EURÓPAI
BIZOTTSÁG

Brüsszel, 2013.2.7.
COM(2013) 48 final

2013/0027 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE

a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről

{SWD(2013) 31 final}
{SWD(2013) 32 final}

INDOKOLÁS

A javasolt irányelv célja az egységesen magas szintű hálózat- és információbiztonság megteremtése. Ez azt jelenti, hogy meg kell erősíteni a társadalmaink és gazdaságaink működésének alapját képező internet, magánhálózatok és információs rendszerek biztonságát. Ezt úgy lehet elérni, ha előírjuk a tagállamok számára, hogy fokozzák a készültséget és az egymással való együttműködést, továbbá a kritikus infrastruktúrák, például az energiaügyi és közlekedési infrastruktúrák üzemeltetői, a kulcsofontosságú információs társadalmi szolgáltatások (e-kereskedelmi platformok, szociális hálózatok stb.) nyújtói, valamint a közigazgatások számára, hogy fogadjanak el megfelelő intézkedéseket a biztonsági kockázatok kezelésére és a súlyos biztonsági eseményeknek a nemzeti illetékes hatóságoknál történő bejelentésére.

E javaslat a Bizottságnak és az Unió külügyi és biztonságpolitikai főképviselőjének az európai kiberbiztonsági stratégiáról szóló közös közleményével összefüggésben kerül előterjesztésre. A stratégia célja biztonságos és megbízható digitális környezet biztosítása az alapvető jogok védelme és az EU más alapvető értékeinek előmozdítása és védelme mellett. Ez a javaslat a stratégia legfontosabb cselekvése. A stratégia keretében e területen tett más intézkedések a tudatosság növelésére, a kiberbiztonsági termékek és szolgáltatások belső piacának megteremtésére, valamint a K+F beruházások ösztönzésére irányulnak. Ezeket az intézkedéseket ki fogják egészíteni más, a számítástechnikai bűnözéssel szembeni határozottabb fellépést és az EU nemzetközi kiberbiztonsági politikájának kialakítását célzó intézkedések.

1.1. A javaslat okai és céljai

A hálózat- és információbiztonság egyre fontosabb a gazdaság és a társadalom számára. Ezenkívül a hálózat- és információbiztonság a szolgáltatások világszintű kereskedelméhez szükséges megbízható környezet megteremtésének is előfeltétele. Mindazonáltal az információs rendszerek olyan biztonsági eseményeknek vannak kitéve, mint az emberi mulasztás, a természeti jelenségek, a műszaki meghibásodások és a rosszindulatú támadások. Ezek az események egyre jelentősebb méreteket öltenek, egyre gyakrabban történnek, és egyre összetettebbek. A Bizottság által az európai hálózat- és információbiztonság javításának témájában szervezett nyilvános online konzultáció[1] keretében kiderült, hogy a válaszadók 57 %-a találkozott az előző év során a tevékenységét komolyan érintő hálózat- és információbiztonsági eseménnyel. A hálózat- és információbiztonság területén jelentkező hiányosságok a hálózati és információs rendszerek integritásától függően veszélyeztethetik a létfontosságú szolgáltatásokat, ami ellehetetlenítheti a vállalkozások működését, jelentős pénzügyi veszteségeket okozhat az uniós gazdaságnak és negatív hatást gyakorolhat a társadalmi jólétre.

Ezen túlmenően a digitális információs rendszerek, ezeken belül pedig különösen az internet – határokon átnyúló kommunikációs eszközök lévén – összekötik a tagállamokat, és alapvetően fontos szerepet játszanak az áruk, a szolgáltatások és a személyek határokon átnyúló szabad mozgásának elősegítésében. Ily módon az egyik tagállam rendszereinek jelentős zavara a többi tagállamban és az EU egészében is zavart okozhat. A hálózati és információs rendszerek ellenálló képessége és stabilitása alapvető fontosságú az egységes digitális piac megvalósítása és a belső piac zavartalan működése szempontjából. A nagy valószínűséggel és gyakran bekövetkező biztonsági események és az azok elleni hatékony védelem biztosításának hiánya

[1] Az európai hálózat- és információbiztonság javításáról szóló online nyilvános konzultáció 2012. július 23-ától október 15-ig tartott.

aláássa a hálózati és információs szolgáltatásokba vetett bizalmat. A kiberbiztonságról készült 2012-es Eurobarométer felmérés például megállapította, hogy az EU-ban az internethasználók 38 %-át foglalkoztatja az online fizetések biztonságának kérdése, és biztonsági aggályaik miatt változtattak szokásaikon: 18 %-uk kevésbé szívesen vásárol online, 15 %-uk pedig kisebb valószínűséggel él online banki szolgáltatásokkal[2].

Az Unióban eddig tisztán önkéntes megközelítést alkalmaztunk, azonban a jelenlegi helyzetből kitűnik, hogy ez a szemlélet nem nyújt EU-szerte megfelelő védelmet a hálózat- és információbiztonsági események és kockázatok ellen. A hálózat- és információbiztonsági képességek és mechanizmusok egyszerűen nem bírnak lépést tartani a gyorsan változó fenyegetésekkel, és nem biztosítják valamennyi tagállamban a közös kritériumokon alapuló magas szintű védelmet.

Az eddigiekben megvalósított kezdeményezések ellenére a tagállamok nagyon különböző képességekkel és felkészültséggel rendelkeznek, így az EU-ban túl sokféle megközelítés érvényesül. Tekintettel arra, hogy a hálózatok és rendszerek egymáshoz kapcsolódnak, azok a tagállamok, amelyekben nem kielégítő szintű a védelem, összességében gyengítik az Európai Unió hálózat- és információbiztonsági szintjét. Ez a helyzet gátolja a hasonló piaci szereplők közötti bizalom megteremtését is, amely az együttműködés és az információmegosztás előfeltétele. Ennek következtében együttműködésről csak a magas szintű képességekkel rendelkező tagállamok viszonylatában beszélhetünk, melyek száma csekély.

Jelenleg nem létezik olyan, hatékony uniós szintű mechanizmus, amely lehetővé tenné a hálózat- és információbiztonsági eseményekre és kockázatokra irányuló hatékony együttműködést és az információk bizalmon alapuló cseréjét a tagállamok között. Ez koordinálatlan szabályozói fellépéshez, összehangolatlan stratégiákhoz és eltérő szabványok kialakulásához, végső soron pedig az európai uniós hálózat- és információbiztonság elégtelenségéhez vezethet. Jelentkezhetnek belső piaci akadályok is, ami az egynél több tagállamban tevékenységet űző vállalkozásoknál megfelelési költségként csapódik le.

Végezetül a társadalom működéséhez nélkülözhetetlen kritikus infrastruktúrákat kezelő és az ilyen szolgáltatásokat nyújtó szereplőkre nem vonatkoznak kockázatkezelési intézkedések elfogadására és az illetékes hatóságokkal való információcserére vonatkozó megfelelő kötelezettségek. Így egyrészt a vállalkozások nem kapnak hatékony ösztönzést a kockázatértékelésre és a hálózat- és információbiztonságot előmozdító megfelelő intézkedésekre is kiterjedő komoly kockázatkezelési tevékenységek elvégzésére, másrészt pedig a biztonsági események híre többnyire nem jut el az illetékes hatóságokhoz, következésképp nem kapnak nyilvánosságot. Ahhoz, hogy az állami hatóságok a biztonsági eseményekre reagálva megfelelő enyhítő intézkedéseket hozhassanak és a hálózat- és információbiztonságra vonatkozóan megfelelő stratégiai prioritásokat határozhassanak meg, rendkívül fontos lenne, hogy a szóban forgó hatóságok értesüljenek ezekről az eseményekről.

A jelenlegi szabályozási keret csak a távközlési vállalatok esetében írja elő a kockázatkezelési intézkedések elfogadását és a súlyos hálózat- és információbiztonsági események jelentését. Ugyanakkor az IKT számos más ágazat számára is alapvető eszköz, ezért indokolt lenne ezeket is bevonni a hálózat- és információbiztonság kezelésébe. Számos konkrét infrastruktúraüzemeltető és szolgáltatásnyújtó a hálózati és információs rendszerek megfelelő működésétől való nagyfokú függése miatt különösen kiszolgáltatott helyzetben van. Ezek az ágazatok a gazdaság és a társadalom számára rendkívül fontos támogató szolgáltatásokat nyújtanak, ezért rendszereik biztonsága különös jelentőséggel bír a belső piac működése szempontjából. Ezen ágazatok közé tartozik a bankszektor, a tőzsdei szolgáltatások, az

[2] 390/2012. sz. Eurobarométer felmérés.

energiatermelés, -szállítás és -elosztás, a közlekedés (légi, vasúti, tengeri), az egészségügy, az internetes szolgáltatások és a közigazgatás.

Az EU-ban tehát radikális változásra van szükség a hálózat- és információbiztonság kezelése területén. Az egyenlő versenyfeltételek biztosítása és a joghézagok kiküszöbölése érdekében jogszabályi kötelezettségek meghatározására van szükség. A problémák megoldása, valamint a hálózat- és információbiztonság Európai Unión belüli növelése érdekében a javasolt irányelv célkitűzései a következők.

Először is a javaslat előírja az összes tagállam számára, hogy a hálózat- és információbiztonság területén illetékes hatóságok létrehozásával, hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT-ek) felállításával és nemzeti hálózat- és információbiztonsági stratégiák és együttműködési tervek elfogadásával nemzeti szinten biztosítsák a képességek minimális szintjét.

Másodszor az illetékes nemzeti hatóságoknak hálózatot kell alkotniuk, amelyben együttműködnek a biztonságos és hatékony koordináció – többek az összehangolt információcsere, valamint az uniós szinten történő felderítés és reagálás – biztosítása érdekében. A tagállamok e hálózaton keresztül – az európai hálózat- és információbiztonsági együttműködési terv alapján – bonyolítják a hálózat- és információbiztonsági fenyegetések és események elleni küzdelemhez szükséges információcserét és együttműködést.

Harmadszor az elektronikus hírközlési keretirányelv mintáját követve a javaslat célja annak biztosítása, hogy kialakuljon egy kockázatkezelési kultúra, és gyakorlattá váljon a magán- és a közszféra közötti információmegosztás. A fentiekben vázolt konkrét kritikus ágazatokban működő vállalatoknak és a közigazgatásoknak ezentúl fel kell mérniük az őket fenyegető kockázatokat, majd megfelelő és arányos intézkedéseket kell alkalmazniuk a hálózat- és információbiztonság garantálása érdekében. Az említett szereplők kötelesek lesznek jelentést tenni az illetékes hatóságoknak a hálózataikat és információs rendszereiket komolyan veszélyeztető, valamint a kritikus szolgáltatások folyamatosságát és az áruellátást jelentősen befolyásolni képes biztonsági eseményekről.

1.2. Háttér-információk

A Bizottság már 2001-ben, „Hálózat- és információbiztonság: javaslat egy európai politikai megközelítésre” című közleményében[3] felhívta a figyelmet a hálózat- és információbiztonság egyre növekvő jelentőségére. Ezt követte 2006-ban a biztonságos információs társadalomra irányuló stratégia[4] elfogadása, amelynek célja az európai hálózat- és információbiztonsági kultúra kialakítása volt. A stratégia főbb elemeit a Tanács állásfoglalásában[5] támogatta.

A Bizottság ezenkívül 2009. március 30-án közleményt fogadott el a kritikus informatikai infrastruktúrák védelméről (CIIP)[6], melynek középpontjában Európa hálózati zavarokkal szembeni védelmének a biztonság javításával történő biztosítása állt. A közlemény cselekvési tervet indított útjára a megelőzés és a reagálás területén tett tagállami erőfeszítések támogatása érdekében. A cselekvési terv a kritikus informatikai infrastruktúrák védelmével foglalkozó, 2009-es tallinni miniszteri konferencia elnökségi következtetéseiben is támogatásra talált. A Tanács 2009. december 18-án állásfoglalást fogadott el „a hálózat- és információbiztonság együttműködésre építő európai megközelítéséről”[7].

---

3 COM(2001) 298.
4 COM(2006) 251, http://eur-lex.europa.eu/LexUriServ/site/hu/com/2006/com2006_0251hu01.pdf.
5 2007/068/01.
6 COM(2009) 149.
7 2009/C 321/01).

A 2010 májusában elfogadott európai digitális menetrend[8] és az ehhez kapcsolódó tanácsi következtetések[9] hangsúlyozták a felek egyetértését a tekintetben, hogy a bizalom és a biztonság az IKT széleskörű elterjedésének és ezáltal az Európa 2020 stratégia „intelligens növekedés" dimenziójával kapcsolatos célkitűzések elérésének alapvető előfeltételei[10]. A bizalomról és a biztonságról szóló szakaszában az európai digitális menetrend hangsúlyozta, hogy valamennyi érdekelt félnek össze kell fognia, és a megelőzésre, a felkészültségre és a tudatosításra, valamint a hatékony és összehangolt biztonsági mechanizmusok kidolgozására összpontosító, átfogó erőfeszítés keretében biztosítania kell az IKT-infrastruktúra biztonságát és ellenálló képességét. Különösen az európai digitális menetrend 6. kulcsintézkedése olyan intézkedések meghozatalára szólít fel, amelyek erős és magas szintű hálózat- és információbiztonsági politika kialakítását célozzák.

2011. márciusban elfogadott CIIP-közleményében („Eredmények és következő lépések: a globális kiberbiztonság felé")[11] a Bizottság számba vette a kritikus informatikai infrastruktúrák védelmére vonatkozó cselekvési terv 2009-es elfogadása óta elért eredményeket, és következtetései szerint a terv megvalósítása során megmutatkozott: a biztonsággal és az ellenálló képességgel kapcsolatos kihívásokat nem elég pusztán nemzeti szinten megközelíteni, és Európának folytatnia kell erőfeszítéseit a következetes és együttműködésen alapuló uniós megközelítés kialakítása érdekében. A 2011-es CIIP-közleményben több cselekvés is bejelentésre került, és a Bizottság felhívta a tagállamokat, hogy hozzanak létre hálózat- és információbiztonsági képességeket, és fejlesszék a határokon átnyúló együttműködést. Ezen intézkedések többségét 2012-ig bezárólag kellett volna végrehajtani, erre azonban még nem került sor.

Az Európai Unió Tanácsa a kritikus informatikai infrastruktúrák védelméről szóló, 2011. május 27-i következtetéseiben hangsúlyozta, hogy az IKT-rendszereket és -hálózatokat mihamarabb ellenállóképessé és biztonságossá kell tenni minden lehetséges zavarral szemben, legyen az véletlen vagy szándékos; EU-szerte magas szintű készültségi, biztonsági és ellenállási képességeket kell kialakítani, naprakésszé kell tenni a műszaki szakértelmet, ezzel lehetővé téve Európa számára, hogy megfelelhessen a hálózati és információs infrastruktúrák védelme jelentette kihívásoknak; továbbá az eseményekre vonatkozó együttműködési mechanizmusok kialakításával ösztönözni kell a tagállamok közötti együttműködést.

1.3. Az ezen a területen meglévő uniós és nemzetközi rendelkezések

Az Európai Közösség 2004-ben a 460/2004/EK rendelettel létrehozta az Európai Hálózat- és Információbiztonsági Ügynökséget (ENISA)[12] abból a célból, hogy hozzájáruljon a magas szintű hálózat- és információbiztonság biztosításához és a hálózat- és információbiztonság kultúrájának kialakításoz az EU-ban. 2010. szeptember 30-án elfogadásra került az ENISA megbízatásának korszerűsítésére vonatkozó javaslat[13], amely jelenleg tárgyalás alatt áll a Tanácsnál és az Európai Parlamentnél. Az elektronikus hírközlésre vonatkozó, 2009. november óta hatályban lévő felülvizsgált keretszabályozás[14] biztonsági kötelezettségeket ír elő az elektronikus hírközlési szolgáltatók számára[15]. Ezeket a kötelezettségeket a tagállamoknak 2011 májusáig kellett átültetniük nemzeti jogukba.

