Plan sectorial: MSI

*Proiect****: Securitatea Cibernetică – Securitatea Reţelelor şi a Sistemelor Informatice: "Scenarii şi soluţii privind soluţionarea incidentelor de securitate – gestionarea incidentelor la nivel naţional cu potenţial impact la scară largă***"

Etapa I **– 30 Noiembrie 2015**

*Denumire etapă***: *Elaborarea studiului de identificare a celor mai bune practici privind soluţionarea incidentelor de securitate a Reţelelor şi a Sistemelor Informatice***

Rezultat: **Studiu asupra metodelor de lucru şi capabilităţilor existente la nivel naţional în ceea ce priveşte gestionarea incidentelor de securitate cibernetică*/* Site-ul proiectului**

Activităţi:

A I.1 **- Analiza asupra metodelor de lucru și capabilităților existente la nivel național în ceea ce privește gestionarea incidentelor de securitate cibernetică**

A I.2 - **Realizarea site-ului Web al proiectului**

A I.3 **- Managementul etapei**

COLECTIV DE ELABORARE

Cuprins

1. INTRODUCERE

În ultimul deceniu, odată cu creșterea diversității și importanței amenințărilor din spațiul cibernetic și a gradului de conștientizare a acestora, au fost dezvoltate diferite metodologii, proceduri și ghiduri de bune practici în ceea ce privește răspunsul la incidentele de securitate cibernetică. De asemenea, au fost dezvoltate tot mai multe tehnologii, proprietare sau libere („free", „open-source"), menite să prevină și să limiteze efectele incidentelor de securitate survenite în cadrul rețelelor și sistemelor informatice.

Majoritatea standardelor de prevenire și răspuns la incidentele de securitate cibernetică, cât și tehnologiile dezvoltate în acest scop, au în vedere sistemele informatice și rețelele dintr-un mediu bine definit, cum ar fi: sisteme informatice independente, rețele locale de calculatoare (LAN) și inter-rețele (WAN). Protejarea infrastructurilor cibernetice bine definite împotriva atacurilor este facilitată de faptul că, de obicei, acestea sunt administrate de aceeași organizație, respectă aceleași standarde tehnologice și respectă politici de securitate comune.

Gestionarea incidentelor de securitate cibernetică la nivel național, spre deosebire de cazul infrastructurilor cibernetice din medii bine definite, se caracterizează printr-un grad ridicat de complexitate, datorat unui cumul de factori: imposibilitatea definirii de granițe statale în mediul cibernetic, standarde tehnologice și de securitate ne-uniforme, infrastructuri cibernetice utilizate în sectoare economice diferite, proprietari diferiți și, nu în ultimul rând, atribuții împărțite între mai multe autorități naționale.

La nivelul UE sunt întreprinse demersuri în privința adoptării unei strategii europene pentru securitatea cibernetică, care să armonizeze eforturile statelor membre în abordarea provocărilor de securitate din spațiul cibernetic și protecția infrastructurilor informatice critice. Totodată, la nivelul UE, s-a conturat necesitatea adoptării unei politici privind lupta împotriva criminalității informatice. Inițiativele subsecvente au pornit de la constatarea creșterii numărului de infracțiuni informatice, a tot mai amplei implicări a grupurilor de criminalitate organizată în criminalitatea informatică, precum și a necesității unei coordonări a eforturilor europene în direcția combaterii acestor acte. Având în vedere că atacurile cibernetice pe scară largă, bine coordonate și direcționate către infrastructurile cibernetice critice ale statelor membre, constituie o preocupare crescândă a UE, întreprinderea de acțiuni pentru combaterea tuturor formelor de criminalitate informatică, atât la nivel european, cât și la nivel național, a devenit o necesitate stringentă.

Statul Român, în concordanță cu demersurile inițiate la nivelul Uniunii Europene și NATO, „își asumă rolul de coordonator al activităților desfășurate la nivel național pentru asigurarea securității cibernetice". Mai mult, România recunoaște existența amenințărilor cibernetice și „susține o abordare comună, integrată și coordonată, atât la nivelul NATO, cât și la nivelul UE, pentru a putea oferi un răspuns oportun la atacurile cibernetice".

1.1 Scopul proiectului

Scopul proiectului constă în identificarea unor soluții, atât cu caracter tehnic cât și procedural, pentru îmbunătățirea capabilităților naționale de gestionare a incidentelor de securitate cibernetică cu impact la scară largă.

1.2 Obiectivele şi fazele proiectului

În vederea realizării scopului propus, proiectul va avea următoarele obiective specifice:

1. Analiza asupra metodelor de lucru și capabilităților existente la nivel național în ceea ce privește gestionarea incidentelor de securitate cibernetică;

   Prin acest obiectiv se urmărește analizarea prevederilor actelor normative naționale în vigoare care reglementează domeniul securității cibernetice în vederea identificării instituțiilor cu responsabilități în domeniu, atribuțiile și capabilitățile acestora și modul în care se realizează schimbul de informații.

2. Studiu asupra modelelor adoptate la nivel internațional sau la nivel european;

   Prin acest obiectiv se urmărește studierea modelelor adoptate la nivel internațional în ceea ce privește gestionarea incidentelor de securitate cibernetică, dar și a experienței acumulate prin intermediul exercițiilor cibernetice și a situațiilor întâmpinate de alte state. Un exemplu elocvent și utilizat deja ca exemplu la nivel internațional este reprezentat de atacurile cibernetice suferite de Estonia în anul 2007, situație în urma căreia acest stat a adoptat o serie de măsuri și a dezvoltat capabilități de contracarare a agresiunilor cibernetice.

3. Definirea unui framework/metodologie pentru gestionarea incidentelor de securitate cibernetică la nivel național;

   Metodologia va detalia cele patru componente majore agreate deja la nivel internațional cu privire la gestionarea incidentelor de securitate cibernetică: Detecția, Trierea, Analiza și Aplicarea măsurilor de răspuns. Practic, se va defini modul de realizare a acestor etape la nivel național.

4. Dezvoltarea și implementarea unui proiect pilot care să conțină o soluție integrată de management al incidentelor de securitate.

În vederea demonstrării modului în care pot fi puse în practică rezultatele proiectului (studii, analize, metodologie etc.) se va dezvolta și implementa o soluție tehnică pilot integrată care să permită realizarea managementului incidentelor de securitate cibernetică la nivel național.

Etapele de realizare ale proiectului stabilite a se realiza pe toată durata cercetării sunt următoarele:

Nr. crt.	**Anul**	**Denumire faza/activităţi**	**Termen de predare**
1	2015	***Elaborarea studiului de identificare a celor mai bune practici privind soluţionarea incidentelor de securitate a Reţelelor şi a Sistemelor Informatice***	**30.11.2015**
2	2016	***Definirea standardelor tehnice pentru gestionarea incidentelor la nivel naţional. Structurarea şi gestionarea într-o concepţie unitară a incidentelor la nivel naţional cu potenţial impact la scară largă***	**29.11.2016**
3	2017	***Realizarea unor scenarii şi soluţii privind soluţionarea incidentelor de securitate (planuri de acţiune destinate asigurării securităţii cibernetice)***	**30.11.2017**

1.3 Obiectivele fazei actuale

Principalul obiectiv al acestei faze se concretizează în analizarea prevederilor actelor normative naționale în vigoare care reglementează domeniul securității cibernetice în vederea identificării instituțiilor cu responsabilități în domeniu, atribuțiile și capabilitățile acestora și modul în care se realizează schimbul de informații.

S-au analizat, printre altele, următoarele acte normative, documente și capabilități:

- Strategia Națională de Securitate Cibernetică a României, aprobată prin H.G. 271/2013;
- H.G. 494/2011 privind înființarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO;
- Setul de politici publice pentru combaterea criminalității informatice, rezultate ca livrabile ale proiectului Sistemul Național de Combatere a Criminalității Informatice "Cyber Crime" – Cod SMIS 37595, implementat de CERT-RO;
- Proiectul pilot al Sistemului Național de Alertă Timpurie dezvoltat de CERT-RO, prevăzut prin H.G. 494/2011.

1.4 Rezumatul fazei actuale

În cadrul fazei actuale intitulată „**Elaborarea studiului de identificare a celor mai bune practici privind soluţionarea incidentelor de securitate a Reţelelor şi a Sistemelor Informatice**" se face analiza asupra metodelor de lucru și capabilităților existente la nivel național în ceea ce privește gestionarea incidentelor de securitate cibernetică.

Raportul de cercetare elaborat în această fază cuprinde 5 capitole principale, un capitol de concluzii, anexe şi un capitol cu bibliografie.

Pentru atingerea obiectivelor fazei, în cadrul **capitolului 1** „Introducere" sunt oferite informaţii referitoare la scopul proiectului, obiectivele şi schema de realizare a proiectului.

Capitolul 2 oferă informaţii despre cadrul legislativ naţional. Capitolul începe prin a menţiona scopul, obiectivele şi principiile Strategiei de Securitate Cibernetică a României. Conform strategiei, eforturile pentru asigurarea securității cibernetice la nivel național se vor focaliza pe următoarele direcții de acțiune

1. Stabilirea cadrului conceptual, organizatoric și de acțiune necesar asigurării securității cibernetice;

2. Dezvoltarea capacităților naționale de management al riscului în domeniul securității cibernetice și de reacție la incidente cibernetice în baza unui program național;
3. Promovarea și consolidarea culturii de securitate în domeniul cibernetic;
4. Dezvoltarea cooperării internaționale în domeniul securității cibernetice.

În continuare sunt oferite informaţii despre Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică (CERT-RO). Este prezentată activitatea acestuia care se concentrează pe realizarea **prevenirii**, **analizei**, **identificării** și **reacției la incidente** în cadrul infrastructurilor cibernetice ce asigură funcționalități de utilitate publică ori asigură servicii ale societății informaționale. Sunt prezentate şi atribuţiile CERT-RO cât şi comitetul de coordonare al acestuia.

Secţiunea 3 a capitolului 2 prezintă Strategia Naţională privind Agenda Digitală pentru România 2020 ce vizează în mod direct sectorul TIC. O parte dintre obiectivele stabilite de Agenda Digitală Europeană au fost preluate și adaptate la contextul actual din România, în măsura în care acestea sunt relevante și aliniate la viziunea strategică TIC a României pentru perioada 2014 - 2020. Scopul acestei acțiuni este de a asigura dezvoltarea TIC a României la nivelul țărilor din regiune, de a stabili premisele integrării României, din punct de vedere TIC, în piața unică digitală a Europei.

Ultima secţiune a acestui capitol prezintă legislaţia naţională în domeniul criminalităţii informatice. Sunt prezentaţi indicatorii de criminalitate informatică a căror definire s-a făcut pe baza informațiilor de natură statistică colectate în prezent de principalele entități implicate în asigurarea protecției utilizatorilor în fața activității de criminalitate informatică, Institutul National de Statistică precum și de organisme Europene sau Internaționale cu preocupări în domeniu.

Tot aici sunt detaliate şi politicile publice pentru combaterea criminalităţii informatice.

Capitolul 3 prezintă „Metode de gestionare a incidentelor de securitate cibernetică la nivel naţional" şi începe cu oferirea de informaţii referitoare la Sistemul Naţional de Securitate Cibernetică (SNSC) care funcționează ca un mecanism unitar și eficient de relaționare și cooperare interinstituțională, în vederea adoptării și aplicării cu celeritate a deciziilor.

Este prezentată coordonarea unitară a SNSC care se realizează de către **Consiliul operativ de securitate cibernetică (COSC)** iar la nivel strategic, activitatea SNSC este coordonată de Consiliul Suprem de Apărare a Țării (CSAT) care avizează Strategia de securitate cibernetică a României și aprobă Regulamentul de organizare și funcționare al Consiliului operativ de securitate cibernetică (COSC).

De asemenea sunt detaliate structurile specializate de răspuns la incidente de securitate cibernetică şi oferite informaţii despre procedura CERT-RO de gestionare a incidentelor de securitate cibernetică. Activitatea de răspuns la incidente de securitate cibernetică se bazează pe primirea de alerte de către CERT-RO, respectiv semnalări asupra identificării unor incidente sau evenimente de securitate cibernetică. Acestea pot fi transmise prin orice mijloc, de către orice entitate (persoană fizică sau juridică), atât timp cât se asigură confidențialitatea comunicării, iar datele transmise sunt coerente și complete.

În **Capitolul 4** sunt descrise capabilităţile existente la nivel naţional pentru gestionarea incidentelor de securitate cibernetică. Subcapitolele care constituie acest capitol sunt:

- Tehnologii şi soluţii de securitate şi
- Sistemul de alertă timpurie şi informare în timp real al CERT-RO;

În spațiul cibernetic național, securitatea rețelelor și sistemelor informatice este asigurată prin utilizarea unor tehnologii consacrate, prin implementarea de proceduri și politici de securitate organizaționale și prin intermediul sistemelor implementate de autoritățile naționale cu atribuții în acest sens.

Capitolul 5 oferă noţiuni de proiectare şi realizare a site-ului de prezentare, arhitectura paginilor web şi conţinutul asociat. Capitolul include, de asemenea, şi informaţii despre administrarea site-ului proiectului.

Documentaţia mai cuprinde (aşa cum s-a menţionat şi în capitolul *Introducere)* un capitol de concluzii, anexe şi un capitol cu bibliografia şi referinţele utilizate în activitatea de cercetare. Anexele conţin listele de figuri, tabele şi acronime.

2. CADRUL LEGISLATIV NAŢIONAL

În prezent, România nu dispune de o lege a securității cibernetice, însă în ultimii ani au fost intensificate eforturile de adoptare a unei asemenea legi. Astfel, o primă inițiativă de adoptare a unei legi a securității cibernetice a existat în anul 2014, însă aceasta a fost declarată neconstituțională de către Curtea Constituțională a României. În anul 2015 au fost reluate eforturile de elaborare a unei noi forme a legii securității cibernetice.

De asemenea, în România nu a fost încă desemnată o autoritate națională în domeniul securității cibernetice. Se așteaptă ca noua formă a legii securității cibernetice să stabilească inclusiv una sau mai multe autorități naționale în domeniul securității cibernetice, cum de altfel s-a încercat și prin inițiativa de lege din anul 2014.

Cu toate acestea, multe aspecte referitoare la asigurarea securității cibernetice a României, gestionarea incidentelor de securitate cibernetică și instituțiile cu atribuții în acest domeniu, sunt reglementate prin:

- **H.G. nr. 494 din 2011**, privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO și
- **H.G. nr. 271 din 2013**, prin care a fost aprobată "Strategia de securitate cibernetică a României" și "Planul de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică".

2.1 Hotărârea de Guvern nr. 271/2013 – Strategia de Securitate Cibernetică a României

Strategia de securitate cibernetică a României pornește de la prezentarea contextului care a generat de fapt nevoia elaborării unui astfel de document, făcând referire la dezvoltarea rapidă a tehnologiilor moderne, caracteristicile spațiului cibernetic (lipsa frontierelor, dinamism şi anonimat), beneficiile informatizării la nivelul societății moderne, dar și la vulnerabilitățile introduse.

Scopul Strategiei de securitate cibernetică a României este de a defini și de a menține un mediu virtual sigur, cu un înalt grad de reziliență și de încredere, bazat pe infrastructurile cibernetice naționale, care să constituie un important suport pentru securitatea națională și buna guvernare, pentru maximizarea beneficiilor cetățenilor, mediului de afaceri și ale societății românești, în ansamblul ei. De asemenea, Strategia urmărește îndeplinirea obiectivului național de securitate privind "asigurarea securității cibernetice", cu respectarea principiilor și caracteristicilor Strategiei naționale de apărare și Strategiei naționale de protecție a infrastructurilor critice.

Obiectivele Strategiei de securitate cibernetică a României sunt:

a) adaptarea cadrului normativ și instituțional la dinamica amenințărilor specifice spațiului cibernetic;

b) stabilirea și aplicarea unor profile și cerințe minime de securitate pentru infrastructurile cibernetice naționale, relevante din punct de vedere al funcționării corecte a infrastructurilor critice;

c) asigurarea rezilienței infrastructurilor cibernetice;

d) asigurarea stării de securitate prin cunoaşterea, prevenirea și contracararea vulnerabilităților, riscurilor și amenințărilor la adresa securității cibernetice a României;

e) valorificarea oportunităților spațiului cibernetic pentru promovarea intereselor, valorilor și obiectivelor naționale în spațiul cibernetic;

f) promovarea și dezvoltarea cooperării între sectorul public și cel privat în plan național, precum și a cooperării internaționale în domeniul securității cibernetice;

g) dezvoltarea culturii de securitate a populației prin conștientizarea fată de vulnerabilitățile, riscurile și amenințările provenite din spațiul cibernetic și necesitatea asigurării protecției sistemelor informatice proprii;

h) participarea activă la inițiativele organizațiilor internaționale din care România face parte în domeniul definirii și stabilirii unui set de măsuri destinate creșterii încrederii la nivel internațional privind utilizarea spațiului cibernetic.

