I

(Jogalkotási aktusok)

IRÁNYELVEK

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/1148 IRÁNYELVE

(2016. július 6.)

a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

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 tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére ([1]),

rendes jogalkotási eljárás keretében ([2]),

mivel:

(1) A hálózati és információs rendszerek és szolgáltatások létfontosságú szerepet játszanak társadalmunkban. Megbízhatóságuk és biztonságuk alapvetően lényeges a gazdasági és társadalmi tevékenységek, és különösen a belső piac működése szempontjából.

(2) A biztonsági események nagyságrendje, gyakorisága és hatása növekszik, ami súlyos fenyegetést jelent a hálózati és az információs rendszerek működésére nézve. E rendszerek emellett a működésük akadályozására vagy megszakítására irányuló szándékos és ártalmas cselekmények célpontjaivá válhatnak. Az ilyen események nehezíthetik a gazdasági tevékenységek folytatását, jelentős pénzügyi veszteségeket okozhatnak, aláásható a felhasználói bizalmat és súlyos károkat okozhatnak az Unió gazdaságának.

(3) A hálózati és információs rendszerek, és mindenekelőtt az internet, alapvető szerepet játszanak az áruk, a szolgáltatások és a személyek határokon átnyúló mozgásának elősegítésében. Transznacionális jellegük miatt e rendszerek jelentős zavara érinthet egyes tagállamokat, de akár az Unió egészét is, függetlenül attól, hogy azt szándékosan vagy nem szándékosan okozták-e, illetve tekintet nélkül az előfordulás helyére. A hálózati és információs rendszerek biztonsága ezért alapvető fontosságú a belső piac zavartalan működése szempontjából.

(4) A tagállamok európai fórumának keretében jelentős előrelépés történt a bevált szakpolitikai gyakorlatokkal – és például a kiberválságokat érintő európai együttműködés elveinek kidolgozásával – kapcsolatos megbeszélések és véleménycserék előmozdításában, amire építve helyénvaló együttműködési csoportot létrehozni a tagállamok képviselői, a Bizottság, valamint az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (a továbbiakban: ENISA) közreműködésével, amelynek feladata a hálózati és információs rendszerek biztonsága tekintetében

([1]) HL C 271., 2013.9.19., 133. o.

([2]) Az Európai Parlament 2014. március 13-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács első olvasatban kialakított 2016. május 17-i álláspontja (a Hivatalos Lapban még nem tették közzé). Az Európai Parlament 2016. július 6-i álláspontja (a Hivatalos Lapban még nem tették közzé).

a tagállamok között folytatott stratégiai együttműködés támogatása és elősegítése. E csoport eredményességének és inkluzív jellegének biztosítása érdekében alapvető fontosságú, hogy minden tagállam rendelkezzen minimális képességekkel, és a saját területén a hálózati és információs rendszerek biztonsága magas szintjét biztosító stratégiával. Ezenkívül biztonsági és bejelentési követelményeknek kell vonatkozniuk az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra a kockázatkezelés kultúrájának előmozdítása és annak biztosítása érdekében, hogy sor kerüljön a legsúlyosabb események bejelentésére.

(5) A meglévő képességek nem elegendőek ahhoz, hogy garantálják a hálózati és információs rendszerek magas biztonsági szintjét az Unión belül. A tagállamok felkészültségi szintje nagyon különböző, ami sokféle megközelítés alkalmazásához vezetett az Unióban. Ez a fogyasztók és a vállalkozások egyenlőtlen védelmét eredményezi, továbbá aláássa a hálózati és információs rendszerek biztonságának általános szintjét az Unión belül. Az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra vonatkozó egységes követelmények hiánya miatt nem lehetséges uniós szinten átfogó és hatékony együttműködési mechanizmust létrehozni. Az egyetemek és a kutatóközpontok döntő szerepet játszanak a szóban forgó területekre irányuló kutatás, fejlesztés és innováció ösztönzésében.

(6) A hálózati és információs rendszerek biztonsági kihívásainak hatékony kezelése ezért olyan globális megközelítést igényel uniós szinten, amely kiterjed a kapacitásépítésre és a tervezésre vonatkozó közös minimumkövetelményekre, az információcserére, az együttműködésre, valamint az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra vonatkozó közös biztonsági követelményekre is. Az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók azonban végrehajthatnak az ebben az irányelvben meghatározottaknál szigorúbb biztonsági intézkedéseket is.

(7) Annak érdekében, hogy a szabályozás valamennyi lényeges biztonsági eseményre és kockázatra kiterjedjen, ezt az irányelvet mind az alapvető szolgáltatásokat nyújtó szereplőkre, mind a digitális szolgáltatókra alkalmazni kell. Az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra vonatkozó kötelezettségeket azonban nem kell alkalmazni azokra a vállalkozásokra, amelyek a 2002/21/EK európai parlamenti és tanácsi irányelv ([1]) szerinti olyan, nyilvános hírközlő hálózatokat üzemeltetnek vagy nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtanak, amelyek az említett irányelvben megállapított különös biztonsági és integritási követelmények hatálya alá tartoznak, továbbá nem kell alkalmazni a 910/2014/EU európai parlamenti és tanácsi rendelet ([2]) szerinti olyan bizalmi szolgáltatókra sem, amelyek az említett rendeletben megállapított biztonsági követelmények hatálya alá tartoznak.

(8) Ezen irányelv nem sértheti a tagállamok számára biztosított azon lehetőséget, hogy megtegyék az alapvető biztonsági érdekeik védelméhez, a közrend és a közbiztonság megóvásához, valamint a bűncselekmények kivizsgálásának, felderítésének és a büntetőeljárások lefolytatásának lehetővé tételéhez szükséges intézkedéseket. Az Európai Unió működéséről szóló szerződés (EUMSZ) 346. cikke értelmében egyetlen tagállam sem köteles olyan információt szolgáltatni, amelynek közlését ellentétesnek tartja alapvető biztonsági érdekeivel. Ebben az összefüggésben figyelembe kell venni a 2013/488/EU tanácsi határozatot ([3]) valamint a titoktartási megállapodásokat és a nem hivatalos megállapodásokat, például a TLP-protokollt (*jelzőlámpa-protokoll*).

(9) Egyes gazdasági ágazatokat már szabályoznak vagy a jövőben szabályozhatnak olyan ágazatspecifikus uniós jogi aktusok, amelyek tartalmaznak a hálózati és az információs rendszerek biztonságával kapcsolatos szabályokat. Minden olyan esetben, amikor uniós jogi aktusok a hálózati és az információs rendszerek biztonságára vagy a biztonsági események bejelentésére vonatkozó követelményeket meghatározó rendelkezéseket tartalmaznak, az említett rendelkezéseket kell alkalmazni, ha azok olyan követelményeket tartalmaznak, amelyek a kötelezettségek hatását tekintve legalább egyenlőek az ebben az irányelvben meghatározottakkal. Ilyen esetben a tagállamoknak az adott ágazatspecifikus uniós jogi aktus rendelkezéseit kell alkalmazniuk, a joghatósággal kapcsolatos rendelkezéseket is beleértve, és nem kell elvégezniük az ezen irányelv meghatározása szerinti alapvető szolgáltatásokat nyújtó szereplők azonosítására szolgáló eljárást. Ezzel összefüggésben a tagállamoknak tájékoztatniuk kell a Bizottságot az ilyen *lex specialis*-ra vonatkozó rendelkezések alkalmazásáról. Annak megállapításakor, hogy a hálózati és információs rendszerek biztonságára és az események bejelentésére vonatkozóan az ágazatspecifikus uniós jogi aktusokban foglalt követelmények egyenértékűek-e az ezen irányelvben szereplőkkel, kizárólag a vonatkozó uniós jogi aktusok rendelkezéseit és azoknak a tagállamokban való alkalmazását kell figyelembe venni.

(10) A vízi közlekedési ágazat esetében a vállalatokra, hajókra, kikötői létesítményekre, kikötőkre és hajóforgalmi szolgálatokra vonatkozó biztonsági követelményeket az uniós jogi aktusok értelmében minden műveletre alkalmazni kell, ideértve a rádió- és távközlési rendszereket, számítógépes rendszereket és hálózatokat is. A követendő kötelező eljárások közé tartozik minden biztonsági esemény bejelentése, és *lex specialis*-nak tekintendők, amennyiben legalább egyenértékűek ezen irányelv vonatkozó rendelkezéseivel.

([1]) Az Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról (Keretirányelv) (HL L 108., 2002.4.24., 33. o.).

([2]) Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (HL L 257., 2014.8.28., 73. o.).

([3]) A Tanács 2013/488/EU határozata (2013. szeptember 23.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (HL L 274., 2013.10.15., 1. o.).

(11) A vízi közlekedési ágazatban működő gazdasági szereplők azonosításakor a tagállamoknak figyelembe kell venniük a már meglévő és a jövőbeli nemzetközi szabályzatokat és iránymutatásokat, különösen a Nemzetközi Tengerészeti Szervezet által kidolgozottakat annak érdekében, hogy a tengerhasznosítási ágazat szereplői számára koherens megközelítést biztosítsanak.

(12) Az elsődleges és másodlagos uniós jog, valamint az európai felügyeleti hatóságokkal közösen kidolgozott szabványok uniós szinten biztosítják a banki és pénzügyi piaci infrastruktúrákra vonatkozó szabályozás és felügyelet magas szintű harmonizációját. Az említett szabályok és szabványok alkalmazásáról és felügyeletéről a bankunión belül az egységes felügyeleti mechanizmus gondoskodik. A bankunió részét nem képező tagállamokban ezt a feladatot a tagállamok megfelelő banki szabályozói látják el. A pénzügyi szabályozás más területeit illetően a Pénzügyi Felügyeletek Európai Rendszere biztosítja a felügyeleti gyakorlatok magas fokú hasonlóságát és összehangoltságát. Az Európai Értékpapír-piaci Hatóság szintén közvetlen felügyeleti szerepet tölt be bizonyos szervek, nevezetesen a hitelminősítő intézetek és a kereskedési adattárak tekintetében.

(13) A működési kockázat a banki és pénzügyi piaci infrastruktúrákra vonatkozó prudenciális szabályozás és felügyelet alapvető része, és kiterjed a működés minden elemére, így a hálózati és információs rendszerek biztonságára, integritására és ellenálló képességére is. Az e rendszerekre vonatkozó követelmények – amelyek gyakran túlmutatnak az ezen irányelvben előírt követelményeken – számos uniós jogi aktusban vannak meghatározva, köztük: a hitelintézetek tevékenységéhez való hozzáférésre és a hitelintézetek és befektetési vállalkozások prudenciális felügyeletére, valamint a hitelintézetekre és befektetési vállalkozásokra vonatkozó prudenciális követelményekre vonatkozó szabályokban, amelyek követelményeket írnak elő a működési kockázat tekintetében; a pénzügyi eszközök piacaira vonatkozó szabályokban, amelyek követelményeket írnak elő a befektetési vállalkozások és a szabályozott piacok kockázatértékelése tekintetében; a tőzsdén kívüli származtatott ügyletekre, a központi szerződő felekre és a kereskedési adattárakre vonatkozó szabályokban, amelyek követelményeket írnak elő a központi szerződő felek és a kereskedési adattárak működési kockázatai tekintetében; továbbá az Unión belüli értékpapír-kiegyenlítés javítására és a központi értéktárakra vonatkozó szabályokban, amelyek követelményeket írnak elő a működési kockázat tekintetében. Ezen túlmenően a biztonsági események bejelentésére vonatkozó követelmények a pénzügyi ágazatra jellemző rendes felügyeleti gyakorlatoknak is részét képezik, és gyakran szerepelnek a felügyeleti kézikönyvekben. A tagállamoknak a *lex specialis* alkalmazása során figyelembe kell venniük az említett szabályokat és követelményeket.

(14) Ahogyan azt az Európai Központi Bank a hálózat- és információbiztonsági javaslatról szóló, 2014. július 25-i véleményében ([1]) megállapította, ez az irányelv nem érinti a fizetési és elszámolási rendszerek eurorendszerbeli felügyeletére vonatkozó uniós jogi szabályozást. Célszerű lenne, hogy az említett felügyeletért felelős hatóságok és az ezen irányelv szerinti illetékes hatóságok tapasztalatot cseréljenek egymással a hálózati- és információs rendszerek biztonságával kapcsolatos kérdésekről. Ugyanez érvényes a Központi Bankok Európai Rendszerének az euroövezetben nem résztvevő tagjaira is, akik nemzeti jogszabályok és előírások alapján végzik a fizetési és elszámolási rendszerek felügyeletét.

(15) Az online piacterek lehetővé teszik, hogy a fogyasztók és a kereskedők online adás-vételi és szolgáltatási szerződéseket kössenek kereskedőkkel, emellett ezek a piacterek az említett szerződések megkötésének végpontjai. Ez nem vonatkozik az olyan online szolgáltatásokra, amelyek csupán köztes lépéseket jelentenek olyan harmadik fél által nyújtott szolgáltatások előtt, amelyek keretében a szerződések végleges megkötésére sor kerülhet. Ennélfogva nem vonatkozik olyan online szolgáltatásokra, amelyek különböző kereskedők által kínált azonos termékek vagy szolgáltatások árát hasonlítják össze, majd a termék megvásárlása céljából a kiválasztott kereskedőhöz irányítják a felhasználót. Az online piacterek által nyújtott számítástechnikai szolgáltatások magukba foglalhatják az ügyletek feldolgozását, adatok összesítését vagy felhasználói profilok alkotását. Az alkalmazásokat értékesítő – harmadik felek alkalmazásainak vagy számítógépes programjainak digitális értékesítését lehetővé tevő – online üzleteket az online piacterek egyik válfajának kell tekinteni.

(16) Az online keresőprogramoknak lehetővé teszik a felhasználók számára, hogy egy adott kulcsszó alapján elvben minden webhelyen keresést hajtsanak végre bármely témában. A keresések meghatározott nyelvű webhelyekre is összpontosulhatnak. Az online keresőprogramok ezen irányelvben szereplő fogalommeghatározása nem terjed ki olyan keresőfunkciókra, amelyek meghatározott webhely tartalmára korlátozódnak, függetlenül attól, hogy a keresőfunkciót külső keresőprogram biztosítja-e. Nem terjed ki olyan online szolgáltatásokra sem, amelyek különböző kereskedők által kínált azonos termékek vagy szolgáltatások árát hasonlítják össze, majd a termék megvásárlása céljából a kiválasztott kereskedőhöz irányítják a felhasználót.

(17) A felhőlapú számítástechnikai szolgáltatások a tevékenységek széles körét foglalhatják magukban, amelyeket különböző modellek szerint lehet biztosítani. Ezen irányelv alkalmazásában a „felhőlapú számítástechnikai szolgáltatások” kifejezés olyan szolgáltatásokra terjed ki, amelyek hozzáférést tesznek lehetővé a megosztható számítástechnikai erőforrások méretezhető és rugalmas pooljához. Az említett számítástechnikai erőforrások olyan erőforrásokat foglalnak magukban, mint a hálózatok, a szerverek vagy más infrastruktúra, a tárolás, az alkalmazások és a szolgáltatások. A „méretezhető” kifejezés olyan számítástechnikai erőforrásokra vonatkozik, amelyeket annak szolgáltatója a keresletbeli ingadozások kezelése érdekében rugalmasan oszt el, az erőforrások földrajzi elhelyezkedésétől függetlenül. A „rugalmas pool” kifejezés azokat a számítástechnikai erőforrásokat

([1]) HL C 352., 2014.10.7., 4. o.

foglalja magában, amelyeket a keresletnek megfelelően nyújtanak és bocsátanak rendelkezésre annak érdekében, hogy a rendelkezésre álló erőforrások a munkatehernek megfelelően gyors ütemben növekedjenek vagy csökkenjenek. A „megosztható" kifejezés alatt az értendő, hogy az adott számítástechnikai erőforrásokat több olyan felhasználó számára biztosítják, akik közös hozzáféréssel rendelkeznek a szolgáltatáshoz, de a feldolgozás minden felhasználó tekintetében külön történik, noha a szolgáltatás nyújtására ugyanazon elektronikus eszközről kerül sor.

