Cod de bune practici

pentru

Securitatea Sistemelor Informatice și de Comunicații

Asociaţia Națională
pentru
Securitatea
Sistemelor Informatice

București 2012

CUPRINS

I. Introducere

1.1. Scopul și audiența codului de bune practici

Codul de bune practici emis de **Asociaţia Naţională pentru Securitatea Sistemelor Informatice** oferă recomandări pentru organizațiile care doresc iniţierea, implementarea sau menţinerea unui sistem de securitate informatică eficient.

Documentul este destinat să ofere o bază comună de standarde minimale în vederea organizării și implementării unor practici de management de securitate eficiente şi creșterea nivelului de încredere în relațiile dintre partenerii de afaceri.

Codul este întocmit în corelare cu reglementările legale naționale și internaționale în domeniu.

1.2. Obiective

Obiectivele prezentului document circumscriu obiectivelor asociației:

a) Contribuirea la dezvoltarea unei strategii naționale de securitate a sistemelor informatice;
b) Promovarea celor mai înalte standarde etice și profesionale în domeniul securității sistemelor informatice;
c) Promovarea bunelor practici pentru a asigura confidențialitatea, integritatea și disponibilitatea resurselor informatice ale unei organizații;
d) Consolidarea culturii securității cibernetice la nivel național și extinderea cunoștințelor și aptitudinilor în domeniul securității informației;
e) Facilitarea interacțiunii și a educării membrilor pentru a răspunde într-un mod eficient și coordonat la amenințările cibernetice;
f) Adoptarea celor mai bune de măsuri de protecție a datelor, a sistemelor de comunicație și de procesare a acestora;
g) Cunoaşterea riscurilor și ameninţărilor la care sunt supuse activităţile desfăşurate în spaţiul cibernetic şi oferirea de soluții de prevenire şi contracarare a acestora.

II. Dimensiunea spațiului cibernetic în cadrul Economiei Naționale

2.1. Definirea spațiului cibernetic

Spațiul cibernetic, din perspectiva economiei naționale, reprezintă rețeaua integrală și integrată de infrastructuri interdependente de tehnologie a informației, reţelele de telecomunicaţii şi sisteme de prelucrare de date pe calculator.

Din punct de vedere social și economic, spațiul cibernetic este un mediu informațional dinamic bazat pe interoperabilitate şi servicii specifice societăţii informaționale unde organizațiile și persoanele fizice pot

interacţiona, schimba idei, informații, să ofere asistenţă socială, derula afaceri sau activități artistice, politice și de mass-media, derula activități economice și financiare, folosind sisteme electronice de plată și tranzacționare.
Din punct de vedere fizic, spațiul cibernetic înglobează totalitatea serverelor, computerelor, echipamentelor de comunicații, de interconectare, centrale telefonice digitale, magistrale de fibră optică, rețele de cabluri de orice tip, echipamente de transmisie wireless, antene, dispozitive de stocare, prelucrare, transmitere, codare, protejare a datelor, precum și spațiile dedicate în care echipamentele sunt utilizate.
Spaţiul cibernetic se caracterizează prin lipsa frontierelor, dinamism şi anonimat, generând deopotrivă, atât oportunităţi de dezvoltare a societăţii informaționale bazate pe cunoaştere care insa prezinta și riscuri la adresa funcționării acesteia.
Pe măsura creșterii gradului de informațizare al societății românești, aceasta este mai vulnerabilă la atacuri, iar asigurarea securităţii spaţiului cibernetic trebuie să constituie o preocupare majoră a tuturor organizațiilor (sau organismelor) implicate.

2.2. Securitatea sistemelor informaționale

Securitatea sistemului informațional trebuie să fie o responsabilitate asumată de către structurile de conducere ale oricărei organizații din mediul privat sau public. Structurile de conducere trebuie să asigure o direcţie clară şi gestionată corespunzator pentru indeplinirea obiectivelor stabilite prinpolitica de securitate, având în vedere următoarele elemente:

a) revizuirea și aprobarea politicii de securitate şi stabilirea de responsabilităţi legate de aceasta;
b) monitorizarea schimbărilor semnificative de expunere a sistemului informațional la ameninţări majore;
c) revizuirea și monitorizarea incidentelor de securitate a sistemului informațional;
d) aprobarea măsurilor de sporire a securității informațiilor.

În vederea stabilirii și menținerii politicilor de securitate este esențială implicarea specialiștilor din domeniu în vederea adoptării deciziilor privind securitatea sistemului informațional.
Accesul la echipamentele de prelucrare informaţiilor organizației de către terţe părţi trebuie să se facă sub supraveghere. Pentru accesul terţilor, o evaluare a riscului ar trebui să fie efectuată pentru a stabili implicaţiile de securitate şi cerinţele de control. Măsurile de protecție trebuie să fie puse de acord şi incluse într-un contract cu terţele părţi. De asemenea în acordurile/contractele de externalizare ar trebui să se abordeze riscurile, controalele și procedurile de securitate pentru sistemele informatice, rețelele şi / sau echipamentele de birou.
Toate activele sistemului informațional ar trebui să fie contabilizate şi să aibă un responsabil desemnat. Responsabilitatea pentru active ajută să se asigure că protecţia corespunzătoare este menţinută. Responsabilul unui element din sistemul informațional trebuie să poată fi identificat pentru toate activele majore și să aibă responsabilități pentru menţinerea și implementarea de controale adecvate. Responsabilitățile pentru control pot fi delegate.
Informațiile trebuie să fie clasificate pentru a indica prioritățile și gradul de protecţie necesare. Informațiile au diferite grade de sensibilitate şi de importanţă, unele dintre acestea necesitând un nivel suplimentar de protecţie sau o manipulare specială. Un sistem de clasificare a informațiilor ar trebui să fie

utilizat pentru a defini un set adecvat de niveluri de protecţie, precum şi necesitatea de a institui măsuri speciale de manipulare.

Pentru a reduce riscurile de eroare umană, furt, fraudă sau de abuz de încredere, responsabilităţi de securitate trebuie să fie implementate încă din etapa de recrutare, incluse în contractele de muncă şi monitorizate în timpul activității la locul de muncă.

Toți angajații proprii sau terțele persoane care au acces la sistemul informațional al unei companii ar trebui să semneze un acord de confidențialitate.

Pentru a ne asigura că utilizatorii sunt conştienţi de ameninţările de securitate a informațiilor şi sunt pregătiți pentru a sprijini politica de securitate organizaţională în cursul activităţii lor la locul de muncă, angajații proprii sau terțele persoane ar trebui să fie instruiţi cu privire la procedurile de securitate şi utilizarea corectă a sistemelor de prelucrare a informațiilor.

Toate incidentele de securitate trebuie raportate și în acest sens trebuie implementat un sistem eficient și rapid de raportare a incidentelor de securitate, care să fie cunoscut de către toți angajații.

Informațiile de business critice sau sensibile trebuie să fie adăpostite în locuri sigure, protejate într-un perimetru de securitate adecvat, cu bariere de securitate corespunzătoare și controale de acces. Acestea ar trebui să fie protejate fizic împotriva accesului neautorizat, deteriorare şi interferenţe. Protecţia oferită trebuie să fie proporţională cu riscurile identificate.

Echipamentele IT&C trebuie să fie protejate fizic împotriva ameninţărilor de securitate şi de pericolele de mediu.

Responsabilităţi şi proceduri pentru gestionarea și exploatarea tuturor sistemelor de prelucrare a informațiilor ar trebui să fie stabilite. Aceasta presupune dezvoltarea unor instrucţiuni de utilizare şi proceduri de răspuns la incidente aprobate de conducerea unității și cunoscute de către tot personalul.

