MINISTERUL EDUCAŢIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronică şi Telecomunicaţii
Departamentul Telecomunicaţii

Admis la susţinere

Şef departament:

_____

„____”_____ 2021

ANALIZA ȘI MODELAREA FENOMENULUI DE SUSTRAGEREA DATELOR PENTRU A EVOLUA VULNERABILITATEA SISTEMELOR INFORMAȚIONALE CORPORATIVE

Teză de master

Student: **Gramaciuc Denis, grupa SISRC-201M**
Conducător: **Tîrșu Valentina lect.univ.dr.**
Consultant: **Sava Lilia, conf.univ.dr..**

Chișinău, 2021

ADNOTARE

Autor: Denis GRAMACIUC.

Tema: Analiza și modelarea fenomenului de sustragerea datelor pentru a evalua vulnerabilitatea sistemelor informaționale corporative.

Termeni-cheie: securitate cibernetică, insecutitate ciberentică, spațiu cibernetic, mediu cibernetic, atacuri cibernetice, amenințări cibernetice, agresiuni cibernetice, delict cibernetic, război ciberentic, intruziune cibernetică, incident ciberentic, sistem informatic corporativ, vulnerabilitate ciberentică.

Scopul lucrării constă în analiza şi modelarea fenomenului de sustragerea datelor pentru a evalua vulnerabilitatea sistemelor informaționale corporative deoarece mediul cibernetic, aflat în plină evoluție, generează deopotrivă oportunități de dezvoltare a societății informaționale, dar şi riscuri la adresa funcţionării acesteia. Existența vulnerabilităților sistemelor informatice corporative ce pot fi exploatate de grupări organizate, face ca asigurarea securității cibernetice prin prisma spațiului cibernetic să constituie o preocupare majoră pentru toate entitățile implicate.

Scopul respectivei lucrări a determinat **structura ei**, fiind compusă din introducere, trei capitole, concluzii, bibliografie şi anexe.

Reieșind din scopul cercetării au fost fixate următoarele **obiective:**

- Definirea caracteristicilor definitorii şi particularități ale haking-ului;
- Analiza securității cibernetice în Republica Moldova;
- Analiza statistică ale CERT.gov în Republica Moldova;
- Analiza impactului organizațiilor non-guvernamentale în reglementarea aplicativității securității cibernetice;
- Elaborarea strategiilor de îmbunătățire a securității cibernetice;
- Constatarea tehnico-ştiințifică a atacurilor cibernetice şi măsuri de înlăturare a lor.
- Elaborarea modalităților de acțiuni în detectarea sistemelor informatice cu cod maliții.

În lucreare au fost utilizate **următoarele metode**: analiză, sinteză, inducție, deducție, analiză comparativă şi analiză predictivă.

Rezultatele obţinute reflectă faptul că societatea informațională prezintă un catalizator efectiv al progresului social şi economic.

Concluziile şi propunerile de remediere a vulnerabilităților ciberentice studiate pot fi real de folos în procesul testării de penetrare a sistemului informațional corporativ (*Pen Testing*), în procesul elaborării actelor normative, modificării şi amendării legislaţiei în vigoare a Republicii Moldova. Teza constituie o contribuţie modestă, dar consider temeinică la îmbogăţirea literaturii naţionale în domeniul securității informației în sisteme şi rețele de comunicații şi poate fi utilizată în procesul didactic la facultăţile din domeniu ale instituţiilor superioare de învăţământ, căutându-şi potenţialii cititori în rândurile studenţilor.

ANNOTATION

Author: Denis GRAMACIUC.

Theme: Analysis and modeling of the data theft phenomenon to evaluate the vulnerability of corporate information systems.

Key terms: cyber security, cyber insecurity, cyber attacks, cyber environment, cyber threats, cyber aggression, cyber crime, cyber warfare, cyber intrusion, cyber incident, corporate computer system, cyber vulnerability.

The aim of the paper is to analyze and model the phenomenon of data theft to evolve the vulnerability of corporate information systems because the evolving cyber environment generates opportunities for the development of the information society, but also risks for its functioning. The existence of vulnerabilities in corporate information systems that can be exploited by organized groups makes ensuring cybersecurity in cyberspace a major concern for all entities involved.

The purpose of this paper determined **its structure**, being composed of introduction, three chapters, conclusions, bibliography, and annexes.

Based on the propose of the research, the following **objectives** were set:

- Defining the defining characteristics and particulatisties of hacking;
- Cyber security analisis in the Republic of Moldova;
- Statistical analysis of CERT.gov in the Republic of Moldova;
- Analysis of the impactv of non-governmantal organizations in regulating the applicability of cyber security;
- Developing strategies to improve cyber security;
- Tehnical-sceintific finding of cyber attacks and measures to eliminate them;
- Elaboration of the modalities of actions in the detection of the computer systems with malicious code.

