MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microeletronică
Departamentul Ingineria Software și Automatică

Admis la susținere
Șef departament:
Fiodorov Ion, conf. univ.
_____
„_____”_____ 2021

Îmbunătățirea managementului incidentelor cibernetice a CERT-urilor departamentale ale Guvernului Republicii Moldova

Teză de master

Student: **Malear Ion, SI-201M**

Conducător: **Bulai Rodica, asist. univ.**

Chișinău, 2022

Rezumatul (Adnotarea)

Scopul lucrării este de a defini și de a menține un mediu virtual sigur, cu un înalt grad de reziliență și de încredere, bazat pe infrastructurile cibernetice de interes național, care să constituie un important suport pentru securitatea națională și buna guvernare, pentru maximizarea beneficiilor cetățenilor, me diului de afaceri și ale societății, în ansamblul ei.

Lucrarea reflectă obiectivele, principiile și direcțiile majore de acțiune pentru cunoașterea, prevenirea și contracararea amenințărilor, vulnerabilităților și riscurilor la adresa securității cibernetice a Republicii Moldova și pentru promovarea intereselor, valorilor și obiectivelor naționale în spațiul cibernetic.

În cadrul lucrării se prezintă o cercetare asupra nivelului de maturitate a procesului de management a incidentelor de securitate cibernetică a CERT-urilor departamentale ale Guvernului Republicii Moldova, desemnate în cadrul entităților publice care dețin infrastructuri/ sisteme de tehnologia informației și comunicații și care dispun de capacitatea necesară pentru a ține evidența operativă obligatorie și a raporta incidente de securitate cibernetică.

Cuvinte-cheie: *incident, amenințări, management, maturitate, evaluare*.

Abstract

The aim of the paper is to define and maintain a secure virtual environment with a high degree of resilience and trust, based on cyber infrastructures of national interest, which will be an important support for national security and good governance, to maximize the benefits of citizens. , the business environment and society as a whole.

The paper reflects the objectives, principles and major directions of action for recognizing, preventing and countering threats, vulnerabilities and risks to cyber security of the Republic of Moldova and for promoting national interests, values and objectives in cyberspace.

Master's thesis project is a research on the level of maturity of the cyber security incident management process of the departmental CERTs of the Government of the Republic of Moldova, designated within the public entities that have information and communication technology infrastructures/ systems and have the necessary capacity to keep mandatory operational records and report cyber security incidents.

Keywords: *incident, threats, management, maturity, assessment*.

CUPRINS

INTRODUCERE 8
1 ACTUALITATEA ŞI PROBLEMATICA DOMENIULUI DE STUDIU 10
1.1 Actualitatea temei 11
1.2 Problema identificată 16
2 DESCRIEREA METODOLOGIILOR/ MODELELOR EXISTENTE DE EVALUARE A MATURITĂȚII PROCESULUI DE MANAGEMENT A INCIDENTELOR DE SECURITATE CIBERNETICĂ 19
3.1 Modelul SIM3 20
3.2 Modelul SIRTFI 25
3.3 Modelul CREST 27
3 NIVELUL DE MATURITATE A MANAGEMENTULUI INCIDENTELOR DE SECURITATE CIBERNETICĂ A ENTITĂȚILOR SPECIALIZATE 31
3.1 Auto-evaluarea CERT Gov 32
3.2 Evaluarea CERT-urilor departamentale 37
3.3 Metodologie privind îmbunătățirea procesului de identificare a amenințărilor și de răspuns la incidente de securitate cibernetică 39
CONCLUZII 46
BIBLIOGRAFIE 48
ANEXE 50
Anexa A – Indicatorii securității cibernetice 50
Anexa B – Tabelul rezultatelor auto-evaluării nivelului de maturitate CERT Gov 53
Anexa C – Chestionarul de evaluare al nivelului de maturitate a capacității CERT-urilor departamentale de răspuns la incidente cibernetice 56
Anexa D – Rezultatele obținute privind nivelul de maturitate a CERT-urilor departamentale 57

INTRODUCERE

Tehnologiile informaționale, resursele de informare și sistemele de comunicare electronică au devenit parte indispensabilă a tuturor domeniilor de activitate ale statului, societății și cetățenilor. Dezvoltarea accelerată a tehnologiilor informaționale și de comunicații moderne contribuie la transformări sociale de esență, fiind un generator pentru apariția și consolidarea societății informaționale la nivel național, regional și internațional, depășind cadrul juridic al frontierelor de stat sau al comunităților de state.

