Consiliul
Uniunii Europene

Bruxelles, 16 septembrie 2022
(OR. en)

12429/22
ADD 6

Dosar interinstituțional:
2022/0272 (COD)

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

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	15 septembrie 2022
Destinatar:	Secretariatul General al Consiliului
Nr. doc. Csie:	SWD(2022) 283 final
Subiect:	DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI REZUMAT AL RAPORTULUI PRIVIND EVALUAREA IMPACTULUI **referitor la Actul european privind reziliența cibernetică** care însoţeşte documentul Propunere de regulament al Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentului (UE) 2019/1020

În anexă, se pune la dispoziția delegațiilor documentul SWD(2022) 283 final.

Anexă: SWD(2022) 283 final

COMISIA
EUROPEANĂ

Bruxelles, 15.9.2022
SWD(2022) 283 final

DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI

REZUMAT AL RAPORTULUI PRIVIND EVALUAREA IMPACTULUI

referitor la Actul european privind reziliența cibernetică

care însoţeşte documentul

Propunere de regulament al Parlamentului European și al Consiliului

privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentului (UE) 2019/1020

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

Fișă rezumat (maximum 2 pagini)

Evaluarea impactului Actului european privind reziliența cibernetică (ARC)

A. Necesitatea de a acționa

Care este problema și de ce constituie o preocupare la nivelul UE?

Produsele hardware și software fac adesea obiectul unor atacuri cibernetice reușite, lucru care a dus la un cost global anual al criminalității informatice estimat la 5,5 mii de miliarde EUR până în 2021. Aceste produse se confruntă cu două probleme majore, care generează costuri suplimentare pentru utilizatori și pentru societate: (1) un nivel scăzut de securitate cibernetică, care se reflectă în răspândirea pe scară largă a vulnerabilităților și în furnizarea insuficientă și inconsecventă de actualizări de securitate pentru abordarea acestora și (2) accesul insuficient la informații și înțelegerea insuficientă a acestora de către utilizatori, ceea ce îi împiedică să aleagă produse cu caracteristici adecvate de securitate cibernetică sau să le utilizeze în mod securizat.

Securitatea cibernetică a produselor cu elemente digitale are o puternică dimensiune transfrontalieră, deoarece produsele fabricate într-o țară sunt adesea utilizate pe întreaga piață internă. În plus, incidentele care afectează inițial o singură entitate sau un singur stat membru se răspândesc adesea în câteva minute pe întreaga piață internă.

Deși legislația existentă privind piața internă se aplică anumitor produse cu elemente digitale, majoritatea produselor hardware și software nu fac în prezent obiectul niciunui act legislativ al UE care să abordeze securitatea cibernetică a acestora. În special, cadrul juridic actual al UE nu abordează securitatea cibernetică a software-ului neîncorporat, chiar dacă atacurile cibernetice vizează din ce în ce mai mult vulnerabilitățile acestor produse, generând costuri societale și economice semnificative. Exemple recente sunt programul de spionaj Pegasus, care a exploatat vulnerabilitățile telefoanelor mobile, și viermele de ransomware WannaCry, care a exploatat o vulnerabilitate a sistemului Windows, afectând calculatoare din întreaga lume.

Care este rezultatul urmărit?

Au fost identificate două obiective principale menite să asigure buna funcționare a pieței interne: (1) crearea condițiilor pentru dezvoltarea de produse cu elemente digitale care să fie sigure prin garantarea faptului că produsele hardware și software sunt introduse pe piață cu mai puține vulnerabilități și că producătorii tratează cu seriozitate securitatea pe parcursul întregului ciclu de viață al unui produs și (2) crearea unor condiții care să le permită utilizatorilor să țină seama de securitatea cibernetică atunci când aleg și utilizează produse cu elemente digitale. Au fost stabilite patru obiective specifice**:** (i) asigurarea faptului că producătorii îmbunătățesc securitatea produselor cu elemente digitale încă din etapa de proiectare și dezvoltare și pe parcursul întregului ciclu de viață; (ii) asigurarea unui cadru coerent de securitate cibernetică, care să faciliteze conformarea producătorilor de hardware și software; (iii) sporirea transparenței proprietăților de securitate ale produselor cu elemente digitale și (iv) facilitarea utilizării în condiții de siguranță a produselor cu elemente digitale de către întreprinderi și consumatori.

Care este valoarea adăugată a acțiunii la nivelul UE (subsidiaritate)?

Caracterul transfrontalier puternic al securității cibernetice și numărul tot mai mare de incidente care au efecte de propagare dincolo de frontiere, sectoare și produse fac ca obiectivele să nu poată fi realizate în mod eficace de către statele membre în mod individual. Din cauza caracterului global al pieței produselor cu elemente digitale, statele membre se confruntă cu aceleași riscuri pentru același produs cu elemente digitale pe teritoriul lor. În același timp, apariția unui cadru neuniform de norme naționale

potențial divergente riscă să constituie o piedică pentru o piață unică deschisă și competitivă a produselor cu elemente digitale. Prin urmare, este necesară o acțiune comună la nivelul UE pentru a spori nivelul de încredere în rândul utilizatorilor și atractivitatea produselor cu elemente digitale introduse pe piața UE. Aceasta ar fi benefică și pentru piața internă, întrucât ar oferi securitate juridică și ar crea condiții de concurență echitabile pentru producătorii de produse cu elemente digitale.

B. Soluții

Care sunt diferitele opțiuni disponibile pentru atingerea obiectivelor? Există o opțiune preferată? Dacă nu, de ce?

Au fost analizate patru opțiuni de politică și subopțiunile conexe care depășesc statu-quo-ul: (1) o abordare bazată pe instrumente juridice neobligatorii și măsuri voluntare; (2) o intervenție normativă ad-hoc specifică produselor pentru securitatea cibernetică a produselor fizice cu elemente digitale și a software-ului încorporat în acestea; (3) o abordare mixtă, incluzând norme orizontale obligatorii pentru securitatea cibernetică a produselor fizice cu elemente digitale și a software-ului încorporat în acestea și o abordare eșalonată pentru software-ul neîncorporat, cu două subopțiuni pentru evaluarea conformității și (4) o intervenție normativă orizontală care să introducă cerințe de securitate cibernetică pentru o gamă largă de produse cu elemente digitale, inclusiv pentru software-ul neîncorporat, cu subopțiuni privind domeniul de aplicare și evaluarea conformității.

Evaluarea impactului a concluzionat că **opțiunea preferată** este opțiunea 4, care acoperă toate produsele cu elemente digitale și prevede o evaluare obligatorie de către terți pentru produsele critice, bazată pe evaluarea eficacității în raport cu obiectivele specifice, a eficienței costurilor în raport cu beneficiile și a coerenței.

Care sunt punctele de vedere ale diferitelor părți interesate? Care sunt susținătorii fiecărei opțiuni?

Atunci când li s-a solicitat să evalueze eficacitatea intervențiilor de politică, respondenții la consultarea publică au fost de acord că opțiunea 4 ar fi cea mai eficace măsură (4,08 pe o scară de la 1 la 5). Printre aceștia s-au numărat organizații de consumatori (5,00), respondenți care se identifică drept utilizatori (4,22), organisme notificate (4,17), autorități de supraveghere a pieței (5,00) și producători de produse cu elemente digitale (3,85), inclusiv cei de dimensiuni mici și mijlocii (4,05).

C. Impactul opțiunii preferate

Care sunt avantajele opțiunii preferate (sau ale opțiunilor principale, în cazul în care nu există o opțiune preferată)?

Opțiunea preferată ar aduce avantaje semnificative diferitelor părți interesate. În ceea ce privește întreprinderile, acest lucru ar preveni normele de securitate divergente pentru produsele cu elemente digitale și ar reduce costurile de conformare pentru legislația conexă în materie de securitate cibernetică. De asemenea, ar reduce numărul de incidente cibernetice, costurile de gestionare a incidentelor și atingerea adusă reputației. În ceea ce privește UE în ansamblu, se estimează că inițiativa ar putea duce la o reducere a costurilor generate de incidentele care afectează întreprinderile cu aproximativ 180-290 de miliarde EUR anual. În plus, inițiativa ar duce la o creștere a cifrei de afaceri ca urmare a utilizării pe scară din ce în ce mai largă a produselor cu elemente digitale. De asemenea, aceasta ar îmbunătăți reputația globală a întreprinderilor, ceea ce ar duce la o creștere a cererii în afara UE. În ceea ce privește utilizatorii finali, opțiunea preferată ar spori transparența proprietăților de securitate și ar facilita utilizarea produselor cu elemente digitale. Consumatorii și cetățenii ar beneficia, de asemenea, de o mai bună protecție a drepturilor lor fundamentale, cum ar fi protecția vieții private și a datelor.

Care sunt costurile aferente opțiunii preferate (dacă există; în caz contrar, ale opțiunilor principale)?
Opțiunea preferată ar adăuga costuri de conformare și de asigurare a respectării legislației pentru întreprinderi, organismele notificate și autoritățile publice, inclusiv pentru autoritățile de notificare, de acreditare și de supraveghere a pieței. Pentru dezvoltatorii de software și producătorii de hardware, aceasta va crește costurile directe de conformare în ceea ce privește noile cerințe de securitate cibernetică, evaluarea conformității, documentația și obligațiile de raportare, ceea ce va duce la costuri de conformare agregate de până la aproximativ 29 de miliarde EUR pentru o valoare de piață estimată a produselor cu elemente digitale de până la 1 485 de miliarde EUR ca cifră de afaceri. Utilizatorii finali, inclusiv utilizatorii finali comerciali, consumatorii și cetățenii se pot confrunta cu prețuri mai mari ale produselor cu elemente digitale. Totuși, acestea ar trebui privite în contextul avantajelor semnificative descrise mai sus. În ceea ce privește organismele notificate, se preconizează că costurile suplimentare vor fi compensate printr-o creștere a cifrei de afaceri.
Care sunt efectele asupra IMM-urilor și asupra competitivității?
IMM-urile vor fi afectate de noile cerințe atât în calitate de producători, cât și de utilizatori finali. În ceea ce privește costurile de conformare, IMM-urile ar fi, în principiu, mai afectate decât întreprinderile mari, care au, de regulă, economii de scară mai importante și o mai bună conștientizare a securității cibernetice. Cu toate acestea, IMM-urile ar beneficia în mare măsură de pe urma inițiativei, întrucât securitatea cibernetică încorporată în produsele cu elemente digitale ar genera economii semnificative de costuri pentru IMM-uri în calitate de utilizatori. În calitate de producători, IMM-urile ar beneficia de o mai mare încredere a utilizatorilor finali și de noi clienți. Accesul neîntrerupt la piața internă și reducerea fragmentării pieței pot fi și mai benefice pentru IMM-uri, care sunt mai puțin pregătite pentru a face față cerințelor de reglementare diferite. Deși au subliniat necesitatea unei abordări proporționale și a unor măsuri de sprijin, IMM-urile s-au exprimat, în general, în sprijinul unor condiții de concurență echitabile între toate întreprinderile și nu au considerat că ar fi dezavantajate în comparație cu întreprinderile mai mari într-un scenariu de cerințe orizontale obligatorii.
Va exista un impact semnificativ asupra bugetelor și administrațiilor naționale?
Inițiativa va avea un impact asupra autorităților naționale, cum ar fi autoritățile naționale de notificare, de acreditare și de supraveghere a pieței, care au responsabilitatea de a monitoriza și de a pune în aplicare măsurile propuse. Aceste autorități vor suporta ajustări suplimentare (de exemplu, din punctul de vedere al formării și al resurselor umane) și costuri de punere în aplicare pentru a ține seama de noile cerințe. Totuși, resursele utilizate de organismele de acreditare sunt compensate și suportate în mare parte de organismele de evaluare a conformității prin achiziționarea de servicii de acreditare.
Vor exista alte efecte semnificative?
Nu se preconizează niciun alt impact negativ semnificativ. Opțiunea de politică preferată ar contribui la reducerea numărului și a gravității incidentelor, inclusiv a încălcărilor securității datelor cu caracter personal, și ar avea efecte pozitive la nivel social, cum ar fi reducerea criminalității informatice. Este probabil ca cererea de profesioniști în domeniul securității să crească, iar asimetriile informaționale în materie de securitate cibernetică să fie reduse.
Proporționalitate?
Opțiunea preferată nu depășește ceea ce este necesar pentru îndeplinirea obiectivelor specifice în mod satisfăcător. Intervenția ar garanta securizarea produselor cu elemente digitale pe parcursul întregului lor

ciclu de viață și proporțional cu riscurile cu care se confruntă acestea.
D. Acțiuni ulterioare
Când va fi reexaminată politica?
Până la [36 de luni] de la data aplicării inițiativei și, ulterior, la fiecare patru ani, Comisia transmite Parlamentului European și Consiliului un raport privind evaluarea și reexaminarea inițiativei.