Az Európai Unió
Tanácsa

Brüsszel, 2020. december 18.
(OR. en)

Intézményközi referenciaszám:
2020/0359(COD)

14150/20
ADD 3

CYBER 281
JAI 1119
DATAPROTECT 155
TELECOM 270
MI 581
CSC 368
CSCI 97

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2020. december 16.
Címzett:	Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	SWD(2020) 344 final
Tárgy:	BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM A HATÁSVIZSGÁLATI JELENTÉS VEZETŐI ÖSSZEFOGLALÓJA amely a következő dokumentumot kíséri: Javaslat – AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről

Mellékelten továbbítjuk a delegációknak az SWD(2020) 344 final számú dokumentumot.

Melléklet: SWD(2020) 344 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2020.12.16.
SWD(2020) 344 final

BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM

A HATÁSVIZSGÁLATI JELENTÉS VEZETŐI ÖSSZEFOGLALÓJA

amely a következő dokumentumot kíséri:

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE

az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Vezetői összefoglaló

Hatásvizsgálat *a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-i (EU) 2016/1148 irányelv (a továbbiakban: a kiberbiztonsági irányelv) felülvizsgálatáról*

A. A fellépés szükségessége

Mi a probléma lényege, és miért jelent problémát uniós szinten?

Figyelemre méltó eredményei ellenére a kiberbiztonsági irányelv – amely számos tagállamban kikövezte az utat a kiberbiztonság felfogásának, intézményi és szabályozási megközelítésének jelentős megváltoztatásához – mára bebizonyította korlátait is. A társadalom digitális átalakulása (amelyet felgyorsított a Covid19-válság) kibővítette a fenyegetettségek körét, és új kihívásokat hoz, amelyek adaptált és innovatív válaszokat igényelnek. A kibertámadások száma továbbra is növekszik, egyre kifinomultabb támadások érkeznek a legkülönbözőbb, EU-n belüli és azon kívüli forrásokból.

A kiberbiztonsági irányelv működésének értékelése alapján a hatásvizsgálat a következő problémákat azonosította: az Unióban működő vállalkozások alacsony szintű kiberrezilienciája; a tagállamok és ágazatok rezilienciájának következetlenségei, a közös helyzetismeret alacsony szintje és a közös válságelhárítás hiánya. Példaként: e problémák és hajtóerők némelyikének eredőjeként állnak elő olyan helyzetek, amikor egy tagállam nagyobb kórházai nem tartoznak a kiberbiztonsági irányelv hatálya alá, és ezért nem kötelesek végrehajtani az ebből eredő biztonsági intézkedéseket, míg egy másik tagállamban az ország szinte minden egyes kórházára vonatkoznak a hálózati és információs rendszerek biztonsági követelményei.

Mit kellene elérni?

A kiberbiztonsági irányelv felülvizsgálatának három általános célkitűzése van:

1. **Az Európai Unióban működő vállalkozások tág köre kiberreziliencia-szintjének emelése az összes érintett ágazatban**, azt biztosító szabályok bevezetésével, hogy a belső piacon megfelelő kiberbiztonsági intézkedéseket rendszeresítsen minden olyan köz- és magánjogi szervezet, amely a gazdaság és az egész társadalom számára fontos feladatokat lát el.
2. **Az irányelv által már lefedett ágazatokban a belső piacon a reziliencia terén mutatkozó következetlenségek csökkentése** a következők további összehangolásával: (1) a tényleges hatály, (2) a biztonsági és eseményjelentési követelmények, (3) a nemzeti felügyeletet és végrehajtást szabályozó rendelkezések és (4) a tagállami illetékes hatóságok képességei.
3. **A közös helyzetismeret szintjének és a kollektív felkészülési és válaszadási képességnek a javítása** az illetékes hatóságok közötti bizalom fokozását szolgáló intézkedések meghozatalával, több információ megosztásával, valamint nagyszabású esemény vagy válság esetére szabályok és eljárások meghatározásával.

Milyen többletértéket képvisel az uniós szintű fellépés (szubszidiaritás)?

A kiberreziliencia nem lehet tényleges az Unió egészében, ha azt nemzeti vagy regionális adatsilókon keresztül eltérő módon közelítik meg. A hálózat- és információbiztonsági irányelv ennek a hiányosságnak az orvoslásával volt hivatott rendezni a hálózati és információs rendszerek biztonságát nemzeti és uniós szinten. Átültetése és végrehajtása azonban bizonyos rendelkezések vagy megközelítések eredendő hibáira is rávilágított, például a kiberbiztonsági irányelv hatályának homályos körülhatárolására. Ezenkívül a Covid19-válság óta az európai gazdaság minden eddiginél jobban függ a hálózati és információs

rendszerektől, és az ágazatok és a szolgáltatások egyre inkább összekapcsolódnak. A kiberbiztonsági irányelv első időszakos felülvizsgálata tehát lehetőséget teremtett további uniós fellépésre. A kiberbiztonsági irányelv jelenlegi intézkedésein túlmutató uniós beavatkozást elsősorban a következők indokolják: i. a probléma határokon átnyúló vonatkozásai; ii. az uniós fellépés potenciálja a hathatós nemzeti politikák javítása és megkönnyítése terén; iii. összehangolt és együttműködő hálózati és információs rendszerekkel kapcsolatos szakpolitikai fellépések az adatvédelem és a magánélet hatékony védelme céljából.

B. Megoldások

Milyen alternatívák kínálkoznak a célok elérésére? Van-e előnyben részesített alternatíva? Amennyiben nincs, miért nincs?

A hatásvizsgálat négy szakpolitikai alternatívát elemzett: (0) a jelenlegi helyzet fenntartása; (1) nem jogalkotási intézkedések az átültetés összehangolására; (2) a kiberbiztonsági irányelv kisebb módosítása a további harmonizáció érdekében; (3) a kiberbiztonsági irányelv rendszerszintű és strukturális változtatásai. Az 1. lehetőséget korai szakaszban elvetették, mivel nem tér el jelentősen a fennálló helyzettől. A hatásvizsgálat arra a következtetésre jutott, hogy az **előnyben részesített lehetőség** a 3. lehetőség (azaz **a hálózati és információs rendszerek biztonsági keretének rendszerszintű és strukturális változtatásai**), mivel ez az egész Unióban a gazdaságok szélesebb szegmensének lefedése irányába mutató alapvetőbb megközelítésváltás, mégis koncentráltabb felügyelettel, amely arányosan a nagy és kulcsfontosságú vállalatokra fókuszál, ugyanakkor egyértelműen meghatározza az alkalmazási kört. Ez egyszerűsítené és tovább harmonizálná a vállalatok biztonsággal kapcsolatos kötelezettségeit, hatékonyabb körülményeket teremtene a működési szempontok tekintetében, valamint egyértelmű alapot teremtene az érintett szereplők megosztott felelősségéhez és elszámoltathatóságához, és ösztönözné az információmegosztást.

Mi az egyes érdekeltek álláspontja? Ki melyik alternatívát támogatja?

Az illetékes hatóságok és vállalkozások többsége támogatásának adott hangot a kiberbiztonsági irányelv felülvizsgálatával kapcsolatban. Több konzultáció során jelezték, hogy a hálózati és információs rendszerek biztonságáról szóló felülvizsgált irányelvnek ki kell terjednie további (al)ágazatokra, össze kell hangolnia vagy egyszerűsítenie kell a további biztonsági intézkedéseket és jelentéstételi kötelezettségeket. Az érdekelt felek támogatták azokat az új koncepciókat vagy szakpolitikával kapcsolatos intézkedéseket is, amelyek csak az előnyben részesített alternatíva részét képezik (pl. ellátási lánc biztonsági politikája, egy működő uniós válságkezelési keretrendszer intézményesítése).

C. Az előnyben részesített alternatíva hatásai

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

Az előnyben részesített alternatíva az alábbi jelentős előnyökkel járna: a kiberbiztonsági irányelv felülvizsgálatához készült támogató tanulmány szerint kidolgozott gazdasági modell alapján készített becslések azt mutatják, hogy az előnyben részesített alternatíva 11,3 milliárd EUR-val csökkentheti a kiberbiztonsági események költségeit.

Az ágazati hatókör jelentősen kibővülne a hálózati és információs rendszerek biztonsági keretén belül, de a fenti előnyök mellett a hálózati és információs rendszerek biztonsági követelményei által előidézhető teher – nevezetesen a felügyelet szempontjából – kiegyensúlyozásra kerülne mind a hatály alá újonnan bekerülő szervezetek, mind az illetékes hatóságok esetében. A hálózati és információs rendszerek új biztonsági kerete kétrétegű megközelítést vezetne be, amelynek középpontjában a nagy és kulcsfontosságú

szervezetek, valamint a felügyeleti rendszer differenciálása áll, amely csak utólagos felügyeletet tesz lehetővé (azaz reaktív felügyeletet a megfelelés módszeres dokumentálásának általános kötelezettsége nélkül) nagy számú, nevezetesen azon szervezetek esetében, amelyeket „fontosnak”, de nem „alapvetőnek” tekintenek.

Összességében az előnyben részesített szakpolitikai alternatíva hatékony kompromisszumokat és szinergiákat eredményezne, az összes elemzett szakpolitikai alternatíva közül a lehető legjobb lehetne annak biztosítása érdekében, hogy a kulcsfontosságú szervezetek magasabb és következetes szintű kiberrezilienciája az egész Unióban biztosítható legyen, ami végül költségmegtakarításhoz vezetne mind a vállalkozások, mind a társadalom számára.

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

Az előnyben részesített szakpolitikai alternatíva bizonyos megfelelési és végrehajtási költségekhez vezetne az érintett tagállami hatóságok számára (a források összességében mintegy 20–30 %-os növekedését becsülték). Az új keret ugyanakkor jelentős előnyökkel járna a kulcsfontosságú vállalkozások jobb áttekintése és az azokkal való interakció, a határokon átnyúló operatív együttműködés fokozása, valamint a kölcsönös segítségnyújtás és a szakértői értékelési mechanizmusok révén is. Ez a tagállamokban a kiberbiztonsági képességek általános növekedését eredményezné.

Becslések szerint azoknak a vállalatoknak, amelyek a hálózati és információs rendszerek biztonsági keretének hatálya alá tartoznának, a hálózati és információs rendszerek új biztonsági keretének bevezetését követő első években a jelenlegi IKT-biztonsági kiadásaik legfeljebb 22 %-os növelésére lenne szükségük (ez 12 % a már a kiberbiztonsági irányelv hatálya alá tartozó vállalatok esetében). Az IKT-biztonsági kiadások ezen átlagos növekedése azonban az említett beruházások arányos hasznát eredményezné, elsősorban a kiberbiztonsági események költségeinek jelentős (becslések szerint tíz év alatt 11,3 milliárd EUR értékű) csökkenése miatt.

Milyen hatást gyakorol az intézkedés a kkv-kra és a versenyképességre?

Az előnyben részesített alternatíva szerint a kis- és mikrovállalkozások mentesülnének a hálózati és információs rendszerek biztonsági keretének hatálya alól. A középvállalkozások esetében várható, hogy a hálózati és információs rendszerek új biztonsági keretének bevezetését követő első években emelkedni fog az IKT-biztonsági kiadások szintje. Ugyanakkor az e szervezetekre vonatkozó biztonsági követelmények emelése ösztönözné kiberbiztonsági képességeiket és elősegítené IKT-kockázatkezelésük javítását.

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

Lesz hatás a tagállamok költségvetésére és közigazgatására: A források esetében körülbelül 20–30 %-os becsült növekedés várható rövid és középtávon.

Lesznek-e egyéb jelentős hatások?

Egyéb jelentős negatív hatás nem várható. Az előnyben részesített szakpolitikai alternatíva várhatóan erőteljesebb kiberbiztonsági képességekhez vezet, és ennek következtében jelentősebb mérséklő hatása lesz az események – ideértve az adatokkal való visszaéléseket is – száma és súlyossága vonatkozásában. Valószínűleg pozitív hatása lesz az egyenlő versenyfeltételek biztosítása tekintetében a tagállamokban a kiberbiztonsági irányelv hatálya alá tartozó valamennyi szervezet számára, és csökkenti a kiberbiztonsági információs aszimmetriákat.

Arányosság?

Az előnyben részesített alternatíva nem lépi túl a konkrét célok kielégítő eléréséhez szükséges mértéket. A biztonsági intézkedések és a jelentéstételi kötelezettségek tervezett összehangolása és korszerűsítése a tagállamok és a vállalkozások azon kéréseihez kapcsolódik, amelyek a jelenlegi keret javítására irányultak.
D. További lépések
Mikor kerül sor a szakpolitikai fellépés felülvizsgálatára?
Az első felülvizsgálatra 54 hónappal a jogi eszköz hatálybalépését követően kerül sor. A Bizottság jelentést nyújt be az Európai Parlamentnek és a Tanácsnak a felülvizsgálatról. A felülvizsgálatot az ENISA és az együttműködési csoport támogatásával készítenék el.