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

A hálózati és információs rendszerek biztonságára vonatkozó Stratégia

Az infokommunikációs technológiai robbanás jelentős változásokat eredményez a társadalom minden területén. A kormány 2014-ben elfogadta és meghirdette a Nemzeti Infokommunikációs Stratégiát, amely négy pillér mentén – digitális infrastruktúra, digitális gazdaság, digitális állam, digitális készségek – a teljes hazai digitális környezet fejlesztését tűzte ki célul.
A modern állam, annak minden szervezete és állampolgára szükségszerűen egyre szélesebb rétegben felhasználója az egyre összetettebb elektronikus infrastruktúráknak, az elektronikus információs rendszereknek.
Az információs társadalom lehetőségeinek dinamikus fejlődésével együtt járó előnyök mellett azonban a visszaélések, a támadások, a fenyegetések erősödése is komoly kihívásként van jelen szinte minden területen.
Feladatok sora vár megoldásra nem csupán a technika fejlődésének követése okán, de ezzel párhuzamosan a biztonság, a fenyegetettség különböző vetületeit illetően is.
Az infokommunikációs technológiák, eszközök lehetőségeket teremtenek a fejlődés az innováció minden területén, de lehetőséget jelentenek a terrorizmus, a kiberbűnözés számára is. Minél szélesebb körű ezen lehetőségek kiterjedése, annál nagyobb energiát, figyelmet igényelnek a biztonsági, védelmi kérdések.
Az innovatív és biztonságos kibertér megvalósítása a kiberbiztonsággal foglalkozó szakemberek, állami és piaci szereplők, illetve az állampolgárok közös érdeke, közös feladata.

A hálózati és információs rendszerek biztonságára vonatkozó Stratégia (a továbbiakban: Stratégia) Magyarországra terjed ki, célja a szabad, biztonságos és innovatív kibertér megteremtése, Magyarország versenyképességének növelése, az innovációk, az új technológiai megoldások biztonságos módon történő bevezetése, illetve adaptálása a digitalizálódott államigazgatási, kormányzati és gazdasági területeken, a biztonságosabb elektronikus közigazgatási rendszer létrehozása, illetve az állami szolgáltatások innovatív fejlesztése, valamint a kiberbiztonság, a tudatosság növelése, a felkészültség szintjének emelése a társadalom minden területén.

A Stratéga a kormányzati stratégiai irányításról szóló 38/2012. (III. 12.) Korm. rendelet stratégiaalkotásra irányadó rendelkezései alapján szakpolitikai stratégiának minősül.

Előzmény, kapcsolódások

Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat (a továbbiakban: NKS) – a kibertér létrejöttének következtében megváltozott nemzeti és nemzetközi környezetben – kiemeli a kiberbiztonság megteremtésének és biztosításának fontosságát, valamint rögzíti, hogy Magyarország a kibertér védelemével összefüggő feladatok ellátását felelősséggel vállalja.
Az NKS alapvető célja, hogy az információbiztonság alappilléreinek megteremtésével, továbbá a már meglévő eszközök, szervezetek és tudás felhasználásával, továbbfejlesztésével biztosítsa a szabad, biztonságos és innovatív kibertér kialakítását, ennek érdekében fontos és alapvető célokat határozott meg, úgymint:
a) a kormányzati felelősségbe tartozó szervezeti rendszer, továbbá koordináció létrehozása,

b) a nemzetközi együttműködések fokozása,
c) a köz- és magánszféra közös felelősségvállalásának kialakítása,
d) az oktatás, kutatás-fejlesztési programok ösztönzése,
e) a tudatosság növelése,
f) a gyermekvédelem szerepének megerősítése.

Az NKS 2013-ban először határozta meg a globális kibertér részeként a magyar kibertér gazdasági és társadalmi életben betöltött meghatározó szerepét. Az NKS mentén, a kibertérből érkező fenyegetések és az ezzel járó kockázatok tudatában megkezdődött a magyar jogi szabályozás előkészítése kormányzati, piaci és társadalmi szereplők összefogásával. Az NKS-sel együtt elfogadott és azóta többször módosított, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Információbiztonsági törvény) megteremtette azt a jogszabályi környezetet, amely elsősorban az állami, közigazgatási elektronikus információs rendszerek tekintetében elősegítette a kiberbiztonság területén működő állami szervezetek kialakítását és megszilárdítását.

A Nemzeti Kibervédelmi Intézet szervezésében és informatikai biztonsági szakértők bevonásával a 2017 elején megalakult Információbiztonsági Stratégiai Bizottság a rendelkezésre álló elemzések, illetve a Digitális Jólét Programban megfogalmazott helyzetértékelés és SWOT elemzés figyelembevételével iránymutatásokat fogalmazott meg az újonnan létrejövő stratégia célkitűzéseire vonatkozóan.

2016. július 19-én az Európai Unió hivatalos lapjában megjelent a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016. július 6-i 2016/1148 (EU) európai parlamenti és tanácsi irányelv (NIS irányelv), mely az első közösségi szintű szabályozás az információbiztonság területén, mely kötelezően és geopolitikai alapon határoz meg szabályokat és kötelező együttműködést egyes intézmények számára. A NIS irányelv előírja az EU-tagállamok számára a rendelkezéseivel harmonizáló stratégiaalkotás kötelezettségét.

A Stratégia megalkotása során az NKS-ben megfogalmazott értékeket megtartva, annak eredményeire építve, de az új kihívásokra, fenyegetésekre reagálva, az új lehetőségek és célok azonosításával kell erősíteni a hálózati és információs rendszerek védelmét annak érdekében, hogy az minden tekintetben megfeleljen a modern kor kihívásainak.

A Stratégia a Nemzeti Infokommunikációs Stratégia 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 (a továbbiakban: DJP 2.0) által az „Információbiztonság és kibervédelem” vonatkozásában deklaráltakkal kiegészítve, annak tartalmával azonosulva együtt funkcionál és azzal párhuzamosan fejlődik. Mindkét dokumentum előmozdítja Magyarország kiberbiztonsági érdekeinek és céljainak elérését azáltal, hogy meghatározza azon nemzeti célokat, irányokat, feladatokat és eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a kibertérben.

A DJP 2.0 komplex rendszere a digitalizáció társadalmi és gazdasági hatásainak optimalizálását célozza meg, annak érdekében, hogy előnyeit maximalizálhassa a társadalom és a gazdaság minden területén.

Jogszabályok, hazai stratégiákhoz való kapcsolódás

Jelen Stratégia:
a) leképezi az Alaptörvényben megfogalmazott alapértékeket (szabadság, biztonság, jogállamiság, nemzetközi és európai együttműködés);
b) alapvetésként kezeli a 2001-ben elfogadott Budapesti Konvencióban („Convention on Cybercrime"), megfogalmazott, nemzetközileg elfogadott alapelveket;
c) illeszkedik a NATO 2010 novemberében elfogadott Stratégiai Koncepciójához, a Szövetség 2011 júniusában elfogadott Kibervédelmi Politikájához és ennek végrehajtási tervéhez, valamint a 2010. november 19–20-ai lisszaboni és a 2012. május 20–21-ei chicagói NATO-csúcs, továbbá a 2016-os varsói NATO-csúcs dokumentumaiban megfogalmazott Szövetségi kibervédelmi elvekhez és célokhoz;
d) igazodik az Európai Bizottság és az Európai Unió közös kül- és biztonságpolitikájának főképviselője által 2013. február 7-én „Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér" címmel közzétett közös közleményhez;
e) hozzájárul a NIS-irányelv hazai implementációjához;
f) illeszkedik az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény információbiztonsági célkitűzéseihez, a törvényben rögzített szervezeti struktúrához;
g) figyelembe veszi a kormányzati stratégiai irányításról szóló 38/2012. (III. 12.) Korm. rendelet stratégiaalkotásra irányadó rendelkezéseit;
h) részletezi az 1035/2012. (II. 21.) Korm. határozattal elfogadott, Magyarország Nemzeti Biztonsági Stratégiájának 31. pontjában felvázolt kihívásokra adandó válaszlépéseket;
i) választ ad a Magyarország Nemzeti Katonai stratégiájának elfogadásáról szóló 1656/2012. (XII. 20.) Korm. határozat 33., 52. és 82. pontjaiban felvázolt kihívásokra;
j) illeszkedik az 1069/2014. (II. 19.) Korm. határozattal kiadott, Magyarország Nemzeti Infokommunikációs Stratégiájában a 2014-2020–as időszakra megfogalmazott információbiztonsági célkitűzésekhez;
k) felhasználja a Nemzeti Infokommunikációs Stratégia 2016. évi monitoring jelentés, illetve a Digitális Jólét Program 2.0 helyzetelemzéseit;
l) integrálja a Digitális Jólét Program keretében létrejött Magyarország Digitális Gyermekvédelmi stratégiájában, Magyarország Digitális Exportfejlesztési Stratégiájában, valamint a Magyarország Digitális Oktatási Stratégiájában (MDOS, 2017) megfogalmazott biztonsági vonatkozású célkitűzéseket.

