I

(Állásfoglalások, ajánlások, iránymutatások és vélemények)

ÁLLÁSFOGLALÁSOK

TANÁCS

A TANÁCS ÁLLÁSFOGLALÁSA

(2007. március 22.)

a biztonságos európai információs társadalomra irányuló stratégiáról

(2007/C 68/01)

AZ EURÓPAI UNIÓ TANÁCSA,

ELFOGADJA EZT AZ ÁLLÁSFOGLALÁST, ÉS

ÜDVÖZLI

a Bizottságnak „A biztonságos információs társadalomra irányuló stratégia: »párbeszéd, partnerség, felvértezés és felelősségvállalás«" című, a Tanácshoz, az Európai Parlamenthez, az Európai Gazdasági és Szociális Bizottsághoz és a Régiók Bizottságához intézett, 2006. május 31-i közleményét,

TUDOMÁSUL VESZI

a kéretlen elektronikus levelek, kémprogramok és számítógépes vírusok elleni küzdelemről szóló, a Tanács, az Európai Parlament, az Európai Gazdasági és Szociális Bizottság, valamint a Régiók Bizottsága számára készített, 2006. november 15-i bizottsági közleményt,

EMLÉKEZTET

1. a hálózati és információs biztonság terén alkalmazandó közös megközelítésről és egyedi intézkedésekről szóló, 2002. január 28-i tanácsi állásfoglalásra ([1]);

2. a hálózat- és információbiztonság kultúrájával kapcsolatos európai megközelítésről szóló, 2003. február 18-i tanácsi állásfoglalásra ([2]);

3. a kéretlen, direkt-marketing célú (spam) levelekről szóló, 2004. március 8–9-i tanácsi következtetésekre, valamint a kéretlen (spam) levelek elleni küzdelemről szóló, 2004. december 9–10-i tanácsi következtetésekre;

4. a lisszaboni stratégiát újraindító 2005. márciusi Európai Tanács következtetéseire, valamint a Bizottságot és a tagállamokat az új i2010 stratégia határozott végrehajtására felhívó 2006. márciusi Európai Tanács következtetéseire;

5. az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások uniós keretszabályozására ([3]), és különösen a kommunikáció biztonságára, a magánélet védelmére és a titokvédelemre vonatkozó rendelkezésekre, amelyek hozzájárultak a személyes adatok és a magánélet védelme magas szintjének szavatolásához, valamint a nyilvános kommunikációs hálózatok sértetlenségéhez és biztonságához;

6. az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) létrehozásáról szóló, 2004. március 10-i 460/2004/EK európai parlamenti és tanácsi rendeletre ([4]);

7. a tuniszi folyamatra és az Információs Társadalom Csúcstalálkozó (WSIS) tuniszi kötelezettségvállalására, amely kiemeli a számítógépes bűnözés és a kéretlen elektronikus levelek elleni küzdelem folytatásának – a magánélet tiszteletben tartásának és a véleménynyilvánítás szabadságának szavatolásával egyidejű – szükségességét, valamint hangsúlyozza a globális számítógépes biztonságpolitika további előmozdítása, fejlesztése és végrehajtása szükségességét az összes érdekelt féllel együttműködve;

8. az idén a finnországi Espoo-ban (2006. szeptember 27–28-án) megtartott „i2010 – A mindenütt jelenlévő európai információs társadalom felé" című, az európai információs társadalommal foglalkozó éves konferencia elnökségi következtetéseire;

([1]) HL C 43., 2002.2.16., 2. o.
([2]) HL C 48., 2003.2.28., 1. o.
([3]) A 2002/58/EK irányelv („Elektronikus hírközlési adatvédelmi irányelv"), a 2002/20/EK irányelv („Engedélyezési irányelv"), valamint a 2002/22/EK irányelv („Egyetemes szolgáltatási irányelv") (HL L 201., 2002.7.31., 37. o., HL L 108., 2002.4.24., 21. o. és HL L 108., 2002.4.24., 51. o.).
([4]) HL L 77., 2004.3.13., 1. o.

