STRATEGIA MINISTERULUI AFACERILOR INTERNE DE SECURITATE A INFORMAȚIILOR ÎN FORMAT ELECTRONIC (2021-2026)

În contextul dinamicii evoluției digitale și dezvoltării tehnologiilor emergente și disruptive s-au concretizat o serie de riscuri și amenințări complexe la adresa securității cibernetice, cu impact implicit asupra securității naționale, generate de o varietate de factori interni și externi.

Perpetuarea și rata crescută de materializare în acțiuni ostile a riscurilor și amenințărilor cibernetice determină mutații semnificative la nivel securitar, fapt pentru care este necesară adoptarea unei viziuni unitare de răspuns, asumate la nivelul tuturor actorilor implicați în asigurarea securității informatice. Pornind de la nevoia de schimbare a paradigmei conceptului actual de securitate cibernetică, noua viziune reclamă o abordare integrată și proactivă pentru a putea asigura efectiv prevenirea, descurajarea, contracararea și chiar atribuirea agresiunilor cibernetice complexe.

Prin obiectivele și direcțiile de acțiune avute în vedere, circumscrise unor principii și concepte fundamentale, precum respectarea drepturilor omului, prezenta Strategie urmărește consolidarea rezilienței infrastructurii IT&C și capacității ministerului de a gestiona eficient o criză de securitate cibernetică.

I. Introducere

1. Sumar

În contextul geopolitic actual, România reprezintă o țintă importantă a agresiunilor cibernetice, aspect determinat, în principal, de poziționarea strategică la limita unor sfere de influență globale, precum și de apartenența în cadrul unor formate de cooperare internaționale: UE, NATO și ONU.

În funcție de factorii generatori, agresiunile cibernetice vizează obținerea unor avantaje strategice sau a unor beneficii financiare, cu potențial impact în domeniul militar, politic, economic și social.

Având în vedere rolul Ministerului Afacerilor Interne (MAI) în domenii esențiale precum asigurarea și restabilirea ordinii publice, gestionarea situațiilor de urgență, securizarea frontierelor de stat, protecția infrastructurilor critice, administrarea unor baze de date ce deservesc interesul public etc., infrastructura IT&C a ministerului a devenit, în ultimii ani, o țintă predilectă a atacurilor informatice, nivelul îngrijorător al amenințării cibernetice fiind determinat de intensificarea acestor acțiuni ostile, de gradul de complexitate ridicat al instrumentelor folosite, precum și de modalitățile de operare utilizate.

Întrucât demersurile de reglementare a activităților subsumate securității cibernetice nu pot ține pasul cu ritmul evoluției tehnologice, abordarea problematicii trebuie realizată în baza unui document strategic care să asigure o viziune proactivă de securizare a infrastructurii IT&C a ministerului, concomitent cu creșterea permanentă a gradului de reziliență.

Recent a fost finalizat un amplu proces de revizuire a cadrului general conferit de *Strategia de Securitate Cibernetică a României din 2013*, subsumat demersurilor interinstituționale de elaborare a noii Strategii de Securitate Cibernetică a României 2.0, aflată în prezent pe circuitul de avizare în vederea aprobării prin hotărâre de guvern.

Pentru asigurarea unei transpuneri coerente a obiectivelor stabilite la nivel național, strategia sectorială a MAI vizează adaptarea acestora la specificul infrastructurii și misiunilor proprii.

2. *Contextul și provocările actuale ale mediului de securitate cibernetică*

Dezvoltarea continuă a tehnologiilor IT&C și nivelul din ce în ce mai ridicat de interconectare și interoperabilitate între sistemele informatice contribuie semnificativ la schimbarea percepției asupra amenințărilor, vulnerabilităților și riscurilor provenite din spațiul cibernetic.

Evaluările interne au relevat o creștere semnificativă a agresiunilor cibernetice identificate la adresa infrastructurii IT&C a ministerului în ultimii doi ani, atât din punct de vedere cantitativ, cât și din punct de vedere al complexității acestora, având următoarea pondere:

- 50% - programe malițioase de tip infostealer de extragere nedirecționată de date, în mod neautorizat (ex: Emotet, Agent Tesla, Trickbot);
- 16% - programe malițioase de tip ransomware de criptare a datelor (ex: Dharma, WannaCry, Ryuk);
- 10% - programe malițioase de tip keylogger de monitorizare și transmitere neautorizată a caracterelor tastate;
- 12% - programe malițioase de tip spyware de extragere direcționată de date în mod neautorizat;
- 8% - programe de tip cryptojacking de utilizare a resurselor informatice pentru minarea de criptomonede;
- 6% - programe malițioase de tip RAT - Remote Acces Trojan pentru obținerea accesului la distanță la sistemele țintă.

Comparativ cu perioada 2018-2019, în ultimii doi ani a fost constatată o creștere de aproximativ 150% a agresiunilor cibernetice lansate asupra infrastructurii IT&C a MAI, aspect determinat atât de intensificarea utilizării resurselor informatice pentru realizarea misiunilor specifice, dar și de sporirea interesului manifestat de o serie de actori ostili pentru compromiterea rețelelor și sistemelor informatice gestionate la nivelul ministerului.

Utilizarea tehnologiilor emergente, precum *Internet of Things*, inteligența artificială, *Machine Learning*, *blockchain* și *5G* constituie o necesitate pentru realizarea misiunilor specifice MAI, fapt pentru care trebuie anticipată modalitate de implementare optimă a acestora în infrastructura IT&C prin prevenirea unor eventuale breșe de securitate care să necesite alocarea ulterioară a unor resurse suplimentare.

Asumarea conceputului *security-by-design* în limitele unor standarde obligatorii va crește semnificativ eficiența măsurilor de securitate, atât din punct de vedere al capacității de detecție și răspuns, cât și din punct de vedere

al costurilor generate de achiziționarea și administrarea rețelelor și sistemelor informatice ale MAI.

Un climat stabil de securitate cibernetică poate fi asigurat doar cu concursul tuturor structurilor ministerului, precum și prin extinderea și consolidarea parteneriatelor cu mediile privat și academic, schimbul de expertiză și rezultatele activităților de cercetare putând fi valorificate pentru constituirea de bune practici în prevenirea și gestionarea incidentelor de securitate IT.

3. Amenințările actuale la nivelul Ministerului Afacerilor Interne

Amenințările cibernetice diferă din punct de vedere al gravității impactului și probabilității de materializare, în funcție de proveniența și scopul acțiunilor malițioase, cele mai grave fiind inclusiv de natură a afecta securitatea națională în domeniul afacerilor interne.

Analiza extinsă a agresiunilor cibernetice care au vizat infrastructura IT&C a ministerului relevă existența următoarelor categorii de atacatori:

- Entități afiliate unor actori statali;
- Entități din sfera criminalității informatice;
- Grupări hacktiviste/actori lone-wolf;
- Grupări/indivizi cu viziuni teroriste/extremiste.

3.1. Entități afiliate unor actori statali

Tipuri de agresiuni informatice caracteristice: infectarea cu malware de tip infostealer, spyware și RAT, spear-phishing, ransomware

Evaluările întocmite în contextul asigurării securității informatice la nivelul MAI au relevat o intensificare a agresiunilor informatice complexe îndreptate asupra resurselor ministerului și personalului acestuia, pentru realizarea cărora este necesară alocare de resurse semnificative de care dispun, în principal, actorii statali ostili interesați de obținerea unor avantaje strategice.

Amenințarea cibernetică generată de entități asociate unor actori statali reprezintă principala formă de amenințare la adresa securității cibernetice a României și implicit a MAI cu un impact ridicat asupra securității naționale.

Motivația atacurilor cibernetice derulate de actori statali este una strategică, aceștia urmărind preluarea și menținerea sub control a sistemelor informatice atacate cu scopul de a:

- sustrage neautorizat informații de interes, cu valențe strategice;
- perturba sau chiar întrerupe funcționalitatea unor infrastructuri cu valențe critice sau în domeniul serviciilor publice de importanță strategică;
- influența procese socio-politice pentru a genera dezechilibre la nivelul societății.

Atacurile cibernetice derulate de actorii statali sunt de regulă de tip *Advanced Persistent Threat (APT)* și au un nivel de complexitate ridicat, determinat de modul de operare și instrumentele folosite care sunt actualizate permanent în vederea eludării mecanismelor de detecție și menținerii persistenței pentru o perioadă îndelungată de timp în rețeaua compromisă.

3.2. Entități din sfera criminalității informatice

Tipuri de agresiuni informatice caracteristice: ransomware, infectarea cu malware de tip infostealer, cryptojacking, phishing

Profesionalizarea grupărilor de criminalitate organizată cu preocupări în sfera criminalității informatice a determinat includerea acestora în documente strategice la nivel național și european, nivelul de risc al infracțiunilor cibernetice fiind unul ridicat.

Evoluția criminalității informatice și profesionalizarea actorilor au dus la apariția conceptului de *„crime-as-a-service”* ce presupune externalizarea capabilităților tehnice și umane ale grupărilor de criminalitate organizată în vederea comiterii de agresiuni informatice în favoarea unor terți, în schimbul unor beneficii patrimoniale.

În perioada 2020-2021, raportat la perioada similară anterioară, a fost constată o creștere de aproximativ 120% a atacurilor cibernetice lansate asupra unor resurse informatice ale MAI și ale personalului propriu, majoritatea dintre acestea vizând extragerea neautorizată de date.

3.3. Grupări hacktiviste/actori lone wolf

Tipuri de agresiuni informatice caracteristice: DDoS, defacement, infectarea cu malware de tip infostealer și spyware, spear-phishing

Dezvoltarea tehnologică a creat posibilitatea dublării realității sub forma unei variante virtuale și crearea de echivalente elementelor societății. Un astfel de exemplu este reprezentat de transferul mișcărilor activiste în mediul online. Echivalentul fenomenul activist în spațiul virtual poartă denumirea de hacktivism.

Hacktivism-ul reprezintă un fenomen de manifestare a unor acțiuni motivate ideologic sub forma unor agresiuni cibernetice menite să compromită/perturbe sistemele informatice utilizate de entități publice și private considerate ca fiind generatoare ale unor nemulțumiri sociale.

Conform analizelor efectuate cu privire la amenințările identificate, atacurile atribuite fenomenului hacktivist ocupă o pondere mare, astfel de atacuri fiind lansate asupra resurselor web ale structurilor MAI cu expunere publică semnificativă, pe fondul unor nemulțumiri sociale.

Hacktiviștii desfășoară în principal agresiuni cibernetice de un nivel de complexitate redus prin lansarea de atacuri de tip *defacement* și *DDoS* asupra unor resurse web gestionate de entități publice și private, în scopul promovării în spațiul public a unor mesaje motivate ideologic.

Întrucât activitatea acestor actori este intensificată în momente de criză (socială, economică, de ordine publică) coroborat cu rolul instituțional al ministerului în gestionarea acestora, resursele web ale MAI sunt considerate ținte prioritare pentru promovarea dezideratelor acestor entități.

Totodată, în scopul susținerii obiectivelor proprii, aceste grupări vizează compromiterea unor resurse informatice în cadrul cărora sunt vehiculate informații nedestinate publicității în vederea publicării pe rețeaua Internet.

3.4 Grupări/indivizi cu viziuni teroriste/extremiste

Tipuri de agresiuni informatice caracteristice DDoS, defacement, infectarea cu malware de tip infostealer

Deși conceptul de terorism cibernetic a fost intens analizat și dezbătut în doctrina de specialitate, acesta reprezintă o noțiune pur teoretică, nefiind identificate în practică cazuri care să confirme posibilitatea realizării unor astfel de atacuri.

Entitățile teroriste/extremiste au în preocupări comiterea de atacuri informatice de complexitate redusă, dar generatoare de impact mediatic, în

scopul generării unei stări de neîncredere a populației în capacitatea structurilor guvernamentale de a asigura un climat de protecție optim.

Pe fondul evoluției fenomenului terorist/extremist, au fost identificate atacuri informatice lansate asupra resurselor web ale MAI, atribuite unor entități afiliate unor grupări teroriste/extremiste, ce au avut ca scop promovarea de mesaje ideologice, dar și intenții de coagulare a unor astfel de actori în vederea creșterii nivelului de complexitate a agresiunilor informatice.

În contextul dezvoltării unor concepte noi precum *crime-as-a-service*, *ransomware-as-a-service* sau *malware-as-a-service,* limitările tehnice și de expertiză ar putea fi eliminate, subzistând posibilitatea ca agresiunile generate de aceste entități să fie de nivel de complexitate ridicat.

Întrucât misiunea acestora este de a crea un climat de nesiguranță prin intermediul unor acțiuni distrugătoarea sau cu impact psihosocial, infrastructurile ministerului și cele aflate sub protecția MAI reprezintă ținte prioritare pentru astfel de agresiuni informatice motivate ideologic.

II. *Viziunea pentru 2021-2026*

Evoluția digitală reconfigurează provocările la adresa misiunilor MAI, fiind create premisele dezvoltării capabilităților tehnologice și implicit a infrastructurii IT&C prin implementarea unor soluții de nouă generație, interconectate, care să permită conjugarea eforturilor structurilor în vederea asigurării atribuțiilor instituționale.

Totodată, având în vedere rolul MAI în asigurarea unor servicii fundamentale de interes public, procesul de digitalizare a acestora se realizează în concordanță cu demersurile întreprinse la nivel național, inclusiv prin dezvoltarea de soluții de tip *cloud* interconectate cu serviciile *cloud-ului* guvernamental, aspect ce presupune provocări de securitate suplimentare.

În acest context, problematica securității cibernetice va cunoaște o diversificare accelerată a metodelor, tehnicilor și mijloacelor de asigurare a protecției infrastructurilor informatice, fapt pentru care este necesară adoptarea unor măsuri programate în baza diagnozelor și prognozelor actualizate.

Procesul de securizare a infrastructurii informatice presupune conștientizarea și asumarea unor standarde de securitate la nivel organizațional și individual prin adoptarea unei atitudini preventive și

proactive, fundamentată pe cunoașterea modului de gestionare a resurselor informatice și a amenințărilor la adresa acestora.

❖ La nivel organizațional acțiunile necesare a fi întreprinse, prin structurile specializate, vizează dezvoltarea următoarele paliere:

- **prevenire și securizare** – cunoașterea amenințărilor, vulnerabilităților și riscurilor în vederea implementării permanente a măsurilor de actualizare a politicilor de securitate;
- **monitorizare și detecție** - dezvoltarea mecanismului de indexare, detectare, investigare și analiză a incidentelor și atacurilor informatice;
- **răspuns și contracarare** – adoptarea unor măsuri proactive de răspuns la atacurile informatice;
- **documentare și atribuire** – creșterea capabilităților investigative pentru identificarea agresorilor cibernetici și atribuirea tehnică a atacurilor.

În conceptul de securitate cibernetică sunt incluse totalitatea măsurilor întreprinse în vederea prevenirii și contracarării amenințărilor din spațiul cibernetic, inclusiv în ceea ce privește nivelul culturii de securitate a personalului propriu.

❖ Astfel, la nivel individual, este necesară abordarea și asumarea următoarelor paliere:

- **cunoaștere și prevenire** – pregătirea continuă pentru cunoașterea amenințărilor, modalităților de realizare și măsurilor minime de securizare;
- **detecție și semnalare** – adoptarea unor măsuri proactive de identificare a elementelor suspecte și de raportare imediată.

Atingerea acestor deziderate se pot concretiza prin proiectarea unei noi paradigme a conceptului de securitate bazată pe intensificarea activităților de cooperare la nivel ministerial, național și internațional cu instituții similare, dar și cu entități din mediul privat și academic.

III. *Concepte, definiții și termeni*

În înțelesul prezentei strategii, termenii și expresiile de mai jos au următoarea semnificație:

infrastructura IT&C a MAI – infrastructura de tehnologia informației și comunicații a MAI, constând în sistemele informatice care gestionează informații clasificate și neclasificate, aplicațiile aferente, rețelele și serviciile de comunicații electronice;

securitate cibernetică – starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea şi non-repudierea informațiilor în format electronic, atât clasificate, cât și neclasificate, vehiculate la nivelul infrastructurii IT&C a MAI;
internet of things – ansamblul dispozitivelor inteligente de uz general, interconectate prin Internet, capabile să primească și să transmită date;
inteligența artificială – capacitatea unui sistem tehnic de a imita funcții umane, cum ar fi raționamentul, învățarea, planificarea și creativitatea în scopul de a percepe mediul în care funcționează și de a prelucra această percepție pentru a rezolva probleme și a acționa pentru atingerea unui anumit obiectiv;
machine learning – proces axat pe construirea de sisteme care pot învăța și reproduce în mod automat comportamente, în funcție de datele pe care le procesează;
blockchain – registru digital descentralizat care păstrează o listă dinamică de înregistrări;
cyber intelligence – ansamblul activităților informativ-operative de cunoaștere, documentare și monitorizare a amenințărilor incidente în spațiul cibernetic;
darknet – rețea neindexată, utilizată, în principal, în scopuri ilicite;
criza cibernetică – ansamblu de evenimente a căror manifestare afectează sau este de natură să afecteze în mod semnificativ securitatea informațiilor în format electronic;
phishing – atac informatic nedirecționat, bazat pe tehnici de inginerie socială, menit să inducă în eroare utilizatorii sistemelor informatice în vederea obținerii de date de interes;
spear-phishing – atac informatic direcționat, bazat pe tehnici de inginerie socială, menit să inducă în eroare utilizatorii sistemelor informatice în vederea obținerii de date de interes;
malware – aplicații sau programe informatice cu caracter malițios;
ransomware – atac informatic ce vizează criptarea datelor din sistemul informatic compromis și obținerea unei recompense în schimbul decriptării;
cryptojacking – atac informatic ce presupune compromiterea resurselor informatice în vederea exploatării acestora pentru producerea de criptomonede;
infostealer – program malițios dezvoltat în scopul de a sustrage în mod neautorizat date din sistemele informatice compromise;

spyware – program malițios dezvoltat pentru monitorizarea activităților derulate pe sisteme informatice;
remote access trojan (RAT) – program malițios conceput pentru obținerea accesului la distanță, neautorizat, pe sistemul informatic țintă;
distributed denial of service (DDoS) – atac informatic distribuit ce presupune transmiterea unui număr semnificativ de solicitări în vederea perturbării disponibilității serviciilor informatice;
defacement – atac informatic ce presupune compromiterea unor resurse web și modificarea conținutului acestora;
ransomware-as-a-service – externalizarea capabilităților de realizare a unor atacuri cu aplicații de tip ransomware;
malware-as-a-service – externalizarea capabilităților de realizare a unor atacuri cu aplicații malware;
igienă cibernetică – complex de măsuri asumate și realizate de utilizatorii sistemelor informatice ce contribuie la asigurarea climatului de securitate informatică.

IV. *Principii*

Transpunerea viziunii 2021-2026 prin atingerea obiectivelor de consolidare a securității cibernetice la nivelul MAI, se va realiza în acord cu următoarele principii:

1. Principiul responsabilității - Securitatea cibernetică, ca parte componentă a securității naționale, este responsabilitatea tuturor entităților MAI, de la nivel de unități la personal individual

Întrucât nivelul de amenințare generat de agresiunile cibernetice este unul ridicat, cu impact semnificativ, tratarea securității cibernetice ca parte componentă a securității naționale este fundamentală, în special pentru stabilirea resurselor și a acțiunilor ce trebuie alocate/întreprinse pentru asigurarea unui climat optim de securitate.

Aceste activități sunt în sarcina tuturor entităților care utilizează sau administrează sisteme informatice incluse în infrastructura IT&C a MAI și vizează dezvoltarea unei culturi de securitate bazată pe prevenirea oricăror forme de vulnerabilizare a infrastructurii.

Coordonarea acestui proces este responsabilitatea structurilor specializate ce trebuie să se asigure de implementarea permanentă a politicilor de securitate, precum și de cunoașterea proactivă a riscurilor cibernetice ce vizează echipamentele aflate în administrare. Totodată, expertiza personalului structurii specializate trebuie transpusă în programe de instruire a utilizatorilor proprii.

Intensificarea utilizării Internetului extinde arealul de manifestare a vulnerabilităților, inclusiv prin compromiterea unor resurse informatice personale ale utilizatorilor pentru obținerea de informații relevante în lansarea de agresiuni cibernetice asupra resurselor oficiale.

Securitatea cibernetică presupune un proces de pregătire continuă asumat și realizat la nivelul tuturor entităților implicate prin adoptarea unor măsuri standard de igienă cibernetică și dezvoltarea unui comportament proactiv în utilizarea tehnologiilor, rețelelor și sistemelor informatice.

2. Principiul integralității - Soluțiile de securizare vor fi parte integranta a procesului de dezvoltare unitară și sustenabilă a infrastructurii IT&C a ministerului

Asumarea conceptului *"security-by-design"* vizează proiectarea și implementarea soluțiilor tehnologice la nivelul structurilor ministerului, unitar și coordonat, astfel încât modernizarea, extinderea, interconectarea resurselor informatice și securizarea acestora să se realizeze în mod operativ, asigurând eficientizarea utilizării resurselor proprii, anticiparea riscurilor și eliminarea vulnerabilităților.

Astfel, dezvoltarea infrastructurii IT&C va încorpora și soluțiile de protecție cibernetică, elaborate pe baza diagnozelor și prognozelor pe termen mediu privind oportunitățile și riscurile generate de utilizarea tehnologiilor emergente în vederea asigurării unui nivel crescut de rezilienta.

3. Principiul predictibilității - Securitatea cibernetică se bazează pe un sistem de standarde și proceduri stabilit printr-un cadru normativ clar

Cadrul intern de reglementare a politicilor și măsurilor de securitate cibernetică va fi adaptat nevoilor operaționale și evoluției digitale și în concordanță cu reglementările naționale și internaționale în vigoare.

Stabilirea unor instrucțiuni și/sau proceduri de lucru determină un proces de standardizare a securității cibernetice prin impunerea unor condiții minime.

Dinamica dezvoltării tehnologice determină diferențierea instrucțiunilor și/sau procedurilor din domeniul cibernetic, aspect susținut de nevoia de actualizare și adnotare a acestora, la intervale de timp scurte, astfel încât să fie asigurată oportunitatea la contextul actual.

4. Principiul cooperării active - Securitatea cibernetică este consolidată printr-o cooperare activă la nivel național și internațional

Securitatea cibernetică presupune conjugarea eforturilor pentru asigurarea unui climat de securitate la nivelul infrastructurilor cibernetice între toți actorii relevanți în acest domeniu. În acest sens este necesară promovarea cooperării între entitățile din mediul public, privat și academic, atât la nivel național cât și internațional.

Cooperarea vizează cunoașterea și documentarea în comun a amenințărilor, vulnerabilităților și riscurilor incidente infrastructurilor cibernetice, prin facilitatea schimbului de date, expertiză, bune practici și lecții învățate.

Caracterul de extraneitate este specific spațiului cibernetic, asigurarea securității informatice fiind potențată de cooperarea cu entități similare care activează la nivelul altor state, precum și cu organizații internaționale.

Schimbul de know-how și investigarea în comun a agresiunilor informatice complexe reprezintă instrumente esențiale în procesul de implementare a valorilor promovate de statele *liked-minded* la nivelul Organizației Națiunilor Unite cu privire la adoptarea și impunerea unui comportament responsabil în spațiul cibernetic.

MAI este reprezentat în mod activ în grupurile de reprezentare națională din cadrul structurilor și inițiativelor majore pe plan internațional legate de acțiunile din domeniul digital și al securității cibernetice susținând politica de consolidare a poziției României în calitate de centru de excelentă și actor relevant pentru securitatea cibernetică europeană și internațională.

5. Principiul profesionalizării - Prevenirea și combaterea amenințărilor la adresa securității cibernetice presupun asigurarea permanentă a unui corp de specialiști cu un nivel ridicat de expertiză în domeniul de referință.

Pregătirea profesională a personalului propriu reprezintă un element fundamental al procesului de asigurare a securității cibernetice, fiind necesară actualizarea permanentă a cunoștințelor de specialitate și abilităților tehnice în scopul consolidării cunoașterii privind complexitatea amenințărilor în spațiul virtual și anticipării noilor modalități de manifestare a acestora.

De asemenea, cooperarea interinstituțională la nivel național și internațional, precum și cu mediul academic, privat și de cercetare permite schimbul de bune-practici și cunoașterea permanentă a noilor tehnologii, metode și tehnici utilizate pentru creșterea nivelului de răspuns la incidente de securitate cibernetică.

6. Principiul protejării valorilor și drepturilor fundamentale - În asigurarea securității cibernetice este garantată respectarea drepturilor și libertăților fundamentale ale cetățenilor, precum și protejarea libertăților individuale și a datelor cu caracter personal

Protecția drepturilor fundamentale este un aspect orizontal, care afectează toate domeniile societății. În spiritul protejării și respectării drepturilor și valorilor fundamentale ale omului, toate organismele implicate în asigurarea securității cibernetice trebuie să urmărească proporționalitatea măsurilor adoptate, astfel încât acestea să nu determine limitări sau îngrădirii ale unor drepturi și libertăți.

Asigurarea proceselor de securitate cibernetică presupune respectarea, promovarea și protejarea exercițiului drepturilor omului și a libertăților fundamentale, în special în ceea ce privește libertatea de opinie, libertatea de exprimare, dreptul de a accesa și de a primi informații, precum și protejarea datelor cu caracter personal și a dreptului la viață privată, atât în mediul online, cât și offline.

V. *Obiective și direcții de acțiune ale Strategiei*

1. Configurarea unei infrastructuri IT&C sigure și reziliente

Pentru proiectarea unui climat de securitate cibernetică optim este necesară adoptarea unor măsuri unitare, standardizate și coordonate care să permită o dezvoltare durabilă a infrastructurii IT&C conform nevoilor operaționale ale MAI.

Ținând cont de principiul necesității de a cunoaște, suveranitatea asupra bazelor de date și sistemelor informatice proprii și rolul distinct al fiecărei structuri în gestionarea domeniului de competență, dar și de nevoia de interconectare tot mai ridicată a elementelor de infrastructură IT&C în scopul creșterii capacității de reacție a ministerului, asigurarea eficientă a protecției rețelelor și sistemelor informatice se poate realiza doar printr-o abordare integrată a tehnologiilor utilizate, inclusiv în privința soluțiilor de securitate cibernetică.

Direcții de acțiune:

1.1. Consolidarea capabilităților de prevenire, monitorizare, detectare și răspuns la incidentele de securitate cibernetică

Pentru întărirea capacității administrative în domeniul protecției resurselor informaționale proprii, la nivelul MAI a fost creat un cadru unitar de colectare și corelare a evenimentelor de sistem și de detectare, raportare, monitorizare și investigare în timp real a alertelor și incidentelor de securitate IT.

În contextul diversificării și creșterii substanțiale a atacurilor desfășurate de actori ostili prin exploatarea spațiului cibernetic, pentru reducerea unor riscuri la adresa confidențialității, integrității, disponibilității, autenticității și non-repudierii informațiilor gestionate prin intermediul sistemelor informatice și de comunicații ale MAI este necesară dezvoltarea și adaptarea permanentă a capabilităților de prevenire, monitorizare, detectare și raportare a alertelor de securitate cibernetică, care să permită un răspuns optim la orice formă de manifestare a amenințărilor cibernetice.

1.2. Consolidarea mecanismului de raportare a incidentelor de securitate IT

Un sistem centralizat al managementului de raportare a incidentelor de securitate IT creează imaginea de ansamblu asupra amenințării cibernetice la adresa unei infrastructuri, a unui domeniu de activitate și chiar a securității naționale.