---

8 COM(2010) 245.

9 A Tanács 2010. május 31-i következtetései az európai digitális menetrendről (10130/10).

10 COM(2010) 2020 és az Európai Tanács 2010. március 25–26-i következtetései (EUCO 7/10).

11 COM(2011) 163.

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:HU:HTML.

13 COM(2010) 521.

14 Lásd: http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 A keretirányelv 13a. és 13b. cikke.

A személyes adatok védelmére vonatkozó szabályozási keret[16] valamennyi olyan szereplőt, amely adatokat kezel (például bankok és kórházak), a személyes adatok védelmét szolgáló biztonsági intézkedések meghozatalára kötelezi. Emellett az általános adatvédelmi rendeletre irányuló 2012. évi bizottsági javaslat[17] értelmében az adatkezelőnek a személyes adatok megsértése esetén jelentést kell tennie a nemzeti felügyeleti hatóságoknak. Ez azt jelenti, hogy például az olyan hálózat- és információbiztonsági eseményt, amely hátrányosan befolyásolja a szolgáltatásnyújtást, de nem jelent veszélyt a személyes adatokra (pl. az áramszolgáltatónál bekövetkező, áramszünetet okozó IKT-zavar), nem kell bejelenteni.

Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelv értelmében „a létfontosságú infrastruktúrák védelmére vonatkozó európai programról” (EPCIP)[18] szóló közlemény meghatározza a létfontosságú infrastruktúrák védelmét szolgáló átfogó uniós megközelítést. Az EPCIP célkitűzései teljes mértékben összhangban állnak e javaslattal, és a javasolt irányelvet a 2008/114/EK irányelv sérelme nélkül kell alkalmazni. Az EPCIP nem kötelezi a szereplőket a jelentős biztonsági események bejelentésére, és nem vezet be az eseményekre való reagálásra és a tagállamok ilyen esetben való együttműködését szolgáló mechanizmusokat.

A társjogalkotók jelenleg vitatják az információs rendszerek elleni támadásokról szóló bizottsági irányelvjavaslatot[19], melynek célja az egyes magatartásformák vonatkozásában kiszabható büntetőjogi szankciók összehangolása. A javaslat csupán egyes magatartásformák büntethetőségével foglalkozik, a hálózat- és információbiztonsági kockázatok és események megelőzésével, az ilyen eseményekre való reagálással és azok hatásainak mérséklésével nem. Az itt előterjesztett irányelvet az információs rendszerek elleni támadásokról szóló irányelv sérelme nélkül kell alkalmazni.

2012. március 28-án a Bizottság közleményt fogadott el a Számítástechnikai Bűnözés Elleni Európai Központ létrehozásáról[20]. A 2013. január 11-én felállított központ az Európai Rendőrségi Hivatal (Europol) részét képezi, és kapcsolattartási pontként működik a számítástechnikai bűnözés elleni uniós szintű küzdelemben. Célja a számítástechnikai bűnözés terén elérhető európai szakértelem összefogása annak érdekében, hogy támogassa a tagállamokat a kapacitásépítésben és a számítástechnikai bűnözéssel kapcsolatos vizsgálatok elvégzésében, valamint a Eurojusttal szorosan együttműködve a számítástechnikai bűncselekményekkel foglalkozó európai nyomozók szócsöve legyen a bűnüldözés és az igazságszolgáltatás egész területén.

Az európai intézmények, ügynökségek és szervek létrehozták saját, hálózatbiztonsági vészhelyzeteket elhárító csoportját, a CERT-EU-t.

Nemzetközi szinten az EU mind kétoldalú, mind többoldalú alapon foglalkozik a kiberbiztonság kérdéseivel. A 2010. évi EU–USA csúcstalálkozón[21] felállították a kiberbiztonsággal és a számítástechnikai bűnözéssel foglalkozó közös EU–USA munkacsoportot. Az EU más kapcsolódó többoldalú fórumokon is szerepet vállal, így például a Gazdasági Együttműködési és Fejlesztési Szervezetben (OECD), az Egyesült Nemzetek Szervezetének Közgyűlésében, a Nemzetközi Távközlési Egyesületben (ITU), az Európai

16 A 2002. július 12-i 2002/58/EK irányelv.
17 COM(2012) 11.
18 COM(2006) 786, http://eur-lex.europa.eu/LexUriServ/site/hu/com/2006/com2006_0786hu01.pdf.
19 COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:HU:PDF.
20 COM(2012) 140, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:hu:PDF.
21 http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

Biztonsági és Együttműködési Szervezetben (EBESZ), az információs társadalmi csúcstalálkozón (WSIS) és az Internetirányítási Fórumban (IGF).

2. AZ ÉRDEKELT FELEKKEL FOLYTATOTT KONZULTÁCIÓK ÉS A HATÁSVIZSGÁLATOK EREDMÉNYEI

2.1. Az érdekelt felekkel folytatott konzultáció és a szakértői vélemények felhasználása

2012. július 23-a és október 15-e között „A hálózat- és információbiztonság javítása az EU-ban” címmel online nyilvános konzultációra került sor. A Bizottság az online kérdőívre összesen 160 választ kapott.

A legfontosabb tanulság az volt, hogy az érintettek általában egyetértettek a hálózat- és információbiztonság javításának szükségességével az Európai Unió egész területén. Konkrétabban: a válaszadók 82 % azon véleményének adott hangot, hogy a tagállamok kormányainak többet kellene tenniük a magas szintű hálózat- és információbiztonság biztosítása érdekében; 82,8 % úgy gondolja, hogy az információ- és rendszerfelhasználók nincsenek tisztában a hálózat- és információbiztonsági fenyegetésekkel és eseményekkel; 66,3 % elvileg támogatná szabályozási követelmények bevezetését a hálózat- és információbiztonsági kockázatok kezelésére; valamint 84,8 % nyilatkozta azt, hogy az ilyen követelményeket uniós szinten kell rögzíteni. Nagy számú válaszadó gondolja úgy, hogy különösen a következő ágazatokban fontos lenne hálózat- és információbiztonsági követelményeket bevezetni: bank és pénzügyek (91,1 %), energia (89,4 %), közlekedés (81,7 %), egészségügy (89,4 %), internetes szolgáltatások (89,1 %) és közigazgatás (87,5 %). A válaszadók véleménye szerint továbbá, ha olyan követelmény kerülne bevezetésre, amely szerint a hálózat- és információbiztonsági eseményeket be kell jelenteni az illetékes nemzeti hatóságnak, akkor azt uniós szinten kellene előírni (65,1 %), valamint megerősítették, hogy a követelményt ki kell terjeszteni a nemzeti közigazgatásokra is (93,5 %). Végül a válaszadók megerősítették, hogy sem a technika mindenkori állapotának megfelelő színvonalú hálózat- és információbiztonsági kockázatkezelés megvalósítása (63,4 %), sem a biztonsági események bejelentése nem járna számukra számottevő többletköltséggel (72,3 %).

A tagállamok véleményét számos érintett tanácsi formáció keretében kikérték, egyrészt a tagállamok európai fórumának (EFMS) keretében a Bizottság és az Európai Külügyi Szolgálat által 2012. július 6-án megrendezésre kerülő kiberbiztonsági konferencián, másrészt az egyes tagállamok kérésére e célból összehívott kétoldalú találkozókon.

Az európai köz-magán reziliencia-partnerség[22], valamint kétoldalú találkozók keretében a magánszektorral folytatott megbeszélésekre is sor került. Ami a közszférát illeti, az EU-intézmények részéről a Bizottság folytatott megbeszéléseket az ENISA-val és a CERT-tel.

2.2. Hatásvizsgálat

A Bizottság a hatásvizsgálat keretében három megoldási lehetőséget vett fontolóra:

1. lehetőség: Változatlan ügymenet (alapforgatókönyv): a jelenlegi megközelítés fenntartása:

2. lehetőség: Szabályozási megközelítés: javaslat olyan jogszabályra, amely közös uniós jogi keretben meghatározza a tagállamok hálózat- és információbiztonsági képességeit, az uniós szintű együttműködés mechanizmusait, valamint az érintett főbb magánszférabeli szereplőkre és a közigazgatásokra vonatkozó előírásokat.

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

3. lehetőség: Kombinált megközelítés, amely a tagállamok hálózat- és információbiztonsági képességeire irányuló önkéntes kezdeményezések, az uniós szintű együttműködési mechanizmusok, valamint az érintett főbb magánszférabeli szereplőkre és a közigazgatásokra vonatkozó előírások ötvözését jelenti.

A Bizottság arra a következtetésre jutott, hogy a 2. lehetőség járna a leginkább pozitív hatással, mivel jelentős mértékben javítaná az uniós fogyasztók, a vállalkozások és a kormányok hálózat- és információbiztonsági eseményekkel szembeni védelmét. Konkrét előnyökre lebontva: a tagállamokra rótt kötelezettségek megfelelő szintű nemzeti felkészültséget biztosítanak, és erősítik a kölcsönös bizalom légkörét, ami előfeltétele a hatékony uniós szintű együttműködésnek. A hálózatban megvalósuló, uniós szintű együttműködés mechanizmusainak felállítása egységes és összehangolt megelőzést és reagálást tesz lehetővé a határokon átnyúló hálózat- és információbiztonsági események és kockázatok felmerülése esetén. A hálózat- és információbiztonsági kockázatkezelésnek a közigazgatási szerveknél és az érintett főbb magánszférabeli szereplőknél történő bevezetésére vonatkozó követelmények erős ösztönzőt jelentenek a biztonsági kockázatok hatékony kezelésére. A jelentős következményekkel járó hálózat- és információbiztonsági események bejelentésére vonatkozó kötelezettség javítja a reagálási képességet és növelné az átláthatóságot. Továbbá azáltal, hogy saját területén rendet teremt, az EU képes lesz nemzetközi befolyását kiterjeszteni, valamint bilaterális és multilaterális szintű együttműködési partnerként hitelét erősíteni. Ezáltal az EU jobb pozíciókra tehet szert az alapvető jogoknak és az Unió alapvető értékeinek külföldön való érvényre juttatásához.

A mennyiségi értékelés kimutatta, hogy a 2. lehetőség nem ró indokolatlanul nagy terhet a tagállamokra. A magánszektorra háruló költségek szintén korlátozottak, mivel az érintett szereplők közül soknak már most is meg kell felelnie a meglévő biztonsági követelményeknek (nevezetesen az adatkezelőkre vonatkozó azon kötelezettségnek, mely szerint műszaki és szervezeti intézkedéseket kell tenniük a személyes adatok védelmének biztosítása érdekében, ideértve a hálózat- és információbiztonságra vonatkozó intézkedéseket is). A biztonsághoz kapcsolódó jelenlegi magánszektorbeli kiadásokat szintén figyelembe vettük.

E javaslat megfelel az Európai Unió Alapjogi Chartájában foglalt elveknek, tiszteletben tartja nevezetesen a magánélet és a magáncélú kommunikáció tiszteletben tartásához való jogot. a személyes adatok védelméhez való jogot, a vállalkozás szabadságát, a tulajdonhoz való jogot, a hatékony jogorvoslathoz való jogot és a Bíróság előtti meghallgatáshoz való jogot. Ezen irányelvet az említett elvekkel és jogokkal összhangban kell végrehajtani.

3. A JAVASLAT JOGI ELEMEI

3.1. Jogalap

Az Európai Unió a Szerződések vonatkozó rendelkezéseivel (az Európai Unió működéséről szóló szerződés [EUMSZ] 26. cikkével) összhangban hatáskörrel rendelkezik, hogy intézkedéseket fogadjon el a belső piac létrehozása, illetve működésének biztosítása érdekében. A 114. cikk értelmében az EU elfogadhatja „azokat a tagállamok törvényi, rendeleti és közigazgatási rendelkezéseinek közelítésére vonatkozó intézkedéseket, amelyek tárgya a belső piac megteremtése és működése”.

Amint a fentiekben jeleztük, a hálózati és információs rendszerek alapvető szerepet játszanak az áruk, a szolgáltatások és a személyek határokon átnyúló mozgásának lehetővé tételében. Ezek a hálózatok gyakran egymáshoz kapcsolódnak, az internet pedig globális természetű. Az internet ezen alapvető, nemzeti határokat nem ismerő jellege miatt az egyik tagállamban bekövetkező zavar hatással lehet más tagállamokra vagy akár az Unió egészére is. Ezért a

hálózati és információs rendszerek ellenálló képessége és stabilitása alapvető fontosságú a belső piac zavartalan működése szempontjából.

Az uniós jogalkotó már felismerte, hogy a belső piac fejlődésének biztosításához harmonizálni kell a hálózat- és információbiztonsági szabályokat. Ez a felismerés vezetett az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendelet[23] elfogadásához, amely az EUMSZ 114. cikkén alapul.

A nem egyforma nemzeti hálózat- és információbiztonsági képességekből, politikákból és védelmi szintekből eredő különbségek akadályozzák a belső piac működését, ezért indokolják az uniós fellépést.

3.2. Szubszidiaritás

A hálózat- és információbiztonság területén való európai uniós fellépést a szubszidiaritás elve is indokolja.

Először is, tekintettel a hálózat- és információbiztonság több országot érintő jellegére, az uniós szintű beavatkozás elmaradása esetén minden tagállam egymagában lépne fel, figyelmen kívül hagyva a hálózati és információs rendszerek egymástól való függőségét. A tagállamok közötti megfelelő szintű koordináció biztosítaná, hogy a hálózat- és információbiztonsági kockázatokat olyan összefüggésben kezeljék, ahogy azok felmerülnek, tehát határokon átnyúló jelenségként. A hálózat- és információbiztonságra vonatkozó szabályok közötti eltérések akadályt jelentenek a több országban működő vállalatok számára, valamint a globális méretgazdaságosság megvalósulása szempontjából.

Másodszor, az egyenlő versenyfeltételek biztosítása és a joghézagok kiküszöbölése érdekében uniós szintű jogszabályi kötelezettségek meghatározására van szükség. A tisztán önkéntes megközelítés azt eredményezte, hogy csak néhány, magasabb szintű képességekkel rendelkező tagállam között jött létre együttműködés. Az összes tagállam bevonása érdekében biztosítani kell, hogy mindegyikük teljesítse a képességekre vonatkozóan előírt minimális szintet. A kormányok által elfogadott hálózat- és információbiztonsági intézkedéseket egyeztetni kell és össze kell hangolni annak érdekében, hogy azok képesek legyenek megfékezni a hálózat- és információbiztonsági eseményeket, illetőleg minimalisra csökkenteni azok következményeit. A hálózaton belül az illetékes hatóságok és a Bizottság – a bevált gyakorlatok cseréje által és az ENISA folyamatos bevonása mellett – együtt fognak működni az irányelv Unió-szerte egységes végrehajtása érdekében. Továbbá a hálózat- és információbiztonságra vonatkozó, kellően összpontosított szakpolitikai fellépés ennek megfelelően komoly mértékben segíthetné az alapjogok, különösen pedig a személyes adatok és a magánélet védelméhez fűződő jog hatékony érvényesülését. Az uniós szintű fellépés tehát fokozná a nemzeti szinten ma is folytatott politikák eredményességét és elősegítené ezek fejlődését.

A javasolt intézkedések az arányosság szempontjából is indokoltak. A tagállamokra vonatkozó követelményeket a megfelelő felkészültség és bizalmon alapuló együttműködés eléréséhez szükséges minimális szinten kell megállapítani. Ez lehetővé teszi a tagállamok számára, hogy figyelembe vegyék nemzeti sajátosságaikat, és biztosítja a közös uniós elvek arányos alkalmazását. A tág alkalmazási körnek köszönhetően a tagállamok az irányelv alkalmazását az adott országban a nemzeti hálózat- és információbiztonsági stratégia keretében feltárt, ténylegesen fennálló kockázatokhoz igazíthatják. A kockázatkezelés végrehajtására vonatkozó követelmények csak a kritikus létesítményeket érintik, és az előírt intézkedések arányosak a kockázattal. A nyilvános konzultáció hangsúlyozta annak

[23] Az Európai Parlament és a Tanács 2004. március 10-i 460/2004/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról, HL L 077., 2004.3.13., 1. o.

fontosságát, hogy e kritikus létesítmények megfelelő védelemben részesüljenek. A jelentéstételi kötelezettség a jelentős következményekkel járó eseményekre korlátozódna. Mint fent már említettük, az intézkedések nem járnának aránytalanul nagy költségekkel, mivel ezek a szereplőknek adatkezelőként – a jelenlegi adatvédelmi szabályok értelmében – már most is kötelesek gondoskodni a személyes adatok védelméről.

Annak elkerülése érdekében, hogy a kis gazdasági szereplőket, különösen a kis- és középvállalkozásokat aránytalanul nagy terhek sújtsák, a követelményeknek az érintett hálózati vagy információs rendszer által megállapított kockázattal arányosnak kell lenniük, és azokat nem szabad a mikrovállalkozásokra alkalmazni. A kockázatokat azok a szereplők állapítják meg, amelyekre az említett követelmények vonatkoznak, ezt követően pedig dönteniük kell a kockázatok enyhítésére alkalmas intézkedések meghozataláról.

A hálózat- és információbiztonsági események és kockázatok határokon átnyúló természetéből fakadóan a kitűzött célokat uniós szinten jobban meg lehet valósítani. Az Unió ezért az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritás elvének megfelelően intézkedéseket hozhat. Az arányosság elvének megfelelően e rendelet nem lépi túl a célkitűzések eléréséhez szükséges mértéket.

A célkitűzések megvalósítása érdekében a Bizottságot fel kell hatalmazni, hogy az Európai Unió működéséről szóló szerződés 290. cikke szerinti, felhatalmazáson alapuló jogi aktusokat fogadjon el az alapul szolgáló jogi aktus nem lényegi elemeinek kiegészítése vagy módosítása céljából. A bizottsági javaslat a magán- és közszférabeli szereplőket érintő követelmények végrehajtásában is egy arányossági folyamat támogatására törekszik.

Az alap-jogiaktus végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságot fel kell hatalmazni arra, hogy végrehajtási jogi aktusokat fogadjon el az Európai Unió működéséről szóló szerződés 291. cikke értelmében.

Figyelembe véve különösen a javasolt irányelv széles alkalmazási körét, azt a tényt, hogy erősen szabályozott terület szabályozására irányul, valamint a IV. fejezetéből adódó jogi kötelezettségeket, az átültető intézkedésekről szóló értesítéshez magyarázó dokumentumot kell mellékelni. A tagállamoknak és a Bizottságnak a magyarázó dokumentumokról szóló, 2011. szeptember 28-i együttes politikai nyilatkozatával összhangban a tagállamok vállalták, hogy az átültető intézkedéseikről szóló értesítéshez indokolt esetben mellékelnek egy vagy több olyan dokumentumot, amely megmagyarázza az irányelv elemei és az azt átültető nemzeti jogi eszköz megfelelő részei közötti kapcsolatot. Ezen irányelv tekintetében a jogalkotó úgy ítéli meg, hogy ilyen dokumentumok átadása indokolt.

4. KÖLTSÉGVETÉSI VONZATOK

A tagállamok közötti együttműködést és információcserét biztonságos infrastruktúra létrehozásával kell támogatni. A javaslatnak csak abban az esetben van hatása az Unió költségvetésére, ha a tagállamok úgy döntenek, hogy már létező infrastruktúrát (pl. sTESTA) alakítanak át erre a célra, és a 2014–2020 közötti időszakra vonatkozó többéves pénzügyi keretein belül a Bizottságot bízzák meg a feladat végrehajtásával. Az intézkedések becsült egyszeri költsége 1 250 000 EUR, amelyet az EU költségvetésének 09.03.02 tételéből kellene fedezni (a nemzeti közszolgáltatások online összekapcsolódásának és interoperabilitásának, valamint az e hálózatokhoz való hozzáférésnek az előmozdítása – 09.03 alcím, Európai Hálózatfinanszírozási Eszköz – távközlési hálózatok), amennyiben az rendelkezik a megfelelő forrásokkal. Alternatív megoldásként a tagállamok megoszthatják a már létező infrastruktúra átalakításának egyszeri költségeit, vagy dönthetnek úgy, hogy új infrastruktúrát hoznak létre és viselik a becslések szerint mintegy évi 10 millió EUR-ra rúgó költségeket.

2013/0027 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE

a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 114. cikkére,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezetének a nemzeti parlamentek számára való megküldését követően,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére[24],

az európai adatvédelmi biztossal való konzultációt követően,

rendes jogalkotási eljárás keretében,

mivel:

(1) A hálózati és információs rendszerek és szolgáltatások nélkülözhetetlen szerepet játszanak társadalmunkban. Megbízhatóságuk és biztonságuk elengedhetetlen a gazdasági tevékenységek és a szociális jólét, és a különösen a belső piac működése szempontjából.

(2) A szándékos vagy véletlen biztonsági események nagyságrendje és gyakorisága növekszik, és ezek az események jelentős veszélyt jelentenek a hálózatok és az információs rendszerek működésére. Az ilyen események akadályozhatják a gazdasági tevékenységek folytatását, jelentős pénzügyi veszteségeket okozhatnak, aláássák a felhasználói bizalmat, és jelentős károkat okozhatnak az Unió gazdaságának.

(3) Határokon átnyúló kommunikációs eszközök lévén a digitális információs rendszerek és elsősorban az internet alapvető szerepet játszanak az áruk, a szolgáltatások és a személyek határokon átnyúló szabad mozgásának elősegítésében. Transznacionális jellegük miatt az egyik tagállam rendszereinek jelentős zavara a többi tagállamban és az EU egészében is zavart okozhat. Ezért a hálózati és információs rendszerek ellenálló képessége és stabilitása alapvető fontosságú a belső piac zavartalan működése szempontjából.

(4) Indokolt uniós szintű együttműködési mechanizmust létrehozni, amely lehetővé teszi az információcserét és a hálózat- és információbiztonsággal kapcsolatos észlelést és reagálást. E mechanizmus eredményességének és inkluzív jellegének biztosítása érdekében alapvető fontosságú, hogy minden tagállam rendelkezzék minimális képességekkel és a saját területükön a hálózat- és információbiztonság magas szintjét biztosító stratégiával. A kockázatkezelés kultúrájának elősegítése és a legsúlyosabb események bejelentése érdekében minimális biztonsági előírásokat indokolt alkalmazni a közigazgatási szervek és a kritikus informatikai infrastruktúrákat üzemeltető gazdasági szereplők esetében.

[24] HL C […]., […], […]. o.

(5) Annak érdekében, hogy a szabályozás valamennyi lényeges eseményre és kockázatra kiterjedjen, ezt az irányelvet valamennyi hálózati és információs rendszerre indokolt alkalmazni. A közigazgatásokra és a piaci szereplőkre vonatkozó kötelezettségeket azonban nem indokolt alkalmazni az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról szóló, 2002. március 7-i európai parlamenti és tanácsi irányelv (Keretirányelv)[25] szerinti nyilvános hírközlési hálózatokat üzemeltető és nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó vállalkozásokra – ezekre az említett irányelv 13a. cikkében meghatározott biztonsági és integritási követelmények vonatkoznak –, sem pedig a bizalmi szolgáltatások nyújtóira.

(6) A meglévő képességek nem elegendőek ahhoz, hogy a magas szintű hálózat- és információbiztonságot garantáljanak az Unió területén. A tagállamok nagyon különböző felkészültséggel rendelkeznek, ami sokféle megközelítés alkalmazásához vezet az Unióban. Így nem biztosított a fogyasztók és a vállalkozások egységes védelme, ami aláássa a hálózat- és információbiztonság általános színvonalát az Unión belül. A közigazgatási szervekre és a piaci szereplőkre vonatkozó közös minimumkövetelmények hiánya miatt nem lehetséges uniós szinten átfogó és hatékony együttműködési mechanizmust létrehozni.

(7) A hálózati és információs rendszerek biztonsági kihívásainak hatékony kezelése ezért globális megközelítést kíván, amely kiterjed a kapacitásépítésre és a tervezésre vonatkozó közös minimumkövetelményekre, az információcserére és a tevékenységek összehangolására, valamint az összes érintett piaci szereplőre és a közigazgatásra vonatkozó közös biztonsági minimumkövetelményekre.

(8) Az irányelv rendelkezései nem érinthetik a tagállamok azon jogát, hogy megtegyék az alapvető biztonsági érdekeik védelméhez, a közrend és a közbiztonság védelméhez, valamint a bűncselekmények kivizsgálásához, felderítéséhez és büntetőeljárások lefolytatásához szükséges intézkedéseket. Az EUMSZ 346. cikke értelmében egyetlen tagállam sem köteles olyan információt szolgáltatni, amelynek közlését ellentétesnek tartja alapvető biztonsági érdekeivel.

(9) A hálózati és információs rendszerek közös magas biztonsági szintjének elérése és fenntartása érdekében minden tagállamban létre kell hozni egy nemzeti hálózat- és információbiztonsági stratégiát, amely meghatározza a stratégiai célokat és a végrehajtandó konkrét szakpolitikai intézkedéseket. Nemzeti szinten a hálózat- és információbiztonságra vonatkozó, az alapvető követelményeknek megfelelő együttműködési tervet szükséges kidolgozni annak érdekében, hogy a biztonsági események bekövetkeztekor nemzeti és uniós szinten megfelelő reagálási kapacitás álljon rendelkezésre az eredményes és hatékony együttműködéshez.

(10) Az ezen irányelv értelmében elfogadott rendelkezések eredményes végrehajtása érdekében valamennyi tagállamban indokolt létrehozni egy olyan szervet, amelynek feladata a hálózat- és információbiztonsággal kapcsolatos kérdések koordinálása, és amely kapcsolattartóként működik a határokon átnyúló, uniós szintű együttműködés számára. Ezen szervek számára célszerű biztosítani a megfelelő műszaki, pénzügyi és emberi erőforrásokat annak érdekében, hogy feladataikat eredményesen és hatékonyan láthassák el, ezzel segítve az irányelv céljainak elérését.

(11) Fontos, hogy valamennyi tagállam rendelkezzék a hálózati és információs rendszereket érintő események és kockázatok megelőzéséhez, észleléséhez,

[25] HL L 108., 2002.4.24., 33. o.

kezeléséhez és mérsékléséhez szükséges műszaki és szervezeti képességekkel. Ezért minden tagállamban létre kell hozni jól működő és az alapvető követelményeknek megfelelő, számítógépes vészhelyzeteket elhárító csoportokat, amelyek biztosítják a biztonsági események és kockázatok esetén mozgósítható hatékony és együttműködni képes kapacitásokat és az eredményes, uniós szintű együttműködést.

(12) A tagállamok európai fórumán (EFMS) belül a bevált szakpolitikai gyakorlatokról szóló viták és eszmecserék, valamint az európai számítógépes válságkezelési együttműködés elveinek kidolgozása terén elért jelentős haladásra építve a tagállamoknak és a Bizottságnak hálózatot kell alkotniuk egymással, így biztosítva a folyamatos párbeszédet és az együttműködés fenntartását. Ez a biztonságos és hatékony együttműködési mechanizmus várhatóan lehetővé teszi az uniós szintű strukturált és összehangolt információcserét, észlelést és reagálást.

(13) Az Európai Hálózat- és Információbiztonsági Ügynökségnek (ENISA) szakértő véleményével és tanácsaival, valamint a bevált gyakorlatok cseréjének elősegítésével indokolt segítenie a tagállamokat és a Bizottságot. A Bizottságnak különösen ezen irányelv alkalmazása kapcsán célszerű kikérnie az ENISA véleményét. A tagállamok és a Bizottság hatékony és kellő időben történő tájékoztatása érdekében az együttműködési hálózatban korai előrejelzést kell adni az eseményekről és a kockázatokról. A kapacitásépítés és az ismeretek gyarapítása érdekében az együttműködési hálózatnak eszközként kell szolgálnia a bevált gyakorlatok cseréje, a hálózatban részt vevő tagállamokban zajló kapacitásépítés segítése, valamint a szakértői értékelések és a hálózat- és információbiztonsági gyakorlatok szervezése számára is.

(14) Az érzékeny és bizalmas információknak az együttműködési hálózaton belüli biztonságos cseréje céljából biztonságos infrastruktúrát indokolt létrehozni A tagállamok azon kötelezettségének sérelme nélkül, mely szerint az együttműködési hálózaton keresztül be kell jelenteniük az uniós hatású eseményeket és kockázatokat, más tagállam számára csak akkor szükséges hozzáférést biztosítani bizalmas információkhoz, ha az igazoltan rendelkezik a hálózatban való eredményes, hatékony és biztonságos részvételhez szükséges műszaki, pénzügyi és emberi erőforrásokkal és eljárásokkal, valamint kommunikációs infrastruktúrákkal.

(15) Mivel a hálózati és információs rendszerek üzemeltetése a legtöbb esetben magánkézben van, a magán- és az állami szektor közötti együttműködés rendkívül fontos. A piaci szereplőket ösztönözni kell, hogy továbbra is tartsák fenn a hálózat- és információbiztonságra irányuló saját informális együttműködési mechanizmusaikat. Emellett fontos, hogy együttműködjenek az állami szektorral, és az események bekövetkeztekor kapott operatív támogatás fejében osszák meg információikat és legjobb gyakorlataikat.

(16) Az átláthatóság, valamint az uniós polgárok és a piaci szereplők megfelelő tájékoztatására érdekében az illetékes hatóságoknak indokolt olyan közös weboldalt létrehozni, amelyen elérhetők az eseményekkel és a kockázatokkal kapcsolatos nem bizalmas információk.

(17) Az üzleti titokra vonatkozó uniós és nemzeti szabályok értelmében bizalmasnak minősített információk esetében az ezen irányelvben előírt tevékenységek végrehajtása és célkitűzések megvalósítása során fontos biztosítani a szóban forgó adatok bizalmas kezelését.

(18) Különösen a nemzeti válságkezelési tapasztalatokra alapozva – az ENISA-val együttműködésben – a Bizottságnak és a tagállamoknak ki kell alakítaniuk egy olyan uniós hálózat- és információbiztonsági együttműködési tervet, amely meghatározza a kockázatok és az események kezelésére irányuló együttműködési mechanizmusokat. E tervet megfelelően figyelembe kell venni az együttműködési hálózatban tett korai előrejelzések alkalmával.

(19) A hálózaton belüli korai előrejelzési értesítés csak akkor előírás, ha az esemény vagy kockázat mértéke és súlyossága uniós szintű tájékoztatást vagy reagálást tesz vagy tehet szükségessé. Ennélfogva a korai előrejelzést célszerű az olyan esetekre korlátozni, amelyekben a tényleges vagy potenciális események vagy kockázatok jelentősége gyorsan nő, meghaladják a nemzeti reagálási kapacitást, vagy egynél több tagállamot érintenek. A megfelelő értékelhetőség érdekében indokolt a kockázat vagy az esemény értékelése szempontjából lényeges valamennyi információt a hálózat résztvevőinek tudomására hozni.

(20) A korai előrejelzés kézhezvételét és értékelését követően az illetékes hatóságoknak meg kell állapodniuk az összehangolt válaszintézkedés módjában, az uniós hálózat- és információbiztonsági együttműködési tervben foglaltaknak megfelelően. Az illetékes hatóságokat és a Bizottságot tájékoztatni kell az összehangolt válaszintézkedés céljából nemzeti szinten elfogadott intézkedésekről.