Una dintre problemele identificate de majoritatea experților în domeniul securității cibernetice este cea legată de lipsa sau ne-uniformitatea terminologiei în acest domeniu. Pornind de la acest aspect, Strategia de securitate cibernetică a României conține un întreg capitol în care sunt definite diferite concepte și termeni, astfel:

- **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 pro-active 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 pro-active 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;

- **apărare cibernetică** - acțiuni desfășurate în spațiul cibernetic în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor și asigurării răspunsului oportun împotriva amenințărilor asupra infrastructurilor cibernetice specifice apărării naționale;

- **operații în rețele de calculatoare** - procesul complex de planificare, coordonare, sincronizare, armonizare și desfășurare a acțiunilor în spațiul cibernetic pentru protecția,

controlul și utilizarea rețelelor de calculatoare în scopul obținerii superiorității informaționale, concomitent cu neutralizarea capabilităților adversarului;

- **amenințare cibernetică** - circumstanță sau eveniment care constituie un pericol potențial la adresa securității cibernetice;

- **atac cibernetic** - acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică;

- **incident cibernetic** - eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică;

- **terorism cibernetic** - activitățile premeditate desfășurate în spațiul cibernetic de către persoane, grupări sau organizații motivate politic, ideologic ori religios ce pot determina distrugeri materiale sau victime, de natură să determine panică ori teroare;

- **spionaj cibernetic** - acțiuni desfășurate în spațiul cibernetic, cu scopul de a obține neautorizat informații confidențiale în interesul unei entități statale sau non-statale;

- **criminalitatea informatică** - totalitatea faptelor prevăzute de legea penală sau de alte legi speciale care prezintă pericol social și sunt săvârșite cu vinovăție, prin intermediul ori asupra infrastructurilor cibernetice;

- **vulnerabilitatea în spațiul cibernetic** - slăbiciune în proiectarea și implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente care poate fi exploatată de către o amenințare;

- **riscul de securitate în spațiul cibernetic** - probabilitatea ca o amenințare să se materializeze, exploatând o anumită vulnerabilitate specifică infrastructurilor cibernetice;

- **managementul riscului** - un proces complex, continuu și flexibil de identificare, evaluare și contracarare a riscurilor la adresa securității cibernetice, 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 cibernetice;

- **reziliența infrastructurilor cibernetice** - capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic și de a reveni la starea de normalitate;

- **entități de tip CERT** - structuri specializate în înțelesul art. 2 lit. a) din Hotărârea Guvernului nr. 494/2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO.

Referitor la asigurarea securității cibernetice, Strategia de securitate cibernetică a României definește 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 și europene;

- **diseminarea** - asigurarea transferului de informații, expertiză și bune practici în scopul protejării infrastructurilor cibernetice;

- **protejarea valorilor** - politicile de securitate cibernetică vor asigura echilibrul între nevoia de creștere a securității în spațiul cibernetic și prezervarea dreptului la intimitate și alte valori și libertăți fundamentale ale cetățeanului;

- **asumarea responsabilității** - toți deținătorii și utilizatorii de infrastructuri cibernetice trebuie să întreprindă măsurile necesare pentru securizarea infrastructurilor proprii și să nu afecteze securitatea infrastructurilor celorlalți deținători sau utilizatori;

- **separarea rețelelor** - reducerea probabilității de manifestare a atacurilor cibernetice, specifice rețelei internet, asupra infrastructurilor cibernetice care asigură funcțiile vitale ale statului, prin utilizarea unor rețele dedicate, separate de internet.

Conform strategiei, eforturile pentru asigurarea securității cibernetice la nivel național se vor focaliza pe următoarele direcții de acțiune:

1. Stabilirea cadrului conceptual, organizatoric și de acțiune 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 cooperării între sectorul public și cel privat, inclusiv prin stimularea schimbului reciproc de informații, privind amenințări, vulnerabilități, riscuri, precum și cele referitoare la 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 amenințărilor și minimizarea riscurilor asociate utilizării spațiului cibernetic;
   - asigurarea unor instrumente de dezvoltare a cooperării dintre sectorul public şi cel privat, în domeniul securității cibernetice, inclusiv pentru crearea unui mecanism eficient de avertizare și alertă, respectiv de reacție la incidentele cibernetice;
   - stimularea capabilităților naționale de cercetare-dezvoltare și inovare în domeniul securității cibernetice;
   - creșterea nivelului de reziliență a infrastructurilor cibernetice;
   - dezvoltarea entităților de tip CERT, atât în cadrul sectorului public, cât și în sectorul privat;

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 amenințările, vulnerabilitățile și riscurile specifice utilizării spațiului cibernetic;

- dezvoltarea de programe educaționale, în cadrul formelor obligatorii de învățământ, privind utilizarea sigură a internetului și a echipamentelor de calcul;
- formarea profesională adecvată a persoanelor care își desfășoară activitatea în domeniul securității cibernetice 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 cibernetice
   - încheierea unor acorduri de cooperare la nivel internațional pentru îmbunătățirea capacității de răspuns în cazul unor atacuri cibernetice majore;
   - participarea la programe internaționale care vizează domeniul securității cibernetice;
   - promovarea intereselor naționale de securitate cibernetică în formatele de cooperare internațională la care România este parte.

2.2 Hotărârea de Guvern nr. 494/2011 privind înființarea CERT-RO

Activitatea CERT-RO se concentrează pe realizarea **prevenirii**, **analizei**, **identificării** și **reacției la incidente** în cadrul infrastructurilor cibernetice ce asigură funcționalități de utilitate publică ori asigură servicii ale societății informaționale.

CERT-RO reprezintă un **punct național de contact** cu structurile de tip CERT care funcționează în cadrul instituțiilor sau autorităților publice ori al altor persoane juridice de drept public sau privat, naționale ori internaționale, cu respectarea competențelor ce revin celorlalte autorități și instituții publice cu atribuții în domeniu, potrivit legii.

CERT-RO are următoarele atribuții:

a) oferă servicii publice de tip preventiv, de tip reactiv și de consultanta;

b) organizează și întreține un sistem de baze de date privind amenințările, vulnerabilitățile și incidentele de securitate cibernetică identificate sau raportate, tehnici și tehnologii folosite pentru atacuri, precum și bune practici pentru protecția infrastructurilor cibernetice;

c) asigură cadrul organizatoric și suportul tehnic necesar schimbului de informații dintre diverse echipe de tip CERT, utilizatori, autorități, producători de echipamente și soluții de securitate cibernetică, precum și furnizori de servicii în domeniu;

d) organizează, desfășoară sau participă la activități de instruire în domeniul securității cibernetice;

e) organizează simpozioane, dezbateri pe teme de securitate cibernetică și asigură diseminarea unor informații specifice prin mass-media;

f) desfășoară activități de cercetare-dezvoltare în domeniu și elaborează proceduri și recomandări privind securitatea cibernetică, potrivit prevederilor legale privind cercetarea științifică și dezvoltarea tehnologică;

g) asigură MCSI suportul tehnic și de specialitate pentru elaborarea politicilor de securitate cibernetică necesar a fi respectate de furnizorii de rețele și servicii de comunicații electronice publice pentru obținerea autorizării de funcționare a acestora, precum și la evaluarea modului de implementare a acestora;

h) asigură consultanță de specialitate autorităților publice responsabile, stabilite conform Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, aprobată cu modificări prin Legea nr.18/2011, cu privire la produsele și sistemele de securitate cibernetică care deservesc infrastructurile critice naționale și europene;

i) asigură puncte de contact pentru colectarea sesizărilor și a informațiilor despre incidente de securitate cibernetică atât automatizat, cât și prin comunicare directă securizată, după caz;

j) identifică, analizează și clasifică incidentele de securitate din cadrul infrastructurilor cibernetice, conform ariei de competență;

k) elaborează propuneri pe care le înaintează către MCSI sau Consiliului Suprem de Apărare a Țării, denumit în continuare CSAT, privind modificarea cadrului legislativ în vederea stimulării dezvoltării securității infrastructurilor cibernetice ce asigură funcționalități de utilitate publică ori asigură servicii ale societății informaționale;

l) planifică și programează în proiectul de buget propriu resursele financiare necesare în vederea realizării politicilor în domeniile sale de competență;

m) coordonează derularea proiectelor, ale căror beneficiari sunt MCSI și/sau instituțiile din subordinea acestuia, cu finanțare națională sau internațională în domeniul securității infrastructurilor cibernetice ce asigură funcționalități de utilitate publică, ori asigură servicii ale societății informaționale, care vizează capacitatea instituțională operațională a CERT-RO;

n) asigură MCSI suportul tehnic și de specialitate pentru urmărirea și controlul aplicării prevederilor cuprinse în actele normative în vigoare sau în acordurile internaționale în domeniul de competență şi notifică organele competente pentru demararea procedurilor legale în vederea cercetării și sancționării, după caz.

Una dintre atribuțiile importante CERT-RO este aceea de a stabili „criteriile și cerințele minime pe care trebuie să le îndeplinească un centru de tip CERT pentru a fi inclus în **Comunitatea CERT din România**, precum și procedurile de colaborare", prin decizie a directorului general CERT-RO, cu avizul Comitetului de coordonare.

Comitetul de coordonare al CERT-RO, al cărui președinte este chiar directorul instituției, este format din reprezentanți ai următoarelor instituții:

a) Ministerul pentru Societatea Informațională;

b) Ministerul Apărării Naționale;

c) Ministerul Administrației și Internelor;

d) Serviciul Român de Informații;

e) Serviciul de Informații Externe;

f) Serviciul de Telecomunicații Speciale;

g) Serviciul de Protecție și Pază;

h) Oficiul Registrului Național al Informațiilor Secrete de Stat;

i) Autoritatea Națională pentru Administrare și Reglementare în Comunicații.

CERT-RO prezintă un raport anual în cadrul CSAT, în timp ce activitatea instituției este analizată semestrial în Comitetul de coordonare, pe baza raportului elaborat în acest sens de către directorul general.

2.3 Strategia Națională privind Agenda Digitală pentru România - 2020

Strategia Națională privind Agenda Digitală pentru România vizează în mod direct sectorul TIC, şi își propune să contribuie la dezvoltarea economică și creșterea competitivității României, atât prin acțiuni directe precum dezvoltarea efectivă a sectorului TIC românesc cât și prin acțiuni indirecte, precum creșterea eficienței și reducerea costurilor sectorului public din România, îmbunătățirea productivității sectorului privat prin reducerea barierelor administrative în relația cu statul, prin îmbunătățirea competitivității forței de muncă din România și nu numai.

Pentru susținerea redresării economice a Europei, dar mai ales pentru asigurarea unei creșteri economice sustenabile, inteligente și care să promoveze incluziunea socială, Uniunea Europeană a elaborat Agenda Digitală cu obiectivul principal de a dezvolta Piața Unică Digitală.

O parte dintre obiectivele stabilite de Agenda Digitală Europeană au fost preluate și adaptate la contextul actual din România, în măsura în care acestea sunt relevante și aliniate la viziunea strategică TIC a României pentru perioada 2014 - 2020. Scopul acestei acțiuni este de a asigura dezvoltarea TIC a României la nivelul țărilor din regiune, de a stabili premisele integrării României, din punct de vedere TIC, în piața unică digitală a Europei.

O dezvoltare pozitivă în domeniul securităţii cibernetice este constituirea CERT-RO, care este punctul de contact național pentru structuri similare şi este responsabil pentru dezvoltarea şi distribuirea politicilor publice de prevenire şi combatere a incidentelor care au loc în infrastructura națională cibernetică.

De asemenea, strategia de securitate cibernetică a României adoptată prin Decizia nr. 271/2013 stabilește obiectivele, principiile şi principalele direcții de acțiune pentru înțelegerea, prevenirea şi împiedicarea amenințărilor, vulnerabilităților şi riscurilor de securitate cibernetică şi promovează interesele, valorile şi obiectivele naționale ale României în spațiul cibernetic. Strategia şi planul de acțiune urmăresc stabilirea de obiective pentru securitatea cibernetică și liniile de acțiune pentru anii ce vin. Abordarea românească este aliniată la liniile directoare propuse de Comisia Europeană în Agenda Digitală şi Pilonul III – Încredere şi Siguranță – precum şi la progresul altor State membre ale Uniunii Europene.

Tema "Securitate rețelelor și a sistemelor informatice" este o prioritate reală atât a Comisiei Europene cât și a structurilor naționale. Conştientizarea, probleme cum ar fi virușii sau malware-ul, cum se utilizează parolele, ingineria socială, cum se utilizează calculatorul acasă, cum se folosesc "mediile de socializare", cum se lucrează în afara biroului, trimiterea şi primirea de emailuri,

utilizarea mașinilor de fax şi a tuturor tipurilor de structuri de date sunt priorități importante ale structurilor naționale ce au responsabilități în domeniu.

Sistemul național de securitate cibernetică (SNSC) este cadrul general pentru cooperare ce aduce împreună autoritățile şi instituțiile publice cu responsabilități şi capacități în domeniu, pentru a coordona acțiunile naționale pentru securitatea cibernetică, inclusiv cooperarea cu academia şi asociațiile comerciale economice şi organizațiile non guvernamentale / ONG-uri.

Centrul Național de reacţie la incidentele de securitate cibernetică - CERT-RO este o structură de expertiză, cercetare şi dezvoltare în domeniul protejării infrastructurii cibernetice, sub coordonarea Ministerului pentru Societatea Informațională, care are capacitatea de a preveni, analiza, identifica şi răspunde la incidentele de securitate cibernetică ale sistemelor informatice.

Dezvoltarea cooperării dintre sectorul public şi sectorul privat pentru a asigura securitatea cibernetică reprezintă o prioritate pentru acțiune la nivel național, dat fiind că spațiul cibernetic include infrastructura cibernetică deținută şi gestionată atât de Stat cât şi de entitățile private.

În prezent, instituțiile din cadrul Sistemului Național de Securitate Cibernetică creează, la nivelul instituțiilor publice, cadrul tehnic şi operațional pentru a asigura interoperabilitatea dintre componentele siguranței informatice pentru a proteja infrastructura cibernetică din cadrului publicului şi mări disponibilitatea şi nivelul de încredere în serviciile publice specializate furnizate cetățenilor, întreprinderilor şi Guvernului.

Agenda Digitală pentru România stabileşte următoarele linii strategice de dezvoltare:

- Stabilirea cadrului conceptual şi organizațional necesar pentru securitatea cibernetică;
    - Constituirea şi operaționalizarea sistemului național de securitate cibernetică;
    - Îmbunătățirea legislației;
    - Consolidarea parteneriatului dintre sectorul public şi cel privat;
- Dezvoltarea capacităților naționale pentru managementul riscului în securitatea cibernetică şi răspunsul la incidentele cibernetice în cadrul unui program național;
    - Constituirea de baze de date cu informații relevante;
    - Intensificarea capacităților de cercetare / dezvoltare în domeniul securității cibernetice;

- Infrastructura securităţii cibernetice;
- CERT-RO;
- Implementarea standardelor de securitate cibernetică;
- Cooperarea inter-instituțională;

- Promovarea şi consolidarea culturii privind securitatea în domeniul cibernetic;
  - Dezvoltarea programelor de conștientizare publică în administrația publică şi în sectorul privat;
  - Dezvoltarea de programe educaționale;
  - Formare;
- Dezvoltarea cooperării internaționale în domeniul securităţii cibernetice;
  - Încheierea de acorduri de cooperare internațională pentru îmbunătățirea capacității de răspuns în cazul atacurilor cibernetice majore;
  - Participarea în programe şi exerciții internaționale în domeniul securității cibernetice;
  - Promovarea intereselor României în domeniul siguranței naționale în cadrul instituțiilor de cooperare internațională în care România este membru.

2.4 Legislaţia naţională în domeniul criminalităţii informatice

Legislația nationala în domeniul criminalității informatice este compusă din:

- Legea nr.161/ 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției, TITLUL III - Prevenirea şi combaterea criminalității informatice;
- Legea nr. 365/2002 privind comerțul electronic.

Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, prin implementarea proiectului "Sistemul național de combatere a criminalității informatice Cyber Crime", Cod SMIS 37595, finanțat din Fondul Social European, prin Programul Operațional

Dezvoltarea Capacității Administrative 2007-2013, a urmărit, printre altele, realizarea următoarelor obiective:

- Stabilirea principalilor indicatori de performanță utilizați în evaluarea gradului de criminalitate informatică la nivel național și analiza lor la momentul începerii proiectului în comparație cu nivelul de referință al Uniunii Europene;
- Corelarea și actualizarea reglementărilor și actelor normative din domeniu prin definirea unui set de politici publice, acte normative și proceduri în vederea combaterii criminalității informatice.

2.4.1 Indicatori de criminalitate informatică

Definirea indicatorilor s-a făcut pe baza informațiilor de natură statistică colectate în prezent de principalele entități implicate în asigurarea protecției utilizatorilor în fața activității de criminalitate informatică, Institutul National de Statistică precum și de organisme Europene sau Internaționale cu preocupări în domeniu. Documentul include, de asemenea, propuneri de indicatori care nu sunt colectați în acest moment dar sunt considerați relevanți și se recomandă preluarea și urmărirea lor în viitor.

Documentul nu își propune să stabilească o definiție a criminalității informatice, pe parcursul său criminalitatea informatică trebuie considerată în accepțiunea legislației naționale din România.

Pentru elaborarea documentului au fost culese informații din surse deschise, s-au utilizat informații proprietare ale unor instituții, disponibile comercial, și au avut loc întâlniri de lucru cu secretariatul tehnic al CERT-RO si grupul de experti cooptat de CERT-RO in acest moment.

