JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

Tanulmány
az Európai Hálózati és Információs Biztonsági Ügynökségről
(European Network and Information Security Agency – ENISA)

készítette: dr. Varga Balázs

2004-2005

I. Kitekintés, előzmények

Manapság a legnagyobb közhelyek egyike az Internet mindent behálózó voltáról, nemzetközi jellegéről, az általa lehetségessé vált gazdasági és kommunikációs előrelépésekről beszélni. Nemcsak a gazdaságot, de mindennapi életünket is (kapcsolattartás, oktatás, pénzügyek, stb.) átalakítják a technika új vívmányai, az általuk biztosított újszerű lehetőségek. Ez a fejlődés természetesen az üzleti életben is jelentős hatásokat gerjeszt, hatása azonban nemcsak anyagilag jelentős, hanem a tetemes anyagi vonzatok miatt mindenkinek érdekében áll a fejlődés töretlensége, és ezen keresztül annak biztonsága is.

Többek között ezt is érintette Erkki Liikanen, az Európai Bizottság vállalatokért és információs társadalomért felelős tagja – akinek kulcsszerepe van az ügynökség létrejöttében - a hannoveri CEBIT kiállításon 2004. március 18-án tartott előadásában[1]. Szavai szerint *„a mai társadalomban sok múlik a hálózatokon és információs rendszereken. Ahogyan a hálózatok és a számítógépek továbbfejlődnek, és ahogyan az elektronikus kommunikáció mindennapi életünk minden egyes aspektusában szerepet kap, gyorsan növekszik a biztonság iránti igény is. A szélessávú elérés lehetővé teszi az emberek számára az always-on[2] létet. Ez természetesen megnöveli a rendszerek sérthetőségét és megtöbbszörözi a kibertámadások valószínűségét. A megnövelt biztonság így a szélessávú elérés kulcselemévé válik.”*

Említette továbbá a mostanság egyre inkább elterjedőben lévő vezeték nélküli kapcsolatok (pl. wifi, de ide tartozhatnak a folyamatosan fejlődő mobilkommunikációs jelenségek is) jelentőségét is, amelyek által az Internet gyakorlatilag bárhonnan elérhetővé válik. Így ahogyan növekszik az Internethez hozzáférők száma, a veszélyek ezzel egyenes arányban nőnek.

Erre szolgálhat példaként az alábbi két táblázat, amelyeket a cert.org, az egyik legnagyobb tekintélyű, biztonsággal foglalkozó weboldal közölt.

1http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.getfile=gf&doc=SPEECH/04/148|0|RAPID&lg=EN&type=DOC

2 A hálózaton töltött, azaz „online” állapot állandósága, tömeges elterjedése az átalánydíjas, nem percalapú kapcsolatoknak (xDSL, kábelnet) köszönhető

1. sz. ábra a napvilágra került Internettel kapcsolatos sebezhetőségek számáról (Forrás: www.cert.org)

Megismert sebezhetőségek száma					
1995-1999					
Év	1995	1996	1997	1998	1999
Sebezhetőség	171	345	311	262	417
2000-2004					
Év	2000	2001	2002	2003	2004
Sebezhetőség	1090	2437	4129	3784	3780
Összesen 1995-2004 :					**16726**

Erkki Liikanen vélekedése szerint – amelynek igazságtartalma vitán felül áll - az információs rendszerek rendestől eltérő működése pedig mindenkire kihat, az állampolgárokra csakúgy, mint az üzleti szervezetekre és a közszférára.

Ennek alátámasztására szolgálhat a következő táblázat, mely az Internet-penetráció növekedését hivatott bemutatni.

2. számú ábra a világ népességéről és az Internet-elterjedtségéről (Forrás: www.internetworldstats.com)

Globális táblázat az Internet-felhasználásról, és vele összefüggésben a populációról						
Világrészek	**Populáció (becs. 2005)**	**Populáció a világ %-ban**	**Internet használata**	**Felhasználás növekedése (2000-2005)**	**Elterjedtség (népesség %-ban)**	**Felhasználók világ %-ban**
Afrika	900,465,411	14.0 %	**12,937,100**	186.6 %	1.4 %	1.6 %
Ázsia	3,612,363,165	56.3 %	**266,742,420**	133.4 %	7.4 %	32.6 %
Európa	730,991,138	11.4 %	**230,923,361**	124.0 %	31.6 %	28.3 %
Közép-Kelet	259,499,772	4.0 %	**17,325,900**	227.8 %	6.7 %	2.1 %
Észak-Amerika	328,387,059	5.1 %	**218,400,380**	102.0 %	66.5 %	26.7 %
Latin-Amerika, Karibi térség	546,917,192	8.5 %	**55,279,770**	205.9 %	10.1 %	6.8 %
Ausztrália Óceánia	33,443,448	0.5 %	**15,838,216**	107.9 %	47.4 %	1.9 %
Összesen	**6,412,067,185**	**100.0 %**	**817,447,147**	**126.4 %**	**12.7 %**	**100.0 %**

Nem véletlen, hogy a fejlődéssel párhuzamosan a „kimarad, ha lemarad” elv alapján – és nemcsak hazánkban – kormányzati erőfeszítések is történnek az elterjedtség növelésére, mivel ezen új lehetőségek meglovagolása jelentős mértékű profittal kecsegtet mind anyagi mind tudományos, oktatási téren.

Természetesen az e téren bekövetkezett fejlődést nemcsak a nemzeti kormányzatok nem nézhetik ölbe tett kézzel, de az Európai Unió szervei sem maradhatnak tétlenek.

A továbbiakban az Európai Bizottság, illetve az Unió más szervei által koordinált tevékenységeket veszem górcső alá, a nemzeti kormányzatok e téren tett erőfeszítései meghaladnák e tanulmány kereteit.

