COMISIA
EUROPEANĂ

Bruxelles, 7.2.2013
SWD(2013) 31 final

DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI

REZUMAT AL EVALUĂRII IMPACTULUI

Care însoţeşte documentul

Propunere de directivă a Parlamentului European şi a Consiliului

privind măsuri de asigurare a unui nivel ridicat de securitate a reţelelor şi a informaţiei în Uniune

{COM(2013) 48 final}
{SWD(2013) 32 final}

DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI

REZUMAT AL EVALUĂRII IMPACTULUI

Care însoțește documentul

Propunere de directivă a Parlamentului European și a Consiliului

privind măsuri de asigurare a unui nivel ridicat de securitate a rețelelor și a informației în Uniune

1. DOMENIU DE APLICARE

Prezenta evaluare a impactului se referă la opțiunile de politică al căror scop este să îmbunătățească securitatea internetului și a altor rețele și sisteme informatice pe care se bazează serviciile ce asigură buna funcționare a societății noastre (de exemplu administrațiile publice, sectoarele financiar și bancar, sectorul energetic, transporturile, sănătatea și anumite servicii de internet care permit derularea unor procese cheie la nivel economic și de societate, precum platformele de comerț electronic și rețelele de socializare). Aceste aspecte sunt reunite sub denumirea securitatea rețelelor și a informației (*Network and Information Security*, NIS).

2. CONTEXT POLITIC

Importanța tot mai mare a securității rețelelor și a informației pentru economiile și societățile noastre a fost recunoscută pentru prima dată de către Comisie în anul 2001. În vederea asigurării unui nivel ridicat și eficace al NIS în Uniune, în 2004 Comunitatea Europeană a luat decizia de a înființa Agenția Europeană pentru Securitatea Rețelelor și a Informației (ENISA). Abordarea pe care Uniunea Europeană a adoptat-o până în prezent în domeniul NIS a constat în principal în adoptarea unei serii de planuri de acțiune și strategii care îndeamnă cu tărie statele membre să-și dezvolte propriile capacități în domeniu și să coopereze în vederea combaterii problemelor de securitate a rețelelor și a informației care au caracter transfrontalier.

A avut loc o consultare a părților interesate cu privire la diferite aspecte ale inițiativei (definirea problemei și opțiuni de abordare a deficiențelor existente) prin:

- o **consultare publică online** privind „Îmbunătățirea securității rețelelor și a informației în UE”, care s-a desfășurat în perioada 23 iulie-15 octombrie 2012. S-au primit în total 169 de răspunsuri prin intermediul instrumentului online, iar Comisia a primit, în scris, alte 10 răspunsuri;
- discuții cu **statele membre** în contextul Forumului european al statelor membre (FESM), în cadrul reuniunilor bilaterale și cu ocazia Conferinței UE privind securitatea cibernetică, organizată de Comisie și de Serviciul european de acțiune externă la 6 iulie 2012;
- discuții cu societăți și asociații din **sectorul privat,** în contextul Parteneriatului european public-privat pentru reziliență (EP3R) și în cadrul reuniunilor bilaterale;
- discuții cu **ENISA și CERT-UE**;
- discuții în contextul **Reuniunii „Agenda digitală” din 2012**.

3. DESCRIEREA PROBLEMEI

3.1. Definirea problemei

Se poate afirma că problema constă într-un ***nivel general insuficient de protecție împotriva incidentelor, riscurilor și amenințărilor la adresa securității rețelelor și a informației care se manifestă în întreaga UE și care subminează buna funcționare a pieței interne***.

Având în vedere faptul că rețelele și sistemele informatice sunt interconectate și dat fiind caracterul mondial al internetului, numeroase incidente de NIS trec dincolo de granițele naționale și afectează funcționarea pieței interne.

Există posibilitatea ca serviciile transfrontaliere să devină indisponibile, să fie suspendate sau întrerupte ca urmare a atentatelor la securitate, precum în cazul atacurilor care au afectat platformele eBay și PayPal. Necesitatea de a se acționa rapid pentru remedierea problemelor și realizarea schimburilor de informații cu privire la incidentele semnificative a fost evidențiată în cazul atacurilor împotriva Diginotar, societatea care emite certificatele internet neerlandeze. Ca urmare a incidentelor din trecut, statele membre încep să introducă propriile lor reglementări. Intervențiile necoordonate în materie de reglementare pot conduce la fragmentare și pot da naștere unor obstacole pe piața internă care, la rândul lor, pot genera costuri de conformare pentru societățile care operează în mai multe state membre, nu doar într-unul singur.

Această problemă afectează toate sectoarele societății și ale economiei (autorități naționale, mediul de afaceri, consumatori). În mod special, o serie de sectoare joacă un rol esențial în furnizarea de servicii-suport esențiale pentru economia și societatea noastră, iar securitatea sistemelor acestora are o importanță deosebită pentru funcționarea pieței interne. Aceste sectoare includ băncile, bursele de valori, generarea, transmisia și distribuția energiei, transportul (aerian, feroviar, maritim), sănătatea, facilitatorii de servicii-cheie de internet și administrațiile publice. Consultarea publică a arătat un sprijin puternic din partea părților interesate în ceea ce privește necesitatea îmbunătățirii securității rețelelor și a informației în aceste sectoare și a luării de măsuri corespunzătoare la nivelul UE.

Dacă nu se adoptă măsuri suplimentare pentru a combate creșterea numărului de incidente, încrederea consumatorilor în serviciile online ar putea avea de suferit, iar acest lucru poate compromite îndeplinirea obiectivelor cuprinse în Agenda digitală.

3.2. Factorii declanșatori ai problemei

Problema definită ia naștere prin acțiunea unor factori diverși.

În primul rând, există o **inegalitate a capacităților la nivel național în întreaga UE**, fapt ce împiedică crearea încrederii între parteneri, condiție prealabilă pentru cooperare și schimbul de informații.

În al doilea rând, **schimbul de informații privind incidentele, riscurile și amenințările este insuficient**. Cele mai multe incidente de NIS rămân nedeclarate și neobservate, în principal din cauza faptului că societățile sunt reticente în a publica astfel de informații, temându-se de repercusiuni la nivelul imaginii sau al responsabilității. Schimbul de informații în cadrul parteneriatelor/platformelor public-privat existente, precum FESM și EP3R, se limitează la sfera bunelor practici.

4. EFICACITATEA MĂSURILOR EXISTENTE

4.1. Lacunele identificate în cadrul de reglementare existent

Normele actuale impun doar societăților de telecomunicații adoptarea de măsuri de gestionare a riscurilor și de raportarea incidentele din sfera NIS. Cu toate acestea, toți actorii a căror activitate se bazează pe rețele și sisteme informatice se confruntă cu riscuri de securitate. Acest lucru conduce la apariția unor condiții de concurență neechitabile, având în vedere că unul și același incident care ar afecta, de exemplu, un furnizor de telecomunicații și o societate furnizoare de servicii de telefonie prin internet (VoIP) ar trebui notificat autorității competente naționale doar în primul caz, nu și în cel de-al doilea.

În conformitate cu dispozițiile cadrului de reglementare privind protecția datelor, toți actorii care sunt operatori de date (de exemplu băncile sau spitalele) au obligația de a institui măsuri de securitate care să fie proporționale cu riscurile existente. Însă operatorii de date au obligația de a notifica numai cazurile de încălcare a securității care compromit datele cu caracter personal.

Directiva 2008/114/CE a Consiliului privind identificarea și desemnarea infrastructurilor critice europene vizează numai sectorul energetic și cel al transportului, iar până în prezent doar câteva dintre aceste infrastructuri au fost identificate ca atare de statele membre. Directiva nu impune operatorilor obligația de a raporta cazurile de atac grav la adresa securității și nu instituie mecanisme care să permită statelor membre să coopereze și să reacționeze la aceste incidente.

În prezent, colegislatorii analizează propunerea de directivă a Comisiei privind atacurile împotriva sistemelor informatice[1]. Această propunere vizează numai incriminarea unor comportamente specifice, fără să abordeze și modalitățile de prevenire a riscurilor și incidentelor din sfera NIS, reacțiile la incidentele de NIS și atenuarea impactului acestora.

4.2. Limitele abordării voluntare

Abordarea voluntară adoptată până în prezent a condus la apariția unui nivel de pregătire inegal și la o cooperare limitată.

FESM are atribuții limitate, dat fiind că statele membre nu schimbă informații cu privire la incidente, riscuri și amenințări și nici nu cooperează în vederea combaterii amenințărilor transfrontaliere. FESM nu are competența necesară pentru a putea impune membrilor săi instituirea unor capacități minime.