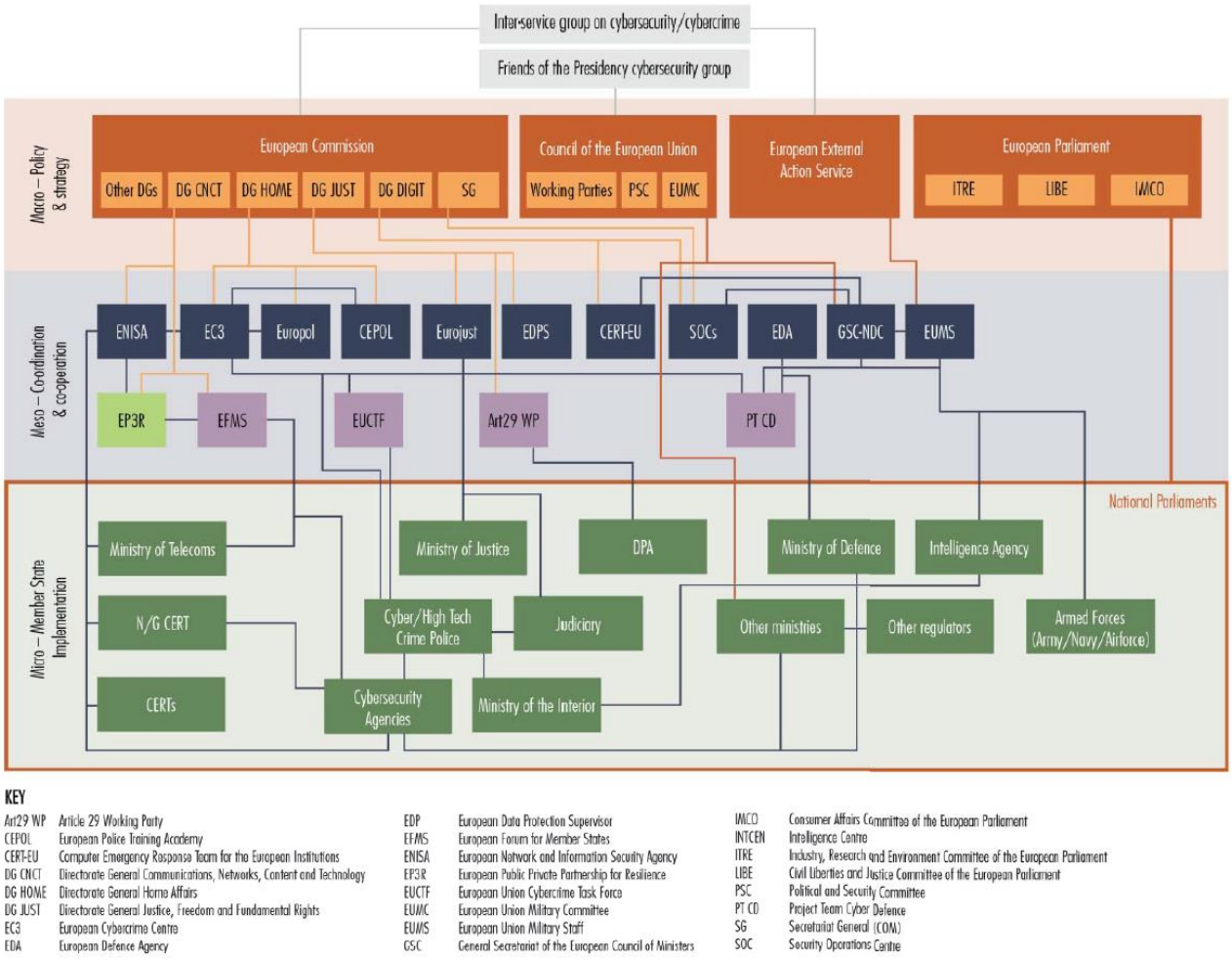
Au fost analizate următoarele tipuri de informații:

- datele de natură statistică culese la nivel național de la instituțiile cu atribuții în domeniu (instituții din subordinea MAI, CERT-RO si INS);
- documente furnizate de CERT-RO;
- date publicate de ITU-ONU;
- date publicate de Banca Mondială;
- date publicate de Forumul Economic Mondial;
- documentația existentă la nivelul Uniunii Europene și în special provenind de la Eurostat;
- tendințele în domeniul criminalității informatice.

Din analiza acestor date reiese faptul că, la fel ca și în cazul definirii criminalității informatice, nu există o abordare unanim acceptată nici la nivel european și nici la nivel mondial. Nu există o instituție care să coordoneze acest domeniu și care să traseze direcția ce trebuie urmată.

Lipsa coordonării și lipsa unei direcții unanim recunoscute se datorează, pe de o parte, faptului că domeniul criminalității informatice este nou și a fost abordat diferit atât la nivelul fiecărui stat cât și la nivelul instituțiilor cu responsabilități din statul respectiv. Fiecare instituție s-a adaptat din mers pentru a răspunde cât mai bine provocărilor. Acest lucru îngreunează interoperabilitatea și definirea unui cadru unitar deoarece ar impacta major modul de lucru curent al fiecărei instituții. Pe de altă parte, chiar dacă s-a demarat stabilirea unui cadru comun la nivelul UE, acest lucru este de durată și nu asigură modificarea completă a legislației existente în statele membre astfel încât să nu existe discrepante și piedici de cooperare. Singura variantă fezabilă este stabilirea unui nivel de bază la care să se raporteze statele membre.

Harta realizata de RAND Europe și care prezintă modul în care comunică instituțiile din Europa pe tematica securității informatice este o exemplificare elocventă a acestei situații. Harta prezintă o rețea de organizații, cu legături complexe pe mai multe niveluri.



KEY

Art29 WP	Article 29 Working Party	EDP	European Data Protection Supervisor	IMCO	Consumer Affairs Committee of the European Parliament
CEPOL	European Police Training Academy	EFMS	European Forum for Member States	INTCEN	Intelligence Centre
CERT-EU	Computer Emergency Response Team for the European Institutions	ENISA	European Network and Information Security Agency	ITRE	Industry, Research and Environment Committee of the European Parliament
DG CNCT	Directorate General Communications, Networks, Content and Technology	EP3R	European Public Private Partnership for Resilience	LIBE	Civil Liberties and Justice Committee of the European Parliament
DG HOME	Directorate General Home Affairs	EUCTF	European Union Cybercrime Task Force	PSC	Political and Security Committee
DG JUST	Directorate General Justice, Freedom and Fundamental Rights	EUMC	European Union Military Committee	PT CD	Project Team Cyber Defence
EC3	European Cybercrime Centre	EUMS	European Union Military Staff	SG	Secretariat General (COM)
EDA	European Defence Agency	GSC	General Secretariat of the European Council of Ministers	SOC	Security Operations Centre

Figură 1. *Harta RAND Europe cu privire la modul în care comunică instituţiile din Europa pe tematica securităţii informatice*

Prin urmare, nu există o tendința europeană sau globală care sa fie urmată cu privire la criminalitatea informatică și stabilirea indicatorilor care o definesc. În afară de urmărirea implementării legislației definite la nivelul Uniunii Europene și a respectării convențiilor în care este parte, dar care nu ajută la stabilirea unui cadru precis, o țară membră a Uniunii Europene nu are alte linii directoare pe care să le urmeze.

Deoarece nu a fost definit încă un nivel de bază la care să se facă raportarea, cea mai bună abordare în definirea indicatorilor de criminalitate informatică din România a fost considerată:

- Reutilizarea indicatorilor existenți:
  - Analiza indicatorilor primari raportați sau calculați în prezent în România, pentru care există date;
    - Corelarea indicatorilor cu indicatori similari existenți la nivelul UE sau internațional.
  - Identificarea indicatorilor existenți la nivelul UE sau internațional pentru care există sau se pot colecta date în Romania;
  - Pentru acești indicatori se propune utilizarea metodei de calcul utilizata în prezent de către instituția ce raportează indicatorul;
- Definirea unor indicatori noi:
  - Stabilirea unor indicatori relevanți, pentru care nu există în prezent date, dar care, datorită importanței, trebuie să fie abordați în viitor;
  - Pentru acești indicatori s-a propus metoda de calcul, instituția care poate furniza datele necesare precum și frecvența culegerii datelor.

Indicatorii sunt abordați gradual, pornind de la nivelul de utilizare al computerelor și Internetului în rândul populației României și ajungând la indicatorii care determină trăsăturile infractorilor cibernetici și ale grupărilor infracționale.

Setul de indicatori de criminalitate informatică este:

1. Nivelul de utilizare al computerelor și Internetului în rândul populației;
2. Mediul online;
3. Nivelul de securitate al mediului on-line;
4. Nivelul de trasabilitate a utilizatorilor care accesează servicii on-line;
5. Dimensiunea pieței de securitate informatică;
6. Nivelul de prevenție, educație și implicare a statului în combaterea criminalității informatice;

7. Nivelul de instruire al tinerilor privind utilizarea Internetului în condiții de siguranța;
8. Capacitatea de răspuns a statului la incidente de securitate informatică;
9. Capacitatea de răspuns a statului cu privire la fenomenul criminalității informatice;
10. Infracționalitatea din domeniul informatic;
11. Impactul infracționalității informatice asupra utilizatorilor individuali;
12. Impactul infracționalității informatice asupra serviciilor de e-guvernare și e-administrație;
13. Impactul infracționalității informatice asupra mediului de afaceri online;
14. Ținte ale infractorilor cibernetici;
15. Influenta trăsăturilor infractorului cibernetic asupra criminalității informatice;
16. Trăsături ale grupărilor infracționale.

2.4.2 Politici publice pentru combaterea criminalităţii informatice

Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO a urmărit ca prin implementarea proiectului "Sistemul național de combatere a criminalității informatice Cyber Crime", Cod SMIS 37595, finanțat din Fondul Social European, prin Programul Operațional Dezvoltarea Capacității Administrative 2007-2013 să realizeze un cadru de lucru adecvat, în vederea creșterii capacității de formulare a politicilor publice și de realizare a unei mai bune reglementări și planificări strategice, prin consolidarea parteneriatelor atât la nivel inter-instituțional, cât și între instituțiile publice și reprezentanții altor domenii, interesați în combaterea criminalității informatice.

În cadrul proiectului, experți tehnici și experți în legislație și politici publice au derulat activități de analiză, documentare, suport, care s-au concretizat într-un set de propuneri de politici publice, acte normative și proceduri în vederea prevenirii și combaterii criminalității informatice.

Documentele menționate au fost supuse consultării publice în perioada mai - august 2014 în cadrul a zece întâlniri cu mediul public, privat, educațional, precum și cu reprezentanți din mediul decizional. Comentariile și observațiile formulate au fost analizate de către echipele de experți desemnate în cadrul proiectului, iar la data de 28 august 2014 a fost elaborată forma finală a setului de propuneri de politici publice, acte normative și proceduri în vederea prevenirii și combaterii criminalității informatice. Documentele au fost înaintate Guvernului spre aprobare și asumare, prin Ministerul pentru Societatea Informațională.

3. METODE DE GESTIONARE A INCIDENTELOR DE SECURITATE CIBERNETICĂ LA NIVEL NAŢIONAL

Conform Strategiei de securitate cibernetică a României, asigurarea securității cibernetice la nivel național se realizează prin intermediul **Sistemului național de securitate cibernetică (SNSC)**, reprezentând „cadrul general de cooperare care reunește autorități și instituții publice, cu responsabilități și capabilități în domeniu, în vederea coordonării acțiunilor la nivel național pentru asigurarea securității spațiului cibernetic, inclusiv prin cooperarea cu mediul academic și cel de afaceri, asociațiile profesionale și organizațiile neguvernamentale".

Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, asigură elaborarea și diseminarea politicilor publice de prevenire și contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competență.

3.1 Sistemul naţional de securitate cibernetică (SNSC)

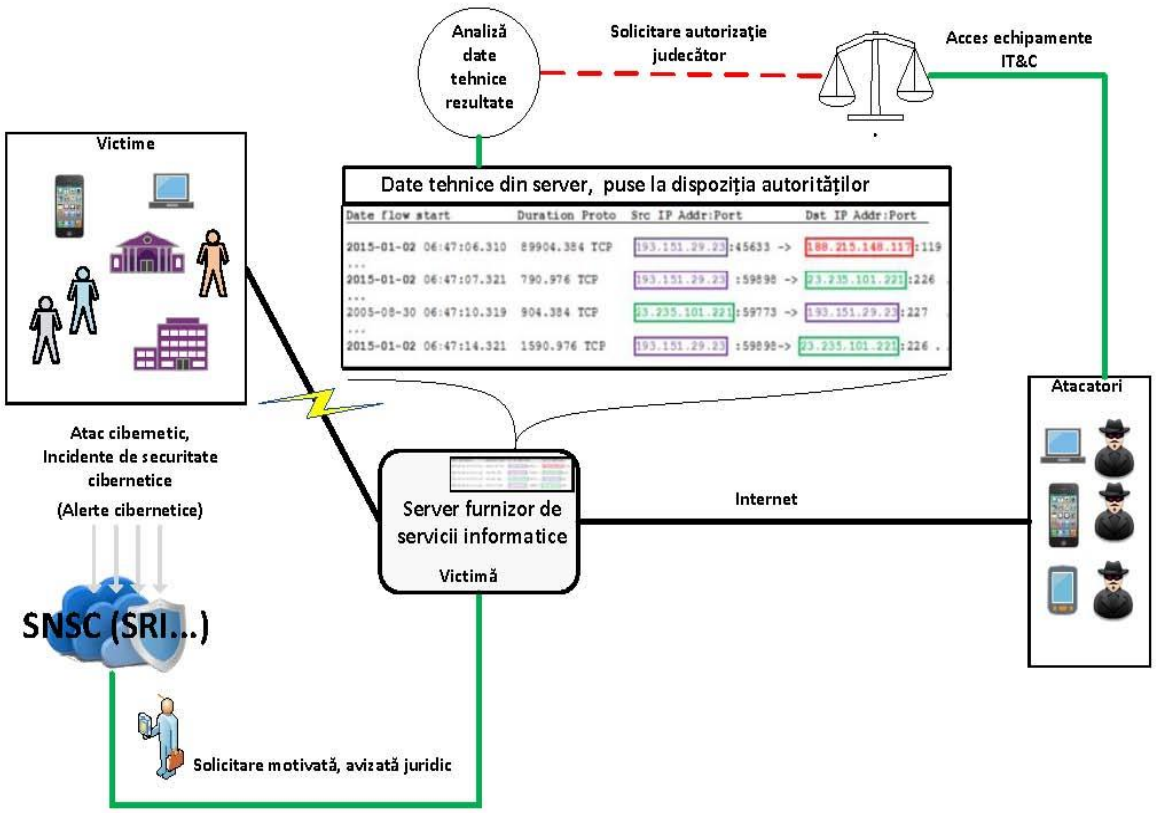
Sistemul Naţional de Securitate Cibernetică funcționează ca un mecanism unitar și eficient de relaționare și cooperare interinstituțională, în vederea adoptării și aplicării cu celeritate a deciziilor.

Coordonarea unitară a SNSC se realizează de către **Consiliul operativ de securitate cibernetică (COSC)**, din care fac parte, în calitate de membri permanenți, reprezentanți din cadrul următoarelor instituții:

- Ministerul Apărării Naționale,
- Ministerul Afacerilor Interne,
- Ministerul Afacerilor Externe,
- Ministerul pentru Societatea Informațională,
- Serviciul Român de Informații,
- Serviciul de Telecomunicații Speciale,
- Serviciul de Informații Externe,
- Serviciul de Protecție și Pază,
- Oficiul Registrului Național pentru Informații Secrete de Stat,
- secretarul Consiliului Suprem de Apărare a Țării.

La nivel strategic, activitatea SNSC este coordonată de Consiliul Suprem de Apărare a Țării (CSAT) care avizează Strategia de securitate cibernetică a României și aprobă Regulamentul de organizare și funcționare al Consiliului operativ de securitate cibernetică (COSC).

În figura de mai jos este reprezentată schematic procedura utilizată de SNSC pentru investigarea atacurilor ce implică infrastructuri din spațiul cibernetic național.



Figură 2. *Procedura SNSC de investigare a atacurilor cibernetice*[1]

Ministerul pentru Societatea Informațională are rolul de a coordona autoritățile publice care nu sunt reprezentate în COSC, în vederea realizării coerenței politicilor și implementarea strategiilor guvernamentale în domeniul comunicațiilor electronice, tehnologiei informației și al serviciilor societății informaționale și societății bazate pe cunoaștere. În plus, prin Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, asigură elaborarea și diseminarea politicilor publice de prevenire și contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competență.

[1] http://www.sri.ro/cu-privire-la-dezbaterea-publica-pe-marginea-prevederilor-legii-securitatii-cibernetice-sri-face-urmatoarele-precizari.html

3.2 Structuri specializate de răspuns la incidente de securitate cibernetică

În România, pe lângă instituțiile reprezentate în Consiliul operativ de securitate cibernetică (COSC), există și structuri specializate de răspuns la incidentele de securitate cibernetică, de tip CERT/CSIRT, atât publice cât și din mediul privat.

Între structurile publice de tip CERT din România se regăsesc:

- **CERT-RO** (Centrul Național de Răspuns la incidente de Securitate Cibernetică) – CERT național cu rol de coordonator al comunității CERT din România;
- **CERTMIL-CTP** (Centrul Tehnic Național de Răspuns la Incidente de Securitate Cibernetică) – CERT militar, din cadrul Ministerului Apărării Naționale, cu capabilități și responsabilități în domeniul apărării cibernetice;
- **RoCSIRT** – CERT academic, dedicat protejării instituțiilor conectate la rețeaua RoEduNet;
- **CERT-INT** – structură de tip CERT din cadrul Ministerului Administrației și Internelor.

În contextul desemnării de către CSAT ca autoritate națională în domeniul CyberIntelligence, SRI a constituit o structură specializată denumită **Centrul Național Cyberint**[2]. Principala misiune a Centrului Național Cyberint este corelarea sistemelor tehnice de apărare cu capacitățile informative în vederea identificării și furnizării, către beneficiarii legali, a informațiilor necesare prevenirii, stopării și/sau limitării consecințelor unei agresiunii asupra sistemelor TIC care reprezintă infrastructuri critice.

3.3 Procedura CERT-RO de gestionare a incidentelor de securitate cibernetică

Conform prevederilor H.G. nr. 494/2011 CERT-RO oferă o serie de servicii de tip pro-activ, reactiv sau de suport printre care: gestiunea incidentelor de securitate cibernetică la nivel național, transmiterea de alerte și atenționări privind apariția unor activități premergătoare atacurilor și diseminarea rezultatelor investigațiilor incidentelor de securitate cibernetică.

La baza activității de răspuns la incidente de securitate cibernetică stau următoarele principii:

1. principiul eficienței și coordonării în gestionarea situației;
2. principiul reducerii rapide la minim a efectelor incidentului/evenimentului;

[2] http://www.sri.ro/Cyberintelligence.html

3. principiul diseminării informațiilor doar către părțile afectate, părțile ce pot fi afectate sau cele cu responsabilități în domeniu;
4. principiul clasificării informațiilor conform protocolului TLP sau conform legislației naționale referitoare la protecția informațiilor clasificate;
5. principiul legalității;
6. principiul confidențialității;
7. principiul nevoii de a cunoaște;
8. principiul prevenirii evenimentelor/incidentelor de securitate în sistemele informatice și de comunicații.