A Stratégia által érintett ágazati jogszabályok és közjogi szervezetszabályozó eszköz:

1. Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény
2. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény
3. Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény
4. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
5. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet
6. Az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 360/2013. (X. 11.) Korm. rendelet

7. A létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről szóló 541/2013. (XII. 30.) Korm. rendelet
8. 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
9. 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
10. Az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendelet
11. A pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 330/2015. (XI. 10.) Korm. rendelet
12. Az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 249/2017. (IX. 5.) Korm. rendelet
13. A bejelentés-köteles szolgáltatást nyújtókról szóló 410/2017. (XII. 15.) Korm. rendelet
14. 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
15. A hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelv átültetésével kapcsolatos feladatok ellátásához szükséges források biztosításáról szóló 1233/2018. (IV. 25.) Korm. határozat

A Stratégia szempontjából alapvető fogalmak értelmezése

A kibertér: globálisan összekapcsolt, decentralizált, folyamatosan változó elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amely Magyarországon található, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.

A kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.

Biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.

Hálózati és információs rendszer: az elektronikus hírközlésről szóló törvényben meghatározott elektronikus hírközlő hálózat, illetve minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy ezek működése, használata, védelme és karbantartása céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

A hálózati és információs rendszerek biztonságára vonatkozó stratégia megalkotásának indokoltságával kapcsolatos megállapítások

A digitális technológia által nyújtott – szinte mindenki számára elérhetővé vált – lehetőségek számottevő kiberbiztonsági kockázatot jelentenek azáltal, hogy a kibertérből érkező fenyegetések megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatok rendeltetésszerű működését, veszélyeztetik a nemzetállamok információs vagyonát és a kritikus infrastruktúra elemeit. A nagyszabású kibertámadások egyre gyakoribbak. Nő a kiberfenyegetések komplexitása és volumene, és a különféle csoportok, szervezetek is egyre intenzívebb módon használják fel a kiberteret ideológiák terjesztésére.

A kiberbűnözés fő célja a károkozás, a pénzügyi és a személyes adatok tömeges megszerzése, illetve a gazdasági, pénzügyi, politikai befolyásolás. Az adatlopáson túl elterjedt az elektronikus szolgáltatások károkozási célú megbénítása, illetve kéretlen levelek és kártékony kódok terjesztése, robothálózatok (fertőzött gépekből álló, kártékony célra felhasználható hálózatok) kialakítása. Jelentős fenyegetés a hacktivizmus, mely gyakran ideológiai motivációjú támadásokat takar valamilyen ideológiai cél elérése vagy valamilyen ideológia közvetítése érdekében. Egyre növekvő veszélyt jelentenek azok a – jellemzően kiberkémkedés célú – kifinomult, rejtett támadások, melyek mögött feltételezhetően állami támogatás áll.

Fontos veszélyforrást jelentenek a rendkívül szofisztikált támadások, amelynek keretében a támadók hosszú időn át elrejtve tudják végezni a károkozó tevékenységüket (információszivárogtatás, rombolás, kémkedés, stb.).
A hálózati és információs rendszerek, mint kritikus információs infrastruktúrák elleni támadások egyre gyakoribbá, komplexebbé és kifinomultabbá válnak. A támadásokra jellemző, hogy a társadalom működésének fenntartásához szükséges alapfunkciókat akadályozzák, ezért pedig a társadalom belső kohézióját próbálják gyengíteni.

A kritikus infrastruktúrák elleni kibertámadások száma szignifikáns növekedést mutat. E növekedést támasztja alá, hogy az ipari rendszereket ért különböző kibertámadások elhárításával foglalkozó ICS-CERT (az USA kritikus infrastruktúrák biztonságával foglalkozó szervezete) adatai alapján míg 2010-ben mindössze 39 incidenst kellett a központnak kezelnie az Egyesült Államok területén, addig ez a szám már 2011-ben 140, 2016-ban pedig 290 volt.

Az Eurostat adatai szerint[1] napjainkban gyakorlatilag az összes EU-ban működő vállalkozás (98%) használ számítógépeket, és közülük csak 32% rendelkezik formálisan meghatározott

[1] Felhasznált források:
https://ec.europa.eu/eurostat/cache/infographs/ict/
https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/main-tables
https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database

információ-biztonsági politikával. A nagyvállalatok esetében ez a részesedés elérte a 72%-ot, míg a kis- és középvállalkozások esetében kevesebb, mint egyharmad volt (31%).

Az Eurostat gazdasági társaságok informatikai biztonsági felkészültségére vonatkozó 2016-os adatai szerint Magyarország lemaradással küzd az Európai Unió országai körében, ugyanis a kis- és középvállalkozási szektor mindössze 9 %-a rendelkezik információbiztonsági politikával, míg a magyar nagyvállalatok esetében ez az arány 53 %.

A magyar gazdasági társaságok közül a legfelkészületlenebbnek mondható építőipari szektorban átlagosan 3%, míg a legfelkészültebb infokommunikációs szektorban is csak 36% rendelkezik informatikai biztonsági szabályzattal. Míg EU átlagban a gazdasági társaságok több mint 20%-a gondoskodik védelemről az adatok megsemmisülésével vagy sérülésével járó biztonsági esemény bekövetkezte esetére, addig ez az arány a magyarországi vállalkozások esetében egyik kockázat esetében sem éri el a 10%-ot.

A vonatkozó adatok szerint a hazai internetezők 75%-a Windows operációs rendszert használ, azon belül az elavult, sérülékeny, a Microsoft által biztonsági frissítésekkel 2014 óta nem támogatott Windows XP-t 10% használja még mindig, miközben annak globális részesedése ennek már alig ötöde (2,2%). Rohamosan terjed a mobiltelefonról vagy egyéb okos eszközről internetezők aránya, azon belül is az Android operációs rendszer a legnépszerűbb (38%), melynek biztonságos használata több odafigyelést igényel a felhasználótól, és a készülékgyártók többsége a kiadástól számított néhány év után nem nyújt biztonsági frissítéseket.

A Világbank 2016. évi adatai alapján a magyarországi internetes kiszolgálók (szerverek) jóval kisebb arányban alkalmaznak biztonságos titkosítási megoldásokat, mint az Európai Unió vagy akár az OECD országainak átlaga.

Az Eurostat IT szakemberek munkaerő-piaci helyzetére vonatkozó 2016-os adatai szerint EU-szerte a vállalkozások alig több mint negyede alkalmaz valamilyen IT szakembert. Amíg ez az üzemeltetési feladatkörök esetében többnyire saját munkavállalót jelent, addig ez az információ- és adatbiztonsági munkakörök esetében a vállalkozások több mint felénél kiszervezésre kerül.
Azon vállalkozások közül, amelyek valamilyen IT szakembert terveztek felvenni, a magyarországiak több mint fele számolt be nehézségről, míg ez az arány EU átlagban csak 40%.

A legfrissebb adatok szerint Magyarországon 14,1 %, világviszonylatban 7,8 % a fertőzött gépek aránya. Néhány európai országhoz való viszonyítás kedvéért pl. Németországban 2,9 %, Franciaországban 5,5 %, Horvátországban 10,2 %, Szlovákiában 7,6 % ez az arány.

A Magyar Nemzeti Bank (MNB) adatai alapján 2016-ban a pénzintézeteknek 1,3 Mrd Ft kára keletkezett elektronikus pénzforgalombeli visszaélésekből – túlnyomó többségében interneten és mobiltelefonon keresztül kezdeményezett tranzakciókból –; ugyan a felismert kísérletek közel 90%-a meghiúsult, a kárértékben ez így is csak 50% körüli csökkenést eredményezett.

---

https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_enterprises
http://ec.europa.eu/information_society/newsroom/image/document/2018-20/hu-desi_2018-country-profile-lang_4AA43283-EC48-996F-09918493E34A691F_52334.pdf

Az ilyen típusú károk nagyságrendileg a bankkártya-csalásokból származó károkkal mérhetőek össze, azonban jóval meghaladták a papíralapú tranzakciókhoz, vagy akár a pénzjegykiadó automatákhoz köthető visszaélésekből eredő károkat.

Az elektronikus rendszerekre visszavezethető káresetek száma és összértéke is növekvő tendenciát mutat az MNB által vizsgált 2008. és 2016. közötti időszakban.

Az Eurostat lakossági internethasználatra vonatkozó 2008-2016-os adatai szerint a magyar 16-74 évesek majdnem fele (48%) használta már arra az internetet, hogy valamilyen közintézménnyel kapcsolatba lépjen, ez az arány a 2008-as 28%-os értékről fokozatosan zárkózott fel az EU országok átlagához, annak ellenére, hogy a magyar lakosság némileg kisebb arányban (79%) használja az internetet, mint az EU-átlag (82%). Az EU polgárainak (akik a 2016-os felmérést megelőző évben internetet használtak) 71%-a valamilyen személyes adatot megosztott már online. A leggyakoribb típusok a kapcsolattartási adatok (az internethasználók 61%-a), amelyet személyes adatok, például név, születési idő vagy személyi igazolvány száma (52%) és fizetési adatok, például hitel / betéti kártya vagy bankszámlaszám (40%). Közel több mint egyötöde (22%) szolgáltatott más személyes adatokat, például fényképeket, vagy az egészségükre, a foglalkoztatásukra vagy a jövedelmükre vonatkozó információkat.

Úgy tűnik, hogy a fiatalabb generációk könnyebben elérhetővé teszik személyes adataikat: a 16-24 éves internethasználók több mint háromnegyede (78%) megosztott valamilyen személyes információt online, szemben a 65-74 év közötti felhasználók 57%-ával.

Magyarországon az internethasználók 36%-a jelentette, hogy számítógépén vírust vagy más fertőzést talált.

