DOCUMENT IN LUCRU

Strategia de securitate cibernetică a României

CUPRINS

I – Introducere

1. Context

Dezvoltarea rapidă a tehnologiilor moderne de informaţii şi comunicaţii – condiţie sine qua non a edificării societăţii informaţionale – a avut un impact major asupra ansamblului social, marcând adevărate mutaţii în filozofia de funcţionare a economicului, politicului şi culturalului, dar şi asupra vieţii de zi cu zi a individului.

Practic, în prezent accesul facil la tehnologia informaţiei şi comunicaţiilor reprezintă una dintre premisele bunei funcţionări a societăţii moderne.

Spaţiul cibernetic se caracterizează prin lipsa frontierelor, dinamism şi anonimat, generând atât deopotrivă, oportunităţi de dezvoltare a societăţii informaţionale bazate pe cunoaştere şi riscuri la adresa funcţionării acesteia (la nivel individual, statal şi chiar cu manifestare transfrontalieră).

Cu cât o societate este mai informatizată, cu atât este mai vulnerabilă, iar asigurarea securităţii spaţiului cibernetic trebuie să constituie o preocupare majoră a tuturor actorilor implicaţi, mai ales la nivel instituţional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu.

România urmăreşte atât dezvoltarea unui mediu informaţional dinamic bazat pe interoperabilitate şi servicii specifice societăţii informaţionale, cât şi asigurarea respectării drepturilor şi libertăţilor fundamentale ale cetăţenilor şi a intereselor de securitate naţională, într-un cadru legal adecvat.

Din această perspectivă, se resimte necesitatea dezvoltării culturii de securitate cibernetică a utilizatorilor sistemelor informatice şi de comunicaţii, adesea insuficient informaţi în legătură cu potenţialele riscuri, dar şi cu soluţiile de contracarare a acestora.

Cunoaşterea pe scară largă a riscurilor şi ameninţărilor la care sunt supuse activităţile desfăşurate în spaţiul cibernetic şi modului de prevenire şi contracarare a acestora necesită o comunicare şi cooperare eficiente între actorii specifici în acest domeniu.

Statul român îşi asumă rolul de coordonator al activităţilor desfăşurate la nivel naţional pentru asigurarea securităţii cibernetice, în concordanţă cu demersurile iniţiate la nivel UE şi NATO. Problematica securităţii cibernetice a devenit prioritară pentru aceste organisme, care au stabilit cadrul de reglementare necesar dezvoltării mecanismelor de apărare cibernetic (Anexa).

2. Scop şi obiective

Prezenta Strategie are rolul de a fundamenta obiectivele, principiile şi direcţiile de acţiune într-o manieră coerentă şi unitară în vederea cunoaşterii, prevenirii şi contracarării riscurilor şi ameninţărilor la adresa securităţii cibernetice a României.

În scopul protecţiei infrastructurilor cibernetice aparţinând instituţiilor guvernamentale, publice şi private, Strategia îşi propune următoarele obiective:

a) adaptarea cadrului normativ şi instituţional la dinamica ameninţărilor specifice spaţiului cibernetic;
b) stabilirea şi aplicarea unor cerinţe minimale de securitate pentru infrastructurile cibernetice naţionale, cu relevanţă pentru funcţionarea infrastructurilor critice;
c) asigurarea rezilienţei infrastructurilor cibernetice;
d) promovarea şi dezvoltarea cooperării în plan naţional şi internaţional;
e) creşterea culturii de securitate a populaţiei prin conştientizarea faţă de vulnerabilităţile, riscurile şi ameninţările provenite din mediul cibernetic şi necesitatea asigurării protecţiei sistemelor informatice proprii.

3. Concepte, definiţii şi termeni

Infrastructuri cibernetice – infrastructuri de tehnologia informaţiei şi comunicaţii, constând în sisteme informatice, aplicaţii aferente, reţele şi servicii de comunicaţii electronice.

Spaţiul cibernetic – mediul virtual, generat de infrastructurile cibernetice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acesta.