Viziunea integrată a incidentelor de securitate IT conferă posibilitatea evaluării și punctării unor situații de criză cibernetică în vederea angrenării resurselor necesare pentru asigurarea unui răspuns proporțional și remedierii vulnerabilităților identificate.

1.3. Alocarea eficientă a resurselor financiare, tehnologice și umane

Dezvoltarea unitară și coordonată a capabilităților cibernetice conferă posibilitatea gestionării eficiente a tuturor resurselor utilizate în acest sens prin limitarea diversificării nevoilor operaționale, în funcție de tehnologiile utilizate.

Acest aspect este reliefat și în oportunitatea dezvoltării unor programe tematice de pregătire profesională a personalului implicat în activități de mentenanță și securizare a rețelelor și sistemelor informatice.

Cunoașterea elementelor ce stau la baza rețelelor și sistemelor informatice utilizate în cadrul unei infrastructuri unitare favorizează transferul rapid de expertiză în situații critice.

Totodată, asigurarea resurselor financiare reprezintă o prioritate pentru sustenabilitatea proiectelor finanțate din fonduri interne/externe și a tehnologiilor deja implementate în raport cu evoluțiile amenințărilor cibernetice.

2. Standardizarea activităților de securitate cibernetică

Standardizarea activităților prin instituirea unor standarde, instrucțiuni și proceduri de lucru este esențială pentru consolidarea nivelului de securitate cibernetică a ministerului. Astfel, fiecare entitate implicată în acest proces va avea delimitate atribuțiile specifice în scopul creșterii capacității de răspuns în situații de criză de securitate cibernetică.

Direcții de acțiune:

2.1. Actualizarea cadrului normativ intern

Unul dintre principalele elemente care condiționează îndeplinirea obiectivelor de securitate cibernetică este reprezentat de asigurarea unui cadru normativ adaptat în permanență evoluțiilor tehnologice și armonizat cu reglementările în materie, la nivel național și internațional.

Stabilirea unui cadru normativ intern care să reglementeze limitele spațiului cibernetic al MAI, rolul și atribuțiile structurilor, modul de evaluare și gestionare a vulnerabilităților și incidentelor de securitate elimină eventuale lacune identificate în procesul de securitate cibernetică la nivel operațional, tactic și strategic.

2.2. Elaborarea de proceduri și instrucțiuni de lucru specifice

Elaborarea și implementarea unor instrucțiuni/proceduri de lucru adaptate realității operaționale determină reducerea timpului de reacție în

situația unor incidente de securitate și uniformizarea metodelor și tehnicilor de lucru utilizate pentru remedierea acestora.

De asemenea, standardizarea măsurilor dispuse în vederea prevenirii amenințărilor, remedierii incidentelor și asigurării răspunsului atacurilor cibernetice favorizează posibilitatea efectuării unui audit obiectiv în baza căruia va fi stabilit impactul incidentului/atacului asupra infrastructurii IT&C și eficiența măsurilor dispuse.

Instrucțiunile/procedurile de lucru trebuie reanalizate anual sau ori de câte ori este nevoie, în vederea adaptării acestora evoluției tehnologice și a mediului securitar.

3. Prevenirea și contracararea amenințărilor, precum și diminuarea riscurilor incidente în spațiul cibernetic al MAI

Dezvoltarea continuă a noilor tehnologii informatice - condiție sine qua non a construcției mediului informațional - are un impact major asupra sistemului social, generând modificări concrete asupra mediilor fundamentale.

Practic, în stadiul actual, accesul facil la noile tehnologii IT&C, în special cele conectate la Internet, reprezintă una dintre principalele premise pentru dezvoltarea fiabilă a societății moderne.

Totodată trebuie avute în vedere noile riscuri și amenințări la adresa securității, derivate din inovarea sectorului IT&C, mare parte dintre acestea fiind amenințări și riscuri clasice transpuse în mediul virtual, dar și noi forme de manifestare hibride, cauzate chiar de apariția unor noi soluții informatice menite să dezvolte calitatea serviciilor publice.

Importanța modului de contracarare a amenințărilor incidente spațiului cibernetic al ministerului este corelată direct cu menținerea nivelului de reziliență necesar pentru furnizarea serviciilor esențiale oferite de minister societății.

Agresivitatea amenințărilor potențată de complexitatea metodelor și tehnicilor utilizate raportat la gradul de digitalizare existent, obligă structurile ministerului cu responsabilități în asigurarea securității cibernetice la adoptarea unui set complex de măsuri tehnice și non-tehnice pentru combaterea acestora în vederea diminuării factorilor de risc.

Direcții de acțiune:

3.1. Dezvoltarea capabilităților de cyber intelligence

Intensificarea activităților ilicite derulate de factorii generatori de riscuri în cadrul rețelei *Darknet* și a forumurilor frecventate de persoane cu preocupări în sfera criminalității informatice determină necesitatea unei abordări proactive pentru prevenirea și contracararea amenințărilor, precum și reducerea riscurilor cibernetice incidente în spațiul MAI.

Prevenirea și contracararea elementelor perturbatoare în infrastructura IT&C presupune o abordare integrată, realizată atât prin mijloace de detecție tehnice, cât și prin activități de informații în scopul consolidării cunoașterii și identificării timpurii a amenințărilor, vulnerabilităților și factorilor de risc care caracterizează mediul de securitate cibernetică al MAI.

Dezvoltarea capabilităților în domeniul *cyber intelligence* presupune o abordare unitară și integrată susținută de cooperarea cu entități din mediul privat și academic implicate în activități similare.

