COMISIA EUROPEANĂ

Bruxelles, 10.01.2017
C(2017) 8 final

Dlui Liviu Dragnea
Președintele
Camerei Deputaților
Palatul Parlamentului
Str. Izvor nr. 2-4, Sector 5
RO – 050563 BUCUREȘTI

Stimate Domnule Președinte,

Comisia mulțumește Camerei Deputaților pentru opinia sa privind Comunicarea intitulată „Consolidarea sistemului de reziliență cibernetică al Europei și încurajarea unui sector al securității cibernetice competitiv și inovator" {COM(2016) 410 final}.

Comisia ia act cu satisfacție de acordul exprimat de Camera Deputaților față de punctul său de vedere potrivit căruia este necesară o acțiune la nivelul Uniunii pentru a consolida sistemul de reziliență cibernetică al Europei și pentru a încuraja un sector al securității cibernetice competitiv și inovator. În lipsa încrederii și a securității, nu poate exista o piață unică digitală. Europa trebuie să fie pregătită să gestioneze atacuri cibernetice care sunt tot mai sofisticate și nu țin seama de granițele naționale.

În acest context, Comisia își propune, prin această comunicare, să consolideze cooperarea transfrontalieră, angrenând toți actorii și toate sectoarele active în domeniul securității cibernetice și să contribuie la dezvoltarea de tehnologii, produse și servicii novatoare și sigure pe întreg teritoriul Uniunii Europene. Planul de acțiune descris în comunicare trebuie raportat la contextul Strategiei privind piața unică digitală[1], prezentată în 2015, și al Strategiei de securitate cibernetică a UE[2], prezentată în 2013, precum și al celor două directive privind securitatea rețelelor și a sistemelor informatice (NIS) și, respectiv, atacurile împotriva sistemelor informatice[3] (AAIS).

Recunoscând necesitatea imperioasă de a realiza progrese pentru a răspunde la evoluția rapidă a provocărilor în materie de securitate cibernetică, Comisia a început deja să pună în practică o serie de inițiative prezentate în comunicare. La 5 iulie 2016 a fost semnat la Strasbourg Acordul privind un parteneriat contractual public-privat privind securitatea

1 COM(2015)/0192 final.
2 JOIN(2013) 1 final.
3 Directiva (UE) 2016/1148 și Directiva 2013/40/UE.

cibernetică (PPPc). Structura sa de guvernanță, precum și o serie de grupuri de lucru, au fost deja instituite.

De asemenea, Comisia a demarat deja consultări cu statele membre și cu alte părți interesate asupra posibilității de a crea un sistem de certificare și de etichetare pentru produsele și soluțiile de securitate din domeniul tehnologiei informației și comunicațiilor (TIC) în Europa. Totodată, au fost deja inițiate lucrările pregătitoare în vederea evaluării mandatului Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA).

Comisia intenționează să informeze cu regularitate statele membre în legătură cu progresele realizate în ceea ce privește diversele activități anunțate în comunicare. Ca răspuns la observațiile de natură mai tehnică formulate în opinia Camerei Deputaților, Comisia ar dori să facă trimitere la anexa atașată.

Comisia speră că aceste observații răspund preocupărilor exprimate de Camera Deputaților și așteaptă cu interes continuarea dialogului politic în viitor.

Cu deosebită considerație,

Frans Timmermans
Prim-vicepreședinte

Andrus Ansip
Vicepreședinte

ANEXĂ

Comisia are plăcerea de a oferi informații suplimentare, grupate pe teme, în legătură cu chestiunile aduse în discuție de Camera Deputaților în opinia sa.

Capacitățile industriale în domeniul securității cibernetice în UE și posibilitățile oferite IMM-urilor

Comisia împărtășește punctele de vedere ale Camerei Deputaților privind dependența UE de un număr restrâns de furnizori de sisteme de operare și programe de calculator. Comisia consideră că, deși Europa nu poate deține controlul întregului lanț valoric al tehnologiilor digitale, este necesar să mențină și să dezvolte cel puțin anumite capacități esențiale pentru siguranța funcționării acestor tehnologii atunci când sunt utilizate în cadrul infrastructurilor critice europene. În acest context, furnizarea de produse și servicii care asigură cel mai ridicat nivel de securitate cibernetică reprezintă o oportunitate pentru sectorul securității cibernetice în Europa și ar putea deveni un puternic avantaj competitiv.

