AZ EURÓPAI KÖZÖSSÉGEK BIZOTTSÁGA

Brüsszel, 2006.5.31
COM(2006) 251 végleges

A BIZOTTSÁG KÖZLEMÉNYE A TANÁCSNAK, AZ EURÓPAI PARLAMENTNEK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK

A biztonságos információs társadalomra irányuló stratégia: „párbeszéd, partnerség, felvértezés és felelősségvállalás”

{SEC(2006) 656}

TARTALOMJEGYZÉK

A BIZOTTSÁG KÖZLEMÉNYE A TANÁCSNAK, AZ EURÓPAI PARLAMENTNEK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK

A Biztonságos információs társadalomra irányuló stratégia: „párbeszéd, partnerség, felvértezés és felelősségvállalás”

1. BEVEZETÉS

Az „i2010: európai információs társadalom a növekedésért és a foglalkoztatásért”[1] című közlemény az egységes európai információs térség létrehozása tekintetében kiemelte a hálózati és az információs biztonság fontosságát. A hálózatok és informatikai rendszerek rendelkezésre állása, megbízhatósága és biztonsága egyre inkább központi kérdéssé válik a gazdaság és a társadalom számára.

E közlemény célja az Európai Bizottság által a „Hálózati és informatikai biztonság: európai politikai megközelítésre irányuló javaslat”[2] című közleményben 2001-ben meghatározott stratégia felfrissítése. Áttekinti az információs társadalom biztonságára leselkedő veszélyek jelenlegi helyzetét, és meghatározza a további lépéseket, amelyeket meg kellene tenni a hálózati és információs biztonság (NIS – *network and information security*) javítása érdekében.

A tagállami és európai közösségi szinten szerzett tapasztalatokból merítve a törekvés egy, a biztonsági kultúrán alapuló, valamint a **párbeszédre, partnerségre, valamint a felvértezésre és felelősségvállalásra alapozott** dinamikus, globális európai stratégia továbbfejlesztésére irányul.

Az információs társadalom biztonsági kihívásaival folytatott küzdelem során az Európai Közösség egy háromrétű megközelítést dolgozott ki: hálózati és információs biztonsági egyedi intézkedések, az elektronikus hírközlésre vonatkozó szabályozási keret (ami a magánélet védelmével és az adatvédelemmel kapcsolatos kérdéseket is magában foglal), valamint a számítógépes bűnözés elleni küzdelem. Noha ezen aspektusok bizonyos mértékig elkülönülten is kidolgozhatók, a számtalan kölcsönhatás koordinált stratégiát kíván. Jelen közlemény meghatározza a stratégiát és azokat a kereteket, amelyeken belül folytatni és finomítani kell a NIS javítására irányuló, koherens megközelítést.

A 2001-es közlemény a NIS-t a következőképpen határozza meg: „*egy hálózati vagy információs rendszer azon képessége, hogy egy adott megbízhatósági szinten ellenáll az olyan véletlen eseményeknek vagy rosszindulatú cselekményeknek, amelyek veszélyeztetik a tárolt vagy továbbított adatok és az ilyen hálózatokon és rendszereken keresztül kínált vagy hozzáférhető kapcsolódó szolgáltatások rendelkezésre állását, hitelességét, integritását és titkosságát*” Az elmúlt években az Európai Közösség számos intézkedést hajtott végre a NIS javítása érdekében.

Az elektronikus hírközlésre vonatkozó szabályozási keret – amelynek felülvizsgálata jelenleg folyik – a biztonságra vonatkozó rendelkezéseket is tartalmaz. Például a magánélet

[1] COM(2005) 229 végleges, 2005.6.1.
[2] COM(2001) 298 végleges, 2001.6.6.

védelméről és az elektronikus hírközlési ágazatról szóló irányelv[3] előírja a nyilvánosan hozzáférhető elektronikus hírközlési szolgáltatások nyújtói kötelezettségét a szolgáltatásai biztonságának megóvására. Továbbá a kéretlen elektronikus levelekre[4] és kémprogramokra (spyware)[5] vonatkozó rendelkezések is le lettek fektetve.

A megbízhatóság és a biztonság fontos részét képezi a kutatásnak és a fejlesztésnek szentelt európai közösségi programoknak is. A hatodik kutatási keretprogram e kérdésekre projektek széles skáláján keresztül próbál választ adni. A biztonsággal kapcsolatos kutatást a hetedik keretprogramban az Európai Biztonságkutatási Program (ESRP)[6] létrehozásával kell megerősíteni. Ezen túlmenően a „Biztonságosabb internet plusz" program támogatja a hálózati projekteket és az információs hálózatokon keringő káros tartalom elleni küzdelemmel kapcsolatos tapasztalatcserét.

A biztonsági fenyegetésekre adott válasz részeként az Európai Közösség 2004-ben úgy határozott, hogy létrehozza az Európai Hálózati és Információs Biztonsági Ügynökséget (ENISA – *European Network and Information Security Agency*). Az ENISA az állampolgárok, fogyasztók, vállalkozások és a közszféra szervezetei érdekében az Európai Unió (EU) teljes területén igyekszik hozzájárulni a hálózati és információs biztonság kultúrájának fejlődéséhez.

Az EU aktív szerepet játszik a témával foglalkozó nemzetközi fórumokon is, mint például az OECD, az Európa Tanács vagy az ENSZ. Az információs társadalomról rendezett csúcsértekezlet tuniszi fordulóján az EU határozottan kiállt a hálózatok és az informatika rendelkezésre állásáról, megbízhatóságáról és biztonságáról folytatott tárgyalások mellett. A nemzetközi vezetők által elfogadott, a globális információs társadalomról folytatott politikai tárgyalásra vonatkozó további lépéseket meghatározó tuniszi menetrend[7] – a tuniszi kötelezettségvállalással együtt – kiemeli a számítógépes bűnözés és a kéretlen elektronikus levelek elleni küzdelem folytatásának szükségességét, a magánélet védelme és a szólásszabadság biztosítása mellett. A dokumentum felismeri az internetes biztonsági kérdésekre vonatkozó közös megegyezés, valamint a biztonsággal kapcsolatos információk gyűjtésének és terjesztésének megkönnyítésére irányuló további együttműködés szükségességét és a biztonsági kockázatok elleni küzdelemre irányuló intézkedésekre vonatkozó tapasztalatok valamennyi érdekelt fél közötti cseréjének szükségességét.

2. AZ INFORMÁCIÓS TÁRSADALOM BIZTONSÁGÁNAK JAVÍTÁSA: A LEGFONTOSABB KIHÍVÁSOK

A nemzetközi, európai és nemzeti szinten megtett erőfeszítések ellenére a biztonság kérdése továbbra is komoly problémákat vet fel.

Először is az informatikai rendszerek elleni támadásokat egyre inkább az anyagi haszonszerzés motiválja, nem pedig az öncélú zavarkeltés szándéka. Az illegális

---

3 2002/58/EK irányelv.

4 Vagy kéretlen kereskedelmi közlemények.

5 A kémprogram (spyware) olyan nyomkövető program, amely a felhasználó megfelelő értesítése, beleegyezése vagy ellenőrzése nélkül telepítődik a felhasználó számítógépére.

6 Az ESPR-t a 2004–-2006-os időszakban folytatott biztonságkutatásra vonatkozó előkészítő intézkedés során dolgozzák ki.

7 *Globális együttműködés felé az információs társadalomban: feladatok az információs társadalomról rendezett csúcsértekezlet tuniszi fordulója után*, COM(2006) 181 végleges, 2006.4.27.

adatbányászat terjed – egyre inkább a felhasználók tudtán kívül – miközben gyorsan növekedik a rosszindulatú szoftverek (malware)[8] variációinak száma (és fejlődésük gyorsasága). A kéretlen elektronikus levelek jó példaként szolgálnak erre a folyamatra: vírusok, csalárd és büntetendő cselekmények hordozójává válnak, például a kémprogramok (spyware), az adathalászat (phishing)[9] és más rosszindulatú szoftverek (malware) esetében. Széleskörű terjesztésük egyre inkább botnetekre[10], azaz a tulajdonosuk tudta nélkül, távolról irányított és adattovábbítóként használt szerverekre és személyi számítógépekre támaszkodik.

A mobileszközök (beleértve a 3G-s mobiltelefonokat, hordozható videojátékokat stb.) terjedése és a mobilalapú hálózati szolgáltatások egyre növekvő száma új kihívásokat teremt az IP-alapú szolgáltatások gyorsan fejlődésével. Ezek az eszközök még közkeletűbb célpontnak bizonyulhatnak, mint a személyi számítógépek, mivel ez utóbbiakat biztonsági szintje mára jellemzően magasabbá vált. Valójában a kommunikációs platformok és az informatikai rendszerek minden új formája elkerülhetetlenül új lehetőségeket nyit meg a rosszindulatú támadások előtt.

Egy másik jelentős fejlődési irány az „interaktív intelligens környezet” megjelenése, amelyben a számítógépes és hálózati technológiával rendelkező intelligens eszközök mindenütt jelen lesznek majd (pl. RFID[11], IPv6 és az érzékelő hálózatokon keresztül). Egy teljesen összekapcsolt és hálózat alapú világ óriási lehetőségeket ígér. Ezzel egy időben azonban további, a biztonsággal, valamint a magánélet védelmével kapcsolatos kockázatokat is teremt. Miközben a közös platformok és alkalmazások pozitívan járulnak hozzá az információs és kommunikációs technológiák (IKT-k) átjárhatóságához és elterjedéséhez, növelhetik a kockázatokat is. Például minél többen használnak szabványosított, „dobozos” szoftvereket, annál nagyobb hatása lesz a gyenge pontok vagy a meghibásodások felszínre kerülésének. Néhány „monokultúra” megjelenése a szoftverplatformokon és alkalmazásokban jócskán megkönnyítheti a biztonsági kockázatok – mint például a rosszindulatú szoftverek (malware) és vírusok – növekedését és terjedését. **A sokféleség, a nyitottság, az átjárhatóság alapvető biztonsági elemek amiket támogatni kell**.

Az IKT-ágazat jelentősége az európai gazdaság és az európai társadalom egésze számára vitathatatlan. Az IKT az innováció kritikus eleme, ami a termelékenység növekedéséért közel 40%-ban felelős. Ennek az innovatív ágazatnak tulajdonítható a teljes európai K+F erőfeszítések több mint negyede, továbbá kulcsfontosságú szerepet játszik a gazdasági növekedésben és a munkahelyteremtésben az egész gazdaságban. Egyre több európai él egy olyan, ténylegesen információalapú társadalomban, amelyben az IKT-k felhasználása – a társadalmi és gazdasági együttműködés alapvető funkciójaként – gyors ütemben halad előre. Az Eurostat szerint az EU vállalkozásainak 89%-a használta az internetet aktívan 2004-ben, és a fogyasztók nagyjából 50%-a használta az internetet a megkérdezést megelőző időszakban[12].

---

8 A „malware” az angol *malicious software* rövidítése.

9 A phishing az internetes csalás értékes információk – mint például a hitelkártyák, bankszámlaszámok, felhasználói azonosítók és jelszavak – illegális megszerzésére irányuló formája.

10 A botnetek olyan adattároló hálózatok, azaz olyan alkalmazások, amelyek egy távoli irányító nevében műveleteket végeznek a számítógépen, és amelyeket egy ennek áldozatául esett számítógépen titokban telepítenek.

11 Rádiófrekvenciás azonosítás.

12 Eurostat, *Internetes tevékenységek az Európai Unióban*, 40/2005.

A NIS sérülésének hatásta a gazdasági dimenziókon túl is kiterjedhet. Általános az aggodalom, hogy a biztonsági problémák elriaszthatják a felhasználókat és csökkenthetik az IKT elterjedését, miközben viszont a rendelkezésre állás, megbízhatóság és biztonság az alapvető jogok online biztosításának előfeltétele.

Ráadásul – a hálózatok közötti megnövekedett számú kapcsolatok miatt – más kritikus infrastruktúrák (mint például a közlekedés, energia stb.) is egyre inkább függnek az informatikai rendszereik integritásától.

Mind az európai vállalkozások, mind pedig az állampolgárok alábecsülik a veszélyeket. Ennek számos oka van, de a legfontosabb– a vállalkozások esetében – a biztonságra fordított befektetések megtérülésének alacsony láthatósága tűnik, míg az állampolgárok esetében az a tény, hogy nincsenek tisztában a globális biztonsági láncban betöltött felelősségükkel.

Valójában az IKT-k és az informatikai rendszerek általános elterjedése miatt a hálózati és információs biztonság mindenki számára kihívást jelent:

- **A közigazgatásnak** foglalkoznia kell a rendszerei biztonságával, nem csupán a közszektor információinak védelme érdekében, hanem azért is, hogy más szereplők számára példaként szolgáljon;

- **A vállalkozásoknak** a versenyképességi előny egyik eszközekén és elemeként, és nem „negatív költségként" kell vele foglalkozniuk;

- **Az egyéni felhasználóknak** meg kell érteniük, hogy otthoni rendszereik kritikusak az átfogó „biztonsági lánc" szempontjából.

Annak érdekében, hogy a fent körülírt problémákkal hatékonyan lehessen megbirkózni, valamennyi érdekeltnek megbízható adatokra van szüksége az információs biztonsági eseményekre és folyamatokra vonatkozóan. Az ilyen eseményekre vonatkozó megbízható és átfogó adatokat azonban számos okból kifolyólag – a biztonsági események bekövetkezésének gyakoriságától kezdve az érintett szervezetek az irányú vonakodásáig, hogy ezeket feltárják vagy közzétegyék – nehéz beszerezni. Mindazonáltal a biztonsági kultúra fejlesztésének egyik sarokköve **a problémával kapcsolatos ismereteink javítása**.

Fontos, hogy a biztonságot fenyegető veszélyek kiemelésére irányuló tudatossági programok ne ássák alá a fogyasztók és a felhasználók bizalmát azzal, hogy csak a biztonság negatív aspektusaira összpontosítanak. Ezért amennyire csak lehetséges felelősség és költség helyett a **NIS-t értékként és lehetőségként kell bemutatni**. A NIS-re a megbízhatóság és a fogyasztói bizalom kiépítésének eszközeként kell tekinteni, ami versenyképes előny az informatikai rendszereket üzemeltető vállalkozások számára és a szolgáltatások minőségével kapcsolatos kérdés mind a köz-, mind pedig a magánszektorban tevékenykedő szolgáltatók számára.

A politikával foglalkozók számára a leglényegesebb kihívás a holisztikus megközelítés elősegítése. E megközelítésnek fel kell ismernie a különböző érdekeltek szerepét. Biztosítania kell az olyan törvények és szabályozók közötti megfelelő koordinációt, melyek közvetlenül vagy közvetve hatással vannak az információs biztonságra. A liberalizáció, a dereguláció és a konvergencia folyamatai az érdekeltek között sokféle szereplők hívtak életre, ami nem könnyíti meg a feladatot. Az ENISA hozzájárulása a cél eléréséhez igen fontos lehet. Az IKT-ipar versenyképességéhez valamint a belső piac jó működéséhez való hozzájárulás érdekében az ENISA az információ-megosztással, az érdekeltek közötti együttműködés elősegítésével és

az gyakorlati tapasztalatok cseréjével foglalkozó központként is szolgálhat mind Európán belül, mind pedig a világ többi részében.

3. A BIZTONSÁGOS INFORMÁCIÓS TÁRSADALOMRA IRÁNYULÓ DINAMIKUS MEGKÖZELÍTÉS FELÉ

A biztonságos információs társadalom alapja a **fokozott mértékű NIS** és a széles körben elterjedt **biztonsági kultúra**. E célból az Európai Bizottság olyan **dinamikus és integrált megközelítést** javasol, amelyben valamennyi érdekelt részt vesz és amely a **párbeszéden, partnerségen valamint a felvértezésen és felelősségvállaláson** alapul. A biztonsági kultúra kialakításában a köz- és magánszektor egymást kiegészítő szerepe miatt az e területtel kapcsolatos politikai kezdeményezéseknek **nyitott, és minden érdekeltre kiterjedő, integráló párbeszéden** kell alapulniuk.

Ez a megközelítés, valamint az ahhoz kapcsolódó intézkedések kiegészítik és gazdagabbá teszik a Bizottság arra irányuló tervét, hogy 2006-ban számos kezdeményezésen keresztül folytassa az átfogó és dinamikus politikai keret kialakítását:

(1) A kéretlen elektronikus levelek és a biztonsági fenyegetések – mint például kémprogramok (spyware) és más rosszindulatú szoftverek (malware)– helyzetének tárgyalása egy külön közleményben.

