PREVIZIUNEA CA INSTRUMENT DE PREVENIRE A ATACURILOR CIBERNETICE

Victoria BEVZIUC
Moldova State University
victoriabevziuc@gmail.com
https://orcid.org/0000-0001-9189-641X

CZU: 004.056.5:343.346.8

Abstract: *Ensuring the prevention of risks and combating threats to information security is one of the basic tasks of the state, implemented through its legal institutions, thus determining the following problems that need to be addressed at the national level. Predicting cyber attacks is imperative in such an environment and is the purpose of this article. There is more research and more data analysis and machine learning in cyber security and attack prediction is no exception. More precisely it can be said that the learning can be used to learn about the attack and automatically anticipate them in time. If data collection and machine learning will only be used to learn about cyber attacks, prediction will still be used for pattern matching. The importance of predicting cyber attacks is an interesting research problem that has been addressed by a large number of researchers.*

Keywords prediction, cyberattacks, crisis, security, information, pattern, model.

Creşterea entropiei în mediul de securitate al începutului de Mileniu III aduce importanţă prognozării. O sinteză valoroasă asupra subiectului este realizată de către Stephen Flanagan, director al Institutului Național pentru Studii Strategice al SUA [1], care arată că abordarea globalizării „impune transformarea modului în care gândim lumea şi concepem politici, impune mai multă sinergie şi dinamism în elaborarea politicilor economice, de securitate şi nu numai”.

De asemenea, globalizarea impune noi abordări în gestionarea schimbării de orice natură şi în controlul crizelor.

Evoluţia istorică a securităţii informaţiilor a debutat odată cu securitatea computerului, care avea drept scop protejarea locaţiilor fizice, hardware-ul şi software-ul împotriva ameninţărilor. Importanţa conectării reţelelor de calculatoare între ele, a condiţionat apariţia şi dezvoltarea Internetului, care a ajuns la publicul larg în anii ’90. Datorită volumului vast de informaţii şi a necesităţii de prelucrare în timp real, cu costuri minime şi accesibilitate mondială, sistemele informaţionale au fost interconectate la reţele. Pentru început, Internetul – instrumentul de partajare a informaţiilor nu fost supus unor standarde, iar informaţiile stocate au devenit expuse ameninţărilor de securitate. În ultimii ani, accentul pus pe securitatea sistemelor informaţionale a crescut

exponenţial datorită conexiunii prin sisteme de operare comerciale şi standarde mondiale precum Ethernet, TCP / IP, dar şi a tehnologiilor web.

Sistemele informatice şi de comunicaţii ale unui stat, precum şi datele gestionate de acestea, sunt tot mai dependente de spaţiul cibernetic. Totodată, mediul cibernetic găzduieşte elementele de manifestare ale lumii reale, începând cu multiple comunităţi de interes şi reţele umane ce se manifestă în mediul virtual. Dincolo de beneficiile evidente pe care acest mediu le are în facilitarea tuturor aspectelor existenţei umane de la cele economice, financiare, sociale, culturale şi până la cele politice şi militare, acesta facilitează şi o serie de riscuri specifice, în special în absenţa unor măsuri de securitate adecvate. Atât entităţile statale, cât şi cele non-statale, în baza propriilor interese, pot recurge la agresiuni cibernetice împotriva competitorilor sau opozanţilor.

Astfel de atacuri cibernetice pot fi îndreptate împotriva sistemelor de tehnologia informaţiei şi de comunicaţii, care fie reprezintă infrastructuri critice în sine, fie sunt esenţiale pentru buna funcţionare a celorlalte infrastructuri critice ale statului. Examinarea punctelor de vedere ale specialiştilor din alte domenii decât domeniul securitate este foarte valoroasă, întrucât supune atenţiei evoluţii şi factori importanţi ai dezvoltării sociale, care pot avea un impact major asupra mediului de securitate.

În condițiile globalizării, cu cât orizontul prognozei este mai îndepărtat, analiştii trebuie să lărgească gama de componente ale vieții sociale pe care trebuie să le ia în considerare iar această cerință tinde să se accentueze pentru orizonturi de prognoză din ce în ce mai apropiate. Noile caracteristici ale viitorului, o entropie ridicată şi o dinamică accelerată, impun atât definirea cât mai fidelă şi mereu actualizată a riscurilor şi provocărilor, cât şi o definire cât mai practică, inclusiv prin flexibilitate, a caracterului mediului de securitate al viitorului.

Nu se poate vorbi despre ameninţări, pentru că ameninţarea presupune intenţie, care este strict umană, deci nu se poate asocia unor persoane care fie nu există încă, fie nu sunt încă în măsură să ia decizii relevante în domeniul securității, deci intenţiile lor nu contează. În cazul definirii riscurilor în mod separat, rolul analizei pe termen lung este destul de clar, pentru că definirea riscurilor duce la planificarea capabilităților, o practică deja consacrată. Astfel, dacă un stat consideră că, în viitor, capacitățile spațiale ale altor state pot atinge niveluri îngrijorătoare, trece la planificarea unor capabilități spațiale proprii.

Aici iese în evidență rolul monitorizării tehnologiilor, atât cele civile cât şi cele militare sau cu valență dual, dar şi monitorizarea capabilităților de altă natură, care pot căpăta relevanță în domeniul securitar (politici economice, de infrastructură, cercetări medicale sau psihologice).

Comitetul pentru Sisteme Naţionale de Securitate (CNSS) defineşte securitatea informaţională ca fiind protecţia informaţiilor şi a elementelor sale critice, inclusiv sistemele şi hardware-ul care utilizează, stochează şi transmite acele informaţii. [2]

Modelul CNSS de securitate a informaţiilor a evoluat dintr-un concept dezvoltat de industria de securitate informatică numit triunghiul CIA. Acesta a fost standardul industriei pentru securitatea computerelor de la dezvoltarea mainframe-ului. Se bazează pe cele trei caracteristici ale informaţiilor care îi conferă valoare organizaţiilor: confidenţialitate, integritate şi disponibilitate. Confidenţialitatea asigură păstrarea datelor secrete, astfel încât, doar persoanele sau dispozitivele autorizate să poată accesa aceste informaţii. Iar dezvăluirea către entităţile neautorizate constituie o infracţiune. Integritatea vizează păstrarea datelor în forma lor originală, garantând nealterarea acestora în procesul de transfer dintre sursă şi destinaţie, nici prin căi ilegale, nici accidental. Integritatea este o măsură a corectitudinii datelor şi a asigurării încrederii în ele. Accesibilitatea este factorul care asigură disponibilitatea datelor şi resurselor în orice moment, persoanelor şi dispozitivelor autorizate.

Începutul secolului XXI este dedicat eforturilor de a dezvolta forme de cooperare şi politici de securitate care să răspundă globalizării insecurităţii, conştientizând, totodată, că globalizarea nu elimină preocupările geopolitice tradiţionale. Kali Linux 2021.3 lansat cu noi instrumente pen test şi îmbunătăţiri Kali Linux 2021.3 a fost lansat la 14 septembrie anul curent, de Ofensive Security şi include un nou set de instrumente, suport de virtualizare îmbunătăţit şi o nouă configuraţie OpenSSL care creşte suprafaţa de atac.

Reducerea resurselor în acest sector în favoarea celor emergente se poate baza pe cooperare şi punerea în comun a resurselor. Colectarea şi diseminarea informaţiilor, raportat la conceptul extins al securităţii naţionale ia în considerare nivelul de percepţie a ameninţărilor şi răspunsul politic la acestea (folosirea forţei militare sau a ameninţării cu forţa, agresiune asimetrică) pentru impunerea voinţei sau apărarea intereselor naţionale. În aceste condiţii, managementul şi exploatarea informaţiei devine decisivă în ce priveşte maximizarea potenţialului fluxului de informaţii, în baza unor principii solide şi eficiente ale sistemului de diseminare.

Alte probleme identificate în efortul de colectare ţin atât de factorii calitativi (credibilitatea sursei şi veridicitatea informaţiei, pregătirea şi experienţa personalului, nivelul de actualizare a tehnologiilor, proceduri, managementul informaţiei), cât şi de cei cantitativi (acoperirea efectivă în timp şi spaţiu a domeniului informaţional, capabilităţi de culegere, reţele de colaborare). În acest cadru, consolidarea culturii de securitate în rândul populaţiei devine o necesitate. Aceasta duce la conştientizarea riscurilor şi responsabilizarea actorilor societăţii civile, cu ecou în acţiunea civică, dar şi în ce priveşte asigurarea cadrului interdisciplinar şi pan-regional al schimbului de informaţii.

Ideea iniţială a proiecţiei atacului datează din 2001 când Geib şi Goldman [3] au propus proiecţia atacului ca o extensie a recunoaşterii planului de atac şi a identificat-o premise şi posibile probleme, cum ar fi nevoia de a lucra cu acţiuni neobservate, neobservare şi consideraţie a mai multor obiective concurente. Au

început să apară primele metode în jurul anului 2003 [4], iar cercetările în acest domeniu sunt încă activ, inclusiv recenzii de literatură [3], [4].

Pentru a proiecta continuarea unui atac şi a prezice evenimentele viitoare, de obicei trebuie să documentăm comportamentul a atacatorilor şi să stabilească o descriere a unui atac pentru utilizare ulterioară. Exemplu de anatomie a unui atac cibernetic a fost dat de Bou-Harb şi colab. [5]. Anatomia constă din următoarele paşi:

1. Scanare cibernetică
2. Enumerare
3. Tentativa de intruziune
4. Elevarea privilegiilor
5. Efectuaţi sarcini rău intenţionate
6. Implementaţi programe malware/Backdoor
7. Ştergeţi dovezile criminalistice şi ieşiţi

Multe tipuri de atacuri cibernetice urmează această secvenţă simplă de evenimente, care pot fi observate fie în traficul de reţea, fie pe sistemul ţintă, unde sistemele de detectare a intruziunilor poate fi găsit. Proiecţia unui atac în curs este, în esenţă, foarte simplu. Dacă vedem o succesiune de evenimente care se potrivesc unui atac model, putem presupune că atacul va continua conform

la model. Astfel, anticipăm următorul pas al adversarului.

Modelele de predicţie pot fi dezvoltate pentru a prezice diferite rezultate ale proiectului şi rezultate intermediare prin utilizarea tehnicilor statistice. Un model de performanţă de proces adoptă conceptele de probabilitate. Acest lucru poate fi, de asemenea, explorat în continuare prin simulări de construcţie. Rezultatele pot fi studiate ca un interval. În funcţie de predicţii, pot fi recomandate corecţii la jumătatea cursului. Modelul poate fi simulat pentru a prezice rezultatele finale pe baza corecţiilor sugerate. Astfel, este un model proactiv care ajută analistul tehnic să analizeze datele şi să prezică rezultatele. Analiştii pot modifica datele şi pot efectua analize de tip what-if. Ei pot înregistra apoi aceste instanţe şi să decidă cu privire la cea mai bună opţiune. Modelul ajută analiştii să decidă ce pârghie să se adapteze pentru a atinge obiectivul final al proiectului. În sistemul actual, accentul pe remedierea vulnerabilităţilor nu se bazează pe impactul potenţial al vulnerabilităţii. În plus, se acordă o importanţă mai mare decât adecvată rezolvării tuturor vulnerabilităţilor sau prea puţină importanţă din cauza constrângerilor de timp şi costuri. Nu este disponibilă o evaluare proactivă a riscurilor înainte de lansarea aplicaţiei IT. Impactul oricărei vulnerabilităţi este identificat prin utilizarea calculatorului CNSS, numai după analizarea modului în care a avut loc atacul. În modelul propus, care a fost, de asemenea, pilotat într-o organizaţie de proiect eşantion, impactul potenţial al vulnerabilităţii este prezis cu mult înainte ca aplicaţia IT să fie lansată pentru utilizare.

Cu aceste informaţii de impact, costurile şi resursele adecvate pot fi alocate pentru rezolvarea vulnerabilităţilor, reducând astfel impactul. Metoda de

regresie multiplă este aleasă pentru a prezice impactul atacurilor în această propunere. Regresiile multiple au anumite ipoteze care stau la baza, cum ar fi liniaritatea, inexistenţa multicollinităţii, homocedasticitatea şi normalitatea.

