



2017/0225(COD)

16.3.2018

VÉLEMÉNY

az Állampolgári Jogi, Bel- és Igazságügyi Bizottság részéről

az Ipari, Kutatási és Energiaügyi Bizottság részére

az ENISA-ról, az Európai Unió Kiberbiztonsági Ügynökségről, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló európai parlamenti és tanácsi rendeletre („kiberbiztonsági jogszabály”) irányuló javaslatról
(COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

A vélemény előadója: Jan Philipp Albrecht

PA_Legam

RÖVID INDOKOLÁS

Az előadó üdvözli a Bizottság kiberbiztonsági jogszabályról¹ szóló javaslatát, mivel az jobban meghatározza az ENISA szerepét a megváltozott kiberbiztonsági ökoszisztémában és intézkedéseket dolgoz ki az információbiztonsági szabványokra, a tanúsításra és a címkézésre az ikt-alapú rendszerek – ideértve az összekapcsolt tárgyakat is – biztonságosabbá tétele érdekében.

Az előadó azonban úgy véli, hogy további javításokat lehet tenni. Az előadó határozott meggyőződése, hogy az információbiztonság, a számítástechnikai bűnözés elleni küzdelem, valamint a demokrácia és a jogállamiság védelme alapvető fontosságú a polgárok alapvető jogainak védelméhez,

Alapvető jogok: A nem biztonságos rendszerek adatokkal kapcsolatos jogsértésekhez vagy személyazonossággal való visszaéléshez vezethetnek, amelyek az embereknek valós károkat és fenyegetettséget okozhatnak, beleértve életük, magánéletük, méltóságuk és vagyonuk veszélyeztetését is. Például a tanúk megfélemlítés vagy fizikai bántalmazás, a nők pedig otthonukban erőszak áldozatai lehetnek, amennyiben laccímük nyilvánosságra kerül. A dolgok internete, amely nem csupán érzékelőkből, hanem fizikai cselekvéseket végző tárgyakból is áll, fenyegetést jelenthet az emberek testi épségére és életére az információs rendszereken keresztül elkövetett támadások esetén. Az előadó által javasolt módosítások elsősorban az EU Alapjogi Chartája 1., 2., 3., 6., 7., 8., 11. és 17. cikkének védelmére összpontosítanak. Az újabb alkotmányjogi joggyakorlat a jelenlegi digitális világra vonatkozóan az általános személyiségi jogokból kiindulva levezet egy különleges „alapvető jogot az információtechnológiai rendszerek bizalmas kezelésére és interagitására”² vonatkozóan.

A számítástechnikai bűnözés elleni küzdelem: Az interneten elkövetett bűncselekmények bizonyos formái, például az adathalászat (phishing), vagy a pénzügyi és banki csalások bizalommal való visszaélést jelentenek, ami ellen nem lehet informatikai biztonsági intézkedésekkel fellépni, ezért a bűncselekmények ilyen formái elleni küzdelem érdekében az előadó üdvözli a javaslatot, hogy az ENISA szervezzen rendszeres tájékoztató és iskolai kampányokat a végfelhasználók számára. Internetes bűnözés egyéb formái magukban foglalják az információs rendszerek elleni támadásokat, például az adatfeltörést vagy szolgáltatásmegtagadást eredményező túlterheléses támadásokat (DDoS), amelyek kapcsán az előadó úgy véli, hogy az információbiztonság megerősítése révén hatékonyan javítható a számítástechnikai bűnözés elleni küzdelem, és főként annak megelőzése.

Demokrácia és jogállamiság: Az it-rendszerek elleni, kormányzati és a nem állami szereplők által elkövetett támadások egyértelmű és egyre nagyobb veszélyt jelentenek a demokráciára, hiszen beavatkozhatnak a szabad és tisztességes választásokba, például azáltal, hogy manipulálják a polgárok szavazatát befolyásoló tényeket és véleményeket, beavatkoznak a

¹ Európai Bizottság, Javaslat az ENISA-ról, az Európai Unió Kiberbiztonsági Ügynökségről, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló európai parlamenti és tanácsi rendeletre („kiberbiztonsági jogszabály”), COM(2017)0477/2.

² Német alkotmánybíróság, 2008. február 27-i ítéletek, 1 BvR 370/07, 1 BvR 595/07.

szavazási folyamatba és megváltoztatják a szavazási eredményeket, vagy aláássák a szavazás megbízhatóságába vetett hitet.

Az előadó ezért a LIBE bizottság véleménytervezetében az alábbi, a LIBE bizottság számára fontos kérdésekben javasolja a bizottsági javaslat módosítását:

- Az Ügynökségnek hangsúlyosabb szerepet kell játszania az arra való ösztönzésben, hogy az európai információs társadalom valamennyi szereplője elfogadjon a magánéletet óvó erős megelőző technológiákat és informatikai biztonsági intézkedéseket;
- Az Ügynökségnek olyan szakpolitikai javaslatokat kell tennie, amelyek egyértelműen meghatározzák az ikt ökoszisztémájában részt vevő valamennyi érdekelt fél felelősségi körét és feladatait abban az esetben, ha nem járnak el kellő gondossággal az informatikai biztonságuk kapcsán, és ez komoly biztonsági hatásokat, a környezet súlyos szennyezését, vagy rendszerszintű pénzügyi vagy gazdasági válságot okozhat;
- Az Ügynökségnek egyértelmű és kötelező alapvető információbiztonsági követelményeket kell javasolnia, konzultálva informatikai biztonsági szakértőkkel;
- Az Ügynökségnek javaslatot kell tennie egy olyan információbiztonsági tanúsítási rendszerre, amely lehetővé teszi, hogy az eladók növeljék az átláthatóságot a fogyasztók számára a frissíthetőség és a szoftveres támogatás ideje vonatkozásában. Egy ilyen tanúsítási rendszernek dinamikusnak kell lennie, mivel a biztonság egy olyan folyamat, amely állandó fejlesztést igényel;
- Az Ügynökségnek iránymutatások révén és a bevált gyakorlatok megosztásával könnyebbé és olcsóbbá kell tenni az ikt-termékek gyártói számára a megtervezett biztonsági elvek végrehajtását;
- Az Ügynökségnek az uniós intézmények, szervek, hivatalok és ügynökségek, valamint a tagállamok kérésére rendszeres megelőző információbiztonsági ellenőrzéseket kell végeznie a kritikus infrastruktúrák esetében (ellenőrzéshez való jog);
- Az Ügynökségnek haladéktalanul jelentenie kell a nyilvánosan még nem ismert informatikai biztonsági sérülékenységeket a gyártóknak. Az Ügynökség nem tusolhatja el vagy használhatja ki saját céljaira a vállalkozások és termékek még nyilvánosságra nem hozott sérülékenységeit. A kormányzati szervek a polgárok biztonságát teszik kockára, ha informatikai rendszerekben az adófizetők pénzéből kiskapukat alakítanak ki, vásárolnak meg és használnak ki. A többi érdekelt fél védelme érdekében, akik felelősen kezelik az ilyen sérülékenységeket, az Ügynökségnek szakpolitikai javaslatot kell tennie a felelős adatcserére a „zéró napokról” és más, a nyilvánosság előtt még nem ismert biztonsági sebezhetőségekről, és meg kell könnyítenie azok felszámolását;
- Annak lehetővé tétele érdekében, hogy az EU felzárkózzon a harmadik országok informatikai biztonsági iparához, az Ügynökségnek ki kell alakítania és el kell indítania egy hosszú távú uniós informatikai biztonsági projektet, amelynek léptéke hasonló az Airbus-projekthez a légi közlekedési ágazatban;

A bizottsági javaslatnak kerülnie kellene a „kiberbiztonság” kifejezés használatát, amely jogilag homályos és bizonytalanságot szülhet. Az előadó a jogbiztonság javítása érdekében a „kiberbiztonság” helyett inkább az „információbiztonság” használatát javasolja.

MÓDOSÍTÁSOK

Az Állampolgári Jogi, Bel- és Igazságügyi Bizottság felkéri az Ipari, Kutatási és Energiaügyi Bizottságot mint illetékes bizottságot, hogy vegye figyelembe az alábbi módosításokat:

Módosítás 1

Rendeletre irányuló javaslat Cím

A Bizottság által javasolt szöveg

AZ EURÓPAI PARLAMENT ÉS A
TANÁCS RENDELETE

az ENISA-ról, az „Európai **Unió**
Kiberbiztonsági Ügynökségről”,
az 526/2013/EU rendelet hatályon kívül
helyezéséről, valamint az információs és
kommunikációs technológiák
kiberbiztonsági tanúsításáról
(„**kiberbiztonsági** jogszabály”)

Módosítás

AZ EURÓPAI PARLAMENT ÉS A
TANÁCS RENDELETE

az ENISA-ról, az „Európai **Hálózat- és**
Információbiztonsági Ügynökségről”,
az 526/2013/EU rendelet hatályon kívül
helyezéséről, valamint az információs és
kommunikációs technológiák **biztonsági**
tanúsításáról („**informatikai biztonsági**
jogszabály”)

*(Ez a módosítás az egész szövegre
érvényes.)*

Indokolás

A „kiber-” előtag a '60-as évek science-fiction irodalmából származik, és egyre inkább az internet negatív aspektusai (kibertámadás, kiberbűncselekmény stb.) vonatkozásában használják, azonban jelentése jogilag rendkívül homályos. Az előadó a jogbiztonság javítása érdekében a „kiberbiztonság” helyett az „informatikai biztonság” használatát javasolja.

Módosítás 2

Rendeletre irányuló javaslat 2 preambulumbekkezdés

A Bizottság által javasolt szöveg

(2) A hálózati és információs

Módosítás

(2) A hálózati és információs

rendszerek használata szerte az EU-ban széles körben elterjedt, mind a magánszemélyek, mind a vállalkozások, mind pedig a közigazgatási szervek körében. Folyamatosan nő azoknak a termékeknek és szolgáltatásoknak a száma, amelyek alapvető jellemzői a digitalizálás és a hálózatba rendeződés, és a dolgok internete is egyre elterjedtebbé válik, így a következő évtizedben várhatóan több millió, ha nem több milliárd összekapcsolt digitális eszközt fognak az EU-ban használatba venni. Egyre több berendezés kapcsolódik az internethez, de mivel ezen eszközök alapértelmezetten nincsenek megfelelő biztonsági és ellenálló képességi szintet biztosító elemekkel ellátva, **kiberbiztonsági szempontból nem teljesen megbízhatók**. A tanúsítás korlátozott használata következtében így sem **az intézményi**, sem a magánfelhasználók nem rendelkeznek kellő információval az IKT-termékek és -szolgáltatások **kiberbiztonsági** jellemzőiről, ami a digitális megoldásokba vetett bizalom megrendüléséhez vezethet.

rendszerek használata szerte az EU-ban széles körben elterjedt, mind a magánszemélyek, mind a vállalkozások, mind pedig a közigazgatási szervek körében. Folyamatosan nő azoknak a termékeknek és szolgáltatásoknak a száma, amelyek alapvető jellemzői a digitalizálás és a hálózatba rendeződés, és a dolgok internete is egyre elterjedtebbé válik, így a következő évtizedben várhatóan több millió, ha nem több milliárd összekapcsolt digitális eszközt fognak az EU-ban használatba venni. Egyre több berendezés kapcsolódik az internethez, de mivel ezen eszközök alapértelmezetten nincsenek megfelelő biztonsági és ellenálló képességi szintet biztosító elemekkel ellátva, **az informatikai biztonság szintje nem lesz megfelelő**. A tanúsítás korlátozott és **széttagolt** használata következtében így sem a **szervezetek**, sem a magánfelhasználók nem rendelkeznek kellő információval az IKT-termékek és -szolgáltatások **informatikai biztonsági** jellemzőiről, ami a digitális megoldásokba vetett bizalom megrendüléséhez vezethet. **Az ikt-hálózatok biztosítják a polgárok életének minden aspektusát megkönnyítő és az európai gazdasági növekedés hajtóerejének számító digitális termékek és szolgáltatások gerincét. Annak biztosítása érdekében, hogy a digitális egységes piac célkitűzései maradéktalanul megvalósuljanak, be kell vezetni azokat a létfontosságú technológiai alapelemeket, amelyekre az olyan fontos területek, mint az e-egészségügy, a dolgok internete, a mesterséges intelligencia, a kvantumtechnológia, valamint az intelligens közlekedési és a korszerű gyártási rendszerek támaszkodnak.**

Módosítás 3

Rendeletre irányuló javaslat 4 preambulumbekkezdés

(4) Egyre gyakoribbak a kibertámadások, és az összekapcsoltság következtében a kiberfenyegetéseknek és -támadásoknak egyre kiszolgáltatottabbá váló gazdaság és társadalom fokozottabb védelmet igényel. Míg a kibertámadások általában nem ismernek országhatárokat, **a kiberbiztonsági** hatóságok szakpolitikai válaszingázkedése, akárcsak a bünüldözési hatáskörök, túlnyomórészt nemzeti szintűek. A nagyszabású kiberbiztonsági események az egész EU-ban megzavarhatják a legalapvetőbb szolgáltatások nyújtását. Ezért hatékony uniós szintű reagálásra és válságkezelésre van szükség, melynek alapját célirányos szakpolitikai intézkedések és az európai szolidaritást és kölcsönös segítségnyújtást szolgáló gazdagabb eszköztárnak kell képeznie. Ennek megfelelően a politika formálói, a gazdasági élet szereplői és a felhasználók számára egyaránt fontos, hogy megbízható uniós adatok alapján rendszeres értékelés készüljön az EU **kiberbiztonságának** és ellenálló képességének mindenkori helyzetéről, továbbá szisztematikus legyen a jövőben várható fejlemények, kihívások és fenyegetések előrejelzése uniós és globális szinten egyaránt.