(2) Javaslatok kidolgozása a bűnüldöző hatóságok közötti együttműködés javítására, illetve az Internet adta lehetőségeket kihasználó és a kritikus infrastruktúrák működtetését aláásó új bűncselekmény-formák kezelésére. Erre egy, a számítógépes bűnözésről szóló külön közlemény fog vonatkozni.

E politikai kezdeményezések kiegészítik a Bizottság által a Tanács 2004. decemberi kérésére válaszul kidolgozott, a létfontosságú infrastruktúrák védelmére vonatkozó európai programról (EPCIP)[13] szóló zöld könyvben szereplő célkitűzések elérésre irányuló törekvéseket is. A zöld könyvvel kapcsolatos folyamat várhatóan olyan cselekvési tervet eredményez, ami a kritikus infrastruktúra védelmére vonatkozó, átfogó „ernyő”-megközelítést kombinálja a szükséges ágazatspecifikus politikákkal, beleértve az IKT-iparági politikát is. Az IKT iparági politika **több érdekeltre kiterjedő párbeszéden** keresztül vizsgálná meg a lényeges gazdasági, üzleti és társadalmi hajtóerőket a hálózatok és az informatikai rendszerek biztonságának és rugalmasságának fokozása céljából.

Ezen túlmenően az elektronikus hírközlésre vonatkozó szabályozási keret 2006-os felülvizsgálata szintén figyelembe fogja venni a NIS javítására irányuló elemeket, mint például a szolgáltatók által megteendő műszaki és szervezeti intézkedések, a biztonsági események bejelentésére vonatkozó rendelkezéseket, valamint a kötelezettségek megsértésének jogkövetkezményeit és a kapcsolódó jogérvényesítési lehetőségeket.

Jórészt a magánszektor feladata ellátni a végfelhasználókat biztonsági megoldásokkal, szolgáltatásokkal és termékekkel. Ennélfogva stratégiai jelentőséggel bír, hogy **az európai ipar** egyszerre legyen a biztonsági termékeket **igénylő felhasználó** és a NIS termékek és szolgáltatások **versenyképes szállítója is**.

---

[13] COM(2005) 576 végleges, 2005.11.17.

A nemzeti kormányoknak ki kell választani, és alkalmazni kell a legjobb megoldásokat a politikájuk kialakításában, valamint meg kell mutatniuk a politikai célkitűzésekkel szembeni elkötelezettségüket saját informatikai rendszereik biztonságos működtetésével is. A tagállami és az EU-szintű hatóságok kulcsszerepet töltenek be a felhasználók megfelelő tájékoztatásában, aminek hatására azok hatékonyabban járulhatnak hozzá saját biztonságukhoz.. A kiemelt célok közé tartozik a NIS–sel kapcsolatos tudatosság javítása, illetve a veszélyekkel, kockázatokkal valamint a legjobb gyakorlati megoldásokkal kapcsolatos információnyújtás a témával foglalkozó honlapokon keresztül a megfelelő módon és időben. Ennek elérése érdekében az ENISA egyik legfontosabb célja lehetne a meglévő vagy tervezett, állami- és magánkezdeményezésekre épülő, valamint azokat összekötő, **európai többnyelvű információ-megosztási és figyelmeztető rendszer létrehozása** megvalósíthatóságának vizsgálata lehetne.

A hálózati és információs biztonság globális dimenziója arra készteti a Bizottságot – mind nemzetközi szinten, mind pedig a tagállamokkal együttműködve –, hogy növelje **a globális együttműködés előmozdítására** irányuló erőfeszítéseit, különösen az információs társadalomról 2005 novemberében tartott világcsúcson (WSIS) elfogadott menetrend végrehajtása tekintetében.

Végül a kutatás és fejlesztés, különösen EU szinten, hozzájárul új és innovatív partnerkapcsolatok kialakulásához, amelyek segítik az európai IKT-ipar, és különösen az európai IKT biztonsági iparág növekedését. A Bizottság ennélfogva törekedni fog arra, hogy a NIS-sel, valamint a rendszermegbízhatósági technológiákkal kapcsolatos, a 7. Keretprogram alapján végzett kutatásokra megfelelő pénzforrásokat különítsenek el.

