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

Building cyber security system in the republic of moldova for the next generation of challenges

Teză de master

Student: **Natalia Spînu, SI-201M**

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

Chișinău, 2022

Abstract

The purpose of the thesis: The purpose of the master's thesis is to identify the objectives and basic principles for the development of a national cyber security governance strategy. In a constantly changing environment of cyber security vulnerabilities and threats that tend to evolve given the digitalization of the Republic of Moldova, it is essential to analyze the reality and develop a general cyber governance strategy that would ensure a general level of national security.

Thesis structure: Introduction, 4 chapters, conclusions, 11 images, 19 bibliographic sources, 53 pages of basic text.

Chapter I: In the first chapter we analysed the general field of cyber security, with reference to current threats and vulnerabilities, the analysis of the objectives and principles of elaboration of a national cyber security strategy based on the existing specialized literature.

Chapter II: In Chapter Two, we analysed the legislative and regulatory framework for cyber security in the Republic, analysed and described the national cyber security strategy currently applied to ensure by 2024 an action plan on security and digitization of services. We also assessed and described the main actors that ensure national cyber governance as a complex mechanism of action and the opportunities and challenges that the state faces in implementing a national CERT.

Chapter III: Chapter 3 contains an analysis of cyber governance models in Estonia, Israel, and Romania. This study made it possible to identify generic action models applicable to any state in their desire to strengthen effective cyber governance for the future.

Chapter IV: Chapter 4 provides a possible model of cyber governance for the Republic of Moldova based on needs, available resources and good practices accumulated from the analysis and synthesis of pre-existing models in neighbouring countries. This chapter summarizes the research efforts of previous chapters to define more effective future governance for the threats that follow.

Keywords: *cyber governance, cyber security vulnerabilities, cyber security threats, national strategy, CERT.*

Rezumat

Scopul tezei: Scopul tezei de master este de a identifica obiectivele și principiile de bază pentru elaborarea unei strategii naționale de guvernare a securității cibernetice. Într-un mediu în continuă schimbare a vulnerabilităților și amenințărilor de securitate cibernetică care tind să evolueze dat fiind digitalizarea Republicii Moldova, este esențială analizarea realității și elaborarea unei strategii generale de guvernanță cibernetică ce ar asigura un nivel general de securitate națională.

Memoriu explicativ: Introducere, 4 capitole, concluzii, 11 imagini, