I

(Rezoluții, recomandări și avize)

REZOLUȚII

CONSILIU

REZOLUȚIA CONSILIULUI

din 18 decembrie 2009

privind o abordare europeană a securității rețelelor și a informațiilor bazată pe colaborare

(2009/C 321/01)

CONSILIUL UNIUNII EUROPENE,

I. AVÂND ÎN VEDERE:

1. Comunicarea Comisiei din 31 mai 2006 privind „Strategia pentru o societate informațională sigură" care propune un proces de „dialog, parteneriat și responsabilizare" care să angajeze statele membre și părțile implicate din domeniul privat;

2. Comunicarea Comisiei din 12 decembrie 2006 privind „Programul european de protecție a infrastructurilor critice (EPCIP)" menit să îmbunătățească protecția infrastructurilor critice din UE și să creeze un cadru UE de protecție a infrastructurilor critice;

3. Directiva Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora;

4. Rezoluția Consiliului din 22 martie 2007 cu privire la o strategie pentru o societate informațională sigură în Europa;

5. Concluziile Consiliului din 19-20 aprilie 2007 privind Programul european pentru protecția infrastructurilor critice;

6. Comunicarea Comisiei din 30 martie 2009 privind protecția infrastructurilor critice de informație (CIIP);

7. Dezbaterea în curs și consultarea publică din cadrul acesteia privind viitorul Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) și rolul acesteia în CIIP;

8. Concluziile Președinției privind CIIP în urma conferinței ministeriale de la Tallinn din perioada 27-28 aprilie 2009;

9. Obiectivele de la Lisabona de competitivitate și creștere economică și lucrările de revizuire a strategiei de la Lisabona aflate în curs de desfășurare;

10. Măsurile de securitate propuse odată cu revizuirea cadrului de reglementare pentru rețele și servicii de comunicații electronice;

11. Pentru a asigura eficiența viitoarei politici în domeniul securității informațiilor și a rețelelor, prezenta rezoluție pleacă de la premisa că nu s-a ajuns la nicio concluzie referitoare la eventualele modificări necesare la regulamentul ENISA. Având în vedere că viitorul politicii în domeniul securității rețelelor și a informațiilor se află în curs de examinare la Comisie, prezenta rezoluție nu ar trebui să aducă atingere rezultatelor acestei examinări cu privire la eventuale modificări la regulamentul ENISA, înainte de publicarea rezultatelor examinării de către Comisie.

II. CONSTATÂND CĂ:

1. Având în vedere importanța comunicațiilor, a infrastructurilor și a serviciilor electronice, care constituie baza activității economice și sociale, securitatea rețelelor și a informațiilor (NIS) își aduce contribuția la unele valori și obiective importante ale societății, precum democrația, confidențialitatea, creșterea economică, libera circulație a ideilor și stabilitatea economică și politică;

2. Sistemele tehnologice, infrastructurile și serviciile de informații și comunicații, inclusiv internetul, joacă un rol vital în societate, iar perturbarea acestora poate cauza daune economice imense, subliniind astfel importanța măsurilor de sporire a protecției și rezilienței, menite să asigure continuitatea serviciilor critice;

3. Riscurile de producere a unor incidente de securitate reduc gradul de încredere al utilizatorilor. În timp ce perturbările grave ale rețelelor și sistemelor de informații ar putea avea un impact economic și social major, problemele și neplăcerile de zi cu zi prezintă, de asemenea riscul de a eroda încrederea publicului în tehnologie, rețele și servicii;

4. Amenințările cresc în amploare și în diversitate, ceea ce dă naștere unei nevoi de a oferi utilizatorilor finali, operatorilor economici și guvernelor infrastructuri de comunicații electronice robuste și reziliente în mod implicit și de a identifica stimulentele corecte pentru ca furnizorii să realizeze aceste obiective în timp util;

5. Există nevoia de a îmbunătăți securitatea rețelelor și a informațiilor și de a o integra în toate domeniile de politică și în toate sectoarele societății și de a aborda provocarea asigurării unor competențe suficiente, prin acțiuni atât la nivel național, cât și european, precum și de a ridica nivelul de conștientizare în rândul utilizatorilor tehnologiei informației și a comunicațiilor (TIC);

6. Finalizarea și funcționarea pieței interne va necesita o cooperare transfrontalieră între proprietarii de rețele și furnizorii de servicii, ținând seama de faptul că posibilele incidente cu efect perturbator pot avea repercusiuni și asupra altor state membre, precum și a UE în ansamblul său;

7. Noile modele de utilizare, precum informatica dematerializată („cloud computing") și software-ul furnizat ca serviciu subliniază și mai mult importanța securității rețelelor și a informațiilor;

8. Securitatea rețelelor și a informațiilor ajută la îndeplinirea obiectivului tuturor părților, din toate sectoarele societății, de a putea acorda încredere sistemelor de informații, motiv pentru care este necesară o abordare transsectorială și transfrontalieră;

9. Odată cu creșterea gradului de utilizare a TIC în societate, securitatea rețelelor și a informațiilor devine o condiție obligatorie pentru furnizarea unor servicii publice de încredere, sigure și în securizate, precum cele de e-guvernare;

10. ENISA deține potențialul de a își consolida rolul important pe care îl joacă în securitatea rețelelor și a informațiilor.

III. SUBLINIAZĂ CĂ:

1. Un nivel ridicat de securitate a rețelelor și a informațiilor în UE este necesar pentru a sprijini:

   (a) libertățile și drepturile cetățenilor, inclusiv dreptul la confidențialitate;

   (b) societate eficientă din punct de vedere al gestionării informațiilor;

   (c) profitabilitatea și creșterea comerțului și a industriei;

   (d) încrederea cetățenilor și a organizațiilor în sistemele de gestionare a informațiilor și în sistemele TIC;

2. Sectorul TIC este vital pentru majoritatea sectoarelor societății, securitatea rețelelor și a informațiilor fiind din acest motiv o responsabilitate comună a tuturor părților implicate, inclusiv a operatorilor, a furnizorilor de servicii, a furnizorilor de hardware și de software, a utilizatorilor finali, a organismelor publice și a guvernelor naționale.

IV. RECUNOAȘTE:

1. Importanța unei comunități europene active și informate în domeniul securității rețelelor și a informațiilor care să contribuie la intensificarea colaborării dintre statele membre și sectorul privat;

2. Avantajele unei utilizări armonizate, acolo unde este cazul, a standardelor internaționale de securitate în întreaga UE în domeniul securității rețelelor și a informațiilor;

3. Necesitatea unei abordări europene a securității rețelelor și a informațiilor bazate pe colaborare la nivel internațional, deoarece aceasta reprezintă o provocare globală;

4. Importanța disponibilității pentru statele membre și instituțiile europene a unor date statistice fiabile privind securitatea rețelelor și a informațiilor în Europa;

5. Necesitatea sporirii conștientizării și a unor instrumente de gestionare a riscului pentru toate părțile implicate;

6. Importanța intensificării eforturilor statelor membre de a ridica gradul de conștientizare, de a efectua schimburi de bune practici și de a oferi îndrumare statelor membre;

7. Importanța modelelor multipartite, precum parteneriatele public-privat (PPP), constituite pe termen lung, piramidale, menite să atenueze riscurile identificate, în condițiile în care această abordare produce valoare adăugată în sprijinul asigurării unui nivel înalt de reziliență a rețelelor;

8. Rolul vital deținut de furnizori în a furniza societății infrastructuri de comunicații electronice robuste și reziliente;

9. Utilitatea exercițiilor europene în domeniul securității rețelelor și a informațiilor, care pot reprezenta oportunități de a desprinde concluzii valoroase pentru operatorii de rețele și furnizorii de servicii, cât și pentru guverne;

10. Echipele naționale sau guvernamentale de intervenție în caz de urgență în domeniul IT (CERT) sau alte mecanisme care să răspundă sau să trateze vulnerabilitățile pot contribui la sporirea nivelului de reziliență și a capacității de a face față perturbărilor rețelelor și sistemelor de informații și de a le remedia;

11. Importanța explorării efectelor strategice, a riscurilor și a perspectivelor legate de înființarea CERT pentru instituțiile UE și luarea în calcul a posibilului rol al ENISA în viitor sub acest aspect;

12. Lucrările întreprinse de ENISA în domeniul securității rețelelor și a informațiilor până în prezent și necesitatea de a continua dezvoltarea acesteia, astfel încât să devină un organism eficient care să aducă beneficii clare în domeniul securității rețelelor și a informațiilor în Europa.

V. REAFIRMĂ CĂ:

1. O strategie europeană îmbunătățită și exhaustivă în ceea ce privește securitatea rețelelor și a informațiilor, în care să fie clar precizate rolurile Comisiei, ale statelor membre și ale ENISA, prezintă o importanță vitală în abordarea provocărilor actuale și viitoare;

2. În urma unor consultări și a unei analize adecvate, ar trebui să se examineze, în procesul legislativ, posibilitatea de a moderniza și de a consolida ENISA, printr-un mandat care să asigure flexibilitatea și capacitatea de supraveghere de către statele membre, precum și un rol eficient al reprezentării părților implicate din sectorul privat. Mandatul acesteia ar trebui să țină seama de cadrul de reglementare pentru rețele și servicii de comunicații electronice și să corespundă ambițiilor prezentate în Agenda de la Lisabona, precum și să înglobeze obiective legate de cercetare, inovare, competitivitate, creștere economică și asigurarea încrederii;

3. ENISA ar putea sprijini elaborarea politicii și a rolurilor de punere în aplicare corespunzătoare Comisiei și respectiv statelor membre, în special prin remedierea disparităților dintre tehnologie și politică și ar trebui să colaboreze strâns cu statele membre și cu alte părți implicate în vederea asigurării alinierii activităților sale la prioritățile UE;

4. ENISA, prin mandatul revizuit, ar trebui să servească drept centru de expertiză al UE pe probleme de securitate a rețelelor și a informațiilor la nivelul UE. Ca atare, instituțiile europene ar trebui să solicite avizul agenției și să țină seama pe deplin de acesta în procesul de elaborare și de punere în aplicare a politicilor cu potențial impact în acest domeniu;

5. ENISA ar putea, de asemenea, să aibă capacitatea de a acorda, la cerere, asistență statelor membre în vederea îmbunătățirii capacităților acestora în domeniul securității rețelelor și a informațiilor și a capacității acestora de a face față la incidentele de securitate.