3.1. Párbeszéd

3.1.1. *A hatóságok közötti párbeszéd javítására első lépésben a Bizottság a **NIS-sel kapcsolatos nemzeti politikák értékelésének** megkezdését javasolja, beleértve a közszférára vonatkozó egyedi biztonsági politikákat. Ez segíteni fogja a leghatékonyabb eljárások azonosítását, hogy ezeket aztán minél szélesebb körben alkalmazni lehessen EU-szerte, továbbá segíteni fogja a közigazgatást abban, hogy a biztonság terén a legjobb eljárások kifejlesztésének motorjává váljon. Például az elektronikus kormányzatra vonatkozó cselekvési terv részeként az elektronikus azonosítással kapcsolatban zajló munka fontos szerepet játszhat e tekintetben.*

A megfelelően elvégzett értékelés eredményeképpen azonosíthatók azok a módszerek, amelyekkel **a KKV-k és az állampolgárok tudatossága fokozható,** hogy foglalkozzanak saját, egyedi NIS kihívásaikkal és szükségleteikkel, valamint az ezekhez szükséges kapacitás megteremtésével. Az ENISA is aktív szerepet kell játsszon a párbeszédben, valamint a legjobb gyakorlatok megszilárdításában és cseréjében.

3.1.2. ***S**trukturált**, több oldalú, nyílt társadalmi vitára van szükség** arról, hogy miként lehet a legjobban kiaknázni a meglévő lehetőségeket és szabályozási eszközöket a biztonság és az alapvető jogok védelme – beleértve a magánélethez való jogot – közötti megfelelő társadalmi egyensúly elérése érdekében. A következő finn elnökség által „i2010 – A mindent felölelő európai információs társadalom felé” címmel tervezett konferencia, és a RFID biztonságra és magánéletre gyakorolt hatásairól szóló konzultáció – a Bizottság által nemrégiben elindított szélesebb körű*

konzultáció részeként – hozzá fog járulni a vitához. Ezen túlmenően a Bizottság az alábbiakat fogja megszervezni:

- Egy rendezvény vállalkozások számára, a biztonsági kultúra megteremtéséhez szükséges hatékony megközelítésre vonatkozó üzleti kötelezettségvállalás ösztönzésére.

- Egy szeminárium, amelynek témája a biztonsággal kapcsolatos tudatosság felkeltését, valamint az elektronikus hálózatok és informatikai rendszerekkel szembeni végfelhasználói bizalom fokozását szolgáló lehetőségek megvitatása.

3.2. Partnerség

3.2.1. A politika hatékony kialakítása során egyértelműen meg kell érteni a kihívások jellegét és mértékét. Ehhez nem csak az információs biztonsági eseményekre és a fogyasztók és felhasználók bizalmi szintjére vonatkozó, megbízható és naprakész statisztikai és gazdasági adatokra van szükség, hanem az európai IKT-biztonsági ipar méretére és fejlődési irányára vonatkozó adatokra is. A Bizottság fel kívánja kérni az ENISA-t, hogy alakítson ki ***bizalmon alapuló partnerséget a tagállamokkal és az érdekeltekkel a megfelelő adatgyűjtési keret*** *kialakítása érdekében, ami felölelné a biztonsági eseményekre és a fogyasztói bizalomra vonatkozó adatok begyűjtésére és elemzésére irányuló eljárásokat és mechanizmusokat EU szinten.*

A Bizottság – az EU erősen tagolt piaca, valamint annak speciális jellege miatt – fel fogja kérni a tagállamokat, a magánszektort és a kutatói közösséget, hogy **hozzon létre stratégiai partnerséget** az IKT-biztonsági iparra, valamint az EU-ban a biztonsági termékek és szolgáltatások piacára vonatkozó adatok rendelkezésre állásának biztosítására.

3.2.2. A hálózati biztonsági fenyegetésekre való európai válaszadási képesség javítása érdekében a Bizottság meg fogja kérni az ENISA-t, hogy vizsgálja meg ***egy európai információ-csere és riadó rendszer kivitelezésének lehetőségét,*** *az elektronikus hálózatokat fenyegető meglévő és jövőbeni veszélyekre való hatékony reagálás megkönnyítése érdekében. Szükséges, hogy a kialakítandó rendszerben szerepet kapjon egy, a fenyegetésekre, veszélyekre és figyelmeztetésekre vonatkozóan testre szabott információkat nyújtó* ***többnyelvű EU portál****.*

3.3. Felvértezés és felelősségvállalás

Az érdekeltek valamennyi csoportjának felvértezése és részükről a felelősségvállalás elfogadása előfeltétele a biztonsági szükségletekkel és veszélyekkel kapcsolatos tudatosság elősegítésének és a NIS elősegítésének.

3.3.1. E tekintetben a Bizottság felszólítja a ***tagállamokat****, hogy:*

- proaktívan vegyenek részt a nemzeti NIS-politikák javasolt értékelési gyakorlatában;

- az ENISA-val szoros együttműködésben folytassanak kampányt a hatékony biztonsági technológiák és eljárások alkalmazásának előnyeiről;

- használják fel az elektronikus kormányzati rendszerek bevezetése adta lehetőséget a helyes biztonsági módszerek kommunikálására és elterjesztésére, amelyek azután más ágazatokra is kiterjeszthetők lennének;

- a felsőoktatási tanterv részeként ösztönözzék a hálózati és információs biztonsági programok kidolgozását.

3.3.2. *A Bizottság **a magánszektor** érdekeltjeit is felszólítja, hogy tegyenek kezdeményezéseket a következőkre:*

- a szoftvergyártók és internetszolgáltatók felelősségének meghatározása a megfelelő és ellenőrizhető biztonsági szintek megteremtésében. Itt támogatni kell a közösen megállapított biztonsági szabványoknak és a legjobb gyakorlatokra vonatkozó szabályoknak megfelelő szabványosított eljárásokat.

- a sokféleség, nyitottság, átjárhatóság, felhasználhatóság és verseny – mint a biztonság legfőbb hordozóinak – elősegítése, valamint a személyazonosság ellopása és a magánéletet sértő egyéb támadások elleni küzdelem jegyében a biztonságot fokozó termékek, eljárások és szolgáltatások kidolgozásának ösztönzése.

- a helyes biztonsági módszerek ismeretének terjesztése a hálózatok működtetői, a szolgáltatók és a KKV-k körében, amelyek alapvető szerepet játszanak a biztonság megteremtésében és az üzleti tevékenységek folyamatosságának biztosításában.

- a képzési programok elősegítése a vállalkozói szektorban, különösen a KKV-k számára, hogy biztosítsák a munkavállalók számára a biztonsági módszerek hatékony alkalmazásához szükséges ismereteket és képességeket.

- a kimondottan EU igényeknek megfelelő (különösen a személyes adatok védelme terén) termékekre, szolgáltatásokra és folyamatokra vonatkozó, széles körben elérhető tanúsítási rendszerek létrehozása.

- a biztosítási ágazat bevonása a megfelelő kockázatkezelési eszközök és módszerek kifejlesztésébe az IKT-vel kapcsolatos kockázatok kezelése érdekében, valamint a különböző szervezeteknél és vállalkozásoknál (különösen a KKV-knál) a kockázatkezelési kultúra elősegítésébe.

4. KÖVETKEZTETÉSEK

Az EU-ban az informatikai rendszerekkel és hálózatokkal kapcsolatos biztonsági kihívások felismerése és az azoknak való megfelelés valamennyi érdekelt teljes elkötelezettségét teszi szükségessé. Az e közleményben körvonalazott politikai megközelítés ennek elérésére törekszik a **több érdekeltre kiterjedő megközelítés** megerősítésével. Ez a kölcsönös érdekekre épülne, meghatározná az egyes résztvevők szerepét, és dinamikus keretet teremtene a hatékony állami politikák és a magánszektor kezdeményezéseinek előmozdítására.

2007 közepén a Bizottság jelentést fog tenni a Tanácsnak és a Parlamentnek az elindított tevékenységekről, a kezdeti megállapításokról és az egyéni kezdeményezések helyzetéről,

beleértve az ENISA és a tagállami szintű, valamint a magánszektorbeli kezdeményezéseket. A Bizottság adott esetben egy, a hálózati és információs biztonságról (NIS) szóló ajánlást fog javasolni.