ENNEK MEGFELELŐEN HANGSÚLYOZZA, HOGY:

1. társadalmaink gyorsan mozdulnak el egy újabb fejlődési szakasz, a mindenütt jelenlévő információs társadalom felé, ahol a polgárok egyre több mindennapi tevékenysége támaszkodik az információs és kommunikációs technológiákra (ICT), valamint az elektronikus kommunikációs hálózatokra; a hálózat- és információbiztonság e társadalom fejlődése és sikere motorjának tekintendő;

2. a bizalom az új információs társadalom sikerének sarkalatos eleme; a bizalom a végfelhasználók tapasztalataira és magánéletük tiszteletben tartásának szükségességére is vonatkozik; következésképp a hálózat- és információbiztonság nem csupán technikai kérdésnek minősül;

3. a hálózat- és információbiztonság az i2010-kezdeményezés részeként kialakuló európai információs tér létrehozásának lényeges része, amely hozzájárul az újraindított lisszaboni stratégia sikeréhez; az ICT ezenfelül a gazdaságban mindenhol az innováció, a gazdasági növekedés és a munkahelyteremtés kritikus eleme;

4. a mindenütt jelenlévő információs társadalom felé vezető új technológiák már fejlesztés alatt állnak; az áttörést jelentő technológiák (mint például a nagy sebességű vezeték nélküli hálózatok, a rádiófrekvencia-kereső berendezések (RFID), az intelligens érzékelő hálózatok), valamint az innovatív, tartalomgazdag szolgáltatások (például az internet protokoll televíziózás (IPTV), az IP-hálózaton keresztül történő hangátvitel (VOIP), a mobiltelevíziózás és más mobilszolgáltatások) eljövetele a tényleges kereskedelmi érték elérése céljából a fejlesztés legelejétől kezdve a hálózat- és információbiztonság megfelelő szintjeit követeli meg; az új, ígéretes találmányok korai bevezetése az európai információs társadalom és versenyképesség alakulása szempontjából rendkívüli jelentőséggel bír; a kormányzati szerveknek és a vállalkozásoknak a biztonságos, kialakulóban lévő új technológiákat és szolgáltatásokat ezek széleskörű elterjedésének felgyorsítása érdekében a lehető leghamarabb be kell vezetniük;

5. az EU számára stratégiai jelentőségű, hogy az európai ipar a hálózati és biztonsági termékeknek és szolgáltatásoknak egyszerre igényes felhasználója és versenyképes szállítója legyen; a sokféleség, a nyitottság és az interoperabilitás a biztonság szerves összetevőit alkotják és mint ilyenek előmozdítandók;

6. a hálózat- és információbiztonsági tudásnak és készségeknek is a társadalom minden egyes tagja és valamennyi érdekelt mindennapi életének szerves részévé kell válniuk; nemzeti és európai szinten egyaránt számos figyelemfelkeltő kampányra került sor, ám ezen a területen – különösen a végfelhasználókat, valamint a kis-és középvállalkozásokat (KKV-ket) illetően – még van tennivaló; különös figyelmet kell fordítani a különleges igényekkel fellépő, vagy a hálózat- és információbiztonság terén alacsony tudatosságot mutató felhasználókra; minden érdekeltnek tudatosítania kell azt, hogy a globális biztonsági lánc részét képezi, ezért ennek megfelelő eljárási jogosultsággal kell rendelkeznie; a hálózat- és információbiztonságot minden ICT-oktatásban és -képzésben szem előtt kell tartani;

7. az ENISA létrehozása lényeges előrelépést jelentett az EU azon törekvésében, hogy megfeleljen a hálózat- és információbiztonsággal összefüggő kihívásoknak; az ENISA hatáskörét, céljait, feladatait és működésének időtartamát a 460/2004/EK rendelet szabályozza;

8. a nemzeti és uniós szinten kutatásra és fejlesztésre (K+F), valamint innovációra szánt források kulcsfontosságú szerepet játszanak az új rendszerek, alkalmazások és szolgáltatások hálózat- és információbiztonsága szintjének erősítésében; az uniós szintű erőfeszítéseket a biztonsággal összefüggő kutatás és innováció terén, különösen a 7. keretprogramon és a versenyképességi és innovációs keretprogramon keresztül, erősíteni kell; az erőfeszítéseknek olyan intézkedésekre is kell irányulniuk, amelyek a programoknak köszönhető eredmények kereskedelmi kiaknázásának elterjesztését vagy ösztönzését célozzák, ideértve az eredmények tágabb közösség számára való hasznosságának értékelését is; ez javítani fogja az európai szolgáltatók képességét az európai piac különleges igényeinek megfelelő biztonsági megoldások nyújtására;

9. a mindenütt jelenlévő információs társadalom számottevő előnyökkel jár ugyan, ám jelentős kihívásokkal is jár, ami a lehetséges kockázatok új terepének megjelenését jelenti; a biztonságot és a magánéletet veszélyeztető, a nyilvánvalóan gazdasági előnyszerzést szolgáló és azt célzó jelenségek – többek között az adatok jogosulatlan elfogása és felhasználása – egyre súlyosabb méreteket öltenek, ezért a megjelenő és a már meglévő veszélyekre innovatív új válaszokat kell adni, melyeknek a rendszer összetettségéből, a hibákból, zavarokból vagy nem egyértelmű iránymutatásokból adódó kérdésekre is ki kell terjedniük; ösztönözni kell és elő kell mozdítani a különböző szereplőket célzó nemzeti számítástechnikai katasztrófa-elhárító szervek létrehozását, illetve fejlesztését, valamint az ezen szervek közötti, illetve a többi érintett érdekelt fél közötti együttműködést;

10. a termékek, szolgáltatások és irányító rendszerek – különösen a meglévő intézmények által végzett – szabványosítása és hitelesítése a bevált gyakorlatnak és a szakmaiságnak a hálózat- és információbiztonság területén való terjesztése eszközeként különleges figyelmet érdemel az EU hálózat- és információbiztonsági politikájában; a valószínűleg kialakuló nyílt és interoperábilis szabványok időben történő elfogadása elsősorban a kialakulóban lévő új technológiák, mint az RFID és a mobiltelevíziózás számára jelentenek majd előnyt; ezen a területen ösztönözni kell az európai szabványügyi testületek működését;

11. minthogy a kritikus infrastruktúrák átfogó működtetésében az elektronikus hálózatok és információs rendszerek egyre növekvő központi szerepet játszanak, ezek rendelkezésre állása és sértetlensége a hivatalok, a vállalkozások, a polgárok biztonsága, illetve életminősége, valamint a társadalmak általános működése szempontjából egyaránt nélkülözhetetlenné válik;

12. az együttműködésre és a gyakorlatias megközelítésekre most nagyobb szükség van, mint valaha; a különböző érdekelt feleknek meg kell határozniuk és fel kell ismerniük saját szerepüket, hatásköreiket és jogaikat.

EZÉRT FELKÉRI A TAGÁLLAMOKAT, HOGY

1. a hálózat- és információbiztonsági kérdésekről a valamennyi polgárt/felhasználót és a gazdaság valamennyi ágazatát – elsősorban a KKV-ket és a különleges igényekkel fellépő, vagy az alacsony tudatosságot mutató végfelhasználókat – megcélzó tájékoztató kampányok indításával támogassák a hálózat- és információbiztonsággal összefüggő képzési programokat és növeljék az e kérdésekkel kapcsolatos általános tudatosságot; 2008-ig ki lehetne választani az európai széleskörű tudatosságnövelő napra (pl. a „Hálózat- és információbiztonsági nap”-ra) egy közös időpontot, amelyet évente, önkéntes alapon minden tagállamban megtartanának;

2. erősítsék a biztonsággal összefüggő kutatáshoz és fejlesztéshez való hozzájárulást, valamint javítsák a K+F-nek köszönhető eredmények felhasználhatóságát és elterjesztését; az európai ICT-biztonsági ipar növekedésének fellendítése, valamint az új hálózat- és információbiztonsági technológiák és szolgáltatások korai felhasználásának és kereskedelmi forgalomban való elterjesztésének fellendítése érdekében ösztönözzék az innovatív partnerségek kialakítását;

3. fordítsanak kellő figyelmet az elektronikus kommunikációs hálózatokra leselkedő új és már meglévő veszélyek megelőzésének és az ellenük való küzdelemnek a szükségességére, az adatok jogosulatlan elfogását és felhasználását is ideértve, ismerjék fel és kezeljék a kapcsolódó kockázatokat, és – adott esetben az ENISA-val együttműködve – nemzeti szinten ösztönözzék az érintett szervezetek és ügynökségek közötti tényleges információcserét, valamint együttműködést; mutassanak elkötelezettséget a kéretlen elektronikus levelek, a kémprogramok és a számítógépes vírusok elleni küzdelemben, különösen az illetékes hatóságok közötti, nemzeti és nemzetközi szintű fokozott együttműködés révén;

4. az i2010 keretstratégia keretében erősítsék kölcsönös együttműködésüket a hálózat- és információbiztonság javítását célzó hatékony és innovatív gyakorlatok meghatározására, valamint e gyakorlatok ismeretének az EU-ban önkéntes alapon történő terjesztésére;

5. ösztönözzék a nemzeti számítástechnikai katasztrófa-elhárító szervek folyamatos fejlesztését;

6. segítsék elő olyan környezet kialakulását, amely a szolgáltatókat és a hálózatüzemeltetőket arra ösztönzi, hogy ügyfeleiknek szilárd szolgáltatásokat nyújtsanak, szavatolják a rendszer ellenálló képességét, valamint biztonsági szolgáltatásaik és megoldásaik tekintetében biztosítsák az ügyfelek választási lehetőségét; adott esetben ösztönözzék a szolgáltatókat és a hálózatüzemeltetőket, vagy követeljék meg tőlük, hogy ügyfeleik számára szavatolják a megfelelő hálózat- és információbiztonságot;

7. az i2010 magas szintű munkacsoportban – az információs társadalom folyamatos fejlődésének szem előtt tartásával – folytassák a stratégiai megbeszéléseket, valamint a kommunikációval és a képzéssel együtt biztosítsák a rendeleti szabályozás, a társszabályozás, a K+F és az *e*kormányzás vetületeinek összefüggő megközelítését;

8. az i2010 *e*kormányzati cselekvési tervvel összhangban biztosítsák az *e*kormányzati szolgáltatások zökkenőmentes kibontakozását, mozdítsák elő az interoperábilis személyazonosság-kezelő megoldásokat és minden ehhez szükséges változtatást tegyenek meg a közszektor szervezetében; a kormányoknak és a közhivataloknak példaként kell szolgálniuk a legjobb gyakorlatra azáltal, hogy valamennyi polgárt hozzásegítik a biztonságos *e*kormányzati szolgáltatásokhoz.

ÜDVÖZLI A BIZOTTSÁG AZON SZÁNDÉKÁT, HOGY

1. a hálózat- és információbiztonság egész Európára kiterjedő, átfogó és dinamikus stratégiájának fejlesztését tovább folytatja; a Bizottság által javasolt holisztikus megközelítés kiemelt jelentőségű;

2. az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közösségi keretszabályozásának felülvizsgálata során a hálózat- és információbiztonsággal egyik célkitűzésként foglalkozik;

3. továbbra is szerepet játszik annak érdekében, hogy fokozódjék a tudatosság a kéretlen elektronikus levelek, a kémprogramok és a számítógépes vírusok elleni küzdelem melletti általános politikai kötelezettségvállalás szükségessége iránt; megerősíti a harmadik országokkal folytatott párbeszédet és együttműködést, különösen a harmadik országokkal kötött megállapodásokon keresztül, ideértve a kéretlen elektronikus levelek, a kémprogramok és a számítógépes vírusok elleni küzdelem kérdését is;

4. a 460/2004/EK rendeletben lefektetett célokkal és feladatokkal összhangban, valamint a tagállamokkal és az érdekelt felekkel szorosabban együttműködve és a munkakapcsolatok szorosabbra fűzésével erősíti az ENISA bevonását az ezen állásfoglalásban meghatározott, a biztonságos európai információs társadalomra irányuló stratégia támogatásába;

5. az i2010 keretstratégia összefüggésében a tagállamokkal és valamennyi érdekelt féllel – elsősorban statisztikai és tagállami információbiztonsági szakemberekkel együttműködve – a biztonsággal és a bizalommal összefüggő vetületeket megcélzó közösségi felmérésekhez megfelelő mutatókat dolgoz ki;