Eme erőfeszítések sorába illeszkednek az eEurope Action Plan néven ismert akciótervek, melyek közül a legújabb az eEurope Action Plan 2005, mely a jelenlegi folyamatokat is alapjaiban meghatározza. Az azt megelőző, eEurope2002 akcióterv jelentős eredményeket ért el az Internet-hozzáférés elterjesztésében a lakosság és az üzleti szervezetek között.

Új irányvonalat adott a kommunikációs hálózatokra vonatkozó szabályozásnak, és új utakat nyitott az új generációs mobil és multimédiás szolgáltatások terén. Lehetőségeket nyújtott az emberek számára a társadalom vérkeringésébe történő bekapcsolódásra, és segítséget nyújtott a munkaerőpiac szereplőinek arra, hogy megszerezzék a tudásalapú gazdaságban szükséges tudást. Uniószerte hozzájárult az Internet-hozzáférésnek az iskolákban történő elterjesztéséhez, a kormányzatok online megjelenéséhez, és a figyelmet a biztonságosabb online-lét biztosítására irányította. [3]

Az Európai Tanács barcelonai ülésén felkérték a Bizottságot, hogy készítsen akciótervet, mely a hangsúlyt arra helyezi, hogy a *„szélessávú hálózatok Unión belüli széleskörű elérhetőségét és használatát biztosítsa 2005-re, az IPv6[4] internetes protokoll fejlesztését [segítse elő] (...), továbbá biztosítsa a hálózatok és az információ, az eGovernment, eLearning, eHealth és eBusiness biztonságát”*[5].

A kész akciótervet, melyet az Európai Bizottság 2002. május 28-án végleges formájában előterjesztett, az Európai Tanács 2002. június 21-22-i sevillai ülésén fogadták el.

Ennek lényege a bevezetőben foglaltak alapján, hogy *„megfelelő környezetet teremtsen a magánberuházások és az új munkahelyek teremtése számára, elősegítse a produktivitást, modernizálja a közcélú szolgáltatásokat, és mindenkinek lehetőséget biztosítson arra, hogy a részt vehessen a globális információs társadalomban. Az eEurope2005 ennélfogva azt célozza, hogy stimulálja a széleskörűen elérhető szélessávú infrastruktúrán alapuló*

3http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf 2. oldal

4 Új generációs ip-protokoll, lásd többek között: http://ipv6.6bone.hu

5http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf 8. oldal

biztonságos szolgáltatásokat, alkalmazásokat és tartalmakat."[6]

Az eEurope2005 célja volt többek között az is, hogy továbbvigye az Európai Tanács feirai ülésén elfogadott eEurope2002 akciótervet. Továbbá az eEurope2005 a Lisszaboni Stratégia[7] része, melynek hosszútávú céljai között szerepel, hogy az Európai Unió legyen 2010-re a leginkább versenyképes és dinamikus tudásalapú gazdaság, mely fejlett foglalkoztatottsággal és szociális kohézióval rendelkezik. Azonban a Lisszaboni Stratégia nem csupán a produktivitásról és a növekedésről, de a foglalkoztatásról és a szociális kohézióról is szól, ennek megfelelően az eEurope2005 akcióterv a felhasználókat helyezi a középpontba. Célkitűzései között szerepel, hogy növeli a participációt, esélyt biztosít mindenkinek, és növeli az általános tudásszintet.

Az akcióterv két fő tevékenységcsoportot ölel fel, az első csoportba tartozó tevékenységek (modern online közszolgáltatások, eGovernment, eLearning, eHealth, a dinamikus eBusiness környezet megteremtése) arra irányulnak, hogy elősegítsék, stimulálják a szolgáltatások, alkalmazások és tartalmak körét, a másik tevékenységcsoport pedig a szélessávú elérés versenyképes áron való széleskörű elérésének biztosításán és a biztonságos információs infrastruktúrán keresztül ennek alapfeltételeire koncentrál. Ezek mindegyikének kifejtésétől ehelyütt eltekintek, a tanulmány címének is megfelelően a biztonság kérdésére koncentrálok, melyet az akcióterv 3.1.3. pontjában fejtettek ki részletesebben.

Az Európai Uniónak már létezik összehangolt stratégiája a hálózati biztonságról[8], az informatikai bűnözésről (a Budapesten elfogadott ún. Cybercrime-egyezmény)[9], továbbá létezik adattovábbítási irányelv is. Az akcióterv tartalmazza, hogy milyen intézkedéseket kell tenni (figyelemfelhívó kampányok, a helyes gyakorlat propagálása, fejlettebb információcsere-mechanizmusok kiépítése), illetőleg milyen szervezeteket (pl. Cyber Security Task Force) kell felállítani 2002 végéig.

Az akciótervben az szerepel, hogy a Cyber Security Task Force-nak 2003 közepére működnie kell.

Itt jelenik meg tehát először a későbbi ENISA gondolata. Az eEurope2005 akcióterv lényegében az ENISA által is magáénak vallott feladatokat sorolja fel, így többek között azt, hogy a biztonsággal kapcsolatos kérdésekben hatásköri gyűjtőpontként kell funkcionálnia, így (az akciótervben foglaltak alapján) pl. ki kell alakítania a tagállamokkal egy egységes európai támadásra figyelmeztető rendszert, intézményesítenie kell a pillérek közötti kommunikációt,

6http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf 6. oldal

7 http://europa.eu.int/comm/lisbon_strategy/index_en.html

8 Network and Information Security: Proposal for A European Policy Approach, COM(2001) 298 of 6.6.2001.

9 Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890 of 22.1.2001.

és erősítenie a határokon átívelő kooperációt.

A Bizottságnak az ENISA felállítását szorgalmazó javaslatát a Parlament és a Tanács (mely jelen esetben természetesen a tagállamok kommunikációs és telekommunikációs minisztereiből állt) első olvasatban, kompromisszumra jutva elfogadta, hogy az ügynökség a munkát mielőbb megkezdhesse.

II. Az ügynökségről szóló 460/2004 EC számú rendelet

Az ENISA-t végül az Európai Parlament és az Európai Tanács 460/2004 számú rendelete hozta létre 2004. március 10-én.
A rendelet hat részből (section) és 28 cikkből (article) áll.
A bevezető rész 29 bekezdésből áll, itt határozták meg létrejöttének okait, a hatásköri elhatárolásokat és az alapvető célkitűzéseket.
Az első rész (1-4. cikk) a hatásköröket**,** célokat és feladatokat tartalmazza, a második rész (5-8. cikk) a szervezettel foglalkozik, a harmadik rész (9-14. cikk) a működést tárgyalja.
A negyedik részben (15-17. cikk) van szó a pénzügyekről, az ötödikben (18-24. cikk) az általános feltételekről, az utolsó, hatodik rész a hatálybalépéssel, az ügynökség fennállásával stb. foglalkozik.

A rendelet bevezető része

A bevezető rész hangsúlyt fektet a részben már általam is vázolt körülményekre, sőt, a telekommunikáció fontosságát az elektromosság és vízellátás alapvető jellegéhez hasonlatosan írja le. Továbbá megfogalmazza, hogy a telekommunikációs és információs rendszerek biztonsága, különösképp azok rendelkezésre állása nagyon fontos, mivel a kulcsrendszerek hibái, melyeket azok komplexitása, továbbá hibák, balesetek, támadások idézhetnek elő, kihathatnak az EU polgárai számára kulcsjelentőségű fizikai szolgáltatások meglétére is.
Erkki Liikanen már említett hannoveri beszédében ezzel kapcsolatban kihangsúlyozta, hogy a megfelelő egyensúlyt kell megtalálni a hálózati és információs biztonság területén. Úgy fogalmazott, hogy az e téren megjelenő európai erőfeszítések három fő kategóriába esnek. Az első az, hogy megfelelő jogi kereteket kell biztosítani a telekommunikációnak és az adatvédelemnek, másodszorra szabályrendszert kell alkotni a kiberbűnözésre, beleértve az infrastruktúra és az információs rendszerek védelmét, harmadszorra pedig az ENISA és az eEurope akciótervek e téren betöltött fontos helyzetét hangsúlyozta ki.
Szól továbbá a rendelet bevezető része arról is, hogy betörések már így is óriási anyagi károkat okoztak, aláásták a felhasználók biztonságérzetét, és hátráltatták az e-kereskedelem elterjedését. Ezekkel szemben magánszemélyek, szervezetek és vállalkozások kifejlesztettek biztonsági technológiákat és biztonságmenedzselési eljárásokat, a tagállamok pedig támogató intézkedéseket foganatosítottak, mint például információs kampányok, kutatási projektek, hogy ezáltal elősegítsék a hálózati és információs biztonságot a társadalomban.

Megemlíti továbbá a bevezető rész a Tanács 2002/21/EC sz. rendeletét, amely a nemzeti hatóságok számára határoz meg feladatokat. Ezek közé tartozik az egymás közötti és a Bizottsággal való transzparens kooperáció annak érdekében, hogy konzisztens gyakorlati szabályozás alakulhasson ki a személyes adatok és a magánélet biztonságának, a közcélú hálózatok integritása és biztonsága biztosításának érdekében.

A (11) bekezdésben kiemeli a rendelet az ügynökség függetlenségét és átláthatóságát, továbbá kimondja, hogy az ügynökség nemzeti és közösségi erőfeszítésekre épít, ezáltal a tagállamokkal a legteljesebb kooperációban működik, de az ipar és más jelentős szervezetek kezdeményezéseire is nyitott, mivel az elektronikus hálózatok túlnyomórészt magánkézben vannak, ezért az onnan érkező adatok is fontosak, továbbá a privátszektorral való kommunikáció is elengedhetetlen.

E passzus véleményem szerint igen helyesen egyensúlyt keres a köz- és magánszféra között, tulajdonképpen bevallva, hogy e téren a közszféra erőfeszítései lényegében nem elegendők, így a felülről történő építkezés eleve kudarcra ítéltetett. A privátszektorral a szakemberek díjazása terén a közszféra nem versenyezhet, így sokkal kifizetődőbb az ott már amúgy is meglévő alkotó jellegű szellemi potenciál kihasználása, annak bevonása a közszféra iránymutatása, koordinációja mellett.

Az ügynökség függetlensége pedig hozzájárul ahhoz, hogy megteremtse az ipar bizalmát, és elősegítse direkt közreműködését az európai biztonsági problémák azonosításában és megoldásában.

A (12) bekezdésben a rendelet megteszi az elengedhetetlen hatásköri elhatárolásokat, lényegében kijelölve, mely területek tartoznak az ügynökség hatáskörébe, eszerint az ügynökség gyakorlata a következő hatáskörökkel, jogosítványokkal nem ütközhet, nem létesülhet előfoglalás (pre-emption), azokat nem gátolhatja**,** illetve nem állhat velük átfedésben:

- A nemzeti hatóságok szabályozási tevékenységével, amint azt az ide vonatkozó, az elektronikus kommunikációról, hálózatokról és szolgáltatásokról szóló rendeletek is meghatározzák, továbbá a 2002/627/EC rendelet által létrehozott European Regulators Group for Electronican Communications Networks and Services, illetőleg a 2002/21/EC által hivatkozott Communications Commitee tevékenységével;
- Az európai és nemzeti harmonizációs testületek, a Standing Commitee tevékenységével, mint az a 98/34/EC rendeletben is meghatározott, mely lefektetett egy eljárást a technikai standardok, az Információs Társadalmi Szolgáltatások (Information Society Services) terén létrejövő szabályozások és szabályok terén;
- A tagállamoknak a magánszemélyeknek a személyes adatok feldolgozása és ezen

adatok szabad áramlása felett gyakorolt felügyeleti tevékenységével.

Ezután a rendelet kimondja, hogy az ügynökségnek elemeznie kell a fennálló, és a későbbiekben felmerülő kockázatokat, melynek érdekében információkat gyűjthet, jellemzően kérdőívekkel, azonban e tevékenysége során nem róhat új kötelezettségeket a privátszektorra vagy a tagállamokra. E szakasz tovább erősítheti a bizalmat a szervezet iránt, és főként annak klasszikus hatósági jellege ellen szól, ami a bizalom megteremtésének egyik sarokköve lehet, azonban magában rejtheti az együttműködési készség esetlegességét, továbbá az esetlegesen mégis szükséges további információk beszerzésének bürokratikus nehézségeit.
Ehelyütt szól továbbá a rendelet a hálózati és információs biztonság területén felmerülő kockázatok – mind a jelenleg fennállók, mind a jövőben esetleg felmerülők – megértésének szükségességéről.
A (14) bekezdés arról a bizalomról szól, amelyet a kívánalmaknak megfelelően a hálózatok és információs biztonság területén tájékozott magánszemélyek, üzleti szervezetek, nyilvános testületek megfelelő informáltsága, oktatás és képzése hoz létre e területen. A közcélú testületeknek ebben nagy szerepe van, ennek továbbfejlesztése szükséges. Az odafigyelési készség növelését célzó akciók során – melyben a tagállamok kommunikációjának óriási szerep jut – az ügynökség az odafigyelési készség növelését célzó gyakorlati tanácsaival, képzésével és kurzusaival szintén szerephez jut. E téren Erkki Liikanen is megemlítette, hogy az Internetet 2003-ban elárasztó vírus- és wormáradat felveti a szorosabb kooperáció szükségességét.
A későbbiekben szó esik arról, hogy az ügynökség a magas szintű hálózati és információs biztonság és annak kultúrájának megteremtése kapcsán végső soron a belső piac működésének zavartalanságát segíti elő (ezen érvnek Erkki Liikanen is több helyütt hangot adott), továbbá arról is, hogy a fenti célok elérése érdekében kockázatmérési módszereket kell kidolgozni illetve megismertetni úgy a privát- mint a közszektor szereplőivel, valamint arról, hogy e folyamat során felhasználandók a közösségi kutatási eredmények is.
Ezenfelül annak érdekében, hogy amennyiben ez céljai elérését szolgálja, az ügynökség tapasztalatot illetve információkat cserél az Európai Unió joga szerint létrehozott testületekkel illetve ügynökségekkel.
A (19) bekezdés egyfajta általános ismertetőként arra világít rá, hogy a biztonsági ügyek globális problémát képeznek, így globális szinten történő szorosabb kooperációra van szükség a biztonsági szabványok és az információáramlás fejlesztése területén, továbbá egyfajta egységes megközelítés kidolgozására, hogy elérhető legyen a biztonsági és információs kultúra kialakítása és elterjesztése.

Erkki Liikanen véleménye szerint pontosan ezen kultúra és a szervezetben megnyilvánuló szakértelem kettőse játszik majd kulcsszerepet Európa digitális gazdaságának és információs társadalmának fejlesztésében. A harmadik országokkal és a globális közösséggel való hatékony kooperáció európai szintű feladattá vált, így az ügynökségnek feladata a harmadik országokkal és amennyiben szükséges nemzetközi szervezetekkel való közösségi együttműködéshez való hozzájárulás. A nemzetközi szervezetek és nemzetközi együttműködés terén megemlítendő a G8 államok, az OECD és az ENSZ keretein belül történő együttes munka.

Megjegyzi továbbá a bevezető, miszerint az ügynökségnek feladatai ellátása során különös figyelmet kell fordítania a kis- és közepes méretű vállalatokra.

A CASES projekt

Ennek kapcsán utalnék a CASES (Cyberworld Awareness and Security Enhancement Structure) projektre, mely több kezdeményezéshez is kapcsolódik mind európai, mind világszinten, ezek közé tartozik pl. az eEurope2005 akcióterv, az OECD Információs Rendszerek és Hálózatok Irányvonala, illetve az eEurope2005 akcióterv végrehajtását figyelő többéves program. [10]

A CASES projekt kifejezetten a végfelhasználók és a kis- és közepes méretű vállalatok oktatását, a felkészültségi szint növelését és támogatást irányozza elő. Ennek kapcsán erősíti az információs társadalomba vetett bizalmat, hozzájárulva ezzel ahhoz, hogy a megcélzott csoportok tagjai lehessenek az információs társadalomnak, illetve profitálhassanak az e-kereskedelem és e-government szolgáltatásaiból. Egyfajta mechanizmust épít ki, mely alkalmas arra, hogy azon keresztül a különböző szervezetek együttműködhetnek, gyorsan oszthatnak meg know-how-t, illetve a megelőzést, védekezést, beavatkozást és felderítést érintő információkat. Jelenleg a projekt két fő területre összpontosít, mégpedig a készültségi szint növelésére és a megelőzésre.

Munkájára azért van elsősorban szükség, mert pont az általa megcélzott csoportok nem tudnak – a nagyvállalatokkal, más, erre felkészült, szakembergárdával rendelkező szervezetekkel szemben – megfelelő módon védekezni olyan kihívások ellen, mint pl. amit a vírusok, wormok, DDoS támadások, spam stb. jelentenek.

Több felmérés[11] tanúsága szerint is – bár nagy jelentőséget tulajdonítanak a problémának - a kis- és közepes vállalkozások egyelőre nem képesek megfelelő szinten felvenni a harcot az

10 http://brief.weburb.dk/frame.php?loc=archive/00000113/

11 pl. http://ccnmag.com/story.php?id=340

internetes veszélyekkel.