(4) Egyre gyakoribbak a kibertámadások, és az összekapcsoltság következtében a kiberfenyegetéseknek és -támadásoknak egyre kiszolgáltatottabbá váló gazdaság és társadalom fokozottabb **és nagyobb biztonságot nyújtó** védelmet igényel. Míg a kibertámadások általában nem ismernek országhatárokat, **az informatikai biztonsági** hatóságok szakpolitikai válaszingázkedése, akárcsak a bünüldözési hatáskörök, túlnyomórészt nemzeti szintűek. A nagyszabású kiberbiztonsági események az egész EU-ban megzavarhatják a legalapvetőbb szolgáltatások nyújtását. Ezért hatékony uniós szintű reagálásra és válságkezelésre van szükség, melynek alapját célirányos szakpolitikai intézkedések és az európai szolidaritást és kölcsönös segítségnyújtást szolgáló gazdagabb eszköztárnak kell képeznie. Ennek megfelelően a politika formálói, a gazdasági élet szereplői és a felhasználók számára egyaránt fontos, hogy megbízható uniós adatok alapján rendszeres értékelés készüljön az EU **informatikai biztonságának** és ellenálló képességének mindenkori helyzetéről, továbbá szisztematikus legyen a jövőben várható fejlemények, kihívások és fenyegetések előrejelzése uniós és globális szinten egyaránt.

Módosítás 4

Rendeletre irányuló javaslat 5 preambulumbekazedés

(5) Az Unió előtt álló egyre nagyobb **kiberbiztonsági** kihívások leküzdéséhez átfogó intézkedéscsomagra van szükség, amely a korábbi uniós fellépésekre épül, és előmozdítja az egymást kölcsönösen erősítő célkitűzéseket. Idetartozik az is, hogy fokozni kell a tagállamok és a

(5) Az Unió előtt álló egyre nagyobb **informatikai biztonsági** kihívások leküzdéséhez átfogó intézkedéscsomagra van szükség, amely a korábbi uniós fellépésekre épül, és előmozdítja az egymást kölcsönösen erősítő célkitűzéseket. Idetartozik az is, hogy

vállalkozások képességeit és felkészültségét, valamint javítani kell az együttműködést és a koordinációt a tagállamok, illetve az uniós intézmények, hivatalok és szervek között. Továbbá, tekintettel a kiberfenyegetések határok nélküli jellegére, a tagállami intézkedések kiegészítése céljával fokozni kell az uniós szintű képességeket, különösen a több országot érintő nagyszabású kiberbiztonsági események és válságok esetére. További erőfeszítésekre van szükség annak érdekében is, hogy a magánszemélyek és a vállalkozások jobban tisztában legyenek **a kiberbiztonsági** kérdésekkel. Emellett a digitális egységes piacba vetett bizalmat is növelni kell azáltal, hogy az IKT-termékek és -szolgáltatások biztonsági szintjéről átlátható információkat bocsátanak rendelkezésre. Ezt a célt könnyebben el lehet érni az egész EU-ra kiterjedő tanúsítással, amely valamennyi tagállam piacán, minden ágazatban közös **kiberbiztonsági** követelményeket és értékelési kritériumokat biztosít.

fokozni kell a tagállamok és a vállalkozások képességeit és felkészültségét, valamint javítani kell az együttműködést és a koordinációt a tagállamok, illetve az uniós intézmények, hivatalok és szervek között. Továbbá, tekintettel a kiberfenyegetések határok nélküli jellegére, a tagállami intézkedések kiegészítése céljával fokozni kell az uniós szintű képességeket, különösen a több országot érintő nagyszabású kiberbiztonsági események és válságok esetére. További erőfeszítésekre van szükség annak érdekében is, hogy **koordinált uniós válasz** **szülessen, valamint hogy** a magánszemélyek és a vállalkozások jobban tisztában legyenek az **informatikai biztonsági** kérdésekkel. Emellett a digitális egységes piacba vetett bizalmat is növelni kell azáltal, hogy az IKT-termékek és -szolgáltatások biztonsági szintjéről átlátható információkat bocsátanak rendelkezésre. Ezt a célt könnyebben el lehet érni az egész EU-ra kiterjedő tanúsítással, amely valamennyi tagállam piacán, minden ágazatban közös **informatikai biztonság** követelményeket és értékelési kritériumokat biztosít. **Az egész EU-ra kiterjedő tanúsításon kívül számos önkéntes intézkedést fogadtak el széles körben a piacon a termék, a szolgáltatás, a felhasználás vagy a szabvány függvényében. Ezeket az intézkedéseket, valamint az iparági alulról felfelé építkező megközelítést – ideértve a biztonsági szempontok szerinti tervezést, a támogatásokat és a nemzetközi szabványokhoz való hozzájárulást – ösztönözni kell.**

Módosítás 5

Rendeletre irányuló javaslat 7 preambulumbekkezdés

A Bizottság által javasolt szöveg

(7) Az Európai Unió már eddig is

Módosítás

(7) Az Európai Unió már eddig is

fontos lépéseket tett **a kiberbiztonság** és a digitális technológiákba vetett bizalom növelése érdekében. 2013-ban uniós szintű kiberbiztonsági stratégia elfogadására került sor, amely irányt szabott az Unió **kiberbiztonsági** fenyegetésekre és kockázatokra adott politikai válaszlépései kidolgozásának. Az európaiak online védelmének javítása érdekében tett erőfeszítései gyanánt az Unió 2016-ban elfogadta az első **kiberbiztonsági** jogalkotási aktust, a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 irányelvet (a továbbiakban: kiberbiztonsági irányelv). A kiberbiztonsági irányelv nemzeti képességekre vonatkozó követelményeket határozott meg **a kiberbiztonság** területén, kialakította az első mechanizmusokat a tagállamok közötti stratégiai és operatív együttműködés elmélyítése érdekében, és a biztonsági intézkedésekre és a biztonsági események bejelentésére vonatkozó kötelezettségeket vezetett be a gazdaság és a társadalom számára létfontosságú területeken, mint például az energia, a közlekedés, a vízellátás, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, a digitális infrastruktúra, valamint a kulcsfontosságú digitális szolgáltatók (keresőprogramok, felhőalapú számítástechnikai szolgáltatások, online piacterek). Az ENISA kulcsfontosságú szerepet kapott ezen irányelv végrehajtásának támogatásában. Emellett a kiberbűnözés elleni hatékony küzdelem az európai biztonsági stratégiában is kiemelt fontosságot élvez, hiszen hozzájárul a magas szintű **kiberbiztonság** elérésének általános céljához.

fontos lépéseket tett **az informatikai biztonság** és a digitális technológiákba vetett bizalom növelése érdekében. 2013-ban uniós szintű kiberbiztonsági stratégia elfogadására került sor, amely irányt szabott az Unió **informatikai biztonsági** fenyegetésekre és kockázatokra adott politikai válaszlépései kidolgozásának. Az európaiak online védelmének javítása érdekében tett erőfeszítései gyanánt az Unió 2016-ban elfogadta az első **informatikai biztonsági** jogalkotási aktust, a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 irányelvet (a továbbiakban: kiberbiztonsági irányelv). A kiberbiztonsági irányelv **megvalósítja a digitális egységes piaci stratégiát, és egyéb eszközökkel együtt, mint például az [Európai Elektronikus Hírközlési Kódexet létrehozó] .../... irányelvvel, az (EU) 2016/679 európai parlamenti és tanácsi rendelettel^{1a}, valamint a 2002/58/EK európai parlamenti és tanácsi irányelvvel^{1b} együtt** nemzeti képességekre vonatkozó követelményeket határozott meg **az informatikai biztonság** területén, kialakította az első mechanizmusokat a tagállamok közötti stratégiai és operatív együttműködés elmélyítése érdekében, és a biztonsági intézkedésekre és a biztonsági események bejelentésére vonatkozó kötelezettségeket vezetett be a gazdaság és a társadalom számára létfontosságú területeken, mint például az energia, a közlekedés, a vízellátás, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, a digitális infrastruktúra, valamint a kulcsfontosságú digitális szolgáltatók (keresőprogramok, felhőalapú számítástechnikai szolgáltatások, online piacterek). Az ENISA kulcsfontosságú szerepet kapott ezen irányelv végrehajtásának támogatásában. Emellett a kiberbűnözés elleni hatékony küzdelem az európai biztonsági stratégiában is kiemelt

fontosságot élvez, hiszen hozzájárul a magas szintű **informatikai biztonság** elérésének általános céljához.

^{1a} Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

^{1b} Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (elektronikus hírközlési adatvédelmi irányelv) (HL L 201., 2002.7.31., 37. o.).

Módosítás 6

Rendeletre irányuló javaslat 8 preambulumbekkezdés

A Bizottság által javasolt szöveg

(8) Ismert tény, hogy a 2013-as uniós kiberbiztonsági stratégia elfogadása és az Ügynökség megbízatásának legutóbbi felülvizsgálata óta az általános politikai kontextus jelentősen megváltozott, a még bizonytalanabb és kevésbé biztonságos globális környezet következtében is. Ezért az új uniós **kiberbiztonsági** politika keretében felül kell vizsgálni az ENISA megbízatását a megváltozott **kiberbiztonsági** ökoszisztémában betöltött szerepének meghatározása érdekében, és biztosítani kell, hogy hatékonyan **hozzájáruljon** a radikálisan új fenyegetésekből fakadó **kiberbiztonsági** kihívásokra adott uniós **reakáláshoz**, hiszen ehhez, amint az az Ügynökség értékeléséből is kiderült, jelenlegi

Módosítás

(8) Ismert tény, hogy a 2013-as uniós kiberbiztonsági stratégia elfogadása és az Ügynökség megbízatásának legutóbbi felülvizsgálata óta az általános politikai kontextus jelentősen megváltozott, a még bizonytalanabb és kevésbé biztonságos globális környezet következtében is. Ezért az új uniós **informatikai biztonsági** politika keretében felül kell vizsgálni az ENISA megbízatását a megváltozott **informatikai biztonsági** ökoszisztémában betöltött szerepének meghatározása érdekében, és biztosítani kell, hogy **vezető szerepet töltsön be, amellyel** hatékonyan **javítja** a radikálisan új fenyegetésekből fakadó **informatikai biztonsági** kihívásokra adott uniós **reakálást**, hiszen ehhez, amint az az Ügynökség értékeléséből is kiderült,

megbízatása nem elegendő.

jelenlegi megbízatása nem elegendő.

Módosítás 7

Rendeletre irányuló javaslat 11 preambulumbekkezdés

A Bizottság által javasolt szöveg

(11) Tekintettel az Unió előtt álló, egyre fokozódó **kiberbiztonsági** kihívásokra, növelni kell az Ügynökség számára elkülönített pénzügyi és emberi erőforrásokat annak érdekében, hogy azok mértéke megfeleljen az Ügynökség kiemelt szerepének, feladatainak és az európai digitális ökoszisztémát védő szervezetek kötelékében betöltött kulcsfontosságú szerepének.