În încercarea de securizare maximă a sistemelor este restricţionat accesul utilizatorului la informaţii şi impune costuri. Securitatea integrală a sistemelor nu întotdeauna poate fi prognozată, utilizatorii trebuie să îşi concentreze atenţia pe domenii şi funcţii critice şi să aplice măsuri de securitate justificate prin valoarea datelor şi a aplicaţiei. Devine imperativă aplicarea măsurilor de securitate proporţională din punct de vedere al costurilor cu valoarea datelor, riscului şi probabilităţii asociate unui incident de securitate, cât şi consecinţelor incidentului. De aceea este necesară reducerea cheltuielilor prin aplicarea unor practici şi politici bine definite şi eficiente de către personalul calificat. Nu există soluţii universale sau mecanisme complet pliabile pe orice problemă, cum nu există nici reguli absolute care să reglementeze securitatea tuturor sistemelor. Protecţia sistemelor poate fi asigurată corespunzător prin înţelegerea riscurilor şi stabilirea unor limite eficiente ale sistemele informaţionale şi ale dispozitivelor cu care interacţionează. Acest efort necesită să se concentreze nu numai pe tehnologie, ci şi pe oameni.

Fiecare dintre aceste ipoteze este validată pentru încercarea noastră de a stabili relaţia dintre impactul atacului şi factorii de influenţă. Pe baza cercetărilor de mai sus, au fost identificaţi factori care pot influenţa impactul unui atac, şi anume nivelul de protecţie a securităţii asupra sistemului ţintă, utilizarea sau traficul în reţeaua identificată, vulnerabilităţile prezente în sistemul ţintă şi valoarea activelor prezente în reţea. Oluwatosin şi Samson [6] au subliniat provocările aplicaţiilor informatice existente care trebuie luate în considerare din punct de vedere al securităţii. Expertul Shar [7] a analizat vulnerabilităţi anticipate cu caracteristici legate de fluxul de date. Khan şi Hussain[8] au afirmat că este sigur să presupunem că toţi aceşti factori au relaţii liniare individuale cu probabilitatea de atac. O relaţie similară este văzută din cea mai mare parte a impactului unui atac şi a factorilor de mediu luaţi în considerare. Aceasta satisface prima condiţie pentru utilizarea tehnicii de regresie multiplă pentru modelul nostru de predicţie. Policolinitatea şi homoscedasticitatea sunt verificate prin factorul de inflaţie de variaţie (VIF).

Normalitatea este testată prin efectuarea testului Anderson-Darling. În plus, un test de ipoteză este rulat individual pentru fiecare dintre factorii de atac pentru a se asigura că probabilitatea ca factorul să nu influenţeze factorul independent este menţinută la un maxim de numai 0,05. Coeficientul de corelaţie (0) şi coeficientul de corelaţie ajustat (Aj). Acest lucru este suficient pentru a dovedi că printre numeroşii factori care pot provoca un atac, factorii selectaţi prezic impactul unui atac cu cea mai bună precizie posibilă. Adică, numărul de factori, dincolo de un anumit punct, devine nesemnificativ. Definiţia operaţională a metricilor de securitate cibernetică luaţi în considerare este menţionată mai jos. (1) este scorul CVSS global, factorul dependent. CVSS [9, 14] este prezis pe baza

caracteristicilor de mediu şi de sistem ale aplicaţiei ţintă. (2) se referă la numărul de vulnerabilităţi, şi anume numărul total de vulnerabilităţi detectate de instrumentele de detectare a vulnerabilităţilor statice şi dinamice pentru aplicaţia ţintă. Instrumentele instalate şi care rulează împotriva aplicaţiei ţintă pot identifica mai multe vulnerabilităţi bazate pe algoritmi, cum ar fi, dar fără a se limita la algoritmi îmbunătăţiţi sau teste de penetrare. Într-o anumită aplicaţie, vulnerabilităţile raportate de instrumente pot fi clasificate în general în 23 categorii: Abuz API, vulnerabilitate de autentificare, vulnerabilitate de autorizare, vulnerabilitate de disponibilitate, vulnerabilitate de permisiune de cod, vulnerabilitate de autorizare, vulnerabilitate de autorizare, vulnerabilitate de autorizare, vulnerabilitate de autorizare, vulnerabilitate de autorizare a codului, vulnerabilitate de securitate, vulnerabilitate de calitate a codului [10], vulnerabilitate de configurare, vulnerabilitate criptografică, vulnerabilitate de codificare, vulnerabilitate de mediu, vulnerabilitate de gestionare a erorilor, vulnerabilitate de eroare logică generală, vulnerabilitate de validare a intrării, vulnerabilitate de înregistrare şi auditare, vulnerabilitate de gestionare a parolelor, vulnerabilitate de cale, erori de protocol, vulnerabilitate de eroare de interval şi tip, vulnerabilitate de protecţie a datelor sensibilă [11].