Securitate cibernetică – starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi non-repudierea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private, din spaţiul cibernetic. Măsurile proactive şi reactive pot include: politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activităţi de instruire şi conştientizare, implementarea de soluţii tehnice de protejare a infrastructurilor cibernetice, managementul identităţii, managementul consecinţelor.

Ameninţare cibernetică – orice circumstanţă sau eveniment care constituie un pericol potenţial la adresa securităţii cibernetice.

Atac cibernetic – orice acţiune ostilă desfăşurată în spaţiul cibernetic de natură să afecteze securitatea cibernetică.

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

Război cibernetic – desfăşurarea de acţiuni ofensive în spaţiul cibernetic de către un stat în scopul *distrugerii sau perturbării funcţionării infrastructurilor critice* ale altui stat, concomitent cu desfăşurarea de acţiuni defensive şi contraofensive pentru protejarea infrastructurii cibernetice proprii.

Terorism cibernetic – activităţile premeditate desfăşurate în spaţiul cibernetic de către persoane, grupări sau organizaţii motivate politic, ideologic sau religios ce pot determina distrugeri materiale sau victime de natură să determine panică sau teroare.

Spionaj cibernetic – acţiuni desfăşurate în spaţiul cibernetic, cu scopul de a obţine neautorizat informaţii confidenţiale în interesul unui stat.

Criminalitatea informatică – totalitatea faptelor prevăzute de legea penală care reprezintă pericol social şi sunt săvârşite cu vinovăţie, prin intermediul sau asupra infrastructurilor cibernetice.

Vulnerabilitatea - o slăbiciune în proiectarea şi implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente care poate fi exploatată de către o ameninţare.

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

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

Managementul identităţii - metode de validare a identităţii persoanelor când acestea accesează anumite infrastructuri cibernetice.

Rezilienţa infrastructurilor cibernetice – capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic şi de a reveni la starea de normalitate.

CERT – Centru de răspuns la incidente de securitate cibernetică – entitate organizaţională specializată care dispune de capabilităţile necesare pentru prevenirea, analiza, identificarea şi reacţia la incidentele cibernetice.

4. Principii

La baza realizării securităţii cibernetice stau următoarele principii:

- ***Coordonarea*** *– activităţile se realizează într-o concepţie unitară, pe baza unor planuri de acţiune convergente destinate asigurării securităţii cibernetice, în conformitate cu atribuţiile şi responsabilităţile fiecărei entităţi;*
- ***Cooperarea*** *– toate entităţile implicate (din mediul public sau privat) colaborează, la nivel naţional şi internaţional, pentru asigurarea unui răspuns adecvat la ameninţările din spaţiul cibernetic;*
- ***Eficienţa*** *– demersurile întreprinse vizează managementul optim al resurselor disponibile;*
- ***Prioritizarea*** *– eforturile se vor concentra asupra securizării infrastructurilor cibernetice ce susţin infrastructurile critice naţionale.*
- ***Diseminarea*** *– asigurarea transferului de informaţii, expertiză şi bune practici în scopul protejării infrastructurilor cibernetice.*

II – Vulnerabilităţi, riscuri şi ameninţări

Ameninţările specifice spaţiului cibernetic se caracterizează prin asimetrie şi dinamică accentuată şi caracter global, ceea ce le face dificil de identificat şi de contracarat prin măsuri proporţionale cu impactul materializării riscurilor.

România se confruntă în prezent cu ameninţări provenite din spaţiul cibernetic la adresa infrastructurilor critice, având în vedere interdependenţa din ce în ce mai ridicată între infrastructurile cibernetice şi infrastructuri precum cele din sectoarele financiar-bancar, transport, energie şi apărare naţională. Globalitatea spaţiului cibernetic este de natură să amplifice riscurile la adresa acestora afectând în aceeaşi măsură atât sectorul privat, cât şi cel public.

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

Ameninţările din spaţiul cibernetic se materializează – prin exploatarea vulnerabilităţilor natură umană, tehnică şi procedurală – cel mai adesea în:

- atacuri cibernetice împotriva infrastructurilor care susţin funcţii de utilitate publică ori servicii ale societăţii informaţionale a căror întrerupere / afectare ar putea constitui un pericol la adresa securităţii naţionale;
- accesarea neautorizată a infrastructurilor cibernetice;
- modificarea, ştergerea sau deteriorarea neautorizată de date informatice ori restricţionarea ilegală a accesului la aceste date;
- spionajul cibernetic;
- cauzarea unui prejudiciu patrimonial, hărţuirea şi şantajul persoanelor fizice şi juridice, de drept public şi privat.

Principalii actori care generează ameninţări în spaţiul cibernetic sunt:

- **Persoane** sau **grupări de criminalitate organizată** care exploatează vulnerabilităţile spaţiului cibernetic în scopul obţinerii de avantaje patrimoniale sau nepatrimoniale;
- **Terorişti** sau **extremişti** care utilizează spaţiul cibernetic pentru desfăşurarea şi coordonarea unor atacuri teroriste, activităţi de comunicare, propagandă, recrutare şi instruire, colectare de fonduri etc., în scopuri teroriste.
- **State** sau **actori non-statali** care iniţiază sau derulează operaţiuni în spaţiul cibernetic în scopul culegerii de informaţii din domeniile guvernamental, militar, economic sau al materializării altor ameninţări la adresa securităţii naţionale.

III – Direcţii de acţiune

România îşi propune asigurarea stării de normalitate în spaţiul cibernetic **reducând riscurile** şi **valorificând oportunităţile specifice**, prin **îmbunătăţirea cunoştinţelor, capabilităţilor şi a mecanismelor de decizie**. În acest sens, eforturile se vor focaliza pe următoarele direcţii de acţiune:

1. Stabilirea cadrului conceptual, organizatoric şi acţional necesar asigurării securităţii cibernetice.

- Constituirea şi operaţionalizarea unui **Sistem Naţional de Securitate Cibernetică**.
- Completarea şi armonizarea cadrului legislativ naţional în domeniu, inclusiv stabilirea şi aplicarea unor cerinţe minimale de securitate pentru infrastructurile cibernetice naţionale.
- Dezvoltarea unui parteneriat public-privat, inclusiv prin stimularea schimbului reciproc de informaţii, privind ameninţări, vulnerabilităţi, riscuri, precum şi incidente şi atacuri cibernetice.

2. Dezvoltarea capacităţilor naţionale de management al riscului în domeniul securităţii cibernetice şi de reacţie la incidente cibernetice în baza unui *Program naţional* vizând:

- Consolidarea, la nivelul autorităţilor competente potrivit legii, a potenţialului de cunoaştere, prevenire şi contracarare a riscurilor asociate utilizării spaţiului cibernetic.
- Asigurarea unor instrumente de dezvoltare a cooperării cu sectorul privat în domeniul securităţii cibernetice, inclusiv pentru crearea unui mecanism eficient de avertizare şi alertă, respectiv de reacţie la incidentele cibernetice.
- Stimularea capabilităţilor naţionale de cercetare-dezvoltare şi inovare în domeniul securităţii cibernetice.
- Creşterea nivelului de rezilienţă infrastructurilor cibernetice.

- Dezvoltarea entităţilor de tip CERT.

3. Promovarea şi consolidarea culturii de securitate în domeniul cibernetic

- Derularea unor programe de conştientizare a populaţiei, a administraţiei publice şi a sectorului privat cu privire la vulnerabilităţile, riscurile şi ameninţările specifice utilizării spaţiului cibernetic.
- Formarea profesională adecvată a persoanelor care îşi desfăşoară activitatea în domeniul securităţii cibernetice şi promovarea pe scară largă a certificărilor profesionale în domeniu.
- Includerea unor elemente referitoare la securitatea cibernetică în programele de formare şi perfecţionare profesională a managerilor din domeniul public şi privat.

4. Dezvoltarea cooperării internaţionale în domeniul securităţii cibernetice

- Încheierea de acorduri de cooperare la nivel internaţional pentru îmbunătăţirea capacităţii de răspuns în cazul unor atacuri cibernetice majore.
- Participarea la programe internaţionale care vizează domeniul securităţii cibernetice.
- Promovarea intereselor naţionale de securitate cibernetică în formatele de cooperare internaţională la care România este parte.

IV. Sistemul Naţional de Securitate Cibernetică

Sistemul Naţional de Securitate Cibernetică – SNSC reprezintă cadrul de cooperare care reuneşte autorităţi şi instituţii publice, mediul academic şi cel de afaceri, asociaţii profesionale, organizaţii neguvernamentale, cu responsabilităţi şi capabilităţi în domeniu, în vederea coordonării acţiunilor pentru asigurarea securităţii componentei naţionale a spaţiului cibernetic.

Coordonarea activităţii Sistemului Naţional de Securitate Cibernetică este asigurată de un comitet, având ca obiective implementarea Programului Naţional în domeniu, managementul acţiunilor, la nivel naţional, în cazul unui atac cibernetic, respectiv corelarea demersurilor instituţiilor componente în cadrul formatelor de cooperare internaţională la care România este parte.

Sistemul Naţional de Securitate Cibernetică asigură cunoaşterea, prevenirea şi contracararea unui atac împotriva componentei naţionale a spaţiului cibernetic, inclusiv managementul consecinţelor.

Componenta de cunoaştere trebuie să asigure informaţiile necesare în elaborarea măsurilor pentru prevenirea efectelor unor incidente cibernetice.

Componenta de prevenire este principalul mijloc de asigurare a securităţii cibernetice. Acţiunile preventive reprezintă cea mai eficientă modalitate atât de a reduce extinderea

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

Componenta de contracarare trebuie să asigure o reacţie eficientă la atacuri cibernetice, prin identificarea şi blocarea acţiunilor ostile în spaţiul cibernetic, menţinerea sau restabilirea disponibilităţii infrastructurilor cibernetice vizate şi identificarea şi sancţionarea potrivit legii a autorilor.

Succesul activităţilor desfăşurate în SNSC depinde în mod esenţial de cooperarea, inclusiv în formule de parteneriat public-privat, între deţinătorii infrastructurilor cibernetice şi autorităţile statului abilitate să întreprindă măsuri de prevenire, contracarare, investigare şi eliminare a efectelor unei ameninţări materializate printr-un atac.

V. Concluzii

Succesul demersului depinde, în mod esenţial, de eficienţa cooperării la nivel naţional pentru protejarea spaţiului cibernetic, respectiv de coordonarea demersurilor naţionale cu orientările şi măsurile adoptate la nivel internaţional, în formatele de cooperare la care România este parte.

Având în vedere dinamismul evoluţiilor globale în spaţiul cibernetic, precum şi obiectivele României în procesul de dezvoltare a societăţii informaţionale şi implementare pe scară largă a serviciilor electronice, este necesară elaborarea unui program naţional detaliat, care - pe baza reperelor oferite de prezenta Strategie – să asigure elaborarea şi punerea în practică a unor proiecte concrete de securitate cibernetică.

Măsurile destinate operaţionalizării Sistemului Naţional de Securitate Cibernetică trebuie armonizate cu eforturile pe dimensiunea protecţiei infrastructurilor critice, respectiv cu evoluţia procesului de dezvoltare a capabilităţilor de tip CERT. În varianta optimă, SNSC trebuie să dispună de o structură flexibilă, adaptativă, care să înglobeze capabilităţi de identificare şi anticipare, resurse şi proceduri operaţionale de prevenire, reacţie şi contracarare şi instrumente pentru documentare şi sancţionare a autorilor atacurilor cibernetice.

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

Autorităţile publice cu responsabilităţi în acest domeniu vor aloca resursele financiare necesare asigurării securităţii cibernetice prin intermediul politicilor de planificare. Pentru asigurarea unei capacităţi sporite de identificare, evaluare şi proiectare a măsurilor adecvate de management al riscului sau de răspuns la incidente şi atacuri cibernetice, este prioritară dezvoltarea schimburilor de informaţii şi transferului de expertiză între autorităţile cu responsabilităţi în domeniu, dezvoltarea parteneriatului public-privat şi

extinderea cooperării cu mediile neguvernamentale şi comunitatea academică.

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

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