PROVOCĂRI ACTUALE ÎN DOMENIUL SECURITĂȚII CIBERNETICE - IMPACT ȘI CONTRIBUȚIA ROMÂNIEI ÎN DOMENIU

Mediul cibernetic, aflat în plină evoluție, generează deopotrivă oportunități de dezvoltare a societății informaționale, dar și riscuri la adresa funcționării acesteia. Existența vulnerabilităților sistemelor informatice, ce pot fi exploatate de grupări organizate, face ca asigurarea securității spațiului cibernetic să constituie o preocupare majoră pentru toate entitățile implicate.

La nivel european au fost întreprinse demersuri pentru a adopta noi politici privind lupta împotriva criminalității informatice și asigurarea securității cibernetice. *Strategia de securitate cibernetică a Uniunii Europene*, adoptată în 2013, stabilește obiective strategice și acțiuni concrete menite să permită obținerea rezilienței, reducerea criminalității cibernetice, dezvoltarea capabilităților de apărare cibernetică și stabilirea unei politici internaționale în ceea ce privește spațiul cibernetic. Strategia Uniunii Europene, precum și strategiile naționale adoptate, reflectă necesitatea unei abordări unitare a domeniului securității cibernetice, nevoia de colaborare, divulgare și actualizare continuă a politicilor și mecanismelor în vederea asigurării siguranței spațiului cibernetic european.

La 6 iulie 2016, Parlamentul European și Consiliul Uniunii Europene a adoptat *Directiva (UE) 1148/2016 (NIS)* privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice. Scopul acestei Directive este de a asigura un nivel comun de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană și cere operatorilor, respectiv furnizorilor de servicii digitale, să adopte măsuri adecvate pentru prevenirea atacurilor cibernetice și managementul riscului și să raporteze incidentele grave de securitate către autoritățile naționale competente.

Un aspect important al securității la nivelul UE este reprezentat de protecția datelor cu caracter personal. În acest sens, Parlamentul European și Consiliul Uniunii Europene au adoptat în data de 27 aprilie 2016 *Regulamentul (UE) 2016/679* privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor). Regulamentul (UE) 2016/679 a intrat în vigoare pe 25 mai 2016, iar prevederile lui vor fi aplicabile în toate statele membre UE, având caracter obligatoriu începând cu data de 25 mai 2018.

La nivel național a fost adoptată *Strategia de securitate cibernetică a României* în anul 2013, cu scopul de a defini și a menține un mediu cibernetic sigur, cu un înalt grad de siguranță și de încredere. Această strategie își propune adaptarea cadrului normativ și instituțional la dinamica amenințărilor mediului virtual, stabilirea și aplicarea unor cerințe minimale de securitate pentru infrastructurile cibernetice naționale, asigurarea rezilienței acestora și dezvoltarea cooperării în plan național și internațional.

Pe 3 octombrie 2017, Ministerul Comunicațiilor și Societății Informaționale a lansat în dezbatere publică *Proiectul de Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*. Acest proiect de act propune adoptarea unui set de norme menite să instituie un cadru național unitar de asigurare a securității cibernetice și a răspunsului la incidentele de securitate survenite la nivelul rețelelor și sistemelor informatice ale operatorilor de

servicii esențiale și ale furnizorilor de servicii digitale în conformitate cu cerințele Directivei NIS. Pentru implementarea directivei NIS, România are obligația de a institui autorități naționale competente, puncte unice de contact și echipe de intervenție în caz de incidente de securitate cibernetică, precum și să se stabilească cerințele de securitate și de notificare a incidentelor care se aplică operatorilor de servicii esențiale și furnizorilor de servicii digitale.

Adoptarea unei legislații comprehensive și actualizate în domeniul securității cibernetice, care să sprijine dezvoltarea capacităților de apărare ale statului, reprezintă o prioritate națională. Asigurarea unui spațiu cibernetic sigur este responsabilitatea atât a statului, cât și a autorităților competente, a sectorului privat și a societății civile. Pentru dezvoltarea culturii de securitate cibernetică, cele mai importante pârghii sunt educația și cercetarea, parteneriatele public-private și mecanismele de cooperare la nivel european.

Cercetarea și educația în domeniul securității cibernetice trebuie să reprezinte priorități ale politicilor publice. Consolidarea cercetării în domeniul securității informatice, îmbunătățirea educației și dezvoltarea forței de muncă instruite sunt esențiale pentru atingerea obiectivelor generale ale politicii privind securitatea cibernetică. Educația, învățarea și instruirea profesională pe tot parcursul vieții reprezintă nu doar obiectivele unui program propus la nivelul Uniunii Europene, ci scopuri în sine, care îmbunătățesc experiența personală a fiecăruia dintre noi. Politicile în cercetare și educație vor fi eficiente doar dacă includ natura multilaterală și multidisciplinară a securității cibernetice ca element fundamental și omniprezent în cultura, abordările, sistemele și infrastructurile tehnice.

Parteneriatele public-private sunt indispensabile în asigurarea securității cibernetice la nivel național. Protejarea spațiului virtual prezintă de fapt o responsabilitate partajată și care poate fi eficient realizată prin colaborarea dintre Guvern și sectorul privat, care de multe ori deține și operează o mare parte a infrastructurii. Pentru a asigura securitatea națională, guvernele trebuie să gestioneze securitatea cibernetică în colaborare cu sectorul privat, ținând cont de faptul că succesul colaborării implică o serie de condiții ce urmează a fi create, cum ar fi încrederea, beneficiile reale și înțelegerea clară a rolurilor reciproce.

Cooperarea internațională joacă un rol-cheie în acest domeniu, deoarece provocările privind securitatea cibernetică depășesc granițele, extinzându-se până la nivelul sistemelor interconectate la nivel global. Colaborarea cu entități europene și internaționale este absolut necesară, fie că este vorba de unități de învățământ, centre de cercetare, companii private sau instituții guvernamentale. Cooperarea dintre instituții, organizații și comunitatea de securitate cibernetică poate fi utilă în găsirea și stabilirea vulnerabilităților. Un mecanism de cooperare dovedit în acest sens este divulgarea coordonată a vulnerabilităților. Adoptarea unor politici publice unitare la nivelul statelor membre privind divulgarea coordonată a vulnerabilităților și a unor mecanisme coordonate de acțiune/cooperare trans-sectoriale vor asigura ecosistemul necesar asigurării securității în spațiul comunitar.

Conf.dr.ing. **Ioan-Cosmin MIHAI –** Academia de Poliție „A.I. Cuza”

Dr.ing. **Costel CIUCHI** – Secretariatul General al Guvernului

Drd.ing. **Gabriel PETRICĂ** – Universitatea Politehnica din București