Az állami és önkormányzati intézmények számára informatikai biztonsági követelményeket előíró Információbiztonsági törvény átmeneti intézkedésként lehetőséget biztosít a szervezetek számára, hogy az előírt biztonsági szintet fokozatosan érjék el, amellyel együtt megállapítható, hogy az intézmények jelentős késedelemben vannak a felzárkózást illetően. Új biztonsági követelmények teljesítése egy meglévő rendszerben lényegesen nagyobb ráfordítást igényel, mint a követelmények figyelembevételének többletigénye egy új rendszer tervezése során. Mivel az intézmények számára sem alanyi, sem pályázati úton nem állt rendelkezésére forrás ezen biztonsági többletigények teljesítésére, így ezen követelmények csak azon kivételes esetekben teljesülnek, ahol az intézmény azt kigazdálkodta, illetve új fejlesztése során figyelembe vette.
A biztonsági követelmények nagyobb arányú teljesülésének kikényszerítése érdekében a Nemzeti Elektronikus Információbiztonsági Hatóság (a továbbiakban: NEIH) 2016-tól a Közigazgatás-fejlesztési Operatív Program (KÖFOP) pályázati felhívásában is publikálásra került módon integrálta ellenőrzését a pályázati eljárásba. Ennek keretében a NEIH a KÖFOP projektek által finanszírozottan létrejövő elektronikus információs rendszerek információbiztonsági előírásoknak és követelményeknek való megfelelésének ellenőrzését végzi már a tervezési szakasztól kezdődően. Az ellenőrzés mellett a NEIH célzott tudatosító, tájékoztató és tanácsadó tevékenységgel, előadásokkal is segíti az érintetteket a projektek sikeres és biztonságos realizálásának támogatása érdekében.

Az üzleti informatikai fejlesztési projektek kiberbiztonsága terén a hazai piac érettsége jelenleg alacsony szintű. A hazai vállalatok, különösen a kis- és középvállalkozások kkv-k a digitális fejlesztési projekteknél jellemzően kevés figyelmet és erőforrást fordítanak a

kiberbiztonságra. Ennek oka az alacsony tőkeellátottságban, valamint abban keresendő, hogy a kiszolgált ügyfelek digitális attitűdjében nem bír központi szereppel a biztonság, így nem is támasztanak magas kiberbiztonsági elvárásokat a szolgáltatókkal szemben.
Az informatikai projektektől a piac elsősorban alacsony beruházási, üzemeltetési költségeket vár el, másodsorban a funkcionális és a teljesítmény-követelmények teljesítésére koncentrál.
A kiberbiztonsági szempontok azoknál a piaci szereplőknél szorulnak kevésbé háttérbe, ahol a hatályos törvényi szabályozás adatvédelmi, üzletfolytonossági követelményeket támaszt, melyeket a hatósági felügyelet érvényesít (pl. pénzforgalmi szolgáltatók, biztosítók esetében).
Mindezek következtében a hazai digitális fejlesztési projekteknél az informatikai biztonsági irányítás nem éri el a kibertérben azonosított jelenlegi és várható fenyegetések és az implementált rendszerek sérülékenységei – valamint az ezekből eredő kockázatok – miatt szükséges színvonalat.

A létfontosságú infrastruktúrák védelmével kapcsolatban a következőket szükséges rögzíteni. A 2008 óta hatályos az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelv alapján a létfontosságú rendszerelem státusz meghatározása ágazatonként eltérő módszertan szerint történik, de minden esetben tételes kijelöléssel zárul. Ágazatok, amelyekben 2017. december 31-ig meghatározásra kerültek a kijelölés kritériumai:
a) energia,
b) víz,
c) agrárgazdaság,
d) közbiztonság-védelem,
e) egészségügy,
f) pénzügy,
g) honvédelem,
h) infokommunikációs technológiák.

Regisztrált bűncselekmények száma az általános ügyekkel és értékeléssel foglalkozó európai uniós munkacsoport (a továbbiakban: GENVAL) definíciói alapján

Regisztrált bűncselekmények száma GENVAL definíciók alapján	**2013.**	**2014.**	**2015.**	**2016.**	**2017.**
Kizárólag az információs rendszereket érintő - elsősorban az informatikai támadásokkal kapcsolatos - cselekmények	**3554**	**2398**	**2819**	**4187**	**5098**
Információs rendszer felhasználásával elkövetett csalás	250	1398	2176	3409	4467
Információs rendszer vagy adat megsértése	823	565	520	702	586
Információs rendszer védelmét biztosító technikai intézkedés kijátszása	580	31	15	44	8
Készpénz-helyettesítő fizetési eszközzel visszaélés	1897	388	95	20	28
Tiltott adatszerzés	4	16	13	12	9
Cselekmények, amelyeknél a számítógépes/informatikai rendszerek eszközként vagy célpontként szolgálnak, különösen az online bankkártyacsalás esetében	**3959**	**917**	**873**	**23439**	**1120**
Készpénz-helyettesítő fizetési eszköz hamisítása	49	118	95	392	713
Készpénz-helyettesítő fizetési eszköz hamisításának elősegítése	3	1	3	3	1
Készpénz-helyettesítő fizetési eszközzel visszaélés	3907	798	775	23044	406
Összesen:	**7513**	**3315**	**3692**	**27626**	**6218**

A GENVAL 2016-ban áttekintette és értékelte a magyarországi számítástechnikai bűnözés megelőzését és az ellene folytatott küzdelmet érintő európai szakpolitikák gyakorlati végrehajtását, illetve működését.

Az értékelés eredményeképpen a GENVAL arra a következtetésre jutott, hogy Magyarország elkötelezett a számítógépes bűnözés elleni hatékony hazai és nemzetközi összefogással történő fellépés tekintetében, amelynek számos kézzel fogható jelét is adta (2011-es elnökségi konferencia, 2012. Budapesti Kibertér Konferencia, Kiberbiztonsági Stratégia, intézmény-rendszer és reagálási képességek átfogó fejlesztése, ET, ENSZ, EU együttműködési formákban való aktív részvétel, valamint a 2018-ban harmadik alkalommal megrendezett Nemzeti Kiberbiztonsági Konferencia, amely az állami és magánszektor közti együttműködés elősegítését, magasabb szintre emelését tűzte ki célul).

Az elmúlt 5 év tapasztalatai alapján kijelenthető, hogy Magyarország a témakört prioritásként kezeli, támogatja a releváns uniós és nemzetközi együttműködési formákat és kezdeményezéseket, igyekszik lépést tartani a trendekkel, a technika fejlődésével. Jelentős előhaladás ment végbe mind az intézményrendszer, mind a rendészeti és válságkezelési mechanizmusok reagálási képességének fejlesztése által. A GENVAL Munkacsoport értékelő Bizottsága néhány javaslatot fogalmazott meg, mint például, hogy szorosabb és szabályozottabb együttműködés kialakítása szükséges a kiberbiztonsági és kiberbűnüldözési terület között.

A Stratégia Irányítási Keretrendszere

A kiberbiztonsággal kapcsolatos jelenlegi és jövőbeni kihívások csak hatékony módon kezelhetők és ehhez hatékony nemzeti kiber-irányítási rendszer szükséges. Figyelembe véve a védelmi kötelezettségvállalásokat a NATO és az Európai Unió szintjén, az európai és a nemzetközi együttműködés és a különböző szintű információ-megosztási megállapodásokat, a NIS-irányelvet, valamint a kiberbiztonságra vonatkozó horizontális jellegű témákat.

Nemzeti Kiberbiztonsági Koordinációs Tanács (a továbbiakban: Tanács) a kormány javaslattevő, véleményező szerve, amely a törvényben meghatározott szervezeteknek a törvényben és végrehajtási rendeleteiben meghatározott tevékenységeit összehangolja, megvalósítva ezzel a Magyarország Nemzeti Kiberbiztonsági Stratégiájában foglalt kormányzati koordinációt. A Tanácsban a kiberbiztonságban érintett szakterületek miniszterei által delegált állami vezetők, valamint egyes, nem a kormány irányítása alatt álló országos hatáskörű szervek vezetői vesznek részt.

A Tanács munkáját az általa felkért gazdasági, tudományos és civil szféra felsővezetőiből álló Kiberbiztonsági Fórum segíti, amely a Tanács munkáját véleményező és javaslattevő szervként segíti.
A Tanács koordinációs tevékenységét, valamint döntéseinek végrehajtását ágazati és funkcionális kiberbiztonsági munkacsoportok segítik. Munkájukban a Tanács és a Fórum javaslatai alapján a kiberkoordinátor által felkért közszolgálati tisztviselők és nem kormányzati szakértők vesznek részt.

Az Információbiztonsági törvény 2015. július 16-ai hatályú módosítása eredményeként 2015. október 1-jétől a Nemzetbiztonsági Szakszolgálat irányítása alatt megalakult a Kormányzati Eseménykezelő Központot (GovCERT-Hungary), a Nemzeti Elektronikus Információbiztonsági Hatóságot, és az E-biztonsági Intelligencia Központot (NBF-CDMA) egységes keretben magába foglaló, koordináltabb, hatékonyabb feladat-végrehajtást és információáramlást lehetővé tevő Nemzeti Kibervédelmi Intézet (NKI). Az NKI rendelkezésre álló kapacitásainak minőségi és mennyiségi fejlesztését indokolja az elektronikus információbiztonsági felügyeleti és támogatási feladatok iránti igények növekedése.

