Az Európai Unió
Tanácsa

Brüsszel, 2017. szeptember 14.
(OR. en)

12183/17
ADD 2

Intézményközi referenciaszám:
2017/0225 (COD)

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Jordi AYET PUIGARNAU igazgató
Címzett:	Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	SWD(2017) 501 final
Tárgy:	BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM A HATÁSVIZSGÁLAT VEZETŐI ÖSSZEFOGLALÓJA amely a következő dokumentumot kíséri: Javaslat – AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az Európai Uniós Kiberbiztonsági Ügynökségről, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály”)

Mellékelten továbbítjuk a delegációknak az SWD(2017) 501 final számú dokumentumot.

Melléklet: SWD(2017) 501 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2017.9.13.
SWD(2017) 501 final

BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM

A HATÁSVIZSGÁLAT VEZETŐI ÖSSZEFOGLALÓJA

amely a következő dokumentumot kíséri

Javaslat
AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

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

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. A FELLÉPÉS SZÜKSÉGESSÉGE

Mi a probléma, és miért az?

A digitális technológiák és az internet az EU gazdaságának és társadalmának gerincét képezik. Számos kritikus fontosságú gazdasági ágazat, mint például a közlekedés, az energetika, az egészségügy vagy a pénzügyi szektor szinte már nem is tudná fő tevékenységét ellátni a hálózati és információs rendszerek nélkül. A dolgok internete a tárgyakat és az embereket kommunikációs hálózatokon keresztül köti össze. Ezek az új realitások páratlan lehetőségeket teremtenek, de egyúttal támadási felületet is kínálnak. A kiberbiztonsági események szinte virágkorukat élik: összetettségüket, előfordulásuk gyakoriságát és hatásukat – amely érintheti az alapvető szolgáltatásokhoz való hozzáférést, de akár a demokratikus folyamatokban való részvételt is – fokozódó tendencia jellemzi.

Ezzel kapcsolatban a következő, egymással összefüggő problémákat sikerült azonosítani:

- A kiberbiztonsággal kapcsolatos tagállami szakpolitikák és szemléletmódok igen különbözők.
- Az uniós intézmények, hivatalok és szervek kiberbiztonságra fordítható forrásai elszórtan állnak rendelkezésre, és a téma megközelítése sem egységes.
- A polgárok és a vállalatok nem kellőképpen tájékozottak a kiberfenyegetésekkel kapcsolatban, és nem ismerik eléggé az általuk vásárolt IKT-termékek és -szolgáltatások biztonsági tulajdonságait, amit még súlyosbít, hogy a tanúsítási rendszerek száma mind nemzeti, mind ágazati szinten egyre nő.

Ezek a problémák kihatnak mind az EU kibertámadásokkal szembeni általános ellenálló képességére, mind a belső piac hatékony működésére.

Mit kellene elérni?

A kezdeményezés konkrét szakpolitikai célkitűzései a következők:

1. A tagállamok és a vállalkozások képességeinek és felkészültségének javítása, különösen a kritikus infrastruktúrák tekintetében.
2. A tagállamok, valamint az uniós intézmények, hivatalok és szervek közötti együttműködés és koordináció javítása.
3. Az uniós szintű képességek növelése a tagállamok által meghozott intézkedések kiegészítése érdekében, különösen a több országot is érintő kiberválságok esetében.
4. A polgárok és a vállalkozások tudatosságának növelése kiberbiztonsági kérdésekkel kapcsolatban.
5. A digitális egységes piacba és a digitális innovációba vetett bizalom megerősítése érdekében általában véve átláthatóbbá tenni az IKT-termékek és -szolgáltatások kiberbiztonsági jellemzőit.
6. Az EU-ban használt tanúsítási rendszerek, valamint a kapcsolódó biztonsági követelmények és értékelési kritériumok széttagoltságának megelőzése valamennyi tagállamban és ágazatban.

Milyen többletértéket képvisel az uniós szintű fellépés?

Mivel a gazdaság és a társadalom digitalizációja és hálózatba kapcsolódása globális méreteket ölt, a problémák jóval túlmutatnak egy-egy tagállam területén. Ezért tehát uniós szintű beavatkozásra van szükség. A jelenlegi helyzetet és a jövőt tekintve is úgy tűnik, hogy az EU kibertámadásokkal szembeni kollektív ellenálló képessége a tagállamok által hozott egyedi intézkedések útján nem fokozható, különösen azért, mert a kiberbiztonsággal — kapcsolatos szemléletmódokat nagy széttagoltság jellemzi, a kiberbiztonsági problémák viszont rendszerint több országot is érintenek.

B. MEGOLDÁSOK

Milyen lehetőségek kínálkoznak a célok elérésére? Van-e előnyben részesített megoldás?

Ez a hatásvizsgálat több szakpolitikai lehetőséget is körbejár, amelyek az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) és az IKT-biztonsági tanúsítás felülvizsgálatára irányulnak.

Az ENISA felülvizsgálata

0. lehetőség – **alapforgatókönyv** – ez az opció a jelenlegi helyzet fenntartásában áll. Az ENISA megbízatását kiterjesztenék; az Ügynökség céljai és feladatai nagyrészt változatlanok maradnának, viszont a későbbi uniós jogszabályok (pl. a kiberbiztonsági irányelv) további feladatokat ruházhatnának rá.

1. lehetőség – **az ENISA megbízatásának lejárta** (az ENISA megszüntetése). Ez az opció az ENISA megszüntetéséhez vezetne megbízatásának lejártakor (2020 júniusában), és adott esetben a hatáskörök/tevékenységek uniós és/vagy nemzeti szinten történő újraelosztásával járna.

2. lehetőség – **az ENISA„megreformálása”**. Ez az opció az ENISA jelenlegi megbízatásából indulna ki, és a kiberbiztonsági fejlemények figyelembevételének érdekében bizonyos célirányos változtatások elfogadását jelentené. Az Ügynökség állandó megbízatást kapna, és tevékenysége a következő fő alapelemekből tevődne össze: az uniós szakpolitikák kidolgozásának és végrehajtásának támogatása; kapacitásfejlesztés; az ismeretek bővítése és terjesztése; a piaccal kapcsolatos feladatok; kutatás és innováció; továbbá operatív együttműködés és válságkezelés.

3. lehetőség – **teljes műveleti képességgel felruházott uniós kiberbiztonsági ügynökség**. Ez a lehetőség az ENISA reformját foglalja magában, három fő funkció egyesítésével: 1. szakpolitikai/tanácsadói funkció; 2. információs és szakértői központ, valamint 3. hálózatbiztonsági vészhelyzeteket elhárító csoport (CERT). Ez az opció lényegében ugyanazt a változást jelentené az Ügynökség megbízásának hatályát illetően, mint a 2. lehetőség. Az Ügynökség azonban a biztonsági eseményekre való reagálás és a válságkezelés terén további feladatokat kapna annak érdekében, hogy funkciója a kiberbiztonság teljes életciklusára, vagyis a kiberbiztonsági események megelőzésére, felderítésére és az azokra való reagálásra is kiterjedjen.

Tanúsítás

<u>0. lehetőség</u> – alapforgatókönyv – semmi nem változik. Ezen opció szerint a Bizottság fenntartaná a jelenlegi helyzetet, és nem hajtana végre szakpolitikai vagy jogalkotási intézkedéseket.

<u>1. lehetőség</u> – nem jogalkotási (ún. puha jogi) intézkedések. Ez az opció abban állna, hogy a Bizottság nem kötelező erejű szakpolitikai eszközöket (pl. értelmező közleményeket, az EU egészére kiterjedő önszabályozási kezdeményezéseket és szabványosítási tevékenységekre irányuló támogatást) vetne be az átláthatóság javítása és a széttagoltság csökkentése érdekében.

<u>2. lehetőség</u> – uniós jogalkotási aktus a SOG-IS megállapodás valamennyi tagállamra való kiterjesztéséről. E szakpolitikai lehetőség értelmében a Bizottság jogalkotási aktust terjesztene elő azzal a céllal, hogy a tagságot valamennyi tagállamra hivatalosan kiterjessze.

<u>3. lehetőség</u> – általános uniós keretrendszer az IKT-biztonsági tanúsításra. Ez az opció az IKT-biztonsági tanúsítás európai keretrendszerének létrehozásával (és egy nemzeti hatóságok képviselőiből álló szakértői csoport megalapításával) jár. Az új keretrendszer a lehető legnagyobb mértékben a már meglévő IKT-biztonsági tanúsítási rendszereken alapulna. Lényegében arról van szó, hogy a keretrendszer révén olyan uniós tanúsítási rendszereket lehetne kialakítani, amelyeket minden tagállamban elfogadnak.

Az előnyben részesített megoldás az ENISA-val kapcsolatos 2. lehetőség és a tanúsításra vonatkozó 3. lehetőség kombinációja.

Kik a különböző érdekeltek? Ki melyik megoldást támogatja?

Úgy tűnik, hogy a konzultációban részt vevő legkülönfélébb érdekelt felek (a tagállamok, az ágazat, az uniós intézmények és a kutatótársadalom) túlnyomó többsége örömmel fogadja az előnyben részesített megoldást, mivel egyetértenek abban, hogy meg kell erősíteni az ENISA-t, és európai IKT-biztonsági tanúsítási keretrendszert kell létrehozni.

Különösen abban a tekintetben van egyetértés, hogy (minimumként) egy állandó megbízatással rendelkező, jól működő uniós ügynökségre van szükség, amely megfelelő forrásokkal és felhatalmazásokkal rendelkezik ahhoz, hogy kezelni tudja a jelenlegi és jövőbeli kiberbiztonsági kihívásokat. Az érdekeltek széles körben egyetértenek abban is, hogy létre kell hozni egy önkéntes, igény szerint méretezhető európai keretrendszert.