(18) Az internetes exchange pontok (a továbbiakban: IXP) funkciója a hálózatok összekapcsolása. Az IXP-k nem biztosítanak hálózati hozzáférést, és nem működnek tranzitszolgáltatóként vagy adattovábbítóként sem. Az IXP-k nem nyújtanak az összekapcsoláshoz nem tartozó egyéb szolgáltatásokat sem, noha ez nem zárja ki azt, hogy egy IXP-üzemeltető ilyen, nem kapcsolódó szolgáltatásokat nyújtson. Az IXP-k célja, hogy összekapcsoljanak egymástól műszakilag és szervezetileg külön álló hálózatokat. A műszakilag önálló hálózatok megnevezésére az „autonóm rendszer" kifejezés használatos.

(19) A tagállamok felelősségi körébe kell tartozzon annak meghatározása, hogy mely szervezetek esetében teljesülnek az alapvető szolgáltatásokat nyújtó szereplő fogalommeghatározásának kritériumai. Az egységes megközelítés biztosítása érdekében az alapvető szolgáltatásokat nyújtó szereplő fogalommeghatározását minden tagállamnak koherens módon kell alkalmaznia. Ennek érdekében ez az irányelv rendelkezik az egyes ágazatokban és alágazatokban tevékenykedő szervezetek értékeléséről, az alapvető szolgáltatások jegyzékének létrehozásáról, az annak eldöntésére szolgáló ágazatközi tényezők közös jegyzékének a mérlegeléséről, hogy egy potenciális biztonsági esemény jelentős zavart okozna-e, az egynél több tagállamban szolgáltatásokat nyújtó szervezetek esetében az érintett tagállamok bevonásával zajló egyeztetési folyamatról, valamint az azonosítási eljárás során az együttműködési csoport támogatásáról. Annak biztosítása érdekében, hogy az azonosított gazdasági szereplők jegyzéke pontosan tükrözze az esetleges piaci változásokat, a jegyzéket a tagállamoknak rendszeresen felül kell vizsgálniuk és szükség esetén naprakésszé kell tenniük. Végezetül a tagállamoknak be kell nyújtaniuk a Bizottság részére az annak értékeléséhez szükséges információkat, hogy ez a közös módszertan milyen mértékben tette lehetővé a fogalommeghatározás tagállamok általi egységes alkalmazását.

(20) Az alapvető szolgáltatásokat nyújtó szereplőkre irányuló azonosítási eljárás során értékelni kell legalább az ebben az irányelvben említett alágazatok mindegyike tekintetében, hogy mely szolgáltatások tekintendők alapvetőnek a kritikus társadalmi és gazdasági tevékenységek fenntartása szempontjából, valamint hogy az ebben az irányelvben említett ágazatokban és alágazatokban tevékenykedő és a szóban forgó szolgáltatásokat nyújtó szervezetek esetében teljesülnek-e a szereplők azonosítására vonatkozó kritériumok. Annak értékelése során, hogy a szervezet kritikus társadalmi és gazdasági tevékenységek fenntartásához szükséges szolgáltatást nyújt-e, elegendő megvizsgálni, hogy az adott szervezet az alapvető szolgáltatások jegyzékében foglalt szolgáltatást nyújt-e. Bizonyítani kell továbbá, hogy az alapvető szolgáltatás nyújtása hálózati és információs rendszerektől függ. Végezetül annak értékelése során, hogy egy biztonsági esemény jelentős zavart okozna-e a szolgáltatás nyújtásában, a tagállamoknak figyelembe kell venniük ágazatközi, valamint adott esetben ágazatspecifikus tényezőket is.

(21) Az alapvető szolgáltatásokat nyújtó szereplők azonosítása céljából egy adott tagállamban történő letelepedés a tevékenység tényleges és valós, állandó keretek között történő végzését jelenti. E keretek jogi formája – legyen szó akár fiókteleprő vagy jogi személyiséggel rendelkező leányvállalatról – e tekintetben nem meghatározó tényező.

(22) Lehetséges, hogy az ezen irányelvben említett ágazatokban és alágazatokban tevékenykedő szervezetek alapvető és nem alapvető szolgáltatásokat is nyújtanak. Például a légi közlekedési ágazatban a repülőterek nyújtanak olyan szolgáltatásokat, amelyeket valamely tagállam alapvetőnek tekint, például a futópályák kezelését, de olyanokat is, amelyeket nem alapvetőnek lehet tekinteni, például a bevásárlóterületek üzemeltetését. Az alapvető szolgáltatásokat nyújtó szereplőkkel szemben csak az alapvetőnek tekintett szolgáltatások vonatkozásában kell különös biztonsági követelményeket támasztani. A gazdasági szereplők azonosítása céljából ezért a tagállamoknak össze kell állítaniuk azon szolgáltatások jegyzékét, amelyeket alapvetőnek tekintenek.

(23) A szolgáltatások jegyzékében szerepelnie kell a tagállam területén nyújtott minden olyan szolgáltatásnak, amelynek esetében teljesülnek az ezen irányelv szerinti követelmények. A tagállamoknak képesnek kell lenniük arra, hogy a meglévő jegyzéket új szolgáltatásokkal egészítsék ki. A szolgáltatások jegyzékének referenciapontként kell szolgálnia a tagállamok számára az alapvető szolgáltatásokat nyújtó szereplők azonosításához. Célja, hogy lehetővé tegye az ezen irányelvben említett bármely ágazatban az alapvető szolgáltatások azonosítását, ezáltal megkülönböztetve ezeket a nem alapvető szolgáltatásoktól, amelyeket az ágazatok bármelyikében tevékeny szervezet nyújthat. A szolgáltatások egyes tagállamok által összeállított jegyzékei további támpontként szolgálnának az egyes tagállamok szabályozási gyakorlatának értékelése során, biztosítandó, hogy az azonosítási eljárás a tagállamok között egységes legyen.

(24) Az azonosítási eljárás céljából, ha egy szervezet két vagy annál több tagállamban nyújt alapvető szolgáltatást, az érintett tagállamoknak két- vagy többoldalú egyeztetéseket kell folytatniuk egymással. Ennek az egyeztetési eljárásnak a célja, hogy segítsék egymást a gazdasági szereplő kritikus jellege határokon átnyúló hatásainak értékelése tekintetében, ezáltal lehetővé téve minden érintett tagállam számára, hogy ismertesse a szolgáltatásokhoz társuló kockázatokkal kapcsolatos nézeteit. Az érintett tagállamoknak figyelembe kell venniük egymás véleményét, illetve kérhetik e tekintetben az együttműködési csoport segítségét.

(25) Az azonosítási eljárás eredményeként a tagállamoknak olyan nemzeti intézkedéseket kell elfogadniuk, amelyek meghatározzák, hogy mely szervezetekre vonatkoznak a hálózati és információs rendszerek biztonságát szabályozó kötelezettségek. Ez történhet az alapvető szolgáltatásokat nyújtó minden gazdasági szereplőt felsoroló jegyzék összeállításával vagy olyan nemzeti intézkedések – köztük objektív módon számszerűsíthető kritériumok – elfogadásával, mint például a gazdasági szereplő teljesítménye vagy a felhasználók száma, amely intézkedések lehetővé tennék annak meghatározását, hogy mely szervezetekre vonatkoznak a hálózati és információs rendszerek biztonságát szabályozó kötelezettségek. A nemzeti intézkedések közé kell tartoznia minden olyan jogi és közigazgatási intézkedésnek, valamint szakpolitikának, amely lehetővé teszi az ezen irányelv szerinti alapvető szolgáltatásokat nyújtó szereplők azonosítását, tekintet nélkül arra, hogy ezek az intézkedések már léteznek vagy elfogadásukra ezen irányelvvel összefüggésben került sor.

(26) Annak érdekében, hogy jelezni lehessen az azonosított, alapvető szolgáltatásokat nyújtó szereplők fontosságát az érintett ágazat szempontjából, a tagállamoknak figyelembe kell venniük az említett szereplők számát és méretét, például piaci részesedésük vagy az általuk előállított vagy szállított mennyiségek tekintetében, anélkül, hogy kötelesek lennének olyan információkat közzétenni, amelyek felfednék az azonosított szereplők kilétét.

(27) Annak meghatározása érdekében, hogy egy adott biztonsági esemény jelentős zavart okozna-e egy adott szolgáltatás nyújtásában, a tagállamoknak több különböző tényezőt kell figyelembe venniük, mint például az adott szolgáltatásra magán vagy szakmai célokból hagyatkozó felhasználók számát. Az említett szolgáltatás használata történhet közvetlenül, közvetetten vagy közvetítőn keresztül. Annak értékelése során, hogy egy biztonsági esemény mértékét és időtartamát tekintve milyen hatást gyakorolna a gazdasági és társadalmi tevékenységekre vagy a közbiztonságra, a tagállamoknak azt is fel kell mérniük, hogy az üzemzavar negatív hatása vélhetően mennyi idő elteltével nyilvánulna meg.

(28) Az ágazatközi tényezőkön túl ágazatspecifikus tényezőket is figyelembe kell venni annak meghatározása érdekében, hogy egy adott biztonsági esemény jelentős zavart okozna-e egy adott szolgáltatás nyújtásában. Ezek a tényezők magukban foglalhatnák a következőket: az energiaszolgáltatók tekintetében a tagállamban előállított energia volumenét vagy arányát; az olajszállítók esetében a napi mennyiséget; a légi közlekedés – beleértve a repülőtereket és a légi fuvarozókat – a vasúti közlekedés és a tengeri kikötők esetében a tagállambeli szállítás volumenének arányát, valamint az utasok vagy a teherszállítási műveletek éves számát; a banki vagy pénzügyi piaci infrastruktúrák tekintetében a teljes vagyonukon vagy e vagyonnak a GDP-hez viszonyított arányán alapuló rendszerszintű jelentőségüket; az egészségügyi ágazat esetében a szolgáltató által évente ellátott betegek számát; a víztermelés, -feldolgozás és -szolgáltatás esetében a mennyiséget, valamint a szolgáltatást igénybe vevő felhasználók számát és típusát, például azt, hogy kórházakról, közszolgálatokról, szervezetekről vagy egyénekről van-e szó, valamint olyan alternatív vízforrások meglétét, amelyekkel ugyanazt a földrajzi területet el lehet látni.

(29) A hálózati és információs rendszerek magas biztonsági szintjének elérése és fenntartása érdekében minden tagállamnak rendelkeznie kell a nemzeti hálózati és információs rendszerek biztonsági stratégiájával, amely meghatározza a stratégiai célokat és a végrehajtandó konkrét szakpolitikai intézkedéseket.

(30) Tekintettel a nemzeti kormányzási struktúrák közötti különbségekre, valamint a meglévő ágazati intézkedések vagy az uniós felügyeleti és szabályozó szervek megőrzése és az átfedések elkerülése érdekében a tagállamoknak lehetőséget kell kapniuk arra, hogy az ezen irányelv hatálya alá tartozó alapvető szolgáltatásokat nyújtó szereplők és digitális szolgáltatók hálózati és információs rendszereinek biztonságával összefüggő feladatok ellátására egynél több nemzeti illetékes hatóságot jelöljenek ki.

(31) A határokon átnyúló együttműködés és a kommunikáció elősegítése, valamint ezen irányelv eredményes végrehajtása érdekében szükség van arra, hogy minden egyes tagállam – az ágazati szabályozási intézkedések sérelme nélkül – kijelöljön egy egyedüli nemzeti kapcsolattartó pontot, amely a hálózati és információs rendszerek biztonságával kapcsolatos kérdések koordinálásáért és az uniós szinten folytatott határokon átnyúló együttműködésért felel. Az illetékes hatóságok és az egyedüli kapcsolattartó pontok számára biztosítani kell a megfelelő műszaki, pénzügyi és emberi erőforrásokat annak érdekében, hogy feladataikat eredményesen és hatékonyan végezhessék el, és hogy ezáltal teljesülhessenek ezen irányelv céljai. Mivel ezen irányelv célja az, hogy bizalomteremtés révén javítsa a belső piac működését, a tagállami szerveknek képesnek kell lenniük eredményesen együttműködni a gazdasági szereplőkkel, és struktúrájukat ennek megfelelően kell kialakítani.

(32) Az illetékes hatóságoknak vagy a számítógép-biztonsági eseményekre reagáló csoportoknak (a továbbiakban: CSIRT) bejelentést kell kapniuk a biztonsági eseményekről. Az egyedüli kapcsolattartó pontoknak nem kell közvetlenül bejelenteni a biztonsági eseményeket, kivéve ha illetékes hatóságként vagy CSIRT-ként is eljárnak. Valamely illetékes hatóság vagy CSIRT azonban megbízhatja az egyedüli kapcsolattartó pontot azzal, hogy továbbítsa az eseményről küldött bejelentést más érintett tagállamok egyedüli kapcsolattartó pontjai részére.

(33) A tagállamok és a Bizottság hatékony tájékoztatásának biztosítása érdekében, az összefoglaló jelentést az egyedüli kapcsolattartó pontnak kell benyújtania az együttműködési csoport részére és azt anonimmá kell tennie a bejelentések bizalmas jellegének megőrzése, valamint az alapvető szolgáltatásokat nyújtó szereplők és digitális szolgáltatók kilétének fel nem fedése érdekében, mivel a bejelentést tevő szervezet kilétére vonatkozó információkra nincs szükség a legjobb gyakorlatoknak az együttműködési csoport keretében történő cseréjéhez. Az összefoglaló jelentésnek tartalmaznia kell a kézhez kapott bejelentések számára vonatkozó adatokat, valamint ismertetnie kell a bejelentett biztonsági események jellegét, például a biztonsági szabályok megsértésének típusát, súlyosságát vagy időtartamát.

(34) A tagállamoknak rendelkezniük kell a hálózati és információs rendszereket érintő biztonsági események és kockázatok megelőzéséhez, észleléséhez, kezeléséhez és mérsékléséhez szükséges műszaki és szervezeti képességekkel. A tagállamoknak biztosítaniuk kell, hogy jól működő CSIRT-ekkel – más néven hálózatbiztonsági vészhelyzeteket elhárító csoportokkal (a továbbiakban: CERT) – rendelkezzenek, amelyek megfelelnek a biztonsági események és kockázatok kezeléséhez szükséges hatékony és kompatibilis képességek garantálására, valamint az eredményes uniós szintű együttműködés biztosítására vonatkozó alapvető követelményeknek. Annak érdekében, hogy az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók minden típusa élhessen az ilyen képességek és együttműködés nyújtotta előnyökkel, a tagállamoknak biztosítaniuk kell, hogy e szereplők és szolgáltatók minden típusa tekintetében sor kerül egy CSIRT kijelölésére. Tekintettel a kiberbiztonság területén folytatott nemzetközi együttműködés fontosságára, a CSIRT-ek számára lehetővé kell tenni, hogy részt vegyenek nemzetközi együttműködési hálózatokban, az ezzel az irányelvvel létrehozott CSIRT-ek hálózatán túl is.