Az Információbiztonsági törvény hatálya alá tartozó állami és önkormányzati szervezetek vonatkozásában a biztonsági események kezelésére általános hatáskörrel a Nemzetbiztonsági Szakszolgálat keretében működő eseménykezelő központ, hatósági jogkörrel pedig a szintén a Nemzetbiztonsági Szakszolgálat keretében működő NEIH rendelkezik.
A Nemzetbiztonsági Szakszolgálat látja el továbbá a NIS irányelv szerinti bejelentés-köteles szolgáltatók tekintetében a hatósági és eseménykezelési feladatokat, valamint – a honvédelmi

célú elektronikus információs rendszerek és a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei kivételével – az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerekkel kapcsolatos eseménykezelési feladatokat.

A honvédelmi célú elektronikus információs rendszerek vonatkozásában a katonai nemzetbiztonsági tevékenységet ellátó szervezet, illetve a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat a saját rendszerei tekintetében önállóan látja el az incidenskezelési, a felügyeleti és egyéb információbiztonsági funkciókat.

Az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt rendszerelemek elektronikus információs rendszerei esetében az Információbiztonsági törvény szerinti hatósági feladatokat a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (BM OKF) látja el.

Az Információbiztonsági törvény hatálya alá nem tartozó elektronikus információs rendszerek, hírközlési szolgáltatók tekintetében az MTA-SZTAKI működtet információbiztonsági eseménykezelő szervezetet (HunCERT).

A Nemzeti Információs Infrastruktúra Fejlesztési (NIIF) Program keretében belül a Kormányzati Informatikai Fejlesztési Ügynökség működtet számítógépes biztonsági esemény-kezelő szervezetet (NIIF CSIRT). Az NIIF CSIRT a magyar köznevelés, felsőoktatás, kutatás és közgyűjtemények szolgáltatójához, az NIIF Programhoz tartozó IT biztonsági és biztonsági eseménykezelő csoport. A csoport célja segíteni a számítógépes és hálózati biztonsági események kezelését és koordinációját minden olyan esetben, amelyben legalább egy NIIF tagintézmény érintett. Az NIIF CSIRT munkacsoportja ezen kívül fontos, biztonsággal, megelőzéssel, illetve elhárítással kapcsolatos információkat is továbbít az NIIF tagintézményeknek.
A Nemzeti Közszolgálati Egyetem Rendészettudományi Kar a felsőoktatási rendszerben szakirányú rendészeti képzésben részt vett, megfelelő létszámú szakember biztosítása érdekében Kiberbűnözés Elleni Tanszéket alapított a Kriminalisztikai Intézeten belül. A kiberbiztonsághoz kapcsolódó képzések, továbbképzések szervezésében, a kibertér biztonságával kapcsolatos oktatási és kutatási tevékenységek és a hozzájuk kapcsolódó erőforrások összehangolásában vesz részt a Nemzeti Közszolgálati Egyetem Kiberbiztonsági Akadémia.

A Stratégia célkitűzései

1. A digitális környezet iránti bizalom erősítése

1.1 Szakmai együttműködés erősítése

A kibertér új kockázataival szemben csak az egymással folytatott megfelelő kommunikáció, a tudásmegosztás és a veszélyhelyzet esetén tanúsított fegyelmezett, koordinált védekezés kínál megoldást.

A biztonsági kérdésekkel, a biztonsági események kezelésének kérdéskörével kapcsolatos feladatok nemcsak az információbiztonsági szakemberek, hanem az elektronikus információs rendszereket működtető szervezetek, az állampolgárok és a média számára is kiemelt jelentőségű, és ennek megfelelő felelősséggel járó tevékenységet jelentenek. Ennek okán a nemzetközi gyakorlatnak megfelelően szükséges létrehozni egy felelősségteljes eljárást és kommunikációt biztosító szabályrendszert (felelős információ-megosztás/„responsible disclosure" szabályai) a sérülékenységek és biztonsági események felismerésére, kezelésére vonatkozóan.

A kiberbiztonsági területen feladatot ellátó kormányzati és nem kormányzati szereplők azonosítása, feladat- és jogköreinek pontos meghatározása, valamint az ezek betöltéséhez szükséges kompetenciák felmérése. Felül kell vizsgálni a szervezetek feladat- és jogköreit, azonosítani kell a lehetséges átfedéseket.
Meg kell határozni az együttműködési és döntéshozatali eljárásrendet ezen szervezetek együttműködésére vonatkozóan.
Prioritás, hogy azonosításra kerüljenek azok a területek, ahol még nem jött létre a szükséges együttműködés. Ezeken a területeken ösztönözni kell az együttműködés kialakítását és a párbeszéd megkezdését.

Intézkedések:

1.) felül kell vizsgálni a kormányzati, piaci, oktatási és civil szereplők együttműködésének eddig létrejött fórumain történő együttműködés hatékonyságát;
2.) olyan fórumot kell biztosítani, ahol lehetőség nyílik a társadalmi párbeszédre és a széleskörű tájékoztatásra, az etikus hackerek szerepének, illetve a társadalom és az etikus hackerek viszonyának tisztázására;
3.) azonosítani kell, hogy mely területen szükséges javítani a meglévő együttműködésen;
4.) a hatóságok, az állami és civil szervezetek, valamint az eseménykezelő központok közötti információ-megosztás, illetve a kölcsönös segítségnyújtás lehetővé tételéhez elengedhetetlen az összehangolt megelőzési, feltárási, mérséklési és reagálási mechanizmusok létrehozása;
5.) ösztönözni szükséges a piaci és államigazgatási szervezetek által indított „Bug Bounty" vagyis „Hibavadász" programokat, amelyek keretében az informatikai rendszerek gyengeségeit feltárni kívánó szereplők rendezett feltételek és egyértelmű szabályok keretei között tudják felhívni a szervezetek figyelmét a biztonsági hibákra;
6.) a reagáló és védekezési képesség továbbfejlesztése érdekében meghatározott időközönként kiberbiztonsági gyakorlatot kell tartani;
7.) szükséges a köz- és magánszféra közös felelősségvállalásának tudatosítása.

1.2 Biztonságtudatosság növelése

A digitalizálódó világban egyre fontosabb feladattá válik, és fokozott aktivitást igényel az állampolgárok, a társadalom különböző szereplőinek a tudatosítása annak érdekében, hogy a mindennapok részévé váló digitális eszközök és szolgáltatások biztonságos használatát elsajátítsák.

Magyarország aktív szerepet vállal a kiberbiztonsággal összefüggő hazai és nemzetközi tudatosítási fórumok, kampányok munkájában, szervezésében, hogy minél szélesebb célközönség számára elérhető legyen a digitális világ biztonságos használatához szükséges tudás. (Az Európai Hálózat és Információbiztonsági Ügynökség által minden év októberében megrendezésre kerülő Európai Kiberbiztonsági Hónap kampány, Safer Internet program, Digitális Immunerősítő program).

A szakosított intézmények – a civil, a gazdasági és a tudományos területek szereplőinek együttműködésével – támogatják a kibertér biztonságos használatát célzó, gyakorlati tudást elősegítő, figyelemfelhívó-tudatosító tevékenységeket, annak érdekében, hogy az egyéni felhasználók, a vállalatok és a szervezetek magabiztos és biztonságos módon használhassák digitális eszközeiket, valamint a kormányzati és piaci elektronikus szolgáltatásokat.

Napjainkban a média és az állampolgárok részéről is egyre nagyobb érdeklődés és figyelem övezi az egyes jelentősebb sérülékenységeket, biztonsági eseményeket, kampányokat, ezért fontos a lakossági és gazdasági szereplők informálása a hiteles információ- és segítségnyújtás fórumainak elérhetőségeiről.

Magyarország számára a digitális világ ellenőrzéséhez kiemelkedően fontos cél, hogy hiteles adat álljon a Kormány rendelkezésére a lakosság és a gazdasági szereplők tájékozottságáról, tudatosságáról, felkészültségéről, illetve fenyegetettségi helyzetéről.

Intézkedések:

8.) a lakosság és gazdasági szereplők legyenek tudatában annak, hogy hol juthatnak hiteles információhoz és hova fordulhatnak segítségért;
9.) álljanak rendelkezésre hiteles, követéses adatok a lakosság és a gazdasági szereplők tájékozottságáról, tudatosságáról, felkészültségéről, fenyegetettségi helyzetéről;
10.) kerüljenek kidolgozásra olyan ösztönzők, melyek segítségével a kis- és középvállalkozási szektorban az információbiztonsági politikával rendelkező szervezetek aránya növekszik.

1.3 Bűnüldözés - kiber-bűnüldözés fejlesztése

A számítógépes rendszerek segítségével, valamint a számítógépek ellen elkövetett bűncselekmények mára speciális bűncselekményi kategóriát képeznek. Az elkövetett jogsértések magas száma, valamint az általuk okozott kár mértéke indokolttá teszi, hogy a bűnüldöző szervezetek minél hatékonyabban foglalkozzanak ezen esetek felderítésével, azonosításával és ezzel együtt a preventív intézkedések megtételével, valamint a károk mérséklésével, ideértve az elkövetők jövőbeni jogsértő magatartásának visszaszorítását.

Intézkedések:

11.) a rendvédelem és az igazságszolgáltatás rendszere fejlessze a kiber-bűncselekmények elleni fellépés képességét;
12.) működjenek együtt aktívan és osszanak meg információkat az illetékes szervek a kiber-bűncselekmények elleni hazai, valamint nemzetközi szervezetekben, összefogásokban.

1.4 A szakmai irányító intézményrendszer fejlesztése

Kiemelt fontosságú célként tekintendő a kormányzati felelősségbe tartozó szervezeti rendszer, a feladatellátásban érintett intézmények (a nemzetbiztonsági, a honvédelmi, a bűnüldözési, a katasztrófavédelmi, továbbá a létfontosságú intézmények és létesítmények védelmével kapcsolatos feladatokat ellátó szervezetek) feladat- és hatáskörének, valamint együttműködésük szabályainak felülvizsgálata.

A digitális gazdaság ösztönzése, a digitális szakadék felszámolása érdekében elengedhetetlen a magánszektor kiberbiztonságának a támogatása olyan intézménnyel, amely fejlett kibervédelmi megoldásokat képes közvetíteni a magyar vállalati szektor számára.

Az EU tagállamainak biztosítaniuk kell, hogy jól működő CSIRT-ekkel (komputereket érintő biztonsági incidenseket elhárító technikai egységek) és az azokat lehetséges módon koordináló ágazati hálózatbiztonsági vészhelyzeteket elhárító csoportokkal (a továbbiakban: CERT) – rendelkezzenek, amelyek birtokában vannak a biztonsági események és kockázatok kezeléséhez szükséges hatékony és kompatibilis képességeknek, valamint megfelelnek az eredményes uniós szintű együttműködés biztosítására vonatkozó alapvető követelményeknek. Ekképpen lehetőség nyílik lefedni a magánkézben lévő létfontosságú vagy egyéb szempontból kritikus infrastruktúra és a lakossági szolgáltatók tevékenységét is (pl. banki rendszerek, egészségügy). Ezeket az egységeket egy szakosított intézmény képes információ-megosztás szempontjából koordinálni, a további hazai és nemzetközi információmegosztó szervek irányába.

Intézkedések

13.) ki kell jelölni vagy létre kell hozni a NIS irányelv hatálya alá tartozó szektorokban szükséges szakosított intézményeket (CSIRT-ek és hatóságok) az irányelvben megfogalmazott követelményeknek megfelelően;
14.) ki kell alakítani a Stratégiában megfogalmazott céloknak megfelelő szervezeti rendszert;
15.) fejleszteni kell a létfontosságú rendszerek, létesítmények és szolgáltatások információbiztonsági hatósági rendszerét az irányelvben megfogalmazott követelmények ágazatokon átívelő érvényesítése érdekében;

16.) létre kell hozni az Információbiztonsági törvény szerinti eseménykezelő központ mellett – a hatályos kibervédelmi szabályozás kiterjesztésének vizsgálatával – a nemzeti eseménykezelő központot a nemzeti kibertér használóinak szélesebb köre számára elérhető kiberbiztonsági szolgáltatások nyújtása érdekében.

2. Digitális infrastruktúra védelem

2.1 Informatikai fejlesztések minőség-menedzsmentje

A kibertámadások elleni eredményes védekezés egyik alapvető feltétele, hogy az informatikai fejlesztésekben már a tervezéskor markáns szerepet kapjon a minőségbiztosítási folyamatok kialakítása, továbbá a kiberbiztonsági kritériumok meghatározása és mérése.

A nemzetközi iparági sztenderdekkel összhangban a fejlődés javasolt iránya az, hogy az informatikai fejlesztési feladatok esetében a tervezésnél meg kell határozni az alapvető minőségi, ezen belül kiberbiztonsági követelményeket az új IT-megoldással szemben. Fontos, hogy kijelölésre kerüljön egy kompetens felelős, aki a biztonsági követelmények teljesülését ellenőrzi, továbbá, hogy rendelkezésre álljon egy könnyen elérhető, érthető módszertan – valamint: dokumentációs és intézkedésminták és más támogató eszközök –, amelyek segítik a minőségbiztosítási folyamatot.

Intézkedések:

17.) könnyen elérhető, érthető és használható információs bázis kialakítása;
18.) a különböző komplexitású informatikai projektekhez modulárisan felépülő módszertani útmutatók kidolgozása;
19.) a belső minőségbiztosításhoz ingyenes segédletek kialakítása;
20.) egy magyar-angol kétnyelvű, ingyenes, modulárisan felépülő, bárki számára elérhető kiberbiztonsági minőségmenedzsment tudástár kialakítása szükséges.

2.2 Kormányzati elektronikus szolgáltatások biztonságának növelése

A kormányzat és a közigazgatás működését olyan stabil és biztonságos informatikai háttér támogassa, amely lehetővé teszi a közigazgatás belső folyamatainak, illetve a lakosságot és vállalkozásokat célzó közigazgatási szolgáltatásoknak a nagyarányú elektronizálását, továbbá az állami érdekkörbe tartozó információk és tartalmak széles körű digitalizációját és nyilvánosan történő hozzáférhetővé tételét.

Mind a közigazgatás megbízható és stabil működése, mind az elektronikus közigazgatási szolgáltatások, illetve elektronikus közszolgáltatások biztosítása szempontjából kulcsfontosságú, hogy a kormányzati elektronikus információs rendszerek biztonságosan, interoperábilis módon és valamennyi alrendszert, intézményt és felhasználói kört kiszolgálva működjenek. Ennek feltétele egy olyan kormányzati IT-háttér szisztematikus felépítése, amely mind infrastrukturális, mind üzemeltetési, mind pedig fejlesztési szempontból képes a hagyományos IT-szolgáltatások és a várhatóan egyre több területen elterjedő felhőalapú megoldások, illetve alkalmazás-bérlet (ASP) és szoftverszolgáltatások (SaaS) stabil és megbízható biztosítására.

Az elektronikus kormányzati szolgáltatások esetében kiemelten fontos, hogy a közigazgatás oldalán a lehető legmagasabb szinten garantálható legyen a hálózatok, rendszerek, folyamatok és felhasználói adatok biztonsága. Az e-közigazgatási szolgáltatások egyik sikerkritériuma épp annak a biztosítása, hogy az állampolgárok és vállalkozások biztosak lehessenek abban, hogy a rendszerek folyamatosan működőképesek, a szolgáltatások elérhetők, és adataikat

csakis az általuk meghatározott célra, csakis az arra feljogosított rendszerek és személyek láthatják.
Az Információbiztonsági törvény és e törvény felhatalmazása alapján kiadott rendeletek megfelelő alapot nyújtanak az állami és önkormányzati szervek kibervédelmi és információbiztonsági tevékenységéhez. A technika fejlődésével párhuzamosan az állami és önkormányzati szerveknek lépést kell tartaniuk az információbiztonság folyamatosan változó követelményeivel.

Intézkedések:

21.) jöjjön létre és üzembiztosan működjön a stabil és biztonságos kormányzati IT-háttér;
22.) valósuljon meg a nemzetbiztonsági szempontból, illetve a közigazgatás belső működése és az elektronikus közigazgatási szolgáltatások elérhetősége szempontjából létfontosságú információs infrastruktúrák, a közigazgatási belső rendszerek és külső alkalmazások, valamint az ezekben megjelenő felhasználói adatok maximális védelme;
23.) biztosítani kell a közigazgatás belső rendszereit és külső szolgáltatásait kiszolgáló hálózatok, informatikai infrastruktúra és alkalmazások maximális védelmét;
24.) az ágazati sajátosságok figyelembe vételével valósuljon meg a közigazgatás teljes spektrumát átfogó, annak valamennyi alrendszerét érintő biztonsági felügyelet;
25.) kormányzati támogatásban részesülő informatikai fejlesztések teljesülését a biztonsági előírások megvalósulásához kell kötni;
26.) készüljön feladatterv a meglévő e-közszolgáltatásoknál az előírt biztonsági szint elérése érdekében;
27.) a jelenlegi gyakorlat és szabályozás szigorításával legyen biztosítva és kötelezővé téve egy egységes biztonsági követelményrendszer az informatikai fejlesztések számára.

2.3 Nemzetközi együttműködés erősítése

Magyarország a globális kibertér szabad és biztonságos használatának szavatolására törekszik a nemzetközi kapcsolati rendszerén és szervezeti tagságain keresztül, ezért a globális kibertér minden, Magyarországgal hasonló értékrendet valló állami és nem állami szereplőjével kölcsönös bizalmon alapuló együttműködés kialakítására törekszik. Magyarország tovább kívánja erősíteni aktív szerepét a stratégiai és operatív szintű regionális és nemzetközi együttműködésekben, kiváltképp az Európai Unió, a NATO és a közép-kelet-európai régió keretein belül történő kiberbiztonsági együttműködésekben, továbbá az ezen szervezeteken belül történő nemzetközi elvárások és szabályozások megfogalmazásában.

Magyarországnak kiemelt érdeke, hogy fenntartsa aktív együttműködését a nemzetközi közösségek kibervédelmi gyakorlataiban és tervezésében, ezzel lehetővé téve szervezeteink nemzetközi tudásának folyamatos fejlesztését, közös műveleti protokoll kialakítását. Különösen fontos, hogy a hazai intézmények és szervezetek részvétele összehangolásra kerüljön a nemzetközi együttműködési platformokon. A szektorális együttműködést biztosító közösségek és központok (ISAC-ok, szektorális CSIRT-ek) együttműködésében és tevékenységében való aktív részvétel kialakítása is nagy jelentőséggel bír az új célok megvalósítására kijelölt és létrehozott szakosított szervezetek által. Magyarország célja, hogy fenntartsa tevékeny szerepét a biztonsági eseményeket kezelő központok euro-atlanti és globális közösségeiben, szervezeteiben, valamint tovább mélyítse aktív együttműködését a kiberbiztonság egyes területeivel foglalkozó európai vagy nemzetközi szervezetekkel.