Spațiul informațional a devenit un domeniu de activitate vital pentru stat, economie, știință, societate și cetățean, un spațiu nou de reglementare a drepturilor și libertăților fundamentale ale omului, cu implicarea directă și indirectă asupra mecanismelor de asigurare a politicilor de securitate și apărare națională într-o societate democratică. [1]

Potrivit raportului anual cu privire la monitorizarea evoluției societății informaționale la nivel mondial „National Cyber Security Index", lansat de către e-Governance Academy, Republica Moldova este plasată pe locul al 62-lea din cele 160 de state incluse în clasament (a se vedea figura I.1). Informațiile furnizate de NCSI sunt bazate pe materialele de evidență disponibile public. Clasarea în index este proporțională cu existența și disponibilitatea publică a informațiilor, fiind grupate și prezentate pe indicatori (a se vedea anexa A). Sunt implementate sau în proces continuu de dezvoltare programe și proiecte on-line de infrastructură și servicii publice digitale, de asemenea sunt lansate strategii sectoriale în domeniul tehnologiei informației și politici de modernizare tehnologică a guvernării. [2,1]

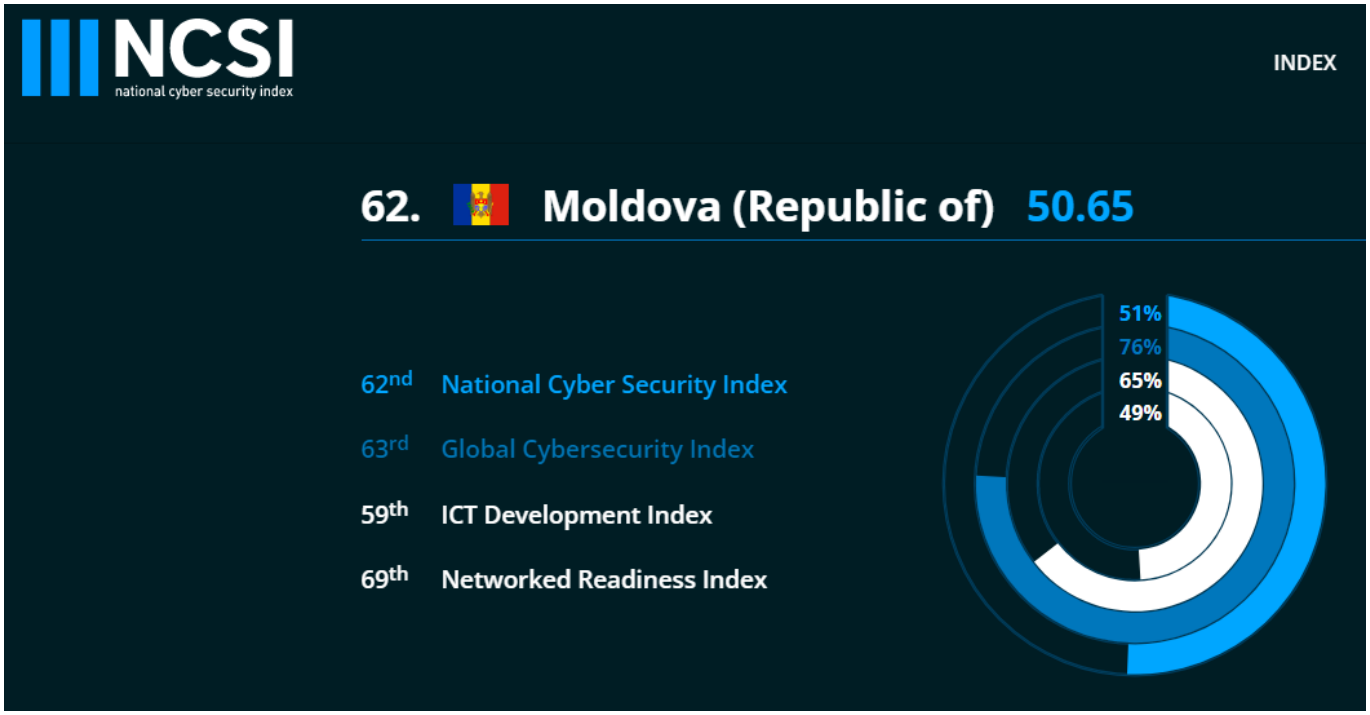

Figura I.1 – Scorul evoluției societății informaționale

Interacțiunea tehnologiilor informaționale cu diversitatea conținutului informațional, pe de o parte, și fuziunea rețelelor de comunicare publică și socială cu sistemele electronice guvernamentale, pe de altă parte, contribuie la o extindere și sinergie a spațiului informațional cu domeniile centrale de securitate și apărare națională, responsabile de asigurarea suveranității, independenței și integrității teritoriale a Republicii Moldova. [1]

Tehnologiile informaționale generează modificări ale dimensiunii de informare și comunicare, care se transformă în ritm accelerat într-o platformă multimedia, fiind dezvoltate noi componente și mijloace de comunicare on-line și off-line, iar libera circulație a informațiilor și ideilor la nivel local, regional și global devin un imperativ pentru crearea și promovarea unui societăți informate într-un stat democratic și de drept.

