CONTRACARAREA POTENȚIALELOR AMENINȚĂRI ȘI GESTIONAREA INCIDENTELOR ÎN REȚELE INFORMAȚIONALE

Andrei ȘESTACOV[1]
Nicoleta POGOR[2]

Rezumat: *Dat fiind faptul, că procesul informatizării are un caracter global, infrastructura informaţională şi de telecomunicaţii este supusă ameninţării atacurilor electronice care poartă un caracter transfrontalier, reieşind din aceste considerente securitatea informaţională prezintă o problemă pentru toată comunitatea mondială care are scopul protejarea şi asigurarea accesibilităţii, confidenţialităţii şi integrităţii informaţiei, prevenirea scurgerilor de informaţii, minimizarea efectelor negative ale evenimentelor ce reprezintă un pericol pentru securitatea informaţională.*

Cuvintele cheie: *Securitatea cibernetică, sistemul informțional, riscuri şi ameninţări cibernetice, tehnologii informaționale (IT), prevenirea,contracararea, strategia securităţii informaționale.*

Summary: *Given that the process of computerization is global, information and telecommunications infrastructure is subject to the threat of cross-border electronic attacks, and therefore information security is a problem for the whole world community, which aims to protect and ensure accessibility, confidentiality and integrity of information, prevent leaks, minimize the negative effects of events that pose a threat to information security.*

Introducere. Dinamica tehnologiei informaţiei induce noi riscuri pentru care instituțiile trebuie să implementeze noi măsuri de control.Lucrul în reţea şi conectarea la Internet induc şi ele riscuri suplimentare, de acces neautorizat la date sau chiar fraudă. Dezvoltarea tehnologică a fost acompaniată şi de soluţii de securitate, producătorii de echipamente şi aplicaţii incluzând metode tehnice de protecţie din ce în ce mai performante. Totuşi, în timp ce în domeniul tehnologiilor informaţionale schimbarea este exponenţială, componenta umană rămâne neschimbată.

[1] Locotenent-colonel, șef catedră Comunicații și Informatică, catedra Științe Militare, Facultatea Științe Militare, Academia Milatară a Forțelor Armate „Alexandru cel Bun ”.
[2] Soldat clasa III, student anul 3, Academia Militară a Forţelor Armate „Alexandru cel Bun”.

Spaţiul cibernetic se caracterizează prin anonimat, dinamism şi lipsa frontierelor. Acest fapt generează atât oportunități de dezvoltare a societăţii informaţionale, cât și riscuri la adresa funcţionării acesteia la toate nivelele (individual, statal şi interstatal).

Tema în sine o considerăm de actuală, deoarece securitatea informațională,la fel ca și protecția datelor, este o sarcină complexă,care are scopul furnizării securității,realizabilă prin implementarea unui sistem de securitate. Astfel una din premizele dezvoltării unei societăți sigure, sănătoase și puternice în Republica Moldova este contracararea riscurilor și amenințărilor la adresa securității cibernetice a republicii.

Riscurile de atac și amenințările la care sunt supuse rețelele informaționale. Tehnologia este omniprezentă și tot mai complexă pentru aproape fiecare aspect al societății moderne. Industria IT inițială a avansat tot mai mult cu industria comunicațiilor într-un sector combinat, denumit în mod obișnuit Tehnologia Informației și Comunicațiilor (TIC).

Penetrarea sistemelor informaţionale sau de comunicaţii electronice ale autorităţilor administraţiei publice şi ale altor instituţii şi întreprinderi de stat sau private, în cadrul cărora se gestionează informaţie sensibilă, poate duce la compromiterea confidenţialităţii, integrităţii sau disponibilităţii acestei informaţii, şi prin urmare, la cauzarea prejudiciilor financiare sau de altă natură, inclusiv la afectarea securităţii statului. De asemenea, penetrarea sistemelor informatice aferente infrastructurii critice ale Republicii Moldova poate duce la obţinerea controlului neautorizat asupra acestor sisteme, şi în consecinţă, la afectarea proceselor economice, sociale, politice, informaţionale, militare etc.

Sistemul informațional este ansamblul de elemente implicate în procesul de colectare, transmisie, prelucrare a datelor. Rolul sistemului informațional este de a transmite informația între diferite elemente.