Intézkedések:

28.) induljon meg, illetve erősödjön az együttműködés a NIS irányelvben meghatározott európai uniós és a kijelölt hazai intézmények között;
29.) szükséges összehangolni és fokozni a hazai intézmények nemzetközi együttműködését;
30.) a nemzetközi együttműködés előmozdítása és a nemzetközi szintű reagáló és védekezési képesség továbbfejlesztése érdekében nemzetközi szintű kiberbiztonsági gyakorlatokon kell részt venni;
31.) Magyarország mind bilaterális, mind multilaterális kapcsolataiban hangsúlyosan képviselje érdekeit és értékeit a kibertérrel kapcsolatos külkapcsolati tevékenysége során.

2.4 Alapvető szolgáltatások, valamint a létfontosságú infrastruktúrák és szolgáltatásaik védelme

Az egyes létfontosságú infrastruktúrák védelme komplex feladat, amelynek végrehajtásában a különböző állami szerveken túlmenően a gazdasági élet szereplőinek is részt kell vállalniuk.

Kiemelt cél, hogy a kijelölt létfontosságú rendszerek és létesítmények, azon belül az alapvető szolgáltatást nyújtó szereplők, valamint a digitális szolgáltatók üzemeltetői fektessenek egyre nagyobb hangsúlyt hálózati és információs rendszereik kockázatokkal arányos, teljes körű védelmének megteremtésére.

Ki kell alakítani egy kockázatértékelési módszertant, amely lehetővé teszi a kockázatok minél pontosabb azonosítását lehetővé tevő adatok korrelált gyűjtését, a fenyegetett szolgáltatások esetleges kiesése által kiváltott üzleti hatás dinamikus becslését és azon intézkedések azonosítását, amelyekkel a fenyegetésekre való felkészülés kellő időben megkezdhető, továbbá esetlegesen kiváltott hatásuk mielőbb minimalizálható.

A módszertan tartalmazzon olyan mérőszámokat, melyek évenkénti jelentése kötelező a szervezetek számára, egyben alapul szolgálhatnak egy évente megjelenő nemzeti kiberbiztonsági fenyegetettségi jelentés elkészítéséhez.

Intézkedések:

32.) ki kell dolgozni az ágazati szintű kockázatértékelés, kockázat-elemzés módszertanát;
33.) legyenek szabadon hozzáférhetők ágazatközi, illetve ágazat-specifikus konszenzust képviselő ajánlások és jó gyakorlatok a biztonsági célok elérésére vonatkozóan;
34.) elő kell mozdítani az állami intézmények és a magánszektor szereplőinek kölcsönös bizalmon alapuló együttműködésének kialakítását és fenntartását;
35.) álljon a kritikus infrastruktúrák üzemeltetőinek minél szélesebb köre rendelkezésére a védelmet kiegészíteni képes egységes szolgáltatáscsomag;
36.) a létfontosságú rendszerek, létesítmények és szolgáltatások fizikai és kiberbiztonsága területén a hatékony megelőzés és gyors reagáló képesség fejlesztésére célzott

pályázati lehetőségek biztosítása szükséges az üzemeltetők, a szolgáltatást nyújtók, az érintett hatóságok és az eseménykezelő központok működésének fejlesztésére;

37.) a létfontosságú rendszerek, létesítmények és szolgáltatások üzemeltetői felé irányuló információbiztonsági tudatosítási tevékenység fokozása szükséges az érintett hatóságok és szervezetek részvételével;

38.) kerüljenek bevonásra a létfontosságú infrastruktúrák üzemeltetői nemzeti és nemzetközi védelmi gyakorlatokba.

2.5 Kiber- védekező elhárító és reagáló képességek fejlesztése

A kibertérből érkező fenyegetések veszélyességének erősödése miatt a hagyományos, észlelő-követő magatartás meghaladott. Alapvető nemzeti érdek a megfelelő kibervédekezési, elhárítási és reagálási képességek koncentrált rendelkezésre állásának biztosítása.

A cél a meglévő bázison a kiber-védekező, elhárító és reagáló képességek passzív és aktív eszközeinek széleskörű kialakítása és alkalmazása.

A passzív kibervédekezési, elhárítási eszközök az informatikai infrastruktúrában elhelyezett rendszerelemek, amelyek a fenyegetések elleni védelmi funkciót töltenek be, illetve biztosítják a fenyegetésekre vonatkozó információk kellő időben történő rendelkezésre állását. A passzív eszközök közül a fejlesztési tevékenység szempontjából kiemelést érdemel a rosszindulatú infrastruktúrák felfedésére, a támadótevékenység nyomon követésére és azonosítására alkalmas eszköz, illetve tevékenység, amely elengedhetetlen az ellenintézkedések célirányosságának biztosításához.

Az aktív intézkedések a jelenlegi technológiai színvonalon elsősorban ember által végzett tevékenységek, amelyek az informatikai rendszereket érő fenyegetések folyamatos monitorozását, és az azokra való különböző fokozatú reakciókat jelentik.

Intézkedések:

39.) szükséges az észlelési, feldolgozási (elemzés), felderítési képességek fejlesztése, amelyek lehetővé teszik a fenyegetések, illetve támadások felismerését, osztályozását és forrásának megállapítását;

40.) meg kell teremteni ezen képességek logikai összefüggése okán az ágazati szinten egységes és ágazatok közötti koordináción alapuló irányítást és menedzsmentet;

41.) ki kell alakítani a gyors helyzetfelismerés, az értékelés és a kockázatelemzés rendszerét;

42.) ki kell fejleszteni a kiberfenyegetésekre történő különböző fokozatú reagálás eszközrendszerét;

43.) meg kell teremteni a lehetőségét annak, hogy különleges esetekben civil, polgári területen dolgozó szakemberek is részt tudjanak venni a nemzeti kibervédelemben.

3. A gazdasági szereplők támogatása

3.1 Kutatóközpontokkal való együttműködés, valamint a kutatás és fejlesztés szerepének erősítése

A felsőoktatási intézményekben és más nyilvános kutató központokban élvonalbeli képesség alakult ki az információs technológiák biztonsága terén. Azért, hogy ezek a képességek továbbra is Magyarországon fejlődjenek tovább és nagyobb arányban járulhassanak hozzá a nemzet biztonsági céljaihoz, fontos, hogy szoros együttműködés legyen ezen műhelyek és a piac, valamint a kormányzat szereplői között. Az állami kiberbiztonsági kutatás-fejlesztés megerősítéséhez elengedhetetlen a kiemelkedő és nemzetközileg is elismert eredményeket felmutató felsőoktatási és tudományos kutatóműhelyekkel a stratégiai együttműködés kialakítása, valamint az ilyen irányú K+F feladatok és források azon kutatóbázisokhoz történő összpontosítása, ahol a megfelelő szaktudás és technikai háttér már biztosított.

Intézkedések:

44.) legyen biztosított a mérnökök, kutatók képzése és a kiemelkedő tehetségek gondozása, illetve magyarországi tevékenységük feltételei;

45.) létre kell hozni egy kiberbiztonsági szakterületet érintő kutatási stratégiát, melynek célja – a magyar intézményrendszer kiberbiztonságának erősítése érdekében – a magyar fejlesztésű kiberbiztonsági eszközök, szoftverek és termékek alkalmazásának fokozása;

46.) kerüljenek azonosításra a kapcsolódó kutatás-fejlesztési témakörök, továbbá kerüljenek megteremtésre az állami ösztönzési lehetőségek, beleértve a magyar korai fázisú vállalkozások ösztönzését is;

47.) a 45. pontban leírt kiberbiztonsági kutatás-fejlesztési-innovációs stratégia kiemelten kezelje az Európai Unió 2021-2027 között meghirdetésre kerülő K+F+I felhívásainak témáit, ezzel segítve az innovatív magyar szervezeteket abban, hogy a kiemelten tudjanak részt venni a nemzetközi projektekben;

48.) a gazdaságdiplomáciai tevékenységek során legyen cél kiberbiztonsággal foglalkozó magyar szolgáltató- és fejlesztőközpontok megjelenésének támogatása.

3.2 Hazai digitális innováció támogatása, támogatási konstrukciók kialakítása, koordinációs feladatok ellátása

Fontos a hazai digitális innováció támogatása információbiztonsági fókusszal, amely komoly segítséget jelenthet a magyarországi digitalizációban, a kiberbiztonsági tudatosság növelésében és az adatvédelmi képességek elérésében.

A kormányzat már eddig is tett (jelen pillanatban is tartó) jelentősebb intézkedéseket a kiberbiztonság javítása kapcsán a vállalkozásoknál, ezek röviden:

1. 2015 végén indult útjára kormányzati-kamarai együttműködésben a GINOP 3.2.1 Modern Vállalkozások Programja (MVP), amely kkv-kat érintő digitális szemléletformáló és motivációs tevékenységeiben kiemelt fókuszt ad az IT biztonság növelésének is a cégeknél. Így a projekt keretében:

- elkészültek, a program portálján https://vallalkozzdigitalisan.hu/ elérhetők (és még fognak létrehozásra kerülni) ilyen tartalmú szemléletformáló anyagok,
- országszerte ingyenesen igénybe vehető kamarai vállalati IKT tanácsadók információbiztonsági témában is segíteni tudnak a kkv-knak, erre külön hangsúlyt helyeznek
- megszervezésre kerültek (és fognak kerülni) IT biztonságra fókuszáló rendezvények,
- több üzleti kiberbiztonsági termék és szolgáltatás is kedvezményesen elérhető
- részletes felmérés is készült a vállalkozások kibervédelmi képességeiről.

