CERTIFICAREA SECURITĂȚII CIBERNETICE ÎN CADRUL REGULAMENTULUI (UE) 2019/881

În toate sectoarele cheie de activitate, în prezent, rețelele și sistemele informatice precum și rețelele și serviciile de comunicații ocupă un loc din ce în ce mai central în societatea umană, devenind astfel „coloana vertebrală a creșterii economice”[1]. Ca urmare, utilizarea la scară generală a acestor rețele și sisteme informatice, caracterizate în principal prin digitalizare și conectivitate, aduc în actualitate provocări și nevoi complexe legate de securitatea și reziliența cibernetică.

Securitatea cibernetică implică un set de activități necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane afectate de amenințări cibernetice tot mai variate. Astfel, se poate spune că securitatea cibernetică combină complex și armonios educația (promovarea „igienei cibernetice”[1]), politicile și procedurile din domeniu, securitatea fizică și tehnologia.

Pentru securitatea cibernetică au fost adoptate strategii la nivel european și la nivelul statelor membre, inclusiv în România, unde, la sfârșitul anului trecut a fost aprobată „Strategia de securitate cibernetică pentru perioada 2022-2027”, care a actualizat și completat documentul anterior din 2013.

Uniunea Europeană a elaborat o serie de documente strategice de securitate cibernetică (2013, 2021) care orientează politicile prin care să se răspundă la amenințările cibernetice și riscurile de securitate cibernetică. Primul act legislativ al UE în domeniul securității cibernetice a fost Directiva UE 2016/1148 a Parlamentului și Consiliului [2], document care a instituit primele cerințe privind capacitățile naționale în domeniu, a creat mecanisme de intensificare a cooperării și a introdus obligații privind măsurile de securitate precum și notificări ale incidentelor în sectoare cum ar fi energia, transporturile, furnizarea și distribuirea de apă potabilă, bănci, infrastructuri ale pieței financiare, asistența medicală, infrastructuri digitale si nu în ultimul rând în sfera furnizorilor de servicii digitale esențiale (motoare de căutare, servicii de cloud computing și piețe on-line).

În anul 2019 a fost adoptat Regulamentul (UE) 2019/881 al Parlamentului European și Consiliului privind ENISA (Agenția UE pentru Securitate Cibernetică) și certificarea securității cibernetice pentru tehnologia informației și comunicațiilor – CyberSecurity Act, document care a întărit rolul acestei Agenții europene și a stabilit cadrul de certificare a produselor și serviciilor TCI.

Certificarea în securitatea cibernetică este inclusă într-unul din obiectivele strategice ale ENISA, formulate în Strategia Agenției din iunie 2020 [3]. Prin obiectivul 6 „High level trust in secure digital solution”, se urmărește atingerea mediului digital cibernetic sigur în spațiul UE în care cetățenii pot să aibă încredere în produsele, serviciile și procesele TCI, prin implementarea de scheme de certificare în domenii tehnologice cheie.

Odată cu intrarea în vigoare a CyberSecurity Act, certificarea securității cibernetice devine un factor determinant atât pentru succesul în afaceri pentru furnizorii unor categorii largi de produse TCI (de ex. internetul, inteligența artificială, componentele 5G software și hardware, aplicațiile web etc.), de servicii TCI (de ex. cloud computing, comercializare on-line etc.) sau de procese TCI (de ex. fabricație, dezvoltare de aplicații, aprovizionare pe lanț etc.), cât și pentru protecția cibernetică a utilizatorilor.

Plecând de la necesitatea de produse și soluții de securitate cibernetică caracterizate prin calitate superioară, accesibile ca preț și interoperabile, nevoi formulate încă din 2016 în Comunicarea Comisiei „Consolidarea sistemului de reziliență cibernetică a Europei și încurajarea unui sector al securității cibernetice competitiv și inovator” și reluate în Comunicarea din anul următor, s-a conturat o nouă prioritate și anume stabilirea normelor privind modul de organizare a certificării de securitate a TCI în UE în cadrul european de securitate.

Cadrul european de certificare a securității cibernetice stabilește principalele cerințe orizontale pentru schemele europene de certificare a securității cibernetice create și permite recunoașterea și utilizarea certificatelor europene de securitate cibernetică și a declarațiilor de conformitate UE pentru produse TIC, servicii TIC sau procese TIC în toate statele membre.

Un exemplu de schemă de certificare dezvoltată, propusă pentru a fi implementată la nivel european, vizează serviciile cloud computers [5].

La nivelul statelor membre, sunt dezvoltate sau sunt în curs de dezvoltare scheme de certificare a securității cibernetice, care implică o conlucrare strânsă a specialiștilor din cele mai diverse domenii.

Pentru dezvoltarea de astfel de scheme, autoritățile de certificare a securității cibernetice și organismele naționale de acreditare colaborează activ pentru dezvoltarea unor sisteme naționale de certificare a securității cibernetice care să stabilească un set cuprinzător de norme, cerințe tehnice, standarde și proceduri aplicabile certificării sau evaluării conformității produselor TIC, serviciilor TIC și proceselor TIC care intră în domeniul respectiv. În cadrul acestor sisteme, organismele de evaluare a conformității îndeplinesc cerințele standardelor relevante și sunt acreditate de organismele naționale de acreditare în temeiul Regulamentului (UE) 765/2005 [6].

Referințe

1. Regulamentul (UE) 2019/881 al Parlamentului european și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică), J.Of. L151/7.06.2019, p.15-69;
2. Directiva (UE) 2016/1148 a Parlamentului european și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune;
3. A TRUSTED AND CYBER SECURE EUROPE, ENISA Strategy, June 2020, ENISA Strategy - A Trusted and Cyber Secure Europe — ENISA (europa.eu)
4. Strenghtening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, 2016, EC Communication: Strenghtening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry | CYBERWISER.eu
5. EUCS – CLOUD SERVICES SCHEME EUCS, a candidate cybersecurity certification scheme for cloud services, December 2020;
6. Regulamentul (CE) Nr. 765/2008 al Parlamentului European şi al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93;
7. Proiecte: RENAR