A citált cikk egy részlete alapján kiválóan jellemezhető a helyzet: *„Noha a kis-és közepes méretű vállalatokat nem éri olyan gyakran támadás mint a nagyvállalatokat, azonban rendkívül sebezhetőek tömeges számítógépes támadások, mint pl. worm- és vírustámadások esetén. Ezenfelül a nagyvállalatok biztonsága sokkal jobb most, mint a múltban volt, ezért a hackereket ez arra bíztatja fel, hogy kis- és közepes vállalatokban lássanak könnyű célpontot”* (Russell Morgannek, az ITSPA - Information Technology Solution Providers Alliance – vezetőjének nyilatkozata)

Az ENISA-t létrehozó rendelet bevezetőjének későbbi szakaszai – a függetlenségét, költségvetését, fennálltának idejét taglaló részeken túl - már a szervezeti felépítéshez kapcsolódó tényezőket tárgyalják, így ezek ismertetésére az adott területek tárgyalása során kerítek sort.

III. Az ügynökség hatásköre, céljai, feladatai

Az első rész, mely a hatásköröket, célokat és feladatokat (továbbá az alapvető definíciókat) tartalmazza, első cikkében, mely a hatáskörökről szól, lényegében megismétli a fent már tárgyalt célokat, deklarálva egyidejűleg az ügynökség létrejöttét.
Ugyanezen rész második pontja deklarálja, miszerint az ügynökségnek a Közösség, a tagállamok, valamint az üzleti szervezetek munkáját elősegítve kell azon dolgoznia, hogy azok a hálózati és információs biztonság követelményeit elérjék, ezáltal biztosítva a belső piac európai jogalkotásban jelenleg foglalt, és későbbiekben megjelenő céljainak teljesülését, mint az pl. a 2002/21/EC irányelvben is megjelenik.
Az első cikk harmadik pontja kimondja, miszerint az ügynökség céljai és feladatai nem sérthetik a tagállamok hálózati és információs biztonsággal kapcsolatos, az Európai Közösségről szóló szerződésben foglaltakon kívül eső, mint például az Európai Unióról szóló Maastrichti Szerződés V. és VI. címében említett kompetenciáit, illetve a közbiztonsággal, védelemmel, nemzetbiztonsággal kapcsolatos, továbbá más, a büntetőjog körébe eső tevékenységeit.
A rendelet második cikke tartalmazza azon célokat, amelyek elérésére az ügynökség fennállása alatt hivatott. A szöveg négy ilyen fő célt említ, ezek a következők:

- Az ügynökség elősegíti a Közösség, a tagállamok, és ezáltal az üzleti szervezetek azon képességét, hogy megelőzzék, azonosítsák a hálózati és információs biztonsággal kapcsolatos problémákat, és azokra megfelelő válaszokat adjanak.
- Az ügynökségnek a rendelet által meghatározott körbe eső, hálózati és információs biztonságot érintő, kompetenciájába tartozó kérdésekben segítséget nyújt és tanácsokkal szolgál a Közösségnek és a Tagállamoknak.
- Közösségi és nemzeti erőfeszítésekre építve az ügynökségnek magas színvonalú gyakorlatot kell kialakítania. Az ügynökségnek erre a gyakorlatra építve kell elősegítenie a közszféra és a privátszféra képviselőinek széleskörű kooperációját.
- Az ügynökségnek felkérésre segítenie kell a Bizottságot a hálózati és információs biztonságot érintő közösségi jogalkotás aktualizálására és fejlesztésére irányuló technikai előkészítő munka során.

A 3. cikk tartalmazza azon tevékenységeket, melyeket az ENISA ellát annak érdekében, hogy a fentebb vázolt feladatainak eleget tegyen. E tevékenységek a következők:

- Az ügynökség feladata a jelenlegi és felmerülő kockázatok elemzéséhez szükséges információk gyűjtése, ezenfelül különösen azon európai vonatkozású információké, melyek az elektronikus kommunikációs hálózatok rugalmasságára és rendelkezésre állására, továbbá a rajtuk keresztül elért ill. rajtuk keresztül továbbított információk azonosíthatóságára, integritására és megbízhatóságára hatással lehetnek, és az ügynökség az ilyeténformán analizált információkat a Bizottság és a tagállamok rendelkezésére bocsátja;
- tanáccsal látja el, és felkérésre céljai körébe eső ügyekben segíti az Európai Parlamentet, a Bizottságot, az európai ill. a tagállamok által kijelölt nemzeti testületeket;
- elősegíti a hálózati és információs biztonság területén tevékenykedő egyes szereplők közötti kooperációt, többek között azzal, hogy rendszeresen konzultál az ipar, az egyetemek és más érdekelt szektorok képviselőivel, továbbá kapcsolati hálózatot épít ki a közösségi testületek, a tagállamok által megjelölt közszektori testületek, illetőleg a privátszektor és a fogyasztói testületek felé;
- kooperációt teremt a Közösség és a tagállamok között a hálózati és információs biztonsági problémák megelőzését, azonosítását, és az azokra adandó válaszokat érintő közös módszerek megteremtése érdekében;
- hozzájárul a készenléti szint növeléséhez, és az információs és hálózati biztonságot érintő, időszerű, objektív és átfogó információk minden felhasználó részére történő elérhetőségéhez többek között az aktuálisan legjobb gyakorlat kicserélésének elősegítésével, beleértve a felhasználók figyelmeztetését és a köz- illetve magánszektor kezdeményezései közötti összhang megteremtését is;
- segítséget nyújt a Közösségnek és a tagállamoknak az iparral folytatott párbeszédéhez a hardver- és szoftvertermékekben megbújó biztonsági hibák meghatározása során;
- elősegíti az információs és hálózati biztonsággal kapcsolatos termékekre és szolgáltatásokra vonatkozó standardok kidolgozását;
- tanácsokkal látja el a Bizottságot a hálózati és információs biztonság területén történő kutatás, illetve a kockázatmegelőző technológiák hatékony használata terén;
- propagálja a kockázatmérési tevékenységeket, kockázatmérési megoldásokat és a megelőzés-menedzselő megoldásokról szóló köz- és magánszektori tanulmányokat;
- hozzájárul a Közösség harmadik országokkal, és amennyiben szükséges nemzetközi szervezetekkel történő együttműködéséhez, hogy elősegítse az információs és hálózati biztonsággal kapcsolatos ügyekben történő közös globális megközelítés kidolgozását,

ezáltal hozzájárul a hálózati és információs biztonság kultúrájának kialakításához;

- független módon kifejti következtetéseit, iránymutatásait, és tanácsokkal szolgál a hatásköre és céljai körébe eső területeken.