Măsuri de precauţie sunt necesare pentru a preveni şi detecta introducerea de software rău intenţionat. Software-ul și echipamentele de calcul sunt vulnerabile la introducerea de software rau intentionat, cum ar fi viruşi, viermi de rețea, cai troieni. Utilizatorii ar trebui să fie conştienţi de pericolele software-ului neautorizat sau rău intenţionat şi managerii ar trebui, acolo unde este cazul, să introducă controale speciale pentru a detecta sau a preveni introducerea de software rău intenționat.

În special, este esenţial să se ia măsuri de precauţie pentru a detecta şi a preveni infectarea cu viruşi informatici ale calculatoarelor angajaților.

Proceduri de rutină ar trebui să fie stabilite pentru efectuarea de back-up-uri strategice, simularea periodică a restaurării de pe copiile realizate, logarea evenimentelor și a defectelor, acolo unde este posibil și monitorizarea permanentă a echipamentelor critice.

Schimburile de informații şi de software între organizații ar trebui să fie controlate, şi trebuie să fie conforme cu legislaţia în vigoare. Proceduri şi standarde care să protejeze informațiile și datele în tranzit ar trebui să fie stabilite iar acestea să fie parafate în acorduri semnate de toate părțile implicate.

2.3. Atributele securității informatice

Securitatea informatică asigură cunoaşterea, prevenirea și contracararea unui atac împotriva spaţiului cibernetic, inclusiv managementul consecinţelor.

Atributele securității informatice sunt următoarele:

- ***Cunoaşterea*** *trebuie să asigure informațiile necesare în elaborarea măsurilor pentru prevenirea efectelor unor incidente informatice.*
- ***Prevenirea*** *este principalul mijloc de asigurare a securităţii informatice. Acţiunile preventive reprezintă cea mai eficientă modalitate atât de a reduce extinderea mijloacelor specifice ale unui atac cibernetic, cât și de a limita efectele utilizării acestora.*
- ***Contracararea*** *trebuie să asigure o reacţie eficientă la atacuri cibernetice, prin identificarea şi blocarea acţiunilor ostile în spaţiul cibernetic, menţinerea sau restabilirea disponibilităţii infrastructurilor cibernetice vizate şi identificarea şi sancţionarea potrivit legii, a autorilor.*

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

De altfel atributele enumerate mai sus se suprapun peste atributele fundamentale ale informației:

- ***Disponibilitatea*** *informației este acea proprietate a sistemului sau rețelei de a asigura utilizatorilor legali informația completă atunci când aceştia au nevoie de ea.*
- ***Confidenţialitatea*** *este acea proprietate a sistemului sau a reţelei de a permite accesul la informații numai utilizatorilor cărora le este destinată şi să ofere garanţii suficiente pentru a interzice accesul celorlalţi utilizatorilor.*
- ***Integritatea*** *informației este acea proprietate a sistemului sau a reţelei de a asigura livrarea informației fără modificări accidentale sau neautorizate.*
- ***Autenticitatea*** *informației este acea proprietate a sistemului sau a reţelei de a permite asocierea informației cu sursa legală de producere a ei.*
- ***Nerepudierea*** *informației este acea proprietate a sistemului sau a reţelei de a asocia informației dovada că informația a fost transmisă de o entitate identificată și a fost recepţionată de o altă entitate identificată fără posibilitate de contestare.*

2.4. Importanța funcției Ofițerului de securitate în cadrul organizației

În cadrul fiecărei organizații, pentru asigurarea unui nivel de securitate optim este necesară existența unei structuri de securitate care să acopere zona de securitate fizică, logică și a personalului. Din punct de vedere al securității logice această funcție este în general îndeplinită de un Information Security Officer (ISO) sau Chief Information Security Officer (CISO).

ISO / CISO este cel care coordonează întreaga activitate a unui department de securitate a informației, realizează și impune politici, proceduri și cele mai bune practici privind modul în care informațiile, datele și resursele digitale sunt administrate și protejate, cu accent asupra următoarelor obiective și responsabilități:

- *Obținerea acceptanței și suportului managementului pentru strategia de securitate aliniată cu obiectivele de business;*
- *Definirea politicilor de securitate IT în concordanță cu strategia;*
- *Definirea standardelor de securitate pentru toate politicile relevante;*
- *Alinierea practicilor și procedurilor din cadrul organizației, cu politica centrală de securitate;*
- *Asignarea clară a rolurilor și responsabilităților relativ la securitatea informației în cadrul organizației;*
- *Integrarea securității IT în lanțul administrării informației la nivelul întregii organizații;*
- *Identificarea și clasificarea bunurilor informaționale în funcție de criticalitate și senzitivitate;*
- *Definirea, implementarea și mentenanța unor obiective de control eficace pentru managemenul securității;*
- *Implementarea unor procese de monitorizare eficiente ale acestor controale;*
- *Managementul incidentelor de securitate, testarea capabilităților de răspuns;*
- *Desfășurarea activităților specifice continuității afacerii, testarea planurilor de recuperare în caz de dezastru;*
- *Aprobarea din perspectiva securității în cadrul proceselor de change management;*
- *Identificarea, evaluarea, comunicarea și managementul riscurilor de securitate;*
- *Managementul proceselor de obținere și menținere a conformității cu reglementările obligatorii;*
- *Inițierea, facilitarea și promovarea activităților menite să ducă la sporirea conștientizării importanței securității atât în cadrul organizației cât și pentru parteneri, furnizori, clienți și alte structuri care au relații directe cu organizația;*
- *Asigurarea conformității cu politicile și procedurile de securitate pentru toți angajații, la nivel individual, prin impunerea regulilor stabilite;*
- *Asistarea la realizarea unor profile de securitate corecte ale personalului și menținerea unor dosare exacte cu profilele de securitate potrivite fiecarei poziții în cadrul organizației;*
- *Monitorizarea utilizării eficiente a resurselor de securitate;*
- *Dezvoltarea și implementarea metricilor și a monitorizării activităților de securitate.*

2.5. Infrastructuri critice la nivel național și organizațional

Societatea, afacerile și politica depind de funcționarea infrastructurilor. Infrastructurile în general şi infrastructurile critice în special, sunt viaţa societăţilor moderne, eficiente. Infrastructurile critice au reprezentat totdeauna domeniul cel mai sensibil, cel mai vulnerabil al oricărui sistem și al oricărui proces.

Termenul colectiv - „infrastructuri” acoperă oamenii, organizațiile, procesele, produsele, serviciile și fluxurile de informații, precum şi instalaţiile tehnice și structurale şi construcţiile care, individual sau parte a unei rețele, permit societăţii, economiei și statului să funcţioneze.

Infrastructurile sunt considerate critice datorită:

- *importanţei vitale pe care o au, ca suport material sau virtual;*
- *rolului pe care îl îndeplinesc în stabilitatea, fiabilitatea, siguranţa, funcţionalitatea şi, mai ales, în securitatea sistemelor;*
- *vulnerabilităţii sporite la ameninţările directe, precum și la cele care vizează sistemele din care fac parte;*
- *sensibilităţii deosebite la variaţia condiţiilor şi, mai ales, la schimbări bruşte ale situaţiei.*

Astfel de infrastructuri există pretutindeni în lume şi în cadrul fiecărui spațiu fizic, cosmic sau virtual, în toate domeniile activităţii umane, practic atât la nivel organizațional, național sau internațional.
Criteriile după care se face evaluarea privind incadrarea în categoria infrastructurilor critice sunt variabile, chiar dacă sfera lor de cuprindere poate rămâne aceeaşi. Astfel de criterii pot fi următoarele:

- *criteriul fizic (locul în rândul celorlalte infrastructuri, mărimea, dispersia, anduranţa, fiabilitatea etc.);*
- *criteriul funcțional (ce anume „face" infrastructura respectivă);*
- *criteriul de securitate (care este rolul ei în siguranţa şi securitatea sistemului);*
- *criteriul de flexibilitate (care arată că există o anumită dinamică și o anumită flexibilitate - practic unele dintre infrastructurile obişnuite pot fi sau deveni, în anumite condiţii, infrastructuri critice.*

Conform Programului European pentru Protecţia Infrastructurilor Critice, acestea pot fi grupate astfel:

Sectoare	**Subsectoare**
Administraţie publică	Președinție, Parlament, Guvern, Justiţie, Administraţie
	Instituţii de cercetare
	Patrimoniu naţional cultural
Industrie chimică și nucleară	Producţie, transport, depozitare şi procesare a produselor chimice și nucleare Conducte de transport a produselor/substanțelor chimice periculoase
Energie	Furnizare energie
	Furnizare combustibil (petrol)
	Furnizare gaz natural
	Transport și distribuție energie
Servicii financiare	Bănci
	Companii de asigurare
Sănătate Publică	Centre de îngrijire medicală şi spitale
	Laboratoare
Tehnologia Informației și Comunicaţii	Telecomunicațiile
	Sisteme şi reţele informatice
	Internet
	Sisteme de instrumentare, automatizare și monitorizare
	Radio şi media
Apă și hrană	Furnizare hranie și securitatea acesteia
	Furnizarea apei potabile
Siguranţă publică, ajutoare şi servicii pentru urgenţe	Organizații pentru urgenţe (poliţie, serviciu de pompieri, urgenţe îngrijire medicală şi servicii de salvare)

	Protecţie civilă
	Forţe armate
Transport	Transport rutier
	Transport feroviar
	Transport aerian
	Transport naval
	Servicii poştale şi logistică

Potrivit Strategiei de Securitate Naţională a României (Capitolul XI cu titlul „Dezvoltarea şi sporirea gradului de protecţie a infrastructurii"), o direcţie prioritară de acţiune pentru realizarea obiectivelor acesteia o reprezintă necesitatea declanşării unui amplu proces de dezvoltare, modernizare și asigurare a protecţiei infrastructurilor critice, a elementelor vitale ce vizează pregătirea instituţiilor, societăţii, economiei și teritoriului naţional pentru a face faţă riscurilor și ameninţărilor la adresa securităţii.

Protecţia infrastructurilor critice (PIC) constituie un obiectiv prioritar al Uniunii Europene, fiind unul dintre subiectele aflate din ce în ce mai frecvent pe agenda politică europeană, iar toate statele membre trebuie să stabilească măsurile necesare pentru a se conforma prevederilor Directivei Consiliului nr. 2008/114/EC „*privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora*" *adoptată la 8 decembrie 2008 și intrată în vigoare prin publicarea în Jurnalul Oficial al Uniunii Europene*.

În același timp, protecția infrastructurilor critice și securitatea cibernetică au devenit subiecte principale pe agenda de lucru NATO (ex. - noul concept „*scut cibernetic*") și sunt elemente esenţiale, strâns legate între ele.

PIC se bazează pe managementului integral al riscului, care conţine, în principal, două părţi: prin prima se efectuează o evaluare detaliată a ameninţării şi a riscului, care serveşte apoi ca bază pentru măsurile din următoarele domenii:

- *prevenire (ex. măsuri structural-tehnice sau zonale);*
- *pregătire (ex. urgenţe şi planificarea continuităţii afacerilor);*
- *intervenţie (ex. sistem de alarmare, protecţie fizică prin personalul de securitate, comunicaţii standardizate în timpul crizelor);*
- *reparare (ex. restaurarea temporară a infrastructurilor);*
- *reconstrucţie (ex. a infrastructurilor).*

Pentru a putea utiliza eficient resursele, infrastructurile critice trebuie prioritizate. "Inventarul" infrastructurilor critice este cuprinzător și trebuie actualizat, în mod regulat, în cooperare cu autorităţile responsabile ale administraţiei guvernamentale și operatorii privați. „Inventarul" serveşte, în principal, ca bază pentru procesele de planificare şi luare a deciziilor la niveluri diferite (administraţie guvernamentală şi operatori privați).

Foarte mulți operatori privați dețin infrastructuri critice (ex. din domeniul tehnologiei informației și comunicații, serviciilor financiare, serviciilor poștale, industriei alimentare etc.), dar nu tot atât de multe se concentrează

pentru asigurarea siguranţei şi securităţii infrastructurilor pe care le deţin în același raport cu interesul acordat maximizării profitului.
Mai mult, la nivel mondial tendința trecerii infrastructurilor critice în proprietate privată este din ce în ce mai accentuată, autoritățile asumându-și rolurile de observare, control și reglementare. Această tendință se datorează în mare parte crizei financiare dar și importanței managementului privat în ceea ce priveşte asigurarea eficienţei economice dovedită de rezultatele financiare obţinute.

Situațiile de criză, care amenință direct infrastructurile critice, pentru operatorii privați reprezintă “business continuity”, iar pentru instituțiile guvernamentale reprezintă “responsabilitate socială”. Între aceste două concepte trebuie să existe sinergii suficient de puternice care să conducă către o manieră proactivă de management al riscurilor astfel încât să să fie evitate situaţiile de criză. În acest sens, parteneriatul între operatorii privați de infrastructuri critice și instituțiile guvernamentale, analizele de risc fundamentate, evaluarea interdependenţelor și investiţiile timpurii vor trebui să fie puncte cheie ale strategiei de dezvoltare durabilă.
Printr-un efort de corelare a reglementărilor legale cu prevederile standardelor de management se poate asigura o alocare optimă a resurselor și responsabilităţilor între instituţiile guvernamentale, proprietari, operatori şi utilizatori, în special în domeniul infrastructurilor critice.
Operatorii privați care dețin infrastructuri critice trebuie să-şi evalueze şi identifice riscurile și ameninţările precum şi activităţiile critice ale proceselor de business, să implementeze proceduri şi măsuri clare de siguranţă şi securitate astfel încât să aibă capacitatea de a face faţă factorilor perturbatori şi a reveni la stadiul iniţial în cel mai scurt timp şi cu pierderi minime.
Standardele ISO 22301:2012 – *Sistemul de Management al Continuității Afacerii* și ISO 22399:2007 - Securitate societală – *Îndrumar privind pregătirea pentru incident şi managementul continuităţii operaţionale* sunt aplicabile oricărui tip de organizație publică sau privată, furnizor de produse sau prestator de servicii care doreşte să:

- *înţeleagă contextul general în care-şi desfăşoară activitatea;*
- *identifice obiectivele critice;*
- *înţeleagă barierele, riscurile și întreruperile care pot afecta obiectivele critice;*
- *evalueze risurile reziduale și toleranţa la risc;*
- *înţeleagă efectul măsurilor și strategiilor de diminuare a riscurilor;*
- *planifice în ce mod organizația îşi poate atinge obiectivele în situaţia apariţiei unui incident;*
- *elaboreze răspunsul la incident şi răspunsul la situaţia de urgenţă, răspunsul de asigurare a continuităţii şi revenirea după incident;*
- *definească roluri şi responsabilităţi și să planifice resurse pentru răspunsul la incident;*
- *îndeplinească conformitatea cu regelementările legale, standarde şi alte cerinţe;*
- *furnizeze asistenţă reciprocă şi asistenţă comunităţii;*
- *coopereze cu instituţiile cu responsabilităţi în managementul situaţiilor de urgenţă;*
- *promoveze formarea și dezvoltarea unei culturi organizaționale care să înteleagă necesitatea gestionării riscului ca element inevitabil în desfăşurarea activităţii şi luarea deciziilor.*

III. Măsuri necesare pentru asigurarea securității informatice

3.1. 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.