ENISA nu are competențe în plan operațional și, de exemplu, nu poate interveni pentru a remedia problemele din sfera NIS.

EP3R nu deține un statut oficial și nu poate impune sectorului privat obligația de a raporta incidentele către autoritățile naționale. La nivelul EP3R nu există un cadru care să permită un schimb de informații securizat și comunicarea de informații cu privire la amenințările, riscurile și incidentele din sfera NIS.

5. NECESITATEA INTERVENȚIEI UE; SUBSIDIARITATE ȘI PROPORȚIONALITATE

Asigurarea securității rețelelor și a informației are o importanță vitală pentru buna funcționare a pieței interne și pentru bunăstarea societății noastre. Articolul 114 din TFUE constituie un temei juridic adecvat pentru armonizarea cerințelor în materie de NIS și introducerea unui nivel minim comun de securitate în întreaga UE.

[1] COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:RO:PDF

Intervenția Uniunii în domeniul NIS este justificată din motive de **subsidiaritate**, datorită naturii transfrontaliere a problemei și faptului că acțiunile întreprinse la nivelul UE ar avea o eficacitate sporită (și, astfel, o valoare adăugată) pentru politicile naționale existente.

Pentru a asigura un cadru de cooperare care să cuprindă toate statele membre, este necesar să se poată garanta faptul că acestea dispun de un nivel minim necesar al capacităților. În plus, este evident că existența unor acțiuni de politică concertate și colaborative în domeniul NIS poate avea un impact puternic și benefic asupra protecției drepturilor fundamentale, în special asupra dreptului la protecția datelor cu caracter personal și a vieții private.

Măsurile din cadrul opțiunii preferate se justifică din motive de **proporționalitate**, având în vedere faptul că cerințele impuse statelor membre sunt stabilite la nivelul minim necesar care să asigure pregătirea adecvată și să permită cooperarea bazată pe încredere, iar cerințele impuse societăților și autorităților publice, și anume gestionarea riscurilor și raportarea incidentelor, vizează numai entitățile de importanță majoră, impun măsuri proporționale cu riscurile și se referă la incidentele cu impact semnificativ. În plus, măsurile din cadrul opțiunii preferate nu ar impune costuri disproporționate.

6. OBIECTIVE

Obiectivul general este mărirea nivelului de protecție împotriva incidentelor, riscurilor și amenințărilor la adresa securității rețelelor și a informației în întreaga UE. Obiectivele specifice sunt următoarele:

- **Obiectivul 1** - instituirea unui nivel minim comun de securitate a rețelelor și a informației în statele membre și creșterea prin urmare a nivelului general de pregătire și reacție;
- **Obiectivul 2** - îmbunătățirea cooperării în domeniul NIS la nivelul UE, cu scopul de a combate cu eficacitate incidentele și amenințările transfrontaliere;
- **Obiectivul 3** - crearea unei culturi a gestionării riscurilor și îmbunătățirea schimbului de informații dintre sectorul public și cel privat.

7. OPȚIUNI DE POLITICĂ

Opțiunile de politică avute în vedere în prezenta evaluare a impactului sunt: statu-quo, abordarea normativă și abordarea mixtă. Posibila opțiune constând în încetarea tuturor activităților UE în domeniul NIS a fost eliminată.

7.1. Opțiunea 1 - Statu-quo („scenariul de bază”)

Comisia, cu sprijinul ENISA, ar continua actuala abordare voluntară, îndemnând statele membre să creeze capacități de securitate a rețelelor și a informației la nivel național (de exemplu organisme CERT, planuri naționale de gestionare a incidentelor cibernetice/de urgență, strategii naționale de securitate cibernetică) și să coopereze la nivelul UE (de exemplu prin intermediul unei rețele de organisme CERT în întreaga Europă și al unui plan european de cooperare/de urgență privind incidentele cibernetice).

7.2. Opțiunea 2 - Abordare normativă

Comisia ar impune tuturor statelor membre obligația de a institui cel puțin un nivel minim al capacităților naționale (organisme CERT, autorități competente, planuri naționale de gestionare a incidentelor cibernetice/de urgență, strategii naționale de securitate cibernetică).

În cadrul acestei opțiuni normative, autoritățile naționale competente și organismele CERT ar urma să facă parte dintr-o **rețea** de cooperare la nivelul UE. În cadrul rețelei, autoritățile și organismele CERT ar face schimb de informații și ar coopera în vederea combaterii

amenințărilor și a incidentelor de NIS, în conformitate cu **Planul european de cooperare/de urgență privind incidentele cibernetice**, asupra căruia statele membre ar trebui să convină.

Societățile (altele decât microîntreprinderile) din sectoare critice specifice, respectiv sectorul bancar, sectorul energetic (electricitate și gaze), transporturile, sănătate, furnizorii de servicii-cheie de internet și administrațiile publice ar fi obligate să evalueze riscurile cu care se confruntă și să adopte măsuri corespunzătoare și proporționale cu dimensiunea riscurilor reale. În plus, aceste entități ar avea obligația de a raporta autorităților competente acele incidente care compromit grav funcționarea rețelelor și a sistemelor informatice proprii și care au, prin urmare, un impact semnificativ asupra continuității serviciilor și a furnizării de bunuri care se bazează pe rețele și sisteme informatice. Această schemă se bazează pe cea prezentată la articolul 13 literele (a) și (b) din Directiva-cadru privind comunicațiile electronice.

7.3. Opțiunea 3 - Abordare mixtă

Comisia ar combina inițiativele voluntare și bunăvoința statelor membre și care ar viza crearea sau consolidarea capacităților statelor membre în domeniul NIS, precum și instituirea unor mecanisme de cooperare la nivelul UE, cu dispoziții normative pentru actorii-cheie din sectorul privat și administrațiile publice.

În esență, inițiativele voluntare ar fi similare celor întreprinse în cadrul opțiunii 1, iar dispozițiile normative ar fi identice cu cele impuse în cadrul opțiunii 2, atât în ceea ce privește entitățile vizate cât și conținutul obligațiilor.

ENISA ar oferi Comisiei, statelor membre și sectorului privat sprijin și asistență tehnică, de exemplu prin emiterea unor orientări și recomandări tehnice.

8. EVALUAREA IMPACTULUI

În plus față de nivelul de securitate, evaluarea vizează impactul economic și social al celor trei opțiuni. Ea acoperă și costurile care ar trebui să fie suportate în cadrul opțiunilor 2 și 3.

Niciuna dintre opțiunile identificate nu va avea vreun impact asupra mediului care să poată fi anticipat cu precizie.

8.1. Opțiunea 1 - Statu-quo („scenariul de bază”)

Nivelul de securitate: Este puțin probabil ca toate statele membre să atingă niveluri comparabile în ceea ce privește capacitățile naționale și gradul de pregătire necesare pentru a îmbunătăți securitatea și pentru a permite cooperarea și schimbul de informații securizate la nivelul UE. Nu s-ar putea asigura condiții de concurență echitabile în ceea ce privește gestionarea riscurilor și creșterea transparenței cu privire la incidente și, prin urmare, ar continua să existe deficiențe legislative.

Impactul economic: Impactul ar depinde de măsura în care statele membre respectă recomandările Comisiei. Nivelul insuficient de securitate din statele membre mai puțin dezvoltate ar compromite competitivitatea și creșterea acestora și le-ar expune la riscuri și incidente. Având în vedere tendințele actuale, incidentele de NIS ar deveni tot mai vizibile pentru mediul de afaceri și consumatori și ar obstrucționa realizarea pieței interne.

Impactul social: Continuarea și agravarea previzibilă a incidentelor, a riscurilor și a amenințărilor ar afecta în mod negativ încrederea cetățenilor în mediul online.

8.2. Opțiunea 2 - Abordare normativă

Nivelul de securitate: Obligațiile impuse statelor membre ar asigura dotarea corespunzătoare a tuturor acestora și ar contribui la crearea unui climat de încredere reciprocă, ceea ce reprezintă o condiție prealabilă pentru o cooperare eficientă la nivelul UE.

Introducerea unor cerințe privind gestionarea riscurilor din sfera NIS pentru administrațiile publice și actorii-cheie din sectorul privat ar constitui un stimulent puternic pentru gestionarea și evaluarea eficientă a riscurilor de securitate. Costurile suplimentare totale care ar trebui să fie suportate de către toate sectoarele UE pentru îndeplinirea acestor cerințe s-ar situa **între 1 și 2 miliarde EUR**. Costul punerii în conformitate a **întreprinderilor mici și mijlocii** s-ar situa între **2 500 și 5 000 de euro per întreprindere**.