O serie de obiective sunt urmărite în cadrul activității de răspuns la incidente de securitate cibernetică. Prin atingerea acestor obiective în activitatea de răspuns la incidente de securitate cibernetică, se respectă mandatul CERT-RO precum și prevederile Strategiei Naționale de Securitate Cibernetică:

1. stoparea imediată sau reducerea la minimul posibil a efectelor incidentului;
2. stabilirea preliminară a impactului incidentului/evenimentului;
3. identificarea si alertarea tuturor părților afectate sau care pot fi afectate de incidentul/evenimentul de securitate precum și a celor responsabile de remedierea situației;
4. identificarea si alertarea tuturor instituțiilor sau autorităților publice responsabile de gestionarea situației;
5. furnizarea de informații complete care să ajute părțile implicate în activitatea de răspuns la incident/eveniment;
6. furnizarea de suport tehnic pentru părțile afectate, la cerere;
7. diseminarea de documente de natură tehnică referitoare la metode de detecție și tratare ale incidentului/evenimentului de securitate, pentru alte entități ce pot fi vizate de un incident similar;
8. dezvoltarea culturii de securitate a populației prin conștientizarea față de vulnerabilitățile, riscurile și amenințările provenite din spațiul cibernetic și necesitatea asigurării protecției sistemelor informatice proprii.

Activitatea de răspuns la incidente de securitate cibernetică se bazează pe primirea de alerte de către CERT-RO, respectiv semnalări asupra identificării unor incidente sau evenimente de securitate cibernetică. Acestea pot fi transmise prin orice mijloc, de către orice entitate (persoană fizică sau juridică), atât timp cât se asigură confidențialitatea comunicării, iar datele transmise sunt coerente și complete.

O serie de etape sunt parcurse odată cu primirea alertei, astfel:

1. Înregistrarea şi investigarea inițială a alertei

Personalul responsabil cu activitatea de răspuns la alertele de securitate are obligația de a lua în considerare toate datele transmise și în orice format. Acesta va verifica corectitudinea datelor transmise și se va asigura că acestea sunt complete și se pot folosi în rezolvarea alertei.

De regulă orice alertă trebuie să conțină cel puțin următoarele date: date de identificare ale petentului; adrese IP, adrese de email, timestamp și servicii afectate ale victimei; adrese IP, adrese de email sau surse generatoare ale atacului; fișiere de tip log care să demonstreze existența și identificarea incidentului/evenimentului sau orice alte fișiere ce pot constitui probe.

În cadrul acestei etape, personalul responsabil se asigură că deține date suficiente pentru identificarea sursei atacului, a victimei și a tipului de incident/eveniment cu care se confruntă.

În cazul în care petentul nu furnizează suficiente date pentru exploatarea incidentului sau în cazul în care sursa nu este credibilă, se solicită detalii suplimentare. În lipsa detaliilor suplimentare sau a neconfirmării alertei, cazul poate fi închis direct din această etapă.

2. Identificarea entităților afectate de incident/eveniment

Pe baza informațiilor complete și corecte referitoare la alertă, personalul responsabil poate trece la identificarea entităților reale ce reprezintă sursa precum și victima incidentului/evenimentului. Acesta poate folosi orice surse disponibile public pe internet (servicii de tip whois, DNS lookup, ping, traceroute, reverse IP, diverse site-uri etc.) precum și surse cu acces restricționat disponibile în baza parteneriatelor dezvoltate de CERT-RO.

În cadrul acestei etape, este obligatorie identificarea persoanelor fizice sau juridice ce trebuie contactate pentru rezolvarea incidentului (ISP, deținători domenii .ro sau clase de adrese IP, persoane fizice juridice etc.)

3. Determinarea probabilității impactului incidentului/evenimentului pentru securitatea spațiului cibernetic național

În această etapă se face o analiză asupra impactului incidentului/ evenimentului de securitate cibernetică.

Se consideră amenințări la adresa securității naționale următoarele tipuri de alerte, concretizate de obicei în atacuri cibernetice:

a) Atacuri ce afectează o serie de instituții publice, din același domeniu de activitate sau care folosesc aceleași tehnologii;

b) Atacuri asupra mai multor organizații din același domeniu de activitate sau care folosesc aceleași tehnologii;

c) Atacuri persistente (APT) asupra instituțiilor publice sau a unor companii reprezentative în economia României;

d) Atacuri asupra unor furnizori de servicii publice online cu importanță deosebită în spațiul cibernetic românesc (ISP volum mare de trafic, magazine online, servicii de certificare, rețele sociale, sisteme de plăți online etc.);

e) Atacuri asupra unor instituții ce procesează informații clasificate sau informații de importanță deosebită pentru economia României (planuri sisteme industriale etc.);

f) Atacuri asupra infrastructurilor critice sau a operatorilor de infrastructuri critice;

g) Vulnerabilități ale unor produse IT ce pot afecta categorii aparte de utilizatori din România.

4. Identificarea instituțiilor și autorităților publice cu responsabilități în gestionarea incidentului/evenimentului.

Odată identificate sursa și victima incidentului/evenimentului se va stabili și tipul incidentului de securitate precum și metodologia de atac. În baza acestor date se va stabili dacă, pentru rezolvarea alertei, este desemnată o altă autoritate sau instituție publică. În cazul în care este identificată o astfel de autoritate, iar rezolvarea incidentul/evenimentul cade în responsabilitatea acesteia, va fi pregătită transmiterea unei alerte și către instituția responsabilă.

5. Alertarea urgentă a entităților afectate precum și a instituțiilor cu responsabilități

În momentul în care sunt colectate date suficiente despre victimă, sursa atacului, entitățile implicate, instituțiile publice responsabile, tipul de incident precum şi date care să confirme existența acestuia, personalul responsabil transmite urgent alerte de notificare către toate părțile implicate.

În cadrul activității de notificare se aplică principiile enumerate mai sus, entitatea afectată fiind prima alertată despre existența incidentului/evenimentului. În cazul în care responsabilitatea rezolvării incidentului/evenimentului cade în sarcina altei instituții/autorități, iar acea instituție/autoritate consideră necesar ca alerta să nu fie transmisă către părțile afectate, pentru a nu perturba activitățile post-incident/eveniment, atunci personalul responsabil va respecta întocmai decizia instituției/autorității.

Alertele transmise către părțile implicate trebuie să conțină următoarele informații:

- Date relevante despre CERT-RO și baza legală în urma căreia se transmit alertele;
- Date despre resursele tehnice ce fac parte din incident/eveniment (resurse afectate sau resursele ce produc atacul);
- Fișiere log, sau orice alte probe ce pot susține existența atacului;
- Măsurile exprese ce trebuie luate de către destinatarul alertei;
- Date de contact pentru comunicări ulterioare asupra incidentului/ evenimentului;
- Solicitare de feedback cu privire la măsurile luate de părțile afectate;
- Detalii despre cum au fost obținute datele despre incident/eveniment (doar în cazul în care este neapărat necesar; dezvăluirea sursei nu reprezintă un obiectiv al activității de alertare).

6. Lansarea investigației detaliate (dacă este cazul)

În cazul în care o parte afectată solicită date suplimentare despre incidentul/evenimentul de securitate, personalul responsabil contactează părțile ce pot oferi aceste informații, solicitându-le în scopul finalizării investigației.

În acest caz investigații suplimentare pot fi demarate, putând fi folosite orice surse disponibile.

7. Publicarea de documente tehnice și rapoarte asupra incidentului / evenimentului

Pentru restrângerea numărului posibilelor victime ale amenințării ce a generat incidentul de securitate, personalul responsabil transmite alerte de atenționare către toți partenerii vizați, sau chiar către publicul larg în caz că se impune.

Alertele sunt transmise prin email, notificări oficiale sau sunt publicate pe pagina de Internet a CERT-RO. Alertele conțin date relevante despre tipul amenințării, modalități de detecție precum și modalități de protecție.

8. Închiderea/clasarea alertei de securitate

Alerta de securitate este considerată închisă/clasată în momentul în care au fost alertate toate părțile responsabile precum și cele afectate (sursă și victimă), acestea confirmând primirea mesajelor și demararea activităților de remediere a problemelor. Pentru ca alerta să poată fi considerată închisă/clasată trebuie ca toate posibilitățile de acțiune ale CERT-RO să fie epuizate.

În cazul în care părțile notificate nu dau curs solicitării CERT-RO timp de o săptămână, incidentul/evenimentul este considerat închis/clasat.

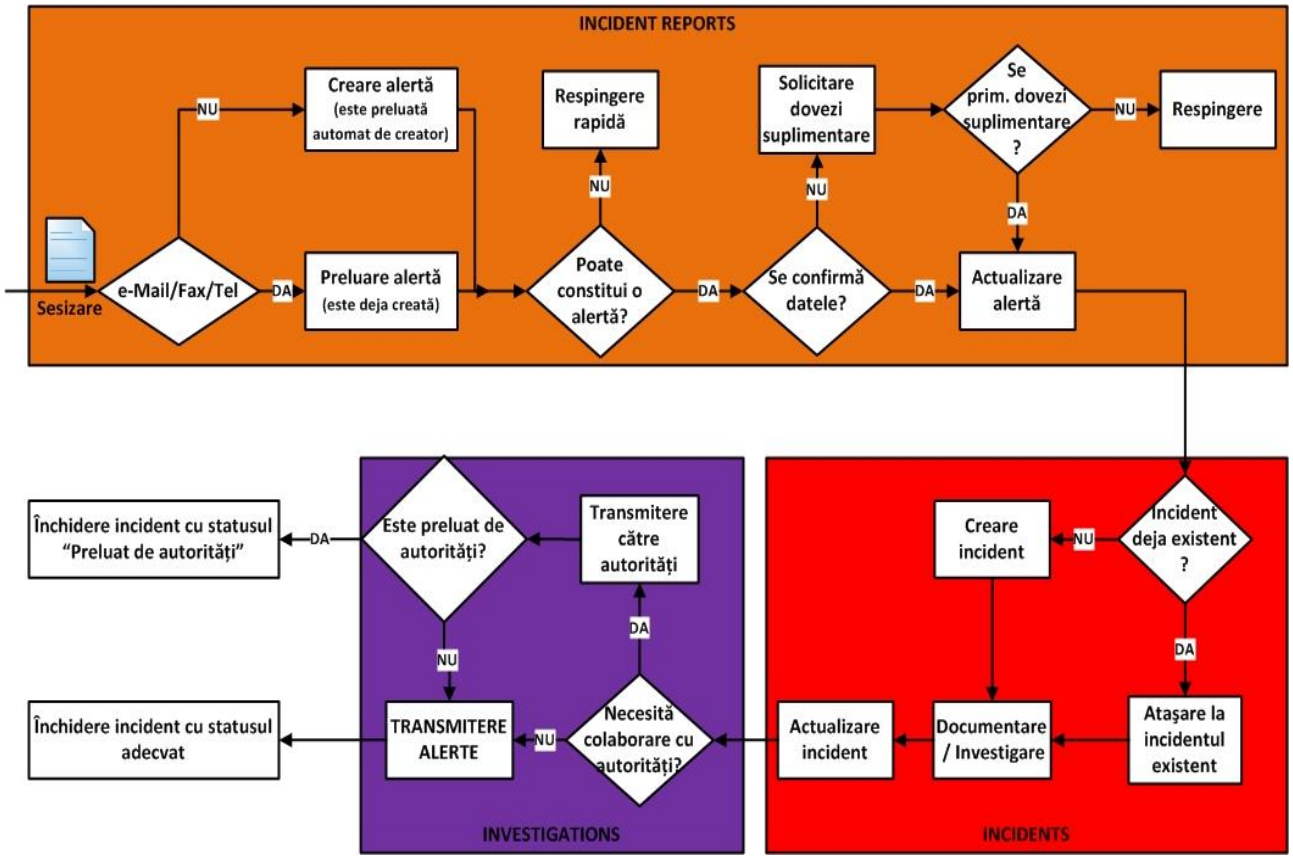
9. Automatizarea activității de răspuns la alerte de securitate cibernetică

Activitatea de răspuns la incidente de securitate cibernetică este automatizată pe cât mai mult posibil. În cazul în care alertele sunt transmise, de către un partener, într-un format standardizat, ușor accesibil, sunt dezvoltate aplicații automate care să identifice părțile implicate cât și autoritățile competente și să le transmită notificări automate sub formă de email.

Toate notificările automate transmise sunt înregistrate în cadrul sistemului de gestionare a alertelor folosit în cadrul CERT-RO.

Din punct de vedere tehnic, gestionarea evenimentelor, alertelor și incidentelor de securitate cibernetică se realizează prin intermediul unei aplicații de ticketing și a unei aplicații dezvoltate intern pentru colectarea, procesarea, normalizarea, analizarea și diseminarea informațiilor.

În figura de mai jos este prezentat un exemplu de workflow pentru gestionarea incidentelor de securitate cibernetică.



Figură 3. *Diagrama proceselor aferente gestionării incidentelor de securitate cibernetică*

4. CAPABILITĂŢI EXISTENTE LA NIVEL NAŢIONAL PENTRU GESTIONAREA INCIDENTELOR DE SECURITATE CIBERNETICĂ

În spațiul cibernetic național, securitatea rețelelor și sistemelor informatice este asigurată prin utilizarea unor tehnologii consacrate, prin implementarea de proceduri și politici de securitate organizaționale și prin intermediul sistemelor implementate de autoritățile naționale cu atribuții în acest sens.

4.1 Tehnologii şi soluţii de securitate

Cele mai utilizate tehnologii/soluții pentru asigurarea securității rețelelor și sistemelor informatice sunt următoarele:

- Antivirus/Antimalware;
- HIDS (Host Intrusion Prevention System);
- Firewall;
- NIDS (Network Intrusion Prevention System);
- IPS (Intrusion Prevention System);
- Web Application Firewall;
- Web/Email Gateway;
- DLP (Data Lost Prevention);
- VPN (Virtual Private Networks);
- UTM (Unified Threat Management);
- SIEM (Security Information and Event Management).

În prezent, nu există definite standarde de securitate la nivel național privind asigurarea securității rețelelor și sistemelor informatice utilizate în cadrul diferitelor sectoare ale economiei. De asemenea, nu există prevederi legale care să impună entităților din diferite sectoare economice respectarea anumitor standarde de securitate informatică.

În continuare sunt prezentate măsurile recomandate pentru asigurarea securității rețelelor și sistemelor informatice din cadrul unei organizații, în baza „*Codului de bune practici pentru Securitatea Sistemelor Informatice şi de Comunicaţii*", întocmit de Asociaţia Naţională pentru Securitatea Sistemelor Informatice (ANSSI), cuprinzând o serie de măsuri recomandate pentru asigurarea securităţii informatice, referindu-se la securitatea fizică, securitatea logică şi controlul accesului (securitatea personalului).

4.1.1. Securitatea fizică

a). Inventarierea echipamentelor autorizate și neautorizate

O practică frecventă a grupurilor infracționale constă în utilizarea tehnicilor de scanare continuă a spațiilor de adrese IP ale organizațiilor țintă, urmărind conectarea sistemelor noi și/sau neprotejate, ori laptop-uri cu definiții sau pachete de securitate (patch-uri) neactualizate datorită faptului că nu sunt conectate frecvent la rețea. Unul din atacurile comune profită de sistemele nou instalate și care nu sunt configurate și securizate din punct de vedere al pachetelor de securitate decât în ziua următoare, fiind ușor de identificat și exploatat prin intermediul Internetului de către atacatori. În ceea ce privește sistemele informatice aflate în interiorul rețelelor protejate, atacatorii care au obținut deja acces pot viza și compromite acele sisteme insuficient sau necorespunzător securizate.

O atenție deosebită trebuie acordată echipamentelor și sistemelor care nu sunt incluse în inventarul organizațiilor, cum ar fi diversele dispozitive mobile personale, sisteme de test, etc. și care nu sunt conectate în mod permanent la rețea. În general, aceste tipuri de echipamente tind să nu fie securizate în mod corespunzator sau să nu aibă controale de securitate care să răspunda cerințelor de securitate. Chiar dacă aceste echipamente nu sunt utilizate pentru a procesa, stoca sau accesa date sau informații critice, odată introduse în rețea, pot oferi atacatorilor o cale de acces spre alte resurse și un punct de unde pot fi lansate atacuri avansate.

Conform ghidului publicat de SANS Institute, intitulat „*Systems and Network Documentation*", menținerea unui inventar precis și actual, controlat prin monitorizare activă și managementul configurației, poate reduce șansele ca atacatorii să identifice și să exploateze sistemele neprotejate. Procedurile de inventariere stabilesc proprietarii de informații și sisteme informatice, documentând responsabilitățile pentru menținerea inventarului pentru fiecare componentă a sistemelor. În funcție de complexitatea fiecărei organizații, se pot utiliza instrumente specializate de monitorizare și inventariere a resurselor sistemelor informatice, care pot efectua "descoperirea" de noi sisteme, odată conectate la rețeaua sistemului informatic, prin intermediul datelor obținute de la echipamentele de rețea. De asemenea, se pot utiliza instrumente de identificare pasivă a resurselor (care "ascultă" în mod pasiv la interfețele de rețea echipamentele care își anunță prezența prin modificarea traficului). Aceste instrumente de monitorizare și inventariere ar trebui să includă funcționalități precum:

- Identificarea echipamentelor noi neautorizate conectate la rețea într-un interval de timp predefinit;
- Alertarea sau transmiterea mesajelor de notificare către o listă predefinită cu personal administrativ;

- Izolarea sistemului neautorizat;

b). Inventarierea aplicațiilor și sistemelor de operare autorizate și neautorizate

Grupurile infracționale utilizează tehnici de scanare a spațiilor de adrese ale organizațiilor vizate în scopul de a identifica versiuni vulnerabile de software care pot fi exploatate de la distanță. Astfel de atacuri pot fi inițiate prin distribuirea de pagini de web ostile, documente, fișiere media și alte tipuri de conținut web prin intermediul propriilor pagini web sau al altor pagini web demne de încredere. Atacurile complexe pot fi și de tipul zero-day, exploatând vulnerabilități în aceeasi zi sau înainte ca acestea sa fie cunoscute public.