Ami az ágazatot illeti, ezt a tanúsítási megoldást a már jelenleg is tanúsítási követelmények hatálya alá tartozó vállalkozások támogatják, amelyeknek előnyére válna, ha lenne egy, a tanúsítványok kölcsönös elismerésén alapuló, az egész EU-ra kiterjedő mechanizmus. A javaslatot a kkv-k is támogatják, amelyeket a lehető leghátrányosabban érintené, ha a különböző tagállamokban különböző tanúsítási eljárásokhoz kellene folyamodniuk most vagy a jövőben. Néhány tagállam, különösen a kevesebb forrással rendelkezők, valamint az ágazat és az uniós intézmények néhány képviselője kedvezően nyilatkozott az ENISA-ra vonatkozó 3. lehetőségről is.

C. AZ ELŐNYBEN RÉSZESÍTETT MEGOLDÁS HATÁSAI

Melyek az előnyben részesített megoldás (ha nincs ilyen, akkor a főbb lehetőségek) előnyei?

Az előnyben részesített megoldás szerint az EU-nak lenne egy olyan ügynöksége, amely azokon a területeken nyújtana támogatást a tagállamoknak, az uniós intézményeknek és a vállalkozásoknak, ahol az a legnagyobb hozzáadott értéket jelenti. A következők tartoznak ide: a kiberbiztonsági irányelv végrehajtásához nyújtott támogatás; uniós szakpolitikák kidolgozása és végrehajtása; tájékoztatás, ismeretterjesztés és tudatosságnövelés; kutatás; operatív együttműködés és válságkezelés; piac. Az ENISA különösen az IKT-biztonsági tanúsításra irányuló uniós szakpolitika területén nyújtana támogatást azáltal, hogy biztosítaná az európai IKT-biztonsági tanúsítás keretrendszerének adminisztratív fenntartását és technikai irányítását. E keretrendszer szabályokat állapítana meg az EU-n belüli IKT-biztonsági tanúsítás irányítására vonatkozóan, ami előmozdítaná a tagállamokban kiállított tanúsítványok kölcsönös elismerésének rendszerét. E két lehetőség együttes alkalmazása tűnik a leghatékonyabb módszernek ahhoz, hogy az EU elérhesse a kiberbiztonsági képességek növelésével, a felkészültséggel, az együttműködéssel, a tudatosítással, az átláthatósággal, valamint a piac széttagoltságának megelőzésével kapcsolatban azonosított célokat. A kiberbiztonsági stratégiában és a kapcsolódó szakpolitikákban (például a kiberbiztonsági irányelvben), valamint a digitális egységes piaci stratégiában lefektetett politikai prioritásokkal is ez a megoldás van leginkább összhangban. Emellett ezzel a megoldással az erőforrások észszerű felhasználása mellett lehet elérni a kitűzött célkitűzéseket.

Milyen költségekkel jár az előnyben részesített megoldás (ha nincs ilyen, akkor milyen költségekkel járnak a főbb lehetőségek)?

Feladatkörének bővülése ellenére a „megreformált” ENISA továbbra is dinamikus szervezet maradna. Az uniós költségvetésből az eddigieknél nagyobb pénzügyi hozzájárulást igényelne, de az még mindig sokkal szerényebb mértékű lenne más kritikus területeken tevékenykedő ügynökségek költségvetésénél.

Az IKT-biztonsági tanúsítás európai keretrendszerének létrehozása nem járna kezdeti többletköltségekkel az iparág számára (a kkv-k számára sem). Azon vállalkozások számára pedig, amelyek vagy már jelenleg is tanúsítják termékeiket, vagy hajlandóak biztonsági tanúsítást végezni, jelentős megtakarításokat eredményezne, ami kedvezően hatna globális versenyképességükre. Másrészről a keretrendszer fenntartásának érdekében bizonyos költségvetési kötelezettségvállalásokra lenne szükség, amelyeket – a technikai és titkársági feladatok ellátását illetően – elsősorban a „megreformált ENISA” modell biztosít.

Jelentős lesz-e a tagállamok költségvetésére és közigazgatására gyakorolt hatás?

Nem. Az ENISA megerősítéséhez kapcsolódó költségeket elsősorban az uniós költségvetés fogja fedezni, a tagállamok azonban önkéntes alapon nyújthatnak pénzügyi hozzájárulást az Ügynökségnek. Ami a tanúsítást illeti, a nemzeti költségvetésekre és közigazgatásokra gyakorolt fő hatás adott esetben egy tanúsító hatóság létrehozásából származna.

Lesznek-e egyéb jelentős hatások?

Nem.

Arányosság

A javasolt megoldás kiegyensúlyozott intézkedéseket foglal magában, amelyek mindegyikére szükség van a kitűzött célok oly módon történő eléréshez, hogy közben ne rójunk túl nagy terhet az érdekeltekre. Ennek fényében ez a kezdeményezés megfelel az arányosság elvének.

D. TOVÁBBI LÉPÉSEK

Mikor kerül sor a szakpolitikai fellépés felülvizsgálatára?

A javaslat jelenlegi formájában azt írja elő, hogy az első értékelésre a jogi eszköz hatálybalépése után öt évvel kerüljön sor. A Bizottság ezt követően jelentést tesz az Európai Parlamentnek és a Tanácsnak az értékeléséről, adott esetben a jogi eszköz felülvizsgálatára vonatkozó javaslattal együtt. Az ezt követő értékelésekre szintén ötévente kerül majd sor.