Az Európai Unió
Tanácsa

Brüsszel, 2022. szeptember 16.
(OR. en)

Intézményközi referenciaszám:
2022/0272(COD)

12429/22
ADD 6

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2022. szeptember 15.
Címzett:	a Tanács Főtitkársága
Biz. dok. sz.:	SWD(2022) 283 final
Tárgy:	BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM A HATÁSVIZSGÁLATI JELENTÉS VEZETŐI ÖSSZEFOGLALÓJA a kiberrezilienciáról szóló jogszabályról amely a következő dokumentumot kíséri: Javaslat – Az Európai Parlament és a Tanács rendelete a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről és az (EU) 2019/1020 rendelet módosításáról

Mellékelten továbbítjuk a delegációknak a SWD(2022) 283 final számú dokumentumot.

Melléklet: SWD(2022) 283 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2022.9.15.
SWD(2022) 283 final

BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM

A HATÁSVIZSGÁLATI JELENTÉS VEZETŐI ÖSSZEFOGLALÓJA

a kiberrezilienciáról szóló jogszabályról

amely a következő dokumentumot kíséri:

Javaslat
AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről és az (EU) 2019/1020 rendelet módosításáról

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Vezetői összefoglaló (legfeljebb 2 oldal)

A kiberrezilienciáról szóló jogszabály (CRA) hatásvizsgálata

A. A fellépés szükségessége

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

A hardver- és szoftvertermékek gyakran sikeres kibertámadások áldozatai, ami a kiberbűnözés becsült éves költségét 2021-re 5,5 billió EUR-ra növelte. Ezek a termékek két fő problémával küzdenek, amelyek növelik a felhasználók és a társadalom költségeit: 1. a kiberbiztonság szintje alacsony, ami a széles körben elterjedt sebezhetőségekben, valamint az ezek kezelését célzó biztonsági frissítések elégtelen és következetlen biztosításában nyilvánul meg, valamint 2. a felhasználók nem értik eléggé a problémát és nem férnek hozzá az információkhoz, ami megakadályozza őket abban, hogy megfelelő kiberbiztonsági jellemzőkkel rendelkező termékeket válasszanak vagy azokat biztonságosan használják.

A digitális elemeket tartalmazó termékek kiberbiztonságának határokon átnyúló jellege erőteljes, mivel az egyik országban előállított termékeket gyakran az egész belső piacon használják. Emellett az eredetileg egyetlen szervezetet vagy egyetlen tagállamot érintő események gyakran perceken belül elterjednek a teljes belső piacon.

Bár a meglévő belső piaci jogszabályok lefednek bizonyos, digitális elemeket tartalmazó termékeket, a hardver- és szoftvertermékek többsége jelenleg nem tartozik a kiberbiztonságukat kezelő egyetlen uniós jogszabály hatálya alá sem. A jelenlegi uniós jogi keret különösen nem foglalkozik a nem beágyazott szoftverek kiberbiztonságával, annak ellenére, hogy a kiberbiztonsági támadások egyre inkább e termékek sebezhetőségeit célozzák, ami jelentős társadalmi és gazdasági költségekkel jár. Közelmúltbeli példa a Pegasus kémszoftver, amely a mobiltelefonok sebezhetőségeit használta ki, illetve a WannaCry zsarolóvírus féreg, amely a Windows egyik sebezhetőségét használta ki, és világszerte hatással volt a számítógépekre.

Mit kellene elérni?

A belső piac megfelelő működésének biztosítása érdekében két fő célkitűzést határoztak meg: 1. megteremteni a digitális elemeket tartalmazó biztonságos termékek fejlesztésének feltételeit annak biztosításával, hogy a hardver- és szoftvertermékeket kevesebb sebezhetőséggel hozzák forgalomba, és hogy a gyártók komolyan vegyék a biztonságot a termék teljes életciklusa során, valamint 2. olyan feltételeket teremteni, amelyek lehetővé teszik a felhasználók számára, hogy a digitális elemeket tartalmazó termékek kiválasztásakor és használatakor figyelembe vehessék a kiberbiztonságot. Négy konkrét célkitűzést határoztak meg: i. annak biztosítása, hogy a gyártók a tervezési és fejlesztési szakasztól kezdve, valamint a teljes életciklus során javítsák a digitális elemeket tartalmazó termékek biztonságát, ii. koherens kiberbiztonsági keret biztosítása, amely megkönnyíti a megfelelést a hardver- és szoftvergyártók számára, iii. a digitális elemeket tartalmazó termékek biztonsági tulajdonságai átláthatóságának fokozása, valamint iv. annak lehetővé tétele, hogy a vállalkozások és a fogyasztók biztonságosan használhassák a digitális elemeket tartalmazó termékeket.

Milyen többletértéket képvisel az uniós szintű fellépés (szubszidiaritás)?

A kiberbiztonság erős határokon átnyúló jellege és a határokon, ágazatokon és termékeken keresztül továbbgyűrűző hatásokkal járó, egyre növekvő számú kiberbiztonsági események miatt a célkitűzéseket a tagállamok önmagukban nem tudják hatékonyan megvalósítani. Tekintettel a digitális elemeket tartalmazó termékek piacának globális jellegére, a tagállamok a digitális elemeket tartalmazó ugyanazon termék tekintetében ugyanazokkal a kockázatokkal szembesülnek a területükön. A kialakulóban lévő,

potenciálisan eltérő nemzeti szabályokból álló, nem egységes keret azzal a veszéllyel is jár, hogy akadályozza a digitális elemeket tartalmazó termékek nyitott és versenyképes egységes piacát. Ezért uniós szintű együttes fellépésre van szükség a felhasználók körében a bizalom és az uniós piacon megjelenő, digitális elemeket tartalmazó termékek vonzerejének növelése érdekében. Ez a belső piac számára is előnyös lenne, mivel jogbiztonságot nyújtana és egyenlő versenyfeltételeket teremtene a digitális elemeket tartalmazó termékek gyártói számára.

B. Megoldások

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

A jelenlegi helyzeten túl négy szakpolitikai alternatívát és kapcsolódó részalternatívát vizsgáltak meg: 1. „puha” jogi megközelítés és önkéntes intézkedések, 2. a digitális elemeket tartalmazó materiális javak és a hozzájuk tartozó beágyazott szoftverek kiberbiztonságára irányuló termékspecifikus eseti szabályozói beavatkozás, 3. vegyes megközelítés, amely a digitális elemeket tartalmazó materiális javak és a hozzájuk tartozó beágyazott szoftverek kiberbiztonságára vonatkozó horizontális kógens szabályokat, valamint a nem beágyazott szoftverekre vonatkozó lépcsőzetes megközelítést tartalmaz, a megfelelőségértékelési eljárásra vonatkozó két részalternatívával, valamint 4. horizontális szabályozói beavatkozás, amely kiberbiztonsági követelményeket vezet be a digitális elemeket tartalmazó termékek széles körére vonatkozóan, beleértve a nem beágyazott szoftvereket is, a hatályra és a megfelelőségértékelési eljárásra vonatkozó részalternatívákkal.

A konkrét célkitűzésekhez viszonyított eredményesség, a hasznokhoz viszonyított költséghatékonyság és a következetesség alapján a hatásvizsgálat arra a következtetésre jutott, hogy az **előnyben részesített alternatíva** a 4. alternatíva, amely a digitális elemeket tartalmazó valamennyi termékre kiterjed, és a kritikus termékek tekintetében harmadik fél általi kötelező értékelést ír elő.

Mi az egyes érdekelt felek álláspontja? Ki melyik alternatívát támogatja?

Amikor azt kérték, hogy értékeljék a szakpolitikai beavatkozások hatékonyságát, a nyilvános konzultáció válaszadói egyetértettek abban, hogy a 4. alternatíva lenne a leghatékonyabb intézkedés (4,08 az 1-től 5-ig terjedő skálán). Ez magában foglalja a fogyasztói szervezeteket (5,00), a magukat felhasználóként azonosító válaszadókat (4,22), a bejelentett szervezeteket (4,17), a piacfelügyeleti hatóságokat (5,00) és a digitális elemeket tartalmazó termékek gyártóit (3,85), a kis- és közepes méretűeket is ideértve (4,05).

C. Az előnyben részesített alternatíva hatásai

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

Az előnyben részesített alternatíva jelentős előnyökkel járna a különböző érdekelt felek számára. A vállalkozások számára megakadályozná a digitális elemeket tartalmazó termékekre vonatkozó eltérő biztonsági szabályokat, és csökkentené a kapcsolódó kiberbiztonsági jogszabályoknak való megfelelés költségeit. Csökkentené a kiberbiztonsági események számát, a biztonsági események kezelésének költségeit és a hírnév romlásával járó károkat. A becslések szerint a kezdeményezés az EU egészére nézve évente mintegy 180–290 milliárd EUR-val csökkentheti a vállalkozásokat érintő kiberbiztonsági eseményekből eredő költségeket. A kezdeményezés továbbá a digitális elemeket tartalmazó termékek növekvő elterjedése miatt a forgalom növekedéséhez vezetne. Emellett javítaná a vállalatok globális hírnevét, ami az EU-n kívülről érkező kereslet növekedéséhez vezetne. A végfelhasználók számára az előnyben részesített alternatíva növelné a biztonsági tulajdonságok átláthatóságát, és megkönnyítené a digitális elemeket tartalmazó termékek használatát. A fogyasztók és a polgárok emellett nagyobb védelmet

élvezhetnének az alapvető jogaik, például a magánélethez és az adatvédelemhez való joguk tekintetében.