(35) Mivel a hálózati és információs rendszerek üzemeltetése a legtöbb esetben magánkézben van, a magán- és a közszektor közötti együttműködés alapvetően fontos. Az alapvető szolgáltatásokat nyújtó gazdasági szereplőket és a digitális szolgáltatókat ösztönözni kell, hogy alakítsanak ki a hálózati és információs rendszerek biztonságának garantálására irányuló saját informális együttműködési mechanizmusokat. Az együttműködési csoportot fel kell jogosítani arra, hogy adott esetben meghívjon érintett érdekelt feleket a megbeszélésekre. Az információk és a legjobb gyakorlatok megosztásának hathatós ösztönzése érdekében lényeges annak biztosítása, hogy az e véleménycserékben részt vevő alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók az együttműködésük következtében ne szenvedjenek hátrányt.

(36) Az ENISA-nak szakértői véleményével és tanácsaival, valamint a bevált gyakorlatok cseréjének előmozdításával kell segítenie a tagállamokat és a Bizottságot. Ezen irányelv alkalmazásában a Bizottságnak ki kell kérnie, a tagállamoknak pedig lehetőségükben áll kikérniük az ENISA véleményét. A tagállamok körében való kapacitásépítés és ismeretgyarapítás érdekében az együttműködési csoportnak olyan eszközként kell szolgálnia, amelynek keretében lehetőség nyílik a bevált gyakorlatok cseréjére, a tagállamok képességeinek és felkészültségének megvitatására, valamint arra, hogy a csoport önkéntes alapon támogassa tagjait a nemzeti hálózati és információs rendszerek biztonsági stratégiájának értékelésében, a kapacitásépítésben valamint a hálózati és információs rendszerek biztonsági gyakorlatainak értékelésben.

(37) Adott esetben lehetővé kell tenni a tagállamok számára, hogy ezen irányelv alkalmazása során használhassák a meglévő szervezeti struktúrákat vagy stratégiákat, illetve azokat az említett rendelkezésekhez igazíthassák.

(38) Az együttműködési csoport és az ENISA feladatai kölcsönösen összefüggenek egymással és kiegészítik egymást. Az ENISA-nak segítséget kell nyújtania a létrehozott együttműködési csoport számára feladatai elvégzésében, mégpedig az ENISA-nak az 526/2013/EU európai parlamenti és tanácsi rendeletben ([1]) foglalt céljának megfelelően, miszerint az ENISA segíti az uniós intézményeket, szerveket, hivatalokat és ügynökségeket, valamint a tagállamokat a hálózati- és információs rendszerek biztonsága területén az Unió jelenlegi és jövőbeni jogi aktusai értelmében alkalmazandó jogi és szabályozási követelmények teljesítéséhez szükséges politikák végrehajtásában. Az ENISA-nak mindenekelőtt a saját feladataival egybeeső területeken kell segítséget nyújtania, az 526/2013/EU rendeletben foglaltak szerint; ilyen feladat például a hálózati és információs rendszerek biztonsági stratégiájának elemzése, az uniós hálózati és információs rendszerek biztonsági gyakorlatai megszervezésének és lebonyolításának támogatása, továbbá a tájékoztatással és a képzéssel kapcsolatos információk és bevált gyakorlatok megosztása. Az ENISA-nak emellett részt kell vennie a biztonsági események által kifejtett hatások jelentőségének meghatározását szolgáló ágazatspecifikus kritériumokra vonatkozó iránymutatások kidolgozásában.

([1]) Az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről (HL L 165., 2013.6.18., 41. o.).

(39) A hálózati és információs rendszerek magasabb szintű biztonságának előmozdítása céljából az együttműködési csoportnak adott esetben együtt kell működnie az érintett uniós intézményekkel, szervekkel, hivatalokkal és ügynökségekkel annak érdekében, hogy – a korlátozott hozzáférésű információk cseréjére vonatkozó rendelkezések betartása mellett – meg lehessen egymással osztani a know-how-t és a bevált gyakorlatokat, valamint tanácsot lehessen nyújtani a hálózati és információs rendszerek biztonságának azon szempontjairól, amelyek esetlegesen hatást gyakorolhatnak az említett szervek munkájára. Amennyiben az együttműködési csoport bűnüldözési hatóságokkal folytat együttműködést olyan hálózat- és információbiztonsági kérdések tekintetében, amelyek azok munkájára esetlegesen hatást gyakorolhatnak, tiszteletben kell tartania a meglévő információs csatornákat és hálózatokat.

(40) A biztonsági eseményekre vonatkozó információk egyre értékesebbé válnak mind a lakosság, mind a vállalkozások, mégpedig elsősorban a kis- és középvállalkozások számára. Néhány esetben ezek az információk tagállami weboldalakon keresztül már rendelkezésre állnak az adott ország nyelvén, és a hangsúlyt itt mindenekelőtt a tagállami dimenzióval bíró biztonsági események kapják. Tekintettel arra, hogy a vállalkozásokra egyre inkább jellemző a határokon átnyúló tevékenység, a polgárok pedig egyre többször vesznek igénybe online szolgáltatásokat, a biztonsági eseményekre vonatkozó információkat összesített formában, uniós szinten kell rendelkezésre bocsátani. Ezért célszerű lenne, ha a CSIRT-ek hálózatának titkársága maga is fenntartana egy olyan weboldalt, vagy egy meglévő weboldalon működtetne egy olyan oldalt, ahol a lakosság általános információkhoz juthat az Unióban bekövetkezett főbb biztonsági eseményekről, különös hangsúlyt helyezve a vállalkozások érdekeire és szükségleteire. A CSIRT-ek hálózatában részt vevő számítógép-biztonsági eseményekre reagáló csoportokat javasolt arra ösztönözni, hogy önkéntes alapon rendelkezésre bocsájtsák azokat az információkat, amelyeket közzé kell tenni ezen a weboldalon, amely weboldal nem tartalmazhat bizalmas vagy különleges adatokat.

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

(42) A tagállamok hálózati és információs rendszerek biztonsága vonatkozásában fennálló felkészültségének és együttműködésének teszteléséhez elengedhetetlenek a valós idejű biztonsági események forgatókönyvét szimuláló gyakorlatok. Az ENISA által koordinált és a tagállamok részvételével zajló CyberEurope gyakorlatok hasznos eszközt jelentenek a tesztelésre és azoknak az ajánlásoknak a kidolgozására, amelyek arra vonatkoznak, hogy hosszabb távon miként lehetne uniós szinten javítani a biztonsági események kezelését. Figyelembe véve azt, hogy a tagállamok számára jelenleg nem kötelező sem ilyen gyakorlatok tervezése, sem az azokban való részvétel, a CSIRT-ek hálózatának ezen irányelv szerinti létrehozása lehetővé tenné a tagállamok számára, hogy pontos tervezési és stratégiai döntések alapján részt vegyenek a gyakorlatokban. Az ezen irányelv értelmében létrehozott együttműködési csoportnak kell megvitatnia a gyakorlatokra vonatkozó stratégiai döntéseket, mindenekelőtt de nem kizárólag a gyakorlatok rendszerességét és a forgatókönyvek kialakítását illetően. Az ENISA-nak a megbízatásával összhangban támogatnia kell az unió szintjén zajló gyakorlatok megszervezését és lebonyolítását, mégpedig annak révén, hogy szakértői véleménnyel és tanácsadással segíti az együttműködési csoportot és a CSIRT-ek hálózatát.

(43) A hálózati és információs rendszerek biztonságát érintő problémák globális jellegére való tekintettel szorosabb nemzetközi együttműködésre van szükség a biztonsági előírások és az információcsere továbbfejlesztése, valamint a biztonságot érintő közös globális megközelítés előmozdítása érdekében.

(44) A hálózati és információs rendszerek biztonságának biztosítása nagymértékben az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók felelőssége. Megfelelő szabályozási követelményeken és önkéntes ágazati gyakorlatokon keresztül ösztönözni és fejleszteni kell a – kockázatértékelésre és a felmerülő kockázatok súlyosságának megfelelő biztonsági intézkedések végrehajtására egyaránt kiterjedő – kockázatkezelési kultúrát. Az együttműködési csoport és a CSIRT-ek hálózatának eredményes működése és ezen keresztül a tagállamok hatékony együttműködése szempontjából mindemellett rendkívül fontos a minden kétséget kizáróan egyenlő versenyfeltételek megteremtése.

(45) Ez az irányelv kizárólag azon közigazgatási szervekre alkalmazandó, amelyeket alapvető szolgáltatásokat nyújtó szereplőként azonosítottak. Az ezen irányelv hatálya nem alá nem tartozó közigazgatási szervek hálózati és információs rendszereik esetében ezért a tagállamok felelőssége, hogy gondoskodjanak azok biztonságáról.

(46) A kockázatkezelési intézkedések körébe olyan intézkedések tartoznak, mint a biztonsági események kockázatainak azonosítása, a biztonsági események megelőzése, felderítése és kezelése, valamint hatásaik enyhítése. A hálózati és információs rendszerek biztonsága magában foglalja a tárolt, továbbított és kezelt adatok biztonságát.

(47) Az illetékes hatóságok számára továbbra is biztosítani kell azt a jogot, hogy nemzeti iránymutatásokat fogadjanak el arról, hogy az alapvető szolgáltatást nyújtó szereplőknek milyen körülmények esetén kell bejelenteniük a biztonsági eseményeket.

(48) Az Unióban számos vállalkozás digitális szolgáltatókat vesz igénybe szolgáltatásai nyújtásához. Mivel néhány digitális szolgáltatás fontos forrást jelenthet az azt igénybe vevői számára, így az alapvető szolgáltatást nyújtó szereplők számára is, és mivel ezeknek a felhasználóknak nem állnak mindig rendelkezésükre más elérhető alternatívák, ezt az irányelvet alkalmazni kell az ilyen szolgáltatókra is. Az ezen irányelvben említett digitális szolgáltatástípusok biztonságos volta, folyamatossága és megbízhatósága számos vállalkozás zavartalan működésének nélkülözhetetlen eleme. A felsorolt digitális szolgáltatásokban bekövetkező zavar akadályozhatja más, arra épülő szolgáltatások nyújtását is, és emiatt az Unió egészében hatást gyakorolhat alapvető gazdasági és társadalmi tevékenységekre. Az ilyen digitális szolgáltatások ezért rendkívül fontosak lehetnek a tőlük függő vállalkozások zavartalan működéséhez, sőt, a belső piacon való szereplésükhöz és az Unión belüli határokon átnyúló kereskedelemben való részvételükhöz is. Az ezen irányelv hatálya alá tartozó digitális szolgáltatók alatt azokat a szolgáltatókat kell érteni, akik olyan digitális szolgáltatásokat kínálnak, amelyeket az Unióban működő vállalkozások egyre nagyobb mértékben igénybe vesznek.

(49) Figyelemmel arra, hogy a digitális szolgáltatók szolgáltatásai mennyire fontosak az Unión belüli más vállalkozások működéséhez, a digitális szolgáltatóknak olyan biztonsági szintről kell gondoskodniuk, amely arányos az általuk nyújtott digitális szolgáltatás biztonságát érintő kockázatok mértékével. A gyakorlatban a kritikus társadalmi és gazdasági tevékenységek fenntartásához gyakran elengedhetetlen alapvető szolgáltatásokat nyújtó szereplők tekintetében jelentkező kockázatok mértéke magasabb, mint a digitális szolgáltatók esetében. A digitális szolgáltatókra vonatkozó biztonsági követelményeknek ezért enyhébbeknek kell lenniük. A digitális szolgáltatók számára továbbra is lehetővé kell tenni, hogy meghozzák azokat az intézkedéseket, amelyeket megfelelőnek ítélnek a hálózati és információs rendszereik biztonságát érintő kockázatok kezelésére. Tevékenységeik határokon átnyúló jellege miatt a digitális szolgáltatókra uniós szinten egy harmonizáltabb megközelítést kell alkalmazni. A vonatkozó intézkedések meghatározását és végrehajtását végrehajtási jogi aktusok útján kell könnyebbé tenni.

(50) Bár a hardvergyártók és a szoftverfejlesztők nem minősülnek alapvető szolgáltatást nyújtó szereplőknek vagy digitális szolgáltatóknak, termékeik fokozzák a hálózati és információs rendszerek biztonságát. Emiatt fontos szerepet játszanak, hiszen lehetővé teszik az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók számára, hogy biztonságossá tegyék hálózati és információs rendszereiket. Az említett hardver- és szoftvertermékekre a termékfelelősségre vonatkozó hatályos szabályok vonatkoznak.

(51) Az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra vonatkozó műszaki és szervezeti intézkedések nem követelhetik meg, hogy egy adott információ- vagy kommunikációtechnológiai kereskedelmi termék tervezése, kialakítása vagy előállítása valamely meghatározott módon történjék.

(52) Az alapvető szolgáltatásokat nyújtó szereplőknek és a digitális szolgáltatóknak gondoskodniuk kell az általuk használt hálózati és információs rendszerek biztonságáról. Ezek elsősorban olyan magánkézben lévő hálózati és információs rendszerek, amelyek kezelését saját informatikus munkatársak végzik, illetve amelyek biztonsági karbantartását kiszervezték. A biztonsági és jelentéstételi követelményeket alkalmazni kell az alapvető szolgáltatásokat nyújtó érintett gazdasági szereplőkre és az érintett digitális szolgáltatókra, függetlenül attól, hogy saját maguk végzik vagy kiszervezik hálózati és információs rendszereik karbantartását.

(53) Annak elkerülése érdekében, hogy az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra aránytalanul nagy pénzügyi és adminisztratív terhek háruljanak, a követelményeknek – a legújabb technikai lehetőségekre figyelemmel – arányosaknak kell lenniük az adott hálózati és információs rendszert érintő kockázatokkal. Digitális szolgáltatók esetében az említett követelmények a mikro- és kisvállalkozásokra nem alkalmazandók.

(54) Amennyiben a tagállami közigazgatási szervek digitális szolgáltatók által kínált szolgáltatásokat, különösen felhőlapú számítástechnikai szolgáltatásokat vesznek igénybe, a szolgáltatótól kérhetik kiegészítő – a digitális szolgáltatók által az ezen irányelv követelményeinek való megfelelés céljából kínált intézkedéseken túlmutató – biztonsági intézkedések meghozatalát. Erre az említett közigazgatási szerveknek szerződéses kötelezettségek útján nyílhat lehetősége.

(55) Az online piactér, az online keresőprogram és a felhőlapú számítástechnikai szolgáltatás fogalmának ezen irányelvben foglalt meghatározása ezen irányelv alkalmazásában érvényes, és nem érint semmilyen más jogi eszközt.

(56) Ez az irányelv nem gátolja a tagállamokat abban, hogy nemzeti szintű intézkedéseket fogadjanak el, amelyek arra kötelezik a közigazgatási szerveket, hogy felhőlapú számítástechnikai szolgáltatásokra vonatkozó szerződések megkötése esetén konkrét biztonsági követelmények érvényesítéséről gondoskodjanak. Minden ilyen nemzeti intézkedésnek az érintett közigazgatási szervre kell vonatkoznia, nem pedig a felhőlapú számítástechnikai szolgáltatást nyújtó szolgáltatóra.

