Consiliul
Uniunii Europene

Bruxelles, 14 septembrie 2017
(OR. en)

12183/17
ADD 2

Dosar interinstituțional:
2017/0225 (COD)

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

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretar general al Comisiei Europene, sub semnătura dlui Jordi AYET PUIGARNAU, director
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	SWD(2017) 501 final
Subiect:	DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI REZUMATUL EVALUĂRII IMPACTULUI care însoţeşte documentul Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind ENISA, „Agenția UE pentru securitate cibernetică”, de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Legea privind securitatea cibernetică”)

În anexă, se pune la dispoziția delegațiilor documentul SWD(2017) 501 final.

Anexă: SWD(2017) 501 final

COMISIA
EUROPEANĂ

Bruxelles, 13.9.2017
SWD(2017) 501 final

DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI

REZUMATUL EVALUĂRII IMPACTULUI

care însoţeşte documentul

Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind ENISA, „Agenția UE pentru securitate cibernetică”, de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Legea privind securitatea cibernetică”)

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

A. SUNT NECESARE MĂSURI

Care este problema și de ce este o problemă?

Tehnologiile digitale și internetul constituie coloana vertebrală a economiei și a societății UE. Sectoare economice critice, cum ar fi transporturile, energia, sănătatea sau sectorul financiar, au devenit tot mai dependente de rețelele și sistemele informatice pentru desfășurarea activității lor principale. Internetul obiectelor conectează obiectele și persoanele prin rețele de comunicații. Această nouă realitate creează oportunități fără precedent, dar și vulnerabilități. Într-adevăr, incidentele cibernetice sunt din ce în ce mai frecvente și mai extinse. Complexitatea, frecvența și sfera impactului acestora, de la accesul la servicii esențiale la procesele democratice - vor crește și mai mult.

În acest context, au fost identificate următoarele probleme interdependente:

- o fragmentare a politicilor și a abordărilor în materie de securitate cibernetică între statele membre;
- resurse și abordări dispersate privind securitatea cibernetică ale instituțiilor, agențiilor și organelor UE;
- o cunoaștere insuficientă de către cetățeni și întreprinderi a amenințărilor cibernetice și informații insuficiente privind proprietățile de securitate ale produselor și serviciilor TIC pe care le achiziționează, alături de apariția unui număr tot mai mare sisteme multiple naționale și sectoriale de certificare.

Aceste probleme au un impact asupra rezilienței cibernetice generale a UE și asupra funcționării eficace a pieței interne.

Care sunt obiectivele urmărite?

Obiectivele specifice de politică ale inițiativei sunt următoarele:

1. sporirea capabilităților și a nivelului de pregătire ale statelor membre și întreprinderilor, în special în ceea ce privește infrastructurile critice;
2. îmbunătățirea cooperării și a coordonării dintre statele membre și instituțiile, agențiile și organele UE;
3. sporirea capabilităților la nivelul UE care să completeze acțiunea statelor membre, în special în cazul unei crize cibernetice transfrontaliere;
4. sporirea gradului de sensibilizare a cetățenilor și a întreprinderilor cu privire la aspectele legate de securitatea cibernetică;
5. sporirea transparenței la nivel global a asigurării securității cibernetice a produselor și serviciilor TIC pentru a consolida încrederea în piața unică digitală și în inovarea digitală;
6. evitarea fragmentării sistemelor de certificare în UE și a cerințelor de securitate aferente, precum și a criteriilor de evaluare în toate statele membre și în toate sectoarele.

Care este valoarea adăugată a unei acțiuni la nivelul UE?

Întrucât digitalizarea și interconectarea economiei și societății au o dimensiune mondială, amploarea problemelor depășește cu mult teritoriul unui singur stat membru. Prin urmare, este necesară o intervenție la nivelul Uniunii. În contextul actual și având în vedere scenariile viitoare, se pare că acțiunile individuale ale statelor membre și o abordare fragmentată a securității cibernetice, dată fiind dimensiunea sa transfrontalieră importantă, nu pot spori reziliența cibernetică colectivă a Uniunii.

B. SOLUȚII

Care sunt opțiunile disponibile pentru atingerea acestor obiective? Există o opțiune preferată?

Prezenta evaluare a impactului analizează un anumit set de opțiuni de politică ce acoperă revizuirea mandatului Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) și certificarea de securitate în domeniul TIC.