Mint azt a fentiek is nyilvánvalóvá teszik, az ügynökségnek nem feladata semmiféle hatósági vagy kvázi-hatósági feladat ellátása, szerepe arra korlátozódik, hogy segítse és összefogja azokat a folyamatokat, kezdeményezéseket, melyek az információs és hálózati biztonság megteremtésére irányulnak.

Elsőként az információgyűjtés szerepel a tevékenységek felsorolásánál, ami az információalapú gazdaságban – sőt, társadalomban – elengedhetetlen, és minden további tevékenységnek is az alapját képezi. Gyakorlatilag az ügynökség tevékenységét főként ezen információkra támaszkodva végzi, ezeken keresztül mint egyfajta közös információs bázis, illetve információs központ, tájékoztatja a magasabb rendű döntéshozó szerveket, illetve előkészítő-segítő munkát végez, továbbá koordinációs szerepének megfelelően az e téren született kezdeményezéseket összefogja.

IV. Az ügynökség szervezete

A rendelet második része az ügynökség szervezeti felépítésével foglalkozik, eszerint három fő részt különböztethetünk meg az ENISA vezetésében, a menedzsment-testületet, az ügyvezető igazgatót és az állandó tagok csoportját.

A menedzsment-testület

A menedzsment-testület tagjai közé minden tagállam jelöl egy-egy személyt, további három tagot jelöl a Bizottság, továbbá a Bizottság javaslatára három tagot a Tanács jelöl ki, ez utóbbiaknak nincsen szavazati joguk, és mindegyikük egy-egy specifikus területet képvisel (ezek: információ- és kommunikációs technológiai ipar, fogyasztói csoportok, a hálózati és információs biztonság akadémiai szakértői). A testület tagjai kiválasztásánál képzettségük és gyakorlatuk dominál, továbbá utóduk egyidejű megjelölése mellett visszahívhatók.

A testület tagjai sorából elnököt illetve elnökhelyettest választ két és fél éves, megújítható időszakra. Az elnökhelyettes ex officio helyettesíti az elnököt, amennyiben az feladatát képtelen ellátni.

Eljárási rendjét a Bizottság előterjesztése alapján maga állapítja meg. Amennyiben máshogyan nem rendelkezik, a testület főszabályként a szavazati joggal rendelkező tagok szótöbbségével dönt. Kétharmados döntés szükségeltetik az ügynökség belső eljárási rendjének megállapításához, a költségvetés és az éves munkaterv elfogadásához, továbbá az ügyvezető igazgató kinevezéséhez és eltávolításához.

A menedzsment-testület üléseit az elnök vezeti. Évente két rendes ülésre kerül sor, illetve az elnök vagy három rendes – szavazati joggal rendelkező – tag indítványára rendkívüli ülések hívhatók össze. Az ügyvezető igazgató az üléseken szavazati jog nélkül vesz részt.

A belső eljárási rendet, mint már említettem, a menedzsment-testület állapítja meg a Bizottság tárgyév előtti év november 30-ig előterjesztett javaslata alapján, és e rendet köteles nyilvánosságra hozni. Ezenfelül a menedzsment-testület határozza meg az ügynökség működésének alapvető irányvonalait, melynek során biztosítania kell azt, hogy az ügynökség a 12-14. és 23. cikkekben foglaltaknak megfelelően, továbbá a tagállami és közösségi erőfeszítésekkel összhangban végzi munkáját.

Az ügyvezető igazgató

Az ügynökséget az ügyvezető igazgató vezeti, aki munkája ellátása során teljes függetlenséget élvez. Az ügyvezető igazgatót a menedzsment-testület nevezi ki öt éves időtartamra a Bizottság által adott névsorban szereplők közül, ahova az Európai Unió Hivatalos Lapjában

(figyelemfelkeltés céljából máshol is) meghirdetett nyílt pályázat útján lehet jelentkezni. Kinevezését megelőzően, de az után, hogy a menedzsment-testület megnevezte a jelöltet, annak részt kell vennie az Európai Parlament előtti meghallgatáson, ahol hozzá kérdések intézhetők.

E szükségszerű meghallgatáson felül az Európai Parlament és a Tanács bármikor meghallgathatja az ügyvezető igazgatót az ügynökség tevékenységi körébe tartozó kérdésekben.

Tevékenységi – és felelősségi – körébe tartozik többek között az ügynökség mindennapi munkájának vezetése, az éves munkaterv javaslatának elkészítése, a munkatervben foglaltak és a menedzsment-testület által elfogadottak végrehajtása, biztosítja azt, hogy az ügynökség feladatait azok érdekének megfelelően végzi, akik szolgáltatásait igénybe veszik, különös tekintettel e szolgáltatások megfelelő voltára. Ezen kívül az ügyvezető igazgató feladatai közé tartozik a költségvetési javaslat (becsült bevételek és kiadások) elkészítése és a költségvetés végrehajtása, a személyzeti ügyek, az Európai Parlamenttel való kapcsolat fejlesztése és fenntartása, az EP megfelelő bizottságaival történő rendszeres párbeszéd, továbbá az üzleti szervezetekkel és fogyasztói csoportokkal való kapcsolat fejlesztése és fenntartása, ezáltal a megfelelő állandó tagokkal való rendszeres párbeszéd, illetve az Állandó Tagok Csoportja ülésein való elnökölés.