Impactul economic: Ca urmare a nivelului crescut de securitate, s-ar reduce pierderile financiare asociate riscurilor și incidentelor din sfera NIS. Ar spori încrederea mediului de afaceri și a consumatorilor în lumea digitală, iar acest lucru ar aduce beneficii la nivelul pieței interne. De asemenea, promovarea unei culturi avansate în domeniul gestionării riscurilor ar stimula cererea de produse și soluții TIC securizate.

Impactul social: Un nivel sporit de securitate ar crește încrederea cetățenilor în mediul online, iar aceștia ar putea să profite pe deplin de beneficiile lumii digitale (de exemplu platformele de comunicare socială, eLearning sau eHealth).

8.3. Opțiunea 3 - Abordare mixtă

Nivelul de securitate: La fel ca în cazul opțiunii 1, nu există nicio garanție că nivelul de securitate bazat pe capacitățile naționale în domeniul NIS și cooperarea la nivelul UE s-ar îmbunătăți ca urmare a inițiativelor voluntare. Pe de altă parte, introducerea unor cerințe de securitate pentru administrațiile publice și actorii-cheie din sectorul privat ar crea un stimulent puternic în ceea ce privește gestionarea și măsurarea riscurilor de securitate. Aceste mecanisme ar fi însă ineficiente în acele state membre care nu vor respecta recomandările Comisiei privind instituirea unor capacități în domeniul NIS.

Impactul economic: Ritmul dezvoltării ar varia în mod semnificativ de la un stat membru la altul. Nivelul de securitate insuficient din statele membre mai puțin dezvoltate ar submina competitivitatea și creșterea acestora și le-ar expune la impactul negativ al riscurilor și al incidentelor.

Impactul social: Continuarea și agravarea previzibilă a incidentelor, riscurilor și amenințărilor ar afecta în mod negativ încrederea cetățenilor în mediul online, în special în statele membre pentru care domeniul securității rețelelor și a informației nu reprezintă o prioritate.

9. COMPARAREA OPțIUNILOR

Opțiunile 1 și 3 nu sunt considerate a fi modalități viabile de îndeplinire a obiectivelor de politică și, prin urmare, nu sunt recomandate, dat fiind că eficacitatea acestora ar depinde de măsura în care abordarea voluntară ar putea să genereze sau nu un nivel minim de securitate a rețelelor și a informației; în ceea ce privește opțiunea 3, aceasta ar depinde de bunăvoința statelor membre de a institui capacități și de a coopera la nivel transfrontalier.

Opțiunea 2 este cea preferată, dat fiind că oferă un cadru în care s-ar îmbunătăți în mod considerabil protecția consumatorilor, a societăților și a administrațiilor naționale din UE împotriva incidentelor, amenințărilor și riscurilor din sfera NIS. În plus, făcând ordine pe plan intern, UE și-ar putea lărgi anvergura internațională și ar putea deveni un partener chiar mai credibil pentru cooperarea la nivel bilateral și multilateral. Prin urmare, ea s-ar găsi totodată într-o poziție mai bună pentru a promova drepturile fundamentale și valorile esențiale ale UE în afara granițelor sale.

10. MONITORIZARE ȘI EVALUARE

Capitolul 10 din raportul de evaluare a impactului prezintă o serie de indicatori de bază ai progreselor făcute în direcția atingerii obiectivelor. Acești indicatori includ, spre exemplu:

- pentru obiectivul 1, numărul de state membre care au desemnat o autoritate competentă în domeniul NIS și un organism CERT sau care au adoptat o strategie națională de securitate cibernetică și un plan național de cooperare/de urgență privind incidentele cibernetice;
- pentru obiectivul 2, numărul de autorități competente și echipe CERT din statele membre care participă la rețea și volumul informațiilor schimbate în cadrul rețelei cu privire la riscurile și incidentele de NIS;
  pentru obiectivul 3, nivelul investițiilor în securitatea rețelelor și a informației efectuate de către actorii-cheie din sectorul privat și administrațiile publice și numărul notificărilor de incidente de NIS cu impact semnificativ.