În cadrul sistemului informațional se regăsesc: informația vehiculată, documentele purtătoare de informații, personalul, mijloace de comunicare, sisteme de prelucrare a informației, etc. Printre posibile activități desfășurate în cadrul acestui sistem, pot fi enumerate:

- achiziționarea de informații din sistemul de bază;
- completarea documentelor și transferul acestora între diferite compartimente;
- centralizarea datelor, etc;

Atacul este o asaltare a securităţii unui sistem, ce va duce la încălcarea politicii de securitate a acelui sistem. Orice activitate dăunătoare ce pretinde să colecteze, modifice sau să distrugă resursele informaţionale a unui sistem poate fi considerat un atac. Există multe motive care pot provoca un atac în reţea. Persoanele care fac aceste atacuri sunt numiţi hackeri sau crackeri.[3]

Cele pasive sunt dificil de detectat, din cauza că ele nu lasă urme după activitatea sa, ci doar monitorizează şi scanează traficul dintre calculatoare. Exemple de atacuri pasive sunt sniffingul pachetelor de date şi analiza traficului.[4]

Atacurile active reprezintă încercările de a face modificări neautorizate în sistem. Ele sunt uşor de detectat, dar pot aduce daune mult mai mari decît atacurile pasive. Ele pot include modificarea datelor transmise sau stocate, sau chiar crearea noilor fluxuri de date pentru a obţine acces la calculator. Exemple de atacuri active sunt: atacurile DoS, DDoS, viruşii, viermii, troienii, backdoor-urile, replay-ul, spargerea parolelor, ingineria socială, spoofing-ul, sniffing-ul şi alte atacuri bazate pe protocoale. Gestionarea riscului pentru sistemele informatice este considerată fundamentală pentru asigurarea unei securități informatice eficiente. Riscurile asociate cu orice atac depind de trei factori: amenințările (cine atacă), vulnerabilitățile (punctele slabe pe care le atacă) și impactul (ceea ce face atacul). Amenințările cibernetice pot proveni de la persoanele care practică sau ar putea efectua atacuri cibernetice. Atacatorii se încadrează în una sau mai multe din următoarele categorii:

- hackeri - persoane, mai ales tineri, care pătrund în sistemele informatice din motivaţii legate mai ales de provocare intelectuală, sau de obţinerea şi menţinerea unui anumit statut în comunitatea prietenilor;
- șpioni - persoane ce pătrund în sistemele informatice pentru a obţine informaţii care să le permită câştiguri de natură politică;

[3] Autor, STĂNESCU Mihaela, Articol: Internetul sub amenințare: viruşii informatici, accesat la data de 24.10.20, ora 14.00.
[4] Autor, APETRII Maria, Lucrare științifică, „ Securitatea rețelelor, metode de atac și protecție" pag. 5.

➢ terorişti - persoane ce pătrund în sistemele informatice cu scopul de a produce teamă, în scopuri politice;

➢ atacatori cu scop economic - pătrund în sistemele informatice ale concurenţei, cu scopul obţinerii de câştiguri financiare;

➢ criminali de profesie - pătrund în sistemele informatice ale întreprinderilor pentru a obţine câştig financiar, în interes personal;

➢ vandali - persoane ce pătrund în sistemele informatice cu scopul de a produce pagube.

Există multe tipuri diferite de atacuri DoS: Ping of Death, Atacuri Teardrop, Atacuri peer-to-peer, Permanent Denial of Service (PDoS), Flood la nivelul de aplicaţie, SPAM-ul.

DDoS(Distributed Denial of Service) - reprezintă atacul în care un singur server este atacat de multe calculatoarea Zombie, care sunt infectate de hacker prin diverse metode, de obicei prin intermediul programelor malware, în care este înscris adresa IP a victimei, deci nu este nevoie de interacţiunea atacatorului pentru a realiza atacul, deşi în unele cazuri el poate prelua controlul asupra calculatoarelor infectate (Figura 1.1.).