(21) A hálózat- és információbiztonság területén felmerülő problémák globális jellegére való tekintettel szorosabb nemzetközi együttműködésre van szükség a biztonsági előírások és az információcsere továbbfejlesztése, valamint a hálózat- és információbiztonságot érintő közös globális megközelítésmód előmozdítása érdekében.

(22) A hálózat- és információbiztonság biztosítása nagymértékben a közigazgatások és a piaci szereplők felelőssége. A kockázatértékelést és a felmerülő kockázatok súlyosságának megfelelő biztonsági intézkedések végrehajtását is magában foglaló kockázatkezelési kultúrát megfelelő követelmények szabályozás útján történő meghatározásával és önkéntes ágazati gyakorlatokon keresztül célszerű ösztönözni. Az együttműködési hálózat eredményes működése és ezen keresztül a tagállamok hatékony együttműködése szempontjából továbbá igen fontos az egyenlő versenyfeltételek megteremtése.

(23) A 2002/21/EK irányelv előírja, hogy a nyilvános elektronikus hírközlési hálózatokat üzemeltető és a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó vállalkozások hozzanak megfelelő intézkedéseket integritásuk és biztonságának védelme érdekében, a biztonság sérülésének és az integritás megszűnésének esetére pedig bejelentési kötelezettséget ír elő. Az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv („Elektronikus hírközlési adatvédelmi irányelv”)[26] előírja a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtói számára, hogy szolgáltatásaik biztonságának biztosítása érdekében tegyenek megfelelő műszaki és szervezeti intézkedéseket.

(24) E kötelezettségeket a műszaki szabványok és szabályok terén történő információszolgáltatási eljárás és az információs társadalom szolgáltatásaira vonatkozó szabályok megállapításáról szóló, 1998. június 22-i 98/34/EK európai

[26] HL L 201., 2002.7.31., 37. o.

parlamenti és tanácsi irányelv[27] alapján indokolt kiterjeszteni az elektronikus hírközlési ágazaton túlra, az olyan alapvető információs társadalmi szolgáltatások nyújtóira, amelyek olyan felhasználói szintű információs társadalmi szolgáltatások és online tevékenységek alapját képezik, mint például az e-kereskedelmi platformok, az internetes fizetési átjárók, a közösségi hálózatok, a keresőprogramok, a számításifelhő-szolgáltatások és az alkalmazásboltok. Ezen információs társadalmi támogató szolgáltatások zavara fennakadást okoz az alapvetően rájuk épülő többi információs társadalmi szolgáltatás nyújtásában. A szoftver- és hardvergyártók nem nyújtanak információs társadalmi szolgáltatást, ezért nem tartoznak ezen irányelv hatálya alá. Az említett kötelezettségeket indokolt kiterjeszteni a közigazgatásokra és a kritikus infrastruktúrákat üzemeltető gazdasági szereplőkre is, amelyek nagymértékben függnek az információs és kommunikációs technológiáktól, és elengedhetetlenül fontos szerepet játszanak az olyan létfontosságú gazdasági és társadalmi feladatok ellátásában, mint a villamosenergia- és gázszolgáltatás, a közlekedés, a hitelintézetek üzemeltetése, a tőzsdei szolgáltatások és az egészségügy. E hálózati és információs rendszerek zavara befolyásolná a belső piac működését.

(25) A közigazgatási szervekre és a piaci szereplőkre vonatkozó műszaki és szervezeti intézkedések nem követelhetik meg, hogy egy adott kereskedelmi információ vagy kommunikációs technológia tervezése, kialakítása vagy előállítása egy meghatározott módon történjék.

(26) A közigazgatások és a piaci szereplők számára indokolt előírni, hogy biztosítsák az ellenőrzésük alatt álló hálózatok és rendszerek biztonságát. Ezek elsősorban olyan, magánkézben lévő hálózatok és rendszerek, amelyek kezelését saját informatikus munkatársak végzik, illetve amelyek biztonsági karbantartását kiszervezték. A biztonsági és jelentéstételi kötelezettségeket a releváns piaci szereplőkre és a közigazgatásokra indokolt alkalmazni függetlenül attól, hogy azok saját maguk végzik hálózati és információs rendszereik karbantartását vagy kiszervezésben végeztetik el.

(27) Annak elkerülése érdekében, hogy a kisebb szolgáltatókat és felhasználókat aránytalanul nagy pénzügyi és közigazgatási terhek sújtsák, a követelményeknek arányosaknak kell lenniük az érintett hálózati vagy információs rendszer által megállapított kockázattal, figyelembe véve az ilyen intézkedések technikai értelemben vett naprakészségét. E követelmények a mikrovállalkozásokra nem alkalmazhatók.

(28) A illetékes hatóságoknak célszerű kellő figyelmet fordítaniuk a piaci szereplők közötti, valamint a köz- és a magánszektor közötti nem hivatalos és bizalmi információmegosztási csatornák megőrzésére. Az illetékes hatóságoknál bejelentett események nyilvánosságra hozatala tekintetében alaposan mérlegelni kell a nyilvánosság fenyegetésekről való tájékoztatásából származó előnyt, illetve az érintett közigazgatási szervek és a bejelentést tevő piaci szereplők lehetséges tekintélyvesztését és az általuk elszenvedett kereskedelmi kárt. A bejelentési kötelezettségek végrehajtása során az illetékes hatóságoknak célszerű különös figyelmet fordítaniuk arra, hogy a megfelelő biztonsági korrekciós intézkedések nyilvánosságra hozataláig a termékek gyenge pontjai szigorúan titokban maradjanak.

(29) Az illetékes hatóságoknak rendelkezniük kell a feladataik teljesítéséhez szükséges eszközökkel, beleértve azt a hatáskört is, hogy a hálózati és információs rendszerek biztonsági szintjének értékeléséhez szükséges megfelelő mennyiségű információt a piaci szereplőktől és a közigazgatásoktól megszerezzék, valamint hogy hozzájussanak

[27] HL L 204., 1998.7.21., 37. o.

a hálózati és információs rendszerek működését befolyásoló tényleges eseményekkel kapcsolatos valamennyi megbízható adathoz.

(30) Az események hátterében sok esetben bűncselekmények állnak. Az események bűncselekmény jellege akkor is feltételezhető, ha erre vonatkozóan nem áll rendelkezésére kezdettől fogva egyértelmű bizonyíték. Ebben az összefüggésben fontos, hogy a biztonsági fenyegetésekre való hatékony és átfogó reagálás részét képezze az illetékes hatóságok és a bűnüldöző hatóságok közötti megfelelő együttműködésnek. A biztonságos, védett és ellenállóbb környezet előmozdítására való törekvés jegyében különösen kívánatos a vélhetően súlyos bűncselekménynek minősülő események bűnüldöző hatóságoknál való módszeres bejelentése. Azt, hogy egy esemény súlyos bűncselekménynek minősül-e, a számítástechnikai bűnözésről szóló uniós jogszabályok alapján kell értékelni.

(31) A biztonsági események kapcsán sok esetben személyes adatok kerülnek veszélybe. Ebben az összefüggésben az illetékes hatóságoknak és az adatvédelmi hatóságoknak együtt kell működniük és információt kell cserélniük a személyes adatok ilyen eseményekből eredő megsértése elleni intézkedések valamennyi releváns vonatkozása kapcsán. A tagállamok a biztonsági események bejelentésére vonatkozó kötelezettséget oly módon hajtják végre, hogy minimálisra csökkentik az adminisztratív terheket, amennyiben a biztonsági esemény a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló európai parlamenti és tanácsi rendelet[28] alapján a személyes adatok megsértésével jár. Az ENISA az illetékes hatóságokkal és az adatvédelmi hatóságokkal való kapcsolattartás révén segítséget nyújthat az információcsere-mechanizmusok és a bejelentési formanyomtatványok kialakításában, kiküszöbölve ezzel a kétféle nyomtatvány használatának szükségességét. Az egységes bejelentési formanyomtatvány használata gördülékenyebbé tenné a személyes adatok biztonságát veszélyeztető események bejelentését, ami által a vállalkozások és a közigazgatások adminisztratív terhei is csökkennének.

(32) A biztonsági követelmények szabványosítása piacvezérelt folyamat. Az uniós szinten magas fokú biztonság elérése érdekében a tagállamoknak ösztönözniük kell a biztonsági szabványok egymáshoz közelítő alkalmazását és a meghatározott szabványoknak való megfelelést. E célból harmonizált szabványok kidolgozására lehet szükség, amit az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről szóló, 2012. október 25-i 1025/2012/EU európai parlamenti és tanácsi rendeletnek[29] megfelelően kell végezni.

(33) A Bizottságnak indokolt ezen irányelv rendelkezéseit időszakonként felülvizsgálni, különösen annak megvizsgálása céljából, hogy a változó technológiai és piaci feltételek fényében szükség van-e az irányelv módosítására.

(34) Az együttműködési hálózat megfelelő működésének lehetővé tétele érdekében a Bizottságot fel kell hatalmazni arra, hogy az Európai Unió működéséről szóló szerződés 290. cikkével összhangban jogi aktusokat fogadjon el a következők meghatározása céljából: a tagállamok által teljesítendő kritériumok a biztonságos információmegosztási rendszerben való részvételhez; a korai előrejelzést kiváltó

[28] SEC(2012) 72 végleges

[29] HL L 316., 2012.11.14., 12. o.

események pontosítása; valamint azon körülmények, amelyek fennállása esetén a piaci szereplők és a hatóságok kötelesek egy adott eseményt bejelenteni.

(35) Különösen fontos, hogy a Bizottság előkészítő munkája során – többek között szakértői szinten – megfelelő konzultációkat folytasson. A felhatalmazáson alapuló jogi aktusok előkészítése és kidolgozása során a Bizottságnak gondoskodnia kell arról, hogy a releváns dokumentumok az Európai Parlamenthez és a Tanácshoz egyidejűleg, megfelelő időben és módon eljussanak.

(36) Az ezen irányelv végrehajtására vonatkozó feltételek egységességének biztosítása érdekében a következők tekintetében célszerű a Bizottságot végrehajtási jogkörrel felruházni: az illetékes hatóságok és a Bizottság között az együttműködési hálózat keretében folyó együttműködés; az információmegosztási infrastruktúrához való hozzáférés; az uniós hálózat- és információbiztonsági együttműködési terv, a nyilvánosság biztonsági eseményekről való tájékoztatására szolgáló formátumok és eljárások; valamint a hálózat- és információbiztonság szempontjából releváns szabványok és/vagy műszaki előírások. Ezeket a hatásköröket a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról szóló, 2011. február 16-i 182/2011/EU európai parlamenti és tanácsi rendeletnek[30] megfelelően kell gyakorolni.

(37) Ezen irányelv alkalmazása során a Bizottság megfelelő kapcsolatot tart fenn az érintett ágazati bizottságokkal és a különösen az energia, a közlekedés és az egészségügy területén uniós szinten létrehozott érintett szervekkel.

(38) Az illetékes hatóság által az üzleti titokra vonatkozó uniós és nemzeti szabályok értelmében bizalmasnak minősített információkat csak abban az esetben kell a Bizottság és a többi illetékes hatóság tudomására hozni, ha az adatszolgáltatás ezen irányelv alkalmazása szempontjából feltétlenül szükséges. A rendelkezésre bocsátott adatokat az ilyen adatszolgáltatás célja szempontjából lényeges és azzal arányos adatokra kell korlátozni.

(39) A kockázatokkal és az eseményekkel kapcsolatos információknak az együttműködési hálózaton keresztül történő megosztása, valamint az események illetékes nemzeti hatóságoknál történő bejelentésére vonatkozó követelményeknek való megfelelés személyes adatok feldolgozását teheti szükségessé. A személyes adatok ilyen feldolgozása szükséges ezen irányelv közérdekű céljainak eléréséhez, ezért a 95/46/EK irányelv 7. cikke alapján indokolt. A szóban forgó indokolt célkitűzésekre való tekintettel az ilyen adatfeldolgozás nem jelent aránytalan és megengedhetetlen beavatkozást, amely sértené a személyes adatok védelmére vonatkozó, az Alapjogi Charta 8. cikke által biztosított jog lényegét. Ezen irányelv alkalmazásakor az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről szóló, 2001. május 30-i 1049/2001/EK európai parlamenti és tanácsi rendeletet[31] kell értelemszerűen alkalmazni. Az adatok uniós intézmények és szervek általi, ezen irányelv végrehajtása céljából történő feldolgozásakor meg kell felelni a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 45/2001/EK európai parlamenti és tanácsi rendeletben foglaltaknak.

(40) Mivel ezen rendelet céljait, nevezetesen a hálózat- és információbiztonság magas uniós szintjének biztosítását a tagállamok egyedül nem tudják kielégítően

[30] HL L 55., 2011.2.28., 13. o.

[31] HL L 145., 2001.5.31., 43. o.

megvalósítani, és ezért az intézkedés hatása miatt az uniós szinten jobban megvalósítható, az Unió az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritás elvének megfelelően intézkedéseket hozhat. Az említett cikkben foglalt arányossági elvvel összhangban az irányelv nem lépi túl a szóban forgó célkitűzések eléréséhez szükséges mértéket.

(41) E javaslat megfelel az Európai Unió Alapjogi Chartájában foglalt elveknek és jogoknak, tiszteletben tartja nevezetesen a magánélet és a magáncélú kommunikáció tiszteletben tartásához való jogot. a személyes adatok védelméhez való jogot, a vállalkozás szabadságát, a tulajdonhoz való jogot, a hatékony jogorvoslathoz való jogot és a Bíróság előtti meghallgatáshoz való jogot. Ezen irányelvet az említett jogokkal és elvekkel összhangban kell végrehajtani.

ELFOGADTÁK EZT AZ IRÁNYELVET:

1. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy és hatály

(1) Ez az irányelv olyan intézkedéseket állapít meg, amelyek biztosítják a hálózat- és információbiztonság közös magas szintjét az Unión belül.

(2) Ennek érdekében az irányelv:

a) valamennyi tagállamra vonatkozó kötelezettségeket ír elő a hálózati és információs rendszereket érintő kockázatok és biztonsági események megelőzése, kezelése és az azokra való reagálás vonatkozásában;

b) a tagállamok közötti együttműködést szolgáló mechanizmust hoz létre az irányelv Unió-szerte egységes alkalmazásának biztosítása, és amennyiben szükséges, a hálózati és információs rendszereket érintő kockázatok és biztonsági események összehangolt és hatékony kezelése és az azokra való reagálás biztosítása érdekében;

c) a piaci szereplőkre és a közigazgatásokra vonatkozóan biztonsági követelményeket állapít meg.

(3) A 14. cikkben előírt biztonsági követelmények nem alkalmazandók sem a 2002/21/EK irányelv szerinti nyilvános hírközlési hálózatokat üzemeltető és nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó vállalkozásokra – ezekre az említett irányelv 13a. és 13b. cikkében meghatározott biztonsági és integritási követelmények vonatkoznak –, sem pedig a bizalmi szolgáltatások nyújtóira.

(4) Ez az irányelv nem sérti sem a számítástechnikai bűnözésre vonatkozó uniós jogszabályok, sem pedig az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelv[32] rendelkezéseit.

(5) Ez az irányelv továbbá nem sérti sem a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv[33], sem az

[32] HL L 345., 2008.12.23., 75. o.

[33] HL L 281., 1995.11.23., 31. o.

elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv, sem pedig a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló európai parlamenti és tanácsi rendelet[34] rendelkezéseit.

(6) Az együttműködési hálózaton keresztül a III. fejezetnek megfelelően történő információmegosztás, valamint a hálózat- és információbiztonsági eseményeknek a 14. cikk alapján történő bejelentése személyes adatok feldolgozását teheti szükségessé. Az ezen irányelv közérdekű céljainak eléréséhez szükséges ilyen adatfeldolgozást a tagállamok a 95/46/EK irányelv 7. cikkét és a 2002/58/EK irányelvet a nemzeti jogukba átültető rendelkezések alapján engedélyezik.

2. cikk

Minimális harmonizáció

A tagállamok – az uniós jog szerinti kötelezettségeik sérelme nélkül – nem akadályozhatók meg abban, hogy magasabb biztonság szintet biztosító rendelkezéseket fogadjanak el vagy tartsanak fenn.

3. cikk

Fogalommeghatározások

Ezen irányelv alkalmazásában:

(1) „hálózati és információs rendszer”:

a) a 2002/21/EK irányelv szerinti elektronikus hírközlő hálózat; valamint

b) bármely olyan eszköz, illetve egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján automatizált számítógépes adatfeldolgozást végez; illetve

c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és fenntartásuk céljából tárolt, feldolgozott, visszakeresett vagy továbbított számítógépes adatok.

(2) „biztonság”: valamely hálózati és információs rendszer képessége – a titkosság meghatározott szintjén – a szóban forgó hálózati és információs rendszerekben tárolt vagy továbbított adatok és az általuk nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, sértetlenségét és titkosságát veszélyeztető véletlen eseményekkel, illetve rosszindulatú tevékenységgel szembeni ellenállásra;

(3) „kockázat”: a biztonságra kedvezőtlen hatást gyakorolni képes körülmény vagy esemény;

(4) „biztonsági esemény”: a biztonságra ténylegesen kedvezőtlen hatást gyakorló körülmény vagy esemény;

(5) „információs társadalmi szolgáltatás”: a 98/34/EK irányelv 1. cikkének 2. pontja szerinti szolgáltatás,;

[34] SEC(2012) 72 végleges.

(6) „hálózat- és információbiztonsági együttműködési terv”: olyan terv, amely meghatározza a hálózatok vagy információs rendszerek működésének fenntartására vagy helyreállítására vonatkozó szervezeti feladatkörök, hatáskörök és eljárások kereteit arra az esetre, ha az említett hálózatokat vagy információs rendszereket érintő kockázat vagy esemény áll fenn;

(7) „biztonsági események kezelése”: a biztonsági események elemzését, megfékezését és a rájuk való reagálást támogató eljárások;

(8) „piaci szereplő”:

a) más, a II. mellékletben nem kimerítő jelleggel felsorolt információs társadalmi szolgáltatások nyújtását lehetővé tevő információs társadalmi szolgáltatást nyújtó szolgáltató;

b) az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a tőzsdei szolgáltatások és az egészségügy szempontjából alapvető fontosságú – a II. mellékletben nem kimerítő jelleggel felsorolt – gazdasági és társadalmi tevékenységek fenntartásához nélkülözhetetlen kritikus infrastruktúra üzemeltetője.

(9) „szabvány”: az 1025/2012/EK rendelet szerinti szabvány;

(10) „előírás”: az 1025/2012/EK rendelet szerinti előírás;

(11) „bizalmi szolgáltatások nyújtója”: elektronikus aláírásoknak, elektronikus bélyegzőknek, elektronikus időbélyegzőknek, elektronikus dokumentumoknak, elektronikus kézbesítési szolgáltatásoknak, weboldal-hitelesítésnek és elektronikus tanúsítványoknak, ezen belül elektronikus aláírások és elektronikus bélyegzők tanúsítványainak létrehozására, ellenőrzésére, hitelesítésére, kezelésére és megőrzésére irányuló elektronikus szolgáltatást nyújtó természetes vagy jogi személy.

II. FEJEZET

NEMZETI HÁLÓZAT- ÉS INFORMÁCIÓBIZTONSÁGI KERETEK

4. cikk

Alapelv

A tagállamok ezen irányelvvel összhangban saját területükön biztosítják a hálózati és információs rendszerek magas szintű biztonságát.

5. cikk

A nemzeti hálózat- és információbiztonsági stratégia és a nemzeti hálózat- és információbiztonsági együttműködési terv

(1) Valamennyi tagállam nemzeti hálózat- és információbiztonsági stratégiát fogad el, amelyben meghatározza a stratégiai célokat, valamint a magas szintű hálózat- és információbiztonság eléréséhez és fenntartásához szükséges konkrét szakpolitikai és szabályozási intézkedéseket. A nemzeti hálózat- és információbiztonsági stratégia különösen a következő témákkal foglalkozik:

a) a stratégia célkitűzéseinek és prioritásainak meghatározása a kockázatok és az események naprakész elemzése alapján;

b) a stratégia célkitűzéseinek és prioritásainak elérését szolgáló irányítási keretrendszer, ideértve a kormányzati szervek és egyéb érintett szereplők szerepkörének és feladatainak egyértelmű meghatározását is;

c) a felkészültségre, a reagálásra és a helyreállításra vonatkozó általános intézkedések meghatározása, ideértve az állami szféra és a magánszféra közötti együttműködést szolgáló mechanizmusokat is;

d) oktatási, tudatosságnövelő és képzési programok létrehozása;

e) kutatási és fejlesztési tervek, valamint annak leírása, hogy ezek a tervek hogyan szolgálják a meghatározott prioritásokat.

(2) A nemzeti hálózat- és információbiztonsági stratégia tartalmazza a nemzeti hálózat- és információbiztonsági együttműködési tervet, amely megfelel legalább az alábbi követelményeknek:

a) a veszélyek azonosítására és az események potenciális hatásainak felmérésére irányuló kockázatértékelési terv;

b) a terv végrehajtásában érintett különböző szereplők szerepkörének és feladatainak meghatározása;

c) a megelőzést, az észlelést, a reagálást és a helyreállítást szolgáló együttműködési és kommunikációs folyamatok meghatározása és az aktuális riasztási szint szerinti kiigazítása;

d) a hálózat- és információbiztonsági gyakorlatokra és képzésre vonatkozó ütemterv a terv megerősítése, validálása és tesztelése céljából. A levont tanulságokat dokumentálni kell, és a frissítések alkalmával be kell építeni a tervbe.

(3) A nemzeti hálózat- és információbiztonsági stratégiát és a nemzeti hálózat- és információbiztonsági együttműködési tervet azok elfogadásától számított egy hónapon belül meg kell küldeni a Bizottságnak.

6. cikk

A hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes hatóság

(1) Minden tagállam kijelöl egy, a hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes hatóságot (a továbbiakban: „illetékes hatóság”).

(2) Az illetékes hatóságok nemzeti szinten nyomon követik ezen irányelv alkalmazását, és hozzájárulnak alkalmazásának az egész Unióban való következetességéhez.

(3) A tagállamok biztosítják, hogy az hatóságok a rájuk bízott feladatok eredményes és hatékony ellátásához és ezáltal a irányelv célkitűzéseinek teljesítéséhez elegendő műszaki, pénzügyi és emberi erőforrással rendelkezzenek. A tagállamok a 8. cikkben említett hálózat segítségével biztosítják az illetékes hatóságok eredményes, hatékony és biztonságos együttműködését.

(4) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok a 14. cikk (2) bekezdésének megfelelően bejelentést kapjanak a közigazgatásoktól és a piaci szereplőktől a biztonsági eseményekről, és rendelkezzenek a 15. cikkben említett végrehajtási és jogalkalmazói jogkörrel.

(5) Az illetékes hatóságok – szükség szerint – konzultálnak és együttműködnek az érintett nemzeti bűnüldöző hatóságokkal és a nemzeti adatvédelmi hatóságokkal.

(6) Minden tagállam késedelem nélkül tájékoztatja a Bizottságot az illetékes hatóság kijelöléséről, feladatairól és bármilyen későbbi változásról. Valamennyi tagállam nyilvánosságra hozza a kijelölt illetékes hatóság nevét.

7. cikk

A hálózatbiztonsági vészhelyzeteket elhárító csoport

(1) Valamennyi tagállam felállít egy hálózatbiztonsági vészhelyzeteket elhárító csoportot (a továbbiakban: „CERT”), melynek feladata a biztonsági eseményeknek és kockázatoknak egy jól meghatározott – az I. melléklet 1. pontjában szereplő követelményeknek megfelelő eljárás alapján történő kezelése. A CERT-et az illetékes hatóságon belül is létre lehet hozni.

(2) A tagállamok biztosítják, hogy a CERT-ek rendelkezzenek az I. melléklet 2. pontjában meghatározott feladataik hatékony ellátásához szükséges megfelelő műszaki, pénzügyi és emberi erőforrásokkal.

(3) A tagállamok gondoskodnak arról, hogy a CERT nemzeti szinten olyan, biztonságos és ellenállóképes kommunikációs és információs infrastruktúrát használjon, amely kompatibilis és interoperábilis a 9. cikkben említett biztonságos információmegosztási rendszerrel.

(4) A tagállamok tájékoztatják a Bizottságot a CERT rendelkezésére álló forrásokról és megbízatásáról, valamint a biztonsági események kezelésére szolgáló eljárásról.

(5) A CERT tevékenységét az illetékes hatóság felügyeli, aminek keretében rendszeresen felülvizsgálja a források megfelelőségét, a CERT megbízatását és a biztonsági események kezelésére szolgáló eljárás hatásosságát.

III. FEJEZET

EGYÜTTMŰKÖDÉS AZ ILLETÉKES HATÓSÁGOK KÖZÖTT

8. cikk

Együttműködési hálózat

(1) Az illetékes hatóságok és a Bizottság hálózatot („együttműködési hálózat”) hoznak létre a hálózati és információs rendszereket érintő események és kockázatok leküzdése terén folyó együttműködés céljából.

(2) Az együttműködési hálózat állandó kapcsolatot teremt a Bizottság és az illetékes hatóságok között. Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) felkérésre szakértő véleményével és tanácsaival segíti az együttműködési hálózatot.

(3) Az együttműködési hálózaton belül az illetékes hatóságok:

a) a 10. cikknek megfelelően korai előrejelzést tesznek közzé a kockázatokról és a biztonsági eseményekről;

b) a 11. cikkel összhangban gondoskodnak az összehangolt válaszintézkedésről;

c) egy közös honlapon rendszeresen közzéteszik a folyamatban lévő korai előrejelzésekre és az összehangolt válaszintézkedésre vonatkozó nem bizalmas információkat;

d) egy tagállam vagy a Bizottság kérésére közös vitára és értékelésre bocsátják az 5. cikkben említett – az irányelv hatálya alá tartozó – adott nemzeti hálózat- és

információbiztonsági stratégiát vagy stratégiákat, illetőleg nemzeti hálózat- és információbiztonsági együttműködési tervet vagy terveket;

e) egy tagállam vagy a Bizottság kérésére közös vitára és értékelésre bocsátják a CERT-ek eredményességét, különösen uniós szintű hálózat- és információbiztonsági gyakorlatok végzése kapcsán;

f) minden releváns kérdésben együttműködnek és információt cserélnek az Europol szervezetén belül működő Számítástechnikai Bűnözés Elleni Európai Központtal, illetve más érintett európai szervekkel, különösen az adatvédelem, az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a tőzsdei szolgáltatások és az egészségügy területén;

g) információt cserélnek és megosztják a bevált gyakorlatokat más illetékes hatóságokkal és a Bizottsággal, és segítik egymást a hálózat- és információbiztonsági kapacitásépítésben;

h) rendszeres jelleggel szakértői értékeléseket szerveznek a képességek és a felkészültség témájában;

i) uniós szintű hálózat- és információbiztonsági gyakorlatokat szerveznek, és adott esetben részt vesznek nemzetközi hálózat- és információbiztonsági gyakorlatokon is.

(4) A Bizottság végrehajtási aktusok útján megállapítja az illetékes hatóságok és a Bizottság közötti, a (2) és (3) bekezdésben említett együttműködés elősegítésének módozatait. Az ilyen végrehajtási jogi aktusokat a 19. cikk (2) bekezdése szerinti konzultációs eljárással összhangban kell elfogadni.

9. cikk

Biztonságos információmegosztási rendszer

(1) Az érzékeny és bizalmas adatoknak az együttműködési hálózaton belüli cseréjét biztonságos infrastruktúrán keresztül kell lebonyolítani.

(2) A Bizottság felhatalmazást kap arra, hogy a 18 cikk alapján felhatalmazáson alapuló jogi aktusokat fogadjon el a biztonságos információmegosztási rendszerben való részvételre jogosult tagállamok által az alábbiak tekintetében teljesítendő kritériumok meghatározására vonatkozóan:

a) biztonságos és ellenállóképes, az együttműködési hálózat biztonságos infrastruktúrájával kompatibilis és interoperábilis, a 7. cikk (3) bekezdésével összhangban lévő hírközlési és információs infrastruktúra rendelkezésre állása nemzeti szinten, valamint

b) illetékes hatóságuk és CERT-jük megfelelő műszaki, pénzügyi és emberi erőforrásokkal és eljárásokkal való olyan mértékű ellátottsága, amely lehetővé teszi a biztonságos információmegosztási rendszerben a 6. cikk (3) bekezdése, a 7. cikk (2) bekezdése és a 7. cikk (3) bekezdése alapján történő hatékony, eredményes és biztonságos részvételt.

(3) A Bizottság – végrehajtási aktusok útján – határozatokat fogad el a tagállamoknak az említett biztonságos infrastruktúrához való hozzáféréséről, a (2) és (3) bekezdésben említett kritériumok alapján. E végrehajtási aktusokat a 19. cikk (3) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

10. cikk

Korai előrejelzés

(1) Az illetékes hatóságok és a Bizottság az együttműködési hálózat keretében korai előrejelzést adnak azokról a kockázatokról és eseményekről, amelyek a következő feltételeknek legalább az egyikét teljesítik:

a) léptékük gyorsan nő vagy gyors növekedésnek indulhat;

b) meghaladják vagy meghaladhatják a nemzeti reagálási kapacitást;

c) több tagállamot érintenek vagy érinthetnek.

(2) A korai előrejelzés keretében az illetékes hatóságok és a Bizottság minden olyan, a birtokukban lévő releváns információt rendelkezésre bocsátanak, amely a kockázat, illetve az esemény értékeléséhez hasznos lehet.

(3) A Bizottság – egy tagállam megkeresésére vagy saját kezdeményezésére – felkérhet egy tagállamot arra, hogy egy adott kockázatról vagy eseményről minden releváns információt rendelkezésre bocsásson.

(4) Amennyiben a korai előrejelzés tárgyát képező kockázat, illetve esemény gyaníthatóan bűnügyi természetű, az illetékes hatóságok vagy a Bizottság tájékoztatja az Europol Számítástechnikai Bűnözés Elleni Európai Központját.

(5) A Bizottság felhatalmazást kap arra, hogy a 18. cikk alapján felhatalmazáson alapuló jogi aktusokat fogadjon el abból a célból, hogy pontosítsa a korai előrejelzést igénylő kockázatoknak és eseményeknek az (1) bekezdésében meghatározott körét.

11. cikk

Összehangolt válaszintézkedés

(1) A 10. cikk szerinti korai előrejelzés nyomán az illetékes hatóságok – a releváns információ értékelését követően – megállapodnak a 12. cikk szerinti uniós hálózat- és információbiztonsági együttműködési tervvel összhangban meghozandó összehangolt válaszintézkedésről.

(2) Az összehangolt válaszintézkedés eredményeképpen nemzeti szinten tett különböző intézkedésekről tájékoztatni kell az együttműködési hálózatot.

12. cikk

Uniós hálózat- és információbiztonsági együttműködési terv

(1) A Bizottság felhatalmazást kap arra, hogy – végrehajtási aktusok útján – uniós hálózat- és információbiztonsági együttműködési tervet fogadjon el. E végrehajtási aktusokat a 19. cikk (3) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

(2) Az uniós hálózat- és információbiztonsági együttműködési tervben rendelkezni kell a következőkről:

a) a 10. cikk alkalmazása céljából:

– a kockázatokra és eseményekre vonatkozó kompatibilis és összevethető információknak az illetékes hatóságok általi összegyűjtésére és megosztására irányadó formátum és eljárások meghatározása,

– a kockázatoknak és eseményeknek az együttműködési hálózat által végzett értékelésére irányadó eljárások és kritériumok meghatározása;

b) a 11. cikk szerinti összehangolt válaszintézkedések tekintetében követendő eljárások, a feladat- és hatáskörök kijelölésére és az együttműködési eljárások rögzítésére is kiterjedően;

c) a terv megerősítésére, validálására és tesztelésére szolgáló hálózat- és információbiztonsági gyakorlatok és képzések ütemezése;

d) a kapacitásépítésre és a társaktól való tanulásra vonatkozó ismereteknek a tagállamok közötti átadására szolgáló program;

e) tagállamközi tudatosságnövelő és képzési program.

(3) Az uniós hálózat- és információbiztonsági együttműködési tervet az ezen irányelv hatálybalépésétől számított egy éven belül el kell fogadni, a továbbiakban pedig rendszeresen felül kell vizsgálni.

13. cikk

Nemzetközi együttműködés

Azon lehetőség sérelme nélkül, hogy az együttműködési hálózat informális nemzetközi együttműködést folytasson, az Unió nemzetközi megállapodásokat köthet harmadik országokkal vagy nemzetközi szervezetekkel az együttműködési hálózat egyes tevékenységeibe való bevonásuk lehetővé tételéről és megszervezéséről. E megállapodásokban figyelemmel kell lenni arra, hogy az együttműködési hálózaton belül továbbított személyes adatoknak megfelelő védelmet kell biztosítani.

IV. FEJEZET

A KÖZIGAZGATÁSI SZERVEK ÉS A PIACI SZEREPLŐK HÁLÓZATAINAK ÉS INFORMÁCIÓS RENDSZEREINEK BIZTONSÁGA

14. cikk

Biztonsági követelmények és eseménybejelentés

(1) A tagállamok biztosítják, hogy a közigazgatási szervek és a piaci szereplők megfelelő műszaki és szervezési intézkedéseket tegyenek a működésük során általuk ellenőrzött és használt hálózatok és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében. Ezen intézkedéseknek – tekintettel a tudomány és a technika mindenkori állására – a felmerülő kockázatnak megfelelő biztonsági szintet kell garantálniuk. Így különösen intézkedéseket kell tenni, hogy a hálózataikat és az információs rendszereiket érintő események ne, illetve minél kevésbé legyenek hatással az e hálózatok, illetve rendszerek nyújtotta alapszolgáltatásokra, s ezáltal biztosítva legyen az e hálózatokra és információs rendszerekre támaszkodó szolgáltatások folytonossága.

(2) A tagállamok biztosítják, hogy a közigazgatási szervek és a piaci szereplők az illetékes hatóságnak bejelentsék az általuk nyújtott alapszolgáltatások biztonságára jelentős hatást gyakorló eseményeket.

(3) Az (1) és (2) bekezdés szerinti követelmények minden, az Európai Unióban szolgáltatást nyújtó piaci szereplőre alkalmazandók.

(4) Az illetékes hatóság tájékoztathatja a nyilvánosságot, vagy a közigazgatási szerveket és a piaci szereplőket a nyilvánosság tájékoztatására kötelezheti, amennyiben úgy véli, hogy az esemény nyilvánosságra hozatala közérdeket szolgál. Az illetékes nemzeti hatóság a beérkező bejelentésekről és az e bekezdésnek megfelelően tett intézkedésekről évente egyszer összefoglaló jelentést terjeszt az együttműködési hálózat elé.

(5) A Bizottság felhatalmazást kap arra, hogy a 18. cikk alapján felhatalmazáson alapuló jogi aktusokat fogadjon el azon körülmények meghatározására, amelyek fennállása esetén a közigazgatási szervek és a piaci szereplők kötelesek az eseményeket bejelenteni.

(6) Az illetékes hatóságok – az (5) bekezdés alapján adott esetben elfogadott, felhatalmazáson alapuló jogi aktusokra is figyelemmel – iránymutatásokat fogadhatnak el és szükség szerint utasításokat adhatnak ki azon körülményeket illetően, amelyek fennállása esetén a közigazgatási szervek és a piaci szereplők kötelesek az eseményeket bejelenteni.

(7) A Bizottság felhatalmazást kap arra, hogy – végrehajtási aktusok útján – meghatározza a (2) bekezdés alkalmazásában követendő formátumokat és eljárásokat. E végrehajtási aktusokat a 19. cikk (3) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

(8) Az (1) és a (2) bekezdés nem alkalmazandó a mikro-, kis- és középvállalkozások meghatározásáról szóló, 2003. május 6-i 2003/361/EK ajánlás[35] szerinti mikrovállalkozásokra.

15. cikk

Végrehajtás és jogalkalmazás

(1) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok minden szükséges hatáskörrel rendelkezzenek arra, hogy kivizsgálják a 14. cikk szerinti kötelezettségek közigazgatási szervek vagy piaci szereplők általi megszegésének eseteit, valamint azoknak a hálózatok és információs rendszerek biztonságára gyakorolt hatását.

(2) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok a piaci szereplőket és közigazgatási szerveket arra kötelezhessék, hogy:

a) rendelkezésre bocsássák a hálózataik és információs rendszereik biztonsági szintjének megállapításához szükséges adatokat, beleértve a biztonsági politikájukra vonatkozó dokumentumokat is;

b) alávessék magukat egy képesített független testület vagy nemzeti hatóság biztonsági ellenőrzésének, és annak eredményét az illetékes hatóság rendelkezésére bocsássák.

(3) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok hatáskörrel rendelkezzenek arra, hogy a piaci szereplőket és közigazgatási szerveket kötelező erővel utasítsák.

(4) Az illetékes hatóságok a gyaníthatóan súlyos büntetőjogi megítélés alá eső eseményeket bejelentik a bűnüldöző hatóságoknak.

[35] HL L 124., 2003.5.20., 36. o.

(5) Az illetékes hatóságok a személyes adatok megsértésével járó események kapcsán szorosan együttműködnek a személyesadat-védelmi hatóságokkal.

(6) A tagállamok biztosítják, hogy a közigazgatási szerveknek és piaci szereplőknek e fejezet szerinti valamennyi kötelezettsége bírósági felülvizsgálat tárgyát képezhesse.

16. cikk

Szabványosítás

(1) A 14. cikk (1) bekezdésének egységes szellemben történő végrehajtása érdekében a tagállamok a hálózat- és információbiztonsági szempontból releváns szabványok és/vagy előírások alkalmazására ösztönöznek.

(2) A Bizottság – végrehajtási aktusok útján – összeállítja az (1) bekezdésben említett szabványok jegyzékét. Ezt a jegyzéket közzé kell tenni az *Európai Unió Hivatalos Lapjában*.

V. FEJEZET

ZÁRÓ RENDELKEZÉSEK

17. cikk

Szankciók

(1) A tagállamok meghatározzák az ezen irányelv alapján elfogadott nemzeti rendelkezések megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és meghoznak minden szükséges intézkedést e szabályok végrehajtásának biztosítása érdekében. Az előírt szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük. A tagállamok e rendelkezésekről legkésőbb az irányelv átültetésére előírt határidő végéig, minden későbbi módosításukról pedig haladéktalanul értesítik a Bizottságot.

(2) A tagállamok biztosítják, hogy a személyes adatot érintő biztonsági esemény esetére előírt szankciók összhangban legyenek a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló európai parlamenti és tanácsi rendeletben[36] előírt szankciókkal.

18. cikk

A felhatalmazás gyakorlása

(1) A Bizottság az e cikkben meghatározott feltételekkel felhatalmazást kap felhatalmazáson alapuló jogi aktus elfogadására.

(2) A Bizottság felhatalmazást kap a 9. cikk (2) bekezdésében, a 10. cikk (5) bekezdésében és a 14. cikk (5) bekezdésében említett, felhatalmazáson alapuló jogi aktusok elfogadására. A Bizottság legkésőbb kilenc hónappal az ötéves időtartam vége előtt jelentést készít a felhatalmazásról. A felhatalmazás hallgatólagosan meghosszabbodik a korábbival megegyező időtartamra, amennyiben az Európai Parlament vagy a Tanács legkésőbb a folyó időszak vége előtt három hónappal nem emel kifogást a meghosszabbítás ellen.

[36] SEC(2012) 72 final

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 9. cikk (2) bekezdésében, a 10. cikk (5) bekezdésében és a 14. cikk (5) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon vagy a határozatban megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

(4) A Bizottság a felhatalmazáson alapuló jogi aktus elfogadását követően haladéktalanul és egyidejűleg értesíti arról az Európai Parlamentet és a Tanácsot.

(5) A 9. cikk (2) bekezdése, a 10. cikk (5) bekezdése és a 14. cikk (5) bekezdése alapján elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha a jogi aktusról szóló értesítéstől számított két hónapos időtartamon belül sem az Európai Parlament, sem a Tanács nem emelt kifogást, vagy akkor, ha az időtartam leteltét megelőzően az Európai Parlament és a Tanács egyaránt arról tájékoztatta a Bizottságot, hogy nem emel kifogást. Ez az időtartam két hónappal meghosszabbodik az Európai Parlament vagy a Tanács kezdeményezésére.

19. cikk

Bizottsági eljárás

(1) A Bizottság munkáját egy bizottság (a hálózat- és információbiztonsági bizottság) segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottság.

(2) E bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 4. cikkét kell alkalmazni.

(3) E bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 5. cikkét kell alkalmazni.

20. cikk

Felülvizsgálat

A Bizottság rendszeresen felülvizsgálja ezen irányelv végrehajtását, és jelentést tesz róla az Európai Parlamentnek és a Tanácsnak. Az első jelentést legkésőbb a nemzeti jogba való átültetésre a 21. cikkben előírt határidőtől számított három éven belül be kell nyújtani. A Bizottság felkérheti a tagállamokat, hogy indokolatlan késedelem nélkül bocsássanak rendelkezésre információkat erre a célra.

21. cikk

Átültetés a nemzeti jogba

(1) A tagállamok legkésőbb [másfél évvel az elfogadás után]-(jé)ig elfogadják és kihirdetik azokat a törvényi, rendeleti és közigazgatási rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek megfeleljenek. E rendelkezések szövegét haladéktalanul megküldik a Bizottságnak.

Ezeket az intézkedéseket [másfél évvel az elfogadás után]-(jé)től alkalmazzák.

Amikor a tagállamok elfogadják ezeket az intézkedéseket, azokban hivatkozni kell erre az irányelvre, vagy azokhoz hivatalos kihirdetésük alkalmával ilyen hivatkozást kell fűzni. A hivatkozás módját a tagállamok határozzák meg.

(2) A tagállamok közlik a Bizottsággal nemzeti joguk azon főbb rendelkezéseinek szövegét, amelyeket az ezen irányelv által szabályozott területen fogadnak el.

22. cikk

Hatálybalépés

Ez az irányelv az *Európai Unió Hivatalos Lapjában* való kihirdetését követő [huszadik] napon lép hatályba.

23. cikk

Címzettek

Ennek az irányelvnek a tagállamok a címzettjei.

Kelt Brüsszelben, -án/-én.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*

I. MELLÉKLET

A hálózatbiztonsági vészhelyzeteket elhárító csoport (CERT) kötelezettségei és feladatai

A CERT kötelezettségeit és feladatait a nemzeti szakpolitikának és/vagy szabályozásnak megfelelően és egyértelműen meg kell határoznia és támogatnia kell. E kötelezettségek és feladatok magukban foglalják a következő elemeket:

1. A CERT kötelezettségei

a) A CERT az egyedi hibapontok kiküszöbölése révén biztosítja hírközlési szolgáltatásai nagyfokú elérhetőségét, továbbá elérhetősége és másokkal való kapcsolattartása céljára több eszközt tart fenn. Kommunikációs csatornáit egyértelműen meg kell határozni, és azokat felhasználóinak és együttműködési partnereinek jól kell ismerniük.

b) A hozzá beérkező és az általa feldolgozott információk bizalmas jellegének, sérthetetlenségének, elérhetőségének és hitelességének biztosítása érdekében a CERT biztonsági intézkedéseket hajt végre és tart fenn.

c) A CERT irodáit és az őket támogató információs rendszereket biztonságos helyszíneken kell elhelyezni.

d) Szolgáltatási minőségbiztosítási rendszert kell létrehozni a CERT teljesítményének figyelemmel kísérésére és az állandó továbbfejlesztés biztosítására. E rendszernek egyértelműen meghatározott – a hivatalos szolgáltatási szinteket és a kulcsfontosságú teljesítménymutatókat is magukban foglaló – mérőeszközökön kell alapulnia.

e) Az üzletmenet folytonossága:

- a CERT-nek megfelelő rendszerrel kell rendelkeznie a megkeresések kezelésére és továbbítására, az átadás megkönnyítése céljából,
- a CERT-et elegendő személyzettel kell ellátni ahhoz, hogy mindig készenlétben legyen,
- a CERT-nek olyan infrastruktúrára kell támaszkodnia, amelynek folytonossága biztosítva van. Ebből a célból redundáns rendszereket és tartalék munkaterületet kell fenntartani annak érdekében, hogy a CERT a kommunikációs eszközökhöz szünetmentes hozzáférést tudjon biztosítani.

2. A CERT feladatai

a) A CERT feladatai magukban foglalják legalább a következőket:

- események nyomon követése nemzeti szinten,
- a kockázatokkal és eseményekkel kapcsolatos korai előrejelzés, riasztás, bejelentéstétel és információterjesztés a releváns érdekeltek irányában,
- az eseményekkel szembeni válaszintézkedések,
- dinamikus kockázat- és eseményelemzés, valamint helyzetmegfigyelés,
- az online tevékenységekkel kapcsolatos kockázatokról történő széles körű ismeretterjesztés,
- hálózat- és információbiztonsági kampányok szervezése;

b) A CERT együttműködési kapcsolatokat alakít ki a magánszférával.

c) Az együttműködés megkönnyítése érdekében a CERT közös vagy szabványosított gyakorlatok elfogadását és alkalmazását szorgalmazza az alábbiakra vonatkozóan:

– esemény- és kockázatkezelési eljárások,

– események, kockázatok és információk osztályozására szolgáló rendszerek,

– mérőeszközök rendszertana,

– a kockázatokról és eseményekről történő információcseréhez használatos formátumok, valamint a rendszerek egyezményes megnevezése.

II. MELLÉKLET

A gazdasági szereplők jegyzéke

A 3. cikk (8) bekezdése a) pontjának alkalmazásában:

1. elektronikus kereskedelmi platformok

2. internetes fizetési átjárók

3. közösségi oldalak

4. keresőprogramok

5. számításifelhő-szolgáltatások

6. alkalmazásboltok

A 3. cikk (8) bekezdése b) pontjának alkalmazásában:

1. Energia

- villamosenergia- és földgázszolgáltatók
- villamosenergia- és földgázelosztó rendszerek üzemeltetői, lakossági villamosenergia- és földgázszolgáltatók
- földgázszállítási rendszerüzemeltetők, földgáztároló-üzemeltetők és LNG-létesítményüzemeltetők
- villamosenergia-átviteli rendszerüzemeltetők
- kőolajvezetékek és kőolajtárolás
- villamosenergia- és földgázpiaci szereplők
- kőolaj- és földgáztermelő, -finomító, illetve -feldolgozó létesítmények üzemeltetői

2. Közlekedés

- légi fuvarozók (légi árufuvarozás és személyszállítás)
- tengeri szállítók (tengeri és part menti vízi személyszállítással, illetve tengeri és part menti vízi árufuvarozással foglalkozó vállalkozások)
- vasutak (pályahálózat-üzemeltetők, integrált vállalatok és vasúti közlekedési szolgáltatók)
- repülőterek
- kikötők
- forgalomirányítási üzemeltetők
- járulékos logisztikai szolgáltatások: a) raktározás és tárolás, b) rakománykezelés és c) egyéb szállítástámogató tevékenység)

3. Banki szolgáltatások: a 2006/48/EK irányelv 4. cikkének 1. pontja szerinti hitelintézetek

4. Pénzügyi piaci infrastruktúra: tőzsdék és központi partner elszámolóházak

5. Egészségügy: egészségügyi ellátó létesítmények (beleértve a kórházakat és a magánklinikákat is), valamint minden egyéb, az egészségügyi ellátásban részt vevő létesítmény

PÉNZÜGYI KIMUTATÁS

1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

1.1. A javaslat/kezdeményezés címe

1.2. A tevékenységalapú irányítás /tevékenységalapú költségvetés-tervezés keretébe tartozó érintett szakpolitikai terület(ek)

1.3. A javaslat/kezdeményezés típusa

1.4. Célkitűzések

1.5. A javaslat/kezdeményezés indoklása

1.6. Az intézkedés és a pénzügyi hatás időtartama

1.7. Tervezett igazgatási módszer(ek)

2. IRÁNYÍTÁSI INTÉZKEDÉSEK

2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

2.2. Irányítási és kontrollrendszer

2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

3.1. A kiadások a többéves pénzügyi keret mely fejezetét/fejezeteit és a költségvetés mely kiadási tételét/tételeit érintik?