A program 2021 tavaszáig folytatódik.

2. Az MVP-vel szorosan kapcsolatban lévő, 2017 tavasza óta elérhető, vállalati IT fejlesztéseket támogató GINOP 3.2.2-8.2.4-16 kombinált pályázaton[2] az IT biztonsággal kapcsolatos hardver, szoftver, tanácsadási, szolgáltatási kiadások elszámolható költségek a pályázó kkv-knál, 2018 májusa óta a konstrukcióban GDPR-al kapcsolatos tanácsadási, szolgáltatási tevékenységek célzottan is a projektbe illeszthetők (támogathatók).

A kormányzati digitális gazdaságfejlesztési programok folytatásában, kiterjesztésében is törekedni kell az IT biztonság további növelésére a kis- és középvállalkozói szektorban. Ezeken kívül, kapcsolódóan még szükséges lehet a vállalkozások munkavállalói számára támogatott formában elérhető oktatási, képzési programok indítására is, a hardver és szoftver elemeken kívül biztonsági üzemeltetési, biztonsági megfelelőség, audit fókusszal.

Mindezek mellett az információs és kommunikációs technológiákkal foglalkozó hazai kis- és középvállalkozói szektor forrásalapú támogatása mellett a megoldás egy célirányos támogatási – akár direkt, akár indirekt (adójóváírás) – rendszer kialakítása, amelynek a célja a fent említett, bizonyítottan fejlesztői- és tudományos irányultságú tevékenységet végző, illetve kiberbiztonsági szempontból védettnek számító intézmények anyagi megerősítése.

Intézkedések:

49.) államilag támogatott kibervédelmi szolgáltatáscsomagok kialakítása a szektor vállalkozásainak az egyébként nehezen elérhető, drága megoldások beszerzésének és implementációjának elősegítése érdekében,

50.) a vállalkozások számára támogatott formában elérhető oktatási, képzési programok, a hardver és szoftver elemeken kívül biztonsági üzemeltetési, biztonsági megfelelőség, audit témában.

[2] *https://www.palyazat.gov.hu/ginop-3.2.2-8.2.4-16-vllalati-komplex-infokommunikcis-s-mobilfejlesztsek-felhalap-online-zleti-szolgltatsok-terjesztsnek-tmogatsa-1*

3.3 Versenyképes hazai tudásbázis létrehozása

Magyarország célja, hogy a kiberbiztonsági oktatás, képzés, valamint a kutatási és fejlesztési lehetőségek olyan versenyképes hazai tudásbázis létrehozását segítsék elő, mely megfelel mind a nemzetközi gyakorlatnak, mind pedig a hazai munkaerőpiac által megfogalmazott igényeknek.
Magyarország Digitális Oktatási Stratégiája a fentiekkel azonos indíttatásból fogalmaz meg célokat és intézkedéseket a digitális kompetenciák, tudatosság és tájékozottság, illetve az információbiztonságot elősegítő oktatási és szakképzési szakterületek fejlesztésére vonatkozásában.

Intézkedések:

51.) a kiberbiztonsági munkacsoport tekintse át az aktuális problémákat és fogalmazzon meg javaslatokat az azonosított problémák kezelésére;
52.) az érintett oktatási és szakképzési végzettségek adjanak megbízható alapot a munkaerő-piaci versenyben;
53.) szükséges megteremteni egy minden érintett szereplő által hozzáférhető közös informatikai tudásbázist;
54.) legyen biztosított az egyes kompetenciaszinteken az információbiztonsági képzéshez való hozzájutás és képesítés szerzésének lehetősége a társadalom széles köre számára;
55.) kerüljenek kidolgozásra az alapvető szolgáltatók személyi állományát érintően az információbiztonságra vonatkozó képzettségi követelmények és a képzési programok;
56.) kapjanak támogatást azok az egységes minőségi követelmények mellett megtartott helyi és országos kiberbiztonsági gyakorlatok és versenyek, melyek a közép- és felsőoktatásban tanuló fiatalok bevonását és tudásnövelését célozzák meg.

A jelenleg hatályos jogszabályok alapján a végrehajtásba bevont szereplők jegyzéke és a rájuk vonatkozó stratégiai feladatok

ágazat	tevékenység	illetékes szerv	vonatkozó jogszabály	feladat	kapcsolat, feladatmegosztás
állami szervek	**hatóság**	**NBSZ NEIH**	**2013. évi L. törvény, 187/2015. (VII. 13.) Korm. r.**	a) az egyedüli kapcsolattartó ponti feladatokat ellátja: a Nemzeti Elektronikus Információbiztonsági Hatóság [NIS 8. cikk (3) és (4) bekezdés, 10. cikk (3) bekezdés, 187/2015. Korm. rendelet 6. §-ának (1) bekezdés i)] b) együttműködik a CSIRT-ek hálózatával [187/2015. Korm. rendelet 6. §-ának (1) bekezdés g)] c) a hálózati és információs rendszerek biztonságáért felelős nemzetközi szervezetekben képviseli Magyarországot [187/2015. Korm. rendelet 6. §-ának (1) bekezdés h)], d) a hatáskörébe tartozó NIS-irányelvnek megfelelően azonosított alapvető szolgáltatásokat nyújtó vagy bejelentés-köteles szolgáltatást nyújtóként azonosított szolgáltatók elektronikus információs rendszerei esetében a megfelelés vizsgálatával összefüggő adatokat, valamint a vizsgálat eredményét megküldi az Európai Bizottság részére, e) együttműködik a GovCERT-el f) megküldi a Bizottság részére a NIS-irányelv szerinti nemzeti stratégiát g) tájékoztatja az érintett EGT tagállamokat a biztonsági eseményről (jelentős zavart okozó esetén) h) konzultációt folytat és együttműködik a rendvédelmi szervekkel és a NAIH-hal [187/2015. Korm. rendelet 6. §-ának (1) bekezdése az alábbi j)-n) pontjai]	**Kapcsolat:** - a magyar szervezetekkel: a BM OKF és a bejelentést fogadó hatóság jelent az NKI-nek; - a többi tagállam érintett hatóságaival, az együttműködési csoporttal és a CSIRT-ek hálózatával

	eseménykezelő központ	**NBSZ GovCERT**	**2013. évi L. törvény, 185/2015. (VII. 13.) Korm. r.**	a) a központi eseménykezelő CSIRT feladatokat ellátja: a Kormányzati Eseménykezelő Központ (GOVCERT) [NIS 9. cikk (1) bekezdés, 24. cikk (3) bekezdés] b) együttműködik a CSIRT-ek hálózatával 185/2015. [Korm. rendelet 3.§ (1) bekezdés h)] c) együttműködik a NEIH-hel [185/2015. Korm. rendelet 3.§ (1) bekezdése az alábbi j)] d) segítséget kérhet az EU Hálózati és Információbiztonsági Ügynökségtől a CSIRT-ek továbbfejlesztéséhez 185/2015. [Korm. rendelet 3.§-a kiegészül az alábbi (3)] e) a hatáskörébe tartozó elektronikus információs rendszerek tekintetében részt vesz a CSIRT-ek hálózatának tevékenységében, amelynek keretében ellátja a többi eseménykezelő központ képviseletét [185/2015. Korm. rendelet 5.§ (4) bekezdése e) pont] f) az alapvető és bejelentés köteles szolgáltatást nyújtók hálózati és információs rendszereire jelentős hatást gyakorló eseményekről tájékoztatja a többi érintett tagállamot g) az érintett eseménykezelő központ tájékoztatása alapján vizsgálja az alapvető, valamint a bejelentés-köteles szolgáltatást nyújtók szolgáltatásaira jelentés hatást gyakorló biztonsági események határon átnyúló hatását [185/2015. Korm. rendelet az alábbi 5/A.§]	**Kapcsolat:** - a magyar szervezetekkel: A BM OKF és a bejelentést fogadó hatóság jelent az NKI-nek; - a többi tagállam érintett hatóságaival, az együttműködési csoporttal és a CSIRT-ek hálózatával