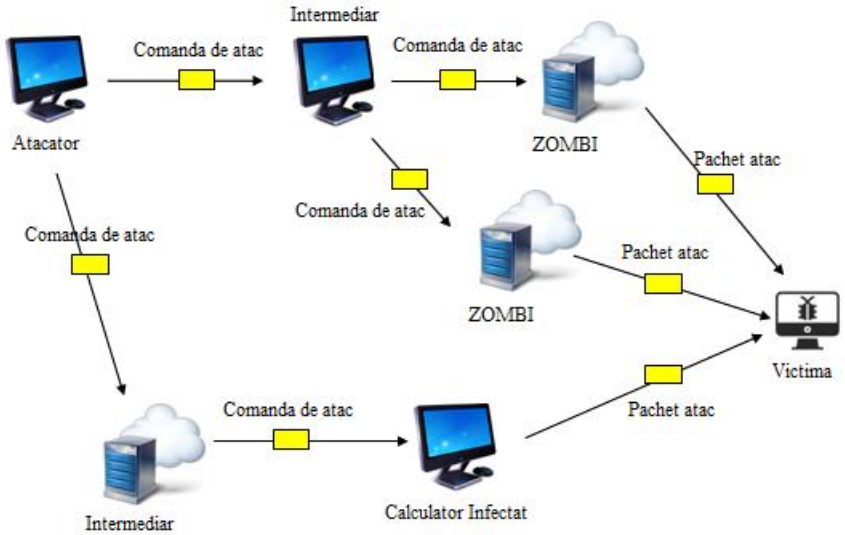

Figura 1.1. Reprezentarea unui atac Denial-of-Service

Software-ul de protecţie împotriva virușilor, cunoscut sub denumirea de software anti-virus, este special conceput pentru a detecta, dezactiva şi elimina virușii, viermi, troieni înainte ca aceștia să infecteze un calculator. Software-ul anti-virus devine repede depășit şi este responsabilitatea tehnicianului de a aplica cele mai recente actualizări, patch-uri, precum şi definiții ale virușilor ca parte a unui program regulat de întreţinere. Multe organizații stabilesc în scris o politică de securitate, precizând că angajaților nu li se permite să instaleze nici un software care nu este oferit. De asemenea, se aduce la cunoștință fiecărui utilizator de pericolele la care se expun atunci când deschid atașamentele e-mail-urilor care ar putea conține un virus sau un vierme.

Principalele ameninţări la adresa securităţii informaţionale sunt:

➢ acțiunile subversive în scopul influenţării politicii interne şi externe a statului;

➢ ameninţările hibride de securitate în scopul subminării securităţii naţionale;

➢ dominația informațională externă pe teritoriul necontrolat de către autoritățile constituționale ale Republicii Moldova;

➢ elaborarea și aplicarea, de către alte state și entități, a concepţiei de război informaţional;

➢ subminarea informaţională a campaniilor electorale;

➢ alterarea conţinutului informaţiilor vehiculate în spaţiul public (prin manipulare, dezinformare, prin tăinuirea sau falsificarea informaţiei) cu scopul de a genera panică, tensiuni ori conflicte sociale;

➢ îngrădirea accesului la informaţiile publice;

➢ difuzarea materialelor cu caracter extremist, a pornografiei infantile şi a mesajelor psihologic distructive;

- activitatea organizaţiilor extremiste şi teroriste, interesul acestora privind posesia şi utilizarea armei informaţionale;
- monopolul asupra formării, recepționării sau răspândirii informaţiei, inclusiv prin intermediul reţelelor de comunicaţii electronice;
- criminalitatea informatică transnaţională, activitatea organizaţiilor criminale internaţionale, a grupurilor sau persoanelor, orientate spre obţinerea accesului neautorizat la resursele de reţea şi informaţie;
- acțiunile de distrugere, deteriorare sau suprimare radioelectronică a resurselor şi sistemelor informaţionale, a reţelelor de comunicaţii electronice şi a sistemelor de protecţie a informaţiei;
- activitatea ilegală a structurilor politice, economice, militare, activitatea de spionaj a serviciilor speciale străine, a unor grupuri sau persoane, orientate spre obținerea accesului neautorizat la resursele informaţionale sau obținerea controlului asupra funcţionării resurselor, tehnologiei informaţiei, sistemelor informaţionale şi reţelelor de comunicaţii electronice;
- nivelul redus de utilizare a tehnologiilor informaționale de către autorităţile administraţiei publice, de către instituțiile financiare de creditare, precum şi în domeniul industriei, al agriculturii, al educaţiei, al sănătăţii, al deservirii populației;
- nivelul redus de instruire a populaţiei privind utilizarea sistemelor informaţionale;
- diversiunile informaționale;
- lipsa culturii de securitate informațională;
- alocarea insuficientă a mijloacelor financiare pentru măsurile de asigurare a securității informaţionale;
- delimitarea neclară a atribuţiilor autorităţilor administraţiei publice responsabile de elaborarea şi realizarea politicii de asigurare a securităţii informaţionale a Republicii Moldova[5] .