Az ügyvezető igazgató minden évben köteles az éves munkáról szóló jelentést, illetve a következő évre vonatkozó munkaterv-tervezetet a menedzsment-testületnek jóváhagyásra benyújtani. A munkatervet a testület jóváhagyása után köteles az Európai Parlamentnek, a Tanácsnak, a Bizottságnak és a tagállamoknak továbbítani, és azt nyilvánosságra hozni. Ugyanez vonatkozik az éves jelentésre is, a továbbítás során azonban a tagállamok kimaradnak, ellenben kötelező azonban azt megküldeni a Számvevőszéknek, továbbá a Gazdasági és Szociális Tanácsnak, valamint a Régiók Tanácsának.

Amennyiben az ügynökség körülményeibe, céljai és feladatai közé illeszkedik, az ügyvezető igazgató szakértőkből álló, technikai és tudományos kérdésekkel foglalkozó ad-hoc munkacsoportokat is létrehozhat az állandó tagok csoportjával való konzultáció után, a menedzsment-testület értesítése mellett. Az ezen munkacsoportok működésére vonatkozó szabályokat a belső működési rend állapítja meg.

Az állandó tagok csoportja

Az ügyvezető igazgatónak létre kell hozni egy olyan, szakértőkből álló testületet, mely az állandó tagokat (információs és kommunikációs technológiai ipar, fogyasztói csoportok, a hálózati és információs biztonság akadémiai szakértői).

A csoport tagjainak számára, összetételére, kinevezésük rendjére, a csoport működésére vonatkozó szabályokat az ügynökség belső eljárási rendje tartalmazza, mely nyilvános.
A csoport elnöki teendőit az ügyvezető igazgató látja el. Tagjai mandátuma két és fél évre szól. Tagjai nem lehetnek egyidejűleg a menedzsment-testület tagjai is.
A Bizottság képviselőinek joguk van a csoport ülésein és munkájában részt venni.
A csoport az ügynökségről szóló rendeletben foglaltak alapján az ügyvezető igazgató munkáját a munkatervre irányuló javaslattal segíti, és biztosítja a rendszeres kommunikációt az állandó tagokkal.

V. Az ügynökség működése

A rendelet harmadik része foglalkozik a tulajdonképpeni működéssel. Főbb pontjaiban – az elfogultság bejelentése mellett - a munkatervről, az ügynökséghez érkező megkeresésekről, az átláthatóságról, a megbízhatóságról és a dokumentumok elérhetőségéről van szó.

A munkaterv

Az ENISA-nak munkáját a fent már említett munkaterv alapján kell végeznie. Ez azonban nem jelenti azt, hogy az ügynökségnek ne lehetne olyan, előre nem látható tevékenységeket felvállalnia, melyek hatásköre és céljai körébe esnek, és amelyek a megengedett költségvetésen belül vannak.

Az ügynökség megkeresése

Az ügynökség hatáskörébe, céljai és feladatai körébe illeszkedő tanácsadás iránti megkereséseket az ügyvezető igazgatónak kell címezni, mellékelve az ügyet kifejtő háttérinformációkat. Az ügyvezető igazgatónak a megkeresésekről értesítenie kell a Bizottságot. Ilyen megkereséseket az Európai Parlament, a Bizottság és a tagállamok által kijelölt bármely kompetens nemzeti szervezet tehet.

Átláthatóság

Az ügynökségnek biztosítania kell, hogy tevékenységét magas szintű átláthatósággal, és a 13. és 14. cikkekben foglaltaknak (megbízhatóság és dokumentumokhoz való hozzáférés szabályai) megfelelően látja el.

Megbízhatóság

A dokumentumokhoz való hozzáférést tartalmazó szakasz megsértése nélkül az ügynökség nem adhat ki harmadik személyek részére általa feldolgozott vagy kapott olyan információt, melynek bizalmas kezelése szükséges.

Ez a kitétel vonatkozik a tisztségviselőkre (ügyvezető igazgató, menedzsment-testület, állandó tagok csoportjának képviselői), a külső képviselőkre és a munkatársakra munkaviszonyuk megszűnte után is, továbbá az ügynökségnek belső eljárási rendjében is le kell fektetnie a megbízhatóságra vonatkozó szabályokat.

Dokumentumokhoz való hozzáférés

Az Európai Tanács EC 1049/2001. számú rendelete szabályozza e kérdéskört. A menedzsment-testületnek kell e kérdéskört a fenti rendelet szabályai szerint rendeznie, mégpedig az ügynökség felállításától számított fél éven belül.

Általános és záró rendelkezések

A fenti passzusokat a költségvetés megalkotásával – ezeket részben már érintettem – illetve felhasználásával kapcsolatos rendelkezések követik. Ezekre külön nem térnék ki, hiszen a szorosabb értelemben vett működéshez e problémakör nem tartozik hozzá.

A rendelet ötödik része általános rendelkezéseket tartalmaz, így az ügynökség jogi státuszára, a munkatársakra, az előjogokra és mentességekre, felelősségre, a nyelvhasználatra, a személyes adatok védelmére és harmadik országok részvételére vonatkozóan.

Ezek közül sem mindegyik bír alapvető fontossággal, így csupán néhány pont kiemelésével kívánom e részt tárgyalni.

Jogi státusz

Az ügynökség a Közösség testülete, valamint jogi személy. A tagállamokban az ügynökségnek a legteljesebb jogi személyiséggel kell rendelkeznie a tagállamok joga szerint, így ingó és ingatlan vagyont szerezhet, és azzal rendelkezhet, továbbá perképes. Képviseletében az ügyvezető igazgató jár el.

