Országos Rendőrfőkapitányság és szervei, valamint a Terrorelhárítási Központ vonatkozásában a BM OKF üzemeltető telephelye szerinti területi szerve,
   bb) a BM OKF és szervei vonatkozásában az általános rendőrségi feladatok ellátására létrehozott szervnek az üzemeltető telephelye szerinti területi szerve.
c. Az agrárgazdasági ágazat tekintetében a Nemzeti Élelmiszerlánc-biztonsági Hivatal[111].
d. A víz ágazat tekintetében a közcélú ivóvíz-szolgáltatást biztosító vízilétesítmény – ideértve a vonatkozó ivóvíz célú kitermelésre szánt felszíni és felszín alatti vizek minőségének ellenőrzését biztosító vízilétesítményt és a vonatkozó ivóvízbázis-védelmet biztosító vízilétesítményt –, valamint a szennyvízelvezetést és -tisztítást szolgáló vízilétesítmény és árvízvédelmi létesítmény tekintetében az illetékes vízügyi hatóság[112].
e. Az egészségügyi ágazat vonatkozásában az egészségügyért felelős miniszter, akit feladatainak ellátásában döntés-előkészítő bizottság segít[113].
f. A pénzügyi ágazat tekintetében a pénz-, tőke- és biztosítási piac szabályozásáért felelős miniszter, akit feladatainak ellátásában döntés-előkészítő bizottság segít[114].
g. A honvédelmi ágazat tekintetében a Honvédelmi Minisztérium[115].
h. Az infokommunikációs technológiák vonatkozásában a Nemzeti Média- és Hírközlési Hatóság Hivatala, amelyet feladatellátásában döntés-előkészítő bizottság segít [116], kivéve a kormányzati informatikai, elektronikus hálózatokat, ahol a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszter[117].

---

107 A honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről szóló 359/2015. (XII. 2.) Korm. rendelet (a továbbiakban: Honvédelmi vhr.) 3. §-a.

108 Az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 249/2017. (IX. 5.) Korm. rendelet (a továbbiakban: Infokom. vhr.) 5. § (1) bekezdés.

109 Az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 360/2013. (X. 11.) Korm. rendelet (a továbbiakban: Energia vhr.) 2. §-a.

110 Rendvédelmi vhr. 1. § (1) bekezdés.

111 Agrár vhr. 1. § (2) bekezdés.

112 Víz vhr. 1. § (2) bekezdés.

113 Eü. vhr. 3. §.

114 Pénzügy vhr. 3. §.

115 Honvédelmi vhr. 3. § (1) bekezdés.

116 Infokom. vhr. 3. § (1) bekezdés és (4) bekezdés.

117 Infokom. vhr. 6. § (1) bekezdés.

2.4.3. Az Lrtv. szerinti azonosítási eljárás

A létfontosságú rendszerelem kijelölését megelőzi az üzemeltető által elvégzett azonosítás[118] folyamata, amely során a lehetséges létfontosságú rendszerelemeket kockázatelemzés[119], valamint az ágazati és horizontális kritériumok alapján határozzák meg. Üzemeltetőnek az a természetes, jogi személy vagy jogi személyiség nélküli szervezet minősül, aki vagy amely az eszköz, létesítmény, rendszer rendszerelemének tulajdonosa, engedélyese, rendelkezésre jogosultja vagy napi működéséért felelős[120].

Az azonosítási eljárás eredményéről az üzemeltető azonosítási jelentést készít, amely tartalmazza[121]:

a. a vizsgált lehetséges létfontosságú rendszerelem megnevezését,
b. az azonosítási eljárás kezdő- és zárónapját,
c. a kockázatelemzést és annak eredményét,
d. a nemzeti vagy európai létfontosságú rendszerelemmé történő kijelölésre irányuló javaslatot vagy a kijelölés visszavonására, vagy a kijelölés fenntartására vonatkozó javaslatot,
e. az alapvető szolgáltatást nyújtó szereplőnek történő megfeleltetés esetén a szolgáltató minősítésére vonatkozó elemzést,
f. az üzemeltetőnek az azonosítási jelentés teljességére vonatkozó nyilatkozatát.

Az azonosítási jelentést első alkalommal az adott ágazatra vonatkozó ágazati kritériumokat megállapító jogszabály hatálybalépését[122] követő 180 napon belül kell az üzemeltetőnek elkészítenie és benyújtania az ágazati kijelölő hatóságnak[123]. Ha az üzemeltető határidőn belül kötelezettségét nem teljesíti, az ágazati kijelölő hatóság határidő tűzésével felszólítja az azonosítási jelentés elkészítésére és benyújtására. Ha a felszólítás eredményeképpen az üzemeltető egyetlen rendszerelemet sem azonosított lehetséges létfontosságú rendszerelemként, ebben az esetben is be kell nyújtani az azonosítási jelentést[124]. Az ágazati kijelölő hatóság az azonosítási jelentést véleményezés céljából megküldi a javaslattevő hatóságnak, aki a jelentés beérkezésétől számított 30 napon belül megvizsgálja az azonosítási jelentést és a kockázatelemzéssel kapcsolatos javaslatait megküldi az ágazati kijelölő hatóságnak[125].

Az üzemeltető további kötelezettsége, hogy minden olyan a tevékenységében bekövetkezett változásról, amely érinti a létfontosságú rendszerelem azonosítását, 8 napon belül írásban értesítse az ágazati kijelölő hatóságot, illetve a kijelölésre vonatkozó döntés véglegessé válásától számított 5 év elteltével új azonosítási jelentést kell készítenie.[126]

További részletszabályokat az ágazati végrehajtási rendeletek tartalmaznak (vö. *4.11. Ágazati szabályok* alcím).

---

118 A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet (a továbbiakban: Lrtv. vhr.) 1. § 1) pont.

119 Kockázatelemzés: fenyegetettségi és kockázati tényezők vizsgálata a rendszerelemek sebezhetőségének, valamint a megzavarásuk vagy megsemmisítésük által okozott következmények értékelése céljából. – Lrtv. vhr. 1. § 2) pont.

120 Lrtv. 1. § h) pont.

121 Lrtv. vhr. 2. § (1)–(2) bekezdései.

122 Az Lrtv. felhatalmazó rendelkezése alapján minden ágazatnak önálló kormányrendeletet kellett készítenie végrehajtás céljából.

123 Lrtv. vhr. 15. §.

124 Lrtv. vhr. 2. § (3)–(4) bekezdései.

125 Lrtv. vhr. 2. § (5) bekezdése.

126 Lrtv. vhr. 2. § (7)–(8) bekezdései.

2.4.4. Az Lrtv. szerinti kijelölési eljárás

Az Lrtv. szerint nemzeti létfontosságú rendszerelem[127] a kijelölési eljárás során kijelölt olyan létfontosságú rendszerelem, amelynek kiesése, a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt, jelentős hatással lenne Magyarországon. Európai létfontosságú rendszerelem[128] a kijelölési eljárás során kijelölt olyan létfontosságú rendszerelem, amelynek kiesése jelentős hatással lenne – az ágazatokon átnyúló kölcsönös függőségből következő hatásokat is ideértve – legalább két EGT-államra.

Az Lrtv. vhr. szerint létfontosságú információs rendszernek és létesítménynek minősülnek a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek.[129]

Ahhoz, hogy a fentiekben felsorolt valamely ágazat alágazatába tartozó eszköz, létesítmény vagy rendszer rendszereleme nemzeti létfontosságú rendszerelemként kerüljön kijelölésre vagy a NIS-irányelv szerinti megfeleltetés esetén alapvető szolgáltatást nyújtó szereplőkként kerüljön azonosításra, az ún. ágazati kijelölő hatóságnak kijelölési eljárást kell lefolytatnia[130].

Az ágazati kijelölő hatóság eljárását hivatalból folytatja le, az üzemeltető[131] által elkészített azonosítási jelentés benyújtását követően, az ún. javaslattevő hatóság javaslata alapján, szakhatóság bevonásával, amely során előzetes szakhatósági állásfoglalásnak nincs helye[132].

Az eljárás során az ágazati kijelölő hatóság, az ágazati és horizontális kritériumok alapján, az azonosítási jelentés kézhezvételétől számított 70 napon belül[133]:

a. határozatban dönt a nemzeti létfontosságú rendszerelemmé történő kijelöléséről és egyidejűleg rendelkezik az üzemeltető felvételéről az alapvető szolgáltatásokat nyújtó szereplők jegyzékébe[134] vagy dönt a kijelölés visszavonásáról és ezzel egyidejűleg rendelkezik az üzemeltető törléséről az alapvető szolgáltatásokat nyújtó szereplők jegyzékéből[135],
b. meghatározza az üzemeltetői biztonsági terv kidolgozásának határidejét, valamint
c. a létfontosságú rendszerelem védelmével[136] összefüggő, a rendszerelem egyedi sajátosságaihoz, környezetéhez, a rendszerelem által potenciálisan előidézhető veszély mértékéhez igazodó feltételeket írhat elő az üzemeltető részére.

Az ágazati kijelölő hatóság határozatában:

a. jóváhagyja az üzemeltető azonosítási jelentését és a rendszerelemet a hatósági nyilvántartásba történő felvétel elrendelése mellett nemzeti létfontosságú rendszerelemnek jelöli ki, feltéve, hogy az ágazati kritériumok közül és a szakhatóság állásfoglalása

127 Lrtv 1. § g) pont.
128 Lrtv 1. § c) pont.
129 Lrtv 1. § 3 pont.
130 Lrtv 2. § (1) bekezdés és 2/A. § (1) bekezdése.
131 Lrtv. 1. § h) pont, üzemeltető: az a természetes, jogi személy vagy jogi személyiség nélküli szervezet, aki vagy amely az eszköz, létesítmény, rendszer rendszerelemének tulajdonosa, engedélyese, rendelkezésre jogosultja vagy napi működéséért felelős.
132 Lrtv 2. § (1) bekezdés, Lrtv. vhr. 4. § (1) és (2) bekezdés.
133 Lrtv 2. § (3)–(4) bekezdései, Lrtv. vhr. 4. § (1) bekezdés.
134 Lrtv. 2/A. § (3) bekezdése.
135 Lrtv. 2/A. § (5) bekezdése.
136 Lrtv. 1. § e) pont, létfontosságú rendszerelem védelme: a létfontosságú rendszerelem funkciójának, folyamatos működésének és sértetlenségének biztosítását célzó, a fenyegetettség, a kockázat, a sebezhetőség enyhítésére vagy semlegesítésére irányuló valamennyi tevékenység.

vagy a kijelölő hatóság döntése[137] alapján a horizontális kritériumok közül legalább egy-egy bekövetkezésének lehetősége fennáll,
b. jóváhagyja az üzemeltető azonosítási jelentését és a kijelölést visszavonja, valamint elrendeli a nyilvántartásból való törlést,
c. a kijelölésre, kijelölés visszavonására irányuló javaslatot elutasítja vagy legfeljebb 90 napos határidő tűzésével és a feltárt hibák, hiányosságok tételes megjelölésével új azonosítási jelentés benyújtását írja elő,
d. jóváhagyja, hogy az üzemeltető egyetlen rendszerelemet sem azonosított lehetséges létfontosságú rendszerelemként,
e. rendelkezik az üzemeltető felvételére vagy törlésére az alapvető szolgáltatásokat nyújtó szereplők jegyzékéből.[138]

A nemzeti létfontosságú rendszerelemmé történő kijelölés visszavonásáról az ágazati kijelölő hatóság a javaslatevő hatóság vagy az üzemeltető kérelmére – szakhatóság bevonásával, előzetes állásfoglalás mellőzésével – dönthet[139], amely döntés alapján a nyilvántartó hatóság törli az alapvető szolgáltatásokat nyújtó szereplők jegyzékéből az üzemeltetőt[140].

Európai létfontosságú rendszerelemmé történő kijelölési eljárást az ágazati kijelölő hatóság hivatalból folytatja le[141]:

a. az üzemeltető által lefolytatott azonosítási eljárás alapján elkészített azonosítási jelentés benyújtását követően,
b. EGT-állam kezdeményezése alapján vagy
c. a javaslattevő hatóság ágazati kijelölő hatóságnál tett kezdeményezése alapján.

A kezdeményezést és az üzemeltető által benyújtott azonosítási jelentést az ágazati kijelölő hatóság – c) pont kivételével – a javaslattevő hatóság bevonásával megvizsgálja és a szakmai álláspontjáról az ágazatért felelős miniszter útján a Belügyminisztert mint a katasztrófák elleni védekezésért felelős minisztert (a továbbiakban: Belügyminiszter) tájékoztatja. A Belügyminiszter az adott ágazat szerinti feladat- és hatáskörrel rendelkező miniszterrel együtt kezdeményezi az európai létfontosságú rendszerelemmé nyilvánítással kapcsolatos nemzetközi szerződés megkötését. A nemzetközi szerződés hatálybalépésétől számított 30 napon belül az ágazati kijelölő hatóság a kijelölésről határozatot hoz, amelyben meghatározza az üzemeltető kötelezettségeit, azok végrehajtásának határidejét és ellenőrzését.[142]

Ha a Belügyminiszter nem ért egyet:

a. az azonosítási jelentésben foglaltakkal vagy a javaslattevő hatóság európai létfontosságú rendszerelemmé történő kijelölésre irányuló kezdeményezésével, a kijelölő hatóság köteles megvizsgálni a nemzeti létfontosságú rendszerelemmé történő kijelölés kérdését és a feltételek fennállása esetén döntenie kell a nemzeti létfontosságú rendszerelemmé történő kijelölésről,
b. az Európai Gazdasági Térségről szóló megállapodásban részes más állam európai létfontosságú rendszerelemmé történő kijelölésre irányuló kezdeményezésével, erről tájékoztatja a kezdeményező államot[143].

[137] Ha kijelölő hatóságként a BM OKF központi, területi vagy helyi szerve jár el, a horizontális kritériumok teljesülése fennállásának a kérdését a hatósági eljárás során a kijelölő hatóság vizsgálja. – Lrtv. vhr. 4. § (1) bekezdés.
[138] Lrtv. vhr. 4. § (3) bekezdés.
[139] Lrtv 2. § (2) bekezdés, Lrtv. vhr. 4. § (2) bekezdés.
[140] Lrtv. 2/A. § (5) bekezdése.
[141] Lrtv 3. § (1) bekezdés.
[142] Lrtv 3. § (2)–(4) bekezdései.
[143] Lrtv. vhr. 5. § (1)-(2) bekezdései.