ágazat	tevékenység	illetékes szerv	vonatkozó jogszabály	feladat	kapcsolat, feladatmegosztás
Létfontosságú infrastruktúrák (NIS irányelv II. melléklet)	**hatóság**	**BM OKF**	**2013. évi L. törvény, 2012. évi CLXVI. törvény, 187/2015. (VII. 13.) Korm. r.**	a) Az alapvető szolgáltatásokat nyújtó szereplők jegyzékének vezetése [Lrtv. 2/A. § (4) és (5) bekezdés, NIS 5. cikk (1) bekezdés] b) Az alapvető szolgáltatásokat nyújtó szereplők jegyzékének kétéves felülvizsgálata [Lrtv. 2/A. § (6) bekezdés, NIS 5. cikk és (5) bekezdés] c) Kijelölt létfontosságú rendszerekkel kapcsolatos nyilvántartó hatósági feladatok ellátása (Lrtv. 5. §) d) Ellenőrzések koordinálásával összefüggő feladatrendszer (Lrtv. 8. §) e) Információbiztonsági hatósági tevékenység ellátása a létfontosságúként, valamint a jövőben az alapvető szolgáltatást nyújtó szereplőként kijelölt szolgáltatók hálózati és információs rendszerei vonatkozásában [187/2015. (VII. 13.) Korm. rendelet 25. §, NIS 8. cikk (1) bekezdés] f) együttműködni az NEIH-val rendszerei vonatkozásában [187/2015. (VII. 13.) Korm. rendelet 25. § (5) bekezdés]	**Kapcsolat:** - az ágazati kijelölő hatóságokkal. A NIS irányelv II. melléklet, azaz az alapvető szolgáltatásokat nyújtó szereplőkkel kapcsolatosan nyilvántartó hatóság; - a NIS irányelv II. melléklet 1-6. ágazatokban meghatározott alapvető szolgáltatásokat nyújtó szereplőkkel. Ellátja az állami és önkormányzati, polgári hírszerzési tevékenységet végző, honvédelmi és zárt célú rendszerek, szervek kivételével az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemek elektronikus információs rendszerei esetében a hatósági feladatokat és a biztonsági felügyeletet; - a Nemzeti Elektronikus Információbiztonsági Hatósággal. Tájékoztatást ad és együttműködik a NIS irányelvben előírt tájékoztatási kötelezettségek teljesítése érdekében.

	eseménykezelő központ	**BM OKF LRLIBEK**	**2013. évi L. törvény, 2012. évi CLXVI. törvény, 185/2015. (VII. 13.) Korm. r.**	a) Eseménykezelő központ működtetése a létfontosságúként, valamint a jövőben az alapvető szolgáltatást nyújtó szereplőként kijelölt szolgáltatók hálózati és információs rendszerei vonatkozásában [185/2015. (VII. 13.) Korm. rendelet 6. § (3)-(4), 7. §, NIS 9. cikk (1) bekezdés] b) tájékoztatási kötelezettséget teljesíteni a Kormány által kijelölt szerv, azaz a Központ részére [185/2015. (VII. 13.) Korm. rendelet 5/A. §. (1) bekezdés, NIS 10. cikk (3) bekezdés] c) felelős a biztonsági eseményekre történő reagálásért, ennek érdekében információt kérhet a hatáskörébe tartozó szervektől, d) dinamikus kockázat- és eseményelemzéseket, valamint a biztonsági eseményekkel kapcsolatos helyzetképet készít, e) felelős a kockázatokkal és biztonsági eseményekkel kapcsolatos tájékoztatásért, korai előrejelzéséért, koordinációért, f) a hatáskörébe tartozó elektronikus információs rendszerek tekintetében – a Központ útján – részt vesz az EU számítógép-biztonsági eseményekre reagáló csoportjának tevékenységében g) megosztja a Központtal a CSIRT szolgáltatási, operatív és együttműködési képességeivel kapcsolatos információit h) tájékoztatja az egyedüli kapcsolattartó pontot a biztonsági események kezelésére vonatkozó, jogszabályban nem részletezett eljárásrendjéről i) tájékoztatja a Központot az alapvető, valamint a bejelentés-köteles szolgáltatást nyújtók szolgáltatásaira jelentős hatást gyakorló biztonsági	**Kapcsolat:** - az ágazati kijelölő hatóságokkal. - a NIS irányelv II. melléklet 1-6. ágazatokban meghatározott alapvető szolgáltatásokat nyújtó szereplőkkel. Eseménykezelő központot működtet, az állami és önkormányzati elektronikus információs rendszerek, a zárt célú elektronikus információs rendszerek, a honvédelmi célú, valamint a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat által üzemeltetett létfontosságú rendszerek és létesítmények kivételével - ellátja a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenységet; - a Központtal. Tájékoztatja a biztonsági eseményekről, és együttműködik a biztonsági események kezelése során, valamint tájékoztatást ad és együttműködik a NIS irányelvben előírt biztonsági eseményekkel kapcsolatos feladatok teljesítése érdekében. - együttműködik a hatósággal, továbbá szükség szerint a biztonsági esemény kezelése tekintetében érintett szervezetekkel. A kapcsolattartás célja együttműködni a NIS irányelvben előírt

				eseményekről, a határon átnyúló hatások jelentőségének vizsgálata érdekében [185/2015. (VII. 13.) Korm. rendelet 6. § (3)-(3a), 7. §, NIS 9. cikk (1) bekezdés]	kötelezettségek teljesítése érdekében.

ágazat	tevékenység	illetékes szerv	vonatkozó jogszabály	feladat	kapcsolat, feladatmegosztás
NIS irányelv III. melléklet (digitális szolg.)	**hatóság**	**BM OKF**		a) a bejelentés-köteles szolgáltatást nyújtók hálózati és információs rendszerei információbiztonsági hatósági tevékenységének ellátása [Ekertv. 6/A-6/d. §, NIS 16. cikk (1) bekezdés NIS 8. cikk (1) bekezdés] b) nyilvántartás vezetése, c) kapcsolattartás a jogszabályban meghatározott szervezetekkel, d) egyedüli kapcsolattartó pont megbízása az eseményről küldött bejelentés más érintett tagállamok részére történő továbbítására, e) monitorozni a NIS irányelv alkalmazását, f) tájékoztatni az egyedüli kapcsolattartó pontot a bejelentett biztonsági eseményekről, g) nyilvánosság tájékoztatása biztonsági eseményekről, h) bejelentés-köteles szolgáltatást nyújtó kötelezése a nyilvánossá tájékoztatására, i) tudatosító és felvilágosító kampányokban való részvétel, j) hatósági ellenőrzés végzése, k) hatósági eljárás indítása biztonsági esemény kivizsgálására [410/2017. (XII. 15.) Korm. rendelet 4. §]	**Kapcsolat:** - a bejelentés-köteles szolgáltatást nyújtókkal, - a bűnüldöző hatóságokkal, - az egyedüli kapcsolattartó ponttal, - más tagállamok illetékes ágazati hatóságaival, - az adatvédelmi hatóságokkal, - az Európai Unióban nem letelepedett, az Európai Unión belül szolgáltatásait kínáló bejelentés-köteles szolgáltatást nyújtók által kinevezett képviselőkkel;
	eseménykezelő központ	**BM OKF**		a) a bejelentés-köteles szolgáltatást nyújtók hálózati és információs rendszereit érintő biztonsági események kezelésével összefüggő tevékenység ellátása [Ekertv. 615/CA-6/d. § (2) bekezdés, NIS 16. cikk (1) bekezdés NIS	**Kapcsolat:** - a bejelentés-köteles szolgáltatást nyújtókkal - a kormányzati információtechnológiai, hálózatbiztonsági és biztonsági

				8. cikk (1) bekezdés] b) a biztonsági eseményekről személyes adatokat nem tartalmazó nyilvántartás vezetése, c) az érintettek számára a biztonsági események kezelése során szakmai támogatás nyújtása, d) riasztási, tájékoztatási és tudatosítási feladatokat lát el, e) felelős a sérülékenységekről és fenyegetésekről, valamint a javasolt biztonsági intézkedésekről rendszeres tájékoztatás nyújtásáért, g) nem kötelező érvényű állásfoglalásokat, ajánlásokat adhat ki, h) a biztonsági események kezelésére irányuló tájékoztatót tarthat, részt vehet az információbiztonság tudatosításáért felelős intézmények tudatosítási programjában, i) együttműködik a kormányzati információtechnológiai, hálózatbiztonsági és biztonsági eseménykezelési rendszer résztvevőivel, j) ellátja a 185/2015. (VII. 13.) Korm. rendelet 6. § (3a)-(3e) bekezdésében foglalt feladatokat, k) végzi a bejelentés-köteles szolgáltatást nyújtók biztonsági eseményeinek kivizsgálásával összefüggő feladatokat [410/2017. (XII. 15.) Korm. rendelet 2. §]	eseménykezelési rendszer résztvevőivel, - a Központtal A kapcsolattartás célja a biztonsági események hatékony kivizsgálása és kezelése, a NIS irányelvben előírt biztonsági eseményekkel kapcsolatos feladatok teljesítése.
honvédelmi ágazat	**hatóság**	**KNBSZ Főigazgató**	**2013. évi L. törvény, 187/2015. (VII. 13.)**	a hatáskörébe tartozó információs rendszerei információbiztonsági hatósági tevékenységének ellátása	**Kapcsolat:** - a hatáskörébe tartozó szervekkel

			Korm. r.		
	eseménykezelő központ	**KNBSZ**	**2013. évi L. törvény, 185/2015. (VII. 13.) Korm. r.**	a hatáskörébe tartozó információs rendszerei eseménykezelő központi feladatok ellátása	**Kapcsolat:** - a hatáskörébe tartozó szervekkel
Polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat	**hatóság**	**IH Főigazgató**	**2013. évi L. törvény, 187/2015. (VII. 13.) Korm. r.**	a hatáskörébe tartozó információs rendszerei információbiztonsági hatósági tevékenységének ellátása	**Kapcsolat:**
	eseménykezelő központ	**IntCERT**	**2013. évi L. törvény, 185/2015. (VII. 13.) Korm. r.**	a hatáskörébe tartozó információs rendszerei eseménykezelő központi feladatok ellátása	**Kapcsolat:**