Módosítás

(11) Tekintettel az Unió előtt álló, egyre fokozódó **informatikai biztonsági** kihívásokra, növelni kell az Ügynökség számára elkülönített pénzügyi és emberi erőforrásokat annak érdekében, hogy azok mértéke megfeleljen az Ügynökség kiemelt szerepének, feladatainak és az európai digitális ökoszisztémát védő szervezetek kötelékében betöltött kulcsfontosságú szerepének. **Megfelelően figyelembe kell venni az Ügynökség kapacitásának további fejlesztését.**

Indokolás

Elengedhetetlen, hogy foglalkozzunk az Ügynökség kapacitáshiányával. Törekednünk kell az Ügynökség további fejlesztésére, figyelembe véve, hogy mennyire fontos napjainkban a kiberbiztonság, és még inkább azt, hogy mennyire fontos lesz „holnap”. Itt jegyezzük meg a választásokba történő orosz beavatkozást, a világ szuperhatalmai és államai kapacitásának növekedését, valamint a jelentős iparágak elkerülhetetlen digitalizálódását.

Módosítás 8

Rendeletre irányuló javaslat 11 a preambulumbekkezdés (új)

A Bizottság által javasolt szöveg

Módosítás

(11a) Az informatikai biztonság kihívásai a digitális korban gyakran összekapcsolódnak az adatvédelmi kihívásokkal, a magánélet védelmével, valamint az elektronikus kommunikáció védelmével. Annak érdekében, hogy az Ügynökség megfelelően kezelhesse ezeket a kihívásokat, szoros együttműködésre és gyakori konzultációra van szükség a

45/2001/EK európai parlamenti és tanácsi rendeletben^{1a}, az (EU) 2016/679 rendeletben, az (EU) 2016/680 irányelvben, valamint az 1211/2009/EK rendeletben létrehozott szervekkel, valamint az iparági szereplőkkel és a civil társadalommal.

^{1a} 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.).

Módosítás 9

Rendelethez irányuló javaslat 12 preambulumbekkezdés

A Bizottság által javasolt szöveg

(12) Az Ügynökségnek magas szintű szakértelmet kell kialakítania és fenntartania, és olyan hivatkozási alapként kell működnie, amely függetlensége, az általa nyújtott tanácsok és az általa terjesztett információk minősége, eljárásainak és működési módszereinek átláthatósága, valamint a feladatai ellátásában tanúsított gondossága révén bizalmat kelt az egységes piac iránt. Az Ügynökségnek proaktívan hozzá kell járulnia a nemzeti és uniós erőfeszítésekhez, és feladatait az uniós intézményekkel, szervekkel és hivatalokkal, valamint a tagállamokkal teljes körű együttműködés keretében kell végeznie. Ezenkívül a magánszektorral, valamint a többi érintett érdekelt féllel is együtt kell működnie, és a tőlük kapott észrevételeket is figyelembe kell vennie. ***Feladatainak leírásával meg kell határozni, hogy az Ügynökségnek hogyan kell céljait elérnie, de egyben***

Módosítás

(12) Az Ügynökségnek magas szintű szakértelmet kell kialakítania és fenntartania, és olyan hivatkozási alapként kell működnie, amely függetlensége, az általa nyújtott tanácsok és az általa terjesztett információk minősége, eljárásainak és működési módszereinek átláthatósága, valamint a feladatai ellátásában tanúsított gondossága révén bizalmat kelt az egységes piac iránt. Az Ügynökségnek proaktívan hozzá kell járulnia a nemzeti és uniós erőfeszítésekhez, és feladatait az uniós intézményekkel, szervekkel és hivatalokkal, valamint a tagállamokkal teljes körű együttműködés keretében kell végeznie. Ezenkívül a magánszektorral, valamint a többi érintett érdekelt féllel is együtt kell működnie, és a tőlük kapott észrevételeket is figyelembe kell vennie. ***Egyértelmű menetrendet kell meghatározni és világosan rögzíteni kell az Ügynökség által teljesítendő***

rugalmasságot is **biztosítani kell működéséhez.**

feladatokat és célokat, megfelelően figyelembe véve a működéséhez szükséges rugalmasságot is. Lehetőség szerint mindenhol a lehető legnagyobb átláthatóságot és információterjesztést kell biztosítani.

Módosítás 10

Rendeletre irányuló javaslat 14 preambulumbekkezdés

A Bizottság által javasolt szöveg

(14) Az Ügynökség alapvető feladata, hogy elősegítse az idevágó jogi keretrendszer következetes végrehajtását, különösen a kiberbiztonsági irányelv eredményes alkalmazását, ami alapvető fontosságú a kibertámadásokkal szembeni ellenálló képesség javításához. Tekintettel **a kiberbiztonsági** fenyegetések gyorsan változó természetére, egyértelmű, hogy a tagállamokat több szakpolitikai területet is felölelő, átfogóbb megközelítéssel kell támogatni a kibertámadásokkal szembeni ellenálló képességük kialakítása érdekében.

Módosítás

(14) Az Ügynökség alapvető feladata, hogy elősegítse az idevágó jogi keretrendszer következetes végrehajtását, különösen a kiberbiztonsági irányelv, az **[Európai Elektronikus Hírközlési Kódexet létrehozó] .../... irányelv, az (EU) 2016/679 rendelet, valamint a 2002/58/EK irányelv** eredményes alkalmazását, ami alapvető fontosságú a kibertámadásokkal szembeni ellenálló képesség javításához. Tekintettel **az informatikai biztonsági** fenyegetések gyorsan változó természetére, egyértelmű, hogy a tagállamokat több szakpolitikai területet is felölelő, átfogóbb megközelítéssel kell támogatni a kibertámadásokkal szembeni ellenálló képességük kialakítása érdekében.

Módosítás 11

Rendeletre irányuló javaslat 21 a preambulumbekkezdés (új)

A Bizottság által javasolt szöveg

Módosítás

(21a) A Bizottságnak javaslatot kell tennie a tagállamok kötelező együttműködésére a kritikus információs infrastruktúrák védelme tekintetében.

Módosítás 12

Rendeletre irányuló javaslat

26 preambulumbekzdés

A Bizottság által javasolt szöveg

(26) *A kiberbiztonság* területén jelentkező kihívások jobb megértése érdekében, valamint a tagállamoknak és az uniós intézményeknek nyújtott hosszú távú stratégiai tanácsadás céljából az Ügynökségnek elemeznie kell mind a már ismert, mind az új keletű kockázatokat. E célból az Ügynökségnek a tagállamokkal és adott esetben a statisztikai hivatalokkal és más szervekkel együttműködésben össze kell gyűjtenie a releváns információkat, elemzéseket kell készítenie az új technológiákról, valamint tematikus értékeléseket kell végeznie a technológiai innovációknak a hálózat- és információbiztonságra, azon belül is különösen *a kiberbiztonságra* gyakorolt várható társadalmi, jogi, gazdasági és szabályozási hatásairól. Az Ügynökségnek továbbá a fenyegetések és biztonsági események elemzésével támogatnia kell a tagállamokat és az uniós intézményeket, hivatalokat és szerveket az új tendenciák azonosításában és *a kiberbiztonsággal* kapcsolatos problémák megelőzésében.

Módosítás

(26) *Az informatikai biztonság* területén jelentkező kihívások jobb megértése érdekében, valamint a tagállamoknak és az uniós intézményeknek nyújtott hosszú távú stratégiai tanácsadás céljából az Ügynökségnek elemeznie kell mind a már ismert, mind az új keletű kockázatokat, ***biztonsági eseményeket és sebezhetőségeket***. E célból az Ügynökségnek a tagállamokkal és adott esetben a statisztikai hivatalokkal és más szervekkel együttműködésben össze kell gyűjtenie a releváns információkat, elemzéseket kell készítenie az új technológiákról, valamint tematikus értékeléseket kell végeznie a technológiai innovációknak a hálózat- és információbiztonságra, azon belül is különösen ***az informatikai biztonságra*** gyakorolt várható társadalmi, jogi, gazdasági és szabályozási hatásairól. Az Ügynökségnek továbbá a fenyegetések, ***a*** biztonsági események ***és a sebezhetőségek*** elemzésével támogatnia kell a tagállamokat és az uniós intézményeket, hivatalokat és szerveket az új tendenciák azonosításában és ***az informatikai biztonsággal*** kapcsolatos problémák megelőzésében.

Módosítás 13

Rendeletre irányuló javaslat

28 preambulumbekzdés

A Bizottság által javasolt szöveg

(28) Az Ügynökségnek hozzá kell járulnia *a kiberbiztonsági* kockázatokkal kapcsolatos tudatosság növeléséhez, és magánszemélyeknek és szervezeteknek címzett, egyedi felhasználói iránymutatást kell nyújtania a már bevált módszerekkel kapcsolatban. *Az* egyéni felhasználók és

Módosítás

(28) Az Ügynökségnek hozzá kell járulnia ***az informatikai biztonsági*** kockázatokkal kapcsolatos tudatosság növeléséhez, és magánszemélyeknek és szervezeteknek címzett, egyedi felhasználói iránymutatást kell nyújtania a már bevált módszerekkel kapcsolatban. ***Az***

szervezetek szintjén azáltal is hozzá kell járulnia a bevált módszerek és megoldások előmozdításához, hogy összegyűjti és elemzi a jelentős biztonsági eseményekre vonatkozó, nyilvánosan elérhető információkat, valamint jelentéseket készít abból a célból, hogy útmutatást nyújtson a vállalkozások és a magánszemélyek számára, **valamint javítsa a felkészültség és az ellenálló képesség általános szintjét.** Emellett a tagállamokkal és az uniós intézményekkel, szervekkel és hivatalokkal folytatott együttműködésben rendszeresen kampányokat kell szerveznie a végfelhasználók tájékoztatása és oktatása érdekében, **melyek** célja a biztonságosabb egyéni online magatartásformák elősegítése, valamint a virtuális térben potenciálisan jelenlévő veszélyek tudatosítása – ideértve az adathalászatot, a botneteket, a pénzügyi és banki csalásokat is magában foglaló kiberbűnözést is –, továbbá az alapvető **hitelesítési és adatvédelmi tanácsadás nyújtása.** Az Ügynökségnek központi szerepet kell játszania az eszközök biztonságosságával kapcsolatos végfelhasználói tudatosság minél gyorsabb növelésében.

általános felkészültség és ellenálló képesség javítása érdekében az Ügynökségnek az egyéni felhasználók és szervezetek szintjén azáltal is hozzá kell járulnia a bevált módszerek és megoldások előmozdításához, hogy összegyűjti és elemzi a jelentős biztonsági eseményekre vonatkozó, nyilvánosan elérhető információkat, valamint jelentéseket készít abból a célból, hogy útmutatást nyújtson a vállalkozások, a magánszemélyek és a **releváns uniós és nemzeti szintű hatóságok számára.** Emellett a tagállamokkal és az uniós intézményekkel, szervekkel és hivatalokkal folytatott együttműködésben rendszeresen kampányokat kell szerveznie a végfelhasználók tájékoztatása és oktatása érdekében. **Ezen kampányok** célja az **informatikai biztonsággal kapcsolatos oktatás és** a biztonságosabb egyéni online magatartásformák elősegítése, valamint a virtuális térben potenciálisan jelenlévő veszélyek tudatosítása – ideértve az adathalászatot, a botneteket, a pénzügyi és banki csalásokat, **valamint a hamisítást és az illegális tartalmakat is** magában foglaló kiberbűnözést is –, továbbá az **adatvédelem előmozdítása és az adat- és személyazonosság-lopás megelőzésére irányuló alapvető hitelesítés.** Az Ügynökségnek központi szerepet kell játszania az eszközök biztonságosságával kapcsolatos végfelhasználói tudatosság minél gyorsabb növelésében.

Módosítás 14

Rendeletre irányuló javaslat 28 a preambulumbekkezdés (új)

A Bizottság által javasolt szöveg

Módosítás

(28a) Az Ügynökségnek tudatosítania kell a nyilvánosság körében az adatcsalási biztonsági események és lopások kockázatait, amelyek súlyosan befolyásolhatják az egyének alapvető

jogait, továbbá veszélyeztethetik a jogállamiságot és a demokratikus társadalmak stabilitását, beleértve a tagállamokban lévő demokratikus folyamatokat is.

Módosítás 15

Rendeletre irányuló javaslat 30 preambulumbekkezdés

A Bizottság által javasolt szöveg

(30) Célkitűzéseinek maradéktalan elérése érdekében az Ügynökségnek kapcsolatot kell kialakítania a megfelelő intézményekkel, hivatalokkal és szervekkel, többek között a CERT-EU-val, az Europol keretében működő Számítástechnikai Bűnözés Elleni Európai Központtal (EC3), az Európai Védelmi Ügynökséggel (EDA), a nagy méretű informatikai rendszerek operatív irányításával foglalkozó európai ügynökséggel (eu-LISA), az Európai Repülésbiztonsági Ügynökséggel (EASA) és **a kiberbiztonságban** érintett bármely más uniós ügynökségekkel. Kapcsolatot kell fenntartania továbbá az adatvédelmi hatóságokkal is a szakismeretek és a bevált módszerek megosztása érdekében, valamint azért, hogy tanácsokat tudjon adni **a kiberbiztonság** azon vonatkozásaival kapcsolatban, amelyek hatással lehetnek a hatóságok munkájára. A nemzeti és uniós bűnüldöző és adatvédelmi hatóságok képviselőinek lehetőséget kell biztosítani arra, hogy képviseltessék magukat az Ügynökséghez tartozó érdekelték állandó csoportjában. Az Ügynökségnek a bűnüldözési szervekkel a munkájukra esetlegesen hatást gyakorló hálózat- és információbiztonsági kérdésekre vonatkozóan folytatott együttműködés során tiszteletben kell tartania a meglévő információs csatornákat és a létező hálózatokat.

Módosítás

(30) Célkitűzéseinek maradéktalan elérése érdekében az Ügynökségnek kapcsolatot kell kialakítania a megfelelő intézményekkel, hivatalokkal és szervekkel, többek között a CERT-EU-val, az Europol keretében működő Számítástechnikai Bűnözés Elleni Európai Központtal (EC3), az Európai Védelmi Ügynökséggel (EDA), a nagy méretű informatikai rendszerek operatív irányításával foglalkozó európai ügynökséggel (eu-LISA), az Európai Repülésbiztonsági Ügynökséggel (EASA), **az Európai GNSS Ügynökséggel (GSA) és az informatikai biztonságban** érintett bármely más uniós ügynökségekkel. Kapcsolatot kell fenntartania továbbá az **európai és nemzeti** adatvédelmi hatóságokkal is a szakismeretek és a bevált módszerek megosztása érdekében, valamint azért, hogy tanácsokat tudjon adni **az informatikai biztonság** azon vonatkozásaival kapcsolatban, amelyek hatással lehetnek a hatóságok munkájára. A nemzeti és uniós bűnüldöző és adatvédelmi hatóságok képviselőinek lehetőséget kell biztosítani arra, hogy képviseltessék magukat az Ügynökséghez tartozó érdekelték állandó csoportjában. Az Ügynökségnek a bűnüldözési szervekkel a munkájukra esetlegesen hatást gyakorló hálózat- és információbiztonsági kérdésekre vonatkozóan folytatott együttműködés során tiszteletben kell tartania a meglévő információs csatornákat

és a létező hálózatokat.

Indokolás

Mivel a Galileo kiberbiztonsági kérdéseket vet fel, különösen a földi szegmensei vonatkozásában, a GNSS Ügynökséggel történő együttműködés erősíti az ENISA szerepét, miközben növeli a Galileo hitelességét.

Módosítás 16

Rendeletre irányuló javaslat 35 preambulumbekkezdés

A Bizottság által javasolt szöveg

(35) Az Ügynökségnek ösztönöznie kell a tagállamokat **és a** szolgáltatókat általános biztonsági előírásaik javítására, hogy minden internetfelhasználó megtehesse a személyes **kiberbiztonságához** szükséges lépéseket. Különösen fontos, hogy a szolgáltatók és a termékek gyártói visszavonják vagy újrahasznosítsák azokat a termékeket és szolgáltatásokat, amelyek nem felelnek meg **a kiberbiztonsági** szabványoknak. Az ENISA az illetékes hatóságokkal együttműködve tájékoztatást adhat a belső piacon kínált termékek és szolgáltatások **kiberbiztonsági** szintjéről, és figyelmeztetéseket is kiadhat, amelyekben a szolgáltatókat és a gyártókat szolgáltatásaik és termékeik biztonságának fokozására – **ideértve a kiberbiztonságot is** – szólítja fel.

Módosítás

(35) Az Ügynökségnek ösztönöznie kell a tagállamokat, **a hardver- és szoftvergyártókat, valamint az ikt- és online** szolgáltatókat általános biztonsági előírásaik javítására, hogy minden internetfelhasználó megtehesse a személyes **informatikai biztonságához** szükséges lépéseket. Különösen fontos, hogy a szolgáltatók és a termékek gyártói visszavonják vagy újrahasznosítsák azokat a termékeket és szolgáltatásokat, amelyek nem felelnek meg **az informatikai biztonsági** szabványoknak. Az ENISA az illetékes hatóságokkal együttműködve tájékoztatást adhat a belső piacon kínált termékek és szolgáltatások **informatikai biztonsági** szintjéről, és figyelmeztetéseket is kiadhat, amelyekben a szolgáltatókat és a gyártókat szolgáltatásaik és termékeik **informatikai** biztonságának fokozására szólítja fel. **Az Ügynökségnek együtt kell működnie az érdekelt felekkel egy, az egész Unióra kiterjedő megközelítés létrehozása érdekében a sebezhetőségek felelős nyilvánosságra hozatala tekintetében, előmozdítva a bevált gyakorlatokat ezen a területen.**

Módosítás 17

Rendeletre irányuló javaslat

44 preambulumbekkezdés

A Bizottság által javasolt szöveg

(44) A magánszektorral, a fogyasztói szervezetekkel és más érdekeltekkel való rendszeres párbeszéd biztosítása céljából az Ügynökségen belül tanácsadó szervként indokolt létrehozni az érdekeltek állandó csoportját. Az érdekeltek állandó csoportjának, amelyet az ügyvezető igazgató javaslata alapján az igazgatótanács állít fel, az a feladata, hogy az érdekeltek számára fontos kérdésekre összpontosítson, illetve felhívja az Ügynökség figyelmét ezekre. Az érdekeltek állandó csoportjának összetételét és a csoportra bízott feladatokat, melyek közül a legfontosabb a munkaprogram-tervezet véleményezése, úgy kell meghatározni, hogy az érdekelt felek az Ügynökség munkájában megfelelő módon képviselve legyenek.

Módosítás

(44) A magánszektorral, a fogyasztói szervezetekkel és más érdekeltekkel való rendszeres párbeszéd biztosítása céljából az Ügynökségen belül tanácsadó szervként indokolt létrehozni az érdekeltek állandó csoportját. Az érdekeltek állandó csoportjának, amelyet az ügyvezető igazgató javaslata alapján az igazgatótanács állít fel, az a feladata, hogy az érdekeltek számára fontos kérdésekre összpontosítson, illetve felhívja az Ügynökség figyelmét ezekre. Az érdekeltek állandó csoportjának összetételét és a csoportra bízott feladatokat, melyek közül a legfontosabb a munkaprogram-tervezet véleményezése, úgy kell meghatározni, hogy az érdekelt felek az Ügynökség munkájában megfelelő módon képviselve legyenek. ***Tekintettel a dolgok internetébe fektetett bizalom biztosítását célzó tanúsítási követelmények fontosságára, a Bizottságnak kifejezetten mérlegelnie kell olyan intézkedések végrehajtását, amelyek biztosítják az egész EU-ra kiterjedő biztonsági szabványok harmonizálását a dolgok internetével kapcsolatos eszközök számára.***

Módosítás 18

Rendeletre irányuló javaslat 50 preambulumbekkezdés

A Bizottság által javasolt szöveg

(50) Jelenleg az IKT-termékek és -szolgáltatások esetében csak korlátozott mértékben alkalmazzák ***a kiberbiztonsági*** tanúsítást. Ha igen, akkor is főként tagállami szinten vagy az ágazat kezdeményezésére kialakított rendszerek keretében kerül sor erre. A valamely nemzeti ***kiberbiztonsági*** hatóság által kiadott tanúsítványt tehát főszabály szerint

Módosítás

(50) Jelenleg az IKT-termékek és -szolgáltatások esetében csak korlátozott mértékben alkalmazzák ***az informatikai biztonsági*** tanúsítást. Ha igen, akkor is főként tagállami szinten vagy az ágazat kezdeményezésére kialakított rendszerek keretében kerül sor erre. A valamely nemzeti ***informatikai biztonsági*** hatóság által kiadott tanúsítványt tehát főszabály

a többi tagállam nem ismeri el. A vállalatoknak így működésük helye szerint több tagállamban is tanúsíttatniuk kell termékeiket és szolgáltatásaikat, ha például nemzeti közbeszerzési eljárásokban kívánnak részt venni. Mindemellett, míg egyre újabb és újabb rendszerek jönnek létre, a horizontális **kiberbiztonsági** kérdések tekintetében – például a dolgok internetét illetően – nincs egységes és holisztikus megközelítés. A meglévő rendszerek az érintett termékek köre, a biztonsági szintek, az alapvető kritériumok és a gyakorlati felhasználás tekintetében jelentős hiányosságokat és különbségeket mutatnak.

szerint a többi tagállam nem ismeri el. A vállalatoknak így működésük helye szerint több tagállamban is tanúsíttatniuk kell termékeiket és szolgáltatásaikat, ha például nemzeti közbeszerzési eljárásokban kívánnak részt venni, **ami további költségeket róhat a vállalkozásokra**. Mindemellett, míg egyre újabb és újabb rendszerek jönnek létre, a horizontális **informatikai biztonsági** kérdések tekintetében – például a dolgok internetét illetően – nincs egységes és holisztikus megközelítés. A meglévő rendszerek az érintett termékek köre, a biztonsági szintek, az alapvető kritériumok és a gyakorlati felhasználás tekintetében jelentős hiányosságokat és különbségeket mutatnak. **Eseti megközelítésre van szükség annak biztosítása érdekében, hogy a szolgáltatások és a termékek megfelelő tanúsítási rendszerek hatálya alá tartozzanak. Ezenkívül kockázatalapú megközelítésre van szükség a kockázatok hatékony azonosítása és mérséklése, valamint annak elkerülése érdekében, hogy a gyártóknak túl nagy költségei legyenek.**

Módosítás 19

Rendeletre irányuló javaslat 52 preambulumbekzdés

A Bizottság által javasolt szöveg

(52) A fentiek alapján szükségesnek mutatkozik egy olyan európai **kiberbiztonsági** tanúsítási keretrendszer létrehozása, amely megállapítja, hogy milyen fő horizontális követelményeket kell kidolgozni az európai **kiberbiztonsági** tanúsítási rendszerekre vonatkozóan, és lehetővé teszi az IKT-termékek és -szolgáltatások tanúsítványainak valamennyi tagállamban történő elismerését és használatát. Az európai keretrendszernek kettős célt kell szolgálnia: egyrészt növelnie kell az ilyen

Módosítás

(52) A fentiek alapján szükségesnek mutatkozik egy olyan **harmonizált** európai **informatikai biztonsági** tanúsítási keretrendszer létrehozása, amely megállapítja, hogy milyen fő horizontális követelményeket kell kidolgozni az európai **informatikai biztonsági** tanúsítási rendszerekre vonatkozóan, és lehetővé teszi az IKT-termékek és -szolgáltatások tanúsítványainak valamennyi tagállamban történő elismerését és használatát. Az európai keretrendszernek kettős célt kell szolgálnia: egyrészt növelnie kell az ilyen

rendszerek alapján tanúsított IKT-termékek és -szolgáltatások iránti bizalmat. Másrészt az is célja, hogy ne legyenek egymásnak ellentmondó vagy egymással átfedő nemzeti **kiberbiztonsági** tanúsítványok, vagyis csökkenjenek a digitális egységes piacon működő vállalkozások költségei. A rendszereknek megkülönböztetésmentesnek kell lenniük, és nemzetközi és/vagy uniós szabványokon kell alapulniuk, kivéve, ha ezek a szabványok nem hatékonyak vagy nem alkalmasak az EU e tekintetben kitűzött legitim céljainak teljesítésére.

rendszerek alapján tanúsított IKT-termékek és -szolgáltatások iránti bizalmat. Másrészt az is célja, hogy ne legyenek egymásnak ellentmondó vagy egymással átfedő nemzeti **informatikai biztonsági** tanúsítványok, vagyis csökkenjenek a digitális egységes piacon működő vállalkozások költségei. A rendszereknek megkülönböztetésmentesnek kell lenniük, és nemzetközi és/vagy uniós szabványokon kell alapulniuk, kivéve, ha ezek a szabványok nem hatékonyak vagy nem alkalmasak az EU e tekintetben kitűzött legitim céljainak teljesítésére.

Módosítás 20

Rendeletre irányuló javaslat 55 preambulumbekzdés

A Bizottság által javasolt szöveg

(55) Az európai **kiberbiztonsági** tanúsítási rendszerek célja annak biztosítása, hogy az ilyen rendszerek keretében tanúsított IKT-termékek és -szolgáltatások megfeleljenek a meghatározott követelményeknek. E követelmények az olyan tevékenységekkel szembeni ellenálló képességet érintik egy adott biztonsági szinten, amelyek célja, hogy veszélyeztessék az e rendelet szerinti termékek, eljárások, szolgáltatások és rendszerek által tárolt vagy továbbított vagy feldolgozott adatok, illetve az említett termékek, eljárások, szolgáltatások és rendszerek által biztosított vagy elérhetővé tett kapcsolódó funkciók vagy szolgáltatások hozzáférhetőségét, hitelességét, sértetlenségét és titkosságát. Lehetetlenség ebben a rendeletben az összes IKT-termék és -szolgáltatás vonatkozásában részletesen meghatározni **a kiberbiztonsági** követelményeket. Az IKT-termékek és -szolgáltatások, valamint a kapcsolódó **kiberbiztonsági** igények olyan különbözök, hogy nagyon nehéz minden eshetőségre érvényes általános

Módosítás

(55) Az európai **informatikai biztonsági** tanúsítási rendszerek célja annak biztosítása, hogy az ilyen rendszerek keretében tanúsított IKT-termékek és -szolgáltatások megfeleljenek a meghatározott követelményeknek. E követelmények az olyan tevékenységekkel szembeni ellenálló képességet érintik egy adott biztonsági szinten, amelyek célja, hogy veszélyeztessék az e rendelet szerinti termékek, eljárások, szolgáltatások és rendszerek által tárolt vagy továbbított vagy feldolgozott adatok, illetve az említett termékek, eljárások, szolgáltatások és rendszerek által biztosított vagy elérhetővé tett kapcsolódó funkciók vagy szolgáltatások hozzáférhetőségét, hitelességét, sértetlenségét és titkosságát. Lehetetlenség ebben a rendeletben az összes IKT-termék és -szolgáltatás vonatkozásában részletesen meghatározni **az informatikai biztonsági** követelményeket. Az IKT-termékek és -szolgáltatások, valamint a kapcsolódó **informatikai biztonsági** igények **és ezek életciklusa** olyan különbözök, hogy

kiberbiztonsági követelményeket kialakítani. Ezért a tanúsítás céljára tág és általános **kiberbiztonság-fogalmat** kell elfogadni, amelyet az európai **kiberbiztonsági** tanúsítási rendszerek kidolgozása során figyelembe veendő, egyedi **kiberbiztonsági** célkitűzések egészítenek ki. Az, hogy ezeket a célkitűzéseket egyes IKT-termékek és -szolgáltatások esetében hogyan kell elérni, részleteiben a Bizottság által elfogadott egyedi tanúsítási rendszerek szintjén kerül meghatározásra, például szabványokra vagy műszaki előírásokra való hivatkozás révén.

nagyon nehéz minden eshetőségre érvényes általános **informatikai biztonsági** követelményeket kialakítani. Ezért a tanúsítás céljára tág és általános **informatikaibiztonság-fogalmat** kell elfogadni, amelyet az európai **informatikai biztonsági** tanúsítási rendszerek kidolgozása során figyelembe veendő, egyedi **informatikai biztonsági** célkitűzések egészítenek ki. Az, hogy ezeket a célkitűzéseket egyes IKT-termékek és -szolgáltatások esetében hogyan kell elérni, részleteiben a Bizottság által – **a tagállamokkal és az ipari érdekelt felekkel folytatott szoros konzultáció során** – elfogadott egyedi tanúsítási rendszerek szintjén kerül meghatározásra, például szabványokra vagy műszaki előírásokra való hivatkozás révén. **Az egyéni tanúsítási rendszereket úgy kell megtervezni, hogy az érintett IT-termékek és -szolgáltatások fejlesztésében részt vevő összes szereplőt ösztönözzék az olyan szabványok, normák és alapelvek kidolgozására és elfogadására, amelyek a teljes életciklus során a lehető legmagasabb biztonsági szintet biztosítják.**

Módosítás 21

Rendeletre irányuló javaslat 55 a preambulumbekzdés (új)

A Bizottság által javasolt szöveg

Módosítás

(55a) Az ENISA-nak ki kell dolgoznia egy globális perspektívájú tanúsítási rendszert a jövőbeli kereskedelmi akadályok kiküszöbölése érdekében. A tanúsítási rendszer kritériumainak kidolgozása során az ENISA-nak párbeszédet kell folytatnia az érintett ágazati partnerekkel a piaci megvalósíthatóság biztosítása érdekében.

Módosítás 22

Rendeletre irányuló javaslat 56 preambulumbekkezdés

A Bizottság által javasolt szöveg

(56) A Bizottságot fel kell hatalmazni arra, hogy felkérhesse az ENISA-t meghatározott IKT-termékekkel vagy -szolgáltatásokkal kapcsolatos rendszerekre irányuló javaslatok kidolgozására. A Bizottságnak ezt követően felhatalmazást kell kapnia arra, hogy végrehajtási jogi aktusok útján – az ENISA által javasolt rendszer alapján – elfogadja az európai **kiberbiztonsági** tanúsítási rendszert. Figyelemmel az e rendelet általános céljára és a benne megállapított biztonsági célkitűzésekre, a Bizottság által elfogadott európai **kiberbiztonsági** tanúsítási rendszereknek az egyes rendszerek tárgyát, alkalmazási körét és működését érintő bizonyos elemeket meg kell határozniuk. Ezeknek többek között a következőket kell magukban foglalniuk: **a kiberbiztonsági** tanúsítás hatályát és tárgyát, ideértve a hatálya alá tartozó IKT-termékek és -szolgáltatások kategóriáit, **a kiberbiztonsági** követelmények részletes leírását, például szabványokra vagy műszaki előírásokra való hivatkozások révén, az egyedi értékelési kritériumokat és értékelési módszereket, valamint a biztonság tervezett szintjét (alapvető, jelentős és/vagy magas).

Módosítás

(56) A Bizottságot fel kell hatalmazni arra, hogy felkérhesse az ENISA-t meghatározott IKT-termékekkel vagy -szolgáltatásokkal kapcsolatos rendszerekre irányuló javaslatok kidolgozására. A Bizottságnak ezt követően felhatalmazást kell kapnia arra, hogy végrehajtási jogi aktusok útján – az ENISA által javasolt rendszer alapján – elfogadja az európai **informatikai biztonsági** tanúsítási rendszert. Figyelemmel az e rendelet általános céljára és a benne megállapított biztonsági célkitűzésekre, a Bizottság által elfogadott európai **informatikai biztonsági** tanúsítási rendszereknek az egyes rendszerek tárgyát, alkalmazási körét és működését érintő bizonyos elemeket meg kell határozniuk. Ezeknek többek között a következőket kell magukban foglalniuk: **az informatikai biztonsági** tanúsítás hatályát és tárgyát, ideértve a hatálya alá tartozó IKT-termékek és -szolgáltatások kategóriáit, **az informatikai biztonsági** követelmények részletes leírását, például szabványokra vagy műszaki előírásokra való hivatkozások révén, az egyedi értékelési kritériumokat és értékelési módszereket, valamint a biztonság tervezett szintjét (alapvető, jelentős és/vagy magas). **A biztonsági szinteket egyedi alapon kell meghatározni, biztosítva, hogy az IKT-szolgáltatásokra és -termékekre megfelelő tanúsítási rendszerek vonatkozzanak, figyelembe véve a különféle egyedi felhasználási eseteket, valamint a felhasználók saját felelősségét és képzettségét.**

Módosítás 23

Rendeletre irányuló javaslat 57 preambulumbekkezdés

(57) Az uniós és nemzeti jogszabályok eltérő rendelkezései hiányában az európai **kiberbiztonsági** tanúsítás igénybevételének továbbra is önkéntes alapon kell történnie. E rendelet céljainak elérése és a belső piac széttagoltságának megakadályozása érdekében azonban az európai **kiberbiztonsági** tanúsítási rendszer hatálya alá tartozó IKT-termékekre és -szolgáltatásokra vonatkozó nemzeti **kiberbiztonsági** tanúsítási rendszerek és eljárások a Bizottság által a végrehajtási jogi aktusban meghatározott időponttól kezdve nem keletkeztethetnek joghatást. Emellett a tagállamok nem vezethetnek be olyan új nemzeti tanúsítási rendszereket, amelyek már valamelyik hatályos európai **kiberbiztonsági** tanúsítási rendszer tárgyát képező IKT-termékek és -szolgáltatások tekintetében szolgálnak **kiberbiztonsági** tanúsítási rendszerként.

(57) Az uniós és nemzeti jogszabályok eltérő rendelkezései hiányában az európai **informatikai biztonsági** tanúsítás igénybevételének továbbra is önkéntes alapon kell történnie. **Ezen kezdeti szakasz után és a tagállamokban történő végrehajtás szintjétől és a termék vagy szolgáltatás kritikus jellegétől függően fokozatos megközelítéssel esetleg kötelező tanúsítási rendszereket lehet bevezetni bizonyos IKT-termékek és -szolgáltatások esetében a jövőbeli technológiák és szakpolitikai célkitűzésekre adott válaszok vonatkozásában.** E rendelet céljainak elérése és a belső piac széttagoltságának megakadályozása érdekében azonban az európai **informatikai biztonsági** tanúsítási rendszer hatálya alá tartozó IKT-termékekre és -szolgáltatásokra vonatkozó nemzeti **informatikai biztonsági** tanúsítási rendszerek és eljárások a Bizottság által a végrehajtási jogi aktusban meghatározott időponttól kezdve nem keletkeztethetnek joghatást. Emellett a tagállamok nem vezethetnek be olyan új nemzeti tanúsítási rendszereket, amelyek már valamelyik hatályos európai **informatikai biztonsági** tanúsítási rendszer tárgyát képező IKT-termékek és -szolgáltatások tekintetében szolgálnak **informatikai biztonsági** tanúsítási rendszerként.

Módosítás 24

Rendeletre irányuló javaslat 58 a preambulumbekkezdés (új)

(58a) Az Ügynökségnek egyértelmű alapvető informatikai biztonsági követelményeket kell kidolgoznia és adott esetben végrehajtási jogi aktusként javasolnia a Bizottság számára az Unióban értékesített vagy onnan exportált valamennyi informatikai eszköz

vonatkozásában. Ezt követően e követelményeket kétfévente felül kell vizsgálni a folyamatos fejlődés érdekében. Ezek az alapvető informatikai biztonsági követelmények többek között előírják, hogy az eszközök nem tartalmazhatnak semmilyen ismert sebezhetőséget, hogy képesek legyenek megbízható biztonsági frissítések fogadására, valamint hogy az eladó tájékoztatja az illetékes hatóságokat minden megismert sebezhetőségről és megjavítja vagy kicseréli az érintett eszközt egészen addig, amíg a gyártó egyértelművé nem teszi, hogy az adott eszköz biztonsági támogatása véget ér.

Módosítás 25

Rendeletre irányuló javaslat 1 cikk – 1 bekezdés – b pont

A Bizottság által javasolt szöveg

b) meghatározza az európai **kiberbiztonsági** tanúsítási rendszerek létrehozásának keretrendszerét annak érdekében, hogy az Unión belül biztosítsa az IKT-termékek és -szolgáltatások megfelelő **kiberbiztonsági** szintjét. Ez a keretrendszer az egyéb uniós jogi aktusokban az önkéntes vagy kötelező tanúsításra vonatkozóan előírt különös rendelkezések sérelme nélkül alkalmazandó.

Módosítás

b) meghatározza az európai **informatikai biztonsági** tanúsítási rendszerek létrehozásának keretrendszerét annak érdekében, hogy az Unión belül biztosítsa az IKT-termékek és -szolgáltatások megfelelő **informatikai biztonsági** szintjét. Ez a keretrendszer az egyéb uniós jogi aktusokban az önkéntes vagy kötelező tanúsításra vonatkozóan előírt különös rendelkezések sérelme nélkül alkalmazandó.

Indokolás

Pusztán nyelvi módosítás, amely megszünteti a bizottsági szöveg szóhalmazását.

Módosítás 26

Rendeletre irányuló javaslat 2 cikk – 1 bekezdés – 8 pont

A Bizottság által javasolt szöveg

Módosítás

8. „kiberfenyegetés”: bármely olyan lehetséges körülmény vagy esemény, amely kedvezőtlen hatást gyakorolhat a hálózati és információs rendszerekre, azok felhasználóira és az érintett személyekre;

8. „kiberfenyegetés”: bármely olyan lehetséges körülmény, **képesség vagy** esemény, amely kedvezőtlen hatást gyakorolhat a hálózati és információs rendszerekre, azok felhasználóira és az érintett személyekre;

Indokolás

Fontos szempont, különösen ami a fenyegetésértékelést illeti.