În ultimii ani Republica Moldova a înregistrat progrese cu pași mari în implementarea tehnologiilor informaţionale, fiind denumită și Imperiul Internetului.

Republica Moldova își consolidează pozițiile în ratingurile internaționale. Conform datelor SpeedTest.net pentru anul 2020, Republica Moldova se află pe locul 50 la conexiuni de internet broadband cu o viteză de megabiți pe secundă (Mbps). Totodată, ne aflăm pe locul 53 la conexiunea la internet pe mobil, cu o viteză de 33.03 Mbps.[6] Potrivit datelor Netindex, la 31 martie 2014, viteza medie de acces (de descărcare) la Internet în Republica Moldova era de 31,4 Mbps şi corespundea locului 16 din clasament.

Astfel, la acest indicator ţara noastră în doar 7 luni a urcat 10 trepte. Conform Molddata zeci de mii de atacuri cibernetice sunt lansate în fiecare secundă. Zi de zi, au loc atacuri pe Internet menite să afecteze sisteme informatice, site-uri și rețele, dar adesea este dificil de a vizualiza acest tip de activitate. Atacurile cibernetice sunt lucruri abstracte despre care auzim în timp sau după ce s-au întâmplat.

Kaspersky Security Bulletin 2019 furnizează date despre gradul de securitate de navigare pe Internet, conform cărora Republica Moldova prezintă un risc, atingând nivelul de 3,37 % la amenințările locale, 3,05% verificare la cerere, 2,19%- amenințări web, 0,84%- atacuri de rețea, 0,02%- malware mail, 0,27%- spamuri.

Potrivit Planului de acțiuni privind implementarea Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016–2020, în perioada de referință sunt prevăzute să fie realizate 50 de acțiuni. Acțiunile din Planul menționat sunt repartizate pe următoarele domenii de intervenție:

1) procesarea, stocarea şi accesarea în siguranță a datelor, inclusiv a celor de interes public;
2) securitatea şi integritatea rețelelor şi a serviciilor de comunicații electronice;
3) dezvoltarea capacităților de prevenire şi de reacție urgentă la nivel
4) prevenirea şi combaterea criminalității informatice;
5) consolidarea capacităților de apărare cibernetică;
6) educația, formarea şi informarea continuă în domeniul securității cibernetice;
7) cooperarea şi interacțiunea internațională în domeniile ce țin de securitatea cibernetică.

---

[5] LEGEA Nr. 299 din 21.12.2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova Publicat : 16.02.2018 în Monitorul Oficial Nr. 48-57 art Nr.122.

[6] Articol: Top 10 țări cu cele mai rapide conexiuni la internet în 2020. Unde se află Republica Moldova. Sursa :Cotidianul.md https://cotidianul.md/2020/06/10/top-10-tari-cu-cele-mai-rapide-conexiuni-la-internet-in-2020-unde-se-afla-republica-moldova/ accesat la data de 28.10.2020,ora 16.30.

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.[7]

Strategia securității informaționale. Tehnologiile informaționale, resursele de informare şi sistemele de comunicare electronică au devenit parte indispensabilă a tuturor domeniilor de activitate ale persoanei, societății și statului. Prin dezvoltarea lor accelerată, tehnologiile informaţionale contribuie la transformări sociale de esenţă, fiind un generator pentru apariţia şi consolidarea societăţii informaţionale de nivel naţional, regional şi internaţional, depăşind cadrul juridic al frontierelor de stat sau al comunităţilor de state.

Spaţiul informaţional a devenit un domeniu de activitate vital pentru stat, economie, ştiinţă, societate şi individ, un spaţiu nou de reglementare a drepturilor şi libertăţilor fundamentale ale omului, cu implicare directă şi indirectă asupra mecanismelor de asigurare a politicilor de securitate şi apărare naţională într-o societate democratică.

