I

(Állásfoglalások, ajánlások és vélemények)

ÁLLÁSFOGLALÁSOK

TANÁCS

A TANÁCS ÁLLÁSFOGLALÁSA

(2009. december 18.)

a hálózat- és információbiztonság együttműködésre építő európai megközelítéséről

(2009/C 321/01)

AZ EURÓPAI UNIÓ TANÁCSA,

I. TEKINTETTEL:

1. a Bizottságnak „A biztonságos információs társadalomra irányuló stratégia” című, 2006. május 31-i közleményére, amely a tagállamokat és a magánszféra érdekelt feleit bevonó „párbeszéd, partnerség, felvértezés” folyamatát ismerteti;

2. a Bizottságnak a létfontosságú infrastruktúrák védelmére vonatkozó európai programról szóló, 2006. december 12-i közleményére, amelynek célja az Unióban található kritikus infrastruktúrák védelmének javítása és a kritikus infrastruktúrák védelmére szolgáló uniós keret létrehozása;

3. az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i tanácsi irányelvre;

4. a biztonságos európai információs társadalomra irányuló stratégiáról szóló, 2007. március 22-i tanácsi állásfoglalásra;

5. a létfontosságú infrastruktúrák védelmére vonatkozó európai programról szóló, 2007. április 19–20-i tanácsi következtetésekre;

6. a kritikus informatikai infrastruktúrák védelméről szóló, 2009. március 30-i bizottsági közleményre;

7. a jelenleg az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) jövőjéről és a kritikus informatikai infrastruktúrák védelmében játszott szerepéről folyó – a vonatkozó nyilvános konzultációt is magában foglaló – vitára;

8. a kritikus informatikai infrastruktúrák védelméről szóló, a 2009. április 27–28-i tallinni miniszteri konferencián elfogadott elnökségi következtetésekre;

9. a versenyképességre és a növekedésre vonatkozó lisszaboni célkitűzésekre és a lisszaboni stratégia felülvizsgálata érdekében jelenleg folyó munkára;

10. az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások keretszabályozásának felülvizsgálata során javasolt biztonsági intézkedésekre;

11. arra, hogy a hálózat- és információbiztonságra vonatkozó, hatékony jövőbeli politika biztosítása érdekében ez az állásfoglalás abból a feltételezésből indul ki, hogy az ENISA-rendelet indokolt változtatásaival kapcsolatban még nem született megállapodás. Mivel a Bizottság jelenleg végzi a hálózat- és információbiztonságra vonatkozó, jövőbeli politika felülvizsgálatát, ez az állásfoglalás – a Bizottság vizsgálati eredményeinek nyilvánosságra hozatala előtt – nem érinti a felülvizsgálat eredményeit az ENISA-rendelet módosításainak tekintetében;

II. TUDOMÁSUL VÉVE, HOGY:

1. az elektronikus hírközlésnek, infrastruktúráknak és szolgáltatásoknak a gazdasági és társadalmi tevékenységek alapjaként játszott jelentős szerepe következtében a hálózat- és információbiztonság a társadalom olyan fontos értékeihez és célkitűzéseihez járul hozzá, mint a demokrácia, a magánélet védelme, a gazdasági növekedés, a gondolatok szabad áramlása, valamint a gazdasági és politikai stabilitás;

2. az információs és kommunikációs technológiai rendszerek, infrastruktúrák és szolgáltatások, köztük az internet, jelentős szerepet játszanak a társadalom életében, zavaruk óriási gazdasági károkat képes okozni, ami felhívja a figyelmet a védelem és az ellenálló képesség fokozását célzó intézkedések jelentőségére, amelyek a kritikus szolgáltatások folyamatosságának zálogai;

3. a biztonsági események magukban rejtik a felhasználói bizalom aláásásának veszélyét. A hálózatok és informatikai rendszerek súlyos megzavarása jelentős gazdasági és társadalmi hatással járhat, azonban a mindennapi problémák és kellemetlenségek is azzal a kockázattal járnak, hogy aláássák a technológiába, hálózatokba és szolgáltatásokba vetett közbizalmat;

4. a fenyegetések folyamatosan változnak és egyre több területre terjednek ki, ezért a végfelhasználókat, vállalkozásokat és kormányokat alapértelmezetten megbízható és ellenálló elektronikus hírközlési infrastruktúrákkal kell ellátni, és meg kell határozni az arra irányuló megfelelő ösztönzőket, hogy a szolgáltatók mindezt időben biztosítsák;

5. valamennyi szakpolitikai területen és társadalmi szektorban meg kell honosítani és növelni kell a hálózat- és információbiztonságot, továbbá válaszolni arra a kihívásra, amely a megfelelő készségek mind nemzeti, mind európai fellépéseken keresztüli biztosítását és az információs és kommunikációs technológiák (IKT) felhasználói tájékozottságának növelését sürgeti;

6. a belső piac kialakítása és működése megköveteli a hálózattulajdonosok és a szolgáltatók határokon átnyúló együttműködését, lévén, hogy az egyes tagállamokban bekövetkező esetleges működési zavarok a többi tagállam és az EU egésze területén is zavart okozhatnak;

7. az olyan új felhasználói megoldások, mint a számítási felhő és a „szoftver mint szolgáltatás” további hangsúlyt helyeznek a hálózat- és információbiztonság jelentőségére;

8. a hálózat- és információbiztonság az informatikai rendszerek megbízhatóságára irányuló célkitűzést szolgálja, amelyet valamennyi társadalmi szektor minden résztvevője magáénak vall, ezért ágazatközi és határokon átnyúló megközelítést kell alkalmazni;

9. mivel a társadalomban egyre elterjedtebb az IKT alkalmazása, a hálózat- és információbiztonság előfeltétele az e-kormányzáshoz hasonló közszolgáltatások megbízható és biztonságos nyújtásának;

10. az ENISA már most is fontos szerepet tölt be a hálózat- és információbiztonságban, és az így szerzett tapasztalatokat jól tudná kamatoztatni a jövőben is;

III. HANGSÚLYOZZA, HOGY:

1. a hálózat- és információbiztonság magas szintje szükséges az Unióban az alábbiak támogatása érdekében:

   a) a polgárok szabadságai és jogai, köztük a magánélethez való jog;

   b) az információkezelés minőségének szempontjából hatékony társadalom;

   c) jövedelmezőség és növekedés a kereskedelem és az ipar területén;

   d) a polgárok és a szervezetek információkezelésbe és IKT-rendszerekbe vetett bizalma;

2. az IKT-ágazat alapvető fontosságú a legtöbb társadalmi szektor számára, ezáltal a hálózat- és információbiztonság valamennyi érdekelt fél – így az üzemeltetők, a szolgáltatók, a hardver- és szoftverkészítők, a végfelhasználók, az állami szervek és a nemzeti kormányok – közös felelősségévé válik;

IV. ELISMERI, HOGY:

1. fontos a tevékeny és tájékozott európai hálózat- és információbiztonsági közösség, amely elősegíti a tagállamok és a magánszféra közötti fokozott együttműködést;

2. számos előnnyel jár a nemzetközi biztonsági előírásoknak adott esetben az EU egésze területén a hálózat- és információbiztonság céljából történő összehangolt alkalmazása;

3. a nemzetközi színtéren szükség van a hálózat- és információbiztonság együttműködésre építő európai megközelítésére, mivel globális kihívásról van szó;

4. fontos, hogy a tagállamok és az uniós intézmények megbízható statisztikai adatokhoz juthassanak az európai hálózat- és információbiztonság vonatkozásában;

5. valamennyi érdekelt félnek tájékozottabbnak kell lennie és eszközökkel kell rendelkeznie a kockázatkezelést illetően;

6. fontos, hogy a tagállamok fokozott erőfeszítéseket tegyenek a területtel kapcsolatos szemléletformálás, a bevált gyakorlatok cseréje és a tagállamok számára nyújtott iránymutatás kialakítása érdekében;

7. fontos, hogy a köz- és magánszféra partnerségéhez hasonló, az összes érdekelt felet egybefogó szerveződések alakuljanak, hosszú távú, alulról felfelé épülő modell alapján, amelyek célja a felismert kockázatok enyhítése, amennyiben ez a megközelítés többletértéket jelent a hálózat magas szintű ellenálló képességének biztosítása szempontjából;

8. a szolgáltatók alapvetően fontos szerepet játszanak abban, hogy a társadalom megbízható és ellenálló elektronikus hírközlési infrastruktúrákat vehessen igénybe;