Európai létfontosságú rendszerelemmé történő kijelölés visszavonásáról az ágazati kijelölő hatóság hivatalból, EGT-állam kezdeményezése alapján hivatalból vagy az üzemeltető kérelmére dönthet[144]. Ha a Belügyminiszteregyet ért az EGT-állam kezdeményezésével, illetve az üzemeltető kérelmével, az adott ágazat szerinti feladat- és hatáskörrel rendelkező miniszterrel együtt kezdeményezi az európai létfontosságú rendszerelemmé nyilvánítással kapcsolatos nemzetközi szerződés felbontását. Ez esetben a nemzetközi szerződés felbontását követően az ágazati kijelölő hatóság a kijelölésről határozatot hoz és a kijelölést visszavonja, valamint a feltételek fennállása esetén dönt a nemzeti létfontosságú rendszerelemmé történő kijelölésről. Ha a Belügyminiszter az üzemeltető kijelölés visszavonására vonatkozó kérelmével nem ért egyet, a kijelölő hatóság tájékoztatja az üzemeltetőt a kijelölés fenntartásáról. Ha a visszavonást EGT-állam kezdeményezi, a fenti szabályok alkalmazásával kezdeményezi a kijelölés fenntartását. [145]

Ha az európai létfontosságú rendszerelemmé történő kijelölés vagy a kijelölés visszavonása kérdésében az ágazatért felelős miniszter és a Belügyminiszter ellentétes álláspontot képvisel, a végleges álláspontról a Kormány dönt. [146]

A kijelölési, valamint a kijelölés visszavonására vonatkozó eljárásban kétszeri hiánypótlásra történő felszólításnak van helye[147].

Az ágazati kijelölő hatóság a kijelölésre és a kijelölés visszavonására vonatkozó, véglegessé vált határozatát haladéktalanul köteles megküldeni a BM OKF-nek mint nyilvántartó hatóságnak. A kijelölés visszavonására vagy elutasítására vonatkozó véglegessé vált határozatát pedig a kijelölési eljárásban érintett valamennyi hatóságnak meg kell küldenie[148].

Az ágazati kijelölő hatóság által lefolytatott kijelölési és kijelölés visszavonására vonatkozó hatósági eljárásban a hatóságok és a szakhatóságok részéről csak olyan személy vehet részt, akinek a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott nemzetbiztonsági ellenőrzését elvégezték és akivel szemben kockázati tényező nem merült fel. Ugyanez a szabály érvényes az európai létfontosságú rendszerelemekre vonatkozó azonosítási eljárás lefolytatása során az üzemeltető által igénybe vett közreműködő szervezet részéről igénybe vett személy esetén is[149].

A BM OKF központi, területi vagy helyi szerve ágazati kijelölő hatósági, illetve szakhatósági eljárásában:

a. a pénz- és adóügyi biztonság vonatkozásában a Nemzeti Adó- és Vámhivatal területi, illetve központi szervétől,
b. a közrend, a közbiztonság, a lakosságvédelem, az alkotmányvédelem, a nemzetbiztonság, a terrorelhárítás vonatkozásában az általános rendőrségi feladatok ellátására létrehozott szerv területi, illetve központi szervétől, az Alkotmányvédelmi Hivatal területi, illetve központi szervétől, valamint a Terrorelhárítási Központtól véleményt kérhet.

144 Lrtv 3. § (1a) bekezdés.
145 Lrtv. vhr. 5. § (3)–(4) bekezdései.
146 Lrtv. vhr. 5. § (6) bekezdése.
147 Lrtv. vhr. 4. § (6) és (9) bekezdése.
148 Lrtv 5. § (3) és (6) bekezdései.
149 Lrtv 4. § (1) bekezdése.

Ezek a szervek ellenőrzési tevékenységük során a kijelölés alapjául szolgáló körülmények változatlan fennállásán kívül vizsgálják:

a. a létfontosságú rendszerelemek,
b. a létfontosságú rendszerelemekhez tartozó közterületek, valamint
c. a létfontosságú rendszerelemeket felügyelő, működtető személyek

azon fizikai, humán és informatikai biztonsági feltételeinek meglétét, amelyek garantálják az azonosított kockázatokkal szembeni védelmet, a rendeltetésszerű működést, a szándékos és nem szándékos károkozás elkerülését[150].

További részletszabályokat az ágazati végrehajtási rendeletek tartalmaznak (vö. *4.11. Ágazati szabályok* alcím).

2.4.5. Horizontális és ágazati kritériumok

Az Lrtv. szerint horizontális kritériumnak[151] minősülnek azok a szempontok, az azokhoz tartozó küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek egy eszköz, létesítmény rendszerelemének kiesése által kiváltott hatásra vonatkoznak és amelyek teljesülése esetén – figyelemmel a bekövetkező emberiélet-veszteségekre, az egészségre gyakorolt hatásra, a gazdasági és társadalmi hatásokra, a természetre és az épített környezetre gyakorolt hatásra – az eszköz, létesítmény, rendszer vagy azok része létfontosságú rendszerelemmé jelölhető ki attól függetlenül, hogy mely ágazatba tartozik.

Az Lrtv. vhr. 1. melléklete szerint horizontális kritériumnak minősül egyetlen vagy egymással közvetlenül összefüggő eseményekkel kapcsolatban Magyarország területén:

1. A veszteségek kritériuma:
   a. 24 óra leforgása alatt az áldozatok száma a 20 főt meghaladja vagy a súlyos sérültek száma legalább 75 fő, vagy
   b. 72 óra leforgása alatt az áldozatok száma a 40 főt meghaladja vagy a súlyos sérültek száma legalább 150 fő.
2. A gazdasági hatás kritériuma: a gazdasági veszteség mértéke vagy termékek és szolgáltatások romlásának mértéke, a rendszer és létesítmény fizikai sérüléséből, elvesztéséből fakadó közvetlen vagy közvetett károk, amelyek ötvenezer fő vonatkozásában meghaladják az egy főre eső bruttó nemzeti jövedelem bármely 30 napos időszakra vetített mértékének 25%-át.
3. A társadalmi hatás kritériuma: 300 fő/km^2-nél sűrűbben lakott területen a köznyugalom súlyos megzavarása, beleértve a lakosságot érő káros pszichológiai és közegészségügyi hatásokat is.
4. A politikai hatás kritériuma: az állam és intézményei iránti közbizalom megszűnése, valamely állami szerv működésképtelenné válása miatt a lakosság biztonságérzete kritikus szint alá csökken.
5. A környezeti hatás kritériuma: az esemény vagy folyamat, amely miatt a természeti vagy épített környezetben, különösen:
   a. az infrastruktúrában bekövetkező sérülés vagy zavar, az épített vagy természetes környezet oly mértékű rongálódását idézi elő, amelynek következtében:
      aa) 10 000 fő kimenekítése vagy kitelepítése válik szükségessé, vagy
      ab) legalább 100 km^2 nagyságú terület tartósan szennyeződik, vagy
      ac) a felszín alatti vizek vagy azok természetes víztartó képződményei, a folyóvizek és természetes tavak, valamint ezek medre vagy élővilága szenved tartós károsodást,
      ad) az ország tájegységeiben, kiemelkedő földrajzi területeiben visszafordíthatatlan negatív változás következik be.

[150] Lrtv. vhr. 11. § (1) és (3) bekezdés.
[151] Lrtv. 1. § d) pont.

A horizontális kritériumok értékeléséhez a BM OKF központi, területi vagy helyi szerve véleményt kérhet:

a. a politikai hatás kritériuma teljesülésének lehetősége tekintetében az illetékes kormánymegbízottól,
b. a környezeti hatás kérdésében a területi környezetvédelmi hatóságtól, a területi vízügyi és vízvédelmi hatóságtól, valamint az országos természetvédelmi és környezetvédelmi hatóságtól[152].

Ágazati kritériumnak[153]minősülnek azok a szempontok, az azokhoz tartozó küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek egy eszköz, létesítmény rendszerelemének megzavarása vagy megsemmisítése (a továbbiakban együtt: kiesés) által kiváltott hatásra vonatkoznak és amelyek teljesülése esetén az eszköz, létesítmény, rendszer vagy azok része létfontosságú rendszerelemmé jelölhető ki azzal szoros összefüggésben, hogy mely ágazatba tartozik.

Az Lrtv. hatálya alá tartozó alágazatok ágazati kritériumait a végrehajtási rendeletek tartalmazzák, amelyek részletes ismertetése nem célja jelen tananyagnak. Az egyes szabályzók és az ágazati kritériumokat felsoroló jogszabályi rendelkezések az alábbiak:

a. az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 360/2013. (X. 11.) Korm. rendelet (a továbbiakban: Energia vhr.) 3–4. §-ai,
b. az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról szóló 512/2013. (XII. 29.) Korm. rendelet (a továbbiakban: Rendvédelmi vhr.) 2. §-a,
c. a létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 540/2013. (XII. 30.) Korm. rendelet (a továbbiakban: Agrár vhr.) 2–4. §-ai,
d. a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről szóló 541/2013. (XII. 30.) Korm. rendelet (a továbbiakban: Víz vhr.) 2. és 4. §-ai,
e. az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendelet (a továbbiakban: Eü. vhr.) 4–11. §-ai,
f. a pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 330/2015. (XI. 10.) Korm. rendelet (a továbbiakban: Pénzügy vhr.) 6–7. §-ai,
g. a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről szóló 359/2015. (XII. 2.) Korm. rendelet (a továbbiakban: Honvédelmi vhr.) 2. §-a,
h. az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 249/2017. (IX. 5.) Korm. rendelet (a továbbiakban: Infokom. vhr.) 9–14. §-ai.

[152] Lrtv. vhr. 11. § (2) bekezdés.
[153] Lrtv. 1. § a) pont.

2.4.6. Hatósági feladatok

1. Az Lrtv. szerinti nyilvántartó hatósági feladatokat – kivéve a honvédelmi létfontosságú rendszerelemeket – a BM OKF[154] látja el, amely feladat- és hatáskörében eljárva nyilvántartja és kezeli[155]:
    a. az üzemeltető nevét, székhelyét vagy lakcímét, levelezési címét, cégjegyzékszámát vagy az egyéni vállalkozói nyilvántartási számát, statisztikai számjelét és adóazonosító számát, képviselőjének nevét, telefon- és telefaxszámát, e-mail-címét,
    b. a biztonsági összekötő személy természetes személyazonosító adatait, telefon- és telefaxszámát, e-mail-címét, szakirányú végzettségét, a végzettséget igazoló okirat sorszámát,
    c. a nemzeti létfontosságú rendszerelemek és azon európai létfontosságú rendszerelemek megnevezését, amelyek esetében Magyarország érintett fél,
    d. az üzemeltetői biztonsági tervet,
    e. az ágazati kijelölő hatóságnak az európai létfontosságú rendszerelem vagy a nemzeti létfontosságú rendszerelem kijelöléséről és a kijelölés visszavonásáról szóló határozatát.

Ezen adatkezelés célja az azonosítási és a kijelölési eljárás, a kijelölés visszavonására vonatkozó eljárás lefolytatásának biztosítása, valamint a hatósági ellenőrzés biztosítása érdekében a létfontosságú rendszerelemek védelmével kapcsolatos kötelezettségek teljesítésének és a kijelölési eljárás során hozott határozatban előírt feltételeknek való megfelelésnek a vizsgálata. A nyilvántartásból – ideértve a javaslattevő, az ágazati kijelölő hatóság és a szakhatóság hatósági nyilvántartásait is – az adatokat az üzemeltető írásbeli értesítése mellett törölni kell[156]:

a. az ágazati kijelölő hatóságnak a kijelölés visszavonásáról szóló határozat véglegessé válása után egy évvel vagy
b. a kijelölést elutasító határozat véglegessé válásakor.

Fentiekben felsorolt alapadatokat tartalmazó hatósági nyilvántartásból az adatkezelési céllal összefüggésben a BM OKF adattovábbítást – az érintett szervek írásbeli, az adatigénylési cél meghatározásával és az átvenni kívánt adatok körének pontos megjelölésével ellátott kérelme alapján[157] – az alábbiak figyelembevételével végezhet[158]:

a. az azonosítási eljárásban, a kijelölési eljárásban, a kijelölés visszavonására vonatkozó eljárásban részt vevő javaslattevő hatóság, ágazati kijelölő hatóság, szakhatóságok részére az eljárások lefolytatásának biztosítása céljából,
b. a kijelölt létfontosságú rendszerelem ellenőrzését koordináló szerv részére a koordinációs feladatok biztosítása céljából,
c. a kijelölt létfontosságú rendszerelem helyszíni ellenőrzését lefolytató szerv részére a helyszíni ellenőrzés lefolytatása céljából,
d. a kijelölt létfontosságú rendszerelem hatósági ellenőrzésére jogszabály alapján feladat- és hatáskörrel rendelkező hatóságok részére a hatósági ellenőrzések lefolytatása céljából,
e. rendkívüli esemény bekövetkezése esetén az eseménykezelésben és a helyreállításban részt vevő szervek tevékenységének támogatása céljából,
f. a BM OKF területi és helyi szervei részére hatósági, megelőzési, kapcsolattartási és tájékoztatási feladatai elvégzése, illetve rendkívüli esemény kezelése céljából,

[154] Lrtv. vhr. 10. § (1) bekezdés.
[155] Lrtv. 5. § (1) és (2) bekezdései.
[156] Lrtv. 5. § (5) bekezdés.
[157] Lrtv. vhr. 10. § (3) bekezdés.
[158] Lrtv. 5. § (4) bekezdés.

g. a Katonai Nemzetbiztonsági Szolgálat, a Központ, az egyedüli kapcsolattartó pont, valamint az Ibtv. szerinti eseménykezelő központok – kivéve az Információs Hivatal illetékes eseménykezelő központját – részére feladataik ellátása céljából.

A BM OKF-nek a szabályszerű adatszolgáltatást 15 napon belül teljesíteni kell.

Fenti nyilvántartási tevékenység végzése mellett az alapvető szolgáltatásokat nyújtó szereplők jegyzékét is a BM OKF, mint nyilvántartó hatóság vezeti[159].

A BM OKF – ideértve a helyszíni ellenőrzést lefolytató szervet is – az ellenőrzési tevékenysége során a biztonsági összekötő büntetlen előéletre vonatkozóan megismert személyes adatait – ha a hatósági ellenőrzése során azt állapítja meg, hogy a biztonsági összekötő e követelményének nem felel meg – további eljárás lefolytatása céljából átadja az ágazati kijelölő hatóságnak. A büntetlen előéletre vonatkozó személyes adatot:

a. a helyszíni ellenőrzést lefolytató szerv a helyszíni ellenőrzés, valamint az ágazati kijelölő hatóságnak történő adattovábbítás időtartamára,
b. a BM OKF a hatósági ellenőrzés, valamint az ágazati kijelölő hatóságnak történő adattovábbítás időtartamára,
c. az ágazati kijelölő hatóság a hiánypótlásra vonatkozó hatósági ellenőrzés időtartamára, valamint ezen határozat véglegessé válásáig

kezeli.[160]

Az üzemeltetői biztonsági tervben meghatározott rendkívüli esemény bekövetkezésekor a BM OKF[161]:

a. jogosult a hatáskörükben érintett hatóságoktól a beavatkozáshoz és elhárításához szükséges adatokat beszerezni, amely adatszolgáltatást soron kívül kötelesek részére az érintettek teljesíteni;
b. koordinálásával történik:
   ba) a rendkívüli eseményre való reagálás,
   bb) a mentés megszervezése és irányítása,
   bc) a lakosság tájékoztatása,
   bd) a károk felmérése,
   be) az eredeti állapot lehetőség szerinti visszaállítása.

Az üzemeltetői biztonsági tervben meghatározott rendkívüli esemény bekövetkezésekor[162] az érintett ágazati kijelölő hatóság feladata javaslatot tenni a szükséges erők, eszközök bevonására.

[159] Lrtv. 2/A. § (4) bekezdése.
[160] Lrtv. 8. § (8)–(9) bekezdései.
[161] Lrtv. vhr. 11 § (6) bekezdés.
[162] Lrtv. vhr. 11 § (6) bekezdés.

2.4.7. Ellenőrzési feladatok

1. Az Lrtv. szerint a BM OKF a kijelölt létfontosságú rendszerelemek hatósági ellenőrzése során mint kijelölt ellenőrzést koordináló szerv jár el[163], kivéve a honvédelmi létfontosságú rendszerelemeket. Ennek keretében a jogszabály alapján feladat- és hatáskörrel rendelkező hatóságok részére hatósági ellenőrzés lefolytatására vonatkozó javaslatot tesz, több társhatóság bevonásával együttes hatósági ellenőrzéseket szervez. Koordinációs feladatkörében eljárva – a NIS-irányelvvel összhangban – ellátja a létfontosságú rendszerelemek védelmével kapcsolatos hálózatbiztonsági intézkedések koordinációját, a hálózatbiztonság fenntartásának elősegítését, a hálózatbiztonsággal kapcsolatos események elemzését és értékelését is.[164]

A BM OKF-nek feladatellátásával összefüggésben[165]:

a. éves ellenőrzési tervet kell összeállítania a tárgyévet megelőző év november 30-ig, figyelemmel arra, hogy minden létfontosságú rendszerelemnek legalább 5 évente el kell végezni az ellenőrzését,
b. az ellenőrzési terv végrehajtásáról összefoglaló jelentést kell készítenie a tárgyévet követő év március 1-ig,
c. az ellenőrzések lefolytatása során az ellenőrzésben részt vevő szervektől eljárásaik kimeneteléről, a megállapított hiányosságok pótlásáról tájékoztatást kérhet, melyet a szervek haladéktalanul kötelesek teljesíteni.

Az éves ellenőrzési terv elkészítése érdekében az érintett hatóságok minden évben legkésőbb a tárgyévet megelőző év október 15. napjáig kötelesek megküldeni a BM OKF részére az ellenőrzési terv elkészítéséhez szükséges javaslataikat, melyeket a saját ellenőrzési rendszerükben is felhasználnak[166].

A BM OKF ellenőrzi[167]:

a. az általa, mint nyilvántartó hatóság által, nyilvántartott és kezelt adatok valódiságát,
b. az üzemeltetői biztonsági tervben foglalt, a létfontosságú rendszerelem teljes körű személyi, fizikai, adminisztratív védelmének, a folyamatos működést veszélyeztető kockázatoknak és kezelésüknek a teljeskörűségét.

Honvédelmi létfontosságú rendszerelemek esetén az ellenőrzést koordináló szerv a Honvédelmi Minisztérium, kivéve a honvédelmi létfontosságú információs rendszerelemeket, ahol az ellenőrzést koordináló szerv feladatait a Katonai Nemzetbiztonsági Szolgálat látja el.[168]

A BM OKF és szervei létfontosságú rendszerei vonatkozásában az ellenőrzést koordináló szerv feladatait a Belügyminiszter az általa kijelölt, ellenőrzési feladatokat ellátó szervezeti egység útján látja el[169].

2. A helyszíni ellenőrzés lefolytatására jogosult szervek a BM OKF koordinálásával ütemezett módon, az általa készített éves ellenőrzési terv alapján végzik az ellenőrzéseket. Kötelezettségük, hogy a kijelölt rendszerelemet legalább két évente ellenőrizzék, amely vizsgálatot a nemzetbiztonsági szempontok figyelembevételével kell lefolytatniuk[170].

[163] Lrtv. 8. § (1) és (4) bekezdése.
[164] Lrtv. 8. § (6) bekezdése.
[165] Lrtv. vhr. 8. § (1)–(3) bekezdései.
[166] Lrtv. vhr. 11. § (4) bekezdés.
[167] Lrtv. vhr. 8. § (4) bekezdése.
[168] Honvédelmi vhr. 3. §-a.
[169] Rendvédelmi vhr. 3. §-a.
[170] Lrtv. vhr. 8. § (3) bekezdés.

Helyszíni ellenőrzésre jogosult szervek:

a. a BM OKF és szervei létfontosságú rendszerei vonatkozásában a Belügyminszter az általa kijelölt, ellenőrzési feladatokat ellátó szervezeti egység közreműködésével látja el a feladatot[171],
b. az egészségügyi ágazat vonatkozásában[172]:
   ba) a kórházak és a laboratóriumok tekintetében a népegészségügyi feladatkörében eljáró fővárosi és megyei kormányhivatal,
   bb) a mentésirányítást végző szervezet, az Állami Egészségügyi Tartalék kezelője, az állami vérkészletek kezelője és a gyógyszer-nagykereskedelem tekintetében az egészségügyért felelős miniszter, aki a minisztériumnak az általa kijelölt, ellenőrzési feladatokat ellátó szervezeti egysége közreműködésével látja el a feladatot.

A helyszíni ellenőrzést lefolytató szerv a hatósági ellenőrzés céljából adatot igényelhet a bűnügyi nyilvántartási rendszerből, amely kizárólag a biztonsági összekötő büntetlen előéletének megállapítására irányulhat.[173]

2.4.8. Szankció

Ha a létfontosságú rendszerelem üzemeltetője nem tesz eleget az Lrtv.-ben vagy a felhatalmazása alapján kiadott más jogszabályokban, illetve az ágazati kijelölő hatóság határozatában foglalt előírásoknak, az ágazati kijelölő hatóság határozatban:

a. felszólítja a kötelezettségei betartására,
b. kötelezi az üzemeltetői biztonsági terv módosítására vagy új üzemeltetői biztonsági terv készítésére,
c. bírságot szabhat ki.[174]

A c) pont szerint kiszabható bírság összege 100 000.- Ft-tól 3 000 000.- Ft-ig terjedhet, melyet a bírság kiszabásáról rendelkező döntés véglegessé válásától számított 15 napon belül kell megfizetni a kijelölő hatóság által megadott bírság letéti számla javára. A bírság kiszabását a létfontosságú rendszerelemmel kapcsolatos hatósági eljárásokban részt vevő hatóságok is kezdeményezhetik a kijelölő hatóságnál.[175]

2.4.9. Biztonsági összekötő

Az üzemeltető kötelezettsége az Lrtv. előírásai szerint, hogy gondoskodjon a biztonsági összekötő személy foglalkoztatásáról és folyamatosan biztosítsa a tevékenységéhez szükséges feltételeket. A biztonsági összekötő személy feladata a kapcsolattartás az üzemeltető és a kijelölési eljárásban részt vevő hatóságok, szakhatóságok között.[176]

[171] Rendvédelmi vhr. 3. §-a.
[172] Eü. vhr. 15. §-a.
[173] Lrtv. 8. § (7) bekezdés.
[174] Lrtv. 9. §
[175] Lrtv. vhr. 9. § (1)–(3) bekezdései.
[176] Lrtv. 6. § (7) bekezdés.

Biztonsági összekötőnek az a büntetlen előéletű személy jelölhető ki, aki az adott ágazatnak megfelelő szakirányú végzettség mellett az alábbiakban meghatározott képzettséggel rendelkezik[177]:

a. védelmi igazgatási, katasztrófavédelmi vagy rendészeti igazgatási szakon szerzett felsőfokú végzettséggel,
b. tűzvédelmi, iparbiztonsági, polgári védelmi szakmai irányú rendészeti szervezői szakképesítéssel vagy ezzel egyenértékű végzettséggel,
c. iparbiztonsági szaktanfolyami végzettséggel,
d. iparbiztonsági szakon szerzett felsőfokú végzettséggel vagy
e. a katasztrófavédelem hivatásos szerveinél legalább 5 év iparbiztonsági szakterületen szerzett gyakorlattal.

Az a)–c) pontjában előírt követelmények alól, a korábban rendvédelmi szerv által, a rendvédelmi szerv alaptevékenységébe tartozó feladatok ellátása körében legalább öt évig foglalkoztatott felsőfokú végzettségű személy mentesül. A mentesülés feltételeinek való megfelelést az érintettnek szükséges igazolnia.

Az adott ágazatra vonatkozó további képzettségi követelmények az alábbiak:

a. az energiaágazatban a fent felsorolt képzettségeken kívül szakirányú műszaki végzettséggel kell rendelkeznie[178],
b. az egészségügyi ágazatban[179] ágazati szakirányú végzettségnek minősül az orvosi végzettség, ezen felül:
   ba) laboratóriumban történő foglalkoztatás esetén a biológus végzettség, illetve a mikrobiológus végzettség,
   bb) gyógyszer-nagykereskedelemben történő foglalkoztatás esetén az orvosi végzettség helyett
      i. a gyógyszerek minőségbiztosítása érdekében meghatalmazott személy képesítési feltételeiről szóló miniszteri rendeletben meghatározott feltételeknek megfelelő végzettség, illetve
      ii. bármely műszaki, mérnöki, logisztikus, gépész, gyógyszerész, vegyész vagy informatikus szakon szerzett felsőfokú végzettség, csak akkor, ha az ott meghatározott végzettséggel rendelkező gyógyszer-kereskedelmi, illetve egyéb gyógyszeripari tevékenységet végző gazdasági társaságnál, vállalkozásnál vagy ilyen területen működő hatóságnál, intézetnél vagy más szervezetnél legalább 3 év gyakorlatot szerzett a végzettségének megfelelő tevékenységet végezve foglalkoztatásra irányuló vagy megbízási jogviszony keretében.
   bc) a gyógyszer-nagykereskedelemben történő foglalkoztatás kivételével az egészségügyi ágazatnak megfelelő szakirányú végzettségnek minősül továbbá minden egyéb felsőfokú végzettség, ha a felsőfokú végzettséggel rendelkező egészségügyi igazgatási feladatkörben legalább hároméves szakmai gyakorlatot szerzett foglalkoztatásra irányuló vagy megbízási jogviszony keretében.
c. a pénzügyi ágazatban felsőfokú szakirányú közgazdasági vagy jogi végzettséggel kell rendelkeznie[180],
d. a honvédelmi ágazatban a katonai felsőfokú végzettséggel és az adott rendszerelem működtetésében legalább kétéves szakmai tapasztalattal kell rendelkeznie[181],

[177] Lrtv. vhr. 6. § (1)–(3) bekezdései.
[178] Energia vhr. 18. §.
[179] Eü. vhr. 13. §.
[180] Pénzügy vhr. 8. §.
[181] Honvédelmi vhr. 6. §.

e. az infokommunikációs technológiák ágazat esetében[182]:
   ea) az üzemeltető által elismert felsőfokú végzettséggel,
   eb) az infokommunikációs technológiák ágazatban eltöltött legalább öt év munkaviszonnyal és okleveles védelmi igazgatási vagy azzal egyenértékű végzettséggel vagy
   ec) az Ibtv. szerinti elektronikus információs rendszer biztonságáért felelős személy tekintetében irányadó képzettséggel,
   ed) fentieken túl az egyetemes postai szolgáltatás esetében a jogi végzettséggel is.

A büntetlen előéletre vonatkozó követelmény teljesülését a biztonsági összekötő igazolja.[183] A BM OKF és a helyszíni ellenőrzést lefolytató szerv, valamint az ágazati kijelölő hatóság a rendszerelemmé történő kijelölés hatálya alatt lefolytatott hatósági ellenőrzése keretében ellenőrizheti azt is, hogy a biztonsági összekötő büntetlen előéletű-e. [184]

2.4.10. Üzemeltetői feladatok és az üzemeltetői biztonsági terv

Az üzemeltető az ágazati kijelölő hatóság határozatában meghatározott határidőn belül – amely nem lehet rövidebb a kijelölő határozat közlésétől számított 60 napnál – köteles kidolgozni a döntésben meghatározott tartalmi és formai követelmények szerinti üzemeltetői biztonsági tervet, amelyben szerepeltetnie kell:

a. a létfontosságú rendszerelemeket és azt a szervezeti- és eszközrendszert, amely biztosítja azok védelmét,
b. azokat a biztonsági intézkedéseket, amelyek kialakítása és működtetése biztosítja a létfontosságú rendszerelem védelmét,
c. azokat az ideiglenes intézkedéseket, amelyeket a különböző kockázati és veszélyszinteknek megfelelően foganatosítani kell,
d. a létfontosságú rendszerelem védelmét szolgáló meglévő vagy kialakítás alatt álló biztonsági megoldásokkal kapcsolatos eljárást.

A hatósági döntés meghozatalánál figyelembevételre kerülő, az üzemeltetői biztonsági terv felépítésére, tartalmi és formai elemeire vonatkozó követelmények az 1. melléklet tartalmazza[185].

Soron kívül módosítani kell az üzemeltetői biztonsági tervet, ha olyan változás áll be, amely érinti a létfontosságú rendszerelem tevékenységét, működését vagy védelmét, ideértve a bekövetkezett rendkívüli eseménnyel összefüggő újonnan felmerülő kockázat kezelését is, ha azt korábban még nem vizsgálták[186]. Soron kívüli felülvizsgálatot kezdeményezhet a kijelölő hatóság vagy a kijelölő hatóságnál a BM OKF, amelynek elvégzésre az üzemeltetőnek a kezdeményezéstől számított 45 nap áll rendelkezésére. Egyéb esetben az üzemeltető felelőssége az üzemeltetői biztonsági terv szükség szerinti módosítása és az elkészítést követő 2 év elteltével annak jegyzőkönyv felvétele mellett történő felülvizsgálata.[187]

Az üzemeltetői biztonsági tervben meghatározott rendkívüli esemény bekövetkezésekor az érintett ágazati kijelölő hatóság, a beavatkozást végző szervek és a biztonsági összekötő személy együtt vesz részt a kiváltó okok azonosításában és a megtett intézkedések értékelésében[188].

[182] Infokom. vhr. 15. §.
[183] Lrtv. 6. § (7) bekezdés.
[184] Lrtv. 8. § (7) bekezdés.
[185] Lrtv. vhr. 7. § (1) bekezdés és 2. melléklet.
[186] Lrtv. 6. § (1), (2), (3), (6) és (6a) bekezdései.
[187] Lrtv. vhr. 7. § (2), (2a), (3) és (4) bekezdés.
[188] Lrtv. vhr. 11 § (6) bekezdés.

Ha az üzemeltetői biztonsági tervet módosítani szükséges, akkor annak módosítással érintett részét, vagy jelentős tartalmi módosítás esetén a módosításokkal egységes szerkezetbe foglalt üzemeltetői biztonsági tervet, az üzemeltetőnek haladéktalanul meg kell küldenie tartalmi és formai ellenőrzésre a kijelölő hatóságnak. Az ellenőrzés határideje a módosított üzemeltetői biztonsági terv kijelölő hatósághoz érkezésének napjától számított 30 nap. Ha a felülvizsgálat eredményeként nem szükséges az üzemeltetői biztonsági tervet módosítani, a felülvizsgálatról szóló jegyzőkönyvet az üzemeltető a felülvizsgálatot követően haladéktalanul másolatban megküldi a BM OKF-nek mint nyilvántartó hatóságnak és a kijelölő hatóságnak[189].

Ha az üzemeltető a kijelölés alkalmával rendelkezik olyan biztonsági dokumentummal, amely az üzemeltetői biztonsági terv tartalmi elemeit magában foglalja, akkor kérelmére az ágazati kijelölő hatóság rendelkezhet úgy, hogy a biztonsági dokumentum az üzemeltetői biztonsági tervet helyettesíti. Az üzemeltető kötelezettsége, hogy a létfontosságú rendszerelem működésének védelmét és folyamatosságát az üzemeltetői biztonsági tervvel összhangban szervezze meg és biztosítja az üzemeltetésében lévő létfontosságú rendszerelem működésének védelmét és folyamatosságát. [190]

Az üzemeltetőnek az üzemeltetői biztonsági tervet – ideértve a fenitek alapján módosított tervet is – papíralapon és elektronikus adathordozón is meg kell küldenie az ágazati kijelölő hatóságnak, aki a nyilvántartásba vételt megelőzően azt a döntésében foglaltak alapján formailag és tartalmilag ellenőrzi, hiányosság esetén az üzemeltetőt hiánypótlásra szólítja fel. Az ellenőrzött és megfelelő üzemeltetői biztonsági tervet az ágazati kijelölő hatóság a BM OKF-nek mint nyilvántartó hatóságnak és az üzemeltetőnek küldi meg.[191]

Az üzemeltetői biztonsági terv és mellékletei, vagy az azokat helyettesítő biztonsági dokumentum, nem nyilvánosak.

Az üzemeltető feladatkörébe tartozik továbbá[192]:

a. a biztonsági esemény bekövetkezését követően a Központ haladéktalan tájékoztatása,
b. a bekövetkezett rendkívüli eseményekről haladéktalanul tájékoztatja a BM OKF területi szervének ügyeleti szolgálatát, valamint az ágazat szerinti eseménykezelő központot,
c. a nyilvántartott adatokban bekövetkezett változásokról a BM OKF 72 órán belül történő tájékoztatása,
d. katasztrófaveszély vagy katasztrófa esetén az ágazati kijelölő hatóság és a BM OKF haladéktalan értesítése.

Az Lrtv. előírásai szerint az üzemeltetőt terhelik az alábbi költségek[193]:

a. az üzemeltetői biztonsági terv elkészítésének és módosításának költségei, azzal, hogy az üzemeltetői biztonsági tervben foglaltakon kívüli védelmi intézkedésre vagy a védelmi intézkedés költségeinek megfizetésére nem köteles,
b. a biztonsági összekötő személy foglalkoztatásának költségei,
c. az üzemeltetői biztonsági tervben foglalt, a létfontosságú rendszerelemek védelmét szolgáló szervezeti és eszközrendszerrel kapcsolatban felmerült költségek.

[189] Lrtv. vhr. 7. § (5)–(6) bekezdései.
[190] Lrtv. 6. § (3)–(4) bekezdések és Lrtv. vhr. 7. § (7) bekezdés.
[191] Lrtv. 6. § (1), (1a) és (6) bekezdései, Lrtv. vhr. 6. § (5) bekezdése.
[192] Lrtv. 6. § (6a) és (6b) bekezdés és Lrtv. vhr. 10 § (2) bekezdés és 11. § (5) bekezdés.
[193] Lrtv. 7. §.

2.4.11. Ágazati szabályok

Az Lrtv. felhatalmazása alapján az Lrtv. vhr. mellett több további kormányrendelet is tartalmaz kiegészítő szabályokat az egyes ágazati szabályokra, specialitásokra vonatkozóan. Ezen rendelkezések fő szabályozási környezethez kapcsolódó elemei (pl. javaslattevő és ágazati kijelölő hatóságok, ágazati kritériumok, biztonsági összekötő képesítési követelményei) fentiekben már rögzítésre kerültek. A további részletszabályok tételes ismertetésére jelen jegyzet nem tér ki, néhány kiegészítő szabályt azok speciális jellegére vonatkozóan azonban kiemelni szükséges.

Az Lrtv. egyedül az energiaágazatra vonatkozóan határoz meg törvényi szintű eltérő rendelkezéseket[194] és eljárási lépéseket az alábbiak szerint. Kimondja, hogy:

a. a villamosenergia-rendszer tekintetében annak létesítményeire,
b. a kőolajipar tekintetében a kőolaj- és cseppfolyós szénhidrogén termék szállítóvezetékre és tárolóra, a kőolajtermelésben és -feldolgozásban használt létesítményre,
c. a földgázipar tekintetében az együttműködő földgázrendszerre, a célvezetékre, a földgáztermelésben, előkészítésben és feldolgozásban használt mezők közötti vezetékre, valamint az ezekhez kapcsolódó bányászati, tároló és gázüzemi létesítményre, valamint a cseppfolyósföldgáz-terminálra,

(a továbbiakban az a)–c) pont együtt: energetikai létesítmény) az Lrtv. rendelkezéseit az alábbi eltérésekkel kell alkalmazni.

Eltérő szabályként rögzíti, hogy az energetikai létesítmények esetében a létfontosságú rendszer, létesítmény vagy eszköz alatt kizárólag a rendszerelemet kell érteni és az energetikai létesítmény alkotórészének kell tekinteni a technológiai hírközlési és informatikai rendszert is.

A nemzeti és az európai létfontosságú rendszerelem Lrtv. szerinti kijelölési eljárását az energetikai létesítményre teljes egészében nem kell alkalmazni, mivel az eljárási szabályokra az Lrtv. az alábbi kiegészítő rendelkezéseket rögzíti:

a. Az üzemeltetőnek külön módszertan[195] szerint azonosítási jelentést kell készítenie, amelyet az ágazati kijelölő hatóságnak kell benyújtania. Ha ezen kötelezettségének nem tesz eleget, az ágazati kijelölő hatóság bírsággal sújthatja, de emellett a kijelölést a javaslattevő hatóság és az ágazati kijelölő hatóság is kezdeményezheti.
b. Az ágazati kijelölő hatóság az üzemeltető által benyújtott azonosítási jelentést:
   ba) döntésével jóváhagyja és az azonosított rendszerelemeket nemzeti létfontosságú rendszerelemnek minősíti, vagy elfogadja, hogy az üzemeltető egyetlen rendszerelemet sem azonosított nemzeti létfontosságú rendszerelemként, vagy
   bb) új azonosítási jelentés benyújtását írja elő.
c. Az európai létfontosságú rendszerelemmé történő kijelölésére vagy a kijelölés visszavonására irányuló folyamat akkor indul meg:
   ca) ha a nemzeti létfontosságú rendszerelemmé történő kijelölésre vagy a kijelölés visszavonására irányuló eljárás megindításával együtt az üzemeltető azonosítási jelentése erre is kiterjed vagy
   cb) ha azt EGT-állam kezdeményezte.

Az energiaágazatra vonatkozó részletszabályokat az Energia vhr. tartalmazza.

[194] Lrtv. 10-12. §-ok.
[195] Erre vonatkozó rendelkezést az Energia vhr. 7–10. §-ai tartalmaznak.

További ágazati végrehajtási szabályok:

a. Közbiztonság és védelem ágazata: Rendvédelmi vhr.,
b. Agrárgazdasági ágazat: Agrár vhr.,
c. Víz ágazata: Víz vhr.,
d. Egészségügyi ágazat: Eü. vhr.,
e. Pénzügyi ágazat: Pénzügy vhr.,
f. Honvédelem ágazata: Honvédelmi vhr.,
g. Infokommunikációs technológiák ágazata: Infokom. vhr.,

A közlekedési ágazat végrehajtási rendeletének, a közlekedési létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 161/2019. (VII. 4.) Korm. rendeletnek a kihirdetése megtörtént, hatálybalépésének időpontja 2019. október 01-je. A társadalombiztosítási ágazatban még nincs kihirdetett végrehajtási rendelet.

2.4.12. Uniós kötelezettségek

Az Lrtv. előírja[196] Magyarország Kormánya részére, hogy évente jelentést nyújtson be az Európai Bizottságnak:

a. az európai létfontosságú rendszerelemnek kijelölt létfontosságú rendszerelemek ágazatonkénti számáról,
b. az Unió azon tagállamainak számáról, amelyek az európai létfontosságú rendszerelemektől függenek,
c. azon ágazatok sebezhetőségi pontjainak, az azokat fenyegető veszélyeknek és kockázatoknak típusairól, amelyekben európai létfontosságú rendszerelemet jelöltek ki.

Az Lrtv. emellett rögzíti a BM OKF kötelezettségeként, hogy kétévente a Kormány által az Európai Bizottságnak történő jelentést megelőzően felülvizsgálja és szükség szerint pontosítja az alapvető szolgáltatásokat nyújtó szereplők jegyzékét.[197]

[196] Lrtv. 13. §.
[197] Lrtv. 2/A. § (6) bekezdés.

2.5. Mellékletek

1. melléklet

AZ ÜZEMELTETŐI BIZTONSÁGI TERV FELÉPÍTÉSE
(az Lrtv. vhr. 2. mellékletével azonos tartalom)

I. Tartalmi követelmények

1. Általános bemutatás

Az üzemeltető megadja a kijelölt rendszerelem adatait: megnevezése, üzemeltetető neve, székhelye, lakcíme, levelezési címe, cégjegyzékszáma vagy az egyéni vállalkozói nyilvántartási száma, adóazonosító száma, képviselőjének neve, telefon- és telefaxszáma, e-mail-címe, pontos cím hiányában a kijelölt rendszerelem elhelyezkedésére vonatkozó más azonosító adat és földrajzi koordináta, a biztonsági összekötő neve, elérhetőségei. Az üzemeltető általánosságban bemutatja a szervezetét, tevékenységét, irányítási rendszerét, a kijelölt rendszerelem védelmével kapcsolatos fő célkitűzéseit, a horizontális és ágazati kritériumok teljesülését, indokoltságát:

a. szervezeti struktúra és üzemvezetés;
b. személyzet (saját munkavállalók, külső, szerződéses munkavállalók);
c. kijelölt rendszerelem tevékenységének/működésének általános bemutatása, az elvárt, normális működés paraméterei;
d. kijelölt rendszerelem elemeinek azonosítása és értékelése a teljesült ágazati és horizontális kritériumok alapján;
e. belső audit és vezetőségi átvizsgálás;
f. a változtatások kezelése és annak követése.

2. A kijelölt rendszerelem környezetének bemutatása
Az üzemeltető bemutatja a kijelölt rendszerelem környezetét a következők szerint:

a. a környező területek jellemzése;
b. a működést biztosító közműszolgáltatások, szolgáltatók bemutatása:
   ba) elektromos áramellátás biztosítása,
   bb) vezetékes gázellátás biztosítása,
   bc) közüzemi ivóvízellátás, közüzemi szennyvízelvezetés és -tisztítás biztosítása,
   bd) infokommunikációs hálózati ellátás,
   be) egyéb;
c. a kijelölt rendszerelem környezetében található, a működésére befolyással bíró veszélyes üzemek, gyárak, erőművek megnevezése, címe, tevékenységi köre;
d. a természeti környezetre vonatkozó legfontosabb információk:
   da) a területre jellemző, a kijelölt rendszerelem sérülését eredményező és a következmények alakulására hatást gyakorló meteorológiai jellemzők,
   db) a helyszínt jellemző, a kijelölt rendszerelem biztonságos tevékenységére, üzemeltetésére, működésére hatást gyakorló legfontosabb geológiai és hidrológiai jellemzők.

3. A kijelölt rendszerelem bemutatása

Az üzemeltető ismerteti a kijelölt rendszerelem felépítését, elemeit, azok részletes tevékenységi körét, továbbá ezen részekről mellékel egy méretarányos ábrát, helyszínrajzot, valamint hozzátartozó útmutatót, magyarázatot. A bemutatás kiemelten tartalmazza a kijelölt rendszerelem működését releváns módon befolyásoló informatikai rendszerek, eszközök, hálózatok ismertetését és a működésben betöltött szerepük leírását.

A kijelölt rendszerelem felépítésének, elemeinek, részletes tevékenységének, termelési, működési folyamatainak bemutatását az alábbi szempontok alapján kell elvégezni:

a. a kijelölt rendszerelem felépítése, elemei (helyszínrajz, amely bemutatja az elemeket és vázlatosan feltünteti a létfontosságú elemet a hozzá tartozó útmutatóval, magyarázattal);
b. kiszolgáló infrastruktúra (közműhálózatok, technikai berendezések, szolgáltatást végző partnerek);
c. részletes tevékenység, a tevékenységekre vonatkozó legfontosabb technológiai és karbantartási folyamatok, műveletek;
d. tartalék rendszerelemek;
e. a lehetséges veszélyt jelentő anyagok, berendezések megjelölése, mennyisége, tárolási adatai;
f. a működésben releváns informatikai rendszerek, alkalmazások, hálózatok, azok funkciója;
g. a normál működési rend során a kijelölt rendszerelem működését garantáló eszközök, berendezések, technológiai és karbantartási folyamatok, műveletek menete, naplózása, ütemezése;
h. belső és külső tájékoztatási rendszerek;
i. felügyeleti és biztonsági szervezetek, eszközrendszerük, működésük (biztonsági szolgálat, elsősegélynyújtó és mentőszervezetek, munka-, tűz- és környezetvédelmi szolgálat, műszaki biztonsági szolgálat, katasztrófaelhárítási szervezet, távfelügyeleti és monitoringhálózatok, laboratóriumi hálózat, beléptető és az idegen behatolást érzékelő rendszerek stb.).

4. Kockázatok azonosítása, értékelése

Az üzemeltető azonosítja és értékeli a kijelölt rendszerelemmel összefüggő kockázatokat a következők szerint:

a. kockázati lista [milyen releváns belső, külső kockázatok veszélyeztetik a kijelölt rendszerelem működését: gazdasági, technológiai, infrastrukturális (közműszolgáltatások kiesése, belső infrastruktúrák kiesése), humán, fizikai, információtechnológiai, természeti, civilizációs katasztrófák, terrorizmus, egészségügyi, környezeti, társadalmi, logikai, földrajzi stb.];
b. a kijelölt rendszerelem kölcsönösen függő (interdependens) kapcsolódásai és az azokból adódó kockázatok felmérése (a kijelölt rendszerelem kiesése milyen más ágazatokra, szervezetekre, személyekre van hatással);
c. a kockázatok valószínűsíthető okainak feltárása, a bekövetkezéskor prognosztizálható negatív hatások meghatározása;
d. a felmerült kockázatok értékelése a bekövetkezési valószínűség és az okozott káros hatások meghatározásával.

5. Kockázatkezelés

Az üzemeltető meghatározza a szükséges beavatkozás szintjeit a kockázati értékek szerint. Az üzemeltető bemutatja a feltárt kockázatok kezelésére vonatkozó szabványok, intézkedések, belső utasítások, eljárások, szabályok rendszerét, szükség szerint röviden ismerteti tartalmát.

6. A kijelölt rendszerelem védelmének eszközrendszere

Az üzemeltető megjelöli azokat a biztonsági intézkedéseket, amelyek kialakítása és működtetése biztosítja a kijelölt rendszerelem védelmét, továbbá meghatározza azokat az ideiglenes intézkedéseket, amelyeket a rendkívüli esemény okozta veszélyhelyzeti működés során a különböző kockázati és veszélyszinteknek megfelelően foganatosít. Ezen belül meghatározza a veszélyhelyzeti működés, rendkívüli esemény kritériumait (a normális működéssel történő összevetésben).

Rendkívüli eseménynek tekintendő olyan külső vagy belső behatás, amely a kijelölt rendszerelem rendeltetésszerű működését jelentős mértékben veszélyezteti, akadályozza. Jelentősnek minősül az az esemény, melyet az üzemeltető saját erőforrásaival, külső segítség nélkül nem képes kezelni, elhárítani.

Az üzemeltető bemutatja a kijelölt rendszerelem elemeinek és egészének védelmére rendszeresített felszereléseket és a vezetéshez, a döntés-előkészítéshez szükséges infrastruktúrát a következők szerint:

a. a veszélyhelyzeti vezetési létesítmények;
b. a vezetői állomány veszélyhelyzeti értesítésének eszközrendszere;
c. a dolgozók veszélyhelyzeti riasztásának eszközrendszere;
d. a veszélyhelyzeti híradás eszközei és rendszerei;
e. a veszélyhelyzet értékelését és a döntések előkészítését segítő informatikai rendszerek;
f. a veszélyhelyzet kezelésének eljárásrendje;
g. a riasztást, a védekezést és a következmények csökkentését végző végrehajtó szervezetek rendszeresített egyéni védőeszközei és szaktechnikai eszközei;
h. a védekezésbe bevonható (nem közvetlenül erre a célra létrehozott) belső és a külső erők és eszközök;
i. a kijelölt rendszerelem kiesése következtében alkalmazható vagy rendelkezésre álló alternatív megoldások;
j. rendkívüli eseménykor értesítendők köre.

7. Az üzemeltetői biztonsági terv elkészítésébe bevont személyek, szervezetek megjelölése

Az üzemeltető megjelöli az üzemeltetői biztonsági terv elkészítésébe bevont személyeket, szervezeteket.

II. Formai követelmények

Az üzemeltetői biztonsági tervet írásban kell elkészíteni és a nyilvántartó, valamint a kijelölő hatóság részére egy-egy eredeti – az üzemeltető és a biztonsági összekötő személy által aláírt – példányban papíralapon, továbbá elektronikus adathordozón is be kell nyújtani. A térképeket, a rajtuk szereplő méretaránynak megfelelően, nyomtatott formában is be lehet nyújtani. A térképvázlat vagy helyszínrajz tartalmazza a kijelölt rendszerelem egészét és olyan méretarányú legyen, amely a megfelelő eligazodást biztosítja.

2.6. Irodalomjegyzék

1. Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.
   URL: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu
   Letöltés ideje: 2019. augusztus 22.

2. Az Unió helyzete 2018 Jean-Claude Juncker, az Európai Bizottság elnökének beszéde - 2018. szeptember 12.
   URL:https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-brochure_hu_0.pdf
   Letöltés ideje: 2019. augusztus 22.

3. Erős kiberbiztonság kialakítása Európában
   URL:https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-cybersecurity_hu.pdf
   Letöltés ideje: 2019. augusztus 22.

3. JOGSZABÁLYTÁR

3.1. Magyar jogszabályok

- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
  https://net.jogtar.hu/jogszabaly?docid=a0100108.tv
- 2001. évi XXXV. törvény az elektronikus aláírásról
  https://mkogy.jogtar.hu/?page=show&docid=a0100035.TV
- 2003. évi C. törvény az elektronikus hírközlésről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300100.TV
- 2009. évi CLV. törvény a minősített adat védelméről
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.323131
- 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1000157.tv
- 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról
  https://net.jogtar.hu/jogszabaly?docid=A1100128.TV
- 2011. évi CXII. törvény információs önrendelkezési jogról és az információszabadságról
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.322945
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv
- 85/2012. (IV. 21.) Korm. rendelet az elektronikus ügyintézés részletes szabályairól
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=148205.295314
- 84/2012. (IV. 21.) Korm. rendelet az egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200084.korű
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323158
- 2013. évi CCXX. törvény az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól
  https://mkogy.jogtar.hu/?page=show&docid=a1300220.TV
- 65/2013 (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
  https://net.jogtar.hu/jogszabaly?docid=a1300065.kor
- 360/2013. (X. 11.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=a1300360.kor

- 512/2013. (XII. 29) Korm. rendelet az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról
  https://net.jogtar.hu/jogszabaly?docid=a1300512.kor
- 540/2013. (XII. 30) Korm. rendelet a létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=A1300540.KOR
- 541/2013. (XII. 30.) Korm. rendelet a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=a1300541.kor
- 186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500186.kor
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500187.KOR
- 157/2016. (VI. 13.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendelet módosításáról
  http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600157.KOR&timeshift=fffffff4&txtreferer=00000001.TXT
- 2016. évi CL. törvény az általános közigazgatási rendtartásról
  https://net.jogtar.hu/jogszabaly?docid=A1600150.TV
- 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=A1500246.KOR
- 330/2015. (XI. 10.) Korm. rendelet a pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=a1500330.kor
- 359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=a1500359.kor
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500042.bm
- 249/2017. (IX. 5.) Korm. rendelet az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=A1700249.KOR
- 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről
  https://net.jogtar.hu/jogszabaly?docid=A1800270.KOR

- 271/2018. (XII. 20. Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól
  https://net.jogtar.hu/jogszabaly?docid=a1800271.kor
- 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=212067.363096

3.2. Európai Uniós jogi aktusok

- Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelv
  https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32008L0114&from=EN
- A fogyasztói jogviták alternatív rendezéséről, valamint a 2006/2004/EK rendelet és a 2009/22/EK irányelv módosításáról szóló, 2013. május 21-i 2013/11/EU európai parlamenti és tanácsi irányelv
  https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0011&from=EN
- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
  http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU
- Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér
  http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52013JC0001&from=-HU
- Számítástechnikai bűnözésről szóló Egyezmény (2001) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa405
- Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10) az Európai Hálózat és Információbiztonsági Ügynökség létrehozásáról
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:HU:HTML
- Az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről
  http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32013R0526&from=HU
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről
  http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=HU
- Az Európai Parlament és a Tanács rendelet tervezete az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról
  https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52017PC0477R%2801%29
- Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról
  http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31995L0046&from=HU
- Az Európai Parlament és a Tanács 2002/58/EK (2002. július 12.) irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről
  http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002L0058&from=HU

- Az Európai Parlament és a Tanács 2013. augusztus 12-i 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l33193&from=EN
- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU
- Közös Közlemény az Európai Parlamentnek és A Tanácsnak: Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése vonatkozásában http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=EN
- Az ENSZ Közgyűlés a 2003. december 8-i 58/32-es számú határozata https://undocs.org/A/RES/58/32
- Az Európai Parlament 2012. június 12-i állásfoglalása „A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: a globális kiberbiztonság felé" című dokumentumról (2011/2284(INI)) https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012IP0237&qid=1521197299768&from=HU
- A Tanács következtetései a kiberdiplomáciáról (2015) http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf
- A Bizottság 2017/1584 ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2017.239.01.0036.01.HUN&toc=OJ:L:2017:239:TOC
- A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről (2017): http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/hu/pdf

3.3. Külföldi jogi aktusok

- Az EBESZ Állandó Tanácsának PC.DEC/1039 számú döntése: https://www.osce.org/pc/90169?download=true
- Az EBESZ bizalomépítő intézkedései: PC.DEC/1106 https://www.osce.org/pc/109168

4. FOGALOMTÁR

- **Adat:** Az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas, számos megjelenési formát vehet fel (például: alfabetikus, numerikus, grafikus, képi forma) és amely új ismeret forrása. [1]
- **Adatbiztonság:** Az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összességét kell érteni. Mindkét esetben alapvető cél az adat jogellenes kezelésének vagy feldolgozásának megakadályozása, azaz az adatok megfelelő intézkedésekkel történő védelme a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy a megsemmisítés ellen, valamint a sérülés elkerülése érdekében. [2]
- **Adathalászat:** Más néven phishing, melynek lényege abban rejlik, hogy az adathalászok a felhasználókat, valamilyen elektronikus csatornán keresztül – például e-mailben, azonnali üzenetben vagy éppen szalagcím hirdetésekben – egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják, ahol arra kérik, hogy adja meg bizalmas adatait. Az adathalászatnak számos válfaja van aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra. [3]
- **Adatfeldolgozás:** Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől). [2]
- **Adatfeldolgozó:** Az személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi. [2]
- **Adathordozó:** Minden olyan anyagi eszköz, mely alkalmas adatok megőrzésére, tárolására. Az Európai Parlament és a Tanács 2002/65/EK irányelve szerint, amely már tartós adathordozóként nevesít: „olyan eszköz, amely lehetővé teszi a fogyasztó számára a személyesen neki címzett adatoknak a jövőben is hozzáférhető módon és az adat céljának megfelelő ideig történő tárolását, valamint a tárolt adatok változatlan formában történő megjelenítését”. Így adathordozó a pendrive, a DVD, CD, SD-kártya, amely alkalmas kisebb vagy nagyobb mennyiségű adat tárolására. [4]
- **Adatkezelés:** Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése. [2]
- **Adatkezelő:** Az a személy vagy szervezet, aki/amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja vagy az általa megbízott adatfeldolgozóval végrehajtatja. [2]
- **Adatvédelem:** A személyes adatok védelme. Az adatkezelés során érintett személyek, azok személyiségi jogainak, adataival való önrendelkezési jogának védelme érdekében megvalósítandó/megvalósított, az adatkezelés módjára, formájára, tartalmára vonatkozó szabályozások és eljárások. [5]

- **Adatvédelmi incidens:** A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. A definíció alapján megállapítható, hogy az olyan biztonsági incidens, amely nem érint személyes adatot, nem adatvédelmi incidens, azonban valamennyi adatvédelmi incidens biztonsági incidens. [2]
- **Adattal rendelkezés:** A birtokban tartás, az adat alapján további adat készítése, az adat másolása, sokszorosítása, a betekintés engedélyezése, a feldolgozás és felhasználás, a minősítés (biztonsági osztályba sorolás) felülvizsgálata, a minősítés (biztonsági osztályba sorolás) felülbírálata, a nyilvánosságra hozatal, titoktartási kötelezettség alóli felmentés, megismerési engedély kiadása. [5]
- **Adatokat érintő beavatkozás:** Információs rendszerekben található digitális adatok törlése, károsítása, rongálása, megváltoztatása, eltávolítása vagy hozzáférhetetlenné tétele. A fogalom emellett magában foglalja az adatlopást, valamint a pénzeszközök, a gazdasági erőforrások, illetve a szellemi tulajdon eltulajdonítását is. [6]
- **Adatkifürkészés:** digitális adatok információs rendszeren belüli, odairányuló vagy onnan kiinduló nem nyilvános továbbításának – így például az információs rendszerből kibocsátott, ilyen digitális adatokat hordozó elektromágneses jeleknek – a kifürkészése műszaki eszközökkel. [6]
- **Advanced persistent threat (APT):** Magas szintű, tartós vagy más néven (és az anyagban is használt) célzott támadás olyan titkos és folyamatos számítógépes hackerfolyamatok sorozatát jelenti, amelyeket gyakran meghatározott személy, személyek vagy szervezet ellen követnek el. Az APT általában magánszervezetek, államok vagy mindkettő ellen irányul, és üzleti vagy politikai motívumok vezérlik az elkövetőket, a cél általában információszerzés, de előfordult már olyan támadás is, melynek célja a szabotázs volt. [7]
- **Aktív kiberbiztonság (Active Cyber Defence Cycle** – ACDC): Aktív kiberbiztonsági intézkedések gyűjtőfogalma. Az aktív kiberbiztonság négy nagyobb tevékenységből áll, ezek a fenyegetéselemzés és információgyűjtés (threat intelligence consumption); az eszközleltár és hálózatbiztonsági monitoring; az incidenskezelés; a fenyegetés és környezet kezelése (threat and enviroment manipulation). [8]
- **Alapvető szolgáltatást nyújtó szereplő:** Alapvető szolgáltatást nyújtó szereplő Magyarországon azon intézmény lehet, amely kijelölt nemzeti létfontosságú rendszerelem üzemeltetője, a NIS-irányelv II. mellékletében felsorolt ágazatok és alágazatok valamelyikébe sorolható szolgáltatást nyújt, szolgáltatása elektronikus információs rendszerektől függ, valamint a szolgáltatását érintő biztonsági esemény jelentős zavart okozna az általa nyújtott szolgáltatás biztosításában. Alapvető szolgáltatásoknak tekinthetők a társadalom vagy gazdaság szempontjából fontos szerepet betöltő magán- és állami vállalkozások, például vízellátás, villamosáram-szolgáltatás stb. [9]
- **Android:** Linux-kernelt használó mobil operációs rendszer, elsősorban érintőképernyős mobileszközökre (okostelefon, táblagép) tervezve. [10]
- **Authentikáció:** Az authentikáció az a folyamat, amelynek során ellenőrizzük a felhasználó identitását és azt, hogy hozzáférhet-e a rendszerhez. A felhasználók azonosításakor az alábbi négy lehetőség közül választhatunk: tudás (valami, amit csak a felhasználó tud), tulajdon vagy birtok (valami, ami csak a felhasználónál van), tulajdonság (a felhasználóra jellemző egyedi biológiai tulajdonság). [11]
- **Automatizált informatikai biztonsági vizsgálat:** Olyan biztonsági vizsgálati eljárás, mely során az érintett szervezet informatikai rendszerének sérülékenységei kimondottan célszoftverek segítségével kerülnek feltérképezésre. [12]
- **Backdoor (hátsó ajtó) program:** A felhasználók számára általában nem látható elem, amelyet a telepítést követően egy vagy több távoli személynek lehetőséget biztosít a számítógép

elérésére és irányítására. Ennek segítségével a támadó megtekintheti a másik eszközön tárolt adatokat, információkat, de akár módosíthatja vagy törölheti is ezeket. A program veszélyessége abban rejlik, hogy nem csak távoli elérést biztosíthat idegeneknek, hanem rendszeradminisztrációs jogok megszerzését is lehetővé teheti. A backdoor programok a többi rosszindulatú programhoz hasonlóan települhetnek adathordozók vagy e-mail, illetve egyéb internetes letöltés mellékleteként. [13]

- **Bejelentésköteles szolgálgatásokat nyújtó szereplő:** Magyarországon bejelentésköteles szolgáltatásoknak nevezzük azon szolgáltatásokat, melyek a NIS-irányelv szerinti digitális szolgáltatók körébe tartoznak. Továbbá azon nem mikro- és kisvállalkozásokat, melyek online piacteret, online keresőprogramot, valamint felhőalapú számítástechnikai szolgáltatást nyújtanak. [9]
- **Betörés detektáló eszköz:** Olyan rendszer, amely minden észlelt aktivitást valós időben megvizsgálva, egyenként eldönti, hogy az adott aktivitás legális-e vagy sem. Fajtái a mintaalapú betörés detektáló eszközök (signatura-based IDS) és a viselkedést vizsgáló betörés detektáló eszközök (behavior-based IDS). Intrusion Detecting Systems (rövidítve: IDS). [14]
- **Big Data:** A cégek, az intelligens hálózatok, a magánszektor és az egyéni felhasználók által világszerte és napi szinten előállított óriási adatmennyiséget jelenti. Strukturáltan és kielemezve ez a rengeteg információ nagy hasznot hozhat a cégek és ügyfelek számára. [15]
- **Biometrikus azonosítás:** Olyan eszközök és eljárások összessége, amely a személyek mérhető testi tulajdonságait használják fel valamilyen technika segítségével azonosításra vagy a személyazonosság megállapítására. Az azonosítás szempontjából a legalkalmasabb adatok, illetve eljárások: a DNS-minta, ujjnyomatok, retinaképek, hangelemzés, íriszdiagnosztika, a tenyér vénamintáinak azonosítása, gépelési mintaalapú azonosítás. [16]
- **Bizalmasság elve:** Az elektronikus információs rendszer azon tulajdonsága, amely szerint az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról csak az arra jogosult és csak a jogosultság szintje szerint férhet az adathoz és használhatja fel. [1]
- **Biztonság:** A biztonságot olyan állapotnak tekinthetjük, amelyben kizárható vagy megbízhatóan kezelhető az esetlegesen bekövetkező veszély, illetve adottak a veszéllyel szembeni eredményes védekezés feltételei. [5]
- **Biztonsági esemény:** Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül. [5]
- **Biztonsági esemény kezelése:** Az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység. [5]
- **Biztonsági osztály:** Az elektronikus információs rendszer védelmének elvárt erőssége. [5]
- **Biztonsági osztályba sorolás:** A kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása. [5]
- **Biztonsági szint:** A szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [5]
- **Biztonsági szintbe sorolás:** A szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [5]
- **Biztonságtudatosság:** A felhasználó azon magatartása, amikor betartja az információbiztonsági szabályokat, megérti az információbiztonságban betöltött szerepét és figyel az őt esetlegesen érintő fenyegetésekre. [17]

- **Célzott támadások** (Targeted Attacks)**:** Célzott támadásoknak nevezzük az olyan fenyegetéseket, melyeket a támadók kifejezetten egy adott célpont (személy vagy szervezet) ellen használnak. Egy számítógépes vírushoz képest a fenyegetés "megalkotója" ebben az esetben nem arra törekszik, hogy a kártékony kód minél jobban elterjedjen, hanem arra, hogy a kiszemelt célpont eszközére, eszközeire bejusson. [14]
- **CIA:** Az elektronikus információs rendszer védelmének alapvető céljának, a bizalmasság (ang.: confidentiality), a sértetlenség (ang.: integrity) és a rendelkezésre állás (ang.: availability) védelmi hármasának jelölése. [5]
- **Cloud computing:** („számítástechnikai felhő", „felhőalapú informatika"): A számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhőalapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások. Felhőalapú informatika-alapon működnek például a milliók által használt internetes levelező rendszerek (például: Gmail) vagy az online tárhelyek (például: Dropbox). Fontos előny, hogy az ügyfél gazdaságosan és személyre szabottan juthat informatikai rendszerhez anélkül, hogy az ehhez szükséges drága beruházásokra költenie és a rendszerek fenntartásához szükséges személyzetet alkalmaznia kellene. A felhőalapú informatika azonban számos adatvédelmi aggályt vet fel. A felhasználó által feltöltött adatok ugyanis folyamatos mozgásban vannak, amelyről a felhasználó nem értesül. Több szolgáltatás esetén a szolgáltatást nyújtó saját, főleg marketing, céljaira is felhasználja az ügyfél személyes adatait. A szolgáltató a világ minden pontján igénybe vesz alvállalkozókat, akik az ügyfél tudta nélkül dolgozzák fel az adataikat. Több (összetettebb vállalati) alkalmazás esetén az adatok a felhőből csak nehézkesen menthetők le, így a felhasználó csak komoly anyagi terhek árán tud a felhőalapú szolgáltatástól szabadulni. [2]
- **Digitális szolgáltatás:** Az (EU) 2015/1535 európai parlamenti és tanácsi irányelv (1) 1. cikke (1) bekezdésének b) pontja szerinti, a III. mellékletben felsorolt típusok valamelyikének megfelelő szolgáltatás. [18]
- **Digitális szolgáltató:** Minden olyan jogi személy, amely digitális szolgáltatást nyújt. [18]
- **Domain Name System (DNS):** A tartománynévrendszer egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az internetre vagy egy magánhálózatra kötött bármilyen erőforrás számára. A részt vevő entitások számára kiosztott tartománynevekhez (doménekhez) különböző információkat társít. Legfontosabb funkciójaként az emberek számára értelmes tartományneveket a hálózati eszközök számára érthető numerikus azonosítókká „fordítja le", „oldja fel", melyek segítségével ezeket az eszközöket meg lehet találni, meg lehet címezni a hálózaton. [19]
- **DNS-szerver:** A DNS-kiszolgáló egy olyan szolgáltató oldali szerver, amely az internetes címek fordításáért felelős. Ezen szerver segítségével tudunk az interneten keresztül weboldalakon böngészni, e-maileket küldeni és fogadni. [19]
- **EC3:** Az Europol Európai Kiberbűnözés Elleni Központja, amelynek fő feladata a szervezett bűnözés ellehetetlenítése, elsősorban a tagállamok nyomozóhatóságainak nyújtott, operatív támogatása által. [18]
- **Egyetlen kapcsolattartó pont (SPOC):** A kapcsolattartó pont fő feladata az Európai Unión belüli nagy hatású kiberincidensek hazai koordinálása, valamint az incidensekkel kapcsolatos jelentések fogadása, küldése az EU-s tagállamok SPOC-ai számára. [9]
- **Elektronikus információbiztonság:** Távközlési és informatikai, valamint egyéb elektronikus rendszerekben és a támogató infrastruktúrákban alkalmazott rendszabályok összessége, amelyek védelmet nyújtanak az elektronikusan előállított, feldolgozott, tárolt, továbbított és megjelenített információk bizalmasságának, sértetlenségének és rendelkezésre állásának véletlen vagy szándékos csökkentése ellen. [3]

- **Elektronikus információs rendszer:** Az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese. [5]
- **Elektronikus információs rendszer biztonsága:** Az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. [5]
- **Elosztott szolgáltatás megtagadásos** támadás**:** Az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. [5]
- **ENISA (Európai Uniós Kiberbiztonsági Ügynökség):** Az EU elsőszámú kiberbiztonsággal foglalkozó intézménye, a kiberbiztonsággal kapcsolatos tanácsadásért felelős ügynökség, amely információs és tudásközpontként működik. [18]
- **EPCIP (European Programme for Critical Infrastructure Protection):** A kritikus infrastruktúrák védelmére irányuló európai program, amelynek célkitűzése, hogy javítsa a létfontosságú infrastruktúrák védelmét az Európai Unióban. [18]
- **Ethernet:** A DEC, Intel és Xerox cégek által kidolgozott alapsávú LAN-ra vonatkozó specifikáció. Az Ethernet-hálózatok az ütközések feloldására a CSMA/CD-t használják. Számos kábeltípuson (csavart érpár, optika stb.) működik legalább 10 Mbps sebességgel. [22]
- **Europol:** Európai Rendőrségi Hivatal, amelynek fő feladata segítséget nyújtani az EU-s tagállamok bűnüldöző hatóságainak a terrorizmus elleni fellépésben, illetve a súlyos nemzetközi bűncselekmények felderítésében. [18]
- **Eseménykezelő Szakterület (Event Detection Team):** Intézmények közti megállapodás keretében a biztonság növelése érdekében folyamatosan monitorozza a hálózati forgalom különböző szegmenseit. A szakterület által végzett feladat preventív és detektív jellegű, hiszen alapvetően passzív adatforgalom ellenőrzésről és annak elemzéséről van szó. A szisztematikusan összegyűjtött támadási kísérletek rendszerezett adatai alapján azonosíthatjuk a támadók által felhasznált internetes erőforrások címeit, másrészt – különböző elemző algoritmusok segítségével – felfedezhetjük a behatolási módszerek alkalmazási trendjeinek aktuális alakulását, valamint következtetéseket vonhatunk le az internetre épülő szolgáltatások hátterét nyújtó szoftverkörnyezet esetleges gyenge pontjairól, illetve sebezhetőségeiről. [20]
- **Fenyegetés:** Olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemeinek védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát. [5]
- **Folytonos védelem:** Az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem. [1]
- **Fluxus:** A fluxus a felületet metsző mágneses erővonalak mennyisége. [21]
- **Gateway:** Átjáró, konverter eszköz különböző protokollon kommunikáló eszközök között. [22]
- **GDPR:** A GDPR röviden az Európai Unió és a Tanács által elfogadott, a személyes adatok védelméről és az ilyen adatok szabad áramlásáról szóló rendelete, más néven általános adatvédelmi rendelet (General Data Protection Regulation). A GDPR közvetlen hatállyal rendelkezik, minden tagállamban kötelezően alkalmazandó. Ennél fogva minden tagállamban ez a rendelet lesz a legfontosabb szabályanyag a személyes adatok kezelése és védelme tekinteté-

ben, attól eltérni csak akkor lehet, ha azt maga a GDPR megengedi. A rendeletet 2018. május 25-től kell alkalmazni.

- **Hacker:** Az informatikai rendszerbe informatikai eszközöket használva, kifejezett ártó szándék nélküli betörő személy. A tömegkommunikációban helytelenül minden számítógépes bűnözőre használják. Eredeti jelentése szerint a hacker olyan mesterember, aki fából tárgyakat farag. [5]
- **Hacktivizmus:** Olyan cselekedet, amelyben a támadók számítógép hálózatokba hatolnak be és az ott megszerzett adatokat közzéteszik, hogy így hívják fel a figyelmet az általuk képviselt célokra. Fogalmilag, bár nem azonos, mégis számos közös pontja van a kiberterrorizmussal. Mindkettőre jellemző, elsősorban kisebb, decentralizált csoportok hajtják végre azokat támadások, amelyek célja, hogy felhívják a figyelmet a csoport által képviselt ideológiai véleményre. Hatásuk, bár elenyésző, ugyanis nem rendelkeznek azzal a képességgel, amely egy hatékony kibertámadáshoz szükséges lenne, a médiahatásuk azonban így is igen komoly lehet. Napjainkban az egyik legismertebb hacktivista csoport a 4chan nevű fórum tagjaiból megalakult Anonymous csoport. [23]
- **Hálózat:** Informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége. [5]
- **Hálózati és információs rendszer:** elektronikus hírközlő hálózat vagy minden olyan eszköz, vagy egymással összekapcsolt eszközök csoportja, amelyek digitális adatokat dolgoznak fel, valamint a tárolt, kezelt, visszakeresett vagy továbbított digitális adatok. [6]
- **Hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia:** Olyan stratégiai dokumentum, amelyben legalább a NIS-irányelv szerinti hálózati és információs rendszerek biztonságára vonatkozóan nemzeti szinten stratégiai célkitűzéseket és prioritásokat állapítanak meg a tagállamok. [9]
- **Hardver:** Az információs rendszerek (talán) legegyértelműbb eleme, mely magában foglal minden olyan eszközt vagy részelemet, mely az információ feldolgozásában, továbbításában, tárolásában részt vesz. Az okoseszközök esetében ez általában maga az eszköz, de időnként kiegészülhet olyan opcionális elemekkel, melyek ideiglenesen vagy állandó módon csatlakoztathatók az eszközhöz. [24]
- **Hitelesség:** Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik. [5]
- **Honeypot (csapdarendszer):** Elsődleges célja az, hogy – valós működést szimulálva – elhitessék a támadókkal, hogy éles szolgáltatást nyújtó rendszert sikerült elérniük. Mindeközben azonban a jól felépített csapdarendszerek a támadó valamennyi tevékenységét letapogatják, módszeresen összegyűjtik, rögzítik és naplózzák. Tekintettel arra, hogy a csapdarendszer valójában nem működtet „igazi" szolgáltatást, a rajta észlelt valamennyi tevékenység jogtalannak minősíthető, azaz potenciális támadásként fogható fel. A csapdarendszerek tehát lényegében arra szolgálnak, hogy a támadók saját magukat leplezzék le egy olyan álcázott környezetben, ahol minden tevékenységük nyomot hagy. [20]
- **IKT-folyamat:** Valamely IKT-termék vagy IKT-szolgáltatás tervezése, fejlesztése, rendelkezésre bocsátása, illetve nyújtása vagy karbantartása céljából végzett tevékenységek összessége. [18]
- **IKT-szolgáltatás:** Olyan szolgáltatás, amely teljes mértékben vagy legnagyobb részben információhálózati és információs rendszerek útján történő továbbításából, tárolásából, lekérdezéséből vagy kezeléséből áll. [18]
- **IKT-termék:** Valamely hálózati vagy információs rendszer eleme vagy elemeinek csoportja. [18]
- **Illetéktelen személy:** Valamely tevékenység végzésére nem jogosult személy. Az informatikai biztonság esetében tipikusan az objektumba, az informatikai rendszerbe történő belépésre, adatkezelésre nem jogosult személy. [5]
- **Információ:** Bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában meg-

adott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti. [1]

- **Információbiztonság:** Olyan tevékenység vagy állapot, amely középpontjában: a bizalmasság, a sértetlenség és rendelkezésre állás jelenik meg, függetlenül attól, hogy az információt hordozó adat milyen megjelenési formát vesz fel (például: alfabetikus, numerikus, grafikus, képi forma) és milyen adathordozón jelenik meg. [25]
- **Informatikai biztonság:** Egy informatikai rendszer olyan állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Ez azt jelenti, hogy egy, az összes fenyegetést figyelembe vevő, a rendszer valamennyi elemére kiterjedő, az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósuló védelmi rendszer. [5]
- **Informatikai biztonságpolitika:** A biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására. [5]
- **Informatikai biztonsági stratégia:** Az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere. [5]
- **Infrastruktúra:** Ember alkotta rendszerek és eljárások hálózata, amelyek szinergikusan együttműködve arra törekszenek, hogy folyamatosan alapvető termékeket és szolgáltatásokat állítsanak elő és terjesszenek. [18]
- **Internet of Things (IoT):** A dolgok internete kifejezés különböző, egyértelműen azonosítható objektumokra és azok internetszerű hálózatára utal. A kifejezést 2009-ben alkotta meg Kevin Ashton, de a koncepció ötlete 1991-ben vetődött fel először. Objektum alatt értjük ebben az esetben az összes olyan elektronikai eszközt, mely képes valamilyen hasznos információt felismerni, „mérni" és ezt kommunikálni is egy másik eszköz felé. Lehet ez egy okostelefon, egy vérnyomásmérő vagy az autónk fedélzeti számítógépe (ECU). Nincsenek sem méretbeli, sem pedig felhasználási megkötései ezen eszközöknek. [26]
- **Ipari irányító rendszerek (Industrial Control Systems):** Ezek nélkül a rendszerek nélkül ma már elképzelhetetlen a közműszolgáltatások, a gyártósorok vagy éppen a közlekedés és szállítmányozás zavartalan működésének biztosítása. Mára a legtöbb ICS-rendszer és -berendezés ugyanolyan vagy legalábbis nagyon hasonló komponensekből épül fel, mint a más szektorok (pénzügy, államigazgatás, szolgáltatói szektorok) IT-rendszerei. [8]
- **iOS:** Az Apple Inc. mobil operációs rendszere, amelyet iPhone, iPod touch és iPad készülékekre fejlesztenek.
- **Katonai Nemzetbiztonsági Szolgálat Kibervédelmi** Központja**:** A honvédelmi célú elektronikus információs rendszereket érintő biztonsági események és fenyegetések kezelését végző szerv.
- **Kémprogramok** (**Spyware**)**:** A rendszerbe jutva a háttérből figyelik a rendszerben lezajló eseményeket, melyekről jelentéseket és adatokat küldenek a támadónak, de céljuk továbbá az infokommunikációs eszközön lévő információk megszerzése a felhasználó tudta nélkül. [13]
- **Kiberbiztonság:** A kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhezés működtetéséhez. [1]
- **Kiberfenyegetés:** Bármely olyan potenciális körülmény, esemény vagy cselekmény, amely károsíthatja vagy megzavarhatja a hálózati és információs rendszereket, az ilyen rendszerek felhasználóit és más személyeket, vagy azokra egyéb kedvezőtlen hatást gyakorolhat. [18]
- **Kibervédelem:** A kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertérképességek megőrzését. [1]

- **Kiberbűnözés:** Célja az informatikai eszközökön keresztüli minél nagyobb jövedelem megszerzése. Ez a bűnelkövetési forma alapvetően a hagyományos szervezett bűnözéshez köthető, amelyek rendkívül adaptív tulajdonsággal jellemezhetőek, hiszen igen korán felismerték az ezen a területen meglevő lehetőségeket.
- **Kiberhadviselés:** Az államok közti nézeteltérésekben jelenik meg, amelynek során a felek informatikai eszközökkel támadják az ellenfél informatikai eszközeit, egyelőre még inkább a konvencionális hadviselés támogatására. [27]
- **Kiberkémkedés:** Az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzés. Napjainkban a kiberbűnözés mellett ez a legaktívabb terület. [28]
- **Kihívás:** Az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége, amelyek eredői hátrányosan befolyásolják a belső és külső stabilitást és kihatással lehetnek egy adott régió hatalmi viszonyaira. [29]
- **Kockázat:** A fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ezáltal okozott kár nagyságának a függvénye. Az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek megvalósulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek. [5]
- **Korai Figyelmeztető Rendszer (Early Warning System – EWS):** Az EWS az egyes vele egyirányúan összekapcsolt védendő elektronikus információs rendszerek hálózati forgalmának az ún. szenzorokkal történő passzív elemzésével automatizált módon azonosít kockázatokat, valamint támadásra, visszaélésre vagy ezek kísérletére utaló eseményt. [20]
- **Közigazgatás:** Azon szervezetek összessége, amelyek közhatalmat gyakorolva, az állam vagy az önkormányzat nevében közfeladatokat látnak el és jogszabályokat hajtanak végre. A helyi közügyekben az önkormányzati igazgatás, az országos jelentőségű ügyekben a központi közigazgatás jár el.
- **Központi alkalmazás (Application Server):** Olyan felhőalapú megoldás, amely gyűjti és kezeli a nagymennyiségű adatokat (Big Data) és megfelelő szoftverek segítségével felhasználja azokat. [30]
- **Kritikus információk:** Azok a saját szándékokra, képességekre, tevékenységekre vonatkozó fontos információk, amelyek a másik fél számára feltétlenül szükségesek saját tevékenységük, hatékony tervezéséhez és végrehajtásához. [20]
- **Kritikus infrastruktúra:** Azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, a közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére. [14]
- **Kritikus sérülékenység:** Kritikusnak tekinthető az a sérülékenység, amely a bizalmasságot, sértetlenséget vagy rendelkezésre állást nagymértékben sérti, illetőleg a sérülékenység távolról, könnyedén vagy hitelesítés nélkül kihasználható, tehát valós és komoly veszélyt jelent a rendszerre és az abban tárolt adatokra. [14]
- **Létfontosságú információs rendszerelem:** Európai vagy nemzeti létfontosságú rendszerelem a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené. [1]
- **Létfontosságú rendszerelem:** Létfontosságú rendszerelemnek tekinthetők azok a rendszerek, illetve rendszerelemek, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok

ellátásához (például az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális szolgáltatások biztosításához) és amelyek kiesése jelentős következménnyel járna. [31]

- **Mágneses tér:** A töltések rendezett mozgása, azaz az áram révén az áramjárta vezető körül elektromágneses erőtér jön létre. Az egy irányba, egyenletesen mozgó töltések áramlásának (azaz az egyenáramnak) a hatására állandó, míg a váltakozó irányba, változó sebességgel mozgó töltések áramlásának (azaz a váltakozó áramnak) a hatására változó mágneses tér keletkezik. Ugyanakkor a folyamat visszafelé is működik, azaz a mágneses erőtér változása erőt fejt ki a vezetőben lévő töltött részecskékre, mely erő elmozdítja e részecskéket, ezzel áramot hoz létre. [21]
- **Malware:** Az angol *malicious software* (kártékony szoftver, káros szoftver, rosszindulatú szoftver) összevonásából kialakított mozaikszó. Rosszindulatú szoftvernek tekinthetők azok a szoftverek, amelyek célja nem az információs rendszer működésének biztosítása és fenntartása, hanem bizonyos információk megszerzése, módosítása, törlése, megsemmisítése, valamint engedély nélküli tevékenységek végzése. Ezen rosszindulatú szoftverek segítségével a támadó könnyedén zavart okozhat a célszemély számára, például túlterhelheti, működésében akadályozhatja, valamint akár működésképtelenné teheti a felhasználó bármely infokommunikációs eszközét. Az esetek jelentős hányadában ezek a programok a felhasználó engedélye és tudta nélkül kerülnek az eszközeire. A malware-ek csoportjába sorolhatók a vírusok, férgek, trójai programok, kémprogramok, zsarolóprogramok, rootkitek, keyloggerek, backdoor programok és számos további rosszindulatú program. [13]
- **Minősített adat:** A minősített adat (korábbi elnevezése: államtitok vagy szolgálati titok) olyan minősítéssel védhető közérdek körébe tartozó információ, amelyről megfelelő eljárásban megállapította a minősítésre jogszabályban felhatalmazott személy, hogy az adat érvényességi időn belüli nyilvánosságra hozatala, illetéktelen személy részére hozzáférhetővé tétele veszélyezteti Magyarország biztonságát. „Szigorúan titkos", „Titkos", „Bizalmas" és „Korlátozott terjesztésű" jelzéssel ellátott dokumentumok minősített adatot tartalmaznak, melyek szándékos felhasználása, nyilvánosságra hozatala bűncselekmény. [5]
- **Mozgási indukció:** A mágneses mező és valamely vezető anyag egymáshoz képesti, a mágneses erővonalakat metsző elmozdulásakor mozgási indukcióról beszélünk. A mozgási indukció a feszültség létrehozásának mozgással történő módja, a villamos energia előállításának, a generátorok működésének az alapja. [21]
- **NAIH:** Nemzeti Adatvédelmi és Információszabadság Hatóság: az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság, melynek feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének felügyelete.
- **NEIH:** Nemzeti Elektronikus Információbiztonsági Hatóság, amely az elektronikus információbiztonsági jogszabályokban előírt követelményeknek való megfelelőség ellenőrzésének letéteményese. A hatóság egyik legfontosabb feladatként elbírálja az Ibtv. hatálya alá tartozó elektronikus információs rendszerek biztonsági osztályba sorolását, valamint ellenőrzi az elektronikus információs rendszerek biztonsági osztályba és a szervezetek biztonsági szintbe sorolására vonatkozó jogszabályi követelmények teljesülését. A rendelkezésre álló információk alapján kockázatelemzést végez és az éves ellenőrzési terv alapján az érintett ügyfeleknél ellenőrzi az információbiztonsági követelményeknek való megfelelést. Ezen túlmenően a hatóság elrendeli az ellenőrzés során feltárt vagy más módon tudomására jutott biztonsági rések elhárítását és ellenőrzi a helyreállító intézkedés eredményességét. [14]
- **Nemzeti Kiberbiztonsági Koordinációs Tanács:** Az e-közigazgatásért felelős miniszter (jelenleg a belügyminiszter) által vezetett Nemzeti Kiberbiztonsági Koordinációs Tanács a Kormány javaslattevő, véleményező szerveként gondoskodik az Ibtv. hatálya alá tartozó szervezetek információbiztonsági tevékenységeinek összehangolásáról. [14]

- **Nemzeti Kibervédelmi Intézet:** A kiberfenyegetések okozta kihívásokra reagálva, a kiberbiztonság növelése, az egységes és hatékony, párhuzamosságokkal kevésbé tagolt kibervédelmi struktúra megteremtése érdekében jött létre a Nemzeti Kibervédelmi Intézet (a továbbiakban: NKI). Az NKI legfőbb feladata és célja, hogy Magyarország egy összehangolt, szervezett tevékenység keretében legyen képes a modern kor egyik legnagyobb kihívásának, a kiberbiztonság megteremtésének és erősítésének az élharcosa és a kibervédelem letéteményese lenni, a globális és a hazai kibertérből érkező fenyegetéseket hatékonyan kezelni, azok megelőzésére szakszerű segítséget nyújtani. [14]
- **Nyugalmi indukció:** El nem mozduló, de változó mágneses mező és el nem mozduló vezető között megvalósuló indukció esetén nyugalmi indukcióról beszélünk. Ebben az esetben az el nem mozduló, de időben változó áram által létrehozott elektromágneses erőtér változó mágneses erővonalai – azaz az időben változó fluxus – révén jön létre az indukció. [21]
- **Okos mérés (Smart metering):** Az okos mérési rendszerek lehetőséget adnak arra, hogy a szolgáltatók és a hálózatüzemeltetők a végfogyasztókra lebontva képesek egyedi adatszolgáltatásra. [30]
- **Okosotthon (Smart Home):** A felhasználó otthoni készülékei (Smart Appliencies) valamilyen hálózati kapcsolat révén kommunikálnak egy központi vezérlő/szabályozó egységgel. Ennek eredményeként a felhasználói készülékek működése valamilyen szintű „intelligenciával" van felruházva. [30]
- **Online piactér:** Olyan digitális szolgáltatás, amely a 2013/11/EU Európai Parlamenti és Tanácsi irányelv (18) 4. cikke (1) bekezdésének a) és b) pontjában meghatározott fogyasztók és/vagy kereskedők számára lehetővé teszi, hogy az online piactér weboldalán vagy valamely kereskedőnek az online piactér által nyújtott számítástechnikai szolgáltatásokat felhasználó weboldalán keresztül online adásvételi vagy szolgáltatási szerződéseket kössenek. [9]
- **Ransomware (zsarolószoftver):** Célja egy adott infokommunikációs eszközhöz vagy információs rendszerhez hozzáférve olyan információk megszerzése, amelyek zsarolás alapját szolgálhatják. A zsarolóprogramok megszakítják egy információs rendszer működését, korlátozva a felhasználót az eszköz használatában, ezt követően a támadó egy zsaroló üzenetben közli az áldozattal, hogy bizonyos összeg fejében visszaállítja az eszközt vagy rendszert a korábbi állapotra. Abban az esetben, ha a célszemély nem teljesíti a támadó kérését, akkor a zsaroló kiterjeszti a fizetésre rendelkezésre álló időt vagy törli az adatokat a felhasználó infokommunikációs eszközéről. [32]
- **Rendelkezésre állás elve:** Annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak. [5]
- **Scareware (pánikprogram):** Álvírusirtók és egyéb más hamis biztonsági termékek csoportja, összefoglaló nevükön scareware-ek. Ahogyan az elnevezésük is utal rá, ezek a kártevők valamilyen vírusirtó programnak, esetleg biztonsági frissítésnek vagy más biztonsági terméknek álcázzák magukat. Általános jellemzőjük, hogy ingyenesek (legalábbis kezdetben, míg meg akarják győzni a felhasználót a „teljes verzió" megvásárlásáról), és semmilyen, vagy legalábbis minimális, víruseltávolító képességgel sem rendelkeznek – viszont annál több kártékony programot töltenek le a számítógépre. [17]
- **Sértetlenség elve:** Az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyezik, az adat az elvárt forrásból származik, azaz hiteles és az adat származása ellenőrizhető, azaz eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. [5]
- **Sérülékenység:** Az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat. [5]
- **Sérülékenységvizsgálat:** Az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása. [5]

- **Social engineering (pszichológiai befolyásolás):** Az emberi tényező kihasználható tulajdonságaira, az emberi hiszékenységre építő támadási forma, olyan technikák és módszerek összessége, amely az emberek befolyásolására, manipulálására alapozva teszi lehetővé bizalmas információk megszerzését vagy éppen egy kártékony program terjedését és működését. [17]
- **Súlyos biztonsági esemény:** Olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek. [14]
- **Számítógépes eseménykezelő központ (CERT/CSIRT):** Az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)]. [33]
- **Számítógépes féreg:** Egy számítógépes vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak, illetve válnak részeivé, addig a férgeknek nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket. [5]
- **Személyes adat:** Az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. [34]
- **Szolgáltatásmegtagadásos támadás:** Az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit vagy valamilyen speciális protokolltulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógéprendszer vagy akár a számítógéphálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. [5]
- **Stuxnet:** A kártevő még 2010 nyarán bukott le Iránban, Busehr (Bushehr) város erőművének egyik számítógépén. Akkor mintegy százezer számítógépet sikerült megfertőznie. Csak az országban legalább 45 ezer felügyeleti számítógép és szerver hordozta a vírust. Az már a felfedezés utáni első elemzések során kiderült, hogy a Stuxnetet ipari folyamatirányító rendszerek ellen fejlesztették ki. A Stuxnet végső célja ipari vezérlő rendszerek automatikus folyamatainak újraprogramozása volt. [35]
- **TCP/IP:** A TCP/IP betűszó az angol Transmission Control Protocol/Internet Protocol (átviteli vezérlő protokoll/internetprotokoll) rövidítése, mely az internetet felépítő protokollstruktúrát takarja. Nevét két legfontosabb protokolljáról kapta, a TCP-ről és az IP-ről. [22]
- **Teljes körű védelem:** Az elektronikus információs rendszer valamennyi elemére kiterjedő védelem. [5]
- **Trójai progam:** Egy olyan malware program, amely nem próbálja magát lemásolni, hanem inkább úgy tesz, mintha egy legális szoftver lenne és a felhasználót veszi rá a telepítésre. A nevét a görög mitológiából kapta, mivel ártalmatlan szoftvernek adja ki magát, de valójában rosszindulatú kódot rejt. A közhiedelemmel ellentétben egy trójai nem feltétlenül tartalmaz rosszindulatú programkódot, azonban a többségük tartalmazza az úgynevezett *hátsó kapu* telepítését, ami a fertőzés után biztosítja a hozzáférést a céleszközhöz. Ezek a programok

látszólag vagy akár valójában is hasznos funkciókat látnak, de emellett végrehajtanak olyan nem kívánt műveleteket is, amelyek adatvesztéssel járnak, például adatokat módosítanak könyvtárakat vagy akár adatállományokat törölnek. [13]

- **Tűzfal:** Olyan kiszolgáló eszköz (számítógép vagy program), amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek annak érdekében, hogy az illetéktelen behatolásoknak ezzel is elejét vegyék. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom, tartalom ellenőrzését is. [36]
- **Üzletmenet-folytonosság tervezés:** Az informatikai rendszer rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek. (Ang.: Business Continuity Planning, rövidítve: BCP). [5]
- **Válságkommunikáció:** Tulajdonképpen nem más, mint a hatóságok, a szervezetek, a média és az érdekelt személyek, illetve csoportok közötti információcsere, amely a válságesemény előtt, alatt és után történik. Az információáramlás három dolog körül összpontosul: a tényleges válság, a válság kezelésének folyamata, a válság (különféle közvéleménycsoportokban és különböző szintű nyilvánosságokban kialakuló) képe. [37]
- **Védelmi intézkedések:** Kockázatok csökkentésére, a védendő rendszerek biztonsági szintjének emelésére meghatározott intézkedések, amelyek lehetnek logikai, fizikai és adminisztratív jellegűek. [5]
- **Vezeték nélküli személyi hálózat (WPAN):** A vezeték nélküli személyi hálózat célja tipikusan egy adott felhasználó közvetlen környezetében, néhány méteres távolságon belül levő intelligens eszközök összekötése egy rádiós interfész segítségével. [30]
- **Villamos erőtér:** Az elektromosan töltött részecskék és testek erőhatást gyakorolnak egymásra. Az azonos töltésűek taszítják, a különböző töltésűek vonzzák egymást. A nyugalomban lévő töltések közötti erővonalak terét villamos erőtérnek nevezzük. [21]
- **Vírus:** A vírus olyan rosszindulatú program, amely saját programkódját fűzi hozzá egy másik programhoz, illetve azáltal, hogy elhelyezi a másik programban saját másolatait, annak segítségével szaporodik, de más programok megfertőzésére is képes. A vírusok a rendszerbe a felhasználó engedélye nélkül kerülnek be, általában valamilyen adathordozó eszköz (pendrive, CD, DVD, SD-kártya, merevlemez, MP3- és videólejátszó, mobiltelefon stb.) vagy akár hálózati kapcsolat (internet) segítségével. Ezen vírusok károsíthatják, illetve törölhetik a számítógépek vagy egyéb infokommunikációs eszközök adatait, de akár a merevlemez tartalmát is törölheti vagy módosíthatja, valamint a különféle levelezőprogramok segítségével továbbíthatják is a vírust más eszközökre. Fontos, hogy nem csak adathordozó eszközök által terjedhet, hanem elektronikus levelezés során az üzenetek csatolmányaként vagy akár az internetről letöltött tartalmakon, dokumentumokon keresztül is. [13]
- **Virtuális magánhálózat (VPN):** Olyan logikai hálózat, amelyben a nyilvános hálózat egyes végpontjai biztonságos átviteli csatornán keresztül vannak összekapcsolva és így a nyilvános hálózaton belül védett kommunikációt valósít meg. [5]
- **Zárt védelem:** Az összes számításba vehető fenyegetést figyelembe vevő védelem. [5]

4.1. A fogalmak forrásjegyzéke

{1} *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.*

{2} Nemzeti Adatvédelmi és Információszabadság Hatóság: *Adatvédelmi Értelmező Szótár*. Forrás: https://www.naih.hu/adatvedelmi-szotar.html (utolsó letöltés: 2018.03.22.)

{3} Muha L. – Krasznay Cs. (2014): *Az elektronikus információs rendszerek biztonságának menedzselése.* Nemzeti Közszolgálati Egyetem, Budapest.

{4} *Az Európai Parlament és a Tanács 2002/65/EK irányelve (2002. szeptember 23.) a fogyasztói pénzügyi szolgáltatások távértékesítéssel történő forgalmazásáról, valamint a 90/619/EGK tanácsi irányelv, a 97/7/EK irányelv és a 98/27/EK irányelv módosításáról.*

{5} Muha L. (2004): *Fogalmak és definíciók.* In. Az informatikai biztonság kézikönyve. URL: http://lmuha.hu/defins.html (utolsó letöltés: 2018.03.22.)

{6} Molnár A. (2019): *Az Európai Unió kiberbiztonsággal kapcsolatos tevékenysége*, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

{7} Ságí G. (2017): *Informatikai rendszer támadási folyamata.* Műszaki Katonai Közlöny, URL: http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2017_3sz/015_Sagi_Gabor.pdf (utolsó letöltés: 2018.03.24.)

{8} Pongrácz P. (2019): *Kibertámadások villamosenergetika környezetben*, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

{9} Tikos A. (2019): *A magyar kibervédelemmel kapcsolatos szabályozás aktuális kérdései*, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

{10} Rédecsi M. – Tóth G.: (2013) *Android*. URL: http://nyelvek.inf.elte.hu/leirasok/Android/index.php?chapter=1 (utolsó letöltés: 2018.03.24.)

{11} Gyurák G. (2015): *Informatikabiztonság I.* Pécsi Tudományegyetem Műszaki és Informatikai Kar, Pécs.

{12} *A kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) Korm. rendelet.*

{13} Haig Zs. – Kovács L. (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. URL: http://hdl.handle.net/11410/285 (utolsó letöltés: 2018.03.24.)

{14} Marsi T. (2018): *A célzott támadások és megelőzésük sérülékenységvizsgálattal.* In. Célzott támadások. Dialóg Campus Kiadó, Budapest.

{15} *A Big Data a hivatalos statisztikában*. 2016. URL: https://www.elte.hu/content/a-big-data-a-hivatalos-statisztikaban.e.3833 (utolsó letöltés: 2018.03.24.)

{16} Mátrai J. (2016): *Azonosítás vagy személyazonosság. Avagy biometrikus azonosítás*. URL: http://arsboni.reblog.hu/azonositas-vagy-szemelyazonossagavagy-biometrikus-azonositas (utolsó letöltés: 2018. 07. 04.)

{17} Oroszi E. (2008): *Social Engineering.* Budapesti Corvinus Egyetem, Budapest.

{18} Bonnyai T. (2019): *Kritikus információs infrastruktúra védelem*, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

{19} Kaczur G. (2018): *Spearphishing.* In. Célzott támadások. Dialóg Campus Kiadó, Budapest.

{20} Marsi T. (2019): *Incidenskezelés kritikus infrastruktúrák esetén*. In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

{21} Görgey P. (2019): *A villamosenergia-szektor mint kritikus infrastruktúra*, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

{22} Danyek M. (2019): *A villamosenergia szektor mint kritikus információs infrastruktúra,* In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

{23} Emmanuel Carabott (2011): *Hacking Motivations – Hactivism*, URL: http://www.gfi.com/blog/hacking-motivations-hacktivism/ (utolsó letöltés: 2018.03. 22.)

{24} Solymos Á. (2018): *Identitás- és jogosultságkezelés, mint a célzott támadások megelőzésének technológiai eszköze.* In. Célzott támadások. Dialóg Campus Kiadó, Budapest.

{25} László G. (2014): *Kockázatértékelés, kockázatmenedzsment*. URL: http://vtki.uni-nke.hu/uploads/media_items/kockazatertekeles_-kockazatmenedzsment.original.pdf (utolsó letöltés: 2018.03.22.)

{26} Kóbor Á. (2014): *Mi az a „dolgok internete”?* URL: https://ithub.hu/blog/post/Mi_az_a_dolgok_internete/ (utolsó letöltés: 2018.07.03.)
{27} Cser O. (2018): *Célzott támadás a pénzügyi szektor ellen.* In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{28} Krasznay Cs. (2012): *A polgárok védelme egy kiberkonfliktusban,* Hadmérnök 2012/4, URL: http://hadmernok.hu/2012_4_krasznay.pdf (utolsó letöltés: 2018.03.22.)
{29} Resperger I. (2002): Kockázatok, kihívások és fenyegetések a XXI. században. ZMNE, Az Országos Kiemelt Kutatási Tanulmányok pályázata, Budapest.
{30} Haddad R. (2019): *Okoseszközök a kritikus információs infrastruktúrákban*. In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.
{31} *A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. tv.*
{32} Yaqoob, I. – Ahmed, E. – Imran, M. (2017): *The rise of ransomware and emerging security challenges in the Internet of Things.* Computer Networks, 6 September (2017), URL: https://doi.org/10.1016/j.comnet.2017.09.003 (Utolsó letöltés: 2017.10.20.)
{33} Bodó A. – Zámbó N.: *A közreműködők kötelezettségei a célzott támadások elhárításában az ibtv. szerint.* In. Célzott támadások. Dialóg Campus Kiadó, Budapest
{34} Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény.
{35} Sebők V. (2018): Új típusú támadások az államok és szervezetek ellen. In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{36} Gyaraki R. (2018): *Belső munkatársak jelentette kockázatok a célzott informatikai támadásokban.* In. Célzott támadások. Dialóg Campus Kiadó, Budapest.
{37} Kriskó E. (2019): *Válságkommunikáció kibertámadás esetén*, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

A Nemzeti Közszolgálati Egyetem kiadványa.

Kiadó:
Nemzeti Közszolgálati Egyetem;
Államtudományi és Közigazgatási Kar
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert Rektorhelyettes

Címe:
1083 Budapest, Üllői út 82.

Olvasószerkesztő:
Zsoldos Sándor

Tördelőszerkesztő:
Friebert Máté

ISBN 978-963-498-238-8 (PDF)