Pe parcursul ultimului deceniu, Republica Moldova a realizat mai multe strategii, programe şi politici de ţară pentru dezvoltarea societăţii informaţionale la nivel naţional, în conformitate cu recomandările forurilor europene şi internaţionale din domeniul tehnologiilor informaționale și comunicaţiilor electronice, al drepturilor şi libertăţilor fundamentale ale omului în mediile on-line şi off-line.

Interacţiunea tehnologiilor informaţionale cu diversitatea conţinutului informaţional, pe de o parte, şi fuziunea reţelelor de comunicare publică şi socială cu sistemele electronice guvernamentale, pe de altă parte, contribuie la o extindere şi sinergie a spaţiului informaţional cu domeniile centrale de securitate şi apărare naţională, responsabile de asigurarea suveranităţii, independenţei şi integrităţii teritoriale a Republicii Moldova.

Pe lîngă beneficiile incontestabile ale tehnologiei moderne, spaţiul informaţional este supus unui șir de vulnerabilități, riscuri şi ameninţări de securitate, facilitând competiţia injustă, confruntarea şi spionajul, dezinformarea şi propaganda, terorismul şi criminalitatea, iar încălcările de confidenţialitate determină răspîndirea de noi forme de ură şi incitare la violenţă, în special pe criterii de gen, rasă, naţionalitate, origine etnică, limbă, religie, apartenenţă politică sau pe orice alte criterii, care rămîn subestimate şi rareori remediate sau contracarate.

Creşterea numărului de utilizatori ai Internetului şi evoluţiile tehnologiilor informaţionale conexe creează provocări substanţiale în ceea ce privește starea mediului de securitate, ordinea publică şi apărarea, prevenirea criminalităţii şi aplicarea legii în direcţia protecţiei drepturilor în spaţiul informațional.

Totodată, Republica Moldova a adoptat Strategia securității informaționale pentru anii 2019–2024 cu scopul de a corela juridic şi de a integra sistemic domeniile prioritare cu responsabilităţi şi competenţe de asigurare a securităţii informaţionale la nivel naţional, fiind bazat pe rezilienţa cibernetică, pluralismul multimedia şi convergenţa instituţională în materie de securitate,destinate protejării suveranităţii, independenţei şi integrităţii teritoriale a RepubliciiMoldova.

Prezenta Strategie descrie situația curentă în domeniul securității informaționale din perspectiva progreselor înregistrate şi atendinţelor de dezvoltare a societăţii informaţionale la nivel naţional, a problemelor existente şi de perspectivă, care generează şi creează riscuri şi ameninţări de securitate, inclusiv hibride. Complexul de acţiuni, conform scopului şi obiectivelor specificate, este compartimentat pe patru piloni:

---

[7] *Cod de bune practici pentru securitatea sistemelor informatice și de comunicații*, p. 6, disponibil la https://cert.ro

1) Pilonul I. Asigurarea securității spațiului informațional-cibernetic și investigarea criminalității informatice;

2) Pilonul II. Asigurarea securității spațiului informațional-mediatic;

3) Pilonul III. Consolidarea capacităților operaționale;

4) Pilonul IV. Eficientizarea proceselor de coordonare internă și decooperare internațională în domeniul securității informaționale[8] .

Dezvoltarea accelerată a tehnologiilor informaţiei şi de comunicaţii moderne ridică la un alt nivel abordarea ameninţărilor, riscurilor şi vulnerabilităţilor într-o societate informaţională. În prezent, la nivel mondial, atacurile cibernetice capătă o frecvenţă, o complexitate şi o amploare din ce în ce mai mari, aducînd pagube enorme sectorului guvernamental, celui privat şi cetăţenilor, ca urmare a caracterului lor asimetric. Accesarea neautorizată a reţelelor şi serviciilor de comunicaţii electronice, modificarea, ştergerea sau deteriorarea neautorizată de date informatice, restricţionarea ilegală a accesului la aceste date şi spionajul cibernetic constituie constrîngeri la nivel global. Ameninţările şi riscurile, atacurile şi incidentele cibernetice, precum şi alte evenimente survenite în spaţiul cibernetic se materializează prin exploatarea vulnerabilităţilor de natură umană, tehnică şi procedurală.