Pe baza valorilor de prag selectate, se efectuează analiza dacă ar exista aceste riscuri şi ameninţări. În funcţie de diferitele scenarii, valorile vulnerabilităţii şi ale traficului de reţea sunt asumate şi furnizate ca intrări pentru model. Rezultatul preconizat este apoi comparat cu pragurile. Este important să reţineţi acest lucru în timp ce se schimbă parametrii, analiştii tehnici ar trebui să înţeleagă implicaţiile practice ale proiectului. Nu este vorba doar despre modelul matematic, ci despre modul în care acesta poate fi pus în practică. De exemplu, dacă scorul CVSS este mare, cum poate fi redus? Cum pot fi reduse vulnerabilităţile în timpul proiectării? Trebuie luate în considerare implicaţiile costurilor. Apoi, analistul tehnic trebuie să se uite la constrângerile de mediu.

Deoarece modelul de predicţie ia în considerare factorii cheie de influenţă pentru a prezice CVSS, valorile factorilor de influenţă ar putea afecta planificarea proiectului şi costul proiectului, care trebuie, de asemenea, analizate. Aceste previziuni servesc drept alerte că ar trebui să ia măsuri pentru a atenua ameninţarea atacurilor cibernetice. Prezicerea scorurilor CVSS ajută la prioritizarea vulnerabilităţilor şi la remedierea celor cu riscuri ridicate. Scorurile CVSS sunt partajate de furnizorii de aplicaţii software cu clienţii lor. Acest lucru ajută clienţii să înţeleagă gravitatea vulnerabilităţilor şi le permite să-şi gestioneze eficient riscurile. Buletinele de vulnerabilitate sunt partajate de câteva organizaţii. Aceste buletine împărtăşesc data atacului, sistemele afectate şi pattern-urile efectuate. Astfel, modelul de predicţie CVSS este vital şi ar trebui utilizat pe scară largă. Analiştii tehnici ar trebui să se simtă confortabil folosind modelul de predicţie pe scară largă.

Pentru fiecare scenariu, analistul trebuie să documenteze ipotezele şi riscurile asociate. Un plan detaliat de prevenire a atacurilor ar trebui să fie în vigoare. La fiecare pas, atacul, tipul, cauza şi acțiunea preventivă trebuie documentate. Diferite tehnici de analiză a cauzelor, cum ar fi -de ce, pot fi utilizate pentru a identifica cauza principală. După identificarea cauzei principale, ar trebui să se gândească şi la următorii paşi în ceea ce priveşte acţiunile corective şi preventive. Experţii tehnici ar trebui să revizuiască aceste planuri, astfel încât să poată aduce experienţa lor şi să evidenţieze orice îmbunătăţiri. Modelele de predicţie nu ar trebui să fie o activitate unică.

Analiştii tehnici ar trebui să utilizeze modelul în mod continuu şi să sugereze, de asemenea, deficienţe. Pe baza scorurilor, deciziile trebuie luate luând în considerare impactul asupra costurilor şi securităţii. Modelele de predicţie sunt de natură statistică şi simulativă. Aceste modele ar trebui să ajute la simularea scenariilor, precum şi la determinarea rezultatelor. De asemenea, pot modela diferiţi factori de variaţie şi pot ajuta analistul cu intervalul prezis sau cu variaţia rezultatelor sale.

Agenţia pentru Securitate Cibernetică a UE (ENISA) a publicat un raport în care sunt incluse şi analizate incidente şi ameninţări cibernetice specifice transportului aerian, maritim, feroviar şi rutier, din perioada ianuarie 2021 – octombrie 2022. Conform raportului, procentajul atacurilor cu ransomware împotriva sectorului transporturilor aproape s-a dublat în 2022 faţă de 2021.

Microsoft spune că actualizarea KB5007651 Microsoft Defender Antivirus declanşează avertismente de securitate Windows pe sistemele Windows 11 care spun că Protecţia Autorităţii locale de securitate (LSA) este dezactivată. După instalarea „Actualizare pentru platforma antimalware Microsoft Defender Antivirus - KB5007651 (Versiunea 1.0.2302.21002)”, utilizatorii primesc o notificare de securitate sau un avertisment ce spune că „Protecţia de securitate locală este dezactivată. Dispozitivul dvs. poate fi vulnerabil”, iar după activare, dispozitivul Windows ar putea solicita în mod persistent că este necesară o repornire.

Etapa actuală de dezvoltare a Republicii Moldova, ca stat suveran, independent, democrat şi de drept, se caracterizează prin dezvoltarea şi răspândirea rapidă a tehnologiilor informaţionale, prin rolul sporit al domeniului informaţional ce include totalitatea informaţiei, infrastructurii informaţionale şi de telecomunicaţii, a subiecţilor care efectuează colectarea, formarea, răspândirea şi utilizarea informaţiei sistemului ce reglementează relaţii sociale apărute în acest sens.

Pe parcursul ultimului deceniu, Republica Moldova a realizat mai multe strategii, programe şi politici de țară, pentru dezvoltarea societății informaționale la nivel național, în conformitate cu recomandările forurilor europene şi internaționale din domeniul tehnologiilor informaţionale şi comunicațiilor

electronice, drepturilor şi libertăților fundamentale ale omului în mediul on-line şi off-line.

Pentru Republica Moldova, securitatea informaţională este un domeniu relativ nou. Legislaţia națională în vigoare nu stipulează nicio prevedere privind securitatea informațională. În conformitate cu decretul prezidențial nr. 374-IV din 22.12.2005, două comisii naționale, formate din înalți demnitari de stat, urmau să elaboreze Concepția securității naționale. Documentul respectiv trebuia să substituie Concepția adoptată prin hotărârea Parlamentului nr. 445-XIII din 5.05.1995. Însă nici în documentul elaborat în 2005 printre pericolele estimate la adresa Republicii Moldova nu s-a regăsit influența mediatică din exterior sau lipsa controlului asupra spațiului informațional în unele teritorii ale țării.

Instituţia Publică "Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" (STISC) a fost creată în anul 2018 prin reorganizarea Întreprinderii de Stat „Centrul de Telecomunicaţii Speciale” şi absorbţia Întreprinderea de Stat „Centrul Informaţional Agricol”, conform Hotărârii Guvernului Nr. 414 din 08.05.2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat. În calitate de operator al serviciilor electronice guvernamentale, STISC are misiunea de a asigura administrarea, menţinerea şi dezvoltarea infrastructurii de tehnologie a informaţiei, Sistemului de telecomunicaţii al autorităților administrației publice, ca parte a rețelei de comunicații speciale şi a sistemelor informaţionale de stat, gestionarea infrastructurii unice a cheii publice a Guvernului, precum şi implementarea politicii statului în domeniul securităţii cibernetice.

În vederea asigurării unui sistem de protecţie şi dezvoltare a spaţiului informaţional în condiţiile globalizării şi liberei circulaţii a informaţiilor, a fost adoptată Strategia de Securitate informaţională pentru anii 2019-2024. Strategia prezintă o evaluare a situaţiei actuale în domeniul securităţii informaţionale, enumeră performanţele înregistrate şi punctează noi tendinţe de dezvoltare a societăţii informaţionale, acestea constituind obiective de preocupare majoră a STISC-ului.

Parlamentul Republici Moldova a aprobat Legea privind securitatea cibernetică, ce are scopul de a îmbunătăţi cadrul normativ în domeniu. Documentul aprobat stabileşte competenţa autorităţilor şi instituţiilor publice în materie de securitate cibernetică, determină cadrul naţional general de gestionare a crizelor în domeniul securităţii cibernetice, instituie cerinţe, măsuri şi mecanisme pentru asigurarea securităţii reţelelor şi sistemelor informatice care sunt esenţiale pentru funcţionarea societăţii, precum şi gestionarea incidentelor cibernetice.

Totodată, potrivit Legii privind securitatea cibernetică, va fi desemnată o autoritate competentă în domeniul securităţii cibernetice, ce va identifica şi supraveghea furnizorii de servicii, pentru ca aceştia să asigure un nivel adecvat

de securitate a reţelelor şi sistemelor informatic În Republica Moldova va fi creată o autoritate competentă în domeniul securităţii cibernetice, iar persoanele juridice de drept public şi unii furnizori de servicii vor fi obligaţi să respecte măsuri de securitate a reţelelor şi sistemelor informatice pentru a se proteja de atacuri cibernetice. Sunt prevederile Legii cu privire la securitatea cibernetică, aprobată în două lecturi la şedinţa Parlamentului din 16 martie. Documentul este o premieră pentru Republica Moldova şi va intra în vigoare începând cu 1 ianuarie 2025. e.