The following methods were used in the paper: nalaysis, synthesis, indiction, deduction, comparative analysis and predictive analysis.

The results show that the information society is an effective catalyst for sociel and economic progress.

The conclusions and proposals for remedying the studied cyber vulnerabilities can be really useful in the process of testing the penetration of the corporate information system (Pen Testing), in the process of drafting normative acts, amending and amending the legislation in force in the Republic of Moldova. The thesis is a modest contribution, but I consider it important to enrich the national literature in the field of information security in communication systems and networks and can be used in teaching in the faculties of higher education institutions, in search of potential readers among students.

CUPRINS

INTRODUCERE

Dezvoltarea tehnologică a societății civile, în ultimii douăzeci de ani, şi globalizarea infrastructurilor de comunicaţii au condus la schimbări profunde în toate sistemele de securitate.

Actualitatea temei rezultă din faptul că extinderea reţelei de Internet, dezvoltarea reţelelor mobile de comunicaţii şi creşterea dependenţei de informaţii a întregii societăți umane, a generat apariţia unor noi riscuri şi ameninţări la adresa securității cibernetice naționale cunoscute ca *„cyber ameninţări”*. Republica Moldova, ca și alte state digitalizate, se află sub ameninţări de atacuri cibernetice, care au ca scop perturbarea activităţilor organizațiilor non/guvernamentale, persoanelor fizice și juridice, prin distrugerea sau atacarea cibernetică a resurselor de informaţii şi a infrastructurii critice, sau prin afectarea imaginii publice şi inducerea unui sentiment de insecuritate și de neîncredere în capacitatea de apărare proprie.

Scopul cercetării constă în analiza și modelarea fenomenului de sustragerea datelor pentru a evolua vulnerabilitatea sistemelor informaționale corporative deoarece mediul cibernetic, aflat în plină evoluție, generează deopotrivă oportunități de dezvoltare a societății informaționale, dar şi riscuri la adresa funcţionării acesteia. Existența vulnerabilităților sistemelor informatice corporative ce pot fi exploatate de grupări organizate, face ca asigurarea securității cibernetice prin prisma spațiului cibernetic să constituie o preocupare majoră pentru toate entitățile implicate. Atunci când sistemele de comunicaţii, infrastructuri critice, instituții financiar-bancare sau organisme guvernamentale devin ținte ale atacatorilor. Trebuie să tragem un semnal de alarmă în ceea ce privește căile prin care ne putem apăra și contracara o eventuală insecuritate cibernetică.

În acelaşi timp spaţiul informatic deschis a încurajat relaţionarea socială şi politică la nivel mondial, a rupt obstacolele dintre ţări, cetăţeni şi etnii, permiţând relaţionarea şi schimbul de informaţii şi idei la nivel planetar.

De mai bine de două decenii, oamenii s-au luptat să înţeleagă ameninţările informatice şi să evalueze riscurile pentru persoanele fizice şi organizaţii, pentru a oferi răspunsuri adecvate. Deşi multe organizaţii au investit în mod semnificativ în obţinerea de informaţii, majoritatea experţilor în securitatea reţelelor de calculatoare cred că un adversar bine echipat din punctul de vedere tehnologic va avea mai mult succes în derularea unor agresiuni cibernetice cu impact semnificativ atât din punct de vedere distructiv, cât şi al complexităţii tehnice, mai ales dacă dezvoltarea mecanismelor de protecţie a sistemelor de calcul este singurul răspuns la un atac. Din acest motiv, o atenţie sporită este acordată, în primă instanţă, descurajării unor astfel de atacuri, în special de către organele care au competenţa de a investiga activitatea din domeniul spionajului informatic, precum şi prerogativa folosirii unei game variate de instrumente pentru a proteja siguranţa publică, precum activităţile ce ţin de securitatea naţională.

Spre deosebire de războaiele nucleare, chimice şi cu arme biologice, sau comerciale, nu există în prezent tratate internaţionale, care să reglementeze războiul informaţional, spionajul informatic sau „*hacking-ul”*.

Prin securitatea cibernetică se înțelege starea de funcționalitate a informațiilor digitale, resurselor și serviciilor oferite de către entitățile publice sau private în spațiul cibernetic. Această stare presupune asigurarea următoarelor obiective:

- *confidențialitatea* - proprietatea ca informațiile, serviciile sau resursele sistemelor informatice să nu fie disponibile unor persoane neautorizate, de ex: (hackerii);

- *integritatea* - proprietatea de păstrare a acurateței informațiilor, serviciilor sau resurselor sistemelor informatice;

- *disponibilitatea* - proprietatea ca informațiile, serviciile sau resursele sistemelor informatice să fie accesibile persoanelor sau proceselor autorizate;

- *autenticitatea* - proprietatea de asigurare a identificării și autentificării persoanelor, dispozitivelor și serviciilor sistemelor informatice și de comunicații;

- *non-repudierea* - proprietatea că o acțiune sau un eveniment să nu poată fi repudiat (negat, contestat) ulterior.

Reieșind din scopul cercetării au fost fixate următoarele **obiective:**

- Definirea caracteristicilor definitorii și particularități ale haking-ului;
- Analiza securității cibernetice în Republica Moldova;
- Analiza statistică ale CERT.gov în Republica Moldova;
- Analiza impactului organizațiilor non-guvernamentale în reglementarea aplicativității securității cibernetice;
- Elaborarea strategiilor de îmbunătățire a securității cibernetice;
- Constatarea tehnico-științifică a atacurilor cibernetice și măsuri de înlăturare a lor.
- Elaborarea modalităților de acțiuni în detectarea sistemelor informatice cu cod malițios.

Securitate cibernetică poate fi garantată prin aplicarea unor măsuri de securitate pro-active ce includ politici, standarde și modele de securitate, prin implementarea unor soluții pentru protecția sistemelor informatice, care sunt gestionate de către utilizator.

În lucreare au fost utilizate **următoarele metode**: analiză, sinteză, inducție, deducție, analiză comparativă și analiză predictivă. Rezultatele obținute reflectă faptul că societatea informațională prezintă un catalizator efectiv al progresului social și economic.

BIOGRAFIE

1. https://stisc.gov.md/ro/republica-moldova-clasata-pe-locul-53-raportul-indicele-global-cybersecurity-2018;
2. https://www.speedtest.net/global-index/moldova#fixed;
3. IONIȚĂ Gheorghe-Iulian, *Infracțiuni din sfera criminalității informatice*, Editura Pro Universitaria, București, 2013, 112 p. **ISBN: 978-606-647-909-7**;
4. Codul penal al Republicii Moldova, nr. 985-XV din 18.04.2002. În: Monitorul Oficial Republicii Moldova nr.128-129/1012 din 13.09.2002. Republicat în: Monitorul Oficial al Republicii Moldova nr.72-74/195 din 14.04.2009;
5. DOBRINOIU Maxim, *Infracțiuni în domeniul informatic*, Editura C.H.Beck, București 2006; 74 p. **ISBN: 978-973-115-607-1**;
6. Lege privind prevenirea și combaterea criminalității informatice, nr. 20-XVI din 03.02.2009. În: Monitorul Oficial nr.11-12/17 din 26.01.2010;
7. HUTCHINS E.M., CLOPPERT M.J., AMIN R.M., *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Lockheed Martin Corporation, 2010; 172 p. **ISBN: 978-1-1908272-08-9**;
8. MIHAI I.C., PETRICĂ G., *Securitatea informațiilor. Ediția a II-a, îmbunătățită și adăugită*, Editura Sitech, 2014; 39 p. **ISBN 978-606-11-4364-1**;
9. MIHA I.C., GIUREA L., *Criminalitatea informatică. Ediția a II-a, îmbunătățită și adăugită*, Editura Sitech, 2014; 100 p. **ISBN 978-606-11-4363-4**;
10. Revista Intelligence, „*Război hibrid și atacuri cibernetice*": http://intelligence.sri.ro/razboi-hibrid-si-atacuri-cibernetice/;
11. MIHAI I.C., PETRICĂ G., *Securitatea informațiilor. Ediția a II-a, îmbunătățită și adăugită*, Editura Sitech, 2014; 87 p. **ISBN 978-606-11-4364-1**;
12. PATRICIU V.V., PIETROSANU M.E., BICA I., PRIESCU J., *Semnături electronice și securitate informatică,* Editura All, 2006, 56 p. **ISBN online: 978-606-8202-60-0**;
13. https://ict.md/about-page/mission/;
14. https://moldovaitpark.md/about-us-ro/;
15. https://aceti.md/istoria-aceti/;
16. https://tekwill.md/about/;
17. http://e-root.cc/, https://www.youtube.com/channel/UCIdQdo1tzwW7bGBH83NGXXw, https://forum.antichat.ru/members/246548/, https://forum.web.money/index.php?/user/893561-wind3str0y/, https://tor.sg/profile/70777-wind3str0y/content/?type=forums_topic_post&change_section=1, https://youhack.xyz/threads/889195/, https://www.youtube.com/user/DenisNicula/featured;
18. https://forum.antichat.ru/threads/460943/#post-4343877;
19. https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro.