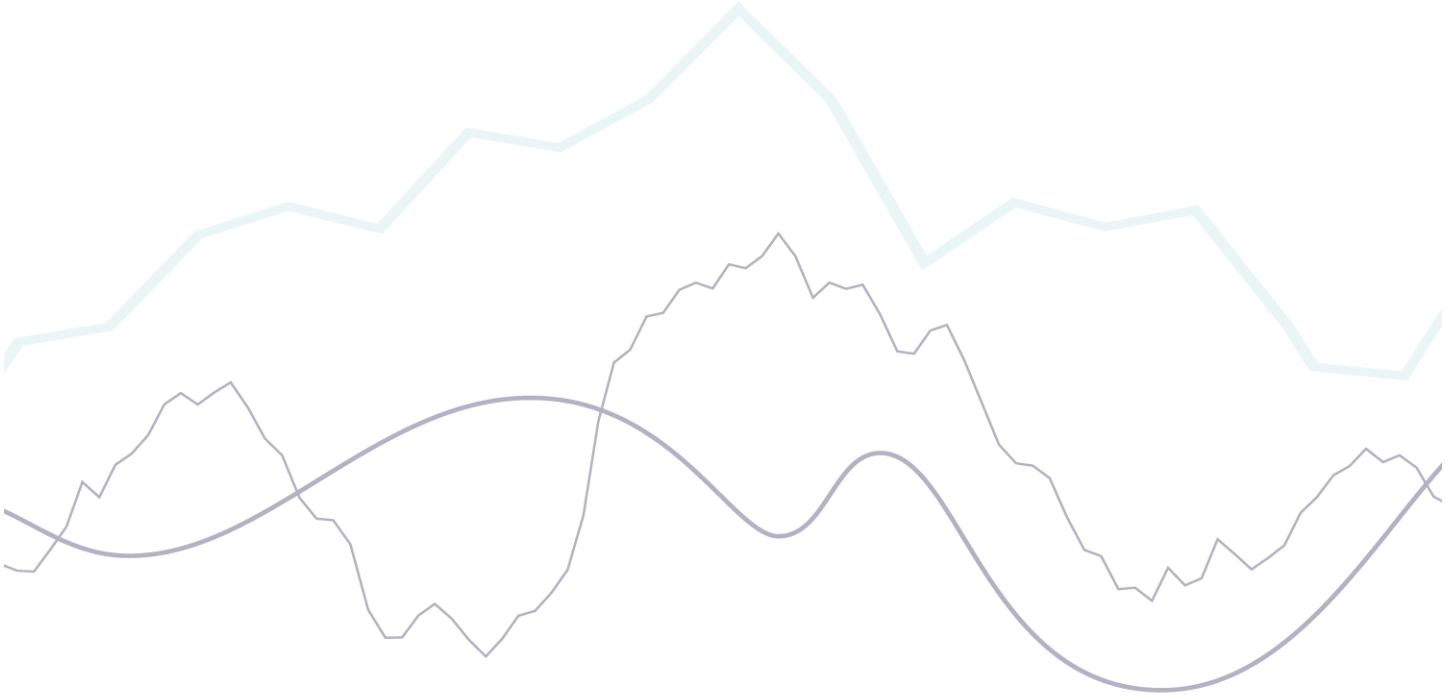
ÁLLAMI SZÁMVEVŐSZÉK

ELEMZÉS

Állami kiberbiztonság

2022.



ÁLLAMI SZÁMVEVŐSZÉK

ELEMZÉS

Állami kiberbiztonság

ÁSZ ÁLLAMI SZÁMVEVŐSZÉK ELNÖK

Engedélyező:

Domokos László
elnök

Szerkesztő:

DR. CSERNYÁK SZABOLCS projektvezető

Az elemzés elkészítését felügyelte:

MAKKAI MÁRIA felügyeleti vezető

Készítették:

DR. CSERNYÁK SZABOLCS projektvezető

NOÉ ANTAL számvevő

BARITSA ORSOLYA számvevő

Az Elemzés az interneten a www.asz.hu oldalon olvasható.

Kiadja az Állami Számvevőszék

EL-3500-006/2022.

TARTALOMJEGYZÉK

VEZETŐI ÖSSZEFOGLALÓ

Az Alaptörvényben rögzítetten „a polgárnak és az államnak közös célja a jó élet, a biztonság, a rend, az igazság, a szabadság kiteljesítése”. Ezen cél nem érhető el a magyar kibertér és ezáltal a nemzeti adatvagyon védelme nélkül. A mai korban az online világ megkerülhetetlen az államháztartás, a piaci szféra szervezetei és az állampolgárok szintjén. Nincs olyan intézmény és ember Magyarországon, ki így vagy úgy ne legyen kapcsolatban a kibertérrel.

A kibertérből eredő támadások, biztonsági események száma világszerte és hazánkban is növekvő tendenciát mutat. A kiber-incidensek számos módon valósulhatnak meg, irányulhatnak akár alapvető közintézmények (egészségügyi, szociális, oktatási), infrastruktúrák (utak, közvilágítás, gátak), közszolgáltatások (vízellátás, áramellátás, távfűtés) működtetésének ellehetetlenítésére.

Az elemzés a magyar kibertér, mint létfontosságú infrastruktúra védelmére, a kiberbiztonság megteremtésében érdekelt felek közül a közszféra, azaz az állami kiberbiztonság témakörére fókuszál, a vonatkozó jogszabályok és szakirodalom áttekintésével, az állami kiberbiztonság egyes intézményi szereplői, a felügyelt elektronikus információs rendszereket működtető szervezetek (a továbbiakban: érintett szervezetek) tekintetében a kibervédelmi „tudatosság” bemutatásával.

A hazai kibervédelem alapját, hosszútávú cél és feladatrendszerét meghatározó stratégiák deklarálják, hogy Magyarországon a kibertér szabadságának és biztonságának szavatolása a kormányzat, a tudományos, a gazdasági és a civil szféra közös felelősségvállaláson alapuló, szoros együttműködésével, összehangolt tevékenységével valósulhat meg.

A vonatkozó törvényi és kapcsolódó végrehajtási rendeleti szabályozás a stratégiai célokkal és feladatokkal összhangban megteremtette az állami kibervédelem jogszabályi keretrendszerét és meghatározta a szervezetek hatás-és feladatköreit.

A magyar kibertér védelme kapcsán az intézményrendszer közös felelősségvállalása mellett az egyes érintett szervezeteknek is önálló felelőssége van. Az elektronikus információs rendszerek biztonságáért az üzemeltető, működtető állami szerv a felelős, ami egyben a kiberbiztonságért való szervezeti felelősséget is jelenti. A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről. A társadalmi feladatok folyamatos ellátásához nélkülözhetetlen, úgynevezett létfontosságú rendszerelemek (pl. energia, közlekedés, ivóvíz-ellátás, egészségügyi, pénzügyi piaci infrastruktúrák) körének bővülése magával hozta az állami kibervédelem intézményrendszerében a felügyelt információs rendszerek számának bővülését is.

A COVID-19 világjárvány kapcsán a távmunka terjedésének fokozódása kiberbiztonsági szempontból új kihívásokat jelentett. A távmunkarendszerek használatához új digitális ismeretek és képességek megszerzése volt szükséges. Kiberbiztonsági szempontból fokozottabb kockázati kitettséget eredményezett a számítástechnikai eszközök magáncélú használata, továbbá az alkalmazottak saját tulajdonában álló IT eszközök munkavégzési céllal történő használata is. Ezt erősíti az állami és önkormányzati szervezeteket érintő, a kiberbiztonsági tudatosság kérdőíves felmérés eredménye is.

A szervezeti szintű kiberbiztonság attól lesz „élő” és eredményes, ha az egyes szervezetek tudatosan járnak el és aktívan tesznek a kibervédelem és biztonság megteremtéséért. Az elemzés bemutatja az állami kiberbiztonság rendszerében az Ibtv. előírásai alapján az ehhez rendelkezésre álló eszközöket.

AZ ELEMZÉS HÁTTERE, CÉLJA ÉS MÓDSZERE

Az elemzés háttere

A XXI. század elején lezajló digitális fejlődés következtében a gazdasági folyamatok, az állampolgárok egymás közötti kommunikációja, a különféle intézményekkel történő kapcsolattartás nagyrésze is ma már egyre inkább az online térben zajlik. A hálózatba kapcsolt digitális eszközöknek, rendszereknek a fizikai és virtuális térben történő egyidejű használata mára az élet mindennapi részévé vált. Ezzel párhuzamosan egyre inkább hangsúlyos fenyegetést jelentenek az elektronikus rendszerek és hálózatok sérülékenységére kockázatot jelentő, a kibertérben felmerülő – ma már a világ bármely pontjáról érkező – támadások, az úgynevezett kiberműveletek.

A digitális világban megjelenő új és folyamatosan változó fenyegetések különböző formái az állami intézményrendszereket, a piaci szereplőket, a társadalom széles rétegeit hátrányosan érinthetik. Ilyen fenyegetettség lehet például, ha illetéktelenek az állampolgárok személyes adataihoz férnek hozzá, álhírek terjednek a különféle közösségi médiafelületeken, hackertámadás miatt nem érhetők el e-közigazgatási vagy banki szolgáltatások. Az ellenük való védekezés nemzeti és nemzetközi szinten is fokozott kihívást jelent a kiberbiztonság megteremtésében érdekelt felek („stakeholder”-ek), így az állam, a közszféra szervezetei, valamint a gazdasági szereplők számára.

Az elemzés célja, fókuszterületei és módszere

Az elemzés célja a magyar kibertér védelmét biztosító állami intézményrendszer felépítésével, működésével, finanszírozásával, illetve a terület jogi és stratégiai keretrendszerével kapcsolatos helyzetkép bemutatása. Továbbá azon lehetőségek feltárása, amelyek hozzájárulhatnak mind a felügyeleti intézményrendszer, mind az érintett szervezetek szintjén a magyar kibertér védelmének erősítéséhez.

Az állami kibervédelem tárgya a kiberbiztonság. A kiberbiztonság az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) meghatározását figyelembe véve nem egyenlő az információ-biztonsággal, annál egy jóval szélesebb körű eszközrendszert jelent.

A **kiberbiztonság**, vagy más néven digitális biztonság a digitális adatok, készülékek, eszközök és folyamatok védelmére irányuló lépések összessége. A kiberbiztonság hazai jogszabályi fogalma szerint a kibertérben létező kockázatok „elfogadható szintjének” megteremtését célzó, széleskörű — politikai, jogi, gazdasági, oktatási, illetve tudatosságnövelő, valamint technikai elemeket is alkalmazó —eszközrendszer, amely a társadalmi és gazdasági folyamatok zavartalan működését hivatott biztosítani. A kiberbiztonság tehát **nem egy konkrétan elérendő cél**, hanem egy **folyamatos törekvés, állapot**, a védelem pedig az erre irányuló tevékenységek rendszere. A kiberbiztonság a szervezetek információ-biztonságával szoros összefüggésben áll, ugyanakkor több is annál. Az Ibtv. az állami kiberbiztonság intézményrendszerében a kibertér védelme érdekében deklarálja az elektronikus információs rendszerek vonatkozásában az informatikai védelem szervezeti szintű alapvető követelményeit. Az Ibtv. preambuluma szerint „*társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme*”. Mindez rámutat arra, hogy az állami kiberbiztonság intézményrendszerében a kiberbiztonság fundamentumát a szervezeti szinten megfelelően kezelt információbiztonság képezi. Megfelelő kiberbiztonság megalapozott szervezeti szintű információbiztonság nélkül tehát nem értelmezhető.

A kibervédelem széles témakört ölel fel, amely az állami és a piaci szférát is érinti. Az elemzés nézőpontját az állami szektor kibervédelmi rendszerének (központi és szervezeti szint) feltérképezése képezi. Az elemzés a szervezeteken és az állami informatikai rendszereken kívülről jövő fenyegetettségek elleni védelmi megoldásokra fókuszál és nem az egyes szervezetek belső információbiztonsági intézkedéseire vagy állami informatikai infrastruktúrán belül jelentkező kockázatokra.

Az elemzés fókuszterületei:

- a vonatkozó hazai jogi szabályozási rendszer – kiegészülve az EU-s keretszabályokkal, irányelvekkel – áttekintése;
- a hazai felügyeleti intézményrendszer és feladatai bemutatása;
- az állami kiberbiztonság intézményi rendszerében az érintett államháztartási szervezetek kiberbiztonsági helyzetképének bemutatása;
- a kialakított szabályoknak, irányelveknek a szervezetek általi érvényesítésének értékelése.

A kibervédelmet érintően egzakt, önmagában vagy egyéb országokkal összevetve értékelhető mutatószámok nem állnak rendelkezésre, ezért az elemzés során a mércét, illetve kritériumot a stratégiai elvek és célok jelentik.

Az elemzés adatforrásai elsődlegesen a jogszabályok (EU és hazai), és stratégiai dokumentumok, hazai és nemzetközi értékelő jelentések voltak. További adatforrást jelentettek a témában megjelent, nyilvánosan hozzáférhető dokumentumok és elemzések, a KSH nyilvánosan elérhető statisztikai adatai, a hazai és nemzetközi szakirodalom, valamint az állami kiberbiztonsági intézményrendszer felügyeleti szervezetét érintően a Nemzetbiztonsági Szakszolgálat által rendelkezésre bocsátott adatok.

A kiberbiztonsági tudatosság intézményi szintű felmérése érdekében az elemzés keretében 24 kérdésből álló kérdőívvel kerestünk meg egyes, az államháztartás központi alrendszerében az elektronikus ügyintézés és bizalmi szolgáltatások szabályai szerint közhiteles nyilvántartások vezetésére kötelezett szervezeteket, továbbá az államháztartás önkormányzati alrendszerében véletlenszerűen kiválasztott nagyobb (megyei jogú) és kisebb (5-20 ezer lakosú) önkormányzatokat, illetve az azokhoz tartozó önkormányzati hivatalokat. A felmérés nem volt reprezentatív, az állami kiberbiztonság intézményi rendszerében az érintett államháztartási szervezetek átfogó kiberbiztonsági helyzetképének bemutatását nem célozta.

ELEMZÉS

1. A vonatkozó hazai szabályozási keretrendszer bemutatása

1.1. Alaptörvényi keretek

A kiberbiztonság megteremtésében és fenntartásában az államnak is hangsúlyos szerepe van, az állam közvagyont (nemzeti adatvagyont) érintő intézményvédelmi kötelezettsége az Alaptörvényből levezethető. A kiber[1] fenyegetettségek, kibertámadások, kiberterrorizmus akadályozhatják az Alaptörvényben meghatározott értékeket úgy, mint a biztonság, a rend, igazság és szabadság kiteljesedését.

Az Alaptörvény rögzíti, hogy **Magyarország védelmezi állampolgárait**. Ez a védelem társadalmi szinten megtestesül abban, hogy Magyarország a béke és a biztonság megteremtése és megőrzése, valamint az emberiség fenntartható fejlődése érdekében együttműködésre törekszik a világ valamennyi népével és országával. Az állam polgárai részére az Alaptörvény értelmében biztosítja az alapvető közintézmények (egészségügyi, szociális, oktatási), infrastruktúrák (utak, közvilágítás, gátak), közszolgáltatások (vízellátás, áramellátás, távfűtés) működtetését. Ezen intézményrendszer védelmének fenntartása egyben a társadalmi közrend fenntartását és az egyén biztonságát is szolgálja. **Ez ma már a biztonságos kibertér megteremtése nélkül nem valósítható meg, amelyben fontos szerepe van annak, hogy a védelem kiterjedjen a kiberkockázatok kezelésére, elhárítására is.**

1.2. Az állami kibervédelmet meghatározó szakpolitikák, stratégiák

Az állami kibervédelem hazai jogi szabályozási rendszerének irányai stratégiai dokumentumokban kerültek kijelölésre. A kijelölt célok alapán került sor az állami kibervédelem intézményi rendszerének kialakítására és jogszabályban történő rögzítésére. A kibervédelem témája számos nemzeti szakpolitikában megjelent.

Nemzeti Biztonsági Stratégia

A kiberbiztonság a 2012-ben közzétett, majd 2020-ban megújított **Magyarország Nemzeti Biztonsági Stratégiájában** hangsúlyos területként szerepel. A dokumentum fokozott veszélyként definiálja az informatikai- és telekommunikációs hálózatok, kormányzati gerinchálózatok működésének, az alapvető szolgáltatások, kritikus infrastruktúrák működésének megzavarását, vagy a tudományos fejlődés mindenki számára elérhető eredményeinek terroristák kezébe jutását. A 2020. évben megújított biztonsági stratégia rögzíti, hogy a felhasználók megfelelő információbiztonsági tudatossága a kiberincidensek megelőzésének egyik kulcseleme, ugyanakkor általános jelenségként emeli ki a felhasználók információbiztonsági tudatosságának alacsony szintjét. A megújított stratégia az átfogó feladatok között rögzíti a kormányzati infokommunikációs rendszerek, a nemzeti létfontosságú információs infrastruktúra, a minősített információk és a nemzeti adatvagyon védelmének erősítését.

Stratégia kiberbiztonsági relevanciája: A kiberbiztonság területét már a 2012. évi stratégia a Magyarországot érintő biztonsági fenyegetések, kihívások között azonosította, annak deklarálásával, hogy a megfelelő szintű kiberbiztonság garantálására Magyarországnak is készen kell állnia. Elsődleges feladatként rögzíti a kibertérben jelentkező fenyegetések és kockázatok rendszeres felmérését és priorizálását, a kormányzati koordináció erősítését, a társadalmi tudatosság fokozását, valamint a nemzetközi együttműködési lehetőségek kiaknázását.

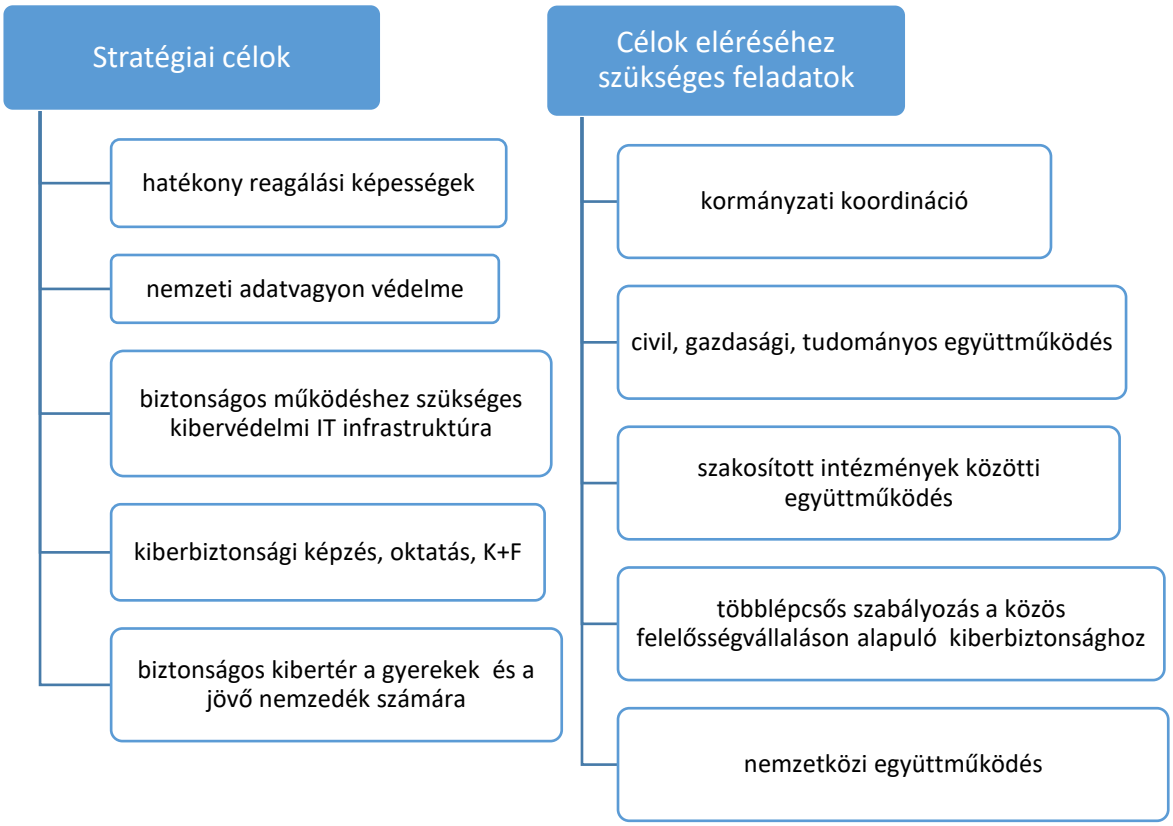
Nemzeti Kiberbiztonsági Stratégia

A Magyarország Nemzeti Biztonsági Stratégia kiberbiztonság témájú pontjainak részletes kifejtéseként a 2013. évben került elfogadásra a **Nemzeti Kiberbiztonsági Stratégia, amelynek** alapvető elvárása, hogy a kibertér nyújtson biztonságos és megbízható környezetet a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.

A dokumentum épít az állami és a nem állami szereplők közötti együttműködésre, Magyarország nemzetközi kapcsolatrendszerére, továbbá a kibervédelmet a védelmi politika szerves részeként tekinti. A Nemzeti Kiberbiztonsági Stratégia kulcsszerepet szán a **kiberbiztonsági tudatosság** fejlesztésének. Deklarálja, hogy a kibervédelem a megelőzésre épülő hatékony védelmi intézkedések útján lehetséges. Ennek kapcsán elsődleges célként rögzíti a kibertérből érkező fenyegetések és az ezzel járó **kockázatok kezelésének**, az ehhez szükséges kormányzati **koordináció és eszköztár erősítését**. A stratégia hangsúlyozza, hogy Magyarországon a kibertér szabadságának és biztonságának szavatolása a kormányzat, a tudományos, a gazdasági és a civil szféra **közös felelősségvállaláson** alapuló, szoros együttműködésével, összehangolt tevékenységével valósulhat meg. A stratégiai célok és e célok eléréséhez szükséges feladatokat az **1. ábra** szemlélteti.

A stratégia értelmében az állami kibervédelem intézményrendszerének összehangoltan, hatékony együttműködés és közös felelősségvállalás alapján, kockázati alapon szükséges működnie, folyamatosan felmérve, értékelve a kockázatokat és azokhoz igazítva a kontrollokat annak érdekében, hogy a külső és belső környezeti változásokra hatékonyan tudjon reagálni. A nemzetgazdasági szinten fennálló kockázatok mérséklése edukációs folyamattal – a kibervédelem szükségességének állampolgárok, intézmények, gazdasági szereplők részére történő tudatosításával – hatékonyan csökkenthető.

1. ábra - A Nemzeti Kiberbiztonsági Stratégiában meghatározott főbb stratégiai célok és célok eléréséhez szükséges feladatokról összefoglaló



(Forrás: Nemzeti Kiberbiztonsági Stratégia alapján ÁSZ szerkesztés)

A dokumentum a **stratégiai célok eléréséhez szükséges eszközök**et az alábbiak szerint határozza meg:

- a magyar kibertér biztonságáért felelős kormányzati szervezetek számbavétele és koordinációja, a hatékony együttműködés kialakítása;
- a magyar kibertér biztonságáért felelős civil, gazdasági és tudományos szervezetek számbavétele és intézményes keretek között folyó együttműködés kialakítása;
- a létfontosságú információs infrastruktúrák és vagyonelemek, illetve a nemzeti adatvagyon számbavétele és védelmének biztosítása;
- a szakosított kormányzati intézmények működtetése;
- a szabályozási környezet biztosítása;
- a nemzetközi és regionális együttműködésekben történő részvétel, politikai, operatív és szabályozási szinten egyaránt;
- a támogatási keretrendszer kialakítása a kutatás és fejlesztés, valamint az oktatás és tudatosítás terén;
- gazdasági motivációs rendszerek megteremtése;
- a kiberbiztonsági szempontok érvényesítése az állami műszaki fejlesztési feladatok, valamint a kormányzati információs rendszerek fejlesztésével és üzemeltetésével kapcsolatos feladatok ellátása során.

Nemzeti Infokommunikációs Stratégia

A 2014-ben közzétett, 2014-2020 közötti időszakra szóló, Magyarország Nemzeti Infokommunikációs Stratégiája (NIS Stratégia) célként határozza meg az infokommunikációs hálózatok, eszközök, szolgáltatások és kompetenciák fejlesztésén keresztül az állampolgárok életminőségének, a vállalkozások versenyképességének és az állami működési hatékonyságának javítását. A NIS stratégia négy alappillére – a digitális infrastruktúra, a digitális kompetenciák, a digitális gazdaság, a digitális állam fejlesztése – mellett **megjelenik a biztonság** is, amely minden fejlesztendő területen jelen kell, hogy legyen. A biztonság célrendszere megköveteli, hogy nemzetbiztonsági, illetve a közigazgatás belső működése és az elektronikus közigazgatási szolgáltatások elérhetősége szempontjából valósuljon meg a kritikus infrastrukturális és informatikai elemek, a közigazgatási belső rendszerek és külső alkalmazások, valamint az ezekben megjelenő felhasználói adatok maximális védelme.

A stratégiában foglalt feladatok megvalósulásáról a 2016. évi **NIS monitoring jelentés** ad számot**,** amely többek között rögzíti, hogy a Kormány kiemelkedően fontosnak tartja a polgárok, a vállalkozások és a közintézmények, valamint a magyarországi digitális hálózatok kiberbiztonságának erősítését, erre tekintettel elrendelte a Nemzeti Kiberbiztonsági Stratégia felülvizsgálatát.

Hálózati Biztonsági Stratégia

A 2018. évben elfogadott **Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiája** tartalmilag a Nemzeti Kiberbiztonsági Stratégia kiegészítése és újragondolása, az abban foglaltakkal együtt funkcionál. A stratégiának az állami kiberbiztonságot érintő elemeit a **2. ábra** szemlélteti.

2. ábra - A Hálózati Biztonsági Stratégiában meghatározott, az állami kiberbiztonságot érintő főbb stratégiai pillérek és elemeik

digitális környezet iránti bizalom erősítése	digitális infrastruktúra védelmére	gazdasági szereplők támogatása
•szakmai együttműködés erősítése •biztonságtudatosság növelése •kiber-bűnüldözés fejlesztése •szakmai intézményrendszer fejlesztése	•az informatikai fejlesztések minőség menedzsmentje •kormányzati elektronikus szolgáltatások biztonságának növelése •nemzetközi együttműködés erősítése •alapvető szolgáltatások, valamint a létfontosságú infrastruktúrák védelme •kiber-védekező és reagáló képességek fejlesztése	•kutatóközpontokkal való együttműködés és a kutatás fejlesztés szerepének erősítése •hazai digitális innováció támogatása, támogatási konstrukciók kialakítása és koordinációs feladatok ellátása •versenyképes hazai tudásbázis kialakítása

(Forrás: Hálózati Biztonsági Stratégia alapján ÁSZ szerkesztés)

1.3. Állami kiberbiztonság jogi keretrendszerének kialakítása

A kibervédelemmel összefüggő stratégiák megalkotását követte az állami kiberbiztonsági intézményrendszer jogi keretrendszerének megteremtése. 2013. július 1-jével lépett hatályba az Ibtv. Az állami kiberbiztonsági intézményrendszer kialakításának szabályozására a Kormány a 2013. évben további jogszabályokban rendelkezett, így különösen a felügyeleti hatóság feladatait meghatározó NEIH rendelet, valamint az elektronikus információs rendszerek kormányzati, ágazati eseménykezelő központjainak, és a létfontosságú rendszerek és létesítmények eseménykezelő központjainak feladatait rögzítő GovCERT rendelet érdemel kiemelést.

Az Ibtv. kettős rendeltetéssel bír. Alapvetően az állam, az önkormányzatok és a közigazgatás szervezeteinek elektronikus információs rendszereiben tárolt adatok információbiztonságát védi, másrészt ezen elektronikus rendszerek kiberbiztonságára és védelmére határoz meg garanciális rendelkezéseket. Ezen rendszerek információbiztonságát, ezáltal a kibertér védelmét az Ibtv. értelmében a kockázatokkal arányosan kell megszervezni, folyamatosan biztosítva a rendszerelemek sértetlenségét és rendelkezésre állását. Az Ibtv. előírásaival érintett szervezeteknek biztosítaniuk kell az elektronikus információs rendszerben kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását, valamint azok zárt, teljes körű, folytonos és kockázatokkal arányos védelmét. A törvény és végrehajtási rendelete, az Ibtv. vhr. részletesen előírja, hogy milyen logikai, fizikai és adminisztratív intézkedéseket kell meghatározni, amelyek támogatják a megelőzést és a korai figyelmeztetést, az észlelést, a reagálást, továbbá a biztonsági események kezelését. A szükséges intézkedéseket az elektronikus információs rendszerek biztonsági osztályba sorolása alapján kell megtenni. Az elektronikus információs rendszerek biztonsági osztályba sorolása alapfeltétele a kockázatokkal arányos kibervédelem megvalósításának.

Az Ibtv. deklarálja, hogy az elektronikus információs rendszerek biztonságáért az üzemeltető, működtető állami szerv a felelős, ez egyben a kiberbiztonságért való önálló, szervezeti felelősséget is meghatározza.

A Nemzeti Kiberbiztonsági Stratégiában meghatározott feladatok és hatáskörök többségében az Ibtv-ben kerültek szabályozásra, ezek részletesen az alábbiak:

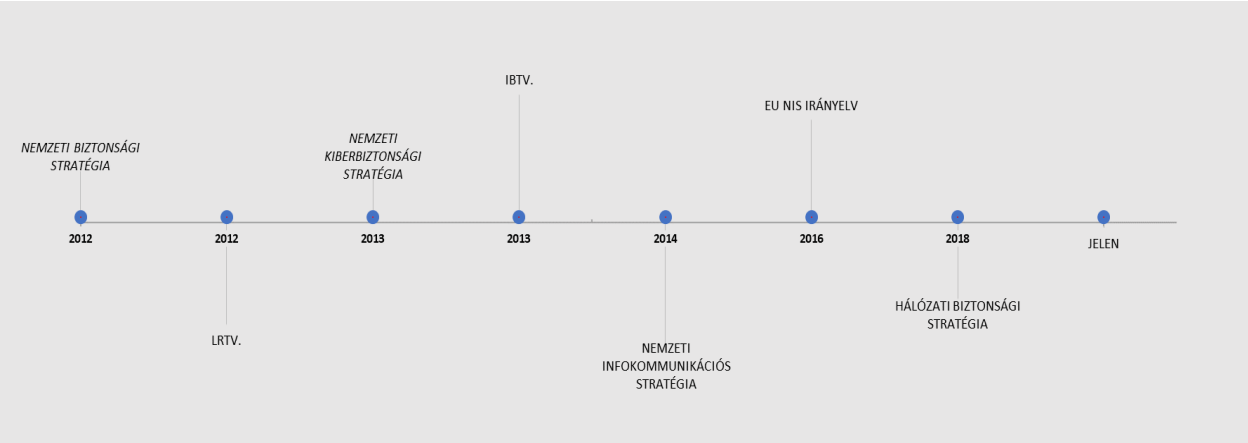
- **kiberbiztonságért felelős kormányzati szervezetek koordinációja:** Az intézményi feladatok és tevékenységek összehangolásáért az NBSZ vezetője, mint tanácsi elnök által vezetett Nemzeti Kiberbiztonsági Koordinációs Tanács felelős.
- **létfontosságú információs infrastruktúrák, a nemzeti adatvagyon védelmének biztosítása:** Az Ibtv. kiterjed az európai- és nemzeti létfontosságúnak kijelölt rendszerelemek védelmére, valamint a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói elektronikus információs rendszereinek védelmére, ezáltal a létfontosságú információs infrastruktúrák és vagyonelemek, illetve a nemzeti adatvagyon számbavétele és védelmének biztosítása is megtörtént.
- **civil, gazdasági és tudományos szervezetekkel intézményes keretek között folyó együttműködés kialakítása:** A magyar kibertér biztonságáért felelős civil, gazdasági és tudományos szervezetekkel történő kooperáció a Kiberbiztonsági Fórum működtetésével valósult meg.
- **szervezetek közötti koordináció és együttműködés:** Az intézményközi koordináció központi funkcióját az elektronikus információs rendszerek biztonsági felügyeletéért felelős hatóság, 2016. január 1-je óta a Nemzetbiztonsági Szakszolgálat látja el. A nem kormányzati szereplőkkel való együttműködésnek keretét a Nemzeti Kiberbiztonsági

Az Ibtv. és kapcsolódó végrehajtási rendeleti szabályozással az Országgyűlés és a Kormány a Nemzeti Kiberbiztonsági Stratégiában meghatározott célokkal és feladatokkal összhangban megteremtette az állami kibervédelem jogszabályi keretrendszerét, az intézményrendszer hatékony működtetésének érdekében meghatározta a szervezeteinek hatás- és feladatköreit.

Fórum és kiberbiztonsági munkacsoportok biztosítják, akik a Tanács munkáját támogatva javaslattételi joggal és véleményezési lehetőséggel élhetnek a Tanács felé.

- **szakosított kormányzati intézmények működtetése:** A Kormány az Ibtv-ben foglalt biztonsági események kezelése érdekében kormányzati eseménykezelő központot működtet, amely hatálya alá központi államigazgatási és alkotmányos szervek, kormányhivatalok, helyi és nemzetiségi önkormányzatok, hatósági igazgatási társulások, valamint a Magyar Honvédség tartozik. Az eseménykezelő központ folyamatosan elérhető 24 órás ügyeletet működtet, a biztonsági eseményeket kivizsgálja, a szervezeteknél előforduló hibákat feldolgozza, melyekről negyedévente jelentést készít a Nemzeti Kiberbiztonsági Koordinációs Tanács felé. Az állami kibervédelem intézményi stratégiai és jogi kereteit meghatározó főbb mérföldköveket a **3. ábra** szemlélteti.

3. ábra - Magyarország kibervédelme – stratégiai és jogszabályi kereteinek megalkotása idővonalon ábrázolva



(Forrás: ÁSZ szerkesztés)

1.4. Nemzetközi együttműködések és az EU jogi aktusainak viszonya a kibervédelmet érintő nemzeti stratégiához és jogalkotáshoz

Az állami kiberbiztonság megteremtése EU tagállami hatáskörbe tartozik, ettől függetlenül a nemzeti stratégiaalkotási és jogalkotási követelményekre a nemzetközi jogi keretek, követelmények és törekvések is kihatással bírnak.

A Nemzeti Biztonsági Stratégia rögzíti, hogy Magyarország nagy jelentőséget tulajdonít a multilaterális szervezetek keretein belül megvalósuló biztonságpolitikai együttműködésnek és fellépésnek, amelynek alapvető keretét a NATO- és EU-tagság jelenti. A Nemzeti Kiberbiztonsági Stratégia és a Hálózati Biztonsági Stratégia is deklarálja, hogy az Alaptörvényben megfogalmazott alapértékek (szabadság, biztonság, jogállamiság, nemzetközi és európai együttműködés) érvényesítésén túl a vonatkozó nemzeti stratégiákkal Magyarország hozzájárul a nemzetközi együttműködésből, valamint EU és NATO tagságából eredő követelmények és törekvések hazai stratégiákban és nemzeti jogalkotásban történő érvényesítéséhez.

Ennek megfelelően az állami kiberbiztonságot meghatározó stratégiák alapvetésként kezelik a 2001-ben elfogadott Budapesti Konvencióban („Convention on Cybercrime”) megfogalmazott, nemzetközileg elfogadott alapelveket. A vonatkozó stratégiák rögzítik, hogy illeszkednek a NATO Stratégiai Koncepciójához, Kibervédelmi Politikájához, valamint a NATO-csúcsok vonatkozó dokumentumaiban megfogalmazott Szövetségi kibervédelmi elvekhez és célokhoz.

Magyarország Nemzeti Kiberbiztonsági Stratégiájában meghirdetett célok az Európai Unió 2013-ban elkészült kiberbiztonsági stratégiájának céljaival összhangban vannak.

Mind az Unió, mind Magyarország stratégiai dokumentumaiban megjelenik a kiberfenyegetettségek elleni preventív védelem, mely a kockázatok felmérésére és azok mérséklésére irányul. Fontos az európai és a nemzeti szintű együttműködés, mely hatékony eszköze lehet az esetleges kibertámadások elleni védekezésnek.

Az uniós stratégiai célokkal összhangban az Európai Unió a kiberbiztonság egyes ágazati területein – az EU kiberbiztonsági rendelete kivételével – irányelvi szintű jogalkotási keretek között rendelkezett. Ezek közé tartozik a hálózati és információs rendszerek biztonságának az Unióban egységesen magas szintjét biztosító intézkedésekről szóló EU NIS irányelv. Az irányelv olyan közösségi, illetve európai uniós jogi jogalkotási aktus, amely kizárólag az elérendő célok tekintetében kötelezi az érintett tagállamot, a megfelelő eljárások és eszközök megválasztását az irányelvi keretek között átengedi a tagállamoknak. Az irányelv tagállami jogba történő átültetést, transzformációt igényel. Az EU NIS irányelv a hazai belső jogba az Ibtv-ben került törvényi szinten átültetésre.

Magyarország maradéktalanul teljesítette az EU NIS irányelvben meghatározott célokat, többek között ezek figyelembevételével alkotta meg a Hálózati Biztonsági Stratégiát, továbbá annak törvényi szintű szabályozással, az Ibtv. 2018. évi módosításával tett eleget.

2. A kiberbiztonsági intézményrendszer stratégiai irányítási, felügyeleti és operatív szintje

2.1. Stratégiai irányítás intézményrendszere

Nemzeti Kiberbiztonsági Koordinációs Tanács

A Nemzeti Kiberbiztonsági Koordinációs Tanács a Kormány javaslattevő, véleményező szerveként az állami és önkormányzati szervek elektronikus információbiztonságával összefüggő stratégiai, kormányzati koordinációs feladatokat lát el. A Tanács feladata az állami kiberbiztonság állami, közigazgatási szerveit érintően az Ibtv-ben meghatározott tevékenységeinek összehangolása, továbbá a Nemzeti Kiberbiztonsági Stratégiában meghatározott cselekvési területeken a kormányzati tevékenység koordinációjának elősegítése és a végrehajtás figyelemmel kísérése.

A Tanács elnöke a Nemzetbiztonsági Szakszolgálat vezetője. A Tanács tagjait a Kiber-irányítási rendeletben kijelölt miniszterek által delegált tagok alkotják. A Tanács tagja továbbá a Szabályozott Tevékenységek Felügyeleti Hatósága elnöke vagy az általa delegált személy, a Katonai Nemzetbiztonsági Szolgálat főigazgatója és a belügyminiszter által delegált **kiberkoordinátor**.

Nemzeti Kiberbiztonsági Fórum

A Tanács tevékenységét a kiberkoordinátor, valamint a kiberbiztonsági munkacsoportok és a nem kormányzati szereplőkkel való együttműködésnek keretet biztosító **Nemzeti Kiberbiztonsági Fórum** támogatja. A Tanács a Fórum javaslatainak és véleményének figyelembevételével készíti el a Nemzeti Kiberbiztonsági Akciótervet, amelyet évente felül kell vizsgálnia.

Kiberkoordinátor

A Fórum munkájának szakmai koordinálását a belügyminiszter által megbízott kiberkoordinátor látja el, aki tagként részt vesz a Tanács, valamint kiberbiztonsági munkacsoportok munkájában. A kiberkoordinátor a Tanács elnökét akadályoztatása esetén helyettesíti.

Titkárság

A Tanács, a Fórum és a kiberbiztonsági munkacsoportok működtetésével kapcsolatos adminisztratív teendőket a kiberkoordinátor irányításával a belügyminisztériumban működő titkárság látja el.

2.2. A kiberbiztonsági intézményrendszer felügyeleti és operatív szintje

Az állami kiberbiztonság intézményi rendszerében a felügyelt elektronikus információs rendszerek biztonsági felügyeletét a Kormány által kijelölt hatóság látja el. A Kormány erre a feladatra a 2013. évben a Nemzeti Fejlesztési Minisztérium irányítása alá tartozó Nemzeti Elektronikus Információbiztonsági Hatóságot (NEIH) jelölte ki. A felügyeleti, hatósági funkció és feladatkör a 2015. évtől a **Nemzetbiztonsági**

Szakszolgálathoz került, amelynek szervezetén belül 2015. október 1-jétől működik a **Nemzeti Kibervédelmi Intézet** (NBSZ NKI).

A nemzetbiztonsági feladatokat ellátó szervezetek esetén az elektronikus információs rendszerek biztonsági felügyeletét szektorális hatóságok látják el. A szektorális hatóságok által ellátott tevékenységek közül meghatározó az európai vagy nemzeti létfontosságú rendszerelemként kijelölt rendszerek, létesítmények elektronikus információs rendszereinek biztonságának felügyelete, melynek hatósági felügyeletét a BM **Országos Katasztrófavédelmi Főigazgatóság** látja el.

NBSZ NKI felügyeleti hatósági feladatai

A Belügyminisztérium irányítása alá tartozó NBSZ NKI a magyarországi kibervédelmi szervezetrendszer központi felügyeleti szerve. A felügyeletet ellátó hatóság feladatai közé tartozik az állami, közigazgatás elektronikus információs rendszereinek információ biztonsági osztályba és biztonsági szintbe sorolás megalapozottságának ellenőrzése. Elrendelheti a feltárt vagy tudomására jutott biztonsági hiányosságok elhárítását és ellenőrizheti az elhárítás eredményességét, ennek elmulasztása esetén bírságot is szabhat ki. A hatóság javasolhatja információbiztonsági felügyelő kirendelését egy adott szervezethez a kiberbiztonsági fenyegetések elhárításához szükséges védelmi intézkedések eredményes megtétele érdekében.

A hatóság feladatai közé tartozik többek között a hazai információbiztonsági, kibervédelmi gyakorlatok szervezése. Az NBSZ NKI feladata, hogy szoros együttműködést folytasson az eseménykezelő központtal, az elektronikus ügyintézési felügyelő hatósággal, a nemzetbiztonsági szolgálatokkal. Javaslattételre jogosult továbbá a nemzeti létfontosságú rendszerelem kijelölésére.

A hatóság nyilvántartja és kezeli többek között az érintett szervezetek elektronikus információs rendszereinek megnevezését és biztonsági osztályba sorolását, az érintett szervezet biztonsági szintjének besorolását. A nyilvántartások vezetésén túl az NBSZ NKI széleskörű hatósági feladatkörrel rendelkezik, többek között engedélyezési eljárások, hatósági ellenőrzések, kockázatelemzések lefolytatása vonatkozásában.

A hatóság jogköre 2021. március 1-jétől kibővült: jogosult elrendelni az ideiglenes hozzáférhetetlenné tételét annak az elektronikus hírközlő hálózat útján továbbított adatnak vagy egyéb információs társadalommal összefüggő szolgáltatásnak, amely a magyar kibertér biztonságára fenyegetést jelent, és amellyel kapcsolatosan az eseménykezelő központ biztonsági eseménykezelést folytat. Ez azt jelenti, hogy lekapcsoltathatja, illetve blokkoltathatja a magyar kibertér biztonságára fenyegetést jelentő rendszereket és szolgáltatásokat, adott esetben a szervezet működésének ellehetetlenülését okozva ezzel.

Az NBSZ NKI a **felügyeleti hatósági feladatain túl számos egyéb**, az állami kibervédelem szempontjából központi jelentőségű feladatkört ellát. A 2019. év óta az NBSZ NKI az állami kiberbiztonság központi felügyeleti intézményként ellátja

- az eseménykezelési feladatokat a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.) szerinti, alapvető szolgáltatást[2] nyújtó, létfontosságú vagy egyéb szempontból kritikus infrastruktúrát üzemeltetők (pl. energia, közlekedés, ivóvíz-ellátás, egészségügyi, pénzügyi piaci infrastruktúrák) tekintetében,
- az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ekertv.) szerinti, úgynevezett bejelentésköteles elektronikus kereskedelmi szolgáltatások (így az online piactér, internetes keresőszolgáltatás, valamint felhőszolgáltatás) kapcsán a szolgáltatást nyújtó szervezetek eseménykezelési, valamint a hatósági felügyeletét.

Az NBSZ NKI évek során egyre inkább széleskörűvé vált feladatkörét indokolja, hogy az állam a felügyeleti intézményrendszer erősítésével kívánja továbbra is fenntartani a kibertérben zajló társadalmi és gazdasági folyamatok zavartalanságát és biztonságát.

Felügyeleti intézményrendszer operatív feladatai - eseménykezelés

Az állami kiberbiztonság felügyeleti intézményrendszerének operatív feladatai közé tartozik az úgynevezett eseménykezelés, amelyet a kibertérből érkező támadásokkal és fenyegetettségekkel közvetlenül foglalkozó eseménykezelő központok látnak el.

Az állami felügyelet alá vont elektronikus információs rendszereket érintő biztonsági események kezelése érdekében 2013. július 1-jétől a **kormányzati eseménykezelő központot** (GovCERT Hungary) a

Nemzetbiztonsági Szakszolgálat működteti. A kormányzati eseménykezelő központ mellett számos **szektorális és ágazati eseménykezelő központ** került létrehozásra, többek között a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenység ellátására.

Az állami kiberbiztonság intézményrendszerében az érintett szervezetek a tudomásukra jutott biztonsági események adatait kötelesek haladéktalanul az illetékes eseménykezelő központ részére továbbítani, az ágazati eseménykezelő központok a kormányzati eseménykezelő felé továbbítják a bejelentéseket. Az eseményközpont jelentősége, hogy a biztonsági események adatait központosítottan kezelik, ezáltal hatékonyabban és gyorsabban reagálva tudnak fellépni a kiberfenyegetések ellen, megelőzve, illetve csökkentve a biztonsági események negatív hatásait és következményeit.

A biztonsági eseményekről rendelkezésre álló központosítottan gyűjtött adatok alapján a kormányzati eseménykezelő központ a magyar kibertér biztonsági helyzetéről, valamint a hazai és nemzetközi információbiztonsági irányokról elemzéseket, jelentéseket készít a Nemzeti Kiberbiztonsági Koordinációs Tanács részére.

Ágazati eseménykezelő központként funkcionál többek között az NBSZ NKI, amelynek feladatköre 2019. január 1-jétől bővült az elektronikus kereskedelem területén a bejelentésköteles szolgáltatók és az alapvető szolgáltatást nyújtó szervezetek eseménykezelésére kiterjedően. Az NBSZ NKI gyűjti és fogadja a Ibtv. és az Ekertv. hatálya alá tartozó szervezetek és gazdálkodók bármely elektronikus információs rendszerét érintő biztonsági eseményről az információkat és azokról rendszeres tájékoztatást ad ki az érintett szervezetek részére. A biztonsági, valamint kiber-incidenseket az állami és önkormányzati szervek mellett más piaci szereplők is jelenteni kötelesek a felügyeleti szerv részére.

NBSZ NKI egyéb operatív feladatai - sérülékenységvizsgálat

A biztonsági események kezelésének, megelőzésének egyik eszköze a sérülékenységvizsgálat, melynek elvégzésére az állami kibervédelmi feladatokat ellátó hatóság kötelezheti az ellenőrzéssel, vagy valamely biztonsági esemény kapcsán érintett szervezetet. A sérülékenységvizsgálat önként is elvégezhető, így preventív eszközként is funkcionál. A **sérülékenységvizsgálat** az elektronikus információs rendszerek gyenge pontjainak (ún. biztonsági rések pl. potenciális szoftverhibák, gyenge jelszavak, hibás beállítások) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárására irányul. További célja a feltárt hibák elhárítására vonatkozó részletes megoldási javaslatok kidolgozása az elektronikus információs rendszerek, rendszerelemek védelmének és biztonságának megerősítése érdekében.

Az állami kiberbiztonság intézményi rendszerében az érintett szervek többsége, így állami-, önkormányzati, vagy nemzetbiztonsági védelem alá eső szervezetek részére, valamint zárt célú elektronikus információs rendszerek[3] vonatkozásában sérülékenységvizsgálatot — a honvédelmi célú elektronikus információs rendszerek sérülékenységvizsgálatának kivételével — kizárólag az NBSZ NKI Eseménykezelő Központja végezhet.

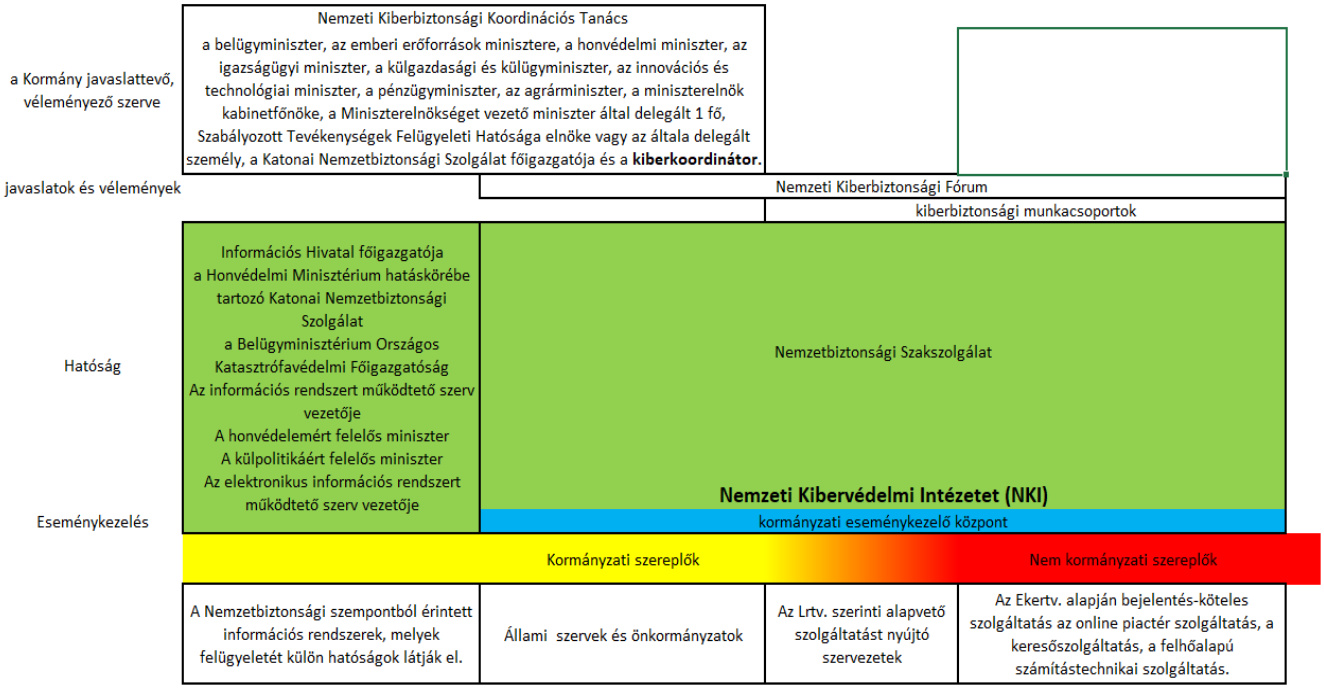
NBSZ NKI egyéb operatív feladatai - korai figyelmeztető rendszer

Az Ibtv. 2019. évben a kiberbiztonság rendszerében bevezette az úgynevezett korai figyelmeztető rendszer[4] (EWS) intézményét, valamint a korai figyelmeztető szolgáltatás igénybevételének rendjét. Az elektronikus információbiztonsági korai figyelmeztető rendszer üzemeltetését, a korai figyelmeztető szolgáltatás nyújtását a Nemzetbiztonsági Szakszolgálaton belül az **NBSZ NKI** látja el. A korai figyelmeztető szolgáltatás keretében az NBSZ NKI, mint rendszer-üzemeltető az alábbi tevékenységeket vállalja:

- az alkalmazott szűrési szabályok szerint folyamatosan monitorozza, vizsgálja a védett infrastruktúrák internet felé irányuló és onnan beérkező hálózati forgalmát,
- detektálja a fenyegetés bekövetkezésére utaló jelzéseket, és
- biztonsági esemény észlelésekor haladéktalanul tájékoztatja az eseménykezelő központot.

Az állami kiberbiztonság intézményrendszeréről a **4. ábra** nyújt áttekintést.

4. ábra: Összefoglaló az állami kiberbiztonság intézményrendszeréről



Forrás: ÁSZ szerkesztés

2.3. Nemzetközi szervezetekkel történő kapcsolattartás, tudásmegosztás és tapasztalatcsere

A kibervédelem területén a nemzetközi kapcsolattartás különös jelentőséggel bír a bevált gyakorlatok tapasztalatainak megosztása, a korai előrejelzés, az eseményekre való reagálás, a kockázatértékelés, a tudatosság növelése vonatkozásában. (EU Kiberbiztonsági Stratégia, 2013)

A **stratégiai szinten** a Nemzeti Kiberbiztonsági Koordinációs Tanács koordinációs tevékenységét, valamint döntéseinek végrehajtását a Nemzeti Kibertér Munkacsoport és a Nemzetközi és Európai Uniós Kibertér Munkacsoport segíti. A Nemzetközi és Európai Uniós Kibertér Munkacsoport feladata az állami szervek közötti, a nemzetközi szervezetekben, az Európai Unióban, valamint a két- és többoldalú együttműködésekben zajló kiberbiztonsági munkával kapcsolatos rendszeres információcsere elősegítése és egyeztetés a Magyarország által képviselendő vonatkozó álláspontjának kialakítását illetően.

A **felügyeleti szinten** az NBSZ NKI széleskörű nemzetközi feladatai közé tartozik az ún. „nemzeti kapcsolattartó pont” működtetése, a kiber-incidensek hazai koordinálása, az incidensekkel kapcsolatos jelentések fogadása, illetve küldése az NBSZ NKI nemzetközi partner-szervezetei irányába. A hazai kibervédelmi hatóság ennek keretében biztosítja az EGT tagállamok hatóságai között folytatott kapcsolattartást és együttműködést.

Az NBSZ NKI az állami kibervédelem és a nemzetközi tudásmegosztás támogatására több európai intézménnyel tart fenn kapcsolatot, illetve vesz részt egyéb, európai szintű együttműködésekben. Így például

- A 2014-ben létrehozott Európai Uniós Kiberbiztonsági Ügynökség, az ENISA[5] célja a tagállami kibervédelmi felügyeletet ellátó hatóságokkal együttműködésben az Európa-szerte egységesen magas szintű kiberbiztonság megvalósítása, amelyben Magyarországot az NBSZ NKI képviseli.
- Az Európai Bizottságon belül a Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósággal, a DG CNECT[6]-tel is kapcsolatot tart, amely az Európai Unióban a digitális egységes piaccal, az internetbiztonsággal, valamint a digitális tudománnyal és innovációval kapcsolatos uniós szakpolitikáért felelős.

Az NBSZ NKI kapcsolatot tart fenn a Közép-európai Kiberbiztonsági Platformmal (CECSP), a V4 államok és Ausztria együttműködési csoportjával, az EBESZ Kiberbiztonsági Informális Munkacsoportjával. Továbbá a Külgazdasági és Külügyminisztériummal közösen az NBSZ NKI képviseli Magyarországot az EBESZ munkacsoport ülésein, illetve az esedékes ülések közötti időszakban részt vesz a munkacsoport munkájában.

Az állami kibervédelmi intézményrendszer **operatív** szintje is széles nemzetközi feladatellátással érintett. A kormányzati eseménykezelő központ, a GovCERT az európai kormányzati eseménykezelő csoport által akkreditált nemzeti eseménykezelő központként vesz részt a nemzetközi együttműködésben.

Az állami kiberbiztonság intézményrendszerét érintően a nemzetközi kapcsolattartás szempontjából említést érdemel még az Európai Unió bűnüldöző egysége, a Bűnüldözési Együttműködés Európai Uniós Ügynöksége, az Europol EC3[7], amelynek operatív részlege aktív feladatokat lát el a tagállamokat érintő, határon átnyúló kiberbűncselekmények felderítésében.

A nemzetközi szintű tudásmegosztás és tapasztalatcsere elengedhetetlen az állami kibervédelem rendszerének hatékony működtetéséhez. Az NBSZ NKI szakpolitikai, felügyeleti és operatív szinten is jelentős nemzetközi kapcsolattartást bonyolít az európai és nemzetközi társintézményekkel, az állami kiberbiztonságot érintő nemzetközi munkacsoportoknak és fórumoknak is aktív résztvevője.

3. Az állami kiberbiztonság intézményi rendszerében az érintett szervezetek köre, helyzetképe

3.1. Az állami felügyelet alá vont elektronikus információs rendszereket üzemeltető szervezetek köre

Az állami felügyelet alá vont elektronikus információs rendszerek vonatkozásában az Ibtv. rögzíti a hatálya alá tartozó, érintett szervezetek körét, mely állami és nem állami szervezeteket egyaránt felölel. Az állami kibervédelem intézményrendszerében az érintett szervezetek közé döntően az állami-, önkormányzati, valamint a nemzetbiztonsági védelem alá eső szervezetek tartoznak. Az érintett szervezetek köre folyamatosan bővül. Ennek egyik oka az állami, önkormányzati, illetve közigazgatási szervek számossága, amely szervek elektronikus információs rendszereinek információ- és kiberbiztonsági védelmét a jogalkotó egyre szélesebb hatókörben garantálni kívánja. Másrészt a nemzeti adatvagyonba tartozó vagyonelemek védelme, továbbá a COVID 19 járványhelyzet.

Az állami kiberbiztonság intézményi rendszerében az érintett szervezetekről, így az állami, önkormányzati és nemzetbiztonsági védelem alá tartozó szervezetekről, valamint egyéb piaci szereplőkről az **1. táblázat** nyújt összefoglaló áttekintést.

1. táblázat - Az állami kiberbiztonság intézményrendszerében a felügyelt elektronikus információs rendszereket működtető szervezetek

Az érintett állami, önkormányzati, nemzetbiztonsági védelem alá tartozó szervezetek és egyéb piaci szereplők	
1.	**Központi államigazgatási szervek**
2.	**Alkotmányos szervezetek**
3.	**Fővárosi és megyei kormányhivatalok**
4.	**Helyi önkormányzatok képviselő-testületeinek hivatalai**
5.	**Hatósági igazgatási társulások**
6.	**Magyar Honvédség**
7.	**Az Ibtv. hatálya alá eső szervezetek részére adatkezelést végzők**
8.	**A nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói**
9.	**Az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeket működtető szervezetek elektronikus információs rendszereik tekintetében**
10.	**Az alapvető szolgáltatás nyújtásában közreműködők**
11.	**Az elektronikus információs rendszert működtető, a központi államigazgatási és kormányzati tevékenység szempontjából fontos, nemzetbiztonsági védelem alá eső szervek**

(Forrás: Ibtv. alapján ÁSZ szerkesztés)

Az Ibtv. deklarálja, hogy kiemelt jelentőséggel bír a nemzeti elektronikus adatvagyon, az állami- és önkormányzati szervek elektronikus információs rendszerei, továbbá a létfontosságú információs rendszerek és rendszerelemek biztonságának védelme.

Ezzel összhangban 2013. július 1-jétől terjedt ki az Ibtv. hatálya az „európai vagy nemzeti létfontosságúnak kijelölt rendszerelemek" elektronikus információs rendszereinek védelmére. A törvényben meghatározott ágazatokban az a rendszerelem minősül létfontosságúnak, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához. Létfontosságú rendszerelemekkel érintett ágazatnak minősül például az egészségügy, a lakosság személy-és vagyonbiztonsága, valamint a gazdasági és szociális közszolgáltatások területe. A létfontosságú rendszerelemmel érintett ágazatok köre 2013. év óta folyamatosan bővült. 2013. március 1-je óta az energia szektor —a villamosenergia-rendszer létesítményei, az atomerőmű kivételével — és a közlekedés létesítményei, 2013. július 1-je óta az agrárgazdaság, az egészség, a pénzügy, az ipar létesítményei tartoztak ebbe a körbe. A létfontosságú rendszerelemek köre 2014. január 1-je óta az Infokommunikációs technológiák és vízszolgáltatást nyújtókkal, a jogrend, a kormányzat, a közbiztonság és a védelem létesítményeivel egészült ki. 2016. január 1-je óta a gyógyszerkereskedelem, 2020. július 1-je óta a kőolajipar, földgázipar, távhő létesítmények minősülnek létfontosságú rendszerelemnek.

A létfontosságú rendszerelemek körének bővülése magával hozta az állami kibervédelem intézményrendszerében az érintett szervezetek számának bővülését is.

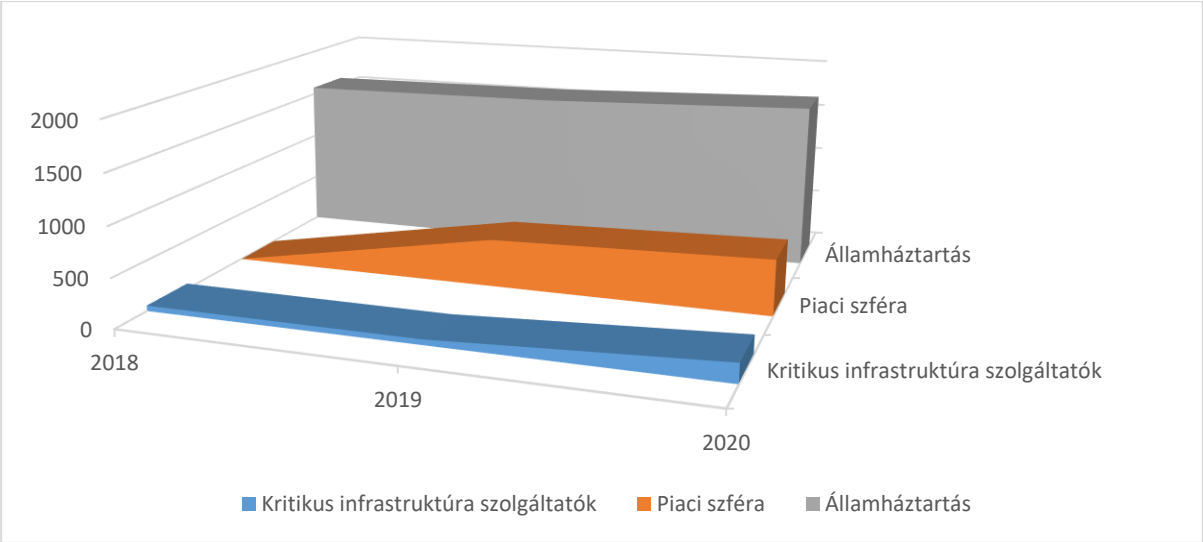
Az NBSZ NKI által felügyelt elektronikus információs rendszereket működtető szervezetek köre **2020. január 1-jétől tovább bővült az alapvető szolgáltatást nyújtó szervezetekkel, 2021. május 14-e óta pedig** az elektronikus információs rendszert működtető, a központi államigazgatási és kormányzati tevékenység szempontjából fontos, **nemzetbiztonsági védelem alá eső szervek** elektronikus információs rendszereinek védelmével.

A 2018-2020. években az NBSZ NKI által felügyelt elektronikus információs rendszereket működtető szervezetek számának növekedését — elkülönítve ezen belül az államháztartás és a piaci szférába tartozó szervezeteket, továbbá a kritikus infrastruktúra szolgáltatókat—az **5. ábra** mutatja be.

Jelentős feladatköri bővülést eredményezett, hogy 2020. július 1-jétől került át az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemek elektronikus információs rendszereivel kapcsolatos információbiztonsági hatósági feladatok ellátása a Belügyminisztériumtól, az Országos Katasztrófavédelmi Főigazgatóságától, az OKF-től az NBSZ NKI hatáskörébe.

Az állami kibervédelem felügyelete alá bevont elektronikus információs rendszerek, a felügyelet hatálya alá tartozó szervezetek és feladatkörök 2013. óta folyamatosan növekvő tendenciát mutatnak, ami fokozott felelősséget, egyben hatékony menedzselést igénylő kihívást támaszt a felügyeleti intézményrendszerrel szemben. Az érintett szervezetek számossága és feladatkörök bővülése – az allokált erőforrások függvényében – rendszer szintű kihatással bír a felügyeleti intézmény feladatellátásának hatékonyságára, amelyre a kibertámadások számának folyamatos növekedése is hatást gyakorol.

5. ábra - NBSZ NKI által felügyelt elektronikus információs rendszereket működtető szervezetek számának növekedése a 2018-2020. években (db)



(Forrás: NBSZ által rendelkezésre bocsátott adatok alapján ÁSZ szerkesztés)

Egyes államháztartási szervezetek kiberbiztonsági helyzetképe

A kiberbiztonsági tudatosság intézményi szintű felmérése érdekében az Állami Számvevőszék az elemzés keretében kérdőívvel keresett meg egyes, az államháztartás központi alrendszerében az elektronikus ügyintézés és bizalmi szolgáltatások szabályai szerint közhiteles nyilvántartások vezetésére kötelezett szervezeteket, továbbá az államháztartás önkormányzati alrendszerében egyes véletlenszerűen kiválasztott nagyobb (megyei jogú) és kisebb (5-20 ezer lakosú) önkormányzatokat, illetve az azokhoz tartozó önkormányzati hivatalokat.

A kérdőíves felmérés eredménye azt mutatja, hogy a megkérdezett szervezetek döntő többségénél az alapvető kiberbiztonsági kellékek és eszközök rendelkezésre álltak, a kibervédelmi támadások alapvető elhárítására megoldást, illetve eszközöket (ezek közé tartozik például a tűzfal, végponti vírusvédelem, behatolás érzékelő rendszer, naplófájl gyűjtő és elemző, levélszűrő) alkalmaznak.

A szervezetek mintegy harmada csatlakozott az NBSZ NKI által működtetett korai figyelmeztető rendszerhez, amely az állami kiberbiztonság rendszerében egységes, magas szintű kiegészítő védelmet biztosít.

A megkeresett szervezetek döntő többsége figyelemmel kíséri és hasznosítja az NBSZ NKI tájékoztatásait, a saját kibervédelmi rendszerének kialakítása és működtetése során e tájékoztatásokat felhasználja. Ez az NBSZ NKI tudásmegosztásának tényleges hasznosulását jelenti.

A távoli (otthoni) munkavégzés a kiberbiztonság területén is új kihívásokat eredményezett. Az IT infrastruktúrát fenyegető szereplők a COVID-19 járványt kihasználva világszerte újfajta támadásokat hajtottak végre, a távmunka terjedése pedig még sebezhetőbbé tette az IT-rendszereket. A megkérdezett szervezetek jelentős többsége biztosított legalább egy munkatársa részére távoli (otthoni) munkavégzés keretében a szervezet információs rendszeréhez történő hozzáférést az elmúlt két évben, amely rámutat az otthoni munkavégzés pandémiás helyzetben való elterjedésére, egyben kockázati kitettségére.

Az információbiztonság és kibervédelem területén különös jelentőséggel bír a képzés és tájékoztatás. A tudatosítás védelembe történő beépülése a munkavállalóknál is kulcsfontosságú. A kérdőíves válaszadás alapján a szervezetek döntő többsége készített és tartott a távmunka témakörében biztonsági tudatossággal kapcsolatos képzést az érintett alkalmazottak részére. Ugyanakkor a válaszadó szervezetek csupán fele mérte fel a COVID-19 járvány miatt erősödő vagy megjelenő kiberbiztonsági kockázatokat. Ez azt is jelenti, hogy a kockázatok kezeléséért felelős szervezetek első számú vezetői nem ismerték meg e kockázatokat, azok hatásait, így elmaradt azokra az adekvát válaszadás.

A megkeresett megyei jogú városi önkormányzatok mindegyike, a közhiteles nyilvántartásokat vezető központi szervek és a nem megyei jogú városi önkormányzatok kétharmada vizsgálta felül a szervezete IT biztonsági kockázatait az elmúlt két évben.

A válaszadó szervezetek mintegy harmadánál engedélyezett volt a szervezet információs rendszeréhez külső, nem a szervezet tulajdonában álló adattároló (pendrive) és egyéb külső eszközök munkavégzés során történő használata. A szervezetek döntő többsége nem készített nyilvántartást az alkalmazottak saját tulajdonában lévő, de munkavégzéshez is használt Informatikai eszközökről (így például az alkalmazott tulajdonában álló, munkavégzéshez használt számítógépekről, laptopokról vagy telefonokról). Ez rámutat a távmunka azon biztonsági kockázatára, hogy annak során az információbiztonsági felügyelet biztosítása is sérülhet.

A kérdőívvel megkeresett szervezetek között jelentős eltérések vannak az éves költségvetésben a kibervédelelmre fordított kiadások aránya terén. A legalacsonyabb érték 0,000052%, a legnagyobb pedig 4% volt, amely jelentős szórást mutat. Mindez rámutat arra, hogy kihívást jelent általános képet kialakítani e területen, mivel a kiberbiztonság mindent átfogó jellege miatt nem állnak rendelkezésre egyértelmű adatok és a kiberbiztonsági kiadásokat sem lehet gyakran elválasztani az általános informatikai kiadásoktól. Ez összhangban van a nemzetközi tapasztalatokkal, az Európai Számvevőszék tájékoztatója is rámutat arra, hogy a kiberbiztonsági kiadásokat gyakran nem lehet megkülönböztetni az általános informatikai kiadásoktól. (ECA tájékoztató, 2019)

Pozitív, hogy a megkérdezett szervezetek felénél a kibervédelem témaköre a szervezet stratégiájában is megjelenik. Továbbá a szervezetek többsége és a megkeresett megyei jogú városi önkormányzatok mindegyike úgy nyilatkozott, hogy van önálló programja, intézkedési terve a szervezet kibervédelmének erősítésére. A kiberbiztonsági tudatosság intézményi szintű felméréséről az összefoglalót a **6. ábra** mutatja be.

6. ábra – Összefoglaló a kiberbiztonsági tudatosság intézményi szintű felméréséről

(Forrás: ÁSZ kérdőíves felmérése alapján saját szerkesztés)

Az ÁSZ felmérésének eredménye összességében rámutat arra, hogy a megkeresett állami és önkormányzati szervezetek többsége a kiberbiztonság szervezeti szintű megteremtése iránt elkötelezett, a kibervédelem terén „tudatos”. A kibervédelmi tudatosságot erősíti, hogy a megkeresett szervezetek döntő többsége alkalmaz kibervédelmi támadások alapvető elhárítására megoldást, illetve eszközöket. Szintén a tudatosságot mutatja, hogy a szervezetek többsége az IT kockázatait felülvizsgálta, továbbá készített önálló programot, intézkedési tervet a szervezet kibervédelmének erősítésére. Kihívást jelent ugyanakkor, hogy válaszadó szervezetek csupán fele mérte fel a COVID-19 járvány miatt erősödő vagy megjelenő kiberbiztonsági kockázatokat, továbbá az, hogy a szervezetek döntő többsége nem készített nyilvántartást az alkalmazottak saját tulajdonában lévő, de munkavégzéshez is használt informatikai eszközökről.

4. A szervezeti kiberbiztonság aktuális kihívásai, mitől lesz „élő” a kibervédelem, nem csupán adminisztratív feladat

A COVID-19 világjárvány a szervezeteket kiberbiztonsági szempontból mind a köz-, mind a magánszférában új kihívások elé állította. A pandémiás időszakban újfajta kiberfenyegetések, többek között COVID-19 tematikájú támadások is tömegesen jelentkeztek. Az IT infrastruktúrát fenyegető szereplők a COVID-19 járványt kihasználva világszerte újfajta támadásokat hajtottak végre, a távmunka terjedése pedig még sebezhetőbbé tette az IT rendszereket. Az NBSZ NKI 2020-as évben az állami és önkormányzati szervektől több mint 900 bejelentett incidenst regisztrált. (Palicz, Bencsik, Szócska 2021) Az ENISA 2020 őszén megjelent jelentése kiemeli, hogy a pandémia egy hónapja alatt az elektronikus kéretlen és adathalász levelek küldése 667%-kal nőtt az európai unióban (ENISA 2020).

4.1. A táv- és otthoni munkavégzés információbiztonsági aspektusairól

A pandémia idején a korábbi atipikus foglalkoztatási formák, mint a táv- illetve otthoni munkavégzés a COVID-19 időszaka alatt tipikus foglalkoztatási formává váltak. Hazánkban a 2020. évben mind a rendszeres, mind az eseti- távmunkavégzés robbanásszerű növekedést mutat. A KSH adatai alapján az állami foglalkoztatóknál a rendszeres távmunkavégzésben dolgozók aránya közel tízszeres növekedést mutatott az utolsó pandémia mentes év és 2020. év között, addig ez az arány csak háromszoros növekedést mutatott a tisztán magán foglalkoztatóknál.

A pandémia idején a munkáltatók és a munkavállalók is számos új kihívással, kockázattal, egyben új lehetőségekkel találták szembe magukat.

A **távmunkavégzés** során a munkavédelmi, munkabiztonsági, és munkajogi szabályok érvényesítésén túl munkáltatói szempontból a szervezeti információ- és kiberbiztonsági szabályok érvényesítése is fokozott kihívást jelent.

Az irodai munkavégzéshez képest, ahol jellemzően zárt hálózatban kapcsolódnak egymáshoz a munkaeszközök, a távmunkavégzésre való átállással a munkavégzés helyszínei távol kerültek a szervezet telephelyétől, amely önmagában is számos új információbiztonsági kockázatot eredményezett. A távoli munkaállomásokon feladatot ellátó alkalmazottak és a munkáltatójuk közé a privát telekommunikációs és internet szolgáltatók kvázi „közbe ékelődtek”, a zárt rendszerű irodai hálózatokhoz képest új szereplőként kitettséget eredményezve. Az irodai munkavégzéssel szemben a távmunkavégzés során a kezelt adatok bizalmassága is fokozott veszélynek van kitéve.

Információbiztonság szempontjából veszélyt jelent, amennyiben a munkavállaló a szervezet távmunka rendszerét megkerülve, illetve azt kiegészítve, esetleg korábban magán célra használt, szervezeti kontrollal nem rendelkező privát email levelező rendszereket, fájlmegosztó-programokat, avagy közösségi felületeket kezd munkavégzéséhez használni. Ennek során a szervezeti adatok rendelkezésre állása és bizalmassága sérülhet.

A munkáltatónál a vonatkozó információbiztonsági szabályok érvényesítésében a szervezet vezetőjére fokozott felelősség hárul, hiszen szervezeti szinten a vezető köteles gondoskodni a szervezet elektronikus információs rendszereinek és adatainak védelméről.

A **humán faktor** szerepe és jelentősége kiemelt a kiberbiztonságban. A pandémia idején kihívásként jelentkezett, hogy a távmunkarendszerek használatához új digitális ismeretek és képességek megszerzése volt szükséges, amely tudás sok esetben a munkavállalói oldalon nem állt rendelkezésre. A kockázatok megelőzése kapcsán a képzés és tudatosítás jelentőségét nem lehet eléggé hangsúlyozni.

A munkavállaló felkészítésében és képzésében a munkáltató közvetlenül is szerepet kell vállaljon. Az állami kiberbiztonság rendszerében megkövetelt, hogy a munkáltatók az alkalmazottak oktatásával, tudatosság képzésével gondoskodjanak az információ- és kiberincidensek bekövetkezésének megelőzéséről.

A védelmi intézkedések közül az adminisztratív és fizikai védelmi intézkedések implementálásán túl fontos a logikai védelmi intézkedések kategóriájába sorolt tevékenységek szakszerű és tudatos végrehajtása is. Hiszen hiába készítjük el az adminisztratív kötelezettségként meghatározott szabályzatokat, eljárás rendeket, illetve hiába szereljük fel rendszereinket az előírt fizikai védelmi intézkedésekkel, ha az alkalmazottak azokat a kellő ismeretek hiányában esetlegesen figyelmen kívül hagyják.

Az információbiztonság területén a teljeskörűség szempontját is folyamatosan szem előtt kell tartani, ezért fontos, hogy az elvárások kiterjedjenek az érintett szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki a szervezet elektronikus információs rendszereivel kapcsolatba kerül, avagy potenciálisan kapcsolatba kerülhet. Alapvető információbiztonsági követelmény, hogy minden érintett számára csak a számukra kijelölt feladatok végrehajtásához szükséges és elégséges hozzáféréseket szükséges engedélyezi és beállítani.

A táv-, illetve otthoni munkavégzés elterjedésével információbiztonság szempontjából mind hangsúlyosabb jelentőséggel bír, hogy a munkáltató biztosít-e informatikai eszközöket (pl. laptopot, internet csatlakozást, titkosítási eszközt, adattárolót) a távoli munkavégzéshez, avagy engedélyezi az idegen, akár az **alkalmazottak saját tulajdonában álló IT eszközök** használatát a munkavégzéshez.

Biztonsági szempontból a védelmi szint lényegesen alacsonyabb, amennyiben otthoni (távoli) munkavégzésben is történik feladatellátás az irodai, személyes jelenlétet kívánó feladatellátással szemben. Továbbá, az információbiztonsági szabályok munkáltató általi érvényesítése is problematikusabb, amennyiben a munkáltató engedélyezi az idegen eszközök alkalmazását a távoli munkavégzés során.

Kiberbiztonsági szempontból a számítástechnikai eszközök **magáncélú használat**a is fokozottabb kockázati kitettséget jelent. A munkajog alapján főszabály szerint a munkavállaló a rendelkezésére bocsátott számítástechnikai eszközt kizárólag a munkaviszony teljesítése érdekében használhatja. A munkáltató jogosult arra, hogy a számítástechnikai eszközök munkavégzéstől eltérő, magáncélú használatát teljeskörűen kizárja. Információ és kiberbiztonsági szempontból a munkáltatói oldalról ez lényegesen magasabb védelmi szintet eredményez. A munkavállaló saját tulajdonban lévő eszközök munka-célú használata adatszivárgásokat is eredményezhet. A munkáltatói érdekkörbe tartozó adatok pontos elkülönítése a magán tulajdonban lévő, de munkavégzésre is használt eszközöknél kibervédelmi kockázatot jelent.

4.2. Mitől lesz „élő” a kibervédelem, nem csupán egy adminisztratív feladat

A kibervédelem és biztonság attól lesz hatékony és „élő”, amennyiben a kibervédelemben érdekelt egyes szervezetek a kibervédelmi „reziliencia” érdekében tudatosan járnak el, maguk is aktívan tesznek a kibervédelem és biztonság megteremtéséért. Ehhez az Ibtv. előírásai alapján szervezeti szinten az alábbi kibervédelmi „eszköztár” áll rendelkezésre, amelyek többségét nem kizárólag az állami kibervédelem érintett szervezetei, hanem az állami kiberbiztonság intézményrendszerén túlmutatva „jó gyakorlatként” a kötelező alkalmazással nem érintett egyéb piaci szereplők, szervezetek is alkalmazhatják a szervezeti kiberbiztonságuk fokozására, a védelmi „ellenállóképesség” erősítésére.

Ezen „eszköztár” egyes elemeinek bemutatása a kibervédelmi tudatosság jelentőségére kívánja felhívni a figyelmet, a kibervédelmi eszközrendszer teljeskörű bemutatását nem célozza. Célja – a vonatkozó jogszabályok és szakirodalom áttekintésével – a témát érintő figyelemfelkeltés és tudatosítás.

A szervezet vezetőjének szerepe a kiberbiztonság megteremtésében

A digitális világ kockázatainak és azok a szervezetek folyamataira és célokra gyakorolt potenciális hatásának ismerete és elemzése nélkül bármely szervezet irányíthatatlan, olyan, mint irányvesztett hajó a viharban. A szervezet vezetőjére a kiberbiztonság megteremtése érdekében kiemelt szerep hárul, hiszen a szervezeti szintű folyamatok, kontrollok és védelmi mechanizmusok megteremtése, illetve hatékony működtetése a szervezet első számú vezetőjének felelőssége.

Az állami kiberbizonság rendszerében az Ibtv. alapján a szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről. Így a vezető köteles kijelölni az elektronikus információs rendszer biztonságáért felelős személyt, aki többek között a felügyeleti hatósággal és az eseménykezelő központtal való kapcsolattartásért felelős.

Kockázatfelmérés, mint első lépés

Az ISACA[8] Magyarország 2021. évi információbiztonsági felmérése rámutat, hogy noha a közelmúltban új informatikai biztonsági kihívások jelentkeztek a pandémiára is tekintettel, válaszadó szervezetek közel fele nem folytatott IT kockázatfelmérést az elmúlt egy évben. A felmérés – melyen a válaszadók több mint egyhatod része költségvetési területen működő szervezet – rávilágít továbbá arra, hogy a megkérdezettek ötöde nem végez kulcs területi megfelelőségi ellenőrzést. (ISACA 2021)

Az állami kiberbiztonság területén a biztonsági auditok rendszeres végrehajtásának kötelezettsége az Ibtv. által előírt. Rendszeres IT kockázatelemzés hiányában a lehetséges biztonsági kockázati értékek változása — többek között az üzletfolytonosság, túlterhelések, licenszek, limitációk és rendszerhibák — a szervezet vezetése számára teljesen ismeretlenek maradhatnak.

Információs rendszerek besorolása és kockázatkezelés

A szervezet információs rendszereinek biztonsága[9] a kibervédelem megteremtésének egyik alapvető eszköze. Az állami kiberbiztonság rendszerében az Ibtv. egyik legfontosabb eleme az alapvető elektronikus információbiztonsági követelményeinek meghatározása, a törvény meghatározott szempontok alapján – bizalmasság[10], sérthetetlenség[11] és rendelkezésre állás[12] – rendszeres kockázati biztonsági besorolási kötelezettséget ír elő a szervezet részére. Kizárólag ennek a besorolásnak az eredményét felhasználva lehet bármilyen védelmi követelményeknek megfelelő (logikai[13], fizikai[14] és adminisztratív[15] védelmi) intézkedéseket tenni, és azok végrehajtását után követni. Az állami kiberbiztonságba bevont szervezet köteles elektronikus információs rendszereinek besorolását nyilvántartás céljából a felügyeleti hatóságnak megküldeni, amely így képes a kockázat besorolási anomáliákra felügyeleti eszközökkel reagálni.

Az állami kiberbiztonság intézményrendszerén túl is, minden szervezetnek érdemes törekednie arra, hogy elérje és fenntartsa azt az optimalizált szintet, ahol minőségszabályozott jelleggel, a szervezetbe beépített folyamatok támogatásával, a potenciális kockázatokkal arányosan, strukturáltan és jól irányítva működik az elektronikus információs rendszereinek védelme, a besorolás pedig ennek az alapvető eszköze.

Kockázatcsökkentés tudatosítással

Az ISACA Magyarország felmérésében 2021. évben résztvevők több mint egyharmada (37%) semmilyen területen nem tervezte tovább képezni az informatikai biztonsági szakembereit. (ISACA.Hu, 2021)

Az állami kiberbiztonság rendszerében a szervezet vezetője köteles gondoskodni saját és a szervezet alkalmazottai információbiztonsági ismereteinek szinten tartásáról.

Intézményközi szinten az állami kiberbiztonság rendszerében a tudatosítás kapcsán a felügyeleti hatóságra kiemelt szerep hárul. Az Ibtv. alapján az NBSZ NKI ezzel kapcsolatos feladata, hogy a biztonságtudatos felhasználói magatartás elősegítése céljából oktatási anyagokat dolgozzon ki, tréningeket tartson, felvilágosító és szemléletformáló kampányokat szervezzen. A kiberbiztonság csökkentése érdekében a szervezetek az NBSZ NKI által kiadott segédanyagokat jogdíj és egyéb költségek megfizetése nélkül szabadon használhatják fel saját alkalmazottaik és beszállítóik képzéséhez, oktatásához.

Hatósági riasztások és tájékoztatások figyelemmel kísérése

Az Ibtv. alapján az információbiztonság és a kibervédelem alapvető feladata a megelőzés és a korai figyelmeztetés. A felügyeleti hatóság, illetve eseménykezelő központok rendszeres tájékoztatást, továbbá riasztásokat adnak ki az állami kiberbiztonság rendszerébe bevont szervezetek részére a potenciális fenyegetettségek elleni kiberbiztonsági intézkedésekről. A hatóság a riasztásait saját honlapján nyilvánosságra hozza, ezen felül közvetlenül is megkeresi az érintett intézményi, szervezeti és egyéb gazdálkodókat a riasztással kapcsolatban. Célszerű a hatósági riasztásokat és tájékoztatásokat szoros figyelemmel kísérni, és aktívan hasznosítani azokat a szervezet elektronikus rendszereinek és folyamatainak felülvizsgálatakor.

Incidens jelzések és eseménykezelés

Előfordulhat olyan — az Ibtv. fogalomrendszerében úgynevezett biztonsági eseménynek minősülő — 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 vész el, illetve megsérülhet. Az állami kiberbiztonság intézményrendszerében az érintett szervezet az Ibtv. alapján köteles a biztonsági incidenseket a felügyeleti hatóságnak bejelenteni és aktívan részt venni annak kezelésében.

A kibervédelmet fenyegető események és incidenshez kapcsolódó információk központosított feldolgozása és kezelése révén a kormányzati, ágazati és szektorális eseménykezelő központok működése élővé teszi az állami kibervédelmet.

Korai figyelmeztető rendszerhez való csatlakozás

Az NBSZ NKI honlapján elérhető tájékoztatás szerint a felügyeleti hatóság által működtett korai figyelmeztető rendszerhez való csatlakozás előnye, hogy a csatlakozott szervezeteknek egységes, magas szintű kiegészítő biztonsági védelmet nyújt, amellyel a szervezetek kibervédelmi észlelési, felügyeleti és megfelelőség-ellenőrzési képessége javulhat. (NKI honlap, 2022) A korai figyelmeztető rendszer az állami kiberbiztonság érintett szervezetei többsége számára – a kormányzati adatközponti szolgáltatások igénybevételére kötelezett szervezetek körétől eltekintve – egy lehetőség, amelyhez önkéntes alapon lehet csatlakozni, aktív eszközként szolgálhat a kiberfenyegetettségek megelőzésében.

Sérülékenységvizsgálat

A biztonsági események kezelésének, megelőzésének egyik eszköze a sérülékenységvizsgálat, amely az NBSZ NKI honlapján elérhető tájékoztatás szerint az elektronikus információs rendszerek gyenge pontjainak (ún. biztonsági rések pl. potenciális szoftverhibák, gyenge jelszavak, hibás beállítások) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárására irányul. További célja a feltárt hibák elhárítására vonatkozó részletes megoldási javaslatok kidolgozása az elektronikus információs rendszerek, rendszerelemek védelmének és biztonságának megerősítése érdekében. A sérülékenységvizsgálat lefolytatása hatóság elrendelése esetén kötelező, de önként is elvégezhető, így preventív eszközként is funkcionál.

Az állami kibervédelem érintett szervezetei számára sérülékenységvizsgálatot az NBSZ NKI Eseménykezelő Központja végezhet, amely szolgáltatás — ahogy arra az NBSZ NKI tájékoztatása is felhívja a figyelmet — részükre térítésmentesen vehető igénybe. (NKI tájékoztatás, 2022) Egyéb szervezetek sérülékenységvizsgálatát a sérülékenységvizsgálat lefolytatására jogosult, hatósági nyilvántartásába bejegyzésre került gazdálkodó szervezetek végezhetik.