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;*
- *Identificarea locației în care s-a efectuat conectarea.*

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

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 și 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 (sau boundary defense)

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 clădireile/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, însă 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 şi 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 şi configurația zonelor care trebuiesc protejate;*
- *sistemul de pază şi apărare;*
- *sistemul de avertizare şi 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 şi modul de implementare a măsurilor de pregătire și instruire pe linie de securitate fizică;*
- *responsabilitățile și modalitățile de realizare a verificărilor, inspecțiilor şi controalelor sistemului de securitate;*
- *măsuri suplimentare de protecție fizică.*

3.2. Securitatea logică

a. Configurații de securitate a componentelor hardware pentru echipamente mobile, stații de lucru şi 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 și organizațiile prin intermediul navigării, atașamentelor email, dispozitivelor mobile precum și 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.*

3.3. Securitatea personalului

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 sp 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 usor 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.

3.4. Asigurarea continuității afacerii

Orice organizație depinde de resurse, personal şi activități care sunt efectuate zilnic, în scopul de a rămâne operațională şi profitabilă. Cele mai multe organizații au resurse tangibile, proprietăți intelectuale, angajaţi, calculatoare, legăturile de comunicare, clădiri pentru sedii principale și puncte de lucru. Dacă oricare dintre aceste elemente este deteriorat sau inaccesibil pentru un motiv sau altul, compania și serviciile furnizate de aceasta pot fi grav afectate. În funcție de gravitatea cazurilor, organizația poate reveni la capacitatea de funcționare normală mai repede sau mai greu, dar există și situații în care companiile nu sunt niciodată în măsură să își reia activitatea și să-și mențină clienții în urma diferitelor dezastre care pot apare. Ca o consecință benefică implementării planului de recuperare în caz de dezastru, s-a constatat că organizațiile care au planificate măsuri de recuperare în caz de dezastru au o şansă mult mai mare de a-și relua activitatea în timp util şi de a rămâne în piaţă.

Scopul implementării unui plan de recuperare în caz de dezastru este acela de a minimiza efectele unui dezastru și pentru a se asigura că resursele, personalul, şi operaţiunile își vor relua funcționarea într-un timp util. Un plan de recuperare în caz de dezastru este aplicat atunci când intervine o situație de nefuncționare și tot personalul este preocupat de a repune sistemele critice din nou online. Un plan de continuare a afacerii (BCP), are o abordare mai largă a problemei. Acesta include activarea și funcționarea sistemelor critice în altă locație în timp ce se lucrează la rezolvarea problemelor și repornirea sistemelor în locația principală.

De asemenea, este important de notat că o societate poate fi mult mai vulnerabilă, după un dezastru, pentru că serviciile de securitate folosite pentru protecția fizică sau logică pot fi indisponibile sau într-o stare de operare la capacitate redusă. Disponibilitatea este una dintre temele principale ale planificării continuităţii (planului de recuperare în caz de dezastru și a planului de continuarea afacerii) în care se asigură că există resursele necesare pentru a menţine operaționalitatea organizației în orice condiții.

Atunci când se are în vedere planificarea continuităţii activităţii, unele companii se concentrează în principal pe backup de date şi existența hardware-ului redundant. Deși aceste elemente sunt extrem de importante, ele sunt doar părți mici din imaginea de ansamblu. Echipamentele au nevoie de oameni pentru a le configura şi le utiliza, iar datele sunt de obicei nefolositoare dacă nu sunt accesibile pentru alte sisteme şi entităţi, eventual, din exterior. Planificarea trebuie să aibă în vedere prezenţa oamenilor potriviţi la locul potrivit, documentarea configuraţiilor necesare, stabilirea de canale alternative de comunicaţii (voce și date), puterea de alimentare necesară și asigurarea că toate dependinţele, inclusiv procesele şi aplicațiile, sunt corect înţelese şi luate în considerare.

De exemplu, în cazul în care liniile de comunicație sau în cazul în care un serviciu este indisponibil pentru orice perioadă semnificativă de timp, trebuie să existe o modalitate rapidă și testată de restabilire a comunicaţiilor și serviciilor afectate.

Incidentele și întreruperile pot apare din multe cauze:

- *Umane – angajați nemulțumiți, revolte, vandalism, accidente, furt, etc;*
- *Tehnice – întreruperi, viruși, viermi, hackeri, probleme de alimentare cu energie electrică, fiabilitatea echipamentelor, etc;*
- *Naturale – cutremure, furtuni, incendii, inundații, etc.*

Fiecare din aceste situații pot cauza probleme de funcționare de tipul:

- *Minor – operațiunile sunt indisponibile pentru o perioadă redusă de timp, de până la câteva ore, sau mai puțin de o zi;*
- *Mediu – operațiunile sunt indisponibile pentru mai mult de o zi. În acest caz o locație secundară poate fi utilă pentru continuarea operațiunilor;*
- *Major – acest tip de eveniment apare în urma unei catastrofe iar locația principală nu mai poate fi utilizată. Este necesară o locație auxiliară pentru continurarea operațiunilor până se va reactiva locația principală.*

Cele mai importante operațiuni care trebuiesc luate în considerare de către o organizație, în procesul de funcționare normală sunt următoarele:

a. *Prevenirea pierderii datelor și capabilitatea de recuperare*

În cadrul operațiunilor zilnice este foarte important să se aibe în vedere securitatea și protecția datelor prelucrate. Datorită faptului că siguranța datelor procesate este esențială în orice organizație, prevenirea pierderii datelor și recuperarea acestora în caz de dezastru este critică. Obiectivul principal al unui plan de salvare a aplicațiilor și datelor critice este acela de a permite restaurarea acestora într-un timp foarte scurt și cu pierderi minime. În cadrul unui astfel de plan vor fi incluse următoarele puncte:

- *Identificarea datelor și aplicațiilor care trebuiesc salvate;*
- *Tipul de salvare pentru diferite seturi de date (salvare completă, parțială, incrementală, continuă);*
- *Regularitatea cu care se vor face salvările;*
- *Unde vor fi păstrate salvările;*
- *Cine are acces la salvările efectuate;*
- *Perioada de timp necesară pentru a fi păstrate datele până vor fi distruse.*

Salvările efectuate trebuiesc depozitate, iar accesul la acestea trebuie sa fie rapid și ușor. Locația în care sunt depozitate salvările de siguranță poate avea un impact major în procesul de restaurare a datelor și a serviciilor afectate. Din acest motiv este util ca salvările de siguranță să se regăsească în două locații diferite, astfel încât riscul de pierderea a lor să fi diminuat semnificativ.

b. *Capabilitatea de a răspunde la incidente*

În crearea planului de răspuns în cazul unui dezastru trebuie avută în vedere atât capabilitatea de a răspunde la incidente cât și identificarea obiectivelor pe termen scurt și pe termen lung, după cum urmează:

- *Identificarea funcțiilor critice și prioritățile pentru restaurare;*
- *Identificarea sistemelor suport necesare funcțiilor critice;*
- *Estimarea potențialelor probleme care pot apare și identificarea resurselor minime necesare pentru recuperare în caz de dezastru;*
- *Alegerea strategiei de recuperare și identificarea elementelor vitale necesare pentru reluarea activității (personal, echipamente, sisteme, etc);*
- *Identificarea persoanei (persoanelor) care vor conduce reluarea activității și procesul de testare;*
- *Calcularea fondurilor necesare pentru atingerea acestor obiective.*

Planul va trebui sa detalieze și modul de contactare și mobilizare a angajaților, comunicarea între angajați, interfațarea cu furnizori externi.

c. *Mentenanta, monitorizarea și evaluarea jurnalelor de audit*

După finalizarea procedurilor de testare a planului de recuperare în caz de dezastru, este important ca acesta să fie întreținut, actualizat și evaluat în continuu. Aceste activități constau în:

- *Responsabilizarea personalului – fișa postului a persoanelor responsabile de planul de recuperare în caz de dezastru trebuie să conțină detalii despre responsabilitățilre acestor în cadrul planului de recuperare în caz de dezastru;*

- *Revizuirea performanțelor – realizarea (sau nerealizarea) acțiunilor de întreținere a planului de recuperare în caz de dezastru în cadrul unor întâlniri bianule cu persoanele responsabile;*
- *Auditare – echipa de auditare trebuie sa verifice planul și să se asigure că este actualizat și în conformitate cu realitatea. Totodată, echipa de audit va trebui să inspecteze toate locațiile suplimentare în care sunt depozitatea copiile de siguranță, politicile de securitate, configurațiile, etc.*

De asemenea, implicațiile planului de recuperare în caz de dezastru în cazul intreținerii, monitorizării și recuperării trebuie luate în considerare în orice discuții referitoare la achiziționarea de echipamente noi, modificarea celor existente sau a infrastructurilor critice ale organizației.

d. Teste de penetrare

Testarea securităţii reprezintă un element important în procesul de asigurare a continuității activității organizației și constă într-o analiză cuprinzătoare a comportamentului sistemelor și aplicațiilor organizației în condițiile unor scenarii prestabilite de atac informatic.

Scopul testelor de penetrare este acela de a analiza comportamentul aplicațiilor în contextul diferitelor atacuri informatice, fiind analizate vulnerabilitățile care pot exista în aplicațiile dezvoltate sau utilizate. Un test de penetrare complet cuprinde atât teste automate cât și manuale. Testele automate identificâ neglijențe sau erori de programare în aplicațiile utilizate și sunt efectuate cu ajutorul unor programe specializate (vulnerability scanners, fuzzers, code scanners, etc). Testele manuale sunt folosite pentru a analiza aspecte ale aplicațiilor care necesită intuiția umană, identificându-se erori logice de programare.

Este recomandat ca un test de penetrare (extern și intern) să fie efectuat anual. Testele de penetrare nu rezolvă problemele aplicațiilor și sistemelor informatice, ci doar le identifică. După fiecare test de penetrare sunt necesare acțiuni de corectare și actualizare a sistemelor și aplicațiilor în testate.

e. Evaluari de securitate periodice şi modalități de remediere

Lumea securității informatice este în continuă dezvoltare. Există o multitudine de metode de atac și apărare care pot fi utilizate atât pentru a ataca un sistem informatic cât și pentru apărarea acestuia. Evaluarea securității sistemelor informatice se poate realiza prin:

- *Revizuirea politicilor de securitate – politicile de securitate sunt utilizate pentru a verifica prezența și rigurozitatea controalelor de securitate implementate;*
- *Scanare periodică pentru identificarea vulnerabilităților informatice (vulnerability scanning) – aceste programe sunt utilizate pentru a descoperi problemele aplicațiilor informatice, configurații eronate și vulnerabilități de securitate;*
- *Remedierea problemelor de securitate – se realizează pe baza rapoartelor rezultate în urma testelor de scanare periodică de securitate. Remedierea se realizează prin implementarea patch-urilor de securitate furnizate de catre producătorii de software, actualizarea la ultima versiune a aplicațiilor, reconfigurarea sistemelor informatice vizate, etc.*

Teste de penetrare – sunt utilizate în principal pentru evaluarea măsurilor de remedierilor implementate în urma scanărilor de securitate.

IV. Atacuri cibernetice și măsuri de prevenire

4.1. Tipuri de atacuri cibernetice și măsuri de prevenire

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

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

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

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

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

Pericolele și amenințările din spaţiul virtual vizează, în general, reţelele, nodurile de rețea şi centrele vitale, mai exact, echipamentele şi sistemele fizice ale acestora (calculatoare, providere, conexiuni şi noduri de reţea etc.), precum și celelalte infrastructuri care adăpostesc astfel de mijloace (clădiri, reţele de energie electrică, cabluri, fibră optică şi alte componente). În aceeaşi măsură, ele vizează și centrele de date, sistemele de înmagazinare, de păstrare şi de distribuţie a informației, suportul material al bazelor de date şi multe altele.

Însă, înainte de toate, asemenea pericole și amenințări vizează sistemele IT (întreprinderi, linii de producţie, sisteme de aprovizionare cu materiale strategice, infrastructuri de resurse şi de pieţe, institute de cercetări, sisteme de comunicaţii).

Din categoria pericolelor şi amenințărilor împotriva infrastructurilor critice ale spațiului cibernetic fac parte şi următoarele:

- *dezvoltarea rețelelor subversive și neconvenţionale IT;*
- *activitatea tot mai intensă a hacker-ilor;*
- *ciberterorismul.*

Fără un sistem de securitate implementat și funcțional, sistemele informatice, de telecomunicații și datele prelucrate, stocate sau trasportate de acestea pot fi oricând supuse unor atacuri informatice. Unele atacuri sunt pasive - informațiile sunt monitorizate sau copiate, iar alte atacuri sunt active - fluxul de informații este modificat cu intenţia de a corupe sau distruge datele sau chiar sistemul sau rețeaua în sine.
Sistemele informatice și de telecomunicații, rețelele formate de acestea și informațiile pe care le dețin sunt vulnerabile la numeroase tipuri de atacuri dacă nu sunt apărate de un plan de securitate informatică eficient. O descriere a tipurilor de atac și reacții de securitate la îndemâna entităților economice care dețin un sistem de securitate informatică funcțional se poate consulta în **Anexa 2** a prezentului document.

4.2. Dezvoltarea entităților de tip CERT

Contextul actual din domeniul securităţii sistemelor informatice și de comunicații la nivel global, ne arată că interconectarea rețelelor publice cu cele private, convergenţa domeniilor media, IT şi comunicaţii şi folosirea comună a resurselor au crescut considerabil dificultatea de a proteja sistemele informatice și de comunicații. Protejarea acestora este esenţială pentru fiecare sector al economiei, iar obiectivele urmărite sunt:

- *prevenirea acţiunilor îndreptate împotriva sistemelor informatice şi reţelelor de comunicaţii,*
- *reducerea vulnerabilităţii la aceste atacuri,*
- *minimizarea pagubelor şi a timpului de recuperare în urma atacurilor.*

Entitățile de tip CERT (Computer Emergency Response Team) au în vedere prevenirea şi detectarea ameninţărilor de securitate la adresa sistemelor informaționale și răspunsul la ameninţări, pe cât de obiectiv şi eficient posibil, dar şi informarea în legătură cu acestea. Entitățile de tip CERT cooperează prin asigurarea de informaţii legate de incidente de securitate pentru utilizatorii sistemelor informaționale prin intermediul Internet-ului.
Deşi pe termen scurt securitatea presupune îndeplinirea atributelor de integritate, disponibilitate și confidenţialitate, pe termen lung, pentru protecţia valorilor organizațiilor şi asigurarea continuităţii serviciilor sunt necesare urmatoarele măsuri:

- ***Preventive**:*
  - *implementarea de controale în cadrul organizațiilor;*
  - *informarea și conştientizarea publicului;*
  - *coduri de conduită;*
  - *instruirea utilizatorilor.*
- ***Protective**:*
  - *măsuri tehnice de protecţie, utilizarea de echipamente şi dispozitive securizate;*
  - *reglementări;*

- *planuri de recuperare în caz de dezastru.*

- ***De reacţie / combatere**:*
  - *crearea și specializarea organismelor abilitate de lege;*
  - *răspuns prompt și coerent al autorităţilor la incidente;*
  - *cooperare între sectorul public și cel privat;*
  - *cooperare internaţională.*
- ***De revizuire şi perfecţionare continuă:***
  - *controale periodice;*
  - *urmărirea progreselor tehnologice;*
  - *adaptarea la noile tehnologii.*

În prezent, există în lume diferite tipuri de entităţi CERT în diverse tipuri de organizații. Acestea s-au format în sectorul privat, în sectorul public și printr-un parteneriat între sectorul privat și cel public.

Constituirea capabilităţilor operaţionale aferente unei entități de tip CERT, care să poată asigura funcții specifice managementului securităţii sistemelor informatice și de comunicații la nivel național și organizațional, necesită eforturi bugetare semnificative, context în care operaţionalizarea unei astfel de structuri la un nivel minim de funcționare este dificil de realizat.

Pentru a fi operaţională și să poată dispune de capacitatea necesară pentru prevenirea, analiza, identificarea şi reacţia la incidentele cibernetice, o structură de tip CERT necesită o dezvoltare pe trei paliere strategice:

I. Definirea şi crearea capabilităţilor tehnice necesare atingerii obiectivelor.
   - *Definirea, pe principii funcționale, a componențelor tehnice ale sistemului de alertă timpurie şi informare în timp real privind incidentele cibernetice astfel încât să poată asigura operaţionalizarea acestuia.*
   - *Clasificarea incidentelor de securitate în baza unei analize de risc realizate în domeniul securităţii cibernetice, adaptate la riscurile și ameninţările ce se manifestă / se pot manifesta la adresa sistemelor informatice şi de comunicații naţionale, coroborat cu contextul internaţional pe această dimensiune a securităţii globale (din punct de vedere geo-politic și de securitate / militar).*
   - *Definirea acţiunilor concrete derulate pe diverse scenarii de manifestare a incidentelor de securitate cibernetică, în raport cu severitatea și impactul acestora, stabilirea concretă a nevoilor acţionale şi asigurarea capabilităţilor tehnice corespunzătoare/adaptate de intervenţie/reacţie/răspuns.*
   - *Definirea unor politici privind asigurarea cadrului de interoperabilitate tehnică a sistemelor ce se vor interconecta la infrastructura CERT în vederea asigurării unor forme inteligibile de detecţie/raportare/avertizare și răspuns/reacţie la incidente de securitate cibernetică, atât la nivel naţional cât şi asigurarea posibilităţilor tehnice necesare conectării infrastructurii tehnice la structuri constituite la nivel internaţional (ENISA – ECG, TERENA, FIRST, etc.).*

- *Politică de achiziţii orientată spre capabilităţi tehnologice multi-vendor şi asigurarea exploatării la maxim a tehnologiilor create pe teritoriul naţional (mediul academic, companii autohtone în domeniu etc.).*
- *Asigurarea capabilităţilor tehnice necesare derulării de investigaţii digitale ale incidentelor de securitate cibernetică după mecanisme tehnologice și procedurale ce permit utilizarea acestora de către organele de aplicare a legii.*

II. Asigurarea personalului specializat pentru managementul proceselor interne, precum și pentru utilizarea capabilităţilor tehnice create.

- *Definirea competenţelor necesare personalul propriu, pe toate palierele de activitate ale structuii de tip CERT (Ex: analiză de risc, asigurarea funcţionării continue şi recuperare în caz de dezastre, managementul securităţii sistemelor informatice și de comunicații, operarea sistemului de alertă, investigaţii digitale, etc.) prin utilizarea vastei expertize accesibile în acest domeniu, în special în mediul privat și cantităţii semnificative de informații pe acest subiect accesibile prin intermediul unor canale media specializate;*
- *Crearea unui cadru de recunoaştere a organismelor/entităţilor naţionale/internaţionale formatoare de competenţe în domeniul securităţii sistemelor informatice și de comunicații (mediul academic, organisme private interne și internaţionale, etc.). Ex: La nivel internaţional, pe lângă mediul universitar, mai multe organisme/entităţi, de regulă private, furnizează competenţe în domeniu, unele recunoscute de industrie (ISACA, ISC2, CE Council, SANS INSTITUTE, BSI), altele fiind create de producători/furnizori de tehnologii în domeniu.*
- *Selectarea de personal cu competenţe recunoscute în domeniul securităţii sistemelor informatice și de comunicații, în baza unor evaluări riguroase.*

III. Asigurarea cadrului de reglementare necesar legalităţii şi funcționalităţii proceselor instituţionale în raport cu terţi.

- *Promovarea unor propuneri legale fundamentate prin date concrețe (analize de risc, analize de impact, analize de fenomen etc.), care să creeze obligativitatea participării, cel puţin a deţinătorilor de sisteme informatice și de comunicații critice, în cadrul sistemului de alertă timpurie şi informare în timp real, cu precizarea procedurilor concrețe şi evidenţierea investiţiilor necesare acestui demers.*
- *Definirea procedurală a cooperării cu instituţiile de aplicare a legii şi limitele acţionale în raport cu atribuţiile structurilor de tip CERT.*
- *Asigurarea statutului juridic necesar formării de competenţe profesionale în domeniul securităţii sistemelor informatice și de comunicații la nivelul structurilor de tip CERT.*

La nivel național există Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), ca structură independentă de expertiză şi cercetare-dezvoltare în domeniul protecţiei infrastructurilor cibernetice, aflată în coordonarea Ministerului Comunicaţiilor şi Societăţii Informaționale.

CERT-RO îşi desfăşoară activitatea în conformitate cu legislaţia în vigoare şi cu regulamentul propriu de organizare și funcționare, în scopul realizării prevenirii, analizei, identificării şi reacţiei la incidente în cadrul infrastructurilor cibernetice ce asigură funcționalităţi de utilitate publică ori asigură servicii ale societăţii informaționale.

CERT-RO nu are competenţe în domeniul infrastructurilor cibernetice destinate procesării, stocării sau transmiterii informațiilor clasificate care se află în administrarea instituţiilor din domeniul apărării, ordinii publice și siguranţei naţionale. Pentru aceste infrastructuiri, CERT-RO îndeplineşte doar atribuţiile de cooperare, în baza unor acorduri dedicate, încheiate cu structurile de tip CERT din cadrul acestor instituții.

Practic, CERT-RO reprezintă un punct naţional de contact cu structurile de tip CERT care funcționează în cadrul instituţiilor sau autorităţilor publice ori al altor persoane juridice de drept public sau privat, naţionale ori internaţionale.

Anexa nr. 1. Termeni și definiții

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

Spaţiul cibernetic – mediul generat de infrastructurile cibernetice interconectate într-o rețea globală, incluzând conţinutul informațional procesat, stocat sau transmis, precum și acţiunile derulate de utilizatori în acesta.

Securitate cibernetică – starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spaţiul cibernetic.

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

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

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

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

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

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

Criminalitatea informatică – totalitatea infracţiunilor comise prin utilizarea rețelelor de comunicare electronice și a sistemelor de informare sau împotriva unor astfel de rețele sau de sisteme.

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

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

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

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

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

Societatea informațională - este societatea în care producerea și consumul de informație este cel mai important tip de activitate, informația este recunoscută drept resursă principală, tehnologiile informației și

comunicațiilor sunt tehnologii de bază, iar mediul informațional, împreună cu cel social și cel ecologic – un mediu de existență a omului.

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

SQL Injection - Este o tehnică de atac asupra aplicațiilor des utilizată pentru atacarea unei baze de date prin intermediul unui site web. Tehnica exploatează vulnerabilitățile de securitate ale site-ului web care fac posibilă accesarea informațiilor din baza de date sau modificarea acestora prin inserarea de instructiuni SQL în anumite câmpuri din paginile web, care insuficient validate sau incorect proiectate, vor permite executarea de cod în baza de date a aplicației.

Cross-site scripting (XSS) - Este o tehnică de atac asupra aplicațiilor care exploateaza vulnerabilitățile de securitate informatică în special din aplicațiile web, cum ar fi browserele web, care permit atacatorilor să injecteze propriul cod în paginile web accesate de alți utilizatori ai aplicației.

DNS spoofing (DNS poisoning) - Este o tehnică de atac la nivel de servicii care constă în hackingul unui computer, astfel încat acesta va reruta requesturile catre anumite servere cu adrese web către alte adrese, de regulă către computere controlate de atacator.

ISACA - Information Systems Audit and Control Association

ISC2 - International Information Systems Security Certification Consortium

CE Council - Council on Continuing Education

SANS INSTITUTE - SysAdmin, Audit, Network, Security Institute

BSI - British Standard Institution

Anexa nr. 2. Descriere tipuri de atac și reacții de securitate la îndemâna entităților economice care dețin un sistem de securitate informatică funcțional

Nr. Crt.	Tip de atac informatic	Descriere	Masuri de prevenire și de eliminare a efectelor producerii atacului
1.	Atacuri ce vizeaza exploatarea vulnerabilităților serviciilor sau aplicațiilor	Acest gen de atacuri vizează servicii și aplicații ale căror versiuni sunt cunoscute a avea vulnerabilități sau sunt necorespunzător configurate. De regula acest tip de atac este precedat de scanarea porturilor masinilor tinta, pentru a determina versiunile sistemelor de operare și a serviciilor rulate. Rezultatul acestor atacuri poate consta în acces neautorizat la date sau la resurse, execuție neautorizată de cod, indisponibilitate a serviciilor sau a aplicațiilor. Vulnerabilitățile provin din erori de proiectare sau programare (buffer overflows, pointeri inițializați sau folosiți în mod eronat), lipsa unei verificări a datelor introduse de utilizatori în aplicații (formatarea greșită a stringurilor, prelurarea incorectă a caracterelor speciale, SQL injection, code injection, e-mail injection, HTTP header injection, HTTP response splitting, directory traversal și cross-site scripting în aplicațiile web) sau rularea unor aplicații cu drepturi ce permit escaladarea de privilegii, premițând unui eventual atacator să preia controlul asupra unor resurse ale sistemului informatic vizat.	1. Elaborarea și implementarea de politici de securitate care să reglementeze și să automatizeze procesele de update pentru produsele software folosite în cadrul organizației, multe din aceste actualizări vizând remedierea unor vulnerabilități 2. O mentenanță riguroasa a hardware-ului, în sensul unei corecte configurări din punct de vedere a securității și a actualizării firmware-ului de fiecare dată când apar noi versiuni 3. Teste periodice de penetrare și audituri de securitate 4. Testarea aplicațiilor dezvoltate in-house 5. Folosirea de echipamente specializate în detecția și prevenirea acestor tipuri de atacuri (IDS și IPS - tehnologii ce se bazează pe recunoașterea atacurilor), web application firewall sau web filtering 6. Folosirea unui SIEM - software de analiza a evenimentelor de securitate și a comportamentelor anormale din rețea ce sunt extrase din jurnalele aplicațiilor și sistemelor și echipamentelor din rețea 7. Implementarea de măsuri de protecția datelor prin proceduri de back-up, replicare și disaster-recovery care să asigure disponibilitatea datelor în orice condiții.
2.	Atacuri de tip phishing	Phishing-ul este comportamentul infracțional prin care se încearcă obținerea de informații (şi, uneori, în mod indirect, de bani), cum ar fi nume de utilizator, parole, detalii despre carduri de credit prin falsificarea unei entități legitime într-o	1. Imbunatațirea autenticității site-ului. Rădăcină a problemei acestui tip de înțelăciune este că utilizatorii nu sunt capabili să identifice dacă site-ul este original sau fals. Privind URL-ul și certificat-ul SSL atent îți poți da seama ușor de fals în cele mai multe cazuri, dar nu toţi utilizatorii au timp și nici aptitudini tehnice pentru a analiza și a lua hotărârea corectă. O metodă eficientă este de a personaliza pagina de conectare pentru fiecare utilizator. Conectarea se poate

Nr. Crt.	Tip de atac informatic	Descriere	Masuri de prevenire și de eliminare a efectelor producerii atacului
		comunicare electronică. Mesajul transmis victimei simuleaza că ar proveni de la site-uri bancare, de licitaţii, procesatori de plăţi online sau administratorii IT și sunt de obicei utilizate pentru a atrage publicul neavizat. Phishing-ul este de obicei efectuat prin e-mail spoofing sau mesaje instant, şi de multe ori direcţionează utilizatorii să introducă detalii confidențiale pe un site fals al cărui aspect este aproape identice cu cel legitim. Mai nou a apărut conceptul de spearphishing. Acesta este similar cu phishing-ul, diferența majoră constând în faptul ca atacul vizează ținte clar identificate și este combinat cu elemente de inginerie socială, în scopul de a induce ideea că mesajul provine de la o persoană cunoscută în cadrul organizației vizate.	face în două etape. În primul rând utilizatorul introduce doar user-ul şi nu parola. Odata ce user-ul este regăsit, serverul returnează o pagină în cazul în care utilizatorul primeşte pentru a vedea o imagine pe care el a ales-o, la momentul înregistrării. În cazul în care imaginea este potrivită el furnizează parola şi totul este ok. Dacă imaginea nu este corectă se ridică o alertă și clientul nu furnizează parola. Atacatorul nu poate ști ce imagine va trebui arătată utilizatorului. Metoda nu este 100% infailibilă dar ingreunează misiunea atacatorului. 2. Parole intr-o singură incercare Transmiterea parolei este insoțita de un cod furnizat de un token care este valabil doar o perioada foarte scurta de timp de regula 60 de secunde. Nici această metodă nu este 100% infailibilă dar ingreunează misiunea atacatorului dacă nu folosește datele furnizate în cele 60 de secunde. O metodă puțin diferită este reconfirmarea accesului cu un cod trimis prin alt sistem (sms) dar acest lucru induce o serie de dificultăți de costuri și de limitare a accesului. 3. Parole separate pentru acces și tranzacționare Userul va trebui să utilizeze o parolă pentru acces și altă parolă pentru tranzacțiile pe care le efectuează. 4. Personalizarea comunicărilor pe email Phishing-ul începe cu un e-mail. Cum vor diferenția utilizatorii un mail de phishing față de unul la un centru autorizat? Dacă putem personaliza email-urile autorizate să includă unele detalii la care atacatorii nu vor avea acces la, există o şansă ca userii să identifice e-mail-urile de phishing care nu au oricare dintre aceste detalii. Unele detalii care ar putea fi incluse în comunicările prin e-mail sunt numele Clientului complet şi ultimele 4 cifre ale numărului contul său. 5. Educarea utilizatorilor Poate cel mai bun mecanism de protectie, dar cel mai greu de pus în aplicare. Dacă putem educa utilizatorii despre cum să detecteze un e-mail/site de phishing și cum poate accesa site-ul web original în siguranţă, o mulţime de atacuri de tip phishing nu ar reuşi. Am putea pune aceaste informații pe pagina de login sau îl putem trimite ca e-mailuri. Metoda variază în funcție de tipul de activitate și de canalele disponibile pentru a ajunge la utilizator. Mai dificil de contracarat este atacul de tip phishing dacă faptuitorul acționează de pe teritoriul altor țări, în acest caz autoritățile române au posibilitatea de a colabora cu instituții internaționale sau cu cele din țările în care atacatorii acționează. De asemenea organizația atacată are posibilitatea de a solicita ISP-ului care furnizeaza găzduirea

Nr. Crt.	Tip de atac informatic	Descriere	Masuri de prevenire și de eliminare a efectelor producerii atacului
			domeniului pentru atacator sa-i blocheze acestuia site-ul falsificat.
3.	Software nociv (malware)	Malware" este un termen general folosit pentru a se referi la o varietate de forme de software conceput în scopul de a aduna informații confidențiale sau de a obține acces neautorizat la resurse informatice. Aici putem include viruşii, viermii, troienii, spyware, adware, rootkit-uri, keyloggere.	1. Elaborarea și implementarea de politici de securitate care să reglementeze și să automatizeze procesele de update pentru produsele software folosite în cadrul organizației 2. Implementarea unei politici privind implementarea și actualizarea a produselor anti-virus și anti-malware, folosind mecanisme automatizate. 3. Limitarea drepturilor utilizatorilor, prevenind instalarea de software neautorizat sau încercările nelegitime de escaladare a drepturilor. 4. Având în vedere ca tendința de propagare a malware-ului se manifestă pregnant din direcția traficului web și e-mail, filtrarea acestui tip de trafic folosind tehnologii de web&e-mail filtering ce includ motoare anti-malware, mecanisme anti-spam, DNSBL și URL-categorization Următoarea este o listă de strategii comună pentru protecţia datelor: 1. Copiile de rezervă facute pe bandă să fie trimise periodic la o altă locație 2. Copii de rezervă pe disk să fie făcute la locație și copiate pe alt disk la altă locație sau copiate direct la altă locație 3. Replicarea datelor esențiale la o altă locație 4. În multe cazuri, se poate alege să se apeleze la un furnizor extern specializat pe recuperare care să ofere un stand-by site care să fie folosit în caz de dezastru.
4.	Interceptarea comunicatiilor (passive wiretapping)	Acest tip de atac consta în interceptarea ilegala a comunicațiilor de voce sau de date vehiculate printr-o rețea de transmisii de voce sau de date.	Sistemele, rețelele, echipamentele și informațiile sensibile sau critice pentru o organizație ar trebui să fie protejate fizic intr-un perimetru de securitate delimitat, cu bariere de securitate adecvate şi mecanisme de control al accesului. Mecanisme speciale pot fi necesare pentru a proteja împotriva riscurilor sau accesului neautorizat şi pentru a proteja instalaţiile de suport, cum ar fi alimentarea cu energie electrică și infrastructura de cablare. Protecţia oferită trebuie să fie proporţională cu riscurile identificate. Instituirea unei politici de clear-desk este recomandată pentru a reduce riscul de acces neautorizat. Totodata, pentru acele rețele de comunicații prin care sunt vehiculate informații sensibile, se pot implementa mecanisme de criptare și, în general, se recomandă folosirea unor versiuni criptate (secure) a protocoalelor de comunicații, acest lucru fiind posibil atât pentru comunicațiile voce, cât și date, având în vedere serviciile de unified-communications oferite de actorii din piața TELCO. Dacă comunicațiile vă sunt interceptate luați legatura cu compania care va furnizeaza serviciile de transfer

Nr. Crt.	Tip de atac informatic	Descriere	Masuri de prevenire și de eliminare a efectelor producerii atacului
			de date. Compania va inspecta liniile pentru a identifica dispozitivele de interceptare. Dacă sunt găsite astfel de dispozitive, compania va verifica pentru a vedea dacă acestea sunt autorizate. Compania vă va avertiza dacă interceptarea este ilegală. Aceasta va notifica, de asemenea, organele legii şi va inlătura dispozitivul. Dacă o companie sau organizație identifică interceptarea în mod intenţionat a comunicațiilor are mijloace legale pentru o acţiune în justiţie. Dacă aveţi sau compania de telefonie a găsit un dispozitiv de interceptare ilegal, trebuie să fie notificate autoritățile naționale în vederea luării măsurilor adecvate de aplicare a legii.
5.	Atacuri de tip Distributed Denial-of-Service (DdoS)	În atacurile de tip Distributed DoS (DDoS), un atacator instalează un agent sau un demon pe numeroase computere. Atacatorul trimite o comandă pentru a lansa atacul unui computer master, care poate fi oricare dintre multele computere gazde. Masterul comunică cu agenţii residenți în alte servere pentru a începe atacul. Atacurile DDoS sunt mai greu de combatut, deoarece blocarea unei singure adrese IP sau de rețea nu va opri atacul. Atacurile pot proveni de la sute sau chiar mii de sisteme individuale şi, uneori, proprietarii computerelor nu sunt măcar conştienţi de faptul că mașinile lor sunt parte a unui atac informatic. Un atac DDoS se soldează cu supraîncărcarea aplicațiilor cu sute de cereri invalide sau, cel mai frecvent, pe transmiterea unui volum mare de trafic aparent legitim (de ordinul Gbps), care saturează banda de acces a clientului final, ducând la imposibilitatea accesării oricărui serviciu.	Organizația interesată în a se proteja împotriva atacurilor de tip DDoS poate opta pentru soluții informatice specializate care se bazează pe echipamente hardware performante, dotate cu interfeţe de rețea specializate. Un astfel de serviciu are rolul de a monitoriza în permanență logurile și nivelul de trafic către adresele IP ale clientului, iar în cazul detectării unui atac traficul este redirecționat prin echipamente de curățare. În faţa atacurilor de acest tip, majoritatea furnizorilor de Internet aleg ca metodă de protecţie traffic blackholing. Mai exact, adresele IP atacate sunt anunţate în mod automat furnizorilor de nivel superior, care blochează în totalitate traficul spre acestea pentru un interval de timp. Metoda este simplă, protejează restul capacităţii de acces Internet, atât a clientului, cât şi a furnizorului, însă serviciile de pe serverele atacate rămân indisponibile pe toată durata aplicării acestor filtre (există cazuri în care atacurile durează zile întregi). Necesitatea asigurării continuităţii serviciilor a făcut ca un număr în creştere de furnizori să adopte metode de tip traffic cleaning - filtrare a traficului de tip flood şi livrarea către client doar a traficului legitim. Practic, în momentul detectării unui atac către o adresă IP, traficul este redirecţionat prin echipamente specializate aflate în data center-ele furnizorului, unde se identifică tipul atacului și se aplică filtre care îl blochează sau îi reduc intensitatea. Durata acestor operaţii este de ordinul a câtorva secunde, iar impactul asupra utilizatorilor serviciului este minim, de multe ori insesizabil. Acest tip de protecţie implică, însă, investiţii importante din partea furnizorului. Pentru a putea susţine atacuri de intensităţi mari (de ordinul Gbps), furnizorul de Internet trebuie să îşi supradimensioneze capacităţile de acces metropolitane şi internaţionale, pentru a lăsa loc vârfurilor de trafic care apar în astfel de situaţii. Un alt cost important este cel al echipamentelor de protecţie care, în funcție de capacitatea filtrată, tipurile de atacuri recunoscute şi posibilităţile de upgrade pot ajunge la preţuri foarte ridicate.