Fără cunoștințele corespunzătoare sau controlul software-ului implementat în organizație, nu se poate asigura protecția necesară pentru resursele informatice. Capacitatea de inventariere și controlul neadecvat asupra programelor care sunt instalate și autorizate a rula pe echipamentele organizațiilor, fac mai vulnerabile aceste medii informatice. Astfel de echipamente inadecvat controlate sunt pasibile să execute software care nu este necesar pentru specificul activității, inducând breșe potențiale de securitate sau rulând programe de tip malware induse de către un atacator, după ce sistemul a fost compromis. Odată ce un echipament a fost exploatat, adesea este utilizat ca și un punct de plecare pentru atacuri ulterioare și pentru colectarea de informații sensibile din sistemul compromis și din alte sisteme conectate la acesta. Echipamentele vulnerabile sunt utilizate ca puncte de lansare pentru "avansarea" în rețea și rețele partenere. Organizațiile care nu utilizează inventarierea completă a pachetelor software nu vor reuși să descopere sistemele pe care rulează software vulnerabil sau malițios și mai departe să reducă problemele sau atacurile.

Software-ul comercial și instrumente specializate de inventariere a resurselor informatice sunt utilizate pe scară largă pentru a facilita verificarea simultană a aplicațiilor utilizate în organizații, extragând informații despre nivelul pachetelor de update al fiecărui program software instalat pentru a se asigura utilizarea celei mai recente versiuni.

Sistemele de monitorizare utilizate ar trebui să includă și funcționalități precum:

- Capacitatea de identificare a software-ului neautorizat prin detectarea tentativelor de instalare sau executare a acestuia;
- Alertarea personalului administrativ într-un interval de timp predefinit;
- Blocarea instalării, prevenirea executării sau trecerea în carantină.

c). Controlul echipamentelor wireless

În absența unor măsuri eficiente de securitate implementate pentru rețelele fără fir, se pot iniția atacuri care vizează în principal furtul de date importante pentru orice tip de organizație.

Deoarece rețelele fără fir nu necesită conexiuni fizice directe, echipamentele wireless oferă atacatorilor un vector convenabil pentru obținerea accesului în mediul țintă.Tehnicile de atac dezvoltate pot fi inițiate din exterior, evitandu-se perimetrele de securitate ale organizațiilor. Astfel, echipamentele portabile pot fi infectate prin exploatare la distanță în intervalul în care acestea sunt scoase din perimetrul de securitate în afara organizației și apoi utilizate ca „back doors" odată intoarse în organizație și reconectate la rețea.

Măsurile de protejare impotriva atacurilor desfășurate prin intermediul rețelelor fara fir vizează utilizarea atât a instrumentelor de scanare, detectare și decoperire a rețelelor cât și a sistemelor de detectare a intruziunilor. Echipa de securitate trebuie să efectueze captura traficului wireless desfășurat în zonele de perimetru pentru a determina dacă sunt utilizate protocoale mai permisive de transmitere sau criptare decât cele impuse. În plus, se pot utiliza instrumente de administrare de la distanță în cadrul rețelelor pentru a colecta informații despre capabilitățile wireless ale dispozitivelor conectate la sistemele administrate.

Instrumentele utilizate trebuie să includă următoarele funcționalități:

- capacitatea de a identifica configurațiile dispozitivelor autorizate sau dispozitivele wireless neautorizate din cadrul ariei de acoperire a organizației și care sunt conectate în aceste rețele;
- identificarea dispozitivelor fără fir noi, neautorizate, conectate recent;
- alertarea personalului administrativ;
- identificarea zonei și izolarea punctului de acces în rețea.

d). Proiectarea securității rețelelor

Măsurile de securitate, chiar bine implementate la nivelul sistemelor informatice, pot fi eludate în rețele concepute deficitar. Fără o arhitectura de rețea atent planificată și implementată în mod corespunzător, atacatorii pot ocoli măsurile de securitate din diferite sisteme, pătrunzând în rețea pentru a obține acces către sistemele țintă.

Atacatorii vizează în mod frecvent hărțile rețelelor pentru a identifica conexiuni neutilizate între sisteme, filtrare necorespunzătoare și rețele fără segregare. Prin urmare, o arhitectură de rețea robustă și securizată poate fi realizată prin implementarea unui proces care să furnizeze și măsurile de securitate necesare.

Pentru a se asigura un mediu robust și ușor de securizat, arhitectura fiecărei rețele trebuie să se bazeze pe modele care descriu structura generală a acesteia și a serviciilor pe care le oferă.

Organizațiile trebuie să documenteze diagrame pentru fiecare rețea în care să fie evidențiate componentele de rețea împreună cu grupurile semnificative de servere și sisteme client.

e). Limitarea și controlul porturilor de rețea, a protocoalelor de comunicație și a serviciilor

Conform ghidului publicat de SANS Institute, intitulat „*CIS Critical Security Controls - Twenty Critical Security Controls for Effective Cyber Defense*", un set de măsuri de securitate foarte important se referă la controlul comunicaţiilor şi serviciilor de reţea.

Atacurile pot fi lansate și prin intermediul serviciilor de rețea accesibile de la distanță care sunt vulnerabile în fața exploatărilor. Exemple comune includ servere web configurate neadecvat, servere de email, servicii de fișiere și imprimare, servere DNS instalate în mod prestabilit pe o varietate de echipamente, de multe ori fără a se ține cont de nevoia de business pentru serviciile oferite. Multe pachete software instalează și pornesc servicii ca parte a instalării pachetului de bază fără a informa utilizatorul sau administratorul despre faptul că serviciile au fost activate. Atacurile urmăresc descoperirea de conturi, parole sau coduri prin scanări şi încercări de exploatare a serviciilor expuse.

Asemenea tipuri de atac pot fi preîntâmpinate prin utilizarea de instrumente de scanare a porturilor pentru a determina serviciile care „ascultă" rețeaua pentru o serie de sisteme țintă. Pentru a determina porturile deschise, instrumentele de scanare pot fi configurate pentru identificarea versiunii de protocol și serviciul care „ascultă" pe fiecare port deschis descoperit. Serviciile descoperite și versiunile acestora sunt comparate cu inventarul serviciilor necesare organizației pentru fiecare echipament.

f). Protejarea zonelor de perimetru

Atacurile pot fi concentrate asupra exploatării sistemelor care pot fi accesate din Internet, inclusiv sistemele aflate în DMZ (termen derivat din „Demilitarized Zone", cunoscut și ca „perimeter networking"), cât și asupra sistemelor client (stații de lucru, laptop) care accesează conținut din Internet prin zona de perimetru a rețelei. Tehnicile de atac lansate de grupurile criminale uzează de punctele de slăbiciune din configurarea sau arhitectura perimetrului, a sistemelor de rețea și a echipamentelor client pentru a obține acces inițial în interiorul organizației. Odată obținut accesul, atacatorii vor pătrunde mai adânc în interiorul rețelei în vederea furtului sau schimbului de informații, ori de a stabili o bază pentru atacuri ulterioare împotriva sistemelor gazdă interne. În multe cazuri, atacurile apar între rețele ale partenerilor de business, uneori calificate ca și „extranet", atacurile mutându-se din rețeaua unei organizații în rețelele altor organizații, exploatând sistemele vulnerabile găzduite în perimetrele din extranet.

Pentru a controla fluxul de trafic efectuat prin rețelele de perimetru și a asigura evidențele în vederea depistării atacurilor efectuate pe sistemele compromise, protejarea zonelor de perimetru trebuie să fie multi-stratificată, utilizând echipamente și aplicații Firewall, Proxy, rețele DMZ, sisteme de prevenire și detectare a intruziunilor la nivel de rețea tip IPS și IDS, precum și filtrarea traficului în și dinspre interiorul rețelelor.

Sistemele de prevenire și detectare a intruziunilor la nivel de perimetru trebuie să includă urmatoarele caracteristici:

- să aibă capacitatea de identificare a pachetelor neautorizate/nelegitime trimise înspre sau primite dinspre o zonă sigură;
- blocarea pachetelor neautorizate/nelegitime;
- alertarea personalului administrativ.

g). Accesul fizic în locații

Asigurarea unui mediu de securitate adecvat, începe chiar de la accesul fizic în clădirile/spațiile/locațiile care trebuiesc protejate. Pentru eficientizarea sistemelor de pază și apărare împotriva pătrunderii neautorizate, măsurile de securitate fizică ar trebui cuprinse într-un Plan de securitate fizică, iar implementarea acestor măsuri să fie bazată pe principiul „apărării în adâncime", urmărindu-se stabilirea:

- spațiului care trebuie protejat;
- unor dispozitive exterioare de securitate destinate să delimiteze zona protejată și să descurajeze accesul neautorizat (gardul de perimetru, barieră fizică care protejează limitele locației, pază cu personal specializat);
- unor dispozitive intermediare de securitate destinate să descopere tentativele sau accesul neautorizat în zona protejată (sisteme de detectare a intruziunilor - SDI, iluminat, televiziune cu circuit închis - TVCI);
- unor dispozitive interioare de securitate destinate să întârzie acțiunile eventualilor intruşi (controlul accesului - electronic, electromecanic sau prin alte mijloace).

Controlul accesului personalului în zonele protejate se efectuează de personal de pază sau prin sisteme electronice, avându-se în vedere următoarele:

- accesul fiecărui angajat se realizează prin locuri anume stabilite, pe baza permisului de acces;
- permisul de acces poate specifica în clar identitatea organizației emitente sau locul în care deținătorul are acces, insă acest aspect nu este recomandat pentru zonele în care sunt

gestionate infromații clasificate (Practic la nivelul fiecărei persoane juridice care gestionează informații clasificate se pot stabili reguli suplimentare proprii privind accesul);

- pentru accesul angajaților agenților economici contractanți care efectuează diverse lucrări de reparații și întreținere a clădirilor sau mentenanță, organizațiile beneficiare vor elibera, pe baza actelor de identitate, la solicitarea reprezentanților autorizați ai agenților în cauză, documente de acces temporar.

Planul de securitate fizică cuprinde descrierea tuturor măsurilor de securitate fizică implementate pentru protecția locațiilor și poate fi structurat astfel:

- delimitarea, marcarea și configurația zonelor care trebuiesc protejate;
- sistemul de pază și apărare;
- sistemul de avertizare și alarmare;
- controlul accesului, al cheilor și combinațiilor de cifru;
- modul de acțiune în situații de urgență;
- modul de raportare, investigare și evidență a încălcării măsurilor de securitate;
- responsabilitățile și modul de implementare a măsurilor de pregătire și instruire pe linie de securitate fizică;
- responsabilitățile și modalitățile de realizare a verificărilor, inspecțiilor și controalelor sistemului de securitate;
- măsuri suplimentare de protecție fizică.

4.1.2. Securitatea logică

a). Configurații de securitate a componentelor hardware pentru echipamente mobile, stații de lucru și servere

Asupra rețelelor Internet cât și a celor interne deja compromise de atacatori, programe automate de atac informatic caută în mod constant rețele țintă pentru a găsi sisteme care au fost configurate cu software vulnerabil instalat. Configurațiile implicite sunt adesea orientate pentru a ușura exploatarea, utilizarea sistemelor, nefiind însă securizate și lăsând servicii inutile exploatabile în starea implicită a acestora. Tehnicile de atac, încearcă să exploateze în acest fel atât serviciile accesibile via rețea, cât și software-ul de navigare al clientului.

Măsurile de protecție împotriva acestor tehnici de atac includ achiziția de componente pentru sisteme și rețea cu configurații de securitate deja implementate, instalarea sistemelor preconfigurate

pentru securitate, actualizarea configurațiilor periodic și urmărirea acestora în cadrul unui sistem de management al configurațiilor.

Aceste măsuri se pot implementa prin crearea de imagini ale sistemelor și stocarea pe servere securizate împreună cu utilizarea instrumentelor de management al configurațiilor. În funcție de soluția adoptată, aceste instrumente pot monitoriza în mod activ devierile de la configurațiile implementate, furnizând informațiile necesare pentru asigurarea utilizării configurațiilor stabilite și vor include următoarele funcționalități:

- Identificarea oricăror modificări/schimbări în cadrul unei imagini securizate care pot include modificări aduse pentru fișiere cheie, porturi, fișiere de configurații sau pentru software-ul instalat;
- Compararea imaginii fiecărui sistem cu imaginea oficială stocată în mod securizat în cadrul sistemului de management al configurațiilor;
- Blocarea instalării și prevenirea executării odată cu alertarea personalului administrativ.

b). Configurații de securitate pentru echipamente de rețea – Firewall, Router, Switch

Atacatorii profită de o practică des întalnită în configurarea nivelului de securitate pe anumite echipamente de rețea: utilizatorii solicită excepții temporare din considerente specifice, de business, aceste excepții sunt aplicate dar nu și îndepărtate imediat ce necesitatea de business dispare. În unele situații și mai grave, riscul de securitate al unei astfel de excepții nu este nici analizat corespunzător nici evaluat din punct de vedere al necesității. Atacatorii caută breșele din firewall-uri, routere și switch-uri și apoi le folosesc în scopul penetrării sistemului. Atacatorii au exploatat deficiențele acestor echipamente de rețea pentru a obține accesul în mediile vizate, pentru a redirecta traficul înspre o altă rețea sau un sistem malițios ce se anunță ca un sistem de încredere, și pentru a intercepta și altera informații pe măsură ce acestea sunt transmise. Cu astfel de acțiuni atacatorul obține acces la date sensibile, alterează informații importante sau chiar utilizează un sistem compromis pentru a „poza" într-un alt sistem de încredere din rețea.

Anumite organizații utilizează unelte comerciale de evaluare a setului de reguli de pe echipamentele de filtrare din rețea, cu scopul de a determina măsura în care acestea sunt consistente sau conflictuale. Se face astfel o verificare automată a stării filtrelor de rețea și se caută erori în seturile de reguli sau în listele de control al accesului (Access Control List - ACL) care ar putea permite servicii nedorite pe acele echipamente. Astfel de unelte ar trebui utilizate la fiecare modificare semnificativă a setului de reguli de pe firewall-uri, a ACL-urilor de pe router sau pe alte tehnologii de filtrare.

Funcționalitățile minim recomandate pentru menținerea unui control optim la nivel de echipamente de rețea:

- Identificarea oricărei modificări la nivel de echipamente de rețea, inclusiv routere, switch-uri, firewall-uri și sisteme IDS și IPS (orice schimbare în fișierele cheie, servicii, porturi, fișiere de configurație sau orice alt software instalat pe echipamente
- Configurația fiecărui sistem trebuie comparată cu baza de date master cu imagini pentru a verifica orice modificare în configurație din punct de vedere al impactului asupra securității.

c). Modalități de protejare împotriva malware-ului

Software-ul malițios constituie un aspect periculos al amenințărilor din mediul Internet, care vizează utilizatorii finali şi organizațiile prin intermediul navigării, atașamentelor email, dispozitivelor mobile precum şi prin utilizarea altor vectori. Codul malițios poate să interacționeze cu conținutul sistemului, să captureze date sensibile și să se răspândească la alte sisteme. Malware-ul modern urmărește să evite detectarea bazată pe semnături și cea comportamentală și poate dezactiva instrumentele anti-virus care rulează pe sistemul țintă. Software-ul anti-virus și anti-spyware, denumite colectiv ca instrumente anti-malware, ajută la apărarea împotriva acestor amenințări prin încercarea de a detecta programele malware și blocarea executării acestora.

Instrumentele anti-malware, pentru a fi eficiente, necesită actualizări periodice. Bazându-se pe politici și acțiuni ale utilizatorilor pentru menținerea instrumentelor anti-malware actualizate, acestea au fost discreditate pe scară largă deoarece mulți utilizatori nu s-au dovedit capabili să aplice în mod consecvent aceste sarcini. Pentru a asigura actualizarea periodică și eficientă a intrumentelor anti-malware, sunt utilizate soluții care automatizează aceste sarcini. Aceste soluții, numite și suite de end-point security, utilizează funcționalități de administrare integrate pentru a verifica activitatea instrumentelor anti-virus, anti-spyware și host-based IDS pe fiecare sistem gestionat. Zilnic sau la intervale predefinite, rulează evaluări automate și efectuează revizuiri ale rezultatelor pentru identificarea sistemelor care au dezactivate instrumentele de protecție, precum și a sistemelor care nu sunt actualizate cu ultimele definiții malware. Pentru creșterea nivelului de siguranță pentru sistemele protejate, cât și pentru sistemele care nu sunt acoperite de soluțiile de management ale organizațiilor, se folosesc tehnologiile de control al accesului în rețea prin intermediul cărora sunt testate echipamentele din punct de vedere al conformității cu politicile de securitate înainte de a permite accesul în rețea.

Unele organizații implementeaza honeypot-uri comerciale sau gratuite și instrumente de „ademenire" – cunoscute ca „tarpit tools" pentru a identifica atacatorii în mediul lor. Personalul de

securitate trebuie să monitorizeze permanent aceste instrumente pentru a determina când traficul este direcționat către atacatori și sunt efectuate tentative de conectare. Odată identificate aceste evenimente, personalul de securitate trebuie să obțina sursa adreselor de unde este generat traficul și alte detalii asociate atacului pentru a furniza datele necesare activităților de investigare.

Instrumentele anti-malware vor include următoarele funcționalități:

- Identificarea instalării de software malițios, a tentativelor de instalare, executare sau a tentativelor de executare;
- Blocarea instalării și prevenirea executării sau trecerea în carantină a software-ului malițios odată cu alertarea personalului administrativ.

d). Securitatea aplicațiilor

Printre prioritățile recente ale grupurilor criminale se numără atacurile asupra vulnerabilităților aplicațiilor web-based precum și asupra aplicațiilor în general. Aplicațiile care nu fac verificări asupra volumului intrărilor generate de utilizator, nu reușesc să „sanitizeze" intrările prin filtrarea secvențelor de caractere care nu sunt necesare sau potențial malițioase sau nu inițiază „curățarea" variabilelor în mod corespunzator, fiind astfel vulnerabile la compromiterea de la distanță. Atacurile pot fi efectuate prin „injectarea" de exploatări specifice incluzând buffer overflows, atacuri de tip SQL injection, cross-site scripting, cross-site request forgery, și click jacking de cod pentru obținerea controlului asupra sistemelor vulnerabile.

