Consiliul
Uniunii Europene

Bruxelles, 18 decembrie 2020
(OR. en)

14150/20
ADD 3

Dosar interinstituțional:
2020/0359(COD)

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

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	16 decembrie 2020
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	SWD(2020) 344 final
Subiect:	DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI REZUMAT AL RAPORTULUI PRIVIND EVALUAREA IMPACTULUI care însoţeşte documentul Propunere de directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148

În anexă, se pune la dispoziția delegațiilor documentul SWD(2020) 344 final.

Anexă: SWD(2020) 344 final

COMISIA
EUROPEANĂ

Bruxelles, 16.12.2020
SWD(2020) 344 final

DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI

REZUMAT AL RAPORTULUI PRIVIND EVALUAREA IMPACTULUI

care însoţeşte documentul

Propunere de directivă a Parlamentului European şi a Consiliului

privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148

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

Fișă rezumat

Evaluarea impactului privind *Revizuirea Directivei (UE) 2016/1148 din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (denumită în continuare „Directiva NIS")*

A. Necesitatea de a acționa

Care este problema și de ce este o problemă la nivelul UE?

În pofida realizărilor sale notabile, Directiva NIS, care a pregătit terenul pentru o schimbare semnificativă de mentalitate și o abordare instituțională și de reglementare a securității cibernetice în multe state membre, și-a dovedit, între timp, și limitările. Transformarea digitală a societății (intensificată de criza provocată de pandemia de COVID-19) a extins situația amenințărilor și generează noi provocări care necesită răspunsuri adaptate și inovatoare. Numărul atacurilor cibernetice este în continuă creștere, atacurile, care sunt tot mai sofisticate, provenind dintr-o gamă largă de surse din interiorul și din afara UE.

Pe baza evaluării funcționării Directivei NIS, evaluarea impactului a identificat următoarele probleme: nivelul scăzut de reziliență cibernetică a întreprinderilor care își desfășoară activitatea în UE inconsecvența rezilienței în toate statele membre și în toate sectoarele și nivelul scăzut de conștientizare comună a situației și lipsa unui răspuns comun în caz de criză. De exemplu, ca urmare a unora dintre aceste probleme și factori determinanți, există situații în care anumite spitale importante dintr-un stat membru nu intră în domeniul de aplicare al Directivei NIS și, prin urmare, nu sunt obligate să pună în aplicare măsurile de securitate corespunzătoare, în timp ce, într-un alt stat membru, aproape fiecare spital din țară trebuie să respecte cerințele de securitate NIS.

Ce obiective ar trebui realizate?

Cu ocazia revizuirii NIS, sunt avute în vedere trei obiective generale:

1. **Îmbunătățirea nivelului de reziliență cibernetică a unui set cuprinzător de întreprinderi care își desfășoară activitatea în Uniunea Europeană în toate sectoarele relevante**, prin instituirea unor norme care să asigure că toate entitățile publice și private de pe piața internă care îndeplinesc funcții importante pentru economie și societate în ansamblu sunt obligate să ia măsuri adecvate în materie de securitate cibernetică.
2. **Reducerea inconsecvențelor în ceea ce privește reziliența pe piața internă în sectoarele care fac deja obiectul directivei**, prin alinierea în continuare (1) a domeniului de aplicare *de facto*, (2) a cerințelor în materie de securitate și raportare a incidentelor, (3) a dispozițiilor care reglementează supravegherea și asigurarea respectării legislației la nivel național și (4) a capacităților autorităților competente din statele membre.
3. **Îmbunătățirea nivelului de conștientizare comună a situației și a capacității colective de pregătire și de răspuns**, prin luarea de măsuri pentru îmbunătățirea nivelului de încredere între autoritățile competente, prin schimbul mai multor informații și prin stabilirea de norme și proceduri în cazul unui incident sau al unei crize de mare amploare.

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

Reziliența în materie de securitate cibernetică în întreaga Uniune nu poate fi eficace dacă este abordată într-un mod disparat prin fragmentări naționale sau regionale. Directiva NIS a ajuns să abordeze această deficiență prin stabilirea unui cadru pentru securitatea rețelelor și a sistemelor informatice la nivel național și la nivelul Uniunii. Cu toate acestea, transpunerea și punerea sa în aplicare au evidențiat, de asemenea,

deficiențe inerente ale anumitor dispoziții sau abordări, cum ar fi delimitarea neclară a domeniului de aplicare al Directivei NIS. În plus, odată cu criza provocată de pandemia de COVID-19, economia europeană a devenit mai dependentă decât oricând de rețele și de sistemele informatice, iar sectoarele și serviciile sunt din ce în ce mai interconectate. Prima revizuire periodică a Directivei NIS a creat, prin urmare, oportunitatea unor acțiuni suplimentare la nivelul UE. Intervenția UE, care depășește măsurile actuale prevăzute în Directiva NIS, este justificată în principal de: (i) caracterul transfrontalier al problemei; (ii) potențialul acțiunii UE de îmbunătățire și de facilitare a unor politici naționale eficace; (iii) contribuția acțiunilor politice concertate și colaborative în domeniul NIS la protejarea eficace a protecției datelor și a vieții private.

B. Soluții

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

Evaluarea impactului a analizat patru opțiuni de politică: (0) menținerea situației actuale; (1) măsuri fără caracter legislativ pentru alinierea transpunerii; (2) modificări limitate ale Directivei NIS în vederea unei armonizări suplimentare; (3) modificări sistemice și structurale ale Directivei NIS. Opțiunea 1 a fost respinsă într-un stadiu incipient, deoarece nu se îndepărtează în mod considerabil de situația actuală. Evaluarea impactului concluzionează că **opțiunea preferată** este opțiunea 3 (și anume, **modificări sistemice și structurale ale cadrului NIS**), întrucât ar avea în vedere o schimbare fundamentală a abordării către acoperirea unui segment mai larg al economiilor din întreaga Uniune, dar cu o supraveghere mai focalizată care să vizeze în mod proporțional întreprinderile mari și esențiale, stabilind în același timp în mod clar domeniul de aplicare. De asemenea, aceasta ar raționaliza și ar armoniza în continuare obligațiile în materie de securitate ale întreprinderilor, ar crea un cadru mai eficace pentru aspectele operaționale, ar stabili o bază clară pentru partajarea responsabilităților și a răspunderii actorilor relevanți și ar stimula schimbul de informații.

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

Majoritatea autorităților competente și a întreprinderilor și-au manifestat sprijinul pentru o revizuire a Directivei NIS. În cadrul mai multor consultări, acestea au semnalat faptul că o Directivă NIS revizuită ar trebui să acopere (sub)sectoare suplimentare și să alinieze sau să raționalizeze măsuri de securitate și obligații de raportare suplimentare. Părțile interesate și-au manifestat, de asemenea, sprijinul pentru noi concepte sau măsuri legate de politici care reprezintă doar o parte a opțiunii preferate (de exemplu, politicile de securitate a lanțului de aprovizionare, instituționalizarea unui cadru operațional al UE de gestionare a crizelor).

C. Impactul opțiunii preferate

Care sunt avantajele opțiunii preferate (dacă există; în caz contrar, ale opțiunilor principale)?

Opțiunea preferată ar aduce beneficii semnificative: estimările efectuate pe baza unei modelări economice elaborate de un studiu în sprijinul revizuirii Directivei NIS indică faptul că opțiunea preferată ar putea duce la o reducere a costului incidentelor de securitate cibernetică cu 11,3 miliarde EUR.

Domeniul de aplicare sectorial ar fi extins în mod considerabil în cadrul NIS, dar, pe lângă beneficiile de mai sus, sarcina care poate fi creată de cerințele în materie de NIS, în special din perspectiva supravegherii, ar fi, de asemenea, echilibrată atât pentru noile entități care urmează să fie acoperite, cât și pentru autoritățile competente. Acest lucru se datorează faptului că noul cadru NIS ar stabili o abordare pe două niveluri, cu accent pe entitățile mari și esențiale și o diferențiere a regimului de supraveghere care

permite doar supravegherea *ex post* (mai precis, reactivă și fără o obligație generală de a documenta în mod sistematic îndeplinirea cerințelor) pentru un număr mare de entități, în special pentru cele considerate „importante”, dar nu „esențiale”.

În general, opțiunea de politică preferată ar conduce la compromisuri și sinergii eficiente, cu cel mai bun potențial dintre toate opțiunile de politică analizate pentru a asigura un nivel sporit și consecvent de reziliență cibernetică a entităților-cheie din întreaga Uniune, ceea ce ar duce, în cele din urmă, la economii de costuri atât pentru întreprinderi, cât și pentru societate.

Care sunt costurile opțiunii preferate (dacă există; în caz contrar, ale opțiunilor principale)?

Opțiunea de politică preferată ar conduce, de asemenea, la anumite costuri de asigurare a conformității și de asigurare a respectării legislației pentru autoritățile relevante ale statelor membre (s-a estimat o creștere globală de aproximativ 20-30 % a resurselor). Cu toate acestea, noul cadru ar aduce, de asemenea, beneficii substanțiale printr-o mai bună imagine de ansamblu a principalelor întreprinderi și prin interacțiunea cu acestea, printr-o cooperare operațională transfrontalieră consolidată, precum și prin asistență reciprocă și mecanisme de evaluare *inter pares*. Acest lucru ar duce la o creștere globală a capacităților în materie de securitate cibernetică în statele membre.

Pentru societățile care s-ar încadra în domeniul de aplicare al cadrului NIS, se estimează că acestea ar trebui să își majoreze cu maximum 22 % cheltuielile actuale în materie de securitate TIC pentru primii ani de la introducerea noului cadru NIS, iar societățile care intră deja sub incidența actualei Directive NIS, cu 12 %. Totuși, această creștere medie a cheltuielilor în materie de securitate TIC ar conduce la un beneficiu proporțional al unor astfel de investiții, în special datorită unei reduceri considerabile a costurilor aferente incidentelor de securitate cibernetică (estimate la 11,3 miliarde EUR pe o perioadă de zece ani).

Care sunt efectele asupra IMM-urilor și asupra competitivității?

Întreprinderile mici și microîntreprinderile ar urma să fie excluse din domeniul de aplicare al cadrului NIS în cadrul opțiunii preferate. Pentru întreprinderile mijlocii, se poate preconiza o creștere a nivelului cheltuielilor în materie de securitate TIC în primii ani de la introducerea noului cadru NIS. În același timp, creșterea nivelului cerințelor de securitate pentru aceste entități le-ar stimula, de asemenea, capacitățile în materie de securitate cibernetică și ar contribui la îmbunătățirea gestionării riscurilor TIC.

Va exista un impact semnificativ asupra bugetelor și a administrațiilor naționale?

Va exista un impact asupra bugetelor și administrațiilor naționale: pe termen scurt și mediu, se preconizează o creștere estimată a resurselor de aproximativ 20-30 %.

Vor exista și alte efecte semnificative?

Nu se preconizează niciun alt impact negativ semnificativ. Conform estimărilor, opțiunea de politică preferată va conduce la capabilități de securitate cibernetică mai solide și, prin urmare, va avea un impact de atenuare mai substanțial asupra numărului de incidente și a gravității acestora, inclusiv asupra încălcărilor securității datelor. De asemenea, este probabil ca opțiunea să aibă un impact pozitiv asupra asigurării unor condiții de concurență echitabile între statele membre pentru toate entitățile care intră în domeniul de aplicare al NIS și să reducă asimetriile informaționale în materie de securitate cibernetică.

Proporționalitatea?

Opțiunea preferată nu depășește ceea ce este necesar pentru îndeplinirea obiectivelor specifice în mod satisfăcător. Alinierea și raționalizarea preconizate ale măsurilor de securitate și ale obligațiilor de

raportare au legătură cu solicitările statelor membre și ale întreprinderilor de îmbunătățire a cadrului actual.
D. Acțiuni ulterioare
Când va fi revizuită politica?
Prima revizuire ar urma să aibă loc la 54 de luni de la intrarea în vigoare a instrumentului juridic. Comisia ar urma să prezinte un raport Parlamentului European și Consiliului cu privire la revizuire, care ar urma să fie pregătită cu sprijinul ENISA și al grupului de cooperare.