Módosítás 27

Rendeletre irányuló javaslat
4 cikk – 3 bekezdés – 1 a albekezdés (új)

A Bizottság által javasolt szöveg

Módosítás

Az Ügynökség feladata az Unió teljes és az egyes tagállamok informatikai biztonsági hálózata kritikus sebezhetőségeinek azonosítása. Abban az esetben, ha az Ügynökség szükségesnek ítéli, ezeket a sebezhetőségeket jelenteni kell az Európai Parlamentnek.

Módosítás 28

Rendeletre irányuló javaslat
4 cikk – 5 bekezdés

A Bizottság által javasolt szöveg

Módosítás

(5) Az Ügynökség fokozza az uniós szintű **kiberbiztonsági** képességeket annak érdekében, hogy kiegészítse a kiberfenyegetések megelőzése és az azokra való reagálás terén tett tagállami intézkedéseket, különösen a több országot érintő biztonsági események esetében.

(5) Az Ügynökség fokozza az uniós szintű **informatikai biztonsági** képességeket annak érdekében, hogy kiegészítse **és támogassa** a kiberfenyegetések megelőzése és az azokra való reagálás terén tett tagállami intézkedéseket, különösen a több országot érintő biztonsági események esetében.

Módosítás 29

Rendeletre irányuló javaslat

4 cikk – 6 bekezdés

A Bizottság által javasolt szöveg

(6) Az Ügynökség előmozdítja a tanúsítás használatát, többek között azáltal, hogy e rendelet III. címével összhangban hozzájárul az uniós szintű **kiberbiztonsági** tanúsítási keretrendszer létrehozásához és fenntartásához annak érdekében, hogy átláthatóbbá tegye az IKT-termékek és -szolgáltatások által nyújtott **kiberbiztonság** szintjét, és megerősítse ezzel a digitális belső piacba vetett bizalmat.

Módosítás

(6) Az Ügynökség előmozdítja a tanúsítás és a szabványosítás használatát, többek között azáltal, **hogy hozzájárul az uniós és nemzetközi informatikai biztonsági szabványok kidolgozásához, valamint** hogy e rendelet III. címével összhangban hozzájárul az uniós szintű **informatikai biztonsági** tanúsítási keretrendszer létrehozásához és fenntartásához annak érdekében, hogy átláthatóbbá tegye az IKT-termékek és -szolgáltatások által nyújtott **informatikai biztonság** szintjét, és megerősítse ezzel a digitális belső piacba vetett bizalmat.

Módosítás 30

Rendeletre irányuló javaslat

4 cikk – 7 bekezdés

A Bizottság által javasolt szöveg

(7) Az Ügynökség elősegíti, **hogy a magánszemélyek és a vállalkozások a kiberbiztonsághoz kapcsolódó kérdésekben nagy mértékben tájékozottak legyenek.**

Módosítás

(7) Az Ügynökség elősegíti **a nagymértékű tájékozottságot az informatikai biztonsági kérdésekkel kapcsolatban.**

Indokolás

A tájékozottságot nemcsak a magánszemélyek és a vállalkozások vonatkozásában kell előmozdítani, hanem a társadalom minden fontos szereplője vonatkozásában, ideértve a hatóságokat és a törvényhozókat is. A módosítás szándékosan hagyja nyitva az ilyen típusú tevékenység címzettjeit.

Módosítás 31

Rendeletre irányuló javaslat

5 cikk – 1 bekezdés – 2 pont

2. segítségnyújtás a tagállamok számára **a kiberbiztonsággal** kapcsolatos uniós szakpolitika és jogszabályok következetes végrehajtásában, különösen az (EU) 2016/1148 irányelv vonatkozásában, többek között vélemények, iránymutatások, tanácsadás nyújtása, továbbá a kockázatkezeléssel, a biztonsági események bejelentésével és az információk megosztásával kapcsolatban bevált módszerek megosztása révén; valamint az e téren bevált módszerek illetékes hatóságok közötti cseréjének elősegítése;

2. segítségnyújtás a tagállamok számára **az informatikai biztonsággal** kapcsolatos uniós szakpolitika és jogszabályok következetes végrehajtásában, különösen az (EU) 2016/1148 irányelv, **az [Európai Elektronikus Hírközlési Kódexet létrehozó] .../... irányelv, az (EU) 2016/679 rendelet, valamint a 2002/58/EK irányelv** vonatkozásában, többek között vélemények, iránymutatások, tanácsadás nyújtása, továbbá a kockázatkezeléssel, a biztonsági események bejelentésével és az információk megosztásával kapcsolatban bevált módszerek megosztása révén; valamint az e téren bevált módszerek illetékes hatóságok közötti cseréjének elősegítése;

Módosítás 32

Rendeletre irányuló javaslat 5 cikk – 1 bekezdés – 2 a pont (új)

2a. a 2016/679/EU rendeletben létrehozott Európai Adatvédelmi Testület támogatása iránymutatások kidolgozásában, amelyek technikai szinten meghatározzák azokat a feltételeket, amelyek lehetővé teszik az adatkezelők számára a személyes adatok informatikai biztonság céljából történő törvényes felhasználását azzal a céllal, hogy megvédjék infrastruktúrájukat az információs rendszereik elleni támadások felderítése és blokkolása által az alábbiakkal összefüggésben:

i. (EU) 2016/679 rendelet;

ii. (EU) 2016/1148 rendelet; és

Módosítás 33

Rendeletre irányuló javaslat
5 cikk – 1 bekezdés – 2 b pont (új)

A Bizottság által javasolt szöveg

Módosítás

2b. *iránymutatások javasolása annak érdekében, hogy az információtechnológiai termékek eladói kellő gondossággal járjanak el a termékeikben és szolgáltatásaikban észlelt informatikai sebezhetőségek időben történő megszüntetése érdekében, elkerülve, hogy felhasználóik kiberfenyegetéseknek legyenek kitéve;*

Módosítás 34

Rendeletre irányuló javaslat
5 cikk – 1 bekezdés – 2 c pont (új)

A Bizottság által javasolt szöveg

Módosítás

2c. *iránymutatások javasolása, pontosan meghatározva az ikt-ökoszisztémákban részt vevő valamennyi érdekelt fél (beleértve a végső felhasználókat is) felelősségi körét és kötelezettségeit;*

Módosítás 35

Rendeletre irányuló javaslat
5 cikk – 1 bekezdés – 2 d pont (új)

A Bizottság által javasolt szöveg

Módosítás

2d. *a nemzeti jogszabályokkal összhangban iránymutatások javasolása a kritikus hálózati infrastruktúrák*

üzemeltetőinek az azon esetekkel kapcsolatos felelősségére vonatkozó szabályozás vonatkozásában, ha a felhasználóikat érintő támadás éri információs rendszereiket amiatt, hogy egyes felhasználók vagy maga az üzemeltető nem járt el kellő gondossággal, vagy ha az üzemeltető nem járt el felelősen az esemény megelőzése vagy a valamennyi felhasználót érintő hatásának enyhítése érdekében;

Módosítás 36

Rendeletre irányuló javaslat
5 cikk – 1 bekezdés – 2 e pont (új)

A Bizottság által javasolt szöveg

Módosítás

2e. iránymutatások javasolása annak korlátozására, hogy a hatóságok „zéró napokat” vásároljanak vagy használjanak informatikai rendszerek elleni támadások érdekében; szoftverellenőrzések támogatása és szakértők finanszírozása;

Módosítás 37

Rendeletre irányuló javaslat
5 cikk – 1 bekezdés – 2 f pont (új)

A Bizottság által javasolt szöveg

Módosítás

2f. iránymutatások javasolása hatóságok, vállalkozások, kutatók, egyetemek és más érintettek számára arra vonatkozóan, hogy a felelős nyilvánosságra hozatal keretében tegyenek közzé minden még nyilvánosan nem ismert kritikus biztonsági sebezhetőséget;

Módosítás 38

Rendeletre irányuló javaslat
5 cikk – 1 bekezdés – 2 g pont (új)

A Bizottság által javasolt szöveg

Módosítás

2g. iránymutatások javasolása az „ellenőrizhető nyílt forráskódot” alkalmazó informatikai megoldások használatának kibővítésére a közférában, valamint az automatikus eszközök kapcsolódó használatára a forráskód vizsgálatának megkönnyítése és a kiskapuk és más lehetséges biztonsági sebezhetőségek hiányának könnyű ellenőrzése érdekében;

Módosítás 39

Rendeletre irányuló javaslat
6 cikk – 1 bekezdés – f a pont (új)

A Bizottság által javasolt szöveg

Módosítás

fa) és szükség esetén együttműködik a nemzeti adatvédelmi felügyeleti hatóságokkal;

Módosítás 40

Rendeletre irányuló javaslat
6 cikk – 2 a bekezdés (új)

A Bizottság által javasolt szöveg

Módosítás

(2a) Az Ügynökség elősegíti egy hosszú távú európai informatikai biztonsági projekt kidolgozását és elindítását a független uniós informatikai biztonsági iparág növekedésének támogatása és az informatikai biztonság valamennyi uniós informatikai fejlesztésbe történő beépítése érdekében.

Az ENISA tanácsot kell adjon a jogalkotóknak azon politikák kialakítása kapcsán, amelyek lehetővé teszik, hogy az EU felzárkózzon a harmadik országok informatikai biztonsági iparához. A projekt léptékének hasonlóan kell lennie a légi közlekedési ágazat korábbi projektjeinek méretéhez (például az Airbus-hoz). Erre van szükség egy erősebb, önálló és megbízható uniós informatikai iparág kialakításához (lásd a Jövő kutatás Osztály (STOA) tanulmányát (PE 614.531)).

Módosítás 41

Rendeletre irányuló javaslat

7 cikk – 5 bekezdés

A Bizottság által javasolt szöveg

(5) **Két vagy több érintett** tagállam kérésére – és kizárólag a jövőbeni biztonsági események megelőzésére vonatkozó tanácsadás céljából – az Ügynökség támogatást nyújt az (EU) 2016/1148 irányelv értelmében jelentős vagy lényeges hatású biztonsági eseményeknek az érintett vállalkozások általi bejelentését követő utólagos technikai vizsgálatához, vagy maga hajtja végre ezt a vizsgálatot. Az Ügynökség az érintett tagállamok egyetértésével a Bizottság kellően indokolt kérésére is végez ilyen vizsgálatot a kettőnél több tagállamot érintő biztonsági események esetében.

A vizsgálat tárgyát és a vizsgálat lefolytatása során követendő eljárást az érintett tagállamok és az Ügynökség határozza meg az ugyanazon biztonsági eseménnyel kapcsolatos, folyamatban lévő bünygyi nyomozás sérelme nélkül. A vizsgálat az Ügynökség által összeállított végleges technikai jelentéssel zárul, amely elsősorban az érintett tagállamok és vállalkozás(ok) által benyújtott és az érintett tagállamokkal egyeztetett információkon és észrevételeken alapul. A jelentésről a jövőbeli biztonsági események megelőzésére vonatkozó ajánlásokra összpontosító összefoglalást kell készíteni,

Módosítás

(5) **Egy** tagállam kérésére – és kizárólag a jövőbeni biztonsági események megelőzésére vonatkozó tanácsadás céljából – az Ügynökség támogatást nyújt az (EU) 2016/1148 irányelv értelmében jelentős vagy lényeges hatású biztonsági eseményeknek az érintett vállalkozások általi bejelentését követő utólagos technikai vizsgálatához, vagy maga hajtja végre ezt a vizsgálatot. Az Ügynökség az érintett tagállamok egyetértésével a Bizottság kellően indokolt kérésére is végez ilyen vizsgálatot a kettőnél több tagállamot érintő biztonsági események esetében.

A vizsgálat tárgyát és a vizsgálat lefolytatása során követendő eljárást az érintett tagállamok és az Ügynökség határozza meg az ugyanazon biztonsági eseménnyel, **vagy egy tagállam nemzetbiztonsági intézkedésével** kapcsolatos, folyamatban lévő bünygyi nyomozás sérelme nélkül. A vizsgálat az Ügynökség által összeállított végleges technikai jelentéssel zárul, amely elsősorban az érintett tagállamok és vállalkozás(ok) által benyújtott és az érintett tagállamokkal egyeztetett információkon és észrevételeken alapul. A jelentésről a jövőbeli biztonsági események

amelyet meg kell osztani a CSIRT-hálózattal.

megelőzésére vonatkozó ajánlásokra
összpontosító összefoglalást kell készíteni,
amelyet meg kell osztani a CSIRT-hálózattal.

Módosítás 42

Rendeletre irányuló javaslat 7 cikk – 8 a bekezdés (új)

A Bizottság által javasolt szöveg

Módosítás

(8a) Az Ügynökségnek uniós intézmények, szervek, hivatalok és ügynökségek vagy egy tagállam kérésére rendszeres független informatikai biztonsági ellenőrzéseket kell végeznie azzal a céllal, hogy adott esetben ajánlásokat fogalmazzon meg ellenállóképességük javítása érdekében.

Indokolás

Az ENISÁ-t fel kell hatalmazni megelőző jellegű informatikai biztonsági ellenőrzések elvégzésére a tagállami hatóságok vagy uniós intézmények, ügynökségek stb. kritikus infrastruktúráin.

Módosítás 43

Rendeletre irányuló javaslat 8 cikk – 1 bekezdés – a pont – 1 pont

A Bizottság által javasolt szöveg

Módosítás

1. európai **kiberbiztonsági** tanúsítási rendszerekre irányuló javaslatok kidolgozása IKT-termékekre és -szolgáltatásokra vonatkozóan e rendelet 44. cikkének megfelelően;

1. európai **informatikai biztonsági** tanúsítási rendszerekre irányuló javaslatok kidolgozása IKT-termékekre és -szolgáltatásokra vonatkozóan **az iparággal történő együttműködés révén és** e rendelet 44. cikkének megfelelően;

Indokolás

Ezen a területen rendkívül fontos az iparággal történő együttműködés.

Módosítás 44

Rendeletre irányuló javaslat 8 cikk – 1 bekezdés – c a pont (új)

A Bizottság által javasolt szöveg

Módosítás

ca) olyan tanúsítási rendszerek kialakítása, amelyek megakadályozzák, hogy az informatikai termékek és szolgáltatások eladói, illetve nyújtói szándékosan titkos kiskapukat alkalmazzanak kereskedelmi termékek és szolgáltatások informatikai biztonságának gyengítése érdekében, ami káros hatással van az internet globális biztonságára.

Indokolás

A tanúsítási rendszereknek ez kell legyen az egyik legfontosabb célja.

Módosítás 45

Rendeletre irányuló javaslat 9 cikk – 1 bekezdés – d pont

A Bizottság által javasolt szöveg

Módosítás

d) az uniós intézmények, hivatalok és szervek által **a kiberbiztonsággal** kapcsolatban rendelkezésre bocsátott információkat összegyűjti, strukturálja és a nyilvánosság számára elérhetővé teszi egy külön erre a célra létrehozott portálon;

d) az uniós intézmények, hivatalok és szervek által **az informatikai biztonsággal** kapcsolatban rendelkezésre bocsátott **és a tagállamok, valamint az állami érdekeltek és a magánszereplők által elérhetővé tett** információkat összegyűjti, strukturálja és a nyilvánosság számára elérhetővé teszi egy külön erre a célra létrehozott portálon;

Módosítás 46

Rendeletre irányuló javaslat 9 cikk – 1 bekezdés – e pont

A Bizottság által javasolt szöveg

Módosítás

e) növeli **a kiberbiztonsági** kockázatokkal kapcsolatos tudatosságot, és magánszemélyeknek és szervezeteknek címzett, egyedi felhasználói iránymutatást ad a már bevált módszerekkel kapcsolatban;

e) növeli **az informatikai biztonsági** kockázatokkal kapcsolatos tudatosságot, **terjeszti a biztonsági események megfelelő megelőzési intézkedéseit**, és magánszemélyeknek és szervezeteknek címzett, egyedi felhasználói iránymutatást ad a már bevált módszerekkel kapcsolatban;

Módosítás 47

Rendeletre irányuló javaslat 9 cikk – 1 bekezdés – e a pont (új)

A Bizottság által javasolt szöveg

Módosítás

ea) létrehozza a nemzeti oktatási kapcsolattartó pontok hálózatát a tagállamok közötti, az informatikai biztonsági tájékoztatásra és tudatosságnövelésre vonatkozó jobb koordináció és a bevált gyakorlatok cseréjének elősegítése érdekében;

Módosítás 48

Rendeletre irányuló javaslat 9 cikk – 1 bekezdés – g pont

A Bizottság által javasolt szöveg

Módosítás

g) rendszeres tájékoztató kampányokat szervez a tagállamokkal, valamint az uniós intézményekkel, szervezetekkel és hivatalokkal együttműködésben **a kiberbiztonság** fokozása és láthatóságának növelése érdekében.

g) rendszeres tájékoztató kampányokat szervez a tagállamokkal, valamint az uniós intézményekkel, szervezetekkel, hivatalokkal **és egyéb releváns érintett felekkel** együttműködésben **az informatikai biztonság** fokozása és láthatóságának növelése érdekében;

Módosítás 49

Rendeletre irányuló javaslat 9 cikk – 1 bekezdés – g a pont (új)

ga) annak előmozdítása, hogy az uniós digitális egységes piacon részt vevő valamennyi szereplő széles körben erős, megelőző jellegű informatikai biztonsági intézkedéseket fogadjon el és a magánélet védelmét erősítő technológiákat alkalmazzon az informatikai rendszerek elleni támadásokkal szembeni első védekezési vonalként.

Indokolás

Az európai adatvédelmi biztos véleménye alapján (PET). Az ENISA szerepe egyértelműen túl kell mutasson a tagállamok, a Bizottság és az uniós ügynökségek támogatásánál, és láthatóbbá kell válnia az iparág és a nagyközönség számára.

Módosítás 50

**Rendeletre irányuló javaslat
10 cikk – 1 bekezdés – a pont**

A Bizottság által javasolt szöveg

a) tanácsokkal látja el az Uniót és a tagállamokat a tekintetben, hogy **a kiberbiztonság** területén milyen kutatási szükségleteknek és prioritásoknak kell eleget tenni egyrészt ahhoz, hogy hatékonyan lehessen reagálni a jelenlegi és jövőbeli kockázatokra és fenyegetésekre, beleértve az új és kialakulóban lévő információs és kommunikációs technológiákat érintő kockázatokat és fenyegetéseket is, másrészt pedig ahhoz, hogy eredményesen lehessen alkalmazni a kockázatmegelőző technológiákat;

Módosítás

a) tanácsokkal látja el az Uniót és a tagállamokat a tekintetben, hogy **az informatikai biztonság, az adatvédelem és a magánélet védelme** területén milyen kutatási szükségleteknek és prioritásoknak kell eleget tenni egyrészt ahhoz, hogy hatékonyan lehessen reagálni a jelenlegi és jövőbeli kockázatokra és fenyegetésekre, beleértve az új és kialakulóban lévő információs és kommunikációs technológiákat érintő kockázatokat és fenyegetéseket is, másrészt pedig ahhoz, hogy eredményesen lehessen alkalmazni a kockázatmegelőző technológiákat;

Módosítás 51

**Rendeletre irányuló javaslat
14 cikk – 1 bekezdés – m pont**

m) e rendelet 33. cikkének megfelelően kinevezi az ügyvezető igazgatót, és adott esetben meghosszabbítja hivatali idejét, vagy felmenti hivatalából;

m) e rendelet 33. cikkének megfelelően **szakmai kritériumokon alapuló kiválasztási eljárások alapján** kinevezi az ügyvezető igazgatót, és adott esetben meghosszabbítja hivatali idejét, vagy felmenti hivatalából;

Módosítás 52

Rendeletre irányuló javaslat 20 cikk – 1 bekezdés

A Bizottság által javasolt szöveg

Módosítás

(1) Az igazgatótanács az ügyvezető igazgató javaslatára létrehozza az érdekelték állandó csoportját, amely egyfelől a releváns érdekelt feleket – IKT-ágazat, a nyilvános elektronikus hírközlő hálózatokat és nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat biztosító vállalkozások, a fogyasztói csoportok és **a kiberbiztonság** területén tevékenykedő tudományos szakemberek – képviselő elismert szakértőkből, másfelől pedig az [Európai Elektronikus Hírközlési Kódex létrehozásáról szóló] irányelv értelmében bejelentett nemzeti szabályozó hatóságok, valamint a bűnüldöző hatóságok és a magánélet védelmével foglalkozó felügyeleti hatóságok képviselőiből áll.

(1) Az igazgatótanács az ügyvezető igazgató javaslatára létrehozza az érdekelték állandó csoportját, amely egyfelől a releváns érdekelt feleket – IKT-ágazat, a nyilvános elektronikus hírközlő hálózatokat és nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat biztosító vállalkozások, a fogyasztói csoportok, **az európai szabványügyi szervek és az informatikai biztonság** területén tevékenykedő tudományos szakemberek – képviselő elismert szakértőkből, másfelől pedig az [Európai Elektronikus Hírközlési Kódex létrehozásáról szóló] irányelv értelmében bejelentett nemzeti szabályozó hatóságok, valamint a bűnüldöző hatóságok és a magánélet védelmével foglalkozó felügyeleti hatóságok képviselőiből áll.

Módosítás 53

Rendeletre irányuló javaslat 30 cikk – 2 bekezdés

A Bizottság által javasolt szöveg

Módosítás

(2) A Számvevőszék jogosult dokumentumalapú és helyszíni **ellenőrzést** végezni a támogatások összes kedvezményezettjénél, valamint az

(2) A Számvevőszék jogosult dokumentumalapú és helyszíni **vizsgálatokat** végezni a támogatások összes kedvezményezettjénél, valamint az

Ügynökségtől uniós forrásokban részesülő vállalkozóknál és alvállalkozóknál.

Ügynökségtől uniós forrásokban részesülő vállalkozóknál és alvállalkozóknál.

Módosítás 54

Rendeletre irányuló javaslat 44 cikk – 2 bekezdés

A Bizottság által javasolt szöveg

(2) Az e cikk (1) bekezdésében említett rendszerekre irányuló javaslatok kidolgozása során az ENISA valamennyi érdekelt féllel konzultál, és szorosan együttműködik a csoporttal. A csoport biztosítja az ENISA számára a rendszerre irányuló javaslat kidolgozásához szükséges segítséget és szakértői tanácsadást, többek között azáltal, hogy szükség esetén véleményeket ad ki.

Módosítás

(2) Az e cikk (1) bekezdésében említett rendszerekre irányuló javaslatok kidolgozása során az ENISA valamennyi érdekelt féllel konzultál, és szorosan együttműködik a csoporttal **és az érdekeltek állandó csoportjával**. A csoport **és az érdekeltek állandó csoportja** biztosítja az ENISA számára a rendszerre irányuló javaslat kidolgozásához szükséges segítséget és szakértői tanácsadást, többek között azáltal, hogy szükség esetén véleményeket ad ki. **Adott esetben az ENISA ezenkívül létrehozhatja az érdekeltek feleket tömörítő tanúsítási munkacsoportot, amelyet az érdekeltek állandó csoportjának tagjai és egyéb releváns érdekelt felek alkotnak, amely szakértői tanácsot ad egy bizonyos rendszerre irányuló javaslat által lefedett terület tekintetében.**

Indokolás

Az ipart konzultációs folyamat révén be kell vonni a rendszerekre irányuló javaslatok válaszába és kidolgozásába annak érdekében, hogy megfelelő szakértelmet nyújtsanak ezen rendszerek hatékony megtervezésének biztosításában.

Módosítás 55

Rendeletre irányuló javaslat 44 cikk – 4 bekezdés

(4) A Bizottság az ENISA által javasolt rendszer alapján az 55. cikk (1) bekezdésének megfelelően végrehajtási jogi aktusokat fogadhat el, amelyekben az IKT-termékekre és -szolgáltatásokra vonatkozó, az e rendelet 45., 46. és 47. cikkében foglalt követelményeknek megfelelő európai **kiberbiztonsági** tanúsítási rendszerekről rendelkezik.

(4) A Bizottság az ENISA által javasolt rendszer alapján az 55. cikk (1) bekezdésének megfelelően végrehajtási jogi aktusokat fogadhat el, amelyekben az IKT-termékekre és -szolgáltatásokra vonatkozó, az e rendelet 45., 46. és 47. cikkében foglalt követelményeknek megfelelő európai **informatikai biztonsági** tanúsítási rendszerekről rendelkezik. **A Bizottság konzultálhat az Európai Adatvédelmi Testülettel és figyelembe veheti véleményét az ilyen végrehajtási jogi aktusok elfogadása előtt.**

Indokolás

Az európai adatvédelmi biztos véleménye alapján. E módosítás összhangot biztosít az európai kiberbiztonsági tanúsítási keret és az általános adatvédelmi rendelet szerinti tanúsítványok között.

Módosítás 56

**Rendeletre irányuló javaslat
46 cikk – 2 bekezdés – bevezető rész**

(2) Az alapvető, jelentős, illetve magas szintű biztonsági **szinteknek értelemszerűen a következő kritériumoknak kell megfelelniük:**

(2) Az alapvető, jelentős, illetve magas szintű biztonsági **szint egy európai informatikai biztonsági tanúsítási rendszer keretében kibocsátott olyan tanúsítványra utal, amely – a megfelelő műszaki leírásokra, szabványokra és eljárásokra, többek között műszaki ellenőrzésekre hivatkozva, melyek célja az informatikai biztonsági események kockázatának csökkentése – az adott IKT-termék vagy -szolgáltatás állítólagos vagy igazolt informatikai biztonsági jellemzőinek megfelelő megbízhatóságot tulajdonít.**

Módosítás 57

Rendeletre irányuló javaslat
46 cikk – 2 bekezdés – a pont

A Bizottság által javasolt szöveg

Módosítás

a) az „alapvető” biztonsági szint egy *törölve*
európai kiberbiztonsági tanúsítási
rendszer keretében kibocsátott olyan
tanúsítványra utal, amely – a megfelelő
műszaki leírásokra, szabványokra és
eljárásokra, többek között műszaki
ellenőrzésekre hivatkozva, melyek célja a
kiberbiztonsági események kockázatának
csökkentése – az adott IKT-termék vagy -
szolgáltatás állítólagos vagy igazolt
kiberbiztonsági jellemzőinek korlátozott
megbízhatóságot tulajdonít;

Módosítás 58

Rendeletre irányuló javaslat
46 cikk – 2 bekezdés – b pont

A Bizottság által javasolt szöveg

Módosítás

b) a „jelentős” biztonsági szint egy *törölve*
európai kiberbiztonsági tanúsítási
rendszer keretében kibocsátott olyan
tanúsítványra utal, amely – a megfelelő
műszaki leírásokra, szabványokra és
eljárásokra, többek között műszaki
ellenőrzésekre hivatkozva, melyek célja a
kiberbiztonsági események kockázatának
jelentős csökkentése – az adott IKT-
termék vagy -szolgáltatás állítólagos vagy
igazolt kiberbiztonsági jellemzőinek
jelentős mértékű megbízhatóságot
tulajdonít;

Módosítás 59

Rendeletre irányuló javaslat
46 cikk – 2 bekezdés – c pont

A Bizottság által javasolt szöveg

Módosítás

c) a „magas” biztonsági szint egy *törölve*

európai kiberbiztonsági tanúsítási rendszer keretében kibocsátott olyan tanúsítványra utal, amely – a megfelelő műszaki leírásokra, szabványokra és eljárásokra, többek között műszaki ellenőrzésekre hivatkozva, melyek célja a kiberbiztonsági események megelőzése – az adott IKT-termék vagy -szolgáltatás állítólagos vagy igazolt kiberbiztonsági jellemzőinek nagyobb mértékű megbízhatóságot tulajdonít, mint a „jelentős” biztonsági szintet igazoló tanúsítványok.

Módosítás 60

Rendeletre irányuló javaslat

47 cikk – 1 bekezdés – a a pont (új)

A Bizottság által javasolt szöveg

Módosítás

aa) a megfelelőségértékelő és ellenőrző szervek;

Módosítás 61

Rendeletre irányuló javaslat

47 cikk – 1 bekezdés – 1 pont

A Bizottság által javasolt szöveg

Módosítás

l) az azonos típusú vagy kategóriájú IKT-termékekre és -szolgáltatásokra kiterjedő nemzeti **kiberbiztonsági** tanúsítási rendszerek azonosítása;

l) **a 49. cikk alapján** az azonos típusú vagy kategóriájú IKT-termékekre és -szolgáltatásokra kiterjedő nemzeti **informatikai biztonsági** tanúsítási rendszerek azonosítása;

Módosítás 62

Rendeletre irányuló javaslat

48 cikk – 6 bekezdés

A Bizottság által javasolt szöveg

Módosítás

(6) A tanúsítványok legfeljebb **hároméves** időtartamra szólnak, és **azonos**

(6) A tanúsítványok legfeljebb **az egyes rendszerek esetében egyedi alapon**

feltételek mellett megújíthatók, feltéve, hogy a megfelelő követelmények továbbra is teljesülnek.

meghatározott, de öt évnél nem hosszabb időtartamra szólnak, és megújíthatók, feltéve, hogy a megfelelő követelmények továbbra is teljesülnek.

Módosítás 63

Rendeletre irányuló javaslat 48 a cikk (új)

A Bizottság által javasolt szöveg

Módosítás

48a. cikk

Alapvető informatikai biztonsági követelmények

(1) *Az Ügynökség ... [két évvel e rendelet hatálybalépésének időpontja után]-ig javaslatot tesz a Bizottságnak az alábbiak szerinti egyértelmű és kötelező alapvető informatikai biztonsági követelményekre az EU-ban értékesített vagy onnan kivitt valamennyi informatikai termék vonatkozásában:*

a) *a gyártó írásbeli igazolást ad arról, hogy az eszköz nem tartalmaz semmilyen olyan hardver-, szoftver- vagy firmware-elemet, amely ismert biztonsági sebezhetőséget rejt magában;*

b) *az eszköz olyan szoftver- vagy firmware-elemeket használ, amelyeket a gyártó megfelelően hitelesített és megbízható módon frissíteni tud;*

c) *az eszköz nem tartalmaz titkosítatlan jelszavakat vagy hozzáférési kódokat; a gyártó legkésőbb a telepítés során dokumentálja az eszköz távoli hozzáférési lehetőségeit és megvédi azt a jogosulatlan hozzáféréstől; a gyártó nem alkalmaz alapértelmezett, fixen kódolt szabványos jelszavakat az eszközhöz; az eladó dokumentálja az eszköz minden felhasználó általi frissítési lehetőségét, és egyértelműen meghatározza, hogy kinek a felelőssége, ha a felhasználó nem frissíti az eszközt;*

d) az internethez kapcsolódó eszközök, szoftverek vagy firmware-elemek gyártója, forgalmazója és importálója tájékoztatja az illetékes hatóságot minden ismert kihasználható biztonsági sebezhetőségről;

e) az internethez kapcsolódó eszközök, szoftverek vagy firmware-elemek gyártója köteles megjavítani vagy kicserélni azokat, ha új biztonsági sebezhetőségre derül fény;

f) az internethez kapcsolódó eszközök, szoftverek vagy firmware-elemek gyártója köteles tájékoztatást adni arról, hogy az eszköz miként kapja az informatikai biztonsági frissítéseket, hogy mikor van az informatikai biztonsági támogatás megszűnésének tervezett időpontja, és hogy mi a felhasználók értesítésének módja;

(2) Az Ügynökség javasolhatja, hogy az (1) bekezdés szerinti minimális informatikai biztonsági követelmények vonatkozzanak egy vagy több konkrét ágazat informatikai eszközeire.

(3) Az Ügynökség két évente felülvizsgálja és szükség esetén módosítja az (1) bekezdésben említett informatikai biztonsági követelményeket és a módosításokat javaslatként benyújtja a Bizottságnak.

(4) A Bizottság végrehajtási jogi aktusok útján és egy hatásvizsgálat alapján határozhat arról, hogy az (1) és (2) bekezdés alapján javasolt vagy módosított informatikai biztonsági követelmények általános érvényűvé válnak az EU-ban. E végrehajtási jogi aktusokat az 55. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(5) A Bizottság gondoskodik azon informatikai biztonsági követelmények megfelelő nyilvánosságáról, amelyek esetében a (3) bekezdés szerint úgy határozott, hogy általánosan érvényesek.

(6) Az Ügynökség valamennyi javasolt informatikai biztonsági követelményt, valamint azok módosításait egy nyilvántartásban foglalja össze, és megfelelő módon nyilvánosan elérhetővé teszi azokat.

Indokolás

Helyettesíti a véleménytervezet 19. módosítása c) pontját az egyértelműség kedvéért. A kiberbűnözés megakadályozása és az információtechnológia használói alapvető jogainak védelme érdekében fontos egy ellenálló informatikai környezet kialakítása. Ezért e rendeletbe be kell illeszteni az Unión belül magas szintű információbiztonsági célokat kitűző alapvető kötelező információbiztonsági követelményeket.

Módosítás 64

Rendeletre irányuló javaslat 50 cikk – 6 bekezdés – d pont

A Bizottság által javasolt szöveg

d) együttműködnek a többi nemzeti tanúsításfelügyeleti hatósággal és más hatóságokkal, többek között azáltal, hogy megosztják az azzal kapcsolatos információkat, ha bizonyos IKT-termékek és -szolgáltatások nem felelnek meg e rendelet vagy egyes európai **kiberbiztonsági** tanúsítási rendszerek követelményeinek;

Módosítás

d) együttműködnek a többi nemzeti tanúsításfelügyeleti hatósággal és más hatóságokkal – **például a nemzeti adatvédelmi felügyeleti hatósággal** –, többek között azáltal, hogy megosztják az azzal kapcsolatos információkat, ha bizonyos IKT-termékek és -szolgáltatások nem felelnek meg e rendelet vagy egyes európai **informatikai biztonsági** tanúsítási rendszerek követelményeinek;

Indokolás

Az európai adatvédelmi biztos véleménye alapján.

ELJÁRÁS A VÉLEMÉNYNYILVÁNÍTÁSRA FELKÉRT BIZOTTSÁGBAN

Cím	Rendelet az Európai Unió Hálózat- és Információbiztonsági Ügynökségről (ENISA), az Európai Unió Kiberbiztonsági Ügynökségről, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály”)
Hivatkozások	COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)
Illetékes bizottság A plenáris ülésen való bejelentés dátuma	ITRE 23.10.2017
Véleményt nyilvánított A plenáris ülésen való bejelentés dátuma	LIBE 23.10.2017
A vélemény előadója A kijelölés dátuma	Jan Philipp Albrecht 20.11.2017
Vizsgálat a bizottságban	25.1.2018 8.3.2018
Az elfogadás dátuma	8.3.2018
A zárószavazás eredménye	+ : 35 – : 2 0 : 4
A zárószavazáson jelen lévő tagok	Asim Ademov, Jan Philipp Albrecht, Heinz K. Becker, Caterina Chinnici, Rachida Dati, Cornelia Ernst, Kinga Gál, Sylvie Guillaume, Monika Hohlmeier, Filiz Hyusmenova, Dietmar Köster, Barbara Kudrycka, Monica Macovei, Péter Niedermüller, Ivari Padar, Judith Sargentini, Birgit Sippel, Branislav Škripek, Sergei Stanishev, Traian Ungureanu, Josef Weidenholzer, Cecilia Wikström, Kristina Winberg, Auke Zijlstra
A zárószavazáson jelen lévő póttagok	Maria Grapini, Sylvia-Yvonne Kaufmann, Jeroen Lenaers, Andrejs Mamikins, Maite Pagazaurtundúa Ruiz, John Procter, Jaromír Štětina, Josep-Maria Terricabras, Axel Voss, Elissavet Vozemberg-Vrionidi
A zárószavazáson jelen lévő póttagok (200. cikk (2) bekezdés)	Andrea Bocskor, Reimer Böge, André Elissen, Ramón Jáuregui Atondo, Julia Reda, Rainer Wieland, Patricija Šulin

NÉV SZERINTI ZÁRÓSZAVAZÁS A VÉLEMÉNYNYILVÁNÍTÁSRA FELKÉRT BIZOTTSÁGBAN

35	+
ALDE	Filiz Hyusmenova, Maite Pagazaurtundúa Ruiz, Cecilia Wikström
ECR	Monica Macovei, John Procter, Branislav Škripek
GUE/NGL	Cornelia Ernst
PPE	Asim Ademov, Heinz K. Becker, Andrea Bocskor, Rachida Dati, Kinga Gál, Barbara Kudrycka, Jeroen Lenaers, Jaromír Štětina, Patricija Šulin, Traian Ungureanu, Elissavet Vozemberg-Vrionidi, Rainer Wieland
S&D	Caterina Chinnici, Maria Grapini, Sylvie Guillaume, Ramón Jáuregui Atondo, Sylvia-Yvonne Kaufmann, Dietmar Köster, Andrejs Mamikins, Péter Niedermüller, Ivari Padar, Birgit Sippel, Sergei Stanishev, Josef Weidenholzer
VERTS/ALE	Jan Philipp Albrecht, Julia Reda, Judith Sargentini, Josep-Maria Terricabras

2	-
ENF	André Elissen, Auke Zijlstra

4	0
EFDD	Kristina Winberg
PPE	Reimer Böge, Monika Hohlmeier, Axel Voss

Jelmagyarázat:

+ : mellette

- : ellene

0 : tartózkodás