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

Az előnyben részesített alternatíva megfelelési és végrehajtási költségeket róna a vállalkozásokra, a bejelentett szervezetekre és az állami hatóságokra, ideértve a bejelentő, az akkreditáló és a piacfelügyeleti hatóságokat. A szoftverfejlesztők és a hardvergyártók számára növelni fogja az új kiberbiztonsági követelményekkel, a megfelelőségértékelési eljárással, a dokumentációs és jelentéstételi kötelezettségekkel kapcsolatos közvetlen megfelelési költségeket, aminek következtében az összesített megfelelési költségek mintegy 29 milliárd EUR-t tesznek majd ki a digitális elemeket tartalmazó termékek becsült piaci értéke alapján, amelyek forgalma akár 1 485 milliárd EUR is lehet. A végfelhasználók, köztük az üzleti végfelhasználók, a fogyasztók és a polgárok a digitális elemeket tartalmazó termékek magasabb árával szembesülhetnek. Ezeket azonban a fent leírt jelentős előnyök fényében kell vizsgálni. A bejelentett szervezetek esetében a többletköltségeket várhatóan ellensúlyozza a forgalom növekedése.

Milyen hatást gyakorol a fellépés a kkv-kra és a versenyképességre?

Az új követelmények mind gyártóként, mind végfelhasználóként hatással lesznek a kkv-kra. A megfelelési költségek elvben nagyobb mértékben érintenék a kkv-kat, mint a nagyvállalatokat, amelyek jellemzően jobb méretgazdaságossággal és nagyobb kiberbiztonsági tudatossággal rendelkeznek. A kkv-k azonban nagymértékben profitálnának a kezdeményezésből, mivel a digitális elemeket tartalmazó termékekbe ágyazott kiberbiztonság jelentős költségmegtakarítást jelentene a kkv-k mint felhasználók számára. Gyártóként a kkv-k a nagyobb végfelhasználói bizalom és az új ügyfelek előnyeit élvezhetnék. A belső piachoz való zökkenőmentes hozzáférés és a piac széttagoltságának csökkenése még előnyösebb lehet a kkv-k számára, mivel kevésbé vannak felkészülve a különböző szabályozói követelmények kezelésére. A kkv-k, miközben hangsúlyozták, hogy arányos megközelítésre és támogató intézkedésekre van szükség, általánosságban támogatták az összes vállalat közötti egyenlő versenyfeltételeket, és úgy vélték, hogy horizontális kötelező követelmények esetén sem lennének hátrányos helyzetben a nagyobb vállalatokhoz képest.

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

A kezdeményezés hatással lesz a nemzeti hatóságokra, például a nemzeti bejelentő hatóságokra, az akkreditáló hatóságokra és a piacfelügyeleti hatóságokra, amelyek felelősek a javasolt intézkedések nyomon követéséért és végrehajtásáért. Ezeknek a hatóságoknak további alkalmazkodási (pl. képzés és emberi erőforrások) és végrehajtási költségeket kell viselniük az új követelmények figyelembevétele érdekében. Az akkreditáló testületek által elköltött forrásokat azonban ellentételezik, és nagyrészt a megfelelőségértékelő szervezetek viselik akkreditációs szolgáltatások vásárlása révén.

Lesznek-e egyéb jelentős hatások?

Egyéb jelentős negatív hatás nem várható. Az előnyben részesített szakpolitikai alternatíva segítene csökkenteni a kiberbiztonsági események számát és súlyosságát, beleértve az adatvédelmi incidenseket is, és pozitív társadalmi hatásokkal járna, például csökkentené a kiberbűnözést. A biztonsági szakemberek iránti kereslet valószínűleg növekedni fog, és csökkennének a kiberbiztonsági információs aszimmetriák.

Arányosság?

Az előnyben részesített alternatíva nem lépi túl a konkrét célok kielégítő eléréséhez szükséges mértéket. A beavatkozás biztosítaná, hogy a digitális elemeket tartalmazó termékek teljes életciklusuk alatt és a

felmerülő kockázatokkal arányosan biztosítva legyenek.
D. További lépések
Mikor kerül sor a szakpolitikai fellépés felülvizsgálatára?
A Bizottság e kezdeményezés alkalmazásának kezdőnapját követő [36 hónappal] később, majd azt követően négyévente jelentést nyújt be az Európai Parlamentnek és a Tanácsnak e kezdeményezés értékeléséről és felülvizsgálatáról.