Pentru ca Europa să profite de această oportunitate, este necesar să se încurajeze un climat de încredere și cooperare între cererea și oferta de produse și soluții de securitate cibernetică, precum și să se sprijine într-un mod mai susținut noile întreprinderi inovatoare (start-upuri) și noile microîntreprinderi care își desfășoară activitatea în acest domeniu. Comisia își exprimă satisfacția cu privire la faptul că întreprinderile mici și mijlocii (IMM-urile) sunt bine reprezentate în cadrul Organizației Europene pentru Securitate Cibernetică, semnatară a parteneriatului contractual public-privat. Asociația a fost primită cu interes și de către actorii din domeniul securității cibernetice din 27 de țări, inclusiv România, ceea ce asigură o distribuție geografică a activităților sale.

Comisia se angajează să colaboreze îndeaproape cu regiunile, în vederea dezvoltării de platforme specializate inteligente, precum și cu Banca Europeană de Investiții și cu Fondul European de Investiții, pentru a examina posibilitățile de facilitare a accesului la finanțare al IMM-urilor care desfășoară activități în domeniul securității cibernetice.

Certificare și etichetare

Comisia ia notă cu atenția cuvenită de punctele de vedere exprimate de Camera Deputaților cu privire la certificarea și etichetarea produselor și serviciilor de securitate din domeniul TIC. Comisia a demarat deja consultări cu statele membre și cu alte părți interesate pentru a elabora o foaie de parcurs care să analizeze posibilitatea de a crea un cadru european de certificare pentru produsele și soluțiile de securitate din domeniul TIC. Opinia Camerei Deputaților le va fi transmisă reprezentanților Comisiei și altor părți interesate implicate în proces, pentru a alimenta aceste discuții. Această inițiativă completează eforturile depuse de Comisie pentru a elabora și a standardiza cerințele de securitate în domeniul internetului obiectelor, al tehnologiilor 5G și al serviciilor de cloud computing.

Sensibilizarea opiniei publice cu privire la securitatea cibernetică

Comisia împărtășește punctul de vedere al Camerei Deputaților potrivit căruia sensibilizarea opiniei publice în legătură cu amenințările la adresa securității cibernetice și dezvoltarea unui comportament preventiv sunt elemente importante pentru îmbunătățirea rezilienței Europei în materie de securitate cibernetică.

Comisia ar dori să atragă atenția Camerei Deputaților asupra Lunii europene a securității cibernetice, campania anuală de promovare desfășurată de UE, organizată de Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor și susținută de Comisie, care are loc anual în octombrie și vizează sensibilizarea cetățenilor față de amenințările la adresa securității cibernetice, promovarea securității cibernetice în rândul cetățenilor și furnizarea de informații la zi privind securitatea, prin intermediul educației și al schimbului de bune practici. Comisia încurajează toate statele membre să ia parte în mod activ la Luna europeană a securității cibernetice și să utilizeze materialele acestei campanii și cu alte ocazii. În urma ediției din 2016 au fost organizate peste 440 de activități de sensibilizare în 31 de țări, inclusiv România.

În plus, Comisia ar dori să evidențieze în general finanțarea pe care o acordă proiectelor de sensibilizare, de exemplu în domeniile securității cibernetice și al protecției datelor electronice.

Pe lângă acestea, Comisia sprijină activitatea centrelor de excelență pentru combaterea criminalității cibernetice, care au fost înființate în întreaga UE cu scopul de a favoriza legătura dintre mediul academic și serviciile de aplicare a legii.

Prostituția infantilă, tratamentul violent al copiilor, hărțuirea pe internet și terorismul

Comisia împărtășește punctul de vedere al Camerei Deputaților potrivit căruia există conexiuni între securitatea cibernetică, atacurile asupra conturilor bancare și finanțarea terorismului. În acest context, există o mare nevoie de coordonare și încurajare a schimbului de informații între toți factorii implicați, inclusiv sectorul financiar, centrele de răspuns la incidente de securitate cibernetică (CERT) și autoritățile de asigurare a respectării legii, în scopul prevenirii, atenuării, cercetării și urmăririi penale a atacurilor cibernetice respective.

De asemenea, Comisia împărtășește punctul de vedere al Camerei Deputaților potrivit căruia orice abuzuri sexuale împotriva copiilor, în special atunci când sunt comise cu utilizarea computerelor, trebuie abordate în mod distinct și cuprinzător în cadrul luptei împotriva criminalității cibernetice. Prevenirea acestor abuzuri trebuie să fie o prioritate pentru societatea noastră. Există o legătură puternică între securitatea cibernetică și măsurile eficace de asigurare a respectării legii în vederea combaterii abuzurilor sexuale asupra copiilor. La rândul lor, părțile interesate joacă un rol esențial, de exemplu prin punerea la dispoziție a unui număr mai mare de linii telefonice de urgență care dispun de un personal special calificat, prin îmbunătățirea competențelor anchetatorilor penali sau prin implicarea voluntară a furnizorilor de servicii de internet. Comisia încurajează activitatea acestor părți interesate, oferind oportunități de schimb direct și de finanțare a proiectelor. Orice discuție pe marginea acestui subiect trebuie să țină seama, de asemenea, că este esențial nu doar să

se faciliteze anchetarea efectivă a acestor infracțiuni, ci și să se ia toate măsurile necesare pentru identificarea și protejarea victimelor.

Directiva din 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile[4] *prevede că lupta împotriva acestor infracțiuni trebuie să se înscrie într-o abordare integrată și cuprinzătoare, care să cuprindă cercetarea și urmărirea penală a infracțiunilor, sprijinirea și protecția victimelor, precum și prevenirea.*

Comisia este de acord cu punctul de vedere al Camerei Deputaților potrivit căruia internetul poate contribui la extinderea criminalității, inclusiv prin procurarea de arme în scopuri teroriste, și că este necesar să se consolideze în continuare cooperarea internațională. Prin urmare, Comisia sprijină consolidarea unor capacități care să permită realizarea de anchete eficace asupra infracțiunilor tradiționale comise online sau cu utilizarea internetului.

Alături de infracțiunile tradiționale, atacurile cibernetice constituie un nou tip de infracțiuni, de sine stătător și în plină răspândire. La nivelul UE, această amenințare a fost abordată prin Directiva privind atacurile împotriva sistemelor informatice, care prevede definiții comune și standarde minime pentru angajarea răspunderii penale a persoanelor implicate în atacuri cibernetice. Directiva vizează în mod expres atacurile împotriva sistemelor de infrastructuri critice, precum și fraudarea online a identității și utilizarea de botneturi. De asemenea, directiva impune statelor membre să înființeze puncte de contact disponibile 24 de ore din 24, 7 zile din 7 și să faciliteze astfel cooperarea efectivă în cadrul anchetelor la nivel internațional.

Amenințările hibride

Comisia este de acord cu aprecierea Camerei Deputaților potrivit căreia atacurile cibernetice pot face parte din „amenințări hibride" mai ample, care presupun o combinație de metode convenționale și neconvenționale utilizate într-un mod coordonat de actori statali și nestatali, rămânând însă sub limita pragului de stare de război declarată oficial. Obiectivul acestui tip de acțiuni nu este doar de a cauza un prejudiciu direct și a exploata vulnerabilitățile, ci și de a destabiliza societățile și a crea ambiguitate în vederea obstrucționării procesului decizional.

Contracararea amenințărilor hibride ține, în mare parte, de competența națională, întrucât răspunderea pentru securitatea națională le revine în primul rând statelor membre. Cu toate acestea, Comisia ar dori să atragă atenția Camerei Deputaților asupra comunicării comune[5] *recent adoptate care stabilește un cadru privind contracararea amenințărilor hibride, ce își propune să ajute statele membre ale UE și țările partenere să contracareze amenințările hibride și să îmbunătățească reziliența, prin corelarea instrumentelor europene și naționale într-un mod mai eficace decât în trecut.*

---

[4] Directiva (UE) 2011/93.

[5] JOIN(2016) 18 final http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52016JC0018.

Raportarea incidentelor

Comisia este de acord cu punctul de vedere exprimat de Camera Deputaților potrivit căruia raportarea incidentelor este unul dintre elementele-cheie ale consolidării rezilienței cibernetice în Europa.

Directiva privind securitatea rețelelor și a informațiilor (Directiva NIS), care a fost recent adoptată și constituie primul act legislativ al UE privind securitatea cibernetică, stabilește cerințe de securitate și obligațiile privind notificarea incidentelor care le revin operatorilor de servicii esențiale, precum și anumitor furnizori de servicii digitale. Deși rămâne de competența statelor membre să structureze raportarea incidentelor, Comisia speră că se va stabili o cooperare fructuoasă între echipele de intervenție în caz de incidente de securitate informatică în cadrul rețelei CSIRT instituite prin Directiva NIS. Activitatea desfășurată în cadrul Programului de lucru privind telecomunicațiile prevăzut de Mecanismul pentru interconectarea Europei în ceea ce privește infrastructurile de servicii digitale de securitate cibernetică poate contribui la dezvoltarea și implementarea de instrumente comune de gestionare a incidentelor în materie de securitate cibernetică.

Comisia se angajează totodată să sprijine inițiative dinspre bază înspre vârf, precum centrele sectoriale de schimb și analiză de informații, pentru a încuraja schimburile de informații între actori industriali omologi care pot contribui la creșterea rezilienței cibernetice din diferite sectoare.