Totodată, conform datelor Centrului de Telecomunicaţii Speciale, numărul atacurilor cibernetice asupra serverelor web a crescut în anul 2014 faţă de anul 2013 cu circa 26%, iar vulnerabilităţile porturilor deschise au sporit cu circa 385%. Posibilităţile de infectare a calculatoarelor cu viruşi informatici au crescut cu circa 27%. Numărul incidentelor asupra poştei electronice guvernamentale s-a micşorat în 2014 faţă de 2013 cu circa 1%. Concomitent, s-a micşorat ponderea acestor incidente în totalul atacurilor cibernetice. În 2014 această pondere s-a diminuat la 40%, faţă de 51% în 2013.

Persistă o serie de probleme specifice ce ţin de asigurarea securităţii cibernetice a Republicii Moldova şi care sunt părţi componente ale problemei de bază identificate mai sus:

1) nu este asigurată siguranţa deplină la procesarea, stocarea şi accesarea datelor publice, indiferent de clasificarea acestora;

2) securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice nu sunt ajustate la standardele şi recomandările Uniunii Europene, Uniunii Internaţionale a Telecomunicaţiilor, la prevederile Acordului de Asociere între Republica Moldova şi Uniunea Europeană;

3) nu există capacităţi suficiente de prevenire şi reacţie urgentă la nivel naţional (CERT), ţinând cont de caracterul asimetric al atacurilor şi incidentelor cibernetice;

4) cadrul legislativ-normativ naţional nu este armonizat integral la prevederile Convenţiei Consiliului Europei privind criminalitatea informatică, instituţiile vizate nu dispun de competenţe clare privind asigurarea securităţii cibernetice;

5) dispunem de capacităţi reduse de apărare cibernetică ca urmare a caracterului asimetric al atacurilor cibernetice;

6) nu sunt asigurate educaţia, formarea şi informarea continuă în domeniul securităţii cibernetice;

7) există o insuficienţă a cooperării şi interacţiunii internaţionale privind identificarea riscurilor, vulnerabilităţilor, altor evenimente survenite în spaţiul cibernetic global şi prevenirea ameninţărilor şi atacurilor cibernetice transfrontaliere.

Importanța măsurilor de prevenire a atacurilor cibernetica. În fiecare zi, suntem expuşi, atât acasă cât şi la locul de muncă, la ameninţări ce îşi au originea în spaţiul virtual. În majoritatea cazurilor nici măcar nu suntem conştienţi de acest lucru, sau dacă-l realizăm, nu reacţionăm la aceste ameninţări într-o manieră adecvată. În media apar zilnic articole referitoare la incidente de securitate şi la impactul pe care acestea îl au asupra noastră, ca indivizi sau organizaţii deopotrivă. Aceste incidente relatate sunt de fapt doar vârful iceberg-ului, în realitate fiind cu mult mai expuşi decât credem noi că suntem având în vedere că, din nefericire, riscurile asociate mediului virtual sunt în continuă creştere. Cu toate că mediul virtual, reprezentat de infrastructurile cibernetice, incluzând conţinutul informaţional procesat, stocat sau transmis, şi acţiunile derulate de utilizatori, este deja o parte integrantă a vieții personale și profesionale, securitatea sa este un

[8] Hotărîre privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 și a Planului de acțiuni pentru implementarea acesteia.

element luat în calcul mult prea rar și poate insuficient. Acest aspect este potenţat de complexitatea noilor tehnologii, care implică noi riscuri ce pot afecta grav individul sau organizația, în condițiile în care există numeroase acţiuni ostile desfăşurate în spaţiul cibernetic de natură să afecteze funcţionarea sistemelor informatice precum şi datele vehiculate prin intermediul acestora.

Acţiunile ostile vizează, în principal:

- perturbarea, blocarea, distrugerea, degradarea sau controlarea în mod maliţios a unui sistem / infrastructură informaţională;
- afectarea integrităţii disponibilităţii, confidenţialităţii, autenticităţii şi non-repudierii datelor sau sustragerea informaţiilor cu acces restricţionat.

De exemplu, date sensibile (contracte, proiecte etc.) pot fi exfiltrate de atacatori informatici sau recuperate de aceștia cu ajutorul unor programe specializate în cazul pierderii sau furtului unui dispozitiv portabil (telefon inteligent, tabletă, laptop etc.).

În consecinţă, securitatea cibernetică trebuie să reprezinte o prioritate pentru buna funcționare a sistemelor guvernamentale sau de control industrial (producția și distribuția de energie electrică, distribuția de apă etc.). Un atac cibernetic asupra unui sistem de control industrial (Superviasory Control and Data Acquisition System - SCADA) poate determina pierderea controlului, oprirea, deteriorarea instalațiilor sau alterarea produsului final. Aceste incidente sunt însoțite adeseori de urmări grave în termeni de securitate, de pierderi economice și financiare și de afectare a imaginii organizației. Pericolele pot fi totuși reduse semnificativ prin aplicarea unei serii de bune practici puțin costisitoare, chiar gratuite, și ușor de aplicat. Conștientizarea riscurilor de către angajați este foarte eficientă pentru a limita o mare parte din riscuri. Măsurile proactive şi reactive pot include politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activităţi de instruire şi conştientizare, implementarea de soluţii tehnice de protejare a infrastructurilor cibernetice, managementul identităţii, managementul consecinţelor.

Concluzii și propuneri. Amenințările cibernetice au devenit un lucru obișnuit în societatea noastră. Ele devin tot mai frecvente, mai diverse și mai complexe reieșind din metodele tehnologice aplicate. Ignorarea lor a devenit imposibilă, deoarece informațiile au devenit un beneficiu absolut și vital, iar confruntarea în spațiul cibernetic duce la pagube economice și fizice considerabile.

Pentru contracararea cu succes a amenințărilor cibernetice este necesar a se concentra asupra următoarelor:

- stabilirea unui cadru conceptual, instituțional (crearea sistemului național de securitate cibernetică, elaborarea legislației, dezvoltarea parteneriatului);
- elaborarea programului național de dezvoltare a potențialului cibernetic (capacităților de prevenire, detectare și contracarare a atacurilor cibernetice, crearea unor structuri specializate, ridicarea nivelului de protecție, dezvoltarea producției produselor de profil);
- consolidarea culturii de securitate informațională (informarea populației, instruirea adecvată a managerilor și a personalului tehnic);
- perfecționarea cooperării internaționale (la nivel de acte normative, schimburi de experiență, de protecție colectivă ompotriva atacurilor de amploare).

Sistemele informaţionale niciodată nu pot fi în siguranţă totală, şi uneori preţul informaţiei este mult mai mare decît preţul acelor sisteme pe care se află, dacă se iau în consideraţie datele confidenţiale, secrete. De aceea, securitatea datelor poate fi un factor critic în economia unei companii. Lupta pentru informaţii nu poate fi stopată, de aceea hackerii vor găsi noi metode complexe de atacuri, pentru a dobîndi informaţiile secrete.

Securitatea unei reţele depinde de foarte mulţi factori, precum am spus, de aceea înainte de a securiza o reţea, este nevoie de a calcula nivelul de protecţie în raport cu datele păstrate în acele sisteme. Un utilizator simplu nu va avea nevoie de securitate foarte ridicată, preţul securizării nu trebuie să depăşească preţul informaţiei.

REFERINȚE BIBLIOGRAFICE:

1. STĂNESCU Mihaela, Articol: Internetul sub amenințare: virușii informatici, accesat la data de 24.10.20.
2. APETRII. Maria, Lucrare științifică, „ Securitatea rețelelor, metode de atac și protecție” pag.5.

3. Legea Nr. 299 din 21.12.2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova Publicat : 16.02.2018 în Monitorul Oficial Nr. 48-57 art. nr.122.
4. Articol: Top 10 țări cu cele mai rapide conexiuni la internet în 2020. Unde se află Republica Moldova. Sursa: Cotidianul.md. https://cotidianul.md/2020/06/10/top-10-tari-cu-cele-mai-rapide-conexiuni-la-internet-in-2020-unde-se-afla-republica-moldova/ accesat la data de 28.10.2020.
5. Hotărîre privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 și a Planului de acțiuni pentru implementarea acesteia.
6. Regulamentul privind asigurarea securităţii informaţionale şi utilizare a resurselor sistemului de comunicaţii şi informatică ale armatei naţionale CI-101.
7. *Cod de bune practici pentru securitatea sistemelor informatice și de comunicații*, p. 24, disponibil la https://cert.ro