

DOCUMENT IN LUCRU

Strategia de securitate cibernetică a României

CUPRINS

I – Introducere

1. Context

2. Scop și obiective

3. Concepte, definiții și termeni

4. Principii

II – Vulnerabilități, riscuri și amenințări

III – Direcții de acțiune

IV – Sistemul Național de Securitate Cibernetică

V – Concluzii

I – Introducere

1. Context

Dezvoltarea rapidă a tehnologiilor moderne de informații și comunicații – condiție sine qua non a edificării societății informaționale – a avut un impact major asupra ansamblului social, marcând adevărate mutații în filozofia de funcționare a economicului, politicului și culturalului, dar și asupra vieții de zi cu zi a individului.

Practic, în prezent accesul facil la tehnologia informației și comunicațiilor reprezintă una dintre premisele buneii funcționări a societății moderne.

Spațiul cibernetic se caracterizează prin lipsa frontierelor, dinamism și anonim, generând atât deopotrivă, oportunități de dezvoltare a societății informaționale bazate pe cunoaștere și riscuri la adresa funcționării acesteia (la nivel individual, statal și chiar cu manifestare transfrontalieră).

Cu cât o societate este mai informatizată, cu atât este mai vulnerabilă, iar asigurarea securității spațiului cibernetic trebuie să constituie o preocupare majoră a tuturor actorilor implicați, mai ales la nivel instituțional, unde se concentrează responsabilitatea elaborării și aplicării de politici coerente în domeniu.

România urmărește atât dezvoltarea unui mediu informațional dinamic bazat pe interoperabilitate și servicii specifice societății informaționale, cât și asigurarea respectării drepturilor și libertăților fundamentale ale cetățenilor și a intereselor de securitate națională, într-un cadru legal adecvat.

Din această perspectivă, se resimte necesitatea dezvoltării culturii de securitate cibernetică a utilizatorilor sistemelor informatice și de comunicații, adesea insuficient informați în legătură cu potențialele riscuri, dar și cu soluțiile de contracarare a acestora.

Cunoașterea pe scară largă a riscurilor și amenințărilor la care sunt supuse activitățile desfășurate în spațiul cibernetic și modului de prevenire și contracarare a acestora necesită o comunicare și cooperare eficiente între actorii specifici în acest domeniu.

Statul român își asumă rolul de coordonator al activităților desfășurate la nivel național pentru asigurarea securității cibernetice, în concordanță cu demersurile inițiate la nivel UE și NATO. Problematika securității cibernetice a devenit prioritară pentru aceste organisme, care au stabilit cadrul de reglementare necesar dezvoltării mecanismelor de apărare cibernetic (Anexa).

2. Scop și obiective

Prezenta Strategie are rolul de a fundamenta obiectivele, principiile și direcțiile de acțiune într-o manieră coerentă și unitară în vederea cunoașterii, prevenirii și contracarării riscurilor și amenințărilor la adresa securității cibernetice a României.

În scopul protecției infrastructurilor cibernetice aparținând instituțiilor guvernamentale, publice și private, Strategia își propune următoarele obiective:

- a) adaptarea cadrului normativ și instituțional la dinamica amenințărilor specifice spațiului cibernetic;
- b) stabilirea și aplicarea unor cerințe minimale de securitate pentru infrastructurile cibernetice naționale, cu relevanță pentru funcționarea infrastructurilor critice;
- c) asigurarea rezilienței infrastructurilor cibernetice;
- d) promovarea și dezvoltarea cooperării în plan național și internațional;
- e) creșterea culturii de securitate a populației prin conștientizarea față de vulnerabilitățile, riscurile și amenințările provenite din mediul cibernetic și necesitatea asigurării protecției sistemelor informatice proprii.

3. Concepte, definiții și termeni

Infrastructuri cibernetice – infrastructuri de tehnologia informației și comunicații, constând în sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice.

Spațiul cibernetic – mediul virtual, generat de infrastructurile cibernetice, incluzând conținutul informațional procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta.

Securitate cibernetică – starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și non-repudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spațiul cibernetic. Măsurile proactive și reactive pot include: politici, concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protejare a infrastructurilor cibernetice, managementul identității, managementul consecințelor.

Amenințare cibernetică – orice circumstanță sau eveniment care constituie un pericol potențial la adresa securității cibernetice.

Atac cibernetic – orice acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică.

Incident cibernetic – orice eveniment survenit în spațiul cibernetic de natură să afecteze securitatea cibernetică.

Război cibernetic – desfășurarea de acțiuni ofensive în spațiul cibernetic de către un stat în scopul *distrugerii sau perturbării funcționării infrastructurilor critice* ale altui stat, concomitent cu desfășurarea de acțiuni defensive și contraofensive pentru protejarea infrastructurii cibernetice proprii.

Terorism cibernetic – activitățile premeditate desfășurate în spațiul cibernetic de către persoane, grupări sau organizații motivate politic, ideologic sau religios ce pot determina distrugerii materiale sau victime de natură să determine panică sau teroare.

Spionaj cibernetic – acțiuni desfășurate în spațiul cibernetic, cu scopul de a obține neautorizat informații confidențiale în interesul unui stat.

Criminalitatea informatică – totalitatea faptelor prevăzute de legea penală care reprezintă pericol social și sunt săvârșite cu vinovăție, prin intermediul sau asupra infrastructurilor cibernetic.

Vulnerabilitatea - o slăbiciune în proiectarea și implementarea infrastructurilor cibernetic sau a măsurilor de securitate aferente care poate fi exploatată de către o amenințare.

Riscul de securitate - probabilitatea ca o amenințare să se materializeze, exploatând o anumită vulnerabilitate specifică infrastructurilor cibernetic.

Managementul riscului - un proces complex, continuu și flexibil de identificare, evaluare și contracarare a riscurilor la adresa securității cibernetic, bazat pe utilizarea unor tehnici și instrumente complexe, pentru prevenirea pierderilor de orice natură.

Managementul identității - metode de validare a identității persoanelor când acestea accesează anumite infrastructuri cibernetic.

Reziliența infrastructurilor cibernetic – capacitatea componentelor infrastructurilor cibernetic de a rezista unui incident sau atac cibernetic și de a reveni la starea de normalitate.

CERT – Centru de răspuns la incidente de securitate cibernetică – entitate organizațională specializată care dispune de capacitățile necesare pentru prevenirea, analiza, identificarea și reacția la incidentele cibernetic.

4. Principii

La baza realizării securității cibernetice stau următoarele principii:

- **Coordonarea** – activitățile se realizează într-o concepție unitară, pe baza unor planuri de acțiune convergente destinate asigurării securității cibernetice, în conformitate cu atribuțiile și responsabilitățile fiecărei entități;
- **Cooperarea** – toate entitățile implicate (din mediul public sau privat) colaborează, la nivel național și internațional, pentru asigurarea unui răspuns adecvat la amenințările din spațiul cibernetic;
- **Eficiența** – demersurile întreprinse vizează managementul optim al resurselor disponibile;
- **Prioritizarea** – eforturile se vor concentra asupra securizării infrastructurilor cibernetice ce susțin infrastructurile critice naționale.
- **Diseminarea** – asigurarea transferului de informații, expertiză și bune practici în scopul protejării infrastructurilor cibernetice.

II – Vulnerabilități, riscuri și amenințări

Amenințările specifice spațiului cibernetic se caracterizează prin asimetrie și dinamică accentuată și caracter global, ceea ce le face dificil de identificat și de contracarat prin măsuri proporționale cu impactul materializării riscurilor.

România se confruntă în prezent cu amenințări provenite din spațiul cibernetic la adresa infrastructurilor critice, având în vedere interdependența din ce în ce mai ridicată între infrastructurile cibernetice și infrastructuri precum cele din sectoarele financiar-bancar, transport, energie și apărare națională. Globalitatea spațiului cibernetic este de natură să amplifice riscurile la adresa acestora afectând în aceeași măsură atât sectorul privat, cât și cel public.

Amenințările la adresa spațiului cibernetic se pot clasifica în mai multe moduri, dar cele mai frecvent utilizate sunt cele bazate pe factorii motivaționali și impactul asupra societății. În acest sens, putem avea în vedere criminalitatea cibernetică, terorismul cibernetic și războiul cibernetic, având ca sursă atât actori statali, cât și non-statali.

Amenințările din spațiul cibernetic se materializează – prin exploatarea vulnerabilităților natură umană, tehnică și procedurală – cel mai adesea în:

- o atacuri cibernetice împotriva infrastructurilor care susțin funcții de utilitate publică ori servicii ale societății informaționale a căror întrerupere / afectare ar putea constitui un pericol la adresa securității naționale;
- o accesarea neautorizată a infrastructurilor cibernetice;
- o modificarea, ștergerea sau deteriorarea neautorizată de date informatice ori restricționarea ilegală a accesului la aceste date;
- o spionajul cibernetic;
- o cauzarea unui prejudiciu patrimonial, hărțuirea și șantajul persoanelor fizice și juridice, de drept public și privat.

Principalii actori care generează amenințări în spațiul cibernetic sunt:

- **Persoane** sau **grupări de criminalitate organizată** care exploatează vulnerabilitățile spațiului cibernetic în scopul obținerii de avantaje patrimoniale sau nepatrimoniale;
- **Teroriști** sau **extremiști** care utilizează spațiul cibernetic pentru desfășurarea și coordonarea unor atacuri teroriste, activități de comunicare, propagandă, recrutare și instruire, colectare de fonduri etc., în scopuri teroriste.
- **State** sau **actori non-statali** care inițiază sau derulează operațiuni în spațiul cibernetic în scopul culegerii de informații din domeniile guvernamental, militar, economic sau al materializării altor amenințări la adresa securității naționale.

III – Direcții de acțiune

România își propune asigurarea stării de normalitate în spațiul cibernetic **reducând riscurile și valorificând oportunitățile specifice**, prin **îmbunătățirea cunoștințelor, capacităților și a mecanismelor de decizie**. În acest sens, eforturile se vor focaliza pe următoarele direcții de acțiune:

1. **Stabilirea cadrului conceptual, organizatoric și acțional necesar asigurării securității cibernetice.**

- Constituirea și operaționalizarea unui **Sistem Național de Securitate Cibernetică**.
- Completarea și armonizarea cadrului legislativ național în domeniu, inclusiv stabilirea și aplicarea unor cerințe minimale de securitate pentru infrastructurile cibernetice naționale.
- Dezvoltarea unui parteneriat public-privat, inclusiv prin stimularea schimbului reciproc de informații, privind amenințări, vulnerabilități, riscuri, precum și incidente și atacuri cibernetice.

2. **Dezvoltarea capacităților naționale de management al riscului în domeniul securității cibernetice și de reacție la incidente cibernetice în baza unui *Program național* vizând:**

- Consolidarea, la nivelul autorităților competente potrivit legii, a potențialului de cunoaștere, prevenire și contracarare a riscurilor asociate utilizării spațiului cibernetic.
- Asigurarea unor instrumente de dezvoltare a cooperării cu sectorul privat în domeniul securității cibernetice, inclusiv pentru crearea unui mecanism eficient de avertizare și alertă, respectiv de reacție la incidentele cibernetice.
- Stimularea capacităților naționale de cercetare-dezvoltare și inovare în domeniul securității cibernetice.
- Creșterea nivelului de reziliență infrastructurilor cibernetice.

- Dezvoltarea entităților de tip CERT.

3. Promovarea și consolidarea culturii de securitate în domeniul cibernetic

- Derularea unor programe de conștientizare a populației, a administrației publice și a sectorului privat cu privire la vulnerabilitățile, riscurile și amenințările specifice utilizării spațiului cibernetic.
- Formarea profesională adecvată a persoanelor care își desfășoară activitatea în domeniul securității cibernetică și promovarea pe scară largă a certificărilor profesionale în domeniu.
- Includerea unor elemente referitoare la securitatea cibernetică în programele de formare și perfecționare profesională a managerilor din domeniul public și privat.

4. Dezvoltarea cooperării internaționale în domeniul securității cibernetică

- Încheierea de acorduri de cooperare la nivel internațional pentru îmbunătățirea capacității de răspuns în cazul unor atacuri cibernetică majore.
- Participarea la programe internaționale care vizează domeniul securității cibernetică.
- Promovarea intereselor naționale de securitate cibernetică în formatele de cooperare internațională la care România este parte.

IV. Sistemul Național de Securitate Cibernetică

Sistemul Național de Securitate Cibernetică – SNSC reprezintă cadrul de cooperare care reunește autorități și instituții publice, mediul academic și cel de afaceri, asociații profesionale, organizații neguvernamentale, cu responsabilități și capacități în domeniu, în vederea coordonării acțiunilor pentru asigurarea securității componente naționale a spațiului cibernetic.

Coordonarea activității Sistemului Național de Securitate Cibernetică este asigurată de un comitet, având ca obiective implementarea Programului Național în domeniu, managementul acțiunilor, la nivel național, în cazul unui atac cibernetic, respectiv corelarea demersurilor instituțiilor componente în cadrul formatelor de cooperare internațională la care România este parte.

Sistemul Național de Securitate Cibernetică asigură cunoașterea, prevenirea și contracararea unui atac împotriva componente naționale a spațiului cibernetic, inclusiv managementul consecințelor.

Componenta de cunoaștere trebuie să asigure informațiile necesare în elaborarea măsurilor pentru prevenirea efectelor unor incidente cibernetică.

Componenta de prevenire este principalul mijloc de asigurare a securității cibernetică. Acțiunile preventive reprezintă cea mai eficientă modalitate atât de a reduce extinderea

pe teritoriul național a mijloacelor specifice unui atac cibernetic, cât și de a limita efectele utilizării acestora.

Componenta de contracarare trebuie să asigure o reacție eficientă la atacuri cibernetice, prin identificarea și blocarea acțiunilor ostile în spațiul cibernetic, menținerea sau restabilirea disponibilității infrastructurilor cibernetice vizate și identificarea și sancționarea potrivit legii a autorilor.

Succesul activităților desfășurate în SNSC depinde în mod esențial de cooperarea, inclusiv în formele de parteneriat public-privat, între deținătorii infrastructurilor cibernetice și autoritățile statului abilitate să întreprindă măsuri de prevenire, contracarare, investigare și eliminare a efectelor unei amenințări materializate printr-un atac.

V. Concluzii

Succesul demersului depinde, în mod esențial, de eficiența cooperării la nivel național pentru protejarea spațiului cibernetic, respectiv de coordonarea demersurilor naționale cu orientările și măsurile adoptate la nivel internațional, în formatele de cooperare la care România este parte.

Având în vedere dinamismul evoluțiilor globale în spațiul cibernetic, precum și obiectivele României în procesul de dezvoltare a societății informaționale și implementare pe scară largă a serviciilor electronice, este necesară elaborarea unui program național detaliat, care - pe baza reperelor oferite de prezenta Strategie – să asigure elaborarea și punerea în practică a unor proiecte concrete de securitate cibernetică.

Măsurile destinate operaționalizării Sistemului Național de Securitate Cibernetică trebuie armonizate cu eforturile pe dimensiunea protecției infrastructurilor critice, respectiv cu evoluția procesului de dezvoltare a capacităților de tip CERT. În varianta optimă, SNSC trebuie să dispună de o structură flexibilă, adaptativă, care să înglobeze capacități de identificare și anticipare, resurse și proceduri operaționale de prevenire, reacție și contracarare și instrumente pentru documentare și sancționare a autorilor atacurilor cibernetice.

Este necesară implementarea, la nivel național, a unor standarde minimale procedurale și de securitate pentru infrastructurile cibernetice (cu valorificarea modelului oferit de Security Operational Center - SOC), care să fundamenteze eficiența demersurilor de protejare față de atacuri cibernetice și să limiteze riscurile producerii unor incidente cu potențial impact semnificativ.

Autoritățile publice cu responsabilități în acest domeniu vor aloca resursele financiare necesare asigurării securității cibernetice prin intermediul politicilor de planificare. Pentru asigurarea unei capacități sporite de identificare, evaluare și proiectare a măsurilor adecvate de management al riscului sau de răspuns la incidente și atacuri cibernetice, este prioritară dezvoltarea schimburilor de informații și transferului de expertiză între autoritățile cu responsabilități în domeniu, dezvoltarea parteneriatului public-privat și

extinderea cooperării cu mediile neguvernamentale și comunitatea academică.

SNSC va integra centrele de coordonare existente, valorificând instrumentele de coordonare și cooperare oferite de acestea, și va acționa pentru consolidarea expertizei în domeniul riscurilor cibernetice, prin stimularea sinergiilor între diferitele planuri de acțiune în domeniul securității cibernetice (militar-civil, public-privat, guvernamental-neguvernamental).

Dat fiind ritmul rapid de evoluție a problematicii, prezenta strategie va fi testată și revizuită permanent, inclusiv în contextul mai larg al Strategiei Naționale de Apărare, în vederea adaptării continue la provocările și oportunitățile generate de un mediu de securitate în permanentă schimbare.