3.2. Dezvoltarea unor capabilități proactive de apărare în scopul prevenirii și combaterii amenințărilor cibernetice la adresa infrastructurii IT&C

Creșterea continuă a gradului de complexitate a agresiunilor cibernetice, în contextul digitalizării societății, determină necesitatea consolidării capabilităților investigative în vederea identificării și atribuirii tehnice a atacurilor la adresa infrastructurii IT&C a MAI, pentru a putea fundamenta o eventuală decizie de expunere și condamnare în spațiul public, respectiv de a asigura probele necesare tragerii la răspundere a persoanelor implicate în realizarea atacurilor.

Abordarea proactivă a apărării cibernetice are avantajul conturării unei posturi de descurajare prin creșterea costului realizării agresiunii cibernetice pentru atacator, respectiv prin implementarea unui sistem de avertizare timpurie și răspuns adecvat.

4. Profesionalizarea personalului de specialitate și dezvoltarea unei culturi de securitate cibernetică în rândul personalului MAI

Securitatea informatică este dependentă de existența unei culturi de securitate ce vizează cunoașterea și asumarea unor norme minime de securitate și igienă cibernetică. Dezvoltarea unei culturi de securitate este un proces pe termen mediu și lung și constă în promovarea unei concepții și formarea unor atitudini proactive, bazate pe reguli, ce au ca scop prevenirea, identificarea și raportarea incidentelor/atacurilor informatice.

Direcții de acțiune:

4.1. Derularea unor programe de conștientizare și consolidare a culturii de securitate cibernetică în rândul utilizatorilor finali

Factorul uman continuă să reprezinte cea mai vulnerabilă componentă a sistemului de securitate cibernetică, aspect cauzat de lipsa unei culturi de securitate în rândul utilizatorilor finali, privind utilizarea resurselor informatice instituționale și personale.

Inițierea și derularea unor programe privind conștientizarea efectelor nefaste ale agresiunilor cibernetice la nivelul utilizatorilor de sisteme informatice va permite creșterea culturii de securitate și adoptarea unor comportamente preventive, concomitent cu reducerea incidentelor de securitate cibernetică.

4.2. Dezvoltarea unor programe de formare/specializare a specialiștilor în domeniul securității cibernetice

Este necesară dezvoltarea unor programe de pregătire pentru personalul care desfășoară activități în domeniul securității cibernetice, în sensul consolidării nivelului de expertiză tehnică, în raport cu evoluția amenințărilor și dezvoltarea tehnologică.

Cooperarea cu instituțiile de învățământ publice și private, în vederea dezvoltării unor programe educaționale de pregătire a personalului responsabil de securitatea infrastructurii IT&C a MAI, reprezintă un element important pentru asigurarea resursei umane specializate, în contextul fluxului mare de personal existent pe piața de muncă din domeniu IT&C.

Rolul acestor programe de învățământ vizează specializarea personalului propriu în funcție de specificul și nevoile operaționale ale ministerului, pe baza unor materiale teoretice și exerciții practice personalizate.

Totodată, în cooperare cu instituțiile de învățământ și formare din cadrul ministerului, autoritatea în domeniul securității cibernetice va asigura instruirea practică a personalului de specialitate pentru formarea expertizei necesare gestionării eficiente a unei crize de securitate cibernetică.

4.3. Constituirea unui centru de excelență ministerial în domeniul securității cibernetice

Actualizarea nivelului de expertiză a personalului ministerului implicat în activități subsumate securității cibernetice vizează inclusiv acumularea de

deprinderi practice, prin intermediul unor exerciții de prevenire și contracarare a unor atacuri malițioase simulate în spațiul virtual.

Exercițiile practice au un rol proactiv în asigurarea rezilienței, reprezentând cadrul în care pot fi testate și îmbunătățite capabilitățile de răspuns, mecanismele de intervenție rapidă, procedurile de cooperare în cazul unor atacuri sau incidente de securitate cibernetică.

Centrul de excelență în domeniul securității cibernetice va asigura expertiza și suportul logistic pentru organizarea unor aplicații practice, complexe, adaptate nevoilor operaționale, precum și cadrul necesar pentru derularea de activități pe linia cercetării și inovării în domeniul securității informației în format electronic.

5. Dezvoltarea unui mecanism de răspuns în situații de criză de securitate cibernetică

Gestionarea corespunzătoare a unei situații de criză de securitate cibernetică la adresa infrastructurii IT&C a MAI, presupune elaborarea și implementarea unui mecanism de răspuns bazat pe o abordare unitară și coordonată a tuturor structurilor afectate.

Direcții de acțiune:

5.1. Dezvoltarea de instrucțiuni și politici de gestionare a crizelor cibernetice

Având în vedere nivelul de risc și gradul de complexitate ale evenimentelor subsumate unei crize de securitate cibernetică, precum și amplitudinea impactului asupra resurselor informatice gestionate la nivelul ministerului, este necesară conceperea unui set de politici și instrucțiuni care să faciliteze un răspuns proporțional din partea structurilor MAI.

5.2. Constituirea Celulei ministeriale de răspuns în situații de criză de securitate cibernetică

În general, crizele, de orice natură, reclamă necesitatea unui răspuns rapid și ferm în scopul blocării imediate/eliminării factorilor generatori, evaluării resurselor compromise și repunerii în funcțiune a serviciilor afectate.

Constituirea unei celule de răspuns la crize de securitate cibernetică are rolul de a facilita adoptarea eficientă a deciziilor la nivel înalt și coordonarea integrată a reacției instituționale și acțiunilor de restabilire a stării de normalitate.