Pentru prevenirea unor asemenea atacuri, aplicațiile dezvoltate intern cât și aplicațiile third-party trebuie testate riguros pentru a identifica deficiențele de securitate. Pentru aplicațiile third-party, organizațiile trebuie să se asigure că furnizorii au efectuat testări riguroase de securitate pentru produse, iar pentru aplicațiile dezvoltate intern, organizațiile trebuie să efectueze testările de securitate sau să angajeze servicii de specialitate pentru efectuarea de astfel de testări.

Tool-urile ce testează cod sursă sau acelea pentru scanarea securității aplicațiilor web s-au dovedit a fi utile în vederea securizării, alături de verificările de securitate tip penetration testing efectuate manual de specialiști cu vaste cunoștințe de programare și expertiză în testarea de aplicații.

Funcționalități recomandate în sistemul de securitate al aplicațiilor:

- Detectarea și blocarea încercărilor de atac la nivel de aplicație;
- Testarea periodică, săptămânal sau chiar zilnic;

- Mitigarea tuturor vulnerabilităților cu risc mare din aplicațiile web accesibile din Internet, identificate cu scannere de vulnerabilități, instrumente de analiză statice și instrumente de revizuire a configurațiilor automate din bazele de date, fie prin modificarea fluxului, fie prin implementarea unui control compensatoriu.

4.1.3. Controlul accesului

a). Utilizarea controlată a privilegiilor de administrare

O primă metodă de atac cu scopul de a se infiltra în rețeaua unei organizații o reprezintă utilizarea eronată a privilegiilor administrative. Două metode comune de atac profită de lipsa de control asupra acestor privilegii administrative:

În prima metodă, un utilizator al unei statii de lucru, folosind un cont privilegiat, este păcălit să deschidă un atașament malițios din email, descărcând și deschizând un fișier de pe un website malițios, sau pur și simplu navigând pe un site web ce găzduiește conținut periculos care poate exploata browserul. Fișierul sau exploit-ul conține cod executabil ce ruleazp pe mașina victimei fie automat, fie convingând utilizatorul să execute conținutul. Daca acest cont de utilizator are privilegii administrative, atacatorul poate prelua complet controlul asupra sistemului victimei și poate instala tool-uri precum keystroke loggers sau keyloggers (aplicație ce reține într-un fișier tot ce se tastează), sniffers (interceptează și decodifică traficul de rețea) și software de control la distanță pentru a identifica parole de administrare și alte informații sensibile. Atacuri similare au loc și prin intermediul emailului: un administrator deschide un email ce conține un atașament infectat, acesta fiind mai apoi utilizat pentru a obține un punct de acces în rețea și de a ataca și alte sisteme.

O a doua metodă o reprezintă elevarea de privilegii ghicind și „spărgând" o parolă a unui cont administrativ, pentru a obține acces la o mașină țintă. Dacă privilegiile administrative sunt folosite pe scară largă în interiorul organizației, atacatorul va obține mai uşor și mai repede controlul asupra sistemelor, întrucât sunt disponibile mai multe conturi cu privilegii administrative de încercat. O situație comună specifică unui astfel de atac este aceea a privilegiilor administrative de domeniu în mediile complexe Windows, atacatorul având astfel un control semnificativ asupra unui număr mare de mașini și asupra datelor conținute de acestea.

Un management optim al conturilor administrative se realizează cu o serie de funcționalitati sau activități precum:

- extragerea listei de conturi privilegiate, atât pe sistemele individuale cât și la nivel de controllere de domeniu și verificarea periodică în lista cu servicii active dacă vreun

browser sau serviciu de email folosește privilegii ridicate (utilizarea de scripturi ce caută anumite browsere, servicii de email și programe de editare a documentelor);

- conturile administrative pot fi configurate să utilizeze un proxy web în anumite sisteme de operare și să nu aibă acces la aplicația de poștă electronică.
- setarea lungimii minime acceptabile a parolei de exemplu la 12 caractere, setarea unui algoritm de complexitate corespunzator.

b). Controlul accesului în baza principiului "Need to Know"

Unele organizații nu își identifică și separă cu atenție datele sensibile de cele mai puțin sensibile sau disponibile public în rețelele interne. În multe medii, utilizatorii interni au acces la toate sau la majoritatea informațiilor din rețea. Odată ce atacatorul a penetrat o astfel de rețea, pot găsi și transmite în exterior informații importante, fără eforturi considerabile. Chiar în câteva situații de pătrundere din ultimii ani, atacatorii au reușit să obțină accesul la date sensibile cu același cont de acces ca și pentru datele obișnuite, stocate pe servere comune.

Este vital ca fiecare organizație să înțeleagă care sunt informațiile sale importante, unde sunt situate și cine are nevoie să le acceseze. Pentru a ajunge la nivelele de clasificare, organizațiile trebuie să treacă în revistă tipurile cheie de date și importanța lor la nivel de organizație. Această analiză poate fi utilă în creionarea schemei de clasificare a informațiilor la nivelul întregii organizații. În cel mai comun caz, schema de clasificare conține două nivele: informații publice (neclasificate) și private (clasificate). Odată ce informațiile private au fost identificate, acestea pot fi ulterior împărțite pe subclase în funcție de impactul în organizație, dacă ar fi compromise.

Ce putem face pentru a aplica principiul cât mai eficient:

- Identificarea datelor, clasificarea pe nivele, corelarea cu aplicațiile de business; segmentarea rețelei astfel încât sisteme de aceeași sensibilitate să fie pe același segment de rețea; accesul la fiecare segment de rețea trebuie controlat de firewall și eventual criptat traficul de pe un segment de rețea cu acces nesecurizat;
- Fiecare grup de utilizatori sau angajați ar trebui să aibă clar specificate în cerințele postului ce tip de informații trebuie sau au nevoie să acceseze în scopul îndeplinirii atribuțiilor. În funcție de cerințele postului, accesul se va permite doar pe segmentele sau serverele necesare pentru fiecare post în parte. Fiecare server ar trebui să înregistreze logurile detaliate, astfel încât accesul să poată fi urmărit, iar situațiile în care cineva accesează date la care nu ar trebui să aibă acces să poată fi examinate;
- Sistemul trebuie să fie capabil să detecteze toate încercările de acces fără privilegii corespunzatoare și să aibă capabilități de alertare.

c). Monitorizarea și controlul conturilor de utilizator

Atacatorii descoperă frecvent și exploatează conturi de utilizator legitime dar nefolosite pentru a impersona utilizatorii legitimi, făcând astfel dificilă depistarea atacului de către sistemul de securitate al rețelei. Sunt des întâlnite cazurile în care conturile de utilizator ale contractorilor sau angajaților care au finalizat colaborarea cu organizația rămân active. Mai mult, actualii angajați rău voitori sau foști angajați au accesat conturile vechi și mult după expirarea contractului, menținand accesul la sistemele organizației și la datele sensibile, în scopuri neautorizate și uneori malițioase.

Monitorizarea și controlul conturilor de utilizator sunt activități ce revin personalului administrativ și au în vedere cel puțin funcționalități precum:

- Activarea funcției de logare a informațiilor legate de utilizarea conturilor, configurarea astfel încât să genereze date coerente și detaliate;
- Folosirea de scripturi sau instrumente dedicate pentru analiza de log astfel încât să se poată evalua profilul accesării pe anumite sisteme;
- Managementul conturilor, cu atenție sporită pe cele inactive;
- Sistemul trebuie să fie capabil să identifice conturile de utilizator neautorizate, atunci când acestea există în sistem.

d). Evaluarea abilităților și instruirea de securitate

Fiecare organizație ce se crede pregatită să identifice și să reacționeze eficient în fața atacurilor este datoare în fața angajaților și contractorilor să observe deficiențele în cunoștințe și expertiză, și să susțină acoperirea acestora prin exercițiu și instruire. Un program solid de evaluare a abilităților poate oferi managementului informații solide despre zonele în care trebuie îmbunătățită conștientizarea în domeniul securității, și devine util pentru determinarea alocării optime a resurselor limitate cu scopul de a îmbunătăți practicile de securitate.

Strâns legată de politici și conștientizare este și activitatea de instruire a personalului. Politicile comunică angajaților ce sa facă, instruirea le oferă metodele și abilitățile în vederea îndeplinirii, iar conștientizarea schimbă atitudini și comportament astfel încât personalul să urmeze prerogativele politicilor. Instruirea trebuie întotdeauna corelată cu necesitățile de cunoștințe pentru a îndeplini o sarcină dată. Dacă după instruire, utilizatorii nu respectă o anumită politică, aceasta ar trebui evidențiată prin conștientizare.

4.2 Sistemul de alertă timpurie şi informare în timp real al CERT – RO

Unul dintre principalele obiective ale CERT-RO, conform art. 7 din H.G. 494/2011, este acela de a constitui „Sistemul de alertă timpurie şi informare în timp real privind incidentele cibernetice".

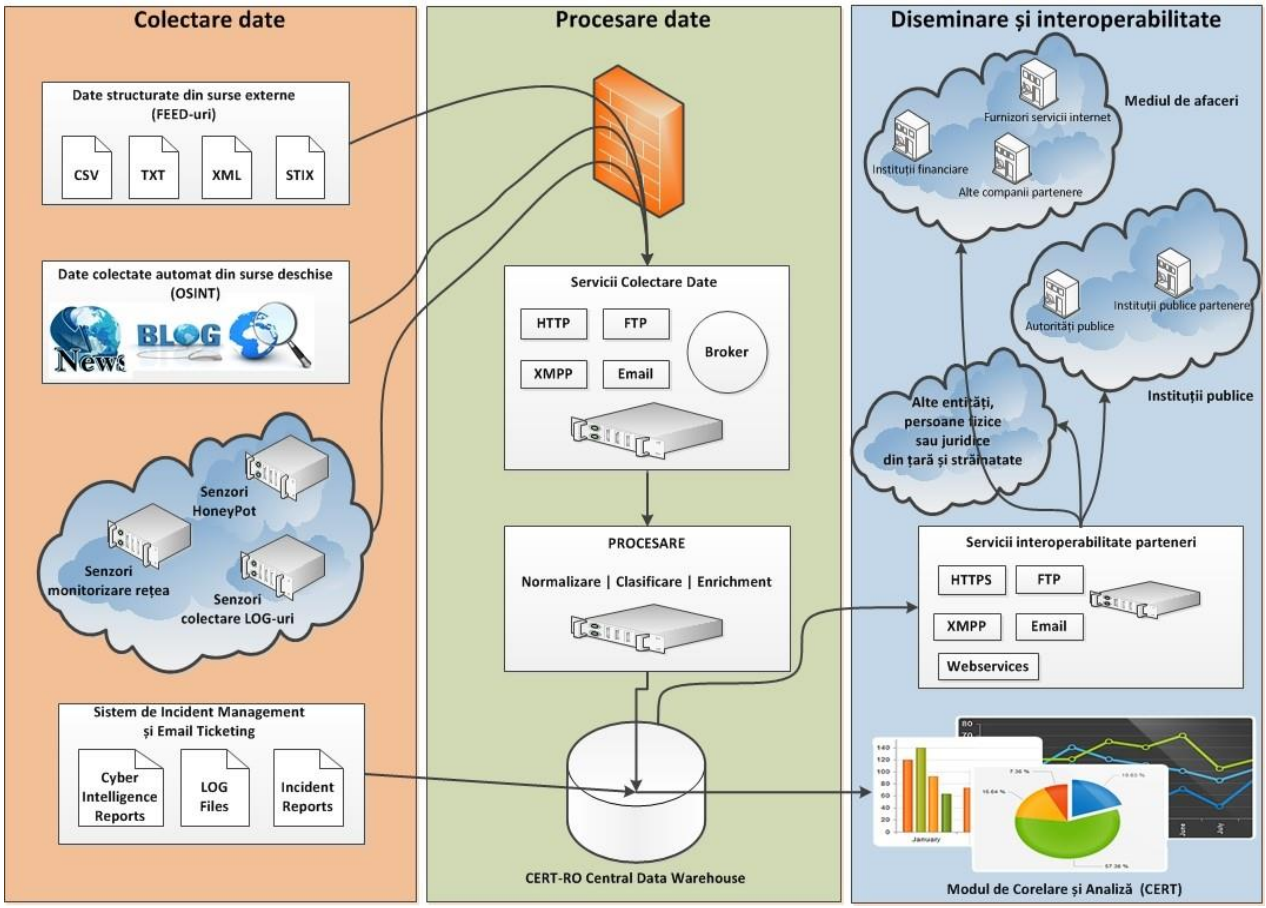
Acest sistem reprezintă ansamblul de sisteme tehnice (software, hardware) și alte resurse ce are ca obiectiv procesarea alertelor[3] de securitate cibernetică primite de CERT-RO, în vederea identificării incidentelor de securitate cibernetică, sau a premiselor de apariție a acestora, în cadrul organizațiilor publice sau private din spațiul cibernetic național, precum și în rândul utilizatorilor individuali Internet (cetățeni). Acesta asigură transmiterea coerentă, rapidă și corectă a datelor către persoanele fizice sau juridice afectate sau autoritățile publice responsabile, în vederea luării măsurilor ce se impun. CERT-RO, în calitate de punct național de contact cu centre de tip CERT este beneficiarul unui volum foarte mare de alerte referitoare la incidentele de securitate cibernetică ce afectează spațiul cibernetic național, transmise de diverși parteneri naționali și internaționali.

În acest sens, prin implementarea Sistemului de alertă timpurie și informare în timp real, se urmărește creșterea nivelului de securitate a spațiului cibernetic național (instituții publice, companii private, utilizatori individuali), precum și creșterea capacității de răspuns la incidente de securitate cibernetică a CERT-RO. În prezent, CERT-RO operează un sistem de alertă timpurie și informare în timp real privind incidentele de securitate cibernetică, denumit RO-SAT, aflat într-o fază pilot și în continuă dezvoltare.

Astfel, se dorește dezvoltarea unui sistem robust, modern, interoperabil și scalabil destinat procesării alertelor de securitate cibernetică primite de CERT-RO, precum și asigurarea interoperabilității sistemului cu instituțiile publice cu responsabilități în domeniu precum și cu orice altă organizație din mediile guvernamental, de afaceri sau universitar, în vederea transmiterii corecte, coerente și rapide a alertelor, sau a altor informații despre amenințări detectate, într-un format clar, ușor de interpretat și ușor de integrat în diverse sisteme de securitate cibernetică.

Principalele componente ale RO-SAT sunt exemplificate în figura de mai jos.

[3] Prin alertă de securitate cibernetică înțelegem orice semnalare a unui incident sau eveniment de securitate cibernetică ce implică, poate implica sau afectează entități de pe teritoriul României.



Figură 4. *Componentele RO-SAT*

Unul dintre obiectivele Sistemului de alertă timpurie și informare în timp real (RO-SAT), operat de CERT-RO, este acela de a furniza o viziune de ansamblu asupra naturii și dinamicii amenințărilor, incidentelor și vulnerabilităților de securitate cibernetică relevante pentru evaluarea riscurilor de securitate cibernetică la adresa infrastructurilor IT și de comunicații aflate în aria legală de competență a CERT-RO.

CERT-RO este prima instituție publică din România care, începând cu anul 2013, a publicat un raport cu privire la alertele de securitate cibernetică ce vizează resurse și infrastructuri IT&C din România. Rapoartele CERT-RO, semestriale și anuale, sunt întocmite pe baza datelor colectate de la partenerii naționali și internaționali, de la senzorii de detecție din cadrul Sistemului de alertă timpurie și informare în timp real (RO-SAT) și de la entitățile care raportează diferite incidente.

Toate datele colectate sunt procesate automat, în sensul că sunt normalizate pe baza unei taxonomii interne, stocate într-o bază de date, analizate și transmise către entitățile implicate și/sau către autoritățile competente de la caz la caz.

Conform raportului CERT-RO pe anul 2014[4], au fost procesate peste **78 de milioane de alerte de securitate cibernetică**, conținând un număr de aproximativ **2,5 milioane de adrese IP unice** alocate entităților din România. Principalele constatări ale raportului sunt:

- 24% din totalul IP-urilor unice alocate spațiului cibernetic romanesc (2.4 mil) au fost implicate in cel puțin o alerta de securitate cibernetica procesata de CERT-RO. In anul 2013, 16% (2.2 mil) din IP-urile unice alocate spațiului cibernetic național au fost implicate în cel puțin o alerta de securitate cibernetică.

- 54% din alertele primite vizează sisteme informatice configurate necorespunzător (misconfigured), nesecurizate sau vulnerabile, ce oferă diverse servicii nesecurizate în Internet, folosite de atacatori pentru ascunderea identității și lansarea de atacuri cibernetice asupra altor ținte. De cele mai multe ori, aceste sisteme nu trebuie compromise, simpla folosire a acestora fiind suficientă (ex: DNS open resolver, open SNMP, open NTP etc.); acest trend se observă și prin creșterea numărului de alerte ce au vizat echipamente de rețea de tip business (routere, firewall, etc.) sau home user (routere wireless, camere web, smart TV, smartphone etc.), față de alte sisteme de operare.

- 46% din alerte vizează sisteme informatice din România, victime ale unor atacatori care au reușit preluarea de resurse în cadrul unor rețele de tip botnet (zombie) prin exploatarea unor vulnerabilități tehnice și infectarea sistemelor cu diverse tipuri de aplicații malware. Rețelele de tip botnet reprezintă cea mai importantă problemă existentă în spațiul cibernetic național deoarece aceste computere compromise pot fi utilizate în derularea de atacuri cibernetice asupra altor ținte din România sau din spațiul extern țării noastre.