3.2. A kiadásokra gyakorolt becsült hatás

3.2.1. A kiadásokra gyakorolt becsült hatás összegzése

3.2.2. Az operatív előirányzatokra gyakorolt becsült hatás

3.2.3. Az igazgatási előirányzatokra gyakorolt becsült hatás

3.2.4. A jelenlegi többéves pénzügyi kerettel való összeegyeztethetőség

3.2.5. Harmadik felek részvétele a finanszírozásban

3.3. A bevételre gyakorolt becsült pénzügyi hatás

PÉNZÜGYI KIMUTATÁS

1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

1.1. A javaslat/kezdeményezés címe

Javaslat: az Európai Parlament és a Tanács irányelve a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről.

1.2. A tevékenységalapú irányítás /tevékenységalapú költségvetés-tervezés keretébe tartozó érintett szakpolitikai terület(ek)[37]

- 09 – Kommunikációs hálózatok, tartalmak és technológiák

1.3. A javaslat/kezdeményezés típusa

☒ A javaslat/kezdeményezés **új intézkedésre** irányul

☐ A javaslat/kezdeményezés **kísérleti projektet/előkészítő intézkedést követő új intézkedésre** irányul[38]

☐ A javaslat/kezdeményezés **jelenlegi intézkedés meghosszabbítására** irányul

☐ A javaslat/kezdeményezés **új intézkedésnek megfelelően módosított intézkedésre** irányul

1.4. Célkitűzések

1.4.1. A javaslat/kezdeményezés által érintett többéves bizottsági stratégiai célkitűzések

A javasolt irányelv célja a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjének biztosítása.

1.4.2. Konkrét célkitűzés(ek) és a tevékenységalapú irányítás/tevékenységalapú költségvetés-tervezés keretébe tartozó érintett tevékenység(ek)

A javaslat olyan intézkedéseket állapít meg, amelyek biztosítják a magas szintű hálózat- és információbiztonságot az egész Unióban.

A konkrét célkitűzések a következők:

1. Minimális szintű hálózat- és információbiztonság megteremtése a tagállamokban, és ezáltal a felkészültség és a reagáló képesség általános szintjének növelése.

2. A hálózat- és információbiztonság területén folytatott együttműködés javítása uniós szinten azzal a céllal, hogy eredményesebben fel lehessen lépni a határokon átnyúló biztonsági eseményekkel és fenyegetésekkel szemben. Az érzékeny és bizalmas információk illetékes hatóságok közötti cseréjének lehetővé tétele érdekében biztonságos információmegosztási infrastruktúra kerül bevezetésre.

3. Kockázatkezelési kultúra teremtése, valamint a magán- és a közszféra közötti információmegosztás javítása.

A tevékenységalapú irányítás/tevékenységalapú költségvetés-tervezés keretébe tartozó érintett tevékenység(ek)

Az irányelv hatálya a következőkre terjed ki: számos ágazat (energiaszolgáltatás, közlekedés, hitelintézetek és tőzsdék, egészségügy, valamint a kulcsfontosságú internetes szolgáltatások alapját képező infrastruktúrák) különféle szereplői (vállalatok és szervezetek, köztük egyes kkv-k), valamint a közigazgatási szervek. Az irányelv

[37] Tevékenységalapú irányítás: ABM (Activity Based Management), tevékenységalapú költségvetés-tervezés: ABB (Activity Based Budgeting).

[38] A költségvetési rendelet 49. cikke (6) bekezdésének a) vagy b) pontja szerint.

foglalkozik továbbá a bűnüldöző és az adatvédelmi hatóságokkal fenntartandó kapcsolatokkal, valamint a hálózat- és információbiztonság nemzetközi vetületével.

- 09 – Kommunikációs hálózatok, tartalmak és technológiák
- 02 – Vállalkozáspolitika
- 32 – Energiaügy
- 06 – Mobilitás- és közlekedéspolitika
- 17 – Egészségügy és fogyasztóvédelem
- 18 – Belügyek
- 19 – Külkapcsolatok
- 33 – Igazságügy
- 12 – Belső piac

1.4.3. Várható eredmény(ek) és hatás(ok)

Tüntesse fel, milyen hatásokat gyakorolhat a javaslat/kezdeményezés a kedvezményezettekre/célcsoportokra.

Jelentős mértékben javul az uniós fogyasztók, vállalkozások és kormányok hálózat- és információbiztonsági fenyegetésekkel és kockázatokkal szembeni védelme.

További részletek a jogalkotási javaslatot kísérő hatásvizsgálatról szóló bizottsági szolgálati munkadokumentum a 8.2. szakaszában (a 2. lehetőség hatásai – szabályozási megközelítés) találhatók.

1.4.4. Eredmény- és hatásmutatók

Tüntesse fel a javaslat/kezdeményezés megvalósításának nyomon követését lehetővé tevő mutatókat.

A nyomon követésre és az értékelésre vonatkozó mutatók a hatásvizsgálat 10. szakaszában találhatók.

1.5. A javaslat/kezdeményezés indoklása

1.5.1. Rövid vagy hosszú távon kielégítendő szükséglet(ek)

Minden tagállamnak rendelkeznie kell:

nemzeti hálózat- és információbiztonsági stratégiával;

nemzeti hálózat- és információbiztonsági együttműködési tervvel;

a hálózat- és információbiztonság területén illetékes nemzeti hatósággal; továbbá

hálózatbiztonsági vészhelyzeteket elhárító csoporttal (CERT)

Uniós szinten a tagállamoknak egy hálózatán keresztül kell együttműködniük.

A közigazgatásoknak és a kulcsfontosságú magánszektorbeli szereplőknek hálózat- és az információbiztonsági kockázatkezelést kell végezniük, és bejelentést kell tenniük az illetékes hatóságoknál a jelentős következményekkel járó hálózat- és információbiztonsági eseményektől.

1.5.2. Az uniós részvételből adódó többletérték

Tekintettel a hálózat- és információbiztonság határokon átnyúló jellegére, a vonatkozó jogszabályok és politikák különbözősége akadályozza a vállalkozások több országban való működését és a globális méretgazdaságosság megvalósulását. Az uniós szintű beavatkozás elmaradása esetén minden tagállam egymagában lépne fel, figyelmen kívül hagyva a hálózati és információs rendszerek egymástól való függőségét.

A kitűzött célokat ennélfogva uniós szintű fellépés útján jobban meg lehet valósítani, mint az egyes tagállamok szintjén.

1.5.3. Hasonló korábbi tapasztalatok tanulsága

A javaslat abból a felismerésből fakad, hogy az egyenlő versenyfeltételek megteremtéséhez és egyes joghézagok megszüntetéséhez szabályozási kötelezettségek előírására van szükség. Ezen a területen a tisztán önkéntes megközelítés azt eredményezte, hogy csak néhány, magasabb szintű képességekkel rendelkező tagállam között jött létre együttműködés.

1.5.4. Összhang és lehetséges szinergia egyéb pénzügyi eszközökkel

A javaslat teljes mértékben összhangban áll az európai digitális menetrenddel és ezáltal az Európa 2020 stratégiával, továbbá összhangban van az uniós elektronikus hírközlési szabályozási kerettel, az európai kritikus infrastruktúrákról szóló irányelvvel és az Unió adatvédelmi irányelvével, és kiegészíti ezeket.

Ez a javaslat alapvető elemét képezi a Bizottságnak és az Unió külügyi és biztonságpolitikai főképviselőjének az európai kiberbiztonsági stratégiáról szóló közös közleményének, amellyel összefüggésben előterjesztésre kerül.

1.6. Az intézkedés és a pénzügyi hatás időtartama

– ☐ A javaslat/kezdeményezés határozott időtartamra vonatkozik

– ☐ A javaslat/kezdeményezés időtartama: ÉÉÉÉ [HH/NN]-tól/-től ÉÉÉÉ [HH/NN]-ig

– ☐ Pénzügyi hatás: ÉÉÉÉ-tól/-től ÉÉÉÉ-ig

– ☒ A javaslat/kezdeményezés határozatlan időtartamra vonatkozik

– Az átültetési időszak közvetlenül a (2015-ben várható) elfogadást követően kezdődik, és 18 hónapon keresztül tart. Az irányelv végrehajtása azonban az elfogadását követően azonnal megkezdődik, és kiterjed a tagállamok együttműködését szolgáló biztonságos infrastruktúra felállítására.

– azt követően: rendes ütem.

1.7. Tervezett igazgatási módszer(ek)[39]

– ☒ Centralizált igazgatás közvetlenül a Bizottság által

– ☒ Centralizált igazgatás közvetetten a következőknek történő hatáskör-átruházással:

– ☐végrehajtó ügynökségek

– ☒ a Közösségek által létrehozott szervek[40]

– ☐ tagállami közigazgatási/közfeladatot ellátó szervek

– ☐ az Európai Unióról szóló szerződés V. címe értelmében külön intézkedések végrehajtásával megbízott, a költségvetési rendelet 49. cikke szerinti vonatkozó jogalapot megteremtő jogi aktusban meghatározott személyek

– ☐ Megosztott igazgatás a tagállamokkal

– ☐ Decentralizált igazgatás harmadik országokkal

– ☐ Nemzetközi szervezetekkel közös igazgatás, ideértve az Európai Űrügynökséget is

Egynél több igazgatási módszer feltüntetése esetén kérjük, adjon részletes felvilágosítást a „Megjegyzések” rovatban.

Megjegyzések
A Közösségek által létrehozott és decentralizált ügynökségként működő ENISA a megbízatása keretében és a 2014–2020 közötti időszakra vonatkozó többéves pénzügyi keretben a számára előirányzott források átcsoportosítása révén segítséget nyújthat a tagállamoknak és a Bizottságnak az irányelv végrehajtásában.

[39] Az egyes igazgatási módszerek ismertetése, valamint a költségvetési rendeletben szereplő megfelelő hivatkozások megtalálhatók a Költségvetési Főigazgatóság honlapján: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

[40] A költségvetési rendelet 185. cikkében említett szervek.

2. IRÁNYÍTÁSI INTÉZKEDÉSEK

2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

Ismertesse a nyomon követés és jelentéstétel gyakoriságát és feltételeit.

A Bizottság időszakonként felülvizsgálja az irányelv működését, és a felülvizsgálat eredményeiről jelentést tesz az Európai Parlamentnek és a Tanácsnak.

A Bizottság továbbá értékelni fogja az irányelv tagállamok általi megfelelő átültetését.

Az Európai Hálózatfinanszírozási Eszközre irányuló javaslat lehetőséget biztosít a projektek végrehajtási módjának, valamint megvalósításuk hatásainak azzal a céllal történő értékelésére, hogy kiderüljön, hogy a meghatározott célkitűzések, beleértve a környezetvédelemmel kapcsolatos célkitűzéseket is, teljesültek-e.

2.2. Irányítási és kontrollrendszer

2.2.1. Felismert kockázat(ok)

a biztonságos infrastruktúra kiépítésére irányuló projektek végrehajtásának késedelme

2.2.2. 2.2.2. Tervezett ellenőrzési mód(ok)

Az Európai Hálózatfinanszírozási Eszköz szerinti cselekvések végrehajtására vonatkozó megállapodások és határozatok rendelkeznek a Bizottság vagy a Bizottság meghatalmazott képviselője által végzett felügyeletről és pénzügyi ellenőrzésről, valamint a Számvevőszék által végzett ellenőrzésekről és az Európai Csalás Elleni Hivatal (OLAF) által végzett helyszíni ellenőrzésekről.

2.2.3. Az ellenőrzésekkel járó költségek és hasznok, valamint a várható meg nem felelési arány

Kockázatalapú előzetes és utólagos ellenőrzések, valamint és a helyszínen végzett ellenőrzések biztosítják, hogy az ellenőrzések költségei az ésszerűség határain belül maradjanak.

2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

Tüntesse fel a meglévő vagy tervezett megelőző és védintézkedéseket.

A Bizottság megfelelő intézkedésekkel – csalás, korrupció és más jogellenes cselekmények elleni megelőző intézkedésekkel, hatásos ellenőrzésekkel, szabálytalanság feltárása esetén a jogosulatlanul kifizetett összegek visszafizettetésével, továbbá szükség esetén hatékony, arányos és visszatartó erejű szankciókkal – biztosítja, hogy az Európai Unió pénzügyi érdekei az ezen irányelv alapján finanszírozott fellépések végrehajtása során ne sérüljenek.

A Bizottság és képviselői, valamint a Számvevőszék jogosultak dokumentumalapú és helyszíni ellenőrzést végezni az e program keretében uniós támogatásban részesülő kedvezményezetteknél, vállalkozóknál és alvállalkozóknál.

Az Európai Csalás Elleni Hivatal (OLAF) jogosult az ilyen finanszírozással közvetlenül vagy közvetetten érintett gazdasági szereplőknél a 2185/96/Euratom, EK rendeletben előírt eljárásoknak megfelelően helyszíni ellenőrzéseket és vizsgálatokat végezni annak megállapítására, hogy történt-e az uniós finanszírozásra vonatkozó támogatási megállapodással, támogatási határozattal vagy szerződéssel

összefüggésben olyan csalás, korrupciós vagy más jogellenes cselekmény, amely az Unió pénzügyi érdekeit sérti.

A fenti bekezdések sérelme nélkül az ezen irányelv végrehajtása keretében harmadik országokkal és nemzetközi szervezetekkel kötött együttműködési megállapodásokban és támogatási megállapodásokban, valamint támogatási határozatokban és szerződésekben kifejezetten rendelkezni kell arról, hogy a Bizottság, a Számvevőszék és az OLAF elvégezheti az említett helyszíni és egyéb ellenőrzéseket és vizsgálatokat.

Az Európai Hálózatfinanszírozási Eszköz előírja, hogy a támogatási és beszerzési szerződéseknek a szabványos mintákat kell követniük, amelyek meghatározzák az általában alkalmazandó csalásellenes intézkedéseket.

3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

3.1. A kiadások a többéves pénzügyi keret mely fejezetét/fejezeteit és a költségvetés mely kiadási tételét/tételeit érintik?

- Jelenlegi költségvetési tételek

A többéves pénzügyi keret fejezetei, azon belül pedig a költségvetési tételek sorrendjében.

A többéves pénzügyi keret fejezete	Költségvetési tétel	Kiadás típusa	Hozzájárulás			
	Szám [Megnevezés……]	diff./nem diff.([41])	EFTA-országokt ól[42]	EFTA-országoktól [43]	harmadik országokt ól	a költségvetési rendelet 18. cikke (1) bekezdésének a) pontja értelmében
	09 03 02 a nemzeti közszolgáltatások online összekapcsolódásának és interoperabilitásának, valamint az e hálózatokhoz való hozzáférésnek az előmozdítása.	diff.	NEM	NEM	NEM	NEM

- Létrehozandó új költségvetési tételek (tárgytalan)

A többéves pénzügyi keret fejezetei, azon belül pedig a költségvetési tételek sorrendjében.