Kiberbiztonsági tanúsítás

Az Ibtv. 2021. évi módosításával az állami kiberbiztonság rendszerében új eszköz lépett életbe, az úgynevezett kiberbiztonsági tanúsítás rendszere, amelynek kialakítása jelenleg is folyamatban van. Az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló rendszer és tanúsítási eljárás a digitális eszközök és szolgáltatások kapcsán az EU kiberbiztonsági rendeletében megfogalmazott célokkal összhangban a minőség-biztosítottságot hivatott garantálni.

4.3. Nemzetközi számvevőszéki tapasztalatok

Nemzetközi tudásmegosztás és tapasztalatcsere

A kiberbiztonság jelentőségére tekintettel az Állami Számvevőszék mind hangsúlyosabb figyelmet fordít a kiberbiztonsági kockázatokkal kapcsolatos tudatosításra, valamint a kibervédelemre vonatkozó tapasztalatok és jó gyakorlatok hazai, illetve a nemzetközi számvevőszéki közösségben történő megosztására. Mindezen célokkal összhangban, 2022. év tavaszán az Állami Számvevőszék a digitális tér kiberbiztonsági kockázatai, illetve azok kezelésének jó gyakorlatai témában rendezett online szakmai eseményt a nemzetközi számvevőszéki közösség szakértőinek részvételével.

A rendezvényen részt vevő valamennyi számvevőszék megerősítette, hogy az elmúlt évek tapasztalatai alapján a nemzetközi kiberfenyegetettség jelentősen megnövekedett és a kockázatokkal arányos — adminisztratív, logikai és fizikai— védelmi intézkedések útján igyekszik mérsékelni azokat. A szakmai esemény többek között rávilágított, hogy a kiberbiztonság témakörében fokozottan érvényes megállapítás, miszerint „a teljes rendszer éppen annyira erős, mint a leggyengébb láncszeme”. A résztvevők megerősítették, hogy a kiberbiztonsághoz kapcsolódó kockázatok mérséklésének egyik kulcstényezője a munkatársak tudatosságának növelése, amelyre kiemelt hangsúlyt szükséges fektetni. A kibervédelemben az „emberi tényező” kiemelten fontos, így az információbiztonság jelentős szemléletformálást és rendszeres szervezeti szintű képzést igényel, amelyhez a megfelelő erőforrás biztosítása elengedhetetlen. A nemzetközi tapasztalatok alapján a tudatosság fokozásán túl a kiberbiztonsági kockázatok csökkentésének további kulcsfontosságú lépése a hatékony biztonsági stratégia kidolgozása. A számvevőszékek között az intézményi szinten alkalmazott információ-technológiai megoldások jó gyakorlatai is megosztásra kerültek. Így többek között az Állami Számvevőszék saját szervezetét érintően is többszintű védelmi megoldást dolgozott ki a kibertér fenyegetéseinek kezelésére, ideértve a biztonságos távoli hozzáférést biztosító technológiákat, kétfaktoros hitelesítést, emellett fejlett végpontvédelmi megoldást támogató rendszereket is alkalmaz. A felsorolt határvédelmi eszközök mellett rendszeres sebezhetőségi teszteket végez, továbbá nagy hangsúlyt fektet az alkalmazottak informatikai biztonsági képzésére.

Nyilvánvaló, hogy a kiberbiztonság területén 100%-os garancia biztosítása elérhetetlen cél, mivel a kibertámadás szervezői, a „láthatatlan emberek és infrastruktúrák” mindig lépéselőnyben vannak. Figyelemmel erre, a szakmai esemény rávilágított a szervezeti kiberbiztonsággal kapcsolatosan a megelőzés kiemelt fontosságára, továbbá arra, hogy a kibervédelmet biztosító védekezési rendszerek fókusza minden sérülékeny területre ki kell, hogy terjedjen. A részt vevő intézmények egyetértettek abban is, hogy szükség van információbiztonsági szemléletformálásra, amelyre vonatkozóan a számvevőszékeknek a jövőben fontos szerepe lesz. A szakmai rendezvény főbb következtetése, hogy a számvevőszékeknek a kiberfenyegetések mérséklésére vonatkozó bevált gyakorlatok megosztásával példát kell mutatniuk a közszféra szervezetei számára.

A nemzetközi tapasztalatcsere és tudásmegosztás érdekében az Állami Számvevőszék a legfőbb ellenőrző szervezetek nemzetközi közösségében is szoros figyelemmel kíséri a kiberbiztonsággal kapcsolatos szakmai rendezvényeket. A Legfőbb Ellenőrző Intézmények Európai Szervezete (EUROSAI) IT munkacsoportjának (ITWG) titkársági feladatait ellátó Észt Számvevőszék szervezésében a 2021. évben megtartott „Felkészülés a számvevőszékeknek a kiberkockázatok feltérképezésére” című szakmai konferencia is hasznos tapasztalatokkal szolgált a kiberbiztonsággal kapcsolatos legújabb nemzetközi tapasztalatok megosztására.

Mindezen nemzetközi tapasztalatok is felhívják a figyelmet arra, hogy a számvevőszékekre az állami kiberbiztonság területén is egyre hangsúlyosabb szerep hárul.

Nemzetközi ellenőrzési tapasztalatok

Az Európai Számvevőszék 2022 márciusában tette közzé az uniós intézmények, szervek és ügynökségek kiberbiztonságáról szóló jelentését. Az Európai Számvevőszék ellenőrzése az európai uniós szervek kiberbiztonságát vizsgálta, arra vonatkozóan, hogy az uniós szervek összességében megfelelő intézkedéseket vezettek-e be a kiberfenyegetésekkel szembeni védelmük érdekében.

Az Európai Számvevőszék jelentése megerősíti, miszerint az uniós intézményeket, szerveket érintő jelentős biztonsági események száma a megelőző években drasztikusan növekedett, a 2018 és 2021 közötti időszakban számuk több, mint tízszeresére nőtt. Ezzel párhuzamosan 2018 óta az európai uniós intézmények,

szervek és ügynökségek illetékes eseménykezelő központját érintően is gyors ütemben nőtt a munkaterhelés.

Az Európai Számvevőszék rámutat, hogy a távmunkára való átállás kapcsán a támadók új sebezhetőségeket, támadási felületeket tudtak kihasználni. Kiemeli, hogy a kiberbiztonsági tudatosság növelését szolgáló szervezeti szintű képzések a kiberbiztonság keretrendszerének kulcsfontosságú elemét képezik. A nemzetközi szabványokkal összhangban hangsúlyozza a kockázatkezelés kiemelt szerepét, amelynek elengedhetetlen eszköze a biztonsági kockázatok rendszeres kiértékelése.

A jelentés rámutat továbbá arra, hogy az európai uniós intézmények, szervek és ügynökségek nem minden esetben jelentették a szervezetüket ért jelentős biztonsági eseményeket az uniós intézmények eseménykezelő központja, a CERT-EU[16] részére. A bejelentés elmulasztása kihat a rendszer-megfigyelési képességre, hiszen az illetékes eseménykezelő központ nem jut hozzá olyan kiberfenyegetésekkel kapcsolatos értesülésekhez, amely hasonló fenyegetéssel szembesülő szervezet kapcsán hasznosak lettek volna.

A jelentés rögzíti, hogy az uniós szervek tekintetében jelentős különbségek mutatkoznak annak vonatkozásában, hogy informatikai kiadásaik hány százalékát fordítják a kiberbiztonságra. Megerősíti továbbá, hogy a kiberbiztonsági kiadások optimális szintjét nehéz abszolút mértékben meghatározni.

FÜGGELÉK

1. számú függelék: Rövidítések jegyzéke

EGT	Európai Gazdasági Térség
EU	Európai Unió
ENISA	Európai Hálózat- és Információbiztonsági Ügynökség
GovCERT Hungary	Nemzetbiztonsági Szakszolgálat Kormányzati Eseménykezelő Központ
NATO	Észak-atlanti Szerződés Szervezete
NBSZ	Nemzetbiztonsági Szakszolgálat
NBSZ NKI	Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet
NISZ	Nemzeti Infrastruktúra-szolgáltató Zrt.
NEIH	Nemzeti Elektronikus Információbiztonsági Hatóság
KSH	Központi Statisztikai Hivatal
OKF	Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság

Jogszabályok, egyéb jogi aktusok rövidítései

Alaptörvény	Magyarország Alaptörvénye (2011. április 25.)
Ekertv.	az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény
Ibtv.	az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
Lrtv.	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
NEIH rendelet	301/2013. (VII. 29.) Korm. rendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról
GovCERT rendelet	233/2013. (VI.30.) Korm. rendelet az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről
Kiber-irányítási rendelet	484/2013. (XII.17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről
Ibtv. vhr.	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
Nemzeti Biztonsági Stratégia	Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat, amely a 1163/2020. (IV. 21.) Korm. határozattal került megújításra
Nemzeti Kiberbiztonsági Stratégia	1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájának elfogadásáról
NIS stratégia	1069/2014. (II. 19.) Korm. határozat Magyarország Nemzeti Infokommunikációs Stratégiájáról
NIS monitoring jelentés	1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről
Hálózati Biztonsági Stratégia	1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról
ECI irányelv	2008/114/EK tanácsi irány (ECI) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről
EU NIS irányelv	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

2. számú függelék: Felhasznált irodalom, jogforrások

Felhasznált irodalom

1. Kovács, L (2018)1: Kovács László: A kibertér védelme (Dialóg Campus Kiadó, 2018) p. 246-247.
2. ECA tájékoztató (2019): Európai Számvevőszék (ECA): Az eredményes uniós kiberbiztonsági politika előtt álló kihívások, Tájékoztató In: ECA honlap, 2019. március (Letöltés dátuma: 2022.04.06.) https://www.eca.europa.eu/hu/Pages/DocItem.aspx?did=49416
3. Kovács, L (2018)2: Kovács László: A kibertér védelme (Dialóg Campus Kiadó, 2018) p. 243.
4. Joan A,, Krzysztof K. (Letöltés dátuma: 2022.01.14) Kiberbiztonsági-kiadások az EU országaiban https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive.
5. Krasznay Cs. (2021) Kiberbiztonság a negyedik ipari forradalom korában (Letöltés dátuma: 2022.01.14) https://www.hte.hu/documents/4176585/4651803/2019_ksz1_5-Krasznay.pdf
6. Krasznay Cs. (2022) Krasznay Csaba, a Nemzeti Közszolgálati Egyetem Kiberbiztonsági Intézet vezetője (Közvetítés időpontja 2022.01.14 18:00) https://infostart.hu/arena/2022/01/14/krasznay-csaba-a-nemzeti-kozszolgalati-egyetem-kiberbiztonsagi-intezet-vezetoje
7. Nemzeti Kibervédelmi Intézet (2021) A SolarWinds incidens (Letöltés dátuma: 2022.01.14) https://nki.gov.hu/wp-content/uploads/2021/09/NBSZ-NKI-Kiberbiztons%C3%A1gi-elemz%C3%A9s-a-SolarWinds-incidensr%C5%91l.pdf
8. Nemzeti Kibervédelmi Intézet (2021) Automatizált sérülékenységvizsgálati rendszer (Letöltés dátuma: 2022.01.14) https://nki.gov.hu/szolgaltatasok/tartalom/serulekenysegvizsgalat/
9. Nemzeti Kibervédelmi Intézet (2021) Automatizált sérülékenységvizsgálati rendszer (Letöltés dátuma: 2022.01.14) https://nki.gov.hu/szolgaltatasok/tartalom/asr/
10. EU Tanács Főtitkársága (Letöltés dátuma: 2022.01.14) Kiberbiztonság: hogyan kezeli az EU a kiberfenyegetéseket? https://www.consilium.europa.eu/hu/policies/cybersecurity/
11. Bodó A., Palicz T., Joó T,. (2020) "AZ IBTV. GYAKORLATA Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2020
12. AZ INFRASTRUKTÚRA-VÉDELEM ÉS AZ INFORMÁCIÓBIZTONSÁG KAPCSOLATA (21. oldaltól) " (Letöltés dátuma: 2022.01.14) https://nke-repo.uninke.hu/xmlui/bitstream/handle/123456789/15923/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20vezeto.pdf;jsessionid=E182A97CE803ED305207B3861938FCEB?sequence=3
13. Nemzeti Elektronikus Információbiztonsági Hatóság (Letöltés dátuma: 2022.01.14) Az Ibtv.-ben meghatározott feladatok áttekintése a törvénye hatálya alá tartozó szervezetek vonatkozásában- http://neih.gov.hu/sites/default/files/u/utmutato_ibtv_final.pdf
14. Kürt Zrt. (Letöltés dátuma: 2022. 01.17) Ibtv. megfelelés mint szolgáltatáshttps://www.kurt.hu/megoldasaink/ibtv-lrtv-megfeleles/
15. PR Audit Kft. (Letöltés dátuma: 2022. 01.17) Ibtv. megfelelés mint szolgáltatáshttps://www.praudit.hu/ibtv-compliance/
16. Kürt Zrt. (Letöltés dátuma: 2022. 01.17) a KÜRT mint 185/2015. (VII. 13.) Korm. Rendelet 14. § (4) bek. b) pontjában hivatkozott sérülékenységvizsgálat lefolytatására jogosult gazdasági társasághttps://www.kurtsec.com/wp-content/uploads/2017/10/Ibtv_Lrtv_portfolio_leiras.pdf
17. Borsod-Abaúj-Zemplén Megyei Kormányhivatal (Letöltés dátuma: 2022. 01.17) A Borsod-Abaúj-Zemplén Megyei Kormányhivatal Informatikai Biztonsági Szabályzata https://www.kormanyhivatal.hu/download/2/48/55000/%5B03%5D%20-%20IBSZ%20-%20Informatikai%20Biztons%C3%A1gi%20Szab%C3%A1lyzat_WEB.pdf
18. Palicz T., Bencsik B., Szócska M. (Letöltés dátuma: 2022. 01.18) Kiberbiztonság a koronavírus idején – a COVID–19 nemzetbiztonsági aspektusai https://akjournals.com/view/journals/112/2/1/article-p78.xml
19. Horváth G. (2013) Közérthetően nem csak az IT biztonságról (Letöltés dátuma: 2022.01.14) https://kifu.gov.hu/sites/default/files/IT_brosura_v7.pdf