Componența celulei de criză trebuie să fie flexibilă și să includă cel puțin reprezentanții structurilor ministerului afectate de criza de securitate cibernetică, coordonarea urmând a fi asigurată de Centrul de Răspuns al MAI la Incidente de Securitate IT (CERT-INT). În funcție de complexitatea crizei, nivelul de decizie va fi ridicat până la nivelul ministrului afacerilor interne.

6. Consolidarea cooperării naționale și internaționale în domeniul securității cibernetice

Direcții de acțiune:

6.1. Dezvoltarea cooperării intra/interinstituționale și asigurarea unui mediu eficient de schimb de informații

Includerea în procesul de elaborare a unei strategii în domeniul securității a conceptului „security by sharing" reprezintă o recunoaștere a valorii adăugate pe care o oferă cooperarea, partajarea cunoașterii, respectiv a responsabilității instituționale. Un prim beneficiu este dat de posibilitatea adresării în comun a provocărilor de securitate în condiții de eficiență sporită în ceea ce privește viteza/forța de reacție și alocarea resurselor.

Consolidarea cooperării în domeniul securității cibernetice trebuie să conducă la activități de pregătire și documentare comună a unor riscuri și amenințări cu impact inclusiv în planul securității naționale (ex. acțiuni de spionaj cibernetic), la utilizarea unor sisteme comune de avertizare timpurie a riscurilor de securitate cibernetică, precum și la îmbunătățirea procedurilor comune de lucru la nivel intra și interinstituțional;

6.2. Asigurarea unei prezențe constante în formule de cooperare internațională, dedicate prevenirii și combaterii amenințărilor cibernetice.

Creșterea capacității de reacție instituțională este condiționată de nivelul de îmbunătățire a schimbului de informații și cooperării cu autoritățile și structurile similare din alte state, organismele și agențiile internaționale ale UE, NATO, ONU, etc., având în vedere nevoia permanentă de actualizare a cunoașterii privind noile moduri de operare ale agresorilor cibernetici, precum și metodele și instrumentele de lucru utilizate pentru prevenirea și contracararea amenințărilor la adresa infrastructurilor IT&C.

VI. Schimbări preconizate

La finalul perioadei de implementare a Strategiei, instituțiile responsabile vor consolida mecanismul de prevenire și contracarare a agresiunilor cibernetice, în regim integrat, capabil să asigure un răspuns adecvat în raport cu evoluția acestui fenomen.

De asemenea, prin implementarea obiectivelor Strategiei, aceste instituții vor avea personal cu un nivel de pregătire mult mai ridicat, precum și dotările tehnice necesare combaterii agresiunilor cibernetice complexe și colectării dovezilor necesare atribuirii tehnice a acestora.

VII. Instituții responsabile

Implementarea prezentei Strategii presupune un efort conjugat al tuturor unităților, instituțiilor și structurilor din cadrul Ministerului Afacerilor Interne, în limitele stabilite prin actele normative în vigoare și în concordanță cu responsabilitățile concret stabilite prin Planul de acțiune pentru punerea în aplicare a Strategiei.

VIII. Implicații bugetare

În vederea îndeplinirii obiectivelor prezentei Strategii vor fi avute în vedere, surse de finanțare din fonduri externe, precum și surse de finanțare de la bugetul de stat, în limita sumelor aprobate anual pentru această destinație.

IX. Implicații asupra cadrului juridic

Consolidarea intervenției împotriva agresiunilor cibernetice ar putea implica, după caz, elaborarea și adoptarea unor acte normative sau intervenția unor evenimente legislative de modificare/completare/abrogare a unor acte normative în vigoare, incidente domeniului securității cibernetice, după cum se menționează în cadrul *Obiectivului 2 - Standardizarea activităților de securitate cibernetică*, respectiv după cum ar putea rezulta în mod implicit din implementarea tuturor celorlalte obiective, ca fiind necesar.

De asemenea, punerea în aplicare a măsurilor preconizate în prezenta strategie, va putea implica și adoptarea de acte administrative cu caracter normativ la nivelul instituțiilor MAI responsabile.

X. Monitorizarea și evaluarea Strategiei

În contextul implementării Strategiei, va fi desfășurat procesul de monitorizare a realizării acțiunilor și evaluare a rezultatelor obținute.

Implementarea Strategiei se realizează sub coordonarea Direcției Generale de Protecție Internă a Ministerului Afacerilor Interne.

Procesul de monitorizare și evaluare vine să asigure că direcțiile de acțiune ale Strategiei sunt urmărite și că îndeplinirea măsurilor indicate duc la atingerea obiectivelor și viziunii formulate în cadrul acestui document programatic.

În context, obiectivele procesului de monitorizare sunt:

- cunoașterea progreselor înregistrate în implementarea *Strategiei Ministerului Afacerilor Interne de securitate a informațiilor în format electronic;*
- identificarea și corectarea eventualelor probleme practice apărute în procesul de implementare a obiectivelor strategice;
- elaborarea unor rapoarte de evaluare cu un grad ridicat de precizie.

Stadiul implementării Strategiei va fi evaluat de către Direcția Generală de Protecție Internă, pe baza rapoartelor de monitorizare întocmite de către instituțiile responsabile, la termenele stabilite prin *Planul de acțiune pentru implementarea Strategiei.*

Evaluarea *ex-post* a impactului Strategiei va urmări să analizeze modul de utilizare a resurselor, nivelul impactului așteptat și eficiența intervențiilor în domeniu. În acest scop, vor fi evaluați factorii de succes sau de eșec, cât și sustenabilitatea rezultatelor și impactului *Strategiei Ministerului Afacerilor Interne de securitate a informațiilor în format electronic.*

Pentru o apreciere adecvată a rezultatelor Strategiei, evaluarea *ex-post* trebuie realizată după trecerea unui interval de timp de la implementare.