A többéves pénzügyi keret fejezete	Költségvetési tétel	Kiadás típusa	Hozzájárulás			
	Szám [Megnevezés……]	diff./nem diff.	EFTA-országokt ól	tagjelölt országoktól	harmadik országokt ól	a költségvetési rendelet 18. cikke (1) bekezdésének a) pontja értelmében
	[XX.YY.YY.YY]		IGEN/ NEM	IGEN/N EM	IGEN/ NEM	IGEN/NEM

41 Diff. = Differenciált előirányzatok / Nem diff. = nem differenciált előirányzatok.

42 EFTA: Európai Szabadkereskedelmi Társulás.

43 Tagjelölt országok és adott esetben a nyugat-balkáni potenciális tagjelölt országok.

3.2. A kiadásokra gyakorolt becsült hatás

3.2.1. A kiadásokra gyakorolt becsült hatás összegzése

millió EUR (három tizedesjegyig)

A többéves pénzügyi keret fejezete:	1	Intelligens és inkluzív növekedés

Főigazgatóság: <…….>			2015* [44]	**2016**. év	**2017**. év	**2018**. év	Ezt követő évek (2019–2021) és később			**ÖSSZESEN**
• Operatív előirányzatok										
09 03 02	Kötelezettségvállalási előirányzatok	(1)	1.250**	0.000						**1.250**
	Kifizetési előirányzatok	(2)	0.750	0.250	0.250					**1.250**
Bizonyos egyedi programok keretéből finanszírozott igazgatási előirányzatok[45]			**0.000**							**0.000**
Költségvetési tétel száma		(3)	**0.000**							**0.000**
A[z] <...> Főigazgatósághoz tartozó előirányzatok ÖSSZESEN	Kötelezettségvállalási előirányzatok	=1+1a +3	1.250	0.000						**1.250**
	Kifizetési előirányzatok	=2+2a +3	0.750	0.250	0.250					**1.250**

• Operatív előirányzatok ÖSSZESEN	Kötelezettségvál	(4)	1.250	0.000						**1.250**

[44] Az N. év a javaslat/kezdeményezés végrehajtásának első éve.

[45] Technikai és/vagy igazgatási segítségnyújtás, valamint uniós programok és/vagy intézkedések végrehajtásához biztosított támogatási kiadások (korábban: BA-tételek), közvetett kutatás, közvetlen kutatás.

	lalási előirányzatok									
	Kifizetési előirányzatok	(5)	0.750	0.250	0.250					**1.250**
• Bizonyos egyedi programok keretéből finanszírozott igazgatási előirányzatok ÖSSZESEN		(6)	**0.000**							
A többéves pénzügyi keret **1. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN**	Kötelezettségvál lalási előirányzatok	=4+ 6	1.250	0.000						**1.250**
	Kifizetési előirányzatok	=5+ 6	0.750	0.250	0.250					**1.250**

*A pontos ütemezés a javaslat jogalkotási hatóság általi elfogadásának időpontjától függ (vagyis ha az irányelv 2014 folyamán jóváhagyásra kerül, a meglévő infrastruktúra átalakítása 2015-ben megkezdődik, különben pedig egy évvel később).

**Ha a tagállamok a meglévő infrastruktúra használata, illetve az egyszeri átalakítási költségek uniós költségvetésből történő finanszírozása mellett döntenek, ahogyan azt az 1.4.3. és 1.7. pontban kifejtettük, a tagállamok közötti együttműködés támogatására szolgáló hálózat testre szabásának becsült költsége az irányelv III. fejezetének (korai előrejelzés, összehangolt válaszintézkedés stb.) megfelelően 1 250 000 EUR. Ez az összeg valamivel magasabb, mint a hatásvizsgálatban említett összeg („kb. 1 millió EUR”), mivel az ilyen infrastruktúra kiépítéséhez szükséges alkotóelemeket illetően pontosabb becsléseken alapul. A szükséges alkotóelemek és a kapcsolódó költségek leírása a JRC-től származik, és a JRC egyéb területeken, például a közegészségügyben hasonló rendszerek kialakítása során szerzett tapasztalatain alapulnak. A szóban forgó alkotóelemek a következők: a hálózat- és információbiztonságot szolgáló gyorsriasztási és bejelentési rendszer (275 000 EUR); információcsere-platform (400 000 EUR); korai előrejelzési és gyorsreagáló rendszer (275 000 EUR); helyzetelemző központ (300 000 EUR), összesen 1 250 000 EUR. A SMART 2012/0010 egyedi szerződéshez kapcsolódóan elkészítendő, „Megvalósíthatósági tanulmány és előkészítő tevékenységek az informatikai támadások és zavarok kivédését szolgáló európai korai előrejelzési és gyorsreagáló rendszer létesítéséhez” című megvalósíthatósági tanulmány várhatóan részletesebb végrehajtási tervet tartalmaz majd.

Amennyiben a javaslat/kezdeményezés több fejezetet is érint:

• Operatív előirányzatok ÖSSZESEN	Kötelezettségvál lalási előirányzatok	(4)	0.000	0.000						
	Kifizetési előirányzatok	(5)	0.000	0.000						

• Bizonyos egyedi programok keretéből finanszírozott igazgatási előirányzatok ÖSSZESEN		(6)	**0.000**	**0.000**						
A többéves pénzügyi keret **1–4. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN (Referenciaösszeg)**	Kötelezettségvállalási előirányzatok	=4+ 6	1.250	0.000						1.250
	Kifizetési előirányzatok	=5+ 6	0.750	0.250	0.250					1.250

A többéves pénzügyi keret fejezete	**5**	„Igazgatási kiadások”

millió EUR (három tizedesjegyig)

		2015. év	**2016**. év	**2017**. év	**2018**. év	Ezt követő évek (2019–2021) és később			**ÖSSZESEN**
Főigazgatóság: CNECT									
• Humánerőforrás		0.572	0.572	0.572	0.572	0.572	0.572	**0.572**	**4.004**
• Egyéb igazgatási kiadások		0.318	0.118	0.318	0.118	0.318	0.118	**0.118**	**1.426**
CNECT Főigazgatóság ÖSSZESEN	Előirányzatok	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

A többéves pénzügyi keret **5. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN**	Összes kötelezettségvállalási előirányzat = Összes kifizetési előirányzat	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

millió EUR (három tizedesjegyig)

		2015. év[46]	**2016**. év	**2017**. év	**2018**. év	Ezt követő évek (2019–2021) és később			**ÖSSZESEN**
A többéves pénzügyi keret **1–5. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN**	Kötelezettségvállalási előirányzatok	2.140	0.690	0.890	0.690	0.890	0.690	0.690	**6.680**
	Kifizetési előirányzatok	1.640	0.940	1.140	0.690	0.890	0.690	0.690	**6.680**

[46] Az N. év a javaslat/kezdeményezés végrehajtásának első éve.

3.2.2. Az operatív előirányzatokra gyakorolt becsült hatás

– ☐ A javaslat/kezdeményezés nem vonja maga után operatív előirányzatok felhasználását.

– ☑ A javaslat/kezdeményezés az alábbi operatív előirányzatok felhasználását vonja maga után:

– Kötelezettségvállalási előirányzatok, millió EUR (három tizedesjegyig)

Tüntesse fel a célkitűzéseket és a teljesítéseket ⇩			**2015**. év*****		**2016**. év		**2017**. év		**2018**. év		Ezt követő évek (2019–2021) és később						**ÖSSZESEN**	
	TELJESÍTÉSEK																	
	Típus[47]	Átlagos költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Teljesítések száma összesen	Összköltség
2. KONKRÉT CÉLKITŰZÉS[48] Biztonságos információmegosztási infrastruktúra																		
- Teljesítés	Az infrastruktúra átalakítása																	
2. konkrét célkitűzés részösszege			1	1.250**													1	1.250
ÖSSZKÖLTSÉG				1.250														1.250

[47] A teljesítés a nyújtandó termékekre és szolgáltatásokra vonatkozik (pl. finanszírozott diákcserék száma, épített utak hossza kilométerben stb.).

[48] Az 1.4.2. pontban („Konkrét célkitűzések...”) feltüntetett célkitűzés.

*A pontos ütemezés a javaslat jogalkotási hatóság általi elfogadásának időpontjától függ (vagyis ha az irányelv 2014 folyamán jóváhagyásra kerül, a meglévő infrastruktúra átalakítása 2015-ben megkezdődik, különben pedig egy évvel később).

**Lásd a 3.2.1 pontban.

3.2.3. Az igazgatási előirányzatokra gyakorolt becsült hatás

3.2.3.1. Összegzés

– ☐ A javaslat/kezdeményezés nem vonja maga után igazgatási előirányzatok felhasználását.

– ☑ A javaslat/kezdeményezés az alábbi igazgatási előirányzatok felhasználását vonja maga után:

millió EUR (három tizedesjegyig)

	2015. év[49]	**2016**. év	**2017**. év	**2018**. év	Ezt követő évek (2019–2021) és később			**ÖSSZESEN**
A többéves pénzügyi keret 5. FEJEZETE								
Humánerőforrás	0.572	0.572	0.572	0.572	0.572	0.572	0.572	**4.004**
Egyéb igazgatási kiadások	0.318	0.118	0.318	0.118	0.318	0.118	0.118	**1.426**
A többéves pénzügyi keret 5. FEJEZETÉNEK részösszege	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**
A többéves pénzügyi keret 5. FEJEZETÉBE[50] bele nem tartozó előirányzatok								
Humánerőforrás	0.000	0.000						**0.000**
Egyéb igazgatási kiadások								
A többéves pénzügyi keret 5. FEJEZETÉBE bele nem tartozó előirányzatok részösszege	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**
ÖSSZESEN	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

A szükséges igazgatási előirányzatokat a CNECT Főigazgatóság rendelkezésére álló, már a cselekvés igazgatásához rendelt és/vagy a főigazgatóságon belüli átcsoportosított

[49] Az N. év a javaslat/kezdeményezés végrehajtásának első éve.

[50] Technikai és/vagy igazgatási segítségnyújtás, valamint uniós programok és/vagy intézkedések végrehajtásához biztosított támogatási kiadások (korábban: BA-tételek), közvetett kutatás, közvetlen kutatás.

előirányzatokból kell fedezni, lehetőség szerint kiegészítve az irányítást végző főigazgatósághoz az éves elosztási eljárás keretén belül, a meglévő költségvetési korlátok betartása mellett rendelt további juttatásokkal.

Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) a megbízatása keretében és a 2014–2020 közötti időszakra vonatkozó többéves pénzügyi keretben a számára előirányzott források átcsoportosítása révén (tehát minden további költségvetési forrás és humánerőforrásra vonatkozó előirányzat felhasználása nélkül) segítséget nyújthat a tagállamoknak és a Bizottságnak az irányelv végrehajtásában.

3.2.3.2. Becsült humánerőforrás-szükségletek

– ☐ A javaslat/kezdeményezés nem igényel humánerőforrást.

– ☑ A javaslat/kezdeményezés az alábbi humánerőforrás-igénnyel jár:

Elvben a javaslat nem igényel több humánerőforrást. A szükséges humánerőforrások igen korlátozottak, és az igényt a főigazgatóságnak a cselekvés irányításával már megbízott személyzete fogja fedezni.

A becsléseket egész számmal (vagy legfeljebb egy tizedesjeggyel) kell kifejezni

		2015. év	**2016**. év	**2017**. év	**2018**. év	Ezt követő évek (2019–2021) és később		
• A létszámtervben szereplő álláshelyek (tisztviselői és ideiglenes alkalmazotti álláshelyek)								
09 01 01 01 (a központban és a bizottsági képviseleteken)		4	4	4	4	4	4	4
XX 01 01 02 (a küldöttségeknél)								
XX 01 05 01 (közvetett kutatás)								
10 01 05 01 (közvetlen kutatás)								
• Külső személyi állomány (teljes munkaidős egyenértékben kifejezve)[51]								
09 01 02 01 (AC, INT, END a teljes keretből)		1	1	1	1	1	1	1
XX 01 02 02 (AC, AL, END, INT és JED a küldöttségeknél)								
XX 01 04 yy[52]	- a központban[53]							
	- a küldöttségeknél							
XX 01 05 02 (AC, END, INT közvetett kutatásban)								
10 01 05 02 (AC, END, INT közvetlen kutatásban)								
Egyéb költségvetési tétel (kérjük megnevezni)								
ÖSSZESEN		**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX: az érintett szakpolitikai terület vagy költségvetési cím.

A humánerőforrás-igényeknek a CNECT Főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt személyzettel és/vagy az adott főigazgatóságon belüli személyzet-átcsoportosítással kell eleget tenni. A források adott esetben a költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további juttatásokkal.

51 AC= szerződéses alkalmazott; AL= helyi alkalmazott; END= kirendelt nemzeti szakértő; INT=átmeneti alkalmazott; JED=küldöttségi pályakezdő szakértő.

52 Az operatív előirányzatoknál a külső személyzetre részleges felső határérték vonatkozik (korábban: BA-tételek).

53 Elsősorban a strukturális alapok, az Európai Mezőgazdasági Vidékfejlesztési Alap (EMVA) és az Európai Halászati Alap (EHA) esetében.

Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) jelenlegi megbízatása keretében és a 2014–2020 közötti időszakra vonatkozó többéves pénzügyi keretben a számára előirányzott források átcsoportosítása révén (tehát minden további költségvetési forrás és humánerőforrásra vonatkozó előirányzat felhasználása nélkül) segítséget nyújthat a tagállamoknak és a Bizottságnak az irányelv végrehajtásában.

Az elvégzendő feladatok leírása:

Tisztviselők és ideiglenes alkalmazottak	Felhatalmazáson alapuló jogi aktusok előkészítése a 14. cikk (3) bekezdése alapján Végrehajtási jogi aktusok előkészítése a 8. cikk, a 9. cikk (2) bekezdése, a 12. cikk, 14. cikk (5) bekezdése , valamint a 16. cikk alapján Együttműködési hozzájárulás a hálózaton keresztüli politikai és operatív szinten egyaránt. Részvétel nemzetközi tárgyalásokon és adott esetben nemzetközi megállapodások kötése
Külső személyzet	Szükség szerint a fenti tevékenységek támogatása.

3.2.4. A jelenlegi többéves pénzügyi kerettel való összeegyeztethetőség

– ☑ A javaslat/kezdeményezés összeegyeztethető a jelenlegi többéves pénzügyi kerettel.

– ☐ A javaslat/kezdeményezés miatt szükséges a többéves pénzügyi keret vonatkozó fejezetének átprogramozása.

A javaslat operatív kiadásokra gyakorolt becsült pénzügyi hatása akkor merül fel, ha a tagállamok a meglévő infrastruktúra átalakítása mellett döntenek, és a Bizottságot bízzák meg a feladatnak a 2014–2020 közötti időszakra vonatkozó többéves pénzügyi kereten belüli végrehajtásával. A kapcsolódó egyszeri költséget az Európai Hálózatfinanszírozási Eszköz fedezné azzal a feltétellel, hogy a megfelelő források rendelkezésre állnak. Alternatív megoldásként a tagállamok megoszthatják az infrastruktúra átalakításának vagy az új infrastruktúra létrehozásának költségeit.

– ☐ A javaslat/kezdeményezés miatt szükség van a rugalmassági eszköz alkalmazására vagy a többéves pénzügyi keret felülvizsgálatára[54].

Tárgytalan.

3.2.5. Harmadik felek részvétele a finanszírozásban

– A javaslat/kezdeményezés nem irányoz elő harmadik felek általi társfinanszírozást.

3.3. A bevételre gyakorolt becsült pénzügyi hatás

– ☑ A javaslatnak/kezdeményezésnek nincs pénzügyi hatása a bevételre.

[54] Lásd az intézményközi megállapodás 19. és 24. pontját.