- 10.759 domenii .ro au fost raportate la CERT-RO ca fiind compromise în cursul anului 2014, cu 5% mai multe domenii decât în cursul anului 2013, perioadă în care au fost raportate 10.239. Din 710.000 domenii înregistrate în România, în luna decembrie 2013, numărul reprezintă aproximativ 1,5% din totalul domeniilor ".ro".

Urmare constatărilor de mai sus, pot fi formulate următoarele concluzii:

- amenințările de natură informatică, asupra spațiului cibernetic național, continuă să se diversifice

[4] https://www.cert-ro.eu/articol.php?idarticol=915

- majoritatea alertelor primite se referă la sisteme infectate cu diverse variante de malware, ce fac parte din diverse rețele de tip botnet, precum și la sisteme informatice configurate necorespunzător (*misconfigured*) sau nesecurizate.

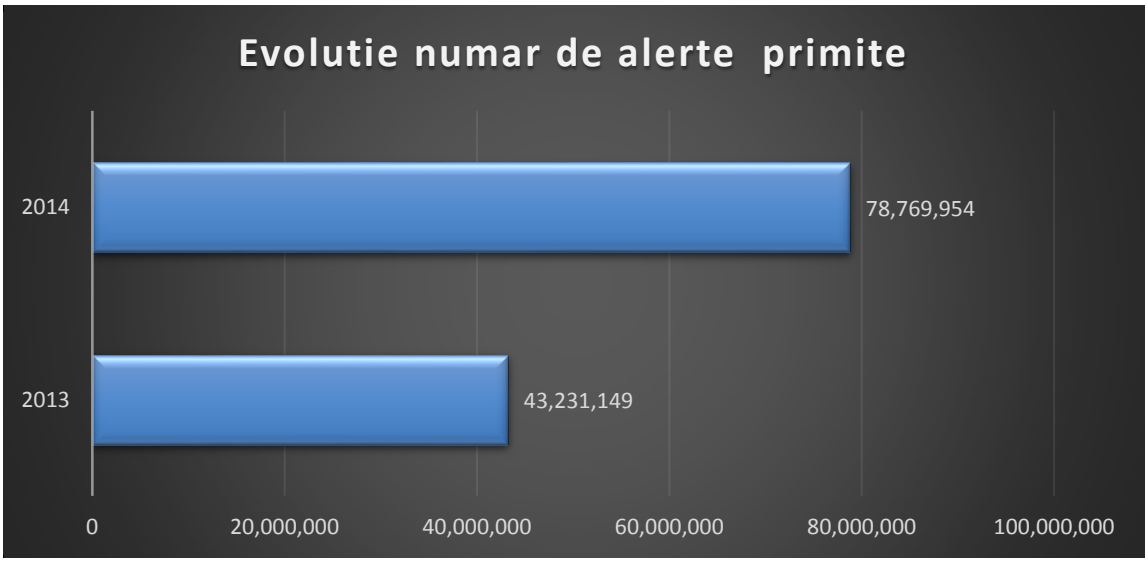
- oricare dintre cele două tipuri de sisteme, menționate mai sus, pot fi folosite cu rol de „proxy" pentru desfășurarea altor atacuri asupra unor ținte din afara țării, reprezentând astfel potențiale amenințări la adresa altor sisteme conectate la Internet;

- dispozitive sau echipamente de rețea de uz casnic (routere wireless) sau care fac parte din categoria Internet of Things (IoT) (camere web, smart TV, smartphone, imprimante etc.) odată conectate la Internet devin ținta atacatorilor, iar vulnerabilitățile acestora sunt exploatate de către atacatori pentru a avea acces în rețeaua în care acestea sunt utilizate sau pentru lansarea de atacuri asupra altor ținte din Internet.

- entități din România au fost ținta unor atacuri informatice direcționate și complexe, de tip APT (Advanced Persistent Threat) lansate de către grupuri ce au capacitatea și motivația necesară pentru a ataca în mod persistent o țintă în scopul obținerii anumitor beneficii (de obicei acces la informații sensibile);

- România nu mai poate fi considerată doar o țară generatoare de incidente de securitate cibernetică, analiza datelor prezentate demonstrând caracterul intermediar/de tranzit al unor sisteme informatice conectate ce fac parte din spațiul cibernetic național.

Numărul alertelor primite de CERT-RO în 2014 a crescut cu 82% (78.767.749) față de 2013 (43.231.149), creșterea fiind expusă în tabelul de mai jos.

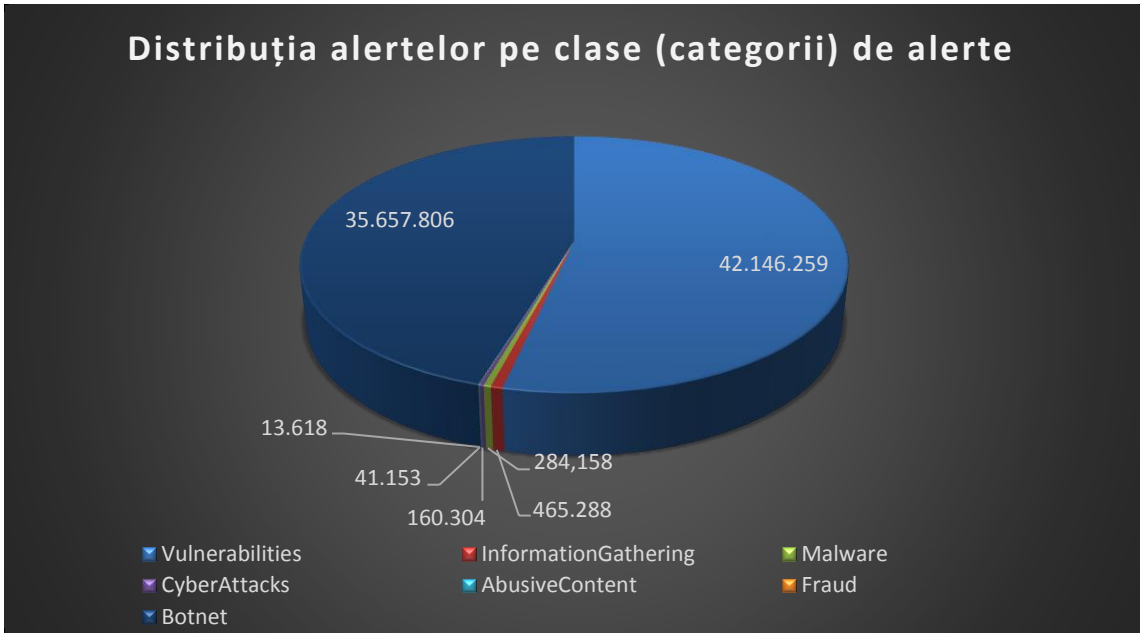


Figură 5. *Evoluția numărului de alerte*

Tabelul și graficul de mai jos redau distribuția primelor 5 tipuri de alerte primite, pe clase de alerte.

Nr.	**Clasă alerte**	**Număr alerte**	**Procent**
1	Vulnerabilities	42.146.259	53,51%
2	Botnet	35.657.806	45,27%
3	Information Gathering	465.288	0,59%
4	Malware	284.158	0,36%
5	CyberAttacks	160.304	0,20%

Tabel 1. *Distribuția alertelor pe clase (categorii) de alerte*



Figură 6. *Distribuția alertelor pe clase (categorii)*

Rezultatele cercetării prezentate în aceste capitole au contribuit la realizarea activităţii *AI.1. Analiza asupra metodelor de lucru şi capabilităţilor existente la nivel naţional în ceea ce priveşte gestionarea incidentelor de securitate cibernetică* – din planul de realizare al proiectului.

5. SITE DE PREZENTARE AL PROIECTULUI

În cadrul acestui capitol se prezintă: noţiuni de proiectare şi realizare site, scopul site-ului, categoriile de utilizatori, ierarhia pe nivele şi conţinutul asociat.

Rezultatele cercetării prezentate în acest capitol au contribuit la realizarea activităţii *AI.2. Realizarea site-ului Web al proiectului* – din planul de realizare al proiectului.

5.1. Noţiuni introductive

Un site web reprezintă un grup de pagini web, gestionate la nivel central. Un site conține informaţii în format text, imagini și alte tipuri de fișiere multimedia prezentate utilizatorilor de Internet într-un mod estetic și ușor accesibile.

Datele conținute în site sunt organizate și puse la dispoziția publicului on-line, cu ajutorul limbajelor de programare și al framework-urilor de dezvoltare. Programarea site-ului este principala metodă de definire a structurii unui site web și de gestionare a comportamentului său, astfel ca vizitatorii să navigheze prin paginile sale aşa cum au intenţionat dezvoltatorii.

Cu ajutorul tehnicilor de web design, informațiile bine structurate capătă un aspect şi un comportament user-friendly. Pentru ca paginile web să fie prezentate corect vizitatorilor, site-ul trebuie să fie găzduit pe un server web, server care le va permite să fie transferate către orice browser web prin intermediul HTTP, protocolul principal al World Wide Web.

Site-urile web reprezintă la ora actuală forma cea mai comună de proiectare şi desfăşurare a activităţilor on-line.

Din punct de vedere tehnic, paginile web sunt create preponderent cu ajutorul limbajului HTML (Hypertext Markup Language) reprezentând în esenţă un ansamblu de instrucţiuni folosite pentru a construi şi reprezenta texte, imagini, link-uri sau orice alte componente ale unei pagini web. Utilizând limbajul HTML pentru structurarea unui document şi style sheet-urile pentru a stiliza prezentarea acestuia, proiectanţii pot obţine mult mai uşor independenţa de periferic/ computer/ platforma hard-soft.

Un document cu o structură complexă poate fi prezentat în diferite moduri pe medii diferite, permiţând documentului însuşi să se adapteze mai uşor noilor tehnologii. În plus, separarea conţinutului de partea de prezentare permite modificarea înfăţişarii chiar a unui întreg site doar prin modificarea unui style-sheet (a unui document care descrie stilul).

Experienţa a demonstrat că o astfel de abordare poate reduce dramatic costurile de deservire a unui spectru larg de platforme şi probleme, facilitând atât întreţinerea ulterioară cât și implementarea modificărilor ulterioare.

5.2. Proiectarea şi realizarea

Procesul de realizare al unui site web este complex şi trebuie să respecte anumite reguli pentru a putea obţine în final un produs web profesionist, complex şi în concordanţă cu normele actuale. Primul pas în realizarea unui site web este stabilirea obiectivului, în funcţie de care se va stabili numele site-ului şi apoi dotările pe care trebuie să le aibă serverul unde se va face găzduirea.

Planificarea site-ului conţine următoarele etape:

1) Stabilirea scopului şi analizarea contextului de încadrare a site-ului

Se determină obiectivele urmărite prin realizarea site-ului şi care pot fi pe termen scurt, mediu şi lung; rolul site-ului web ca parte a temei de cercetare; contextul concurenţial on-line şi off-line în care se plasează domeniul abordat;

2) Stabilirea specificaţiilor de realizare

Se stabilesc tehnologiile care vor fi utilizate în realizarea site-ului. Pe lângă acestea, se stabileşte necesarul pentru găzduirea şi rularea site-ului în condiţii optime pentru vizitatori.

3) Proiectarea site-ului

În această etapă se stabileşte structura site-ului. Se decide modalitatea de interconectare a paginilor şi se conturează categoriile care vor face parte din site. Această etapă este foarte importantă pentru asigurarea unei navigări intuitive pentru utilizatori, astfel încât aceştia să aibă acces la informaţie pe căile cele mai rapide, evitând astfel paşi inutili în navigarea prin site.

În cadrul acestei etape trebuie efectuată o procedură de validare a proiectării. Aceasta urmăreşte:

- corectitudinea sintactică şi morfologică a textelor (validare gramaticală);
- structura semantică a întregului conţinut;
- alcătuirea codului;
- linia generală de prezentare;

4) Stabilirea modului de prezentare

Se stabileşte structura grafică a site-ului. Se creează fişierele CSS, fişiere care conţin stilurile care se aplică întregului site. Clasele şi stilurile definite în CSS se pot aplica şi se pot folosi cu uşurinţă în cadrul întregului site.

Etapele post-proiectare sunt caracteristice campaniei de promovare şi întreţinere / dezvoltare ulterioară a unui site în acord cu strategiile abordate. Acestea sunt următoarele:

- Definirea elementelor ce trebuie avute în vedere după proiectarea site-ului. Acestea se referă la:

  - coodonatele generale ale campaniei de promovare;
  - elementele de măsurare a performanţei;
  - alocarea bugetului şi atribuirea proporţionată a acestuia;

- Analizarea vizualizării de către utilizatori a site-ului:

  - volumul căutărilor online zilnice/săptamânale/lunare ale utilizatorilor de Internet**,** volumul căutărilor cu subiect tangenţial sau complementar, după cuvintele şi expresiile cheie caracteristice domeniului vizat;
  - determinarea din analizarea vizitelor pe site a punctelor forte şi a punctelor slabe ale site-ului.

- Subscrierea site-ului în:

  - directoare web gratuite;
  - motoare de căutare gratuite;

- Întreţinere şi optimizare :

  - asigurarea funcționării site-ului și ajustarea capacităților serverului coordonat cu activitățile de analizare și monitorizare a vizitelor efectuate de utilizatori pe site;
  - revizuirea constantă a potenţialului diferitelor cuvinte şi expresii cheie aferente domeniului şi tendinţele acestora;

5.3. Arhitectura paginilor web

Site-ul Web al proiectului Securitatea Cibernetică – Securitatea Rețelelor și a Sistemelor Informatice pune la dispoziţia dezvoltatorilor proiectului, beneficiarului direct al rezultatelor proiectului şi tuturor persoanelor interesate informaţii referitoare privind desfăşurarea proiectului.

Adresa site-ului este http://cybersec.ici.ro

În figura următoare este afișată și descrisă pagina de start a proiectului.

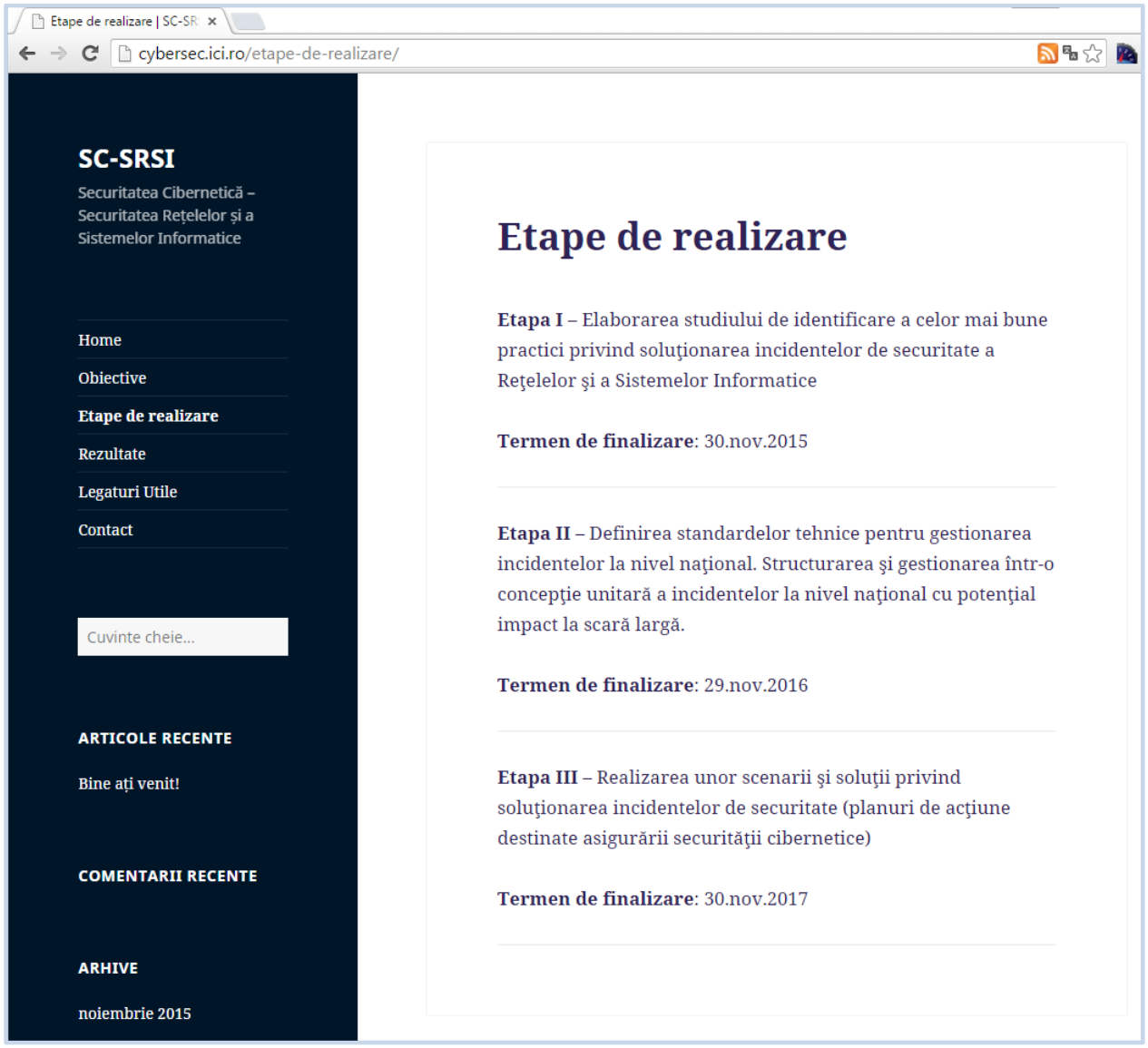
Figură 7. *Pagina de start a proiectului*

În cadrul paginii de start este afișată o prezentare succintă a proiectului SC-SRSI. În partea stângă se regăsesc legături către principalele secțiuni din site.

În pagina „Obiective", pe lângă obiectivul general al proiectului sunt arătate și obiectivele specifice pe care și le propune proiectul.

Figură 8. *Pagina Obiective*

În pagina „Etape de realizare" sunt prezentate etapele de realizare ale proiectului conform planului de realizare.