(57) Szem előtt tartva azokat a jelentős különbségeket, amelyek egyrészről az alapvető szolgáltatásokat nyújtó szereplők között állnak fenn különösen a fizikai infrastruktúrához való közvetlen kapcsolódásuk tekintetében, másrészről pedig a digitális szolgáltatók között különösen a határokon átnyúló jellegük tekintetében, ez az irányelv e két csoport esetében differenciált megközelítést alkalmaz a harmonizáció szintjét illetően. Az alapvető szolgáltatásokat nyújtó szereplők vonatkozásában a tagállamoknak képesnek kell lenniük mind az érintett szereplők azonosítására, mind pedig arra, hogy az ezen irányelvben foglalt követelményeknél szigorúbb követelményeket állapítsanak meg e szereplők számára. A tagállamoknak a digitális szolgáltatókat nem kell azonosítaniuk, mivel ezt az irányelvet a hatálya alá tartozó minden digitális szolgáltatóra alkalmazni kell. Ezen túlmenően ennek az irányelvnek – csakúgy, mint az értelmében elfogadott valamennyi végrehajtási jogi aktusnak – a digitális szolgáltatók esetében biztosítania kell a biztonsági és bejelentési követelmények magas szintű harmonizációját. Mindennek lehetővé kell tennie az Unió egészében a digitális szolgáltatók egységes kezelését, a jellegükkel és az őket esetlegesen érintő kockázatok mértékével arányos módon.

(58) Ez az irányelv nem gátolja a tagállamokat abban, hogy az uniós jog szerinti kötelezettségeik sérelme nélkül biztonsági és bejelentési követelményeket állapítsanak meg azon szervekre vonatkozóan, amelyek nem minősülnek az e rendelet hatálya szerinti digitális szolgáltatónak.

(59) Az illetékes hatóságoknak kellő figyelmet kell fordítaniuk az informális és bizalmi információmegosztási csatornák megőrzésére. Az illetékes hatóságok felé bejelentett biztonsági események nyilvánosságra hozatala tekintetében két dolgot kell kellően mérlegelni: egyrészt azt, hogy milyen előnyök származnak abból, ha a nyilvánosságot tájékoztatják a fenyegetésekről, másrészt pedig azt, hogy a nyilvánosságra hozatal esetlegesen milyen károkat okozhat a biztonsági eseményeket bejelentő, alapvető szolgáltatásokat nyújtó szereplők és digitális szolgáltatók hírneve és kereskedelmi tevékenysége szempontjából. A bejelentési kötelezettségek teljesítése során az illetékes hatóságoknak és a CSIRT-eknek külön figyelmet kell fordítaniuk arra, hogy a megfelelő biztonsági korrekciós intézkedések meghozataláig a termékek gyenge pontjai szigorúan titokban maradjanak.

(60) A digitális szolgáltatókra az általuk nyújtott szolgáltatások és az általuk végzett tevékenységek jellege okán kevésbé szigorú és reaktív utólagos felügyeleti tevékenységnek kell vonatkoznia. Az érintett illetékes hatóságnak ezért csak akkor – különösen egy biztonsági esemény bekövetkeztét követően – kell lépéseket tennie, ha minden kétséget kizáróan tudomást szerez arról, például magától a digitális szolgáltatótól, egy másik – akár egy másik tagállami – illetékes hatóságtól, vagy a szolgáltatás igénybevevőjétől, hogy a digitális szolgáltató nem felel meg ezen irányelv követelményeinek. A digitális szolgáltatók felügyeletét ezért nem kell az illetékes hatóság számára általános kötelezettségként előírni.

(61) Az illetékes hatóságoknak rendelkezniük kell a feladataik teljesítéséhez szükséges eszközökkel, beleértve azt a hatáskört is, hogy megszerezzék a hálózati és információs rendszerek biztonsági szintjének értékeléséhez szükséges megfelelő mennyiségű információt.

(62) A biztonsági események hátterében bűncselekmények is állhatnak, ezek megelőzését, kivizsgálását és büntetőeljárás alá vonását elősegíti, ha az alapvető szolgáltatásokat nyújtó szereplők, a digitális szolgáltatók, az illetékes hatóságok és a bűnüldöző hatóságok koordinálják tevékenységeiket és együttműködnek egymással. Amennyiben egy biztonsági esemény gyaníthatóan uniós vagy nemzeti jog szerinti súlyos bűncselekményekhez köthető, a tagállamoknak arra kell ösztönözniük az alapvető szolgáltatásokat nyújtó szereplőket és a digitális szolgáltatókat, hogy a gyaníthatóan súlyos bűncselekmény jellegét öltő biztonsági eseményt jelentsék az érintett bűnüldöző hatóságok felé. Adott esetben ajánlott, hogy a Számítástechnikai Bűnözés Elleni Európai Központ és az ENISA elősegítse a különböző tagállamokban működő illetékes hatóságok és bűnüldöző hatóságok közötti koordinációt.

(63) 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 egymással minden vonatkozó kérdésről, hogy fel lehessen venni a küzdelmet a személyes adatok biztonsági eseményekből eredő bármely megsértése ellen.

(64) A digitális szolgáltatónak azon tagállam joghatósága alá kell tartoznia, amelyben az érintett digitális szolgáltatónak az Unióban a központi ügyvezetés helye található, és amely elvben megegyezik az Unión belüli székhelyével. A letelepedés valamely tevékenység tényleges és valós, tartós jelleget biztosító keretek közötti gyakorlását feltételezi. E keretek jogi formája – legyen szó akár fiókteleprő vagy jogi személyiséggel rendelkező leányvállalatról – e tekintetben nem meghatározó tényező. Ez a kritérium nem függhet attól, hogy a hálózati és

információs rendszerek fizikailag egy adott helyen találhatók-e; e rendszerek tényleges jelenléte és használata önmagában nem hoz létre központi ügyvezetési helyet, ezért nem is alkalmazható kritériumként a központi ügyvezetés helyének meghatározásához.

(65) Annak a digitális szolgáltatónak, amely szolgáltatásait az Unión belül kínálja, de az Unióban nincs letelepedve, képviselőt kell kineveznie. Annak megállapítása érdekében, hogy az ilyen digitális szolgáltató az Unión belül kínálja-e szolgáltatásait, meg kell bizonyosodni arról, hogy nyilvánvaló-e, hogy a digitális szolgáltatónak szándékában áll szolgáltatásokat nyújtani személyek számára egy vagy több tagállamban. Nem tekintendő e szándék nyilvánvaló jelének annak a puszta ténye, hogy a digitális szolgáltató vagy valamely közvetítő honlapja, e-mail címe vagy más elérhetősége hozzáférhető az Unióban, sem pedig a digitális szolgáltató letelepedési helye szerinti harmadik országban általánosan használt nyelv használata. Ha viszont például a digitális szolgáltató olyan nyelvet vagy pénznemet használ, amely egy vagy több tagállamban is általánosan használatos, és így lehetőséget biztosít szolgáltatásoknak az említett másik nyelven történő megrendelésére, vagy unióbeli fogyasztókra vagy felhasználókra tesz utalást, az egyértelműen jelezheti, hogy a digitális szolgáltató szolgáltatásokat szándékozik kínálni az Unión belül. A képviselőnek a digitális szolgáltató nevében kell eljárnia, az illetékes hatóságoknak vagy a CSIRT-nek pedig lehetősége kell hogy legyen arra, hogy felvegye a kapcsolatot a képviselővel. A digitális szolgáltatónak írásban kell felhatalmaznia a képviselőt arra, hogy a nevében eljárjon az ezen irányelv szerinti kötelezettségei vonatkozásában, ideértve a biztonsági események bejelentését is.

(66) A biztonsági követelmények szabványosítása piacvezérelt folyamat. A biztonsági szabványok egymáshoz közelítő alkalmazásának biztosítása érdekében a tagállamoknak ösztönözniük kell a meghatározott szabványoknak való megfelelést, hogy ezzel uniós szinten is érvényesüljön a hálózati és információs rendszerek magas szintű biztonsága. Az ENISA-nak e kérdésben tanácsadással és iránymutatásokkal kell segítenie a tagállamokat. E célból hasznos lehet harmonizált szabványok kidolgozása, amit az 1025/2012/EU európai parlamenti és tanácsi rendelettel ([1]) összhangban kell végezni.

(67) Az ezen irányelv hatályán kívül eső szervezetek is szembesülhetnek olyan biztonsági eseményekkel, amelyek jelentős hatást gyakorolnak az általuk nyújtott szolgáltatásokra. Lehetővé kell tenni, hogy amennyiben ezek a szervezetek úgy vélik, hogy közérdeket szolgál az ilyen események bejelentése, azt önkéntes alapon megtehessék. A bejelentéseket az illetékes hatóságoknak vagy a CSIRT-nek kell feldolgozniuk, ha az nem jelent aránytalan vagy indokolatlan terhet az érintett tagállamok számára.

(68) Ezen irányelv egységes feltételek mellett történő végrehajtásának biztosítása érdekében a Bizottságot végrehajtási hatáskörökkel kell felruházni annak érdekében, hogy meghatározza az együttműködési csoport működéséhez szükséges eljárásrendet, valamint a digitális szolgáltatókra alkalmazandó biztonsági és bejelentési követelményeket. Ezt a hatáskört a 182/2011/EU európai parlamenti és tanácsi rendeletnek ([2]) megfelelően kell gyakorolni. Az együttműködési csoport működéséhez szükséges eljárásrendre vonatkozó végrehajtási jogi aktusok elfogadásakor a Bizottságnak a lehető legnagyobb mértékben figyelembe kell vennie az ENISA véleményét.

(69) A digitális szolgáltatókra alkalmazandó biztonsági és bejelentési követelményekre vonatkozó végrehajtási jogi aktusok elfogadásakor a Bizottságnak a lehető legnagyobb mértékben figyelembe kell vennie az ENISA véleményét, és konzultálnia kell az érdekelt felekkel. Emellett ajánlott, hogy a a Bizottság vegye figyelembe a következőket: a rendszerek és létesítmények biztonsága tekintetében: fizikai és környezeti biztonság, az ellátás biztonsága, a hálózati és információs rendszerek integritása és az e rendszerekhez való hozzáférés ellenőrzése; a biztonsági események kezelése tekintetében: a biztonsági esemény kezelésére szolgáló eljárások, a biztonsági esemény észlelésének képessége, a biztonsági esemény bejelentése és az eseményről való tájékoztatás; az üzletmenetfolytonosság-menedzsment tekintetében: a szolgáltatások folytonosságát szolgáló stratégiai és vészhelyzeti tervek, katasztrófaelhárítási képességek; a monitoring, az audit és a tesztelés tekintetében: a monitoringra és a naplózásra vonatkozó előírások, a vészhelyzeti tervek gyakorlása, a hálózati és információs rendszerek tesztelése, biztonsági értékelések és a megfelelés monitoringja.

(70) Ezen irányelv végrehajtása során a Bizottságnak megfelelő kapcsolatot kell fenntartania az érintett ágazati bizottságokkal és az irányelv hatálya alá tartozó területeken uniós szinten létrehozott érintett szervekkel.

([1]) Az Európai Parlament és a Tanács 1025/2012/EU rendelete (2012. október 25.) 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 (HL L 316., 2012.11.14., 12. o.).

([2]) Az Európai Parlament és a Tanács 182/2011/EU rendelete (2011. február 16.) a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról (HL L 55., 2011.2.28., 13. o.).

(71) A Bizottságnak ezen irányelv rendelkezéseit – az érdekelt felekkel egyeztetve – időszakonként felül kell vizsgálnia, különösen annak megállapítása céljából, hogy a társadalmi, politikai, technológiai és piaci feltételek változásai tükrében szükség van-e az irányelv módosítására.

(72) A kockázatokkal és a biztonsági eseményekkel kapcsolatos információknak az együttműködési csoportokon és a CSIRT-ek hálózatán keresztül történő megosztása, valamint a biztonsági eseményeknek a nemzeti illetékes hatóságok vagy a CSIRT-ek számára történő bejelentésére vonatkozó követelményeknek való megfelelés személyes adatok kezelését teheti szükségessé. Az ilyen adatkezelésnek meg kell felelnie a 95/46/EK európai parlamenti és tanácsi irányelvben ([1]) és a 45/2001/EK európai parlamenti és tanácsi rendeletben ([2]) foglaltaknak. Ezen irányelv alkalmazásakor adott esetben alkalmazni kell az 1049/2001/EK európai parlamenti és tanácsi rendeletet ([3]).

(73) Az európai adatvédelmi biztossal való konzultáció a 45/2001/EK rendelet 28. cikkének (2) bekezdésével összhangban megtörtént, a biztos 2013. június 14-én nyilvánított véleményt ([4]).

(74) Mivel e rendelet célját, nevezetesen a hálózati és információs rendszerek egységesen magas szintű biztonságának uniós megvalósítását a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban az intézkedés hatása miatt e cél jobban megvalósítható, az Unió intézkedéseket hozhat az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritás elvének megfelelően. Az említett cikkben foglalt arányosság elvének megfelelően ez az irányelv nem lépi túl az említett cél eléréséhez szükséges mértéket.

(75) Ez az irányelv tiszteletben tartja az Európai Unió Alapjogi Chartája által elismert alapvető jogokat és szem előtt tartja az abban rögzített elveket, különösen a magánélet és a kapcsolattartás tiszteletben tartásához való jogot, a személyes adatok védelméhez való jogot, a vállalkozás szabadságát, a tulajdonhoz való jogot, a bíróság előtti hatékony jogorvoslathoz való jogot és a meghallgatáshoz való jogot. Ezen irányelvet az említett elvekkel és jogokkal összhangban kell végrehajtani,

ELFOGADTA EZT AZ IRÁNYELVET:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy és hatály

(1) Ez az irányelv a belső piac működésének javítása érdekében intézkedéseket állapít meg a hálózati és információs rendszerek egységesen magas szintű biztonságának az Unión belüli megvalósítása céljából.

(2) Ennek érdekében ez az irányelv:

a) valamennyi tagállam számára kötelezettségeket állapít meg a hálózati és információs rendszerek biztonsága nemzeti stratégiájának elfogadására vonatkozóan;

b) létrehoz egy együttműködési csoportot a tagállamok közötti stratégiai együttműködés és információcsere támogatása és elősegítése, valamint a közöttük lévő bizalom erősítése céljából;

c) létrehozza a számítógép-biztonsági eseményekre reagáló csoportok hálózatát (a továbbiakban: CSIRT-ek hálózata) a tagállamok közötti bizalom erősítéséhez való hozzájárulás, valamint a gyors és hatékony operatív együttműködés előmozdítása céljából;

([1]) Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (HL L 281., 1995.11.23., 31. o.).
([2]) Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról (HL L 8., 2001.1.12., 1. o.).
([3]) Az Európai Parlament és a Tanács 1049/2001/EK rendelete (2001. május 30.) az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről (HL L 145., 2001.5.31., 43. o.).
([4]) HL C 32., 2014.2.4., 19. o.

d) biztonsági és bejelentési követelményeket állapít meg az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók számára;

e) a tagállamok számára kötelezettségeket állapít meg arra vonatkozóan, hogy a hálózati és információs rendszerek biztonságával kapcsolatos feladatok ellátására jelöljenek ki nemzeti illetékes hatóságokat, egyedüli kapcsolattartó pontokat, valamint CSIRT-eket.

(3) Az ezen irányelvben megállapított biztonsági és bejelentési követelmények nem alkalmazandók a 2002/21/EK irányelv 13a. és 13b. cikkében foglalt követelmények hatálya alá tartozó vállalkozásokra és a 910/2014/EU rendelet 19. cikkében foglalt követelmények hatálya alá tartozó bizalmi szolgáltatókra.

(4) Ez az irányelv nem érinti a 2008/114/EK tanácsi irányelvet ([1]), a 2011/93/EU ([2]) és a 2013/40/EU európai parlamenti és tanácsi irányelvet ([3]).

(5) Az EUMSZ 346. cikkének sérelme nélkül, az uniós és a nemzeti szabályok – például az üzleti titokra vonatkozó szabályok – értelmében bizalmasnak minősülő információkat csak abban az esetben kell a Bizottság és más érintett illetékes hatóságok rendelkezésére bocsátani, ha az ilyen információcsere ezen irányelv alkalmazásához szükséges. A kicserélt információknak az említett információcsere célja szempontjából lényeges és azzal arányos információkra kell korlátozódniuk. Az ilyen információcsere során meg kell őrizni a szolgáltatott információk bizalmas jellegét, és óvni kell az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók biztonsági és kereskedelmi érdekeit.

(6) Ez az irányelv nem érinti azokat az intézkedéseket, amelyeket a tagállamok az alapvető állami funkcióik védelme, és különösen a nemzetbiztonság védelme érdekében hoznak, ideértve az olyan információk védelmét szolgáló intézkedéseket is, amelyek közlését a tagállamok ellentétesnek tartják alapvető biztonsági érdekeikkel, továbbá a közrend fenntartása, és különösen a bűncselekmények kivizsgálásának, felderítésének és büntetőeljárás alá vonásának lehetővé tétele érdekében hozott intézkedéseiket.

(7) Amennyiben valamely ágazatspecifikus uniós jogi aktus előírja az alapvető szolgáltatásokat nyújtó szereplők vagy a digitális szolgáltatók számára, hogy gondoskodjanak hálózataik és információs rendszereik biztonságáról vagy hogy jelentsék be a biztonsági eseményeket – feltéve, hogy e követelményekkel legalább olyan hatás érhető el, mint az ezen irányelvben előírt kötelezettségekkel –, akkor az említett ágazatspecifikus uniós jogi aktus rendelkezéseit kell alkalmazni.

2. cikk

A személyes adatok kezelése

(1) A személyes adatoknak az ezen irányelv szerinti kezelését a 95/46/EK irányelvvel összhangban kell végezni.

(2) A személyes adatoknak az uniós intézmények és szervek által történő, ezen irányelv szerinti kezelését a 45/2001/EK rendelettel összhangban kell végezni.

3. cikk

Minimális harmonizáció

A 16. cikk (10) bekezdésének és az uniós jog szerinti kötelezettségeiknek a sérelme nélkül, a tagállamok a hálózati és információs rendszerek magasabb szintű biztonságának megvalósítása érdekében rendelkezéseket fogadhatnak el vagy tarthatnak fenn.

([1]) A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (HL L 345., 2008.12.23., 75. o.).

([2]) Az Európai Parlament és a Tanács 2011/93/EU irányelve (2011. december 13.) a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról (HL L 335., 2011.12.17., 1. o.).

([3]) Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról (HL L 218., 2013.8.14., 8. o.).

4. cikk

Fogalommeghatározások

Ezen irányelv alkalmazásában:

1. „hálózati és információs rendszer”:

   a) a 2002/21/EK irányelv 2. cikkének a) pontja szerinti elektronikus hírközlő hálózat;

   b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy

   c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

2. „hálózati és információs rendszerek biztonsága”: a hálózati és információs rendszer arra való képessége, hogy adott bizonyossággal ellenálljon az olyan cselekményeknek, amelyek veszélyeztetik a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszeren nyújtott vagy rajta keresztül elérhető kapcsolódó szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét és bizalmasságát;

3. „hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia”: olyan keret, amelyben a hálózati és információs rendszerek biztonságára vonatkozóan nemzeti szinten stratégiai célkitűzéseket és prioritásokat állapítanak meg;

4. „alapvető szolgáltatásokat nyújtó szereplő”: a II. mellékletben említett típusú olyan közjogi vagy magánjogi szervezet, amely megfelel a 5. cikk (2) bekezdésében meghatározott kritériumoknak;

5. „digitális szolgáltatás”: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv ([1]) 1. cikke (1) bekezdésének b) pontja szerinti, a III. mellékletben felsorolt típusok valamelyiknek megfelelő szolgáltatás;

6. „digitális szolgáltató”: minden olyan jogi személy, amely digitális szolgáltatást nyújt;

7. „biztonsági esemény”: minden olyan esemény, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára;

8. „biztonsági esemény kezelése”: a biztonsági események észlelését, elemzését és elszigetelését, valamint a rájuk való reagálást támogató eljárások;

9. „kockázat”: minden olyan észszerűen azonosítható körülmény vagy esemény, amely kedvezőtlen hatást gyakorolhat a hálózati és információs rendszerek biztonságára;

10. „képviselő”: az Unióban letelepedett minden olyan természetes vagy jogi személy, akit vagy amelyet kifejezetten kijelöltek arra, hogy az Unióban nem letelepedett digitális szolgáltató nevében eljárjon, és akihez vagy amelyhez az illetékes nemzeti hatóság vagy a CSIRT a digitális szolgáltató ezen irányelv szerinti kötelezettségeit illetően az adott digitális szolgáltató helyett fordulhat;

11. „szabvány”: az 1025/2012/EU rendelet 2. cikkének 1. pontja szerinti szabvány;

12. „előírás”: az 1025/2012/EU rendelet 2. cikkének 4. pontja szerinti műszaki előírás;

13. „internetes exchange pont (IXP)”: olyan hálózati létesítmény, amely elsősorban az internetes forgalomcsere megkönnyítése érdekében lehetővé teszi kettőnél több, egymástól független, autonóm rendszer összekapcsolását; az IXP kizárólag autonóm rendszerek részére biztosít összekapcsolást; az IXP nem kívánja meg, hogy a részt vevő bármely két autonóm rendszer között zajló internetes forgalom egy bármely harmadik autonóm rendszeren is áthaladjon, továbbá nem változtatja meg az említett forgalmat és egyéb módon sem avatkozik be abba;

14. „doménnévrendszer (DNS)”: olyan hierarchikusan felépülő elnevezési rendszer, amely a hálózatban doménnév lekérdezéseket szolgál ki;

([1]) Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve (2015. szeptember 9.) a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról (HL L 241., 2015.9.17., 1. o.).

15. „DNS-szolgáltató”: olyan szervezet, amely DNS-szolgáltatásokat nyújt az interneten;

16. „legfelső szintű doménnév-nyilvántartó”: olyan szervezet, amely egy konkrét legfelső szintű domén (TLD) alatti internetes doménnevek regisztrációját irányítja és működteti;

17. „online piactér”: olyan digitális szolgáltatás, amely a 2013/11/EU európai parlamenti és tanácsi irányelv ([1]) 4. cikke (1) bekezdésének a) és b) pontjában meghatározott fogyasztók és/vagy kereskedők számára lehetővé teszi, hogy az online piactér weboldalán vagy valamely kereskedőnek az online piactér által nyújtott számítástechnikai szolgáltatásokat felhasználó weboldalán keresztül online adásvételi vagy szolgáltatási szerződéseket kössenek;

18. „online keresőprogram”: olyan digitális szolgáltatás, amelynek segítségével a felhasználók elvben valamennyi weboldalon, illetve konkrét nyelvű weboldalakon kulcsszó, kifejezés vagy egyéb formában megadott lekérdezés alapján bármilyen témában kereséseket végezhetnek, és amely ennek eredményeként olyan hivatkozásokat ad meg, ahol a keresett tartalommal kapcsolatos információk találhatók;

19. „felhőlapú számítástechnikai szolgáltatás”: olyan digitális szolgáltatás, amely megosztható számítástechnikai erőforrások méretezhető és rugalmas pooljához enged hozzáférést.

5. cikk

Az alapvető szolgáltatásokat nyújtó szereplők azonosítása

(1) A tagállamok 2018. november 9-ig a II. mellékletben említett valamennyi ágazat és alágazat vonatkozásában azonosítják a területükön letelepedett, alapvető szolgáltatásokat nyújtó szereplőket.

(2) A 4. cikk 4. pontjában említett alapvető szolgáltatásokat nyújtó szereplők azonosítására vonatkozó kritériumok a következők:

a) a szervezet a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt;

b) az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ; és

c) az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában.

(3) Az (1) bekezdés alkalmazása céljából mindegyik tagállam összeállítja a (2) bekezdés a) pontjában említett szolgáltatások jegyzékét.

(4) Az (1) bekezdés alkalmazása céljából, amennyiben valamely szervezet két vagy több tagállamban nyújtja a (2) bekezdés a) pontjában említett szolgáltatást, az említett tagállamok egyeztetnek egymással. Az egyeztetésre az azonosításról szóló döntés meghozatala előtt kell sort keríteni.

(5) A tagállamok rendszeresen, illetve 2018. május 9-ét követően legalább kétévente felülvizsgálják és adott esetben aktualizálják az azonosított, alapvető szolgáltatásokat nyújtó szereplők jegyzékét.

(6) Az együttműködési csoport a 11. cikkben említett feladatokkal összhangban támogatást nyújt a tagállamoknak ahhoz, hogy az alapvető szolgáltatásokat nyújtó szereplők azonosítási eljárásában egységes megközelítést alkalmazzanak.

(7) A tagállamok a 23. cikkben említett felülvizsgálat céljából 2018. november 9-ig, azután pedig kétévente megküldik a Bizottságnak azokat az információkat, amelyek szükségesek ahhoz, hogy a Bizottság értékelhesse ezen irányelv végrehajtását különösen az alapvető szolgáltatásokat nyújtó szereplők azonosításakor a tagállamok általi megközelítés egységessége tekintetében. Az említett információknak legalább a következőkre kell kiterjedniük:

a) az alapvető szolgáltatásokat nyújtó szereplők azonosítását lehetővé tevő nemzeti intézkedések;

([1]) Az Európai Parlament és a Tanács 2013/11/EU irányelve (2013. május 21.) a fogyasztói jogviták alternatív rendezéséről, valamint a 2006/2004/EK rendelet és a 2009/22/EK irányelv módosításáról (fogyasztói alternatív vitarendezési irányelv) (HL L 165., 2013.6.18., 63. o.).

b) a (3) bekezdésben említett szolgáltatások jegyzéke;

c) a II. mellékletben felsorolt egyes ágazatokban azonosított, alapvető szolgáltatásokat nyújtó szereplők száma, és annak feltüntetése, hogy az adott ágazat szempontjából mekkora a jelentőségük;

d) küszöbértékek – ha vannak – az adott szolgáltatásra támaszkodó felhasználók 6. cikk (1) bekezdésének a) pontjában említett száma vagy az alapvető szolgáltatásokat nyújtó konkrét gazdasági szereplő 6. cikk (1) bekezdésének f) pontjában említett jelentősége alapján történő releváns ellátási szint meghatározásához.

Annak elősegítése érdekében, hogy a szolgáltatott információk összehasonlíthatók legyenek, a Bizottság – a lehető legnagyobb mértékben figyelembe véve az ENISA véleményét – megfelelő technikai iránymutatásokat fogadhat el az e bekezdésben említett információk paramétereire vonatkozóan.

6. cikk

Jelentős zavar

(1) Az 5. cikk (2) bekezdésének c) pontjában említett zavar jelentőségének meghatározásához a tagállamok legalább a következő ágazatközi tényezőket veszik figyelembe:

a) az érintett szervezet által nyújtott szolgáltatásra támaszkodó felhasználók száma;

b) a II. mellékletben említett más ágazatok függése az említett szervezet által nyújtott szolgáltatástól;

c) az, hogy a biztonsági események – mértéküket és időtartamukat tekintve – milyen hatást gyakorolnának a gazdasági és társadalmi tevékenységekre vagy a közbiztonságra;

d) az említett szervezet piaci részesedése;

e) az adott biztonsági esemény által esetlegesen érintett terület földrajzi kiterjedése;

f) az, hogy a szervezetnek mekkora jelentősége van a szolgáltatás elégséges szintjének fenntartásában, figyelembe véve az adott szolgáltatás nyújtásához rendelkezésre álló egyéb lehetőségeket is.

(2) A tagállamok annak meghatározásához, hogy az adott biztonsági esemény jelentős zavart okozna-e, adott esetben ágazatspecifikus tényezőket is figyelembe vesznek.

II. FEJEZET

A HÁLÓZATI ÉS INFORMÁCIÓS RENDSZEREK BIZTONSÁGÁRA VONATKOZÓ NEMZETI KERETEK

7. cikk

A hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia

(1) Valamennyi tagállam elfogad egy hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiát, amelyben meghatározza a stratégiai célokat, valamint a hálózati és információs rendszerek magas szintű biztonságának megteremtéséhez és fenntartásához szükséges megfelelő szakpolitikai és szabályozási intézkedéseket, legalább a II. mellékletben említett ágazatokra és a III. mellékletben említett szolgáltatásokra vonatkozóan. A hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia különösen a következő témákkal foglalkozik:

a) a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia céljai és prioritásai;

b) a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia céljainak és prioritásainak teljesítését szolgáló irányítási keretrendszer, ideértve a kormányzati szervek és egyéb érintett szereplők szerepkörét és felelősségét is;

c) a felkészültségre, a reagálásra és a helyreállításra vonatkozó intézkedések azonosítása, ideértve a köz- és a magánszféra közötti együttműködést is;

d) a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiához kapcsolódó oktatási, tájékoztató és képzési programok megjelölése;

e) a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiához kapcsolódó kutatási és fejlesztési tervek megjelölése;

f) a kockázatok feltárására szolgáló kockázatértékelési terv;

g) a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia végrehajtásába bevont különböző szereplők jegyzéke.

(2) A tagállamok az ENISA segítségét kérhetik a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia kidolgozásához.

(3) A tagállamoknak a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiájukat az elfogadásuktól számított három hónapon belül meg kell küldeniük a Bizottságnak. E tájékoztatásból a tagállamok kihagyhatják a stratégia nemzetbiztonsággal kapcsolatos elemeit.

8. cikk

Nemzeti illetékes hatóságok és egyedüli kapcsolattartó pont

(1) Minden tagállam kijelöl egy vagy több, a hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes hatóságot (a továbbiakban: illetékes hatóság), legalább a II. mellékletben említett ágazatokra és a III. mellékletben említett szolgáltatásokra vonatkozóan. A tagállamok már létező hatóságot vagy hatóságokat is megbízhatnak ezzel a feladattal.

(2) Az illetékes hatóságoknak tagállami szinten kell monitoringozniuk ezen irányelv alkalmazását.

(3) Minden tagállam kijelöl egy, a hálózati és információs rendszerek biztonságáért felelős nemzeti egyedüli kapcsolattartó pontot (a továbbiakban: egyedüli kapcsolattartó pont). A tagállamok egy már létező hatóságot is megbízhatnak ezzel a feladattal. Amennyiben valamely tagállam csak egy illetékes hatóságot jelöl ki, ez az illetékes hatóság lesz egyúttal az egyedüli kapcsolattartó pont is.

(4) Az egyedüli kapcsolattartó pontnak kell ellátnia az összekötő feladatokat a tagállami hatóságok közötti és a többi tagállam érintett hatóságaival folytatott, határokon átnyúló együttműködés, valamint a 11. cikkben említett együttműködési csoporttal és a 12. cikkben említett CSIRT-ek hálózatával folytatott együttműködés biztosítása céljából.

(5) A tagállamok biztosítják, hogy az illetékes hatóságok és az egyedüli kapcsolattartó pontok elegendő erőforrással rendelkeznek a rájuk bízott feladatok hatékony és eredményes ellátásához és ezáltal ezen irányelv célkitűzéseinek teljesítéséhez. A tagállamok biztosítják, hogy a kijelölt képviselők hatékonyan, eredményesen és biztonságosan működnek együtt az együttműködési csoportban.

(6) Az illetékes hatóságok és az egyedüli kapcsolattartó pont szükség szerint és a nemzeti joggal összhangban konzultál és együttműködik az érintett nemzeti bűnüldöző hatóságokkal és a nemzeti adatvédelmi hatóságokkal.

(7) Minden tagállam késedelem nélkül tájékoztatja a Bizottságot az illetékes hatóság és az egyedüli kapcsolattartó pont kijelöléséről, feladataikról és bármilyen ezekhez kapcsolódó későbbi változásról. Minden tagállam közzéteszi, hogy mely illetékes hatóságot és egyedüli kapcsolattartó pontot jelölte ki. A Bizottság közzéteszi a kijelölt egyedüli kapcsolattartó pontok jegyzékét.

9. cikk

Számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek)

(1) Minden tagállam – legalább a II. mellékletben említett ágazatokra és a III. mellékletben említett szolgáltatásokra vonatkozóan – kijelöl egy vagy több, az I. melléklet 1. pontjában megállapított követelményeknek megfelelő CSIRT-et, amelyek a kockázatoknak és a biztonsági eseményeknek egy jól meghatározott eljárással összhangban történő kezeléséért felelősek. A CSIRT egy illetékes hatóságon belül is létrehozható.

(2) A tagállamok biztosítják, hogy a CSIRT-ek elegendő erőforrással rendelkeznek az I. melléklet 2. pontjában meghatározott feladataik hatékony ellátásához.

A tagállamok biztosítják, hogy a CSIRT-jeik hatékonyan, eredményesen és biztonságosan működnek együtt a 12. cikkben említett CSIRT-ek hálózatában.

(3) A tagállamok gondoskodnak arról, hogy a CSIRT-jeik nemzeti szinten megfelelő, biztonságos és ellenállóképes kommunikációs és információs infrastruktúrát használnak.

(4) A tagállamok tájékoztatják a Bizottságot a CSIRT-ek hatásköréről, valamint a biztonsági események kezelésére szolgáló eljárás főbb elemeiről.

(5) A tagállamok az ENISA segítségét kérhetik a nemzeti CSIRT-ek továbbfejlesztéséhez.

10. cikk

Nemzeti szintű együttműködés

(1) Ugyanazon tagállam illetékes hatósága, egyedüli kapcsolattartó pontja, valamint CSIRT-jei, amennyiben különállóak, kötelesek együttműködni az ezen irányelvben meghatározott kötelezettségek végrehajtása tekintetében.

(2) A tagállamok biztosítják, hogy vagy az illetékes hatóságok vagy a CSIRT-ek megkapják az ezen irányelv alapján tett bejelentéseket a biztonsági eseményekről. Amennyiben egy tagállam úgy határoz, hogy a CSIRT-ek nem kapnak tájékoztatást a bejelentésekről, akkor CSIRT-ek részére – a feladataik ellátásához szükséges mértékben – hozzáférést kell biztosítani az alapvető szolgáltatásokat nyújtó szereplők által a 14. cikk (3) és (5) bekezdésének megfelelően bejelentett biztonsági események adataihoz, illetve a digitális szolgáltatók által a 16. cikk (3) és (6) bekezdésének megfelelően bejelentett biztonsági események adataihoz.

(3) A tagállamok biztosítják, hogy az illetékes hatóságok, illetve a CSIRT-ek tájékoztatják az egyedüli kapcsolattartó pontokat az ezen irányelv alapján bejelentett biztonsági eseményekről.

Az egyedüli kapcsolattartó pont 2018. augusztus 9-ig, azt követően pedig évente egyszer köteles összefoglaló jelentést benyújtani az együttműködési csoportnak a 14. cikk (3) és (5) bekezdésének és a 16. cikk (3) és (6) bekezdésének megfelelően kapott bejelentésekről, és a jelentésnek tartalmaznia kell a bejelentések számát, a bejelentett biztonsági események jellegét, valamint a hozott intézkedéseket.

III. FEJEZET

EGYÜTTMŰKÖDÉS

11. cikk

Együttműködési csoport

(1) Egy együttműködési csoport kerül létrehozásra a tagállamok közötti stratégiai együttműködés és információcsere támogatása és megkönnyítése, a bizalom megteremtése, valamint a hálózati és információs rendszerek egységesen magas szintű biztonságának Unión belüli megvalósítása érdekében.

Az együttműködési csoport a (3) bekezdés második albekezdésében említett kétéves munkaprogramok keretében végzi feladatait.

(2) Az együttműködési csoport a tagállamok, a Bizottság és az ENISA képviselőiből áll.

Az együttműködési csoport szükség esetén az érdekeltek képviselőit is felkérheti a munkájában való részvételre.

A titkárságot a Bizottság biztosítja.

(3) Az együttműködési csoport a következő feladatokat látja el:

a) stratégiai iránymutatást nyújt a 12. cikk értelmében létrehozott CSIRT-ek hálózata által végzett tevékenységekhez;

b) megosztja a 14. cikk (3) és (5) bekezdésében, valamint a 16. cikk (3) és (6) bekezdésében említett biztonsági események bejelentésével kapcsolatos információcserére vonatkozó bevált gyakorlatot;

c) biztosítja a bevált gyakorlatok tagállamok közötti cseréjét, és az ENISA közreműködésével segítséget nyújt a tagállamoknak a hálózati és információs rendszerek biztonságának kapacitásbővítéséhez;

d) megvitatja a tagállamok képességeit és felkészültségét, önkéntes alapon értékeli a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiákat és a CSIRT-ek hatékonyságát, továbbá meghatározza a bevált gyakorlatokat;

e) megosztja a tájékoztatással és képzéssel kapcsolatos információkat és bevált gyakorlatot;

f) megosztja a hálózati és információs rendszerek biztonságának kutatásával és fejlesztésével kapcsolatos információkat és bevált gyakorlatot;

g) adott esetben megosztja a hálózati és információs rendszerek biztonságával kapcsolatos tapasztalatokat az érintett uniós intézményekkel, szervekkel, hivatalokkal és ügynökségekkel;

h) megvitatja az érintett európai szabványügyi szervezetek képviselőivel a 19. cikkben említett szabványokat és előírásokat;

i) összegyűjti a kockázatokkal és biztonsági eseményekkel kapcsolatos bevált gyakorlatra vonatkozó információkat;

j) évente megvizsgálja a 10. cikk (3) bekezdésének második albekezdésében említett összefoglaló jelentéseket;

k) megvitatja a hálózati és információs rendszerek biztonsági gyakorlataival, az oktatási programokkal és a képzéssel kapcsolatos munkát, ideértve az ENISA által végzett munkát is;

l) az ENISA segítségével megosztja a bevált gyakorlatot az alapvető szolgáltatásokat nyújtó szereplők tagállami meghatározásával kapcsolatban, beleértve a határokon átnyúló függőségeket, a biztonsági kockázatokra és biztonsági eseményekre vonatkozóan is;

m) megvitatja a biztonsági eseményekkel kapcsolatban tett, a 14. és a 16. cikkben említett bejelentések alapján hozott szabályokat.

Az együttműködési csoport 2018. február 9-ig, majd azt követően kétévente munkaprogramot állít össze a céljai és feladatai végrehajtása érdekében megvalósítandó, ezen irányelv célkitűzéseivel összhangban levő intézkedésekről.

(4) Az együttműködési csoport a 23. cikkben említett felülvizsgálat céljából 2018. augusztus 9-ig, azt követően pedig másfél évente jelentést készít, amelyben értékeli az e cikk értelmében folytatott stratégiai együttműködésből szerzett tapasztalatokat.

(5) A Bizottság végrehajtási jogi aktusokat fogad el az együttműködési csoport működéséhez szükséges eljárásrend megállapítása céljából. Az említett végrehajtási jogi aktusokat a 22. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

Az első albekezdés végrehajtása érdekében a Bizottság 2017. február 9-ig benyújtja a 22. cikk (1) bekezdésében említett bizottságnak a végrehajtási jogi aktus első tervezetét.

12. cikk

A CSIRT-ek hálózata

(1) A tagállamok közötti bizalom erősítése, valamint a gyors és hatékony operatív együttműködés előmozdítása érdekében létrejön a nemzeti CSIRT-ek hálózata (a továbbiakban: CSIRT-ek hálózata).

(2) A CSIRT-ek hálózata a tagállamok CSIRT-jei és CERT-EU képviselőiből áll. A Bizottság megfigyelőként vesz részt a CSIRT-hálózatban. Az ENISA biztosítja a titkárságot, és aktívan támogatja a CSIRT-ek közötti együttműködést.

(3) A CSIRT-ek hálózata a következő feladatokat látja el:

a) megosztja a CSIRT-ek szolgáltatási, operatív és együttműködési képességeivel kapcsolatos információkat;

b) egy biztonsági esemény által potenciálisan érintett tagállami CSIRT képviselőjének kérésére megosztja és megvitatja az adott eseményre és a kapcsolódó kockázatokra vonatkozó, üzleti szempontból nem érzékeny információkat, bármely tagállami CSIRT megtagadhatja azonban az e vitában való közreműködést, ha emiatt sérülhet a biztonsági esemény kivizsgálása;

c) önkéntesen megosztja és rendelkezésre bocsátja az egyes biztonsági eseményekre vonatkozó nem bizalmas információkat;

d) valamely tagállami CSIRT képviselőjének kérésére megvitatja az érintett tagállam joghatósága alá tartozó területen bekövetkezett biztonsági eseményt, és lehetőség szerint koordinált választ ad a problémára;

e) segítséget nyújt a tagállamoknak a határon átnyúló biztonsági események önkéntes kölcsönös segítségnyújtás keretében történő kezeléséhez;

f) megvitatja, megvizsgálja és meghatározza az operatív együttműködés további formáit, többek között az alábbiakkal kapcsolatban:

   i. a kockázatok és biztonsági események kategóriái;

   ii. korai előrejelzés;

   iii. kölcsönös segítségnyújtás;

   iv. a koordináció elvei és módjai olyan esetekben, amikor a tagállamok határokon átnyúló kockázatokra és biztonsági eseményekre reagálnak;

g) tájékoztatja az együttműködési csoportot a tevékenységeiről és az operatív együttműködésnek az f) pont szerint megvitatott további formáiról, és iránymutatást kér az operatív együttműködésre nézve;

h) megvitatja a hálózati és információs rendszerek biztonsági gyakorlataiból levont tanulságokat, ideértve az ENISA által szervezett gyakorlatok tanulságait is;

i) egy adott CSIRT kérésére megvitatja e CSIRT képességeit és felkészültségét;

j) iránymutatásokat bocsát ki az e cikk rendelkezéseinek alkalmazása tekintetében az abban foglalt operatív együttműködésre vonatkozóan a működési gyakorlatok közelítésének megkönnyítése érdekében.

(4) A CSIRT-ek hálózata a 23. cikkben említett felülvizsgálat céljából 2018. augusztus 9-ig, azután pedig másfél évente jelentést készít, amelyben értékeli az e cikk értelmében folytatott operatív együttműködésből szerzett tapasztalatokat, valamint következtetéseket és ajánlásokat mellékel hozzá. E jelentést az együttműködési csoport számára is be kell nyújtani.

(5) A CSIRT-ek hálózata meghatározza saját eljárási szabályzatát.

13. cikk

Nemzetközi együttműködés

Az Unió az EUMSZ 218. cikkével összhangban nemzetközi megállapodásokat köthet harmadik országokkal vagy nemzetközi szervezetekkel, ezáltal lehetővé téve és megszervezve az együttműködési csoport egyes tevékenységeiben való részvételüket. E megállapodásokban figyelemmel kell lenni arra, hogy biztosítsák az adatok megfelelő védelmét.

IV. FEJEZET

AZ ALAPVETŐ SZOLGÁLTATÁSOKAT NYÚJTÓ SZEREPLŐK HÁLÓZATI ÉS INFORMÁCIÓS RENDSZEREINEK BIZTONSÁGA

14. cikk

Biztonsági követelmények és a biztonsági események bejelentése

(1) A tagállamok biztosítják, hogy az alapvető szolgáltatásokat nyújtó szereplők megfelelő és arányos műszaki és szervezési intézkedéseket tesznek a működésük során általuk használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében. A hálózati és információs rendszerek tekintetében az említett intézkedéseknek – tekintettel a tudomány és a technika mindenkori állására – a felmerülő kockázatnak megfelelő biztonsági szintet kell biztosítaniuk.

(2) A tagállamok gondoskodnak arról, hogy az alapvető szolgáltatásokat nyújtó szereplők megfelelő intézkedéseket tesznek az ilyen alapvető szolgáltatások nyújtása során alkalmazott hálózati és információs rendszerek biztonságát érintő biztonsági események megelőzésére és azok hatásainak csökkentésére annak céljából, hogy biztosítsák az említett szolgáltatások folytonosságát.

(3) A tagállamok biztosítják, hogy az alapvető szolgáltatásokat nyújtó szereplők indokolatlan késedelem nélkül bejelentik az illetékes hatóságnak vagy a CSIRT-nek az általuk nyújtott alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági eseményeket. A bejelentéseknek tartalmazniuk kell az ahhoz szükséges információkat, hogy az illetékes hatóság vagy a CSIRT meg tudja határozni az adott biztonsági esemény esetleges határon átnyúló hatásait. A bejelentés nem róhat többletfelelősséget a bejelentő félre.

(4) Egy biztonsági esemény hatása jelentőségének meghatározása érdekében elsősorban az alábbi paramétereket kell figyelembe venni:

a) az alapvető szolgáltatás zavara által érintett felhasználók száma;

b) a biztonsági esemény időtartama;

c) a biztonsági esemény által érintett terület földrajzi kiterjedése.

(5) Az illetékes hatóságnak vagy CSIRT-nek az alapvető szolgáltatásokat nyújtó szereplőktől kapott bejelentésben foglalt információk alapján tájékoztatnia kell a többi érintett tagállamot, amennyiben a biztonsági esemény az adott tagállamban jelentős hatást gyakorol az alapvető szolgáltatások folytonosságára. Az illetékes hatóságnak vagy a CSIRT-nek ennek során – az uniós jognak, valamint az uniós joggal összhangban lévő nemzeti jogszabályoknak megfelelően – biztosítania kell az alapvető szolgáltatásokat nyújtó szereplő biztonságát, gondoskodnia kell arról, hogy ne sérüljenek a kereskedelmi érdekei és a bejelentésben foglalt információk bizalmassága.

Amennyiben a körülmények lehetővé teszik, az illetékes hatóságnak vagy a CSIRT-nek a bejelentést tevő, alapvető szolgáltatásokat nyújtó szereplő rendelkezésére kell bocsátania a bejelentését követő intézkedésekkel kapcsolatos releváns információkat, így például az olyan információkat, amelyek segíthetik a biztonsági esemény eredményes kezelését.

Az illetékes hatóság vagy a CSIRT kérésére az egyedüli kapcsolattartó pontnak az első albekezdésben említett bejelentéseket továbbítania kell a többi érintett tagállam egyedüli kapcsolattartó pontjai részére.

(6) Az alapvető szolgáltatásokat nyújtó és a bejelentést tevő gazdasági szereplővel folytatott egyeztetést követően az illetékes hatóság vagy CSIRT tájékoztathatja a nyilvánosságot az egyes biztonsági eseményekről, amennyiben erre egy adott biztonsági esemény megelőzéséhez vagy egy már folyamatban lévő biztonsági esemény kezeléséhez szükség van.

(7) Az együttműködési csoport keretében közösen eljáró illetékes hatóságok iránymutatásokat dolgozhatnak ki és fogadhatnak el azon körülményekre vonatkozóan, amelyek fennállása esetén az alapvető szolgáltatásokat nyújtó szereplőknek a biztonsági eseményeket be kell jelenteniük, beleértve a biztonsági esemény hatása jelentőségének meghatározását lehetővé tevő, a (4) bekezdésben említett paramétereket is.

15. cikk

Végrehajtás és alkalmazás

(1) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok rendelkezzenek az ahhoz szükséges hatáskörrel és eszközökkel, hogy felmérjék, hogy az alapvető szolgáltatásokat nyújtó szereplők teljesítik-e a 14. cikk szerinti kötelezettségeiket, valamint hogy értékeljék azoknak a hálózati és információs rendszerek biztonságára gyakorolt hatását.

(2) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok rendelkezzenek az ahhoz szükséges hatáskörrel és eszközökkel, hogy megköveteljék a következőket az alapvető szolgáltatásokat nyújtó szereplőktől:

a) bocsássák rendelkezésre a hálózatai és információs rendszereik biztonságának megállapításához szükséges adatokat, beleértve a biztonsági szabályzatukra vonatkozóakat is;

b) igazolják a biztonsági szabályzatok eredményes végrehajtását, például egy illetékes hatóság vagy egy képesített ellenőr által végzett biztonsági ellenőrzés eredményeinek benyújtásával, és az utóbbi esetben bocsássák az eredményeket – az azokat alátámasztó bizonyítékokat is beleértve – az illetékes hatóság rendelkezésére.

Az illetékes hatóságoknak az említett információkra vagy bizonyítékokra vonatkozó megkeresésben fel kell tüntetniük a megkeresés célját, és meg kell határozniuk a kért információkat.

(3) Az információknak vagy a biztonsági ellenőrzések eredményeinek a (2) bekezdésben említett értékelését követően az illetékes hatóság kötelező erejű utasításokat adhat az alapvető szolgáltatásokat nyújtó szereplőknek arra vonatkozóan, hogy megfelelően orvosolják az azonosított hiányosságokat.

(4) Az illetékes hatóságnak a személyes adatok megsértésével járó biztonsági események kapcsán szorosan együtt kell működnie az adatvédelmi hatóságokkal.

V. FEJEZET

A DIGITÁLIS SZOLGÁLTATÓK HÁLÓZATI ÉS INFORMÁCIÓS RENDSZEREINEK BIZTONSÁGA

16. cikk

Biztonsági követelmények és a biztonsági események bejelentése

(1) A tagállamok biztosítják, hogy a digitális szolgáltatók megfelelő és arányos műszaki és szervezési intézkedéseket határoznak és tesznek meg a III. mellékletben említett szolgáltatásoknak az Unión belül történő nyújtása során általuk használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében. A hálózati és információs rendszerek tekintetében az említett intézkedéseknek – tekintettel a tudomány és a technika mindenkori állására – a felmerülő kockázatnak megfelelő biztonsági szintet kell biztosítaniuk, és figyelembe kell venniük a következő elemeket:

a) a rendszerek és a létesítmények biztonsága;

b) a biztonsági események kezelés;,

c) üzletmenetfolytonosság-menedzsment;

d) monitoring, ellenőrzés és vizsgálat;

e) a nemzetközi szabványoknak való megfelelés.

(2) A tagállamok biztosítják, hogy a digitális szolgáltatók intézkedéseket hoznak annak érdekében, hogy megelőzzék és csökkentsék a hálózati és információs rendszereik biztonságát érintő biztonsági események által a III. mellékletben említett, az Unión belül kínált szolgáltatásokra gyakorolt hatásokat, annak céljából, hogy biztosított legyen az említett szolgáltatások folytonossága.

(3) A tagállamok biztosítják, hogy a digitális szolgáltatók indokolatlan késedelem nélkül bejelentenek az illetékes hatóságnak vagy a CSIRT-nek minden olyan biztonsági eseményt, amely jelentős hatást gyakorol az általuk az Unión belül kínált, a III. mellékletben említett szolgáltatás nyújtására. A bejelentéseknek tartalmazniuk kell az ahhoz szükséges információkat, hogy az illetékes hatóság vagy a CSIRT meg tudja határozni az esetleges határon átnyúló hatás jelentőségét. A bejelentés nem róhat többletfelelősséget a bejelentő félre.

(4) Annak meghatározása érdekében, hogy egy biztonsági esemény hatása jelentős-e elsősorban az alábbi paramétereket kell figyelembe venni:

a) a biztonsági esemény által érintett felhasználók száma, különös tekintettel azon felhasználókra, akik az érintett szolgáltatásra alapozzák a saját szolgáltatásaik nyújtását;

b) a biztonsági esemény időtartama;

c) a biztonsági esemény által érintett terület földrajzi kiterjedése;

d) a szolgáltatás működésében támadt zavar mértéke;

e) a gazdasági és társadalmi tevékenységekre gyakorolt hatás mértéke.

A biztonsági esemény bejelentésére vonatkozó kötelezettség csak abban az esetben áll fenn, ha a digitális szolgáltató számára elérhetők azok az információk, amelyek alapján az első albekezdésben említett paraméterek figyelembevételével ki tudja értékelni a biztonsági esemény hatását.

(5) Amennyiben egy alapvető szolgáltatásokat nyújtó szereplő valamely, a kritikus társadalmi és gazdasági tevékenységek fenntartása szempontjából alapvetőnek tekintett szolgáltatás nyújtását egy harmadik fél digitális szolgáltatóra alapozza, az említett szereplőnek be kell jelentenie minden olyan esetet, amikor a digitális szolgáltatót érintő biztonsági esemény jelentős hatást gyakorol az alapvető szolgáltatások folytonosságára.

(6) Adott esetben, és különösen akkor, ha a (3) bekezdésben említett biztonsági esemény két vagy több tagállamot érint, az illetékes hatóságnak vagy CSIRT-nek tájékoztatnia kell a többi érintett tagállamot. Az illetékes hatóságoknak, a CSIRT-eknek és az egyedüli kapcsolattartó pontoknak ennek során – az uniós jognak, valamint az uniós joggal összhangban lévő nemzeti jogszabályoknak megfelelően – biztosítaniuk kell a digitális szolgáltató biztonságát, gondoskodniuk kell arról, hogy ne sérüljenek a digitális szolgáltató kereskedelmi érdekei, valamint meg kell őrizniük a szolgáltatott információk bizalmasságát.

(7) Az érintett digitális szolgáltatóval folytatott egyeztetést követően az illetékes hatóság vagy CSIRT, és adott esetben a többi érintett tagállam hatóságai vagy CSIRT-jei tájékoztathatják a nyilvánosságot az egyes biztonsági eseményekről vagy kötelezhetik a digitális szolgáltatót a nyilvánosság tájékoztatására, amennyiben erre egy adott biztonsági esemény megelőzéséhez vagy egy már folyamatban lévő biztonsági esemény kezeléséhez szükség van, vagy ha a biztonsági esemény nyilvánosságra hozatala egyéb módon közérdeket szolgál.

(8) A Bizottság végrehajtási jogi aktusokat fogad el az e cikk (1) bekezdésében említett elemek és a (4) bekezdésében felsorolt paraméterek pontosabb meghatározása érdekében. Az említett végrehajtási jogi aktusokat, a 22. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban 2017. augusztus 9-ig kell elfogadni.

(9) A Bizottság végrehajtási jogi aktusokat fogadhat el a bejelentési követelményekre vonatkozó formátumok és eljárások megállapítása céljából. Az említett végrehajtási jogi aktusokat a 22. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

(10) A tagállamok – az 1. cikk (6) bekezdésének sérelme nélkül – semmilyen további biztonsági vagy bejelentési követelményt nem róhatnak a digitális szolgáltatókra.

(11) Az V. fejezet nem alkalmazandó a 2003/361/EK bizottsági ajánlásban ([1]) meghatározott mikro- és kisvállalkozásokra.

([1]) A Bizottság 2003/361/EK ajánlása (2003. május 6.) a mikro-, kis- és középvállalkozások fogalmának meghatározásáról (HL L 124., 2003.5.20., 36. o.).

17. cikk

Végrehajtás és alkalmazás

(1) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok lépéseket tegyenek – szükség esetén utólagos felügyeleti intézkedések révén –, amennyiben bizonyítékokat tárnak eléjük arra vonatkozóan, hogy valamely digitális szolgáltató nem teljesíti a 16. cikkben meghatározott követelményeket. Ilyen bizonyítékot olyan másik tagállam illetékes hatósága nyújthat be, ahol sor kerül az adott szolgáltatás nyújtására.

(2) Az (1) bekezdés alkalmazásában az illetékes hatóságoknak rendelkezniük kell az ahhoz szükséges hatáskörrel és eszközökkel, hogy kötelezzék a digitális szolgáltatókat arra, hogy:

a) bocsássák rendelkezésre a hálózati és információs rendszereik biztonságának megállapításához szükséges adatokat, beleértve a biztonsági szabályzataikra vonatkozóakat is;

b) gondoskodjanak minden, a 16. cikkben foglalt követelményeknek való megfelelés terén tapasztalt hiányosság megszüntetéséről.

(3) Ha egy digitális szolgáltató központi ügyvezetésének helye vagy képviselője az egyik tagállamban van, míg a hálózati és információs rendszerei egy vagy több másik tagállamban találhatók, a központi ügyvezetés helye vagy a képviselő helye szerinti tagállam illetékes hatóságának és az említett másik tagállamok illetékes hatóságainak szükség szerint együtt kell működniük és segíteniük kell egymást. Ez a segítségnyújtás és együttműködés magában foglalhat az érintett illetékes hatóságok közötti információcseréket, valamint a (2) bekezdésben említett felügyeleti intézkedések foganatosítására irányuló megkereséseket is.

18. cikk

Joghatóság és területiség

(1) Ezen irányelv alkalmazásában úgy kell tekinteni, hogy a digitális szolgáltatók annak a tagállamnak a joghatósága alá tartoznak, amelyben a központi ügyvezetésük helye található. Úgy kell tekinteni, hogy egy digitális szolgáltató központi ügyvezetésének helye abban a tagállamban van, amelyben a székhelye található.

(2) Azon digitális szolgáltatóknak, amelyek az Unióban nincsenek letelepedve, azonban az Unión belül kínálják a III. mellékletben említett szolgáltatásokat, az Unióban képviselőt kell kijelölniük. A képviselőnek le kell telepednie a szolgáltatásnyújtás által érintett valamely tagállamban. Úgy kell tekinteni, hogy a digitális szolgáltató annak a tagállamnak a joghatósága alá tartozik, amelyben a képviselő letelepedett.

(3) Az a tény, hogy a digitális szolgáltató képviselőt jelöl ki, nem érinti a magával a digitális szolgáltatóval szembeni keresetindításhoz való jogot.

VI. FEJEZET

SZABVÁNYOSÍTÁS ÉS ÖNKÉNTES BEJELENTÉS

19. cikk

Szabványosítás

(1) A 14. cikk (1) és (2) bekezdése, valamint a 16. cikk (1) és (2) bekezdése egységes végrehajtásának előmozdítása érdekében a tagállamok – anélkül, hogy kötelezővé tennék vagy előnyben részesítenék valamely konkrét technológiatípus alkalmazását – ösztönzik a hálózati és az információs rendszerek biztonságának szempontjából releváns európai vagy nemzetközileg elfogadott szabványok és előírások alkalmazását.

(2) Az ENISA a tagállamokkal együttműködésben tanácsot ad és iránymutatásokat készít az olyan műszaki területeket illetően, amelyeket tekintetbe kell venni az (1) bekezdés alkalmazásában, továbbá azon már létező szabványokat illetően – a tagállamok nemzeti szabványait is beleértve –, amelyek alkalmazásával lefedhetők az említett területek.

20. cikk

Önkéntes bejelentés

(1) A 3. cikk sérelme nélkül, azok a szervezetek, amelyeket nem azonosítottak alapvető szolgáltatásokat nyújtó szereplőként és amelyek nem digitális szolgáltatók, önkéntes alapon bejelenthetik az olyan biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az általuk nyújtott szolgáltatások folytonosságára.

(2) A tagállamok a bejelentések feldolgozásakor a 14. cikkben meghatározott eljárásnak megfelelően járnak el. A tagállamok az önkéntes bejelentésekkel szemben előnyben részesíthetik a kötelező bejelentések feldolgozását. Az önkéntes bejelentéseket csak akkor kell feldolgozni, ha az nem jelent aránytalan vagy indokolatlan terhet az érintett tagállamok számára.

Az önkéntes bejelentés eredményeként a bejelentő szervezet számára nem írható elő olyan kötelezettség, amely ne vonatkozott volna rá a bejelentés megtétele nélkül is.

VII. FEJEZET

ZÁRÓ RENDELKEZÉSEK

21. cikk

Szankciók

A tagállamok megállapítják az ezen irányelv alapján elfogadott nemzeti rendelkezések megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és megtesznek minden szükséges intézkedést e szabályok végrehajtásának biztosítására. A megállapított szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük. A tagállamok az említett szabályokról és intézkedésekről 2018. május 9-ig értesítik a Bizottságot, és haladéktalanul értesítik az azokat érintő minden későbbi módosításról is.

22. cikk

A bizottsági eljárás

(1) A Bizottságot a hálózati és információs rendszerek biztonsági bizottsága segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottságnak minősül.

(2) Az e bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 5. cikkét kell alkalmazni.

23. cikk

Felülvizsgálat

(1) A Bizottság 2019. május 9-ig jelentést nyújt be az Európai Parlamentnek és a Tanácsnak, amelyben értékeli a tagállamok által az alapvető szolgáltatásokat nyújtó szereplők azonosítása során alkalmazott megközelítés következetességét.

(2) A Bizottság rendszeresen felülvizsgálja ezen irányelv működését, és jelentést tesz arról az Európai Parlamentnek és a Tanácsnak. Ennek érdekében, illetve a stratégiai és az operatív együttműködés további előmozdítása céljából a Bizottság figyelembe veszi az együttműködési csoportnak és a CSIRT-ek hálózatának a stratégiai és operatív szinten szerzett tapasztalatokról szóló jelentéseit. A Bizottság a felülvizsgálat során értékeli továbbá a II. és III. mellékletben szereplő jegyzékeket, valamint az alapvető szolgáltatásokat nyújtó szereplők azonosítása és a II. mellékletben említett szolgáltatások terén megfigyelhető következetességet. Az első jelentést 2021. május 9-ig kell benyújtani.

24. cikk

Átmeneti intézkedések

(1) A 25. cikk sérelme nélkül, valamint annak céljából, hogy a tagállamok számára további lehetőségek álljanak rendelkezésre az átültetés időszakában történő megfelelő együttműködésre, az együttműködési csoportnak és a CSIRT-ek hálózatának 2017. február 9-ig meg kell kezdenie a 11. cikk (3) bekezdésében, illetve a 12. cikk (3) bekezdésében meghatározott feladatait ellátását.

(2) A 2017. február 9. és a 2018. november 9. közötti időszaktól, továbbá annak céljából, hogy a tagállamokat segítse az alapvető szolgáltatásokat nyújtó szereplőkre irányuló azonosítási eljárás során a következetes megközelítés alkalmazásában, az együttműködési csoportnak meg kell vitatnia azon nemzeti intézkedések eljárásait, tartalmát és típusát, amelyek lehetővé teszik egy meghatározott ágazatban alapvető szolgáltatásokat nyújtó szereplőknek az 5. és 6. cikkben megállapított kritériumoknak megfelelő azonosítását. Az együttműködési csoportnak valamely tagállam kérésére meg kell továbbá vitatnia az adott tagállam azon konkrét nemzeti intézkedéseinek a tervezetét, amelyek lehetővé teszik egy meghatározott ágazatban alapvető szolgáltatásokat nyújtó szereplőknek az 5. és 6. cikkben megállapított kritériumoknak megfelelő azonosítását.

(3) A tagállamok 2017. február 9-ig és e cikk alkalmazásában gondoskodnak az együttműködési csoportban és a CSIRT-ek hálózatában való megfelelő képviseletről.

25. cikk

Átültetés

(1) A tagállamok 2018. május 9-ig elfogadják és kihirdetik azokat a törvényi, rendeleti és közigazgatási rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek megfeleljenek. Erről haladéktalanul tájékoztatják a Bizottságot.

Ezeket a rendelkezéseket 2018. május 10-től kezdve alkalmazzák.

Amikor a tagállamok elfogadják ezeket a 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.

26. cikk

Hatálybalépés

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

27. cikk

Címzettek

Ennek az irányelvnek a tagállamok a címzettjei.

Kelt Strasbourgban, 2016. július 6-án.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*
M. SCHULZ	I. KORČOK

I. MELLÉKLET

A SZÁMÍTÓGÉP-BIZTONSÁGI ESEMÉNYEKRE REAGÁLÓ CSOPORTOK (CSIRT-ek) KÖTELEZETTSÉGEI ÉS FELADATAI

A nemzeti szakpolitikának és/vagy szabályozásnak megfelelően és egyértelműen meg kell határoznia a CSIRT-ek kötelezettségeit és feladatait, és támogatnia kell azok teljesítését. E kötelezettségeknek és feladatoknak magukban kell foglalniuk a következőket:

(1) A CSIRT-ek kötelezettségei

a) A CSIRT-eknek a kritikus hibapontok kiküszöbölése révén biztosítaniuk kell a hírközlési szolgáltatásaik magas szintű elérhetőségét, továbbá elérhetőségük és másokkal való kapcsolattartásuk céljára folyamatosan több eszközt kell fenntartaniuk. A kommunikációs csatornákat egyértelműen meg kell határozni, és azokat a felhasználóiknak és az együttműködési partnereiknek jól kell ismerniük.

b) A CSIRT-ek hivatali helyiségeit és a támogató információs rendszereket biztonságos helyszíneken kell elhelyezni.

c) Az üzletmenet folytonossága:

i. a CSIRT-eknek megfelelő rendszerrel kell rendelkeznie a megkeresések kezelésére és továbbítására, az átadás megkönnyítése céljából.

ii. a CSIRT-eket elegendő személyzettel kell ellátni ahhoz, hogy mindig készenlétben legyenek.

iii. a CSIRT-eknek olyan infrastruktúrára kell támaszkodnia, amelynek biztosított a folytonossága. Ennek érdekében redundáns rendszereket és tartalék munkaterületet kell fenntartani.

d) A CSIRT-ek számára lehetővé kell tenni, hogy amennyiben kívánnak, részt vehessenek nemzetközi együttműködési hálózatokban.

(2) A CSIRT-ek feladatai

a) A CSIRT-ek feladatainak magukban kell foglalniuk legalább a következőket:

i. a biztonsági események nemzeti szintű monitoringja;

ii. a kockázatokkal és biztonsági eseményekkel kapcsolatos korai előrejelzés, riasztás, bejelentéstétel és információterjesztés a releváns érdekeltek számára;

iii. reagálás a biztonsági eseményekre;

iv. dinamikus kockázat- és eseményelemzés, valamint helyzetkép nyújtása;

v. a CSIRT-ek hálózatában való részvétel.

b) A CSIRT-eknek együttműködési kapcsolatokat kell kialakítania a magánszférával.

c) Az együttműködés megkönnyítése érdekében a CSIRT-eknek közös vagy szabványosított gyakorlatok elfogadását és alkalmazását kell szorgalmaznia az alábbiakra vonatkozóan:

i. a biztonsági események és a kockázatok kezelésére vonatkozó eljárások;

ii. a biztonsági események, kockázatok és információk osztályozására szolgáló rendszerek.

II. MELLÉKLET

A SZERVEZETEK TÍPUSAI A 4. CIKK 4. PONTJÁNAK ALKALMAZÁSÁBAN

Ágazat	Alágazat	A szervezet típusa
1. Energia	a) Villamos energia	— A 2009/72/EK európai parlamenti és tanácsi irányelv ([1]) 2. cikkének 35. pontjában meghatározott villamosenergia-ipari vállalkozások, amelyek az említett irányelv 2. cikkének 19. pontjában meghatározott „ellátás” funkciót látja el
		— A 2009/72/EK irányelv 2. cikkének 6. pontjában meghatározott elosztórendszer-üzemeltetők
		— A 2009/72/EK irányelv 2. cikkének 4. pontjában meghatározott átvitelirendszer-üzemeltetők
	b) Kőolaj	— Kőolajvezetékek üzemeltetői
		— Kőolajtermelő, -finomító, illetve -feldolgozó létesítmények, -tárolók és -vezetékek üzemeltetői
	c) Földgáz	— A 2009/73/EK európai parlamenti és tanácsi irányelv ([2]) 2. cikkének 8. pontjában meghatározott ellátó vállalkozások
		— A 2009/73/EK irányelv 2. cikkének 6. pontjában meghatározott elosztórendszer-üzemeltetők
		— A 2009/73/EK irányelv 2. cikkének 4. pontjában meghatározott szállításirendszer-üzemeltetők
		— A 2009/73/EK irányelv 2. cikkének 10. pontjában meghatározott tárolásirendszer-üzemeltetők
		— A 2009/73/EK irányelv 2. cikkének 12. pontjában meghatározott LNG-létesítmény rendszerüzemeltetői
		— A 2009/73/EK irányelv 2. cikkének 1. pontjában meghatározott földgázipari vállalkozások
		— Földgázfinomító, illetve -feldolgozó létesítmények üzemeltetői
2. Közlekedés	a) Légi közlekedés	— A 300/2008/EK európai parlamenti és tanácsi rendelet ([3]) 3. cikkének 4. pontjában meghatározott légi fuvarozók
		— A 2009/12/EK európai parlamenti és tanácsi irányelv ([4]) 2. cikkének 2. pontjában meghatározott repülőtér-irányító szervezetek, az említett irányelv 2. cikkének 1. pontjában meghatározott repülőterek, a törzshálózathoz tartozó, az 1315/2013/EU európai parlamenti és tanácsi rendelet ([5]) II. mellékletének 2. szakaszában felsorolt repülőtereket is beleértve; valamint a repülőtereken található kapcsolódó létesítményeket üzemeltető szervezetek

Ágazat	Alágazat	A szervezet típusa
		— Az 549/2004/EK európai parlamenti és tanácsi rendelet [6] 2. cikkének 1. pontjában meghatározott légiforgalmi irányító (ATC) szolgálatot ellátó forgalomirányítási üzemeltetők
	b) Vasúti közlekedés	— A 2012/34/EU európai parlamenti és tanácsi irányelv [7] 3. cikkének 2. pontjában meghatározott pályahálózat-működtetők
		— A 2012/34/EU irányelv 3. cikkének 1. pontjában meghatározott vállalkozó vasúti társaságok, a kiszolgáló létesítményeknek a 2012/34/EU irányelv 3. cikkének 12. pontjában meghatározott üzemeltetőit is beleértve
	c) Vízi közlekedés	— A tengeri szállításnak a 725/2004/EK európai parlamenti és tanácsi rendelet [8] I. mellékletében foglalt meghatározása szerinti belvízi, tengeri és part menti vízi személyszállítással, illetve vízi árufuvarozással foglalkozó vállalkozások, nem beleértve azonban az e vállalkozások által üzemeltetett egyes hajókat
		— A 2005/65/EK európai parlamenti és tanácsi irányelv [9] 3. cikkének 1. pontjában meghatározott kikötőket irányító szervek, a 725/2004/EK rendelet 2. cikkének 11. pontjában meghatározott kikötőlétesítményeket is beleértve; valamint a kikötőkben található létesítményeket és berendezéseket üzemeltető szervek
		— A 2002/59/EK európai parlamenti és tanácsi irányelv [10] 3. cikkének o) pontjában meghatározott hajóforgalmi szolgálatok üzemeltetői
	d) Közúti közlekedés	— Az (EU) 2015/962 felhatalmazáson alapuló bizottsági rendelet [11] 2. cikkének 12.pontjában meghatározott, a forgalomirányításért felelős közúti hatóságok
		— A 2010/40/EU európai parlamenti és tanácsi irányelv [12] 4. cikkének 1. pontjában meghatározott intelligens közlekedési rendszerek üzemeltetői
3. Banki szolgáltatások		Az 575/2013/EU európai parlamenti és tanácsi rendelet [13] 4. cikkének 1. pontjában meghatározott hitelintézetek
4. Pénzügyi piaci infrastruktúrák		— A 2014/65/EU európai parlamenti és tanácsi irányelv [14] 4. cikkének 24. pontjában meghatározott kereskedési helyszínek működtetői
		— A 648/2012/EU európai parlamenti és tanácsi rendelet [15] 2. cikkének 1. pontjában meghatározott központi szerződő felek
5. Egészségügy	Egészségügyi ellátó létesítmények (beleértve a kórházakat és a magánklinikákat is)	A 2011/24/EU európai parlamenti és tanácsi irányelv [16] 3. cikkének g) pontjában meghatározott egészségügyi szolgáltatók

Ágazat	Alágazat	A szervezet típusa
6. Ivóvízellátás és -elosztás		A 98/83/EK tanácsi irányelv ([17]) 2. cikke 1. pontjának a) alpontjában meghatározott emberi fogyasztásra szánt víz szolgáltatói és elosztói, kivéve azokat az elosztókat, amelyek esetében az emberi fogyasztásra szánt víz elosztása csupán egy részét teszi ki az egyéb, alapvető szolgáltatásoknak nem tekinthető közszolgáltatások és áruk elosztására irányuló általános tevékenységüknek
7. Digitális infrastruktúra		— IXP-k
		— DNS-szolgáltatók
		— TLD név-nyilvántartók

([1]) Az Európai Parlament és a Tanács 2009/72/EK irányelve (2009. július 13.) a villamos energia belső piacára vonatkozó közös szabályokról és a 2003/54/EK irányelv hatályon kívül helyezéséről (HL L 211., 2009.8.14., 55. o.).
([2]) Az Európai Parlament és a Tanács 2009/73/EK irányelve (2009. július 13.) a földgáz belső piacára vonatkozó közös szabályokról és a 2003/55/EK irányelv hatályon kívül helyezéséről (HL L 211., 2009.8.14., 94. o.).
([3]) Az Európai Parlament és a Tanács 300/2008/EK rendelete (2008. március 11.) a polgári légi közlekedés védelmének közös szabályairól és a 2320/2002/EK rendelet hatályon kívül helyezéséről (HL L 97., 2008.4.9., 72. o.).
([4]) Az Európai Parlament és a Tanács 2009/12/EK irányelve (2009. március 11.) a repülőtéri díjakról (HL L 70., 2009.3.14., 11. o.).
([5]) Az Európai Parlament és a Tanács 1315/2013/EU rendelete (2013. december 11.) a transzeurópai közlekedési hálózat fejlesztésére vonatkozó uniós iránymutatásokról és a 661/2010/EU határozat hatályon kívül helyezéséről (HL L 348., 2013.12.20., 1. o.).
([6]) Az Európai Parlament és a Tanács 549/2004/EK rendelete (2004. március 10.) az egységes európai égbolt létrehozására vonatkozó keret megállapításáról (keretrendelet) (HL L 96., 2004.3.31., 1. o.).
([7]) Az Európai Parlament és a Tanács 2012/34/EU irányelve (2012. november 21.) az egységes európai vasúti térség létrehozásáról (HL L 343., 2012.12.14., 32. o.).
([8]) Az Európai Parlament és a Tanács 725/2004/EK rendelete (2004. március 31.) a hajók és kikötőlétesítmények védelmének fokozásáról (HL L 129., 2004.4.29., 6. o.).
([9]) Az Európai Parlament és a Tanács 2005/65/EK irányelve (2005. október 26.) a kikötővédelem fokozásáról (HL L 310., 2005.11.25., 28. o.).
([10]) Az Európai Parlament és a Tanács 2002/59/EK irányelve (2002. június 27.) a közösségi hajóforgalomra vonatkozó megfigyelő és információs rendszer létrehozásáról és a 93/75/EGK irányelv hatályon kívül helyezéséről (HL L 208., 2002.8.5., 10. o.).
([11]) A Bizottság (EU) 2015/962 felhatalmazáson alapuló rendelete (2014. december 18.) a 2010/40/EU európai parlamenti és tanácsi irányelvnek az EU egészére kiterjedő valós idejű forgalmi információs szolgáltatások nyújtása tekintetében történő kiegészítéséről (HL L 157., 2015.6.23., 21. o.).
([12]) Az Európai Parlament és a Tanács 2010/40/EU irányelve (2010. július 7.) az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keretről (HL L 207., 2010.8.6., 1. o.).
([13]) Az Európai Parlament és a Tanács 575/2013/EU rendelete (2013. június 26.) a hitelintézetekre és befektetési vállalkozásokra vonatkozó prudenciális követelményekről és a 648/2012/EU rendelet módosításáról (HL L 176., 2013.6.27., 1. o.).
([14]) Az Európai Parlament és a Tanács 2014/65/EU irányelve (2014. május 15.) a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról (HL L 173., 2014.6.12., 349. o.).
([15]) Az Európai Parlament és a Tanács 648/2012/EU rendelete (2012. július 4.) a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról (HL L 201., 2012.7.27., 1. o.).
([16]) Az Európai Parlament és a Tanács 2011/24/EU irányelve (2011. március 9.) a határon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről (HL L 88., 2011.4.4., 45. o.).
([17]) A Tanács 98/83/EK irányelve (1998. november 3.) az emberi fogyasztásra szánt víz minőségéről (HL L 330., 1998.12.5., 32. o.).

III. MELLÉKLET

A DIGITÁLIS SZOLGÁLTATÁSOK TÍPUSAI A 4. CIKK 5. PONTJÁNAK ALKALMAZÁSÁBAN

1. Online piactér.
2. Online keresőprogram.
3. Felhőlapú számítástechnikai szolgáltatás.