Concluzie Tendințele de dezvoltare continuă a interacţiunii dimensiunii tehnologice cu dimensiunea de informare, în toate formele de structură şi funcționare, de natură individuală, publică, privată sau de stat, de factură națională sau globală, conduce la apariția unei noi configurații de comunicare şi schimb de date pe domeniile publice şi private de care depinde nivelul şi starea sectorială sau generală de securitate.

Riscurile din spaţiul cibernetic sunt proporţionale cu gradul de informatizare a societăţii, iar combaterea fenomenului de criminalitate cibernetică trebuie să constituie o preocupare majoră a tuturor actorilor implicați. Mediul virtual facilitează comiterea infracţiunilor, pune la dispoziția conduitei criminale atât un nou obiect (informația conținută şi procesată de sistemele informatice), cât şi un nou instrument. Acesta oferă un repertoriu vast de tehnici şi strategii de săvârşire a infracțiunilor, generând tendinţe noi de infracțiuni.

Totodată, natura globală a sistemelor informaționale şi a rețelelor de comunicații electronice, precum şi natura transnațională a criminalității informatice necesită o coordonare strânsă între toate instituțiile responsabile atât la nivelul național, cît şi la nivel global**.** Prognoza în preîntâmpinarea atacurilor cibernetice este o încercare de a exploata sistemele şi reţelele informatice. Atacurile cibernetice folosesc coduri rău intenţionate pentru a modifica algoritmii, logica sau datele. Securitatea sistemelor informatice este, prin urmare, esenţială. Modelul CVSS este un cadru industrial care ajută la cuantificarea impactului vulnerabilității. Prin acest model matematic prezentat se poate prezice impactul unui atac bazat pe factori semnificativi care influenţează securitatea cibernetică. Vulnerabilitatea şi traficul de reţea au fost selectate ca factori de influenţă pentru a prezice scorul CVSS. Pe baza scorului, analistul tehnic poate analiza impactul şi poate lua măsurile preventive necesare. Acest model ia în considerare, de asemenea, informaţiile de mediu necesare. Este astfel generalizată si poate fi personalizată nevoilor de securitate a informaţiilor din cadrul diferitor organizaţii.

Bibliografia:

1. Stephen J. Flanagan and Irina A. Chindea Russia, NATO, and Black Sea Security Strategy Regional Perspectives from a 2019 Workshop, RAND Coorporation
2. T. Spring, „Introduction to Information Security”, Elsevier, 2014.

3. C. W. Geib and R. P. Goldman, “Plan recognition in intrusion detection systems,” in DARPA Information Survivability Conference amp; Exposition II, 2001. DISCEX ’01. Proceedings, vol. 1, 2001, pp. 46–55 vol.1.
4. T. Hughes and O. Sheyner, “Attack scenario graphs for computer network threat analysis and prediction,” Complexity, vol. 9, no. 2, pp. 15–18, 2003
5. Bou-Harb, M. Debbabi, and C. Assi, “Cyber Scanning: A Comprehensive Survey,” Communications Surveys & Tutorials, IEEE, vol. 16, no. 3, pp. 1496–1519, 2013.
6. O. T. Oluwatosin and D. D. Samson, “Computer-based test security and result integrity,” International Journal of Computer and Information Technology, vol. 2, no. 2, pp. 324–329, 2013.
7. L. K. Shar, H. Beng Kuan Tan, and L. C. Briand, “Mining SQL injection and cross site scripting vulnerabilities using hybrid program analysis,” in Proceedings of the 35th International Conference on Software Engineering (ICSE ’13), pp. 642–651, IEEE Press, May 2013.
8. M. A. Khan and M. Hussain, “Cyber security quantification model,” Bahria University Journal of Information and Communication Technology, vol. 3, no. 1, pp. 23–27, 2010.
9. P. Mell, K. Scarfone, and S. Romanosky, A Complete Guide to the Common Vulnerability Scoring System Version 2.0, National Institute of Standards and Technology, Carnegie Mellon University, 2007.
10. Redhat, Bash Code Injection Vulnerability via Specially Crafted Environment Variables (CVE-2014-6271, CVE-2014-7169), Redhat, 2014, https://access.redhat.com/articles/1200223.
11. Sensitive Data Protection Vulnerability, OWASP, https://www.owasp.org/index.php/Category:Sensitive Data Protection Vulnerability.