9. hasznosnak bizonyulnak az európai hálózat- és információbiztonsági gyakorlatok, amelyek értékes tanulságokkal szolgálhatnak a hálózatok üzemeltetőinek és a szolgáltatóknak, valamint a kormányoknak;

10. a fenyegetésekre reagáló és a problémaelhárító nemzeti vagy kormányzati számítástechnikai katasztrófaelhárító csoportok (CERT) vagy más válságkezelési csoportok hozzájárulhatnak az ellenálló képesség magas szintjének kialakításához és a hálózatok és információs rendszerek megzavarásának kivédésére vagy orvoslására szolgáló képességhez;

11. fontos a számítástechnikai katasztrófaelhárító csoportok uniós intézmények számára való kialakítása vonatkozásában a stratégiai hatások, kockázatok és kilátások feltérképezése, valamint az ENISA e kérdésben játszandó jövőbeli szerepének vizsgálata;

12. azt a munkát, amelyet a hálózat- és információbiztonság területén az ENISA eddig végzett, amely ügynökséget az európai hálózat- és információbiztonság területén egyértelmű előnyöket biztosító, hatékony szervezetté kell fejleszteni;

V. HANGSÚLYOZZA, HOGY:

1. elengedhetetlenül fontos a jelenlegi és a jövőbeli kihívások megválaszolása szempontjából a kibővített és átfogó látásmódot érvényesítő, valamint az Európai Bizottság, a tagállamok és az ENISA szerepét egyértelműen elkülönítő európai hálózat- és információbiztonsági stratégia;

2. megfelelő konzultáció és elemzés után a jogalkotási eljárásban meg kell vizsgálni annak lehetőségét, hogy az ENISA-t korszerűsítsék és megerősítsék egy olyan megbízatással, amely egyfelől biztosítaná a rugalmasságot és a tagállamok és a Bizottság általi felügyeletet, másfelől pedig a magánszférabeli érdekeltek képviselőinek eredményes részvételét. A megbízatás meghatározásakor figyelembe kell venni az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások keretszabályozását, valamint a lisszaboni menetrendben meghatározott célokat, továbbá célokat kell kitűzni a kutatással, az innovációval, a versenyképességgel, a gazdasági növekedéssel és a bizalom megóvásával kapcsolatban;

3. az ENISA támogatni tudná a Bizottságot és a tagállamokat a szakpolitikák kialakításában és végrehajtásában, különösen azáltal, hogy kapcsolatot teremt a technológia és a szakpolitikák között, és szorosan együtt kell működnie a tagállamokkal és más érdekelt felekkel annak érdekében, hogy tevékenységei kellőképpen össze legyenek hangolva az uniós prioritásokkal;

4. a módosított megbízatással működő ENISA-nak az EU szakértői központjaként kell működnie az EU-val kapcsolatos hálózat- és információbiztonsági kérdésekben. Ebből következően az európai intézményeknek ki kell kérniük és teljes mértékben figyelembe kell venniük az ENISA állásfoglalását az olyan politikák kialakításakor és végrehajtásakor, melyek befolyásolhatják ezt a területet;

5. az ENISA továbbá kérésre segítséget nyújthatna a tagállamoknak abban, hogy javítsák a saját hálózat- és információbiztonsági képességeiket és a biztonsági események kezelésére való képességüket;

VI. FELKÉRI A TAGÁLLAMOKAT, HOGY:

1. folytassák a végfelhasználók IKT-kbe vetett bizalmának tájékoztató kampányok révén történő erősítését;

2. szervezzenek a hálózat- és információbiztonsággal kapcsolatos nemzeti gyakorlatokat és/vagy vegyenek részt az ezzel kapcsolatos rendszeres európai gyakorlatokban, tekintve, hogy a terület összetettsége és a magánszféra részvétele miatt kiterjedt tervezésre van szükség. Az ENISA kérésre segítséget nyújthatna a tagállamoknak ezzel kapcsolatban. A gyakorlatok tárgyának és földrajzi kiterjedésének az idők során természetszerűleg változnia kell, és a felismert kockázatokon kell alapulnia;

3. hozzanak létre számítástechnikai katasztrófaelhárító csoportokat (CERT) azokban a tagállamokban, amelyek még nem alakították ki ezen képességüket, és az egyes tagállamok ilyen csoportjai között fokozzák az európai szintű együttműködést. Az ENISA segítséget nyújthatna a tagállamoknak ezzel kapcsolatban;