Felelősség

Az ügynökség szerződésekért való felelősségére a kérdéses szerződés jogát kell alkalmazni. Szerződésen kívüli károkozás esetén (okozza bár azt az ügynökség vagy valamely munkavállalója munkaköre ellátása során) a tagállamok jogának megfelelően az ügynökség felelősséggel tartozik. A munkavállalóknak az ügynökséggel szembeni felelősségét a jelentkezésük idején irányadó feltételek szerint kell elbírálni.

Harmadik országok részvétele

Az ügynökségnek nyitottnak kell lennie olyan harmadik országok részvételére, amelyek olyan egyezményt kötöttek az Európai Unióval, melyben kinyilvánítják, hogy átvették az e területen uralkodó közösségi joganyagot. Azon megegyezések alapján intézkedéseket kell tenni, hogy meghatározzák a harmadik országoknak az ügynökség munkájában történő részvételének

természetét, kiterjedését és módját, beleértve az ügynökség kezdeményezéseiben, finanszírozásában és munkatársi körének meghatározásában történő megegyezést is.

Hogy miért kell harmadik országok részvétele? Mert a probléma globális, mint azt több e témában írott cikk és tanulmány is állítja. Így ír pl. Peter D. Bylenchuk ukrán jogászprofesszor egy tanulmányában[12]: *„Nem kétséges, a technikailag fejlett országok többsége szenved a számítógépes bűncselekményektől (...) Az Internet mint globális számítógép-hálózat lehetőséget teremt arra, hogy a világban bármely számítógéprendszert elérjünk, akár katonait is. Emellett ezt a világon bármely helyről megtehetjük (...) A közeljövőben ezek a bűncselekmények globális katasztrófához vezethetnek – természeti, gazdasági, szállítási stb. téren egyaránt."*

A záró rendelkezések közül végül megemlítendők azok, melyek az ügynökség létrejöttének idejét és fennálltának időtartamát jelölik meg. Ezek szerint az ügynökség 2004. március 14-én jön létre ötéves időtartamra.

Azóta – követve az ENISA honlapját és a tudósításokat – kiderült, hogy 2005 elejére tervezik a munkatársak toborzásának lezárását, majd a működést ténylegesen valamikor 2005 közepén-végén kezdi meg a szervezet.

12 http://www.crime-research.org/library/Bileng.htm

VI. Záró gondolatok

Hogy miért is van szükség az információs biztonságra?

Először is nézhetjük a kérdést úgy, mint az üzleti élet előmozdításához szükséges feltételt. A megbízható rendszerek megléte által a fogyasztók és üzleti szervezetek kihasználhatják Európa kommunikációs infrastruktúráját. Az ENISA-nak hozzá kell járulnia ahhoz, hogy segítségére legyen Európa polgárainak abban, hogy megelégedettséggel használják az új technológiákat, és bízzanak bennük.

Másodszor pedig tekinthetjük a kérdést úgy, hogy az összeköttetés új, kicsi és nagy veszélyeknek tesz ki mindannyiunkat. Elsősorban az üzleti szervezetek támaszkodnak erősen az információs hálózatokra és struktúrákra. Ezáltal kiváltképpen nekik kell mélységében megérteniük az újfajta sérthetőségek által támasztott veszélyeket is. Remélhetőleg, ez hozzájárul egyfajta új kockázatmenedzselési struktúra felépítéséhez.

A kockázatokra való felkészültség, és a kockázatmenedzselési szabványok ismerete egyre inkább gazdasági tényezővé válik a globális ellátórendszerben.

A hálózati és információs biztonság mindenkit érint, minden országban, minden felhasználói csoportban. Szorosabb együttműködésre van szükség, és nemcsak szűk körben, de országhatárokon és piaci szegmenseken is átívelően, hogy a biztonsági kockázatok kezelése terén együttműködés alakulhasson ki, és hogy a kiberbűnözést megelőzzük és legyőzzük.

Az ENISA pontosan ezen együttműködés elősegítése céljából jött létre, e téren tekinthető- és megálmodói szerint remélhetőleg egyre inkább tekintendő – egyfajta gyűjtőpontnak, katalizátornak.

Irodalomjegyzék

Gattiker, Urs E. & Thill, F. (November 13, 2003). CASES – Strategy and deliverables.

eEurope 2005: An information society for all

Erkki Liikanen: Towards a security research programme

Erkki Liikanen: European Network Security

Erkki Liikanen: Information Society Policy in an Enlarged Europe

Bozic-Schuurman-Cormack: Computer security in Europe

Első Magyar Jogi Portál
és online Ügyvédi Szaknévsor

JOGI FÓRUM

jogi hírek

interjúk

publikációk

vitafórum

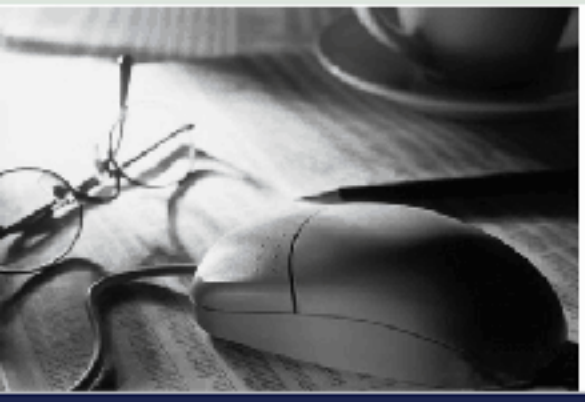
szaknévsor

jogi szakkönyv-katalógus

jogi állásbörze

szakmai rendezvények

heti hírlevél



országos ügyvédi szaknévsor

magyar, angol és német nyelven

ügyfél keres ügyvédet szolgáltatás

www.jogiforum.hu