6. a kritikus infrastruktúrák védelmére vonatkozó tervezett európai programhoz történő potenciális hozzájárulásként, a hálózati és információs rendszerek biztonságának és ellenállásának növelését célzó ágazat-specifikus ICT-politika kialakításának érdekében ösztönzi a tagállamokat arra, hogy tanulmányozzák – az érintett felekkel folytatott többoldalú párbeszéd útján – a gazdasági, üzleti és társadalmi mozgatóerőket;

7. folytatja az érintett nemzetközi partnerekkel és szervezetekkel folytatott párbeszéd előmozdítására irányuló, a tagállamokkal összehangolt erőfeszítéseit a hálózat- és információbiztonság terén folytatott világméretű együttműködés erősítése irányában, konkrétan a WSIS cselekvési irányvonalainak végrehajtása, valamint a Tanácsnak történő rendszeres jelentéstétel útján.

VALAMINT FELHÍV ARRA, HOGY

1. a 460/2004/EK rendeletben rögzített feladatok és célok megvalósítása, valamint annak érdekében, hogy segítse a Bizottságot és a tagállamokat a hálózat- és információbiztonság követelményeinek való megfelelést célzó erőfeszítéseikben, az ENISA továbbra is dolgozzon szoros együttműködésben a tagállamokkal, a Bizottsággal és a többi érdekelt féllel, ily módon járulva hozzá az ezen állásfoglalásban meghatározott, a biztonságos európai információs társadalomra irányuló stratégia végrehajtásához és továbbfejlesztéséhez;
2. az ezen állásfoglalásban meghatározott, a biztonságos európai információs társadalomra irányuló stratégiával összhangban valamennyi érdekelt fél javítsa a szoftverek biztonságát, valamint a hálózati és információs rendszerek biztonságát és ellenállását, és vegyen részt a meglévő eszközök és szabályozó eszközök jobb felhasználásának mikéntjéről szóló, az érdekelt felekkel folytatott többoldalú, strukturált vitában;
3. annak érdekében, hogy fejlettebb és biztonságosabb termékeket és szolgáltatásokat hozzanak létre, a vállalkozások pozitívan álljanak hozzá a hálózat- és információbiztonság kérdéséhez, és az ilyen termékekbe és szolgáltatásokba való befektetést tekintsék versenyelőnynek;
4. a gyártók és a szolgáltatók a biztonsági, a magánélet védelmét és a titokvédelmet szolgáló követelményeket értelemszerűen építsék be a termék-, a szolgáltatástervezésbe, a hálózati infrastruktúra kiépítésébe, az alkalmazások és szoftverek fejlesztésébe, valamint hajtsák végre és kísérjék figyelemmel a biztonsági megoldásokat;
5. az érdekelt felek folytassanak együttműködést, valamint az új technológiák és szolgáltatások biztonságos módon történő teszteléséhez és irányításához indítsanak kísérleti környezeteket; az érdekelt felek az új biztonságos technológiák és szolgáltatások kereskedelmi bevezetését követően időben alkalmazzák ezeket;
6. valamennyi érdekelt fél tegyen további erőfeszítéseket a kéretlen elektronikus levelek és más online jogsértő cselekmények ellen, valamint folytasson az illetékes hatóságokkal aktív együttműködést nemzeti és nemzetközi szinten;
7. a személyazonosság-lopás és egyéb, a magánélet sérelmére elkövetett támadások megelőzése és az ezek elleni küzdelem, valamint a megbízhatóság érdekében a szolgáltatók és az ICT-ipar fordítson fokozott figyelmet a termékekben, a folyamatokban és a szolgáltatásokban a biztonság, a magánélet védelme és a használhatóság javítására;
8. a hálózatüzemeltetők, a szolgáltatók és a magánszektor osszák meg egymással és hajtsák végre a bevált biztonsági gyakorlatokat, erősítsék a kockázatelemzés és -kezelés kultúráját a szervezetekben és vállalkozásokban azáltal, hogy megfelelő képzési programokat támogatnak és fejlesztik a vészhelyzeti tervezést, valamint szolgáltatásaik részeként ügyfeleik számára elérhetővé teszik a biztonsági megoldásokat.