Figură 9. *Pagina Etape de realizare*

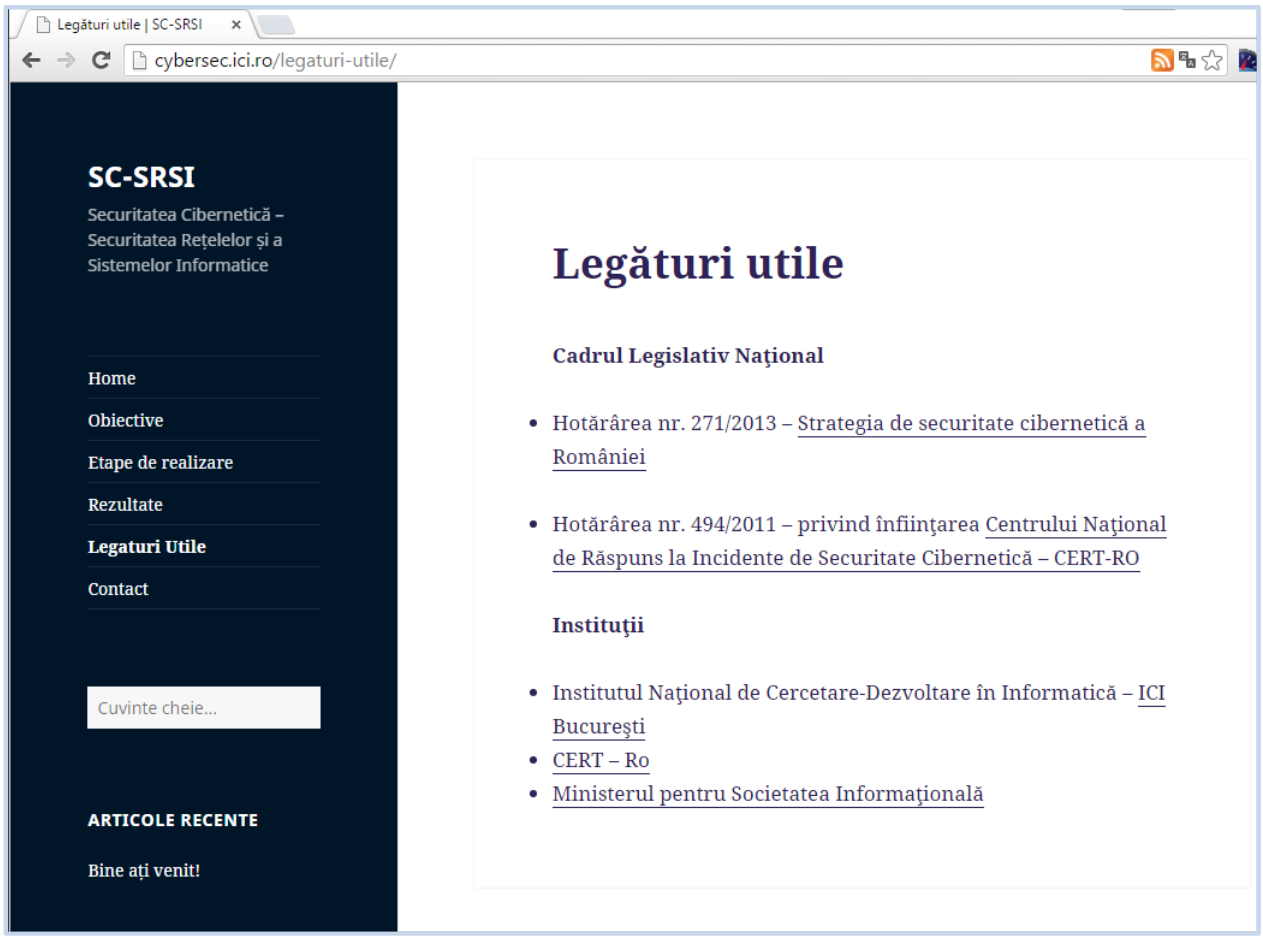
În cadrul acestei secțiuni sunt prezentate pe scurt Etapele de realizare pentru proiect împreună cu termenele te finalizare pentru fiecare etapă.

În pagina „Rezultate" sunt arătate rezultatele obținute deja sau care urmează a fi obținute din implementarea proiectului.

Figură 10. *Pagina Rezultate ale proiectului*

Rezultatele sunt structurate pe etape, fiind prezentate distinct la fiecare dintre cele 3 etape de realizare.

Secțiunea „Legături utile" conține referințe privind Cadrul Legislativ Naţional în domeniul securității și privind înființarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică – CERT-RO.



Figură 11. *Pagina Legături utile*

Pe lânga referințe, sunte prezente legături web către principalele părți implicate în buna desfășurare proiectului:Institutul Naționale de Cercetare-Dezoltare în Informatica; Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică și Ministerul pentru Societatea Informațională.

În secțiunea de Contact sunt afișate infomații cu datele de contact ale Institutului Naționale Cercetare-dezvoltare în Informatică:

Figură 12. *Pagina Contact*

5.4. Administrarea site-ului proiectului

Site-ul de prezentare, www.cybersec.ici.ro, a fost realizat utilizând platforma Wordpress.

WordPress este utilizat pentru aproximativ 24% din web - o cifra care se ridică în fiecare zi. Wordpress este folosit de la simple site-uri web, sau blog-uri, până la portaluri complexe și site-uri de bussiness aplicații. WordPress combină simplitatea în utilizare şi editare cu o complexitate în back-end pentru dezvoltatori, acest lucru conferindu-i şi flexibilitate.

Principalele capabilități ale platformei Wordpress:

- Simplitatea face posibil ca utilizatorii să își puna ideile on-line foarte rapid. WordPress este construit pentru a facilita ajungerea rapidă a conținutului în site.
- Management utilizatorilor - Nu toată lumea are nevoie de același acces la site. Administratorii pot gestiona site-ul, editorii pot să gestioneze conținut, colaboratorii să scrie acel conținut. Aceasta permite o varietate de contribuitori la site.

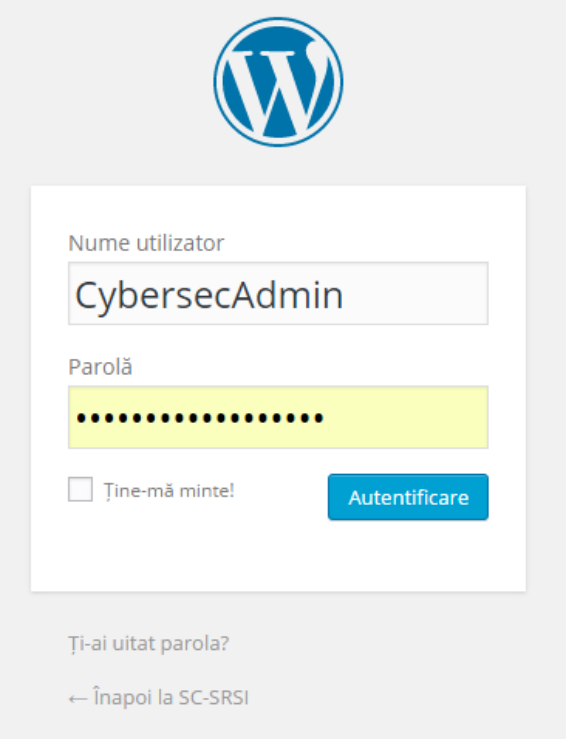
- SEO - Platforma WordPress poate fi utilizată cu uşurinţă pentru optimizarea paginilor în motoarele de căutare. Datorită codurilor simple şi constante WordPress, Google facilitează indexarea paginilor. Mai mult, elementele SEO pot fi modificate în funcţie de fiecare pagină, astfel că este decizia administratorului care pagini vor optimizate.

- Social Media - WordPress se integrează cu reţelele de socializare. Prin urmare, nu este necesară autentificarea de fiecare dată pe Facebook, Linkedln, Google+ ori Twitter, Astfel de rețele de socializare vor fi informate de apariția de conținut nou pe site.

- Îmbunătățire continuă - WordPress permite îmbunătățirea capacităților site-ului, prin instalarea a diverse plug-in-uri.

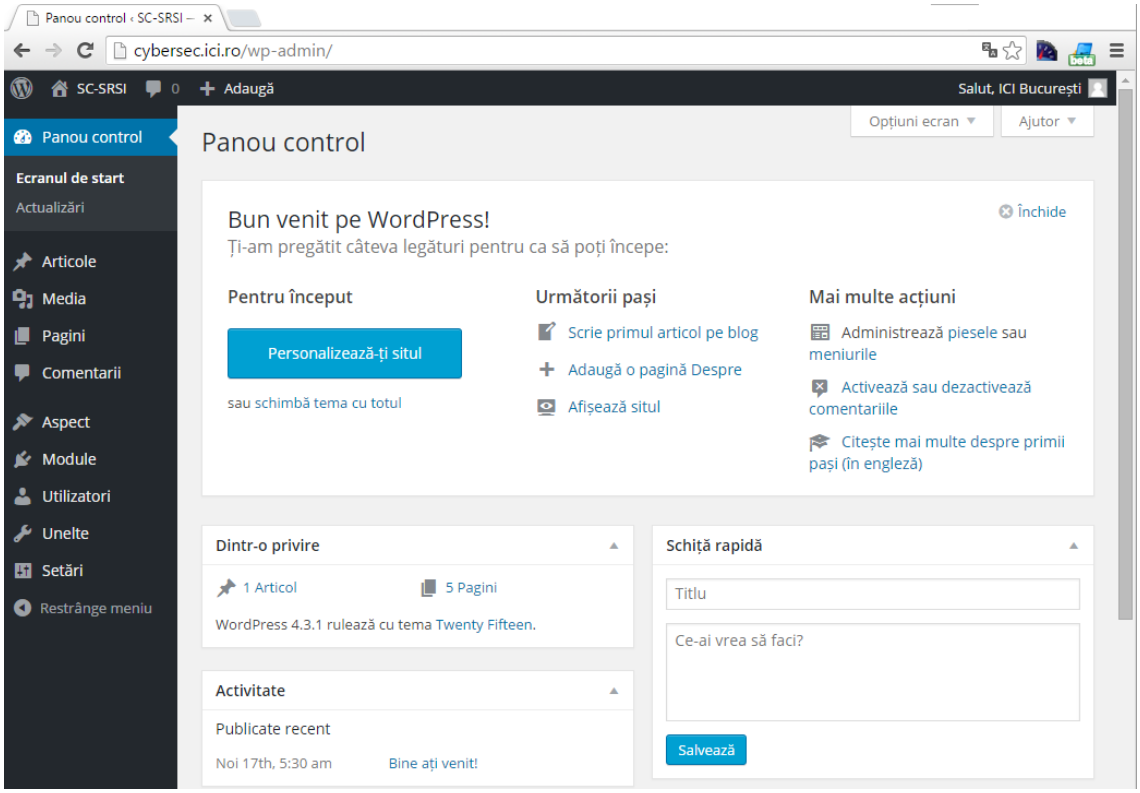
- Respectarea totală a Standardelor de conformitate - Fiecare bucată de cod WordPress generat este în deplină conformitate cu standardele stabilite de W3C. Site-ul funcționează în browser-ele curente dar mențin compatibilitatea cu generațiile anterioare de browsere.

Pentru a putea gestiona site-ul SC-SRSI, primul pas constă în autentificarea administratorului:



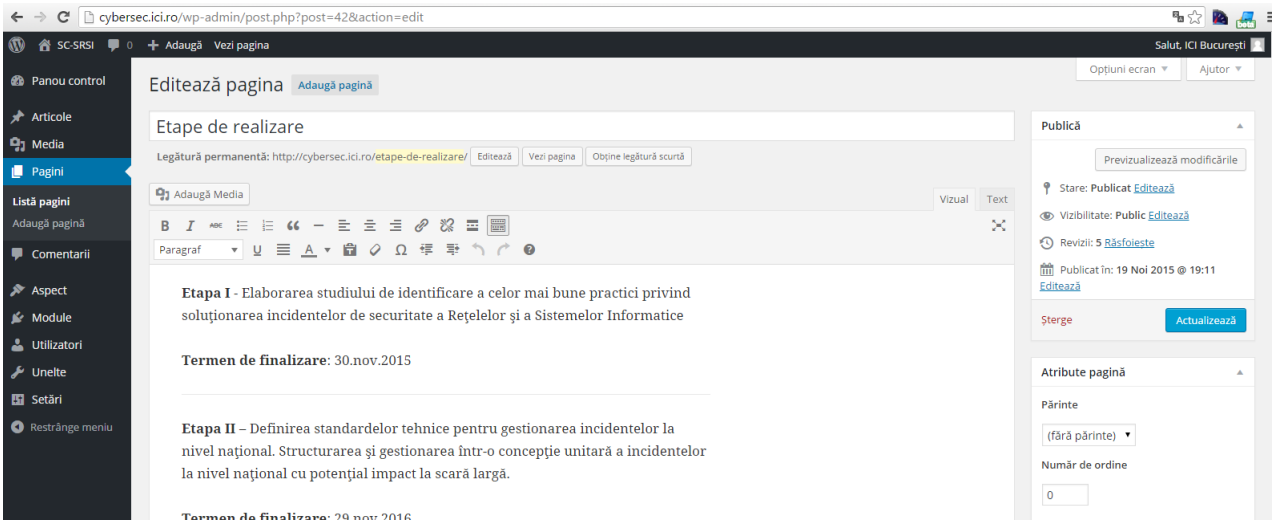
Figură 13. *Autentificare site*

După autentificare, administratorul are la dispoziție un panou de control al site-ului. Din acest panou utilizatorul poate să gestioneze aspectul și stilul site-ului, poate gestiona paginile din site, adăuga conținut sau schimba setările pentru site.



Figură 14. *Panoul de control*

Administrarea conținutului în pagină se poate face având la dispoziție o paletă de instrumente de gestionare a conținutului:



Figură 15. *Paletă de instrumente de gestionare*

CONCLUZII

Studiile și rapoartele publicate în ultimii ani, referitor la domeniul securității cibernetice, scot în evidență faptul că amenințările din spațiul virtual devin tot mai numeroase, complexe și cu un grad ridicat de periculozitate. De asemenea, incidentele de securitate cibernetică au un impact din ce în ce mai ridicat asupra infrastructurilor afectate și a organizațiilor care le dețin sau operează.

Din perspectiva securității cibernetice la nivel național, devine tot mai îngrijorător fenomenul atacurilor cibernetice conduse de actori statali împotriva infrastructurilor cibernetice ale altor state. În România au fost identificate în ultimii ani atacuri complexe, de tip APT (Advanced Persistent Threat), care au vizat instituții publice și organizații importante din România.

În acest context, devine tot mai evidentă nevoia de a intensifica eforturile la nivel național în direcția combaterii amenințărilor cibernetice, prin îmbunătățirea legislației naționale în domeniul securității cibernetice și sporirea capabilităților și metodelor de lucru pentru gestionarea incidentelor de securitate cibernetică la nivel național.

Rezultatele prezentata în lucrare confirmă realizarea obiectivelor etapei actuale şi se constituie într-o bază solidă de informaţii necesare pentru realizarea etapei următoare „*Definirea standardelor tehnice pentru gestionarea incidentelor la nivel naţional. Structurarea şi gestionarea într-o concepţie unitară a incidentelor la nivel naţional cu potenţial impact la scară largă.*"

Direcţii de continuare

Pornind de la rezultatele obţinute, în etapă următoare colectivul de cercetare are de realizat următoarele activităţi:

i. Studiu asupra modelelor adoptate la nivel internaţional sau la nivel European
ii. Definire framework/metodologie pentru gestionarea incidentelor de securitate cibernetică la nivel naţional.

Anexa 1. Figuri

Anexa 2. Tabele

Anexa 3. Glosar de termeni

Nr. Crt.	Acronim	Descriere
1.	SNSC	Sistemul Naţional de Securitate Cibernetică
2.	CERT-RO	Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică
3.	CERT	Computer Emergency Response Team
4.	CSIRT	Computer Security Incident Response Team
5.	SEO	Search Engine Optimization

Bibliografie

1 H.G. 271 din 2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică;

2 H.G. 494 din 2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO;

3 Agenda Digitală pentru România 2020 ,februarie 2015, https://ec.europa.eu/epale/sites/epale/files/strategia-nationala-agenda-digitala-pentru-romania-20202c-20-feb.2015.pdf

4 Serviciul Român de Informaţii – CyberIntelligence - http://www.sri.ro/cyberintelligence-en.html

5 RAPORT cu privire la alertele de securitate cibernetică procesate de CERT-RO in cursul anului 2014, https://www.cert-ro.eu/articol.php?idarticol=915

6 Ministerul Apărării Naţionale, Centrul Tehnic Principal de răspuns la incidente de securitate cibernetică, https://www.certmil.ro/

7 RoCSIRT, serviciul CSIRT operat de către Agenția ARNIEC/RoEduNet, https://www.csirt.ro/

8 „Implementarea unui sistem de apărare cibernetică la nivelul Ministerului Afacerilor Interne prin Departamentul Informaţii şi Protecţie Internă (CERT-INT)" , http://www.dgipi.ro/articole/articol.php?idarticol=1016

9 „*Securitatea Sistemelor Informatice*" – suport de curs, Popa Sorin Eugen, 2007, http://cadredidactice.ub.ro/sorinpopa/files/2011/10/Curs_Securit_Sist_Inf.pdf

10. Sistemul Naţional de Combatere a Criminalităţii Informatice „CyberCrime" Cod SMIS: 37595, www.cyber-team.ro

11. *„Cod de bune practici pentru securitatea sistemelor informatice şi de comunicaţii*", ANSSI, Bucureşti 2012, http://cyber-team.ro/Cod%20de%20bune%20practici%20pentru%20securitatea%20sistemelor%20informatice%20si%20de%20comunicatii.pdf

12. Systems and Network Documentation„Global Information Assurance Certification Paper", SANS Institute, https://www.giac.org/paper/gsec/1961/system-network-documentation/103414

13. „Critical Security Controls", SANS Institute, https://www.sans.org/critical-security-controls