20. Hanganov Kft. (Letöltés dátuma: 2022. 01.18) Ibtv. megfelelés mint szolgáltatáshttps://www.hanganov.hu/?gclid=EAIaIQobChMI2ZjTmKi49QIVjs53Ch0mEAZhEAMYASAAEgJrJfD_BwE
21. Györkös R., Nagyné Takács V. (2014) javaslat az elektronikus információs rendszerek 77/2013. (XII.19.) NFM rendelet alapján végzendő biztonsági osztályba sorolása vonatkozásában. (Letöltés dátuma: 2022.01.14) http://hadmernok.hu/143_11_gyorkosr_ntv.pdf
22. Magyar Államkincstár(2018) Tájékoztatás az önkormányzati ASP rendszerekhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről (Letöltés dátuma: 2022.01.14) https://alkalmazaskozpont.asp.lgov.hu/sites/asp/files/2018-06/asp_tajekoztato_az_onkormanyzati_asp-hez_csatlakozaskor_megvalositando_bizto.pdf
23. Nyikes Z. (2019) Az információbiztonság növelése a felhasználó támogatásának lehetőségeivel (Letöltés dátuma: 2022.01.14) http://lib.uni-obuda.hu/sites/lib.uni-obuda.hu/files/Nyikes_Zoltan_ertekezes.pdf
24. Számadó R. (2018) Önkormányzatok kiberbiztonságának és online képességének vizsgálata, figyelemmel az emberi tényező fejlesztésének kérdéseire (Letöltés dátuma: 2022.01.14) https://bdi.uni-obuda.hu/sites/default/files/Doktori_(PhD)_ertekezes_-_Szamado_Roza.pdf
25. Bányűsz P., Katona G.(2020) A távoli munkavégzés kiberbiztonsági kockázatai (Letöltés dátuma: 2022.01.14) https://www.ludovika.hu/blogok/cyberblog/2020/11/23/a-tavoli-munkavegzes-kiberbiztonsagi-kockazatai/
26. Wikipédia (Letöltés dátuma: 2022. 01.18) Árbevételi Globális 500 lista (Letöltés dátuma: 2022.01.14) https://en.wikipedia.org/wiki/Fortune_Global_500
27. Vargha B., Kovács T. Dávid G. (2021) Távmunka, otthoni munkavégzés, lehetőségek, kockázatok (Letöltés dátuma: 2022.01.14) https://www.asz.hu/storage/files/files/elemzesek/2021/tavmunka_20210108.pdf
28. KSH (2021) A 15–74 éves foglalkoztatottak távmunkavégzésének éves alakulása (2009–2020) (Letöltés dátuma: 2022.01.14) http://www.ksh.hu/stadat_files/mun/hu/mun0014.html
29. KSH (2021) A 15–74 éves foglalkoztatottak távmunkavégzése demográfiai jellemzőik szerint (2011–2020) (Letöltés dátuma: 2022.01.14) http://www.ksh.hu/stadat_files/mun/hu/mun0015.html
30. KSH (2021) A 15–74 éves foglalkoztatottak távmunkavégzése munkaerőpiaci jellemzőik szerint (2011–2020) (Letöltés dátuma: 2022.01.14) http://www.ksh.hu/stadat_files/mun/hu/mun0016.html
31. Magyar Idők (Letöltés dátuma: 2022. 01.26) Kibervédelem: a Debreceni Egyetemet is érte dzsihadista hackertámadás https://www.dehir.hu/belfold/kibervedelem-a-debreceni-egyetemet-is-erte-dzsihadista-hackertamadas/2016/07/21/feed/
32. Erdősi P. M., Solymos Á. (2018) IT biztonságról közérthetően (Letöltés dátuma: 2022.01.14) https://nki.gov.hu/wp-content/uploads/2019/03/NJSZT_IT_Biztonsag_kozerthetoen_v3.pdf
33. Hausner G. (2021) Szemelvények a katonai műszaki tudományok eredményeiből II. (Letöltés dátuma: 2022.01.14) https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16208/905_KDMI_II_hallgatoi_tanulmanykotet.pdf
34. IBM (2012) BYOD: The landscape and security risks a CIO should consider (Letöltés dátuma: 2022.01.14) https://www.ibm.com/blogs/cloud-computing/2012/06/20/byod-the-landscape-and-security-risks-a-cio-should-consider/?mhsrc=ibmsearch_a&mhq=what%20is%20bring%20your%20own%20device
35. IDG (2014) Kibervédelmi érettség állapota (Letöltés dátuma: 2022.01.14) http://resources.forescout.com/rs/forescouttechnologies/images/IDGConnect_ForeScout_StateofITCyberDefenseMaturity.pdf
36. Kovács L. (2019) Biztonságpolitika: a kibertérben (Letöltés dátuma: 2022.01.14) https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12821/Biztonsagpolitika%20a%20kiberterben.pdf;jsessionid=CAD064F3C830F28E4E1DA371070078A1?sequence=1
37. Kovács L. (2018) Kiberbiztonság és -stratégia (Letöltés dátuma: 2022.01.14) http://kovacsx.hu/download/books/KovacsLaszlo_A_kiberbiztonsag_es_strategia.pdf
38. ISACA.Hu (2021) ISACA Információbiztonsági Helyzetkép 2021 (Letöltés dátuma: 2022.01.14) https://www.Isaca.hu

39. Arzl G. (2014) Nemzeti infokommunikációs stratégia 2014-2020 (Letöltés dátuma: 2022.01.14) https://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf
40. Som Zoltán (2021) Doktori (PhD) értekezés, Kibertudatosság különböző színtereken (Letöltés dátuma: 2022.01.14) https://antk.uni-nke.hu/document/akk-copy-uni-nke-hu/Som%20Zolt%C3%A1n%20diszszert%C3%A1ci%C3%B3tervezet.pdf
41. EU Kiberbiztonsági Stratégia (2013): Az Európai Unió Kiberbiztonsági Stratégiája, Cybersecurity Strategy of the European Union, 2013 (Letöltés dátuma: 2022.01.14) https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
42. 25. számú Magyar Informatikai Biztonsági Ajánlások 1.0 verzió, Közigazgatási Informatikai Bizottság, (KIB) 2008. június). (Letöltés dátuma: 2022.01.14) https://regi.ugyintezes.magyarorszag.hu/srv/letolt?id=47417241&lang=hu
43. NKI honlap (2022): Korai figyelmeztető rendszer, early warning system (EWS) In: NBSZ NKI honlap, 2022 (Letöltés dátuma: 2022.03.28.) https://nki.gov.hu/ews/
44. NKI tájékoztatás (2022): Sérülékenységvizsgálat, automatizált sérülékenységi rendszer In: NBSZ NKI honlap, 2022 (Letöltés dátuma: 2022.03.28.) https://nki.gov.hu/szolgaltatasok/tartalom/serulekenysegvizsgalat/
45. ECA jelentés (2022): Európai Számvevőszék (ECA) különjelentés - Az uniós intézmények, szervek és ügynökségek kiberbiztonsága In: ECA honlap, 2022 március (Letöltés dátuma: 2022.04.06.) https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=60922

Felhasznált jogszabályok, közjogi szervezetszabályozó eszközök, EU jogi aktusok

Törvények:

Magyarország Alaptörvénye (2011. április 25.) (Alaptörvény)

Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ekertv.)

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.)

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. (Lrtv.)

2019. évi LXXIX. törvény a Magyarország 2018. évi központi költségvetéséről szóló 2017. évi C. törvény végrehajtásáról

2020. évi CXVII. törvény a Magyarország 2019. évi központi költségvetéséről szóló 2018. évi L. törvény végrehajtásáról

2021. évi CXVI. Törvény a Magyarország 2020. évi központi költségvetéséről szóló 2019. évi LXXI. törvény végrehajtásáról

Rendeletek:

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 szóló 41/2015. (VII. 15.) BM rendelet (Ibtv. vhr.)

A Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 301/2013. (VII. 29.) Korm. rendelet (NEIH rendelet)

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

A Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 301/2013. (VII. 29.) Korm. rendelet

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 (Kiber-irányítási rendelet)

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

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 Kormányzati Adatközpont működéséről szóló 467/2017. (XII. 28.) Korm. rendelet

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

Az elektronikus információbiztonsági korai figyelmeztető rendszerről szóló 214/2020. (V.18.) Korm. rendelet

Európai Unió jogi aktusai:

2008/114/EK tanácsi irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (ECI irányelv)

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 (EU NIS irányelv)

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/881 RENDELETE (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (EU kiberbiztonsági rendelet)

A Bűnüldözési Együttműködés Európai Uniós Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről szóló, AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/794 rendelete

Kormányhatározat:

Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat, amely a 1163/2020. (IV. 21.) Korm. határozattal került megújításra (Nemzeti Biztonsági Stratégia)

Magyarország Nemzeti Kiberbiztonsági Stratégiájának elfogadásáról szóló 1139/2013. (III. 21.) Korm. határozat (Nemzeti Kiberbiztonsági Stratégia)

Magyarország Nemzeti Infokommunikációs Stratégiájáról szóló 1069/2014. (II. 19.) Korm. határozat (NIS stratégia)

A Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről szóló 1456/2017. (VII. 19.) Korm. határozat (NIS monitoring jelentés)

A Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről szóló 1456/2017. (VII. 19.) Korm. határozat megvalósításához kötődő feladatok teljes körű ellátásához szükséges költségvetési források biztosításáról, valamint a feladatokhoz kapcsolódó egyes határidők módosításáról szóló 1988/2017. (XII. 19.) Korm. határozat

Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat (Hálózati Biztonsági Stratégia)

3. számú függelék: Fogalomtár

[1] kiber	(a kübernétész görög szóból, jelentése: kormányos) eredeztethető a szabályozás, vezérléssel foglalkozó kibernetika tudomány-ból levágott önállóan is megjelenő (elsőként tudományos fantasztikus irodalomban) fogalom, átvett értelmezés szerint a húsbavágó (meta-space) ellentétje (cyber-space).
[2] alapvető szolgáltatás	Az Lrtv. szerinti alapvető szolgáltatást nyújtó szervezeteknek az a szervezet minősülhet,akinek az EU NIS irányelv szerinti ágazatban, alágazatban nyújtott szolgáltatása elektronikus információs rendszertől függ, melyet érintő biztonsági esemény jelentős zavart okozna az általa nyújtott szolgáltatás biztosításában. Az alapvető szolgáltatást nyújtó szervezetek körét az ágazati kijelölő hatóság határozza meg.
[3] zárt célú elektronikus információs rendszer	Az Ibtv. alapján zárt célú elektronikus információs rendszer a nemzetbiztonsági, honvédelmi, rendészeti, diplomáciai információs feladatok ellátását biztosító, rendeltetése szerint elkülönült elektronikus információs rendszer, amely kizárólagosan a speciális igények kielégítését, az e célra létrehozott szervezet és technika működését szolgálja.
[4] korai figyelmeztető rendszer (EWS)	A 214/2020. (V. 18.) Korm. rendelet 1. § g) pontjában foglaltak szerint a korai figyelmeztető rendszer („early warning system") központosított előrejelző rendszer, amely az egyes egyirányúan összekapcsolt védett elektronikus információs rendszerek hálózati forgalmának szenzorokkal történő elemzésével automatizált módon azonosít információbiztonsági kockázatokat, valamint biztonsági eseményekre, adatokkal való visszaélésre vagy ezek kísérletére utaló eseményeket.
[5]ENISA	Az ENISA (European Union Agency for Cybersecurity) a 2004-ben létrehozott és a 2019/881 számú EU rendeletnek (kiberbiztonsági rendelet) által megerősített Európai Uniós Kiberbiztonsági Ügynökség, amely célja szerint hozzájárul az uniós kiberpolitikához, kiberbiztonsági tanúsítási rendszerek alkalmazásával javítja az információ-kommunikációs termékek, -szolgáltatások és -folyamatok megbízhatóságát, együttműködik a tagállamokkal és az uniós szervekkel és segíti Európát abban, hogy felkészüljön a jövő kiberbiztonsággal kapcsolatos kihívásaira. A közösségi intézmény a tagállamokkal együttműködésben arra törekszik, hogy fokozza az uniós infrastruktúra ellenálló-képességét, és megőrizze Európa polgárainak digitális biztonságát.
[6]DG CNECT	Az Európai Bizottság Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága (DG for Communications Networks, Content and Technology) az Európai Unióban a digitális egységes piaccal, az internetbiztonsággal, valamint a digitális tudománnyal és innovációval kapcsolatos uniós szakpolitikáért felelős. Közösségi szinten felelősségi területei közé tartozik a digitális gazdaság és társadalom, valamint a kutatás és innováció.
[7]Europol EC3	A Bűnüldözési Együttműködés Európai Uniós Ügynöksége (European Cyber Crime Center) fő célja az uniós polgárok javát szolgáló biztonságosabb Európa megteremtése, a számítástechnikai bűnözés tagállami szintű felszámolása. Az EU 216/794 számú rendelete megerősíti az Europolnak az uniós bűnüldöző hatóságok közötti együttműködés támogatásában betöltött szerepét, annak érdekében hogy fokozni tudja erőfeszítéseit a terrorizmus, a kiberbűnözés, valamint a bűnözés egyéb súlyos, szervezett formái elleni küzdelemben. Minden nemzeti egység legalább egy összekötő tisztviselőt jelöl ki az Europolhoz.
[8] ISACA	Az ISACA-t (Information Systems Audit and Control Association)1969-ben alapították az egyesült államokban a számítástechnika

	elterjedésével felmerülő problémák közös szakmai fórumaként az elektronikus adatfeldolgozó rendszerek ellenőreinek egyesületét. 1976-tól oktatási és kutatási közösséggé is vált az információtechnológia irányítása és ellenőrzése terén szerzett ismeretek és értékek bővítésére. Jelenleg több mint 140 000 tagot számláló nemzetközi közösséggé fejlődött. 1991-óta magyarországi egyesületként a nemzetközi ISACA magyarországi szakmai szervezeteként is működik tagozat.
[9] információs rendszerek biztonsága	Az Ibtv. fogalmi definíciója szerint az elektronikus információs rendszer biztonságát jelenti 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.
[10] bizalmasság	Az Ibtv. fogalmi definíciója szerint a bizalmasság az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról
[11] sérthetetlenség	Az Ibtv. fogalmi definíciója szerint a sérthetetlenség az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
[12] rendelkezésre állás	Az Ibtv. fogalmi definíciója szerint a rendelkezésre állás annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.
[13] logikai védelem	Az Ibtv. fogalmi definíciója szerint a logikai védelem az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.
[14] fizikai védelem	Az Ibtv. fogalmi definíciója szerint a fizikai védelem a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem.
[15] adminisztratív védelem	Az Ibtv. fogalmi definíciója szerint az adminisztratív védelem a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás.
[16]CERT-EU	A CERT-EU az Európai Unió intézményeinek, szerveinek és hivatalainak eseménykezelő központja, számítógépes vészhelyzeteket elhárító csoportja (EUCERT Computer Emergency Response Team for the EU Institutions).

1052 Budapest, Apáczai Cs. J. u. 10. | 1364 Budapest 4. Pf. 54
TEL: +36 1 484 9100
email: szamvevoszek@asz.hu
web: www.asz.hu | www.aszhirportal.hu