4. fokozzák a hálózat- és információbiztonsággal kapcsolatos oktatási, képzési és kutatási programokra irányuló erőfeszítéseket annak érdekében, hogy az EU-ban rendelkezésre álljanak a szükséges technikai készségek és szakemberek, és növekedjék a professzionalizmus e területen;

5. határon átnyúló események bekövetkeztekor közösen reagáljanak, és javítsák az ennek megfelelő végrehajtásához szükséges képességeiket, ami megkívánja, hogy a döntéshozók között, különösen a titoktartási kérdésekben, intenzívebbé váljon a párbeszéd;

VII. FELKÉRI A BIZOTTSÁGOT, HOGY:

1. adott esetben támogassa a tagállamokat ezen állásfoglalás végrehajtásában;

2. rendszeresen tájékoztassa az Európai Parlamentet és a Tanácsot a hálózat- és információbiztonsággal kapcsolatos uniós szintű kezdeményezésekről;

3. az ENISA-val együttműködésben kezdeményezzen az európai közszférabeli és magánszférabeli szereplőket megcélzó tájékoztató kampányt a hálózat- és információbiztonsággal kapcsolatos megfelelő kockázatkezelésről;

4. a tagállamokkal együttműködésben folytassa azoknak az ösztönzőknek a meghatározását, amelyek arra serkentenék az elektronikus hírközlési infrastruktúrák szolgáltatóit, hogy alapértelmezetten megbízható és ellenálló infrastruktúrákat biztosítsanak a végfelhasználók, vállalkozások és a közigazgatás számára;

5. a tagállamokkal együttműködésben határozzon meg olyan módszereket, melyek segítségével uniós szinten összehasonlítható értékelést lehet készíteni a biztonsági események társadalmi-gazdasági hatásáról és a megelőző intézkedések hatékonyságáról;

6. ösztönözze és javítsa az összes érdekelt felet egybefogó szerveződéseket, amelyeknek egyértelműen többletértéket kell jelenteniük a végfelhasználók és az ágazat számára;

7. terjesszen be átfogó hálózat- és információbiztonsági stratégiát, [1] beleértve az ENISA megerősített és rugalmas megbízatására és a tagállamok és a Bizottság megerősített felügyeleti szerepére vonatkozó javaslatokat is;

8. a tagállamokkal együttműködésben végezzen elemzést a számítástechnikai katasztrófaelhárító csoportokkal (CERT) kapcsolatban annak feltérképezése végett, hogy mely területeken van szükség további együttműködésre;

9. folytassa a közös és interoperábilis megközelítés meghatározását az uniós intézmények számára a biztonságos IKT-rendszerek és -szolgáltatások beszerzéséhez;

VIII. FELHÍVJA AZ ENISA-T, HOGY:

1. továbbra is támogassa aktívan a tagállamokat, az Európai Bizottságot és a többi érdekelt felet az európai hálózat- és információbiztonsági politikák és a kritikus informatikai infrastruktúrák védelmével kapcsolatos cselekvési terv végrehajtásában;

2. működjön együtt a tagállamokkal, a Bizottsággal és a statisztikai hivatalokkal a hálózat- és információbiztonság európai helyzetére vonatkozó statisztikai keretek kialakításában;

IX. FELHÍVJA AZ ÉRDEKELTEKET, HOGY:

1. fokozzák a hálózat- és információbiztonság növelésére irányuló erőfeszítéseket, különösen a megbízható, bizalmat ébresztő és könnyen használható termékek és szolgáltatások nyújtását illetően;

2. a felhasználókat tájékoztassák megfelelően a termékek és szolgáltatások biztonsági kockázatairól, és arról, hogy hogyan védhetik meg magukat;

3. tegyenek meg minden műszaki és szervezési intézkedést az elektronikus hírközlési hálózatok és szolgáltatások folyamatos működésének, sértetlenségének és titokvédelmének biztosítására;

4. folytassák a hálózat- és információbiztonság szabványosításával kapcsolatos munkát, melynek célja harmonizált és interoperábilis megoldások biztosítása;

5. vegyenek részt a tagállamokkal együtt a gyakorlatokban annak érdekében, hogy a szükséghelyzetekre megfelelő válaszlépéseket tudjanak meghatározni.

---

[1] A Bizottság azt javasolja, hogy ide illesszék be a „lehetőleg” szót.