VI. INVITĂ STATELE MEMBRE:

1. Să continue lucrările de sporire a gradului de încredere a utilizatorilor finali în TIC prin campanii de conștientizare;

2. Să organizeze exerciții naționale și/sau să participe la exerciții europene periodice în domeniul securității rețelelor și a informațiilor, ținând seama de necesitatea unei planificări minuțioase datorate complexității domeniului și implicării sectorului privat. ENISA ar putea, la cerere, să acorde asistență statelor membre în această privință. Domeniul de aplicare și dimensiunea geografică a exercițiilor ar trebui să evolueze în mod firesc în timp și ar trebui să se bazeze pe riscuri recunoscute;

3. Să creeze echipe de intervenție în caz de urgență în domeniul IT (CERT) în statele membre care nu au dezvoltat încă această capacitate și să consolideze cooperarea între CERT naționale la nivel european. ENISA ar putea să acorde asistență statelor membre în această privință;

4. Să intensifice eforturile legate de programele de educație, formare și cercetare în domeniul securității rețelelor și a informațiilor pentru a asigura disponibilitatea în UE a competențelor tehnice și a specialiștilor, precum și pentru a ridica nivelul de profesionalism al specialiștilor în acest domeniu;

5. Să aibă o reacție comună în cazul unui incident transfrontalier și să consolideze capacitatea de a reacționa corespunzător, ceea ce necesită consolidarea dialogului dintre factorii de decizie implicați, în special cu privire la aspecte legate de confidențialitate.

VII. INVITĂ COMISIA:

1. Să sprijine statele membre, după caz, la punerea în aplicare a prezentei rezoluții;

2. Să informeze periodic Parlamentul European și Consiliul privind inițiativele la nivelul UE legate de securitatea rețelelor și a informațiilor;

3. În colaborare cu ENISA, să inițieze o campanie de conștientizare în rândul actorilor publici și privați europeni cu privire la importanța unei gestionări adecvate a riscului în ceea se privește securitatea rețelelor și a informațiilor;

4. Să continue, în colaborare cu statele membre, procesul de identificare a stimulentelor pentru ca furnizorii de infrastructuri de comunicații electronice să furnizeze în mod implicit utilizatorilor finali, operatorilor economici și guvernelor infrastructuri robuste și reziliente;

5. În colaborare cu statele membre, să elaboreze metode care să permită realizarea unei evaluări comparabile la nivelul UE privind impactul socioeconomic al incidentelor și eficiența măsurilor preventive;

6. Să încurajeze și să îmbunătățească modelele multiparite, care să aducă o valoare adăugată clară în ceea ce privește beneficiile pentru utilizatorii finali și industrie;

7. Să propună o strategie globală privind securitatea rețelelor și a informațiilor, [1] inclusiv prin prezentarea unor propuneri privind un mandat consolidat și flexibil pentru ENISA, precum și o capacitate de supraveghere sporită pentru statele membre și Comisie;

8. Să realizeze o analiză, în colaborare cu statele membre, privind echipele de intervenție în caz de urgență în domeniul IT (CERT) pentru a identifica domeniile în care este necesară o colaborare mai strânsă;

9. Să continue explorările pentru a identifica o abordare comună a achizițiilor de sisteme și servicii TIC securizate, sau care să asigure interoperabilitatea, pentru toate instituțiile UE.

VIII. INVITĂ ENISA:

1. Să continue acordarea de sprijin activ statelor membre, Comisiei Europene și altor părți implicate relevante, la punerea în aplicare a politicilor europene în domeniul securității rețelelor și a informațiilor și a planului de acțiune privind CIIP;

2. Să colaboreze cu statele membre, cu Comisia și cu organismele statistice pentru a elabora un cadru de date statistice privind securitatea rețelelor și a informațiilor în Europa.

IX. INVITĂ PĂRȚILE IMPLICATE:

1. Să intensifice eforturile de îmbunătățire a nivelului de securitate a rețelelor și a informațiilor, în special în ceea ce privește furnizarea unor produse și servicii solide, fiabile și ușor de utilizat;

2. Să informeze utilizatorii în privința riscurilor de securitate asociate produselor și a modului în care se pot proteja;

3. Să ia toate măsurile tehnice și organizaționale pentru a garanta continuitatea, integritatea și confidențialitatea serviciilor și rețelelor de comunicații electronice;

4. Să continue lucrările la standardizarea securității rețelelor și a informațiilor și să facă eforturi în vederea identificării unor soluții armonizate, care să asigure interoperabilitatea;

5. Să participe împreună cu statele membre la exerciții pentru a asigura un răspuns adecvat în caz de urgențe.

[1] Comisia propune introducerea în acest loc a cuvântului „posibil”.