Revizuirea ENISA

Opțiunea 0 - Scenariul de referință - Această opțiune se referă la menținerea situației actuale. Mandatul ENISA ar fi extins, iar obiectivele și sarcinile agenției ar rămâne în cea mai mare parte neschimbate, ținându-se seama în același timp de sarcinile încredințate Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor prin legislația ulterioară a UE (de exemplu, Directiva privind securitatea rețelelor și a informațiilor).

Opțiunea 1 - Expirarea mandatului ENISA (desființarea Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor). Această opțiune ar conduce la desființarea Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor la sfârșitul mandatului său (iunie 2020) și, eventual, la o redistribuire a competențelor/activităților la nivelul UE și/sau la nivel național.

Opțiunea 2 - „ENISA reformată”. Această opțiune ar urma să se bazeze pe mandatul actual al ENISA, avându-se în vedere adoptarea unor modificări selective care țin seama de evoluțiile din domeniul securității cibernetice. Agenția ar primi un mandat permanent, ce are la bază următoarele elemente esențiale: sprijin pentru elaborarea și punerea în aplicare a politicilor UE, consolidarea capacităților, cunoștințe și informații, sarcini legate de piață, cercetare și inovare și cooperare operațională și gestionarea crizelor.

Opțiunea 3 - o agenție a UE pentru securitate cibernetică cu capacități operaționale depline. Această opțiune presupune reformarea ENISA, prin reunirea a trei funcții principale: 1. o funcție privind politicile/de consiliere; 2. un centru de informații și expertiză și 3. un centru de răspuns la incidente de securitate cibernetică (CERT). Această opțiune ar presupune, într-o mare măsură, aceeași modificare a domeniului de aplicare al mandatului ca în cazul opțiunii 2. Cu toate acestea, s-ar adăuga sarcini suplimentare în domeniul răspunsului la incidente și al gestionării situațiilor de criză, astfel încât agenția să acopere întregul ciclu de viață al securității cibernetice și să se ocupe de prevenirea și detectarea incidentelor cibernetice și de răspunsul la acestea.

Certificarea

Opțiunea 0- Scenariul de referință - nu se întreprinde nicio acțiune. În cadrul acestei opțiuni, Comisia ar menține situația actuală și nu ar întreprinde nicio acțiune legislativă sau de politică.

Opțiunea 1 - Măsuri nelegislative („fără caracter obligatoriu"). În cadrul acestei opțiuni, Comisia ar folosi instrumente de politică fără caracter obligatoriu (de exemplu, comunicările interpretative, susținerea inițiativelor de autoreglementare la nivelul UE și activitățile de standardizare) cu scopul de a îmbunătăți transparența și de a reduce fragmentarea.

Opțiunea 2 - Un act legislativ al UE care să extindă acordul SOG-IS la toate statele membre. În cadrul acestei opțiuni de politică, Comisia ar propune un act legislativ pentru a extinde din punct de vedere juridic acordul la toate statele membre.

Opțiunea 3 - Un **cadru UE de certificare generală de securitate în domeniul TIC**. Această opțiune presupune instituirea unui cadru european de certificare de securitate în domeniul TIC (care include un grup de experți alcătuit din autoritățile naționale) având la bază, într-o cât mai mare măsură posibil, sistemele existente de certificare de securitate în domeniul TIC. În esență, cadrul ar urma să permită instituirea unor sisteme de certificare la nivelul UE care să fie acceptate în toate statele membre.

Opțiunea preferată este o combinație între opțiunea 2 pentru ENISA și opțiunea 3 pentru certificare.

Care sunt diferitele părți interesate? Cine sunt susținătorii fiecărei opțiuni?

Marea majoritate a părților interesate din toate categoriile (statele membre, sectorul, instituțiile UE, comunitatea de cercetare) care au luat parte la consultări par să salute opțiunea preferată deoarece sunt pentru consolidarea ENISA și crearea unui cadru european de certificare de securitate în domeniul TIC.

În special, există un consens cu privire la necesitatea de a avea (cel puțin) o agenție a UE care funcționează bine, cu un mandat permanent, care dispune de resurse adecvate și care este mandatată să facă față provocărilor prezente și viitoare în materie de securitate cibernetică. Există, de asemenea, un amplu consens în rândul părților interesate cu privire la crearea unui cadru european voluntar, care să poată fi extins.

În ceea ce privește sectorul, această soluție pentru certificare este susținută de întreprinderile care fac deja obiectul unor cerințe de certificare și care ar avea de câștigat de pe urma unui mecanism la nivelul UE bazat pe recunoașterea reciprocă a certificatelor. Acest punct de vedere este susținut și de IMM-uri, care suferă cel mai mult dacă trebuie deja sau vor trebui să demareze procese de certificare diferite de la un stat membru la altul. Unele state membre, în special cele cu resurse mai puține, și unii reprezentanți ai sectorului și ai instituțiilor UE au exprimat opinii favorabile și în ceea ce privește opțiunea 3 pentru ENISA.

C. IMPACTUL OPȚIUNII PREFERATE

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

În cadrul opțiunii preferate, UE ar dispune de o agenție axată pe sprijinirea statelor membre, a instituțiilor UE și a întreprinderilor în domeniile în care ar aduce cea mai mare valoare adăugată. Acestea acoperă: sprijin pentru punerea în aplicare a Directivei privind securitatea rețelelor și a informațiilor; elaborarea de politici și punerea lor în aplicare; cunoștințe și sensibilizare în domeniul informațiilor; cercetare; cooperarea operațională și gestionarea crizelor; piața. În special, ENISA ar sprijini politica UE în ceea ce privește certificarea de securitate în domeniul TIC, asigurând întreținerea din punct de vedere administrativ și gestionarea tehnică a unui cadru european de certificare de securitate în domeniul TIC. Un astfel de cadru va pune efectiv în aplicare un set de norme privind guvernanța în materie de certificare de securitate în domeniul TIC în UE, care ar promova un sistem de recunoaștere reciprocă a certificatelor emise în diferitele state membre. Soluția combinării acestor opțiuni este considerată a fi cea mai eficace pentru ca UE să atingă obiectivele identificate: capabilități sporite de securitate cibernetică, pregătire, cooperare, sensibilizare, transparență și evitarea fragmentării pieței. Această opțiune este, de asemenea, cea mai coerentă cu prioritățile de politică, stabilite în Strategia de securitate cibernetică și în politicile conexe (de exemplu Directiva privind securitatea rețelelor și a informațiilor), precum și în Strategia privind piața unică digitală. În plus, această opțiune ar atinge obiectivele printr-o utilizare rezonabilă a resurselor.

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

Deși a obținut noi roluri, „ENISA reformată”ar trebui să rămână o organizație flexibilă. Contribuția financiară necesară din bugetul UE ar fi mai mare decât este în prezent, dar ar rămâne destul redusă față de alte agenții care își desfășoară, de asemenea, activitatea în domenii critice.

Crearea unui cadru european de certificare de securitate în domeniul TIC nu ar presupune costuri inițiale suplimentare pentru sector (inclusiv pentru IMM-uri). Mai degrabă, aceasta ar genera economii semnificative pentru firmele care și-au certificat deja produsele sau doresc să demareze procese de certificare de securitate, ceea ce ar avea efecte benefice asupra competitivității lor la nivel mondial. Pe de altă parte, ar fi implicate anumite angajamente bugetare pentru a se asigura întreținerea cadrului, care ar fi puse la dispoziție în principal prin modelul „ENISA reformată”, în măsura în care este vorba de sarcinile tehnice și de secretariat.

Va exista un impact semnificativ asupra bugetelor și administrațiilor naționale?

Nu. Costurile aferente consolidării ENISA ar putea fi, în cea mai mare parte, cele suportate de la bugetul UE, în timp ce statele membre ar putea în continuare să ofere agenției contribuții financiare voluntare. În ceea ce privește certificarea, principalul impact asupra bugetelor și administrațiilor naționale ar decurge din instituirea unei autorități de certificare, după caz.

Vor exista și alte impacturi semnificative?

Nu.

Proporționalitate

Opțiunea preferată include luarea unor măsuri echilibrate, considerate în totalitate ca fiind necesare pentru a se atinge obiectivele vizate, fără a se impune sarcini excesive pentru părțile interesate relevante. În acest sens, se consideră că prezenta inițiativă respectă principiul proporționalității.

D. ACȚIUNE SUBSECVENTĂ

Când va fi revizuită politica?

Se propune ca prima evaluare să aibă loc la cinci ani de la intrarea în vigoare a instrumentului juridic. Comisia va trimite ulterior Parlamentului European și Consiliului un raport privind evaluarea sa, însoțit, după caz, de o propunere de revizuire. O dată la cinci ani va trebui să se efectueze câte o evaluare.