Tendințele de dezvoltare continuă a interacțiunii dintre dimensiunea tehnologică și dimensiunea de informare în toate formele de structură și funcționare, de natură individuală, publică, privată sau de stat, de factură națională sau globală, conduc la apariția unei noi configurații de comunicare și schimb de date pe domeniile publice și private de care depind nivelul și starea sectorială sau generală de securitate. [1]

Concomitent, prin dezvoltarea accelerată a tehnologiilor informației și de comunicații moderne, abordarea amenințărilor, riscurilor și vulnerabilităților într-o societate informațională se ridică la un alt nivel. În prezent, la nivel mondial, atacurile cibernetice capătă o frecvență, o complexitate și o amploare din ce în ce mai mari, aducând pagube enorme sectorului guvernamental, celui privat și cetățenilor, ca urmare a caracterului lor asimetric. [3]

Spațiul cibernetic se caracterizează prin lipsa frontierelor, dinamism și anonimat, generând deopotrivă oportunitățile de dezvoltare a societății informaționale bazate pe cunoaștere, dar și riscuri la adresa funcționării acesteia (la nivel individual, statal și chiar cu manifestare transfrontalieră).

Domeniile politic, economic, social, și militar sunt ținte ale războiului informațional care tinde, în mod special, să influențeze procesele decizionale. În aceste condiții, asigurarea securității informaționale este esențială pentru a întări discernământul social, atașamentul social și interesul social. Asigurarea securității informaționale este necesară și pentru contracararea abuzului informațional, care poate genera rupturi sociale și dezechilibre în societate. [1]

BIBLIOGRAFIE

1. Hotărârea Parlamentului nr. 257/2018 privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia. [citat 07.09.2021]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=110324&lang=ro;
2. National Cyber Security Index. Moldova (Republic of). [citat 09.09.2021]. Disponibil: https://ncsi.ega.ee/country/md/
3. Hotărârea Guvernului nr. 811/2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020. [citat 10.09.2021]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=110324&lang=ro;
4. Cyber Security Incident Response High-level Maturity Assessment Tool. [citat 17.09.2021]. Disponibil: https://www.crest-approved.org/wp-content/uploads/2014/10/Maturity-Model-example.pdf;
5. Security Incident Management Maturity Model Manual. [citat 13.09.2021]. Disponibil: https://sim3-check.opencsirt.org/#/;
6. SIM3: Security Incident Management Maturity Model. [citat 13.09.2021]. Disponibil: http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf;
7. What is the SIM3 Model ? [citat 13.09.2021]. Disponibil: https://lifars.com/2020/10/what-is-the-sim3-model/;
8. A Security Incident Response Trust Framework for Federated Identity (Sirtfi). [citat 15.09.2021]. Disponibil: https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf;
9. The CREST Cyber Security Incident Response Maturity Assessment Tool. [citat 17.09.2021]. Disponibil: https://www.crest-approved.org/wp-content/uploads/2014/10/CSIR-Maturity-assessment-tool_Info1.pdf;
10. CREST Incident Response Maturity Assessment [citat 17.09.2021]. Disponibil: https://lifars.com/2021/03/crest-incident-response-maturity-assessment/;
11. Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat. [citat 04.10.2021]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro;
12. Concept SIA RSISC. [citat 08.12.2021]. Disponibil: https://particip.gov.md/ro/download_attachment/14551
13. Parteneriate STISC. [citat 06.10.2021]. Disponibil: https://stisc.gov.md/ro/parteneriate;

14. Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică. [citat 04.10.2021]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro;
15. Cyber Security Incident Response Guide. [citat 16.11.2021]. Disponibil: https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf;
16. Effective cyber security incident response. [citat 02.12.2021]. Disponibil: https://studylib.net/doc/8366491/effective-cyber-security-incident-response;
17. CERN'S COMPUTER. SECURITY OPERATIONS CENTRE. [citat 25.11.2021]. Disponibil: https://www.dsn.kastel.kit.edu/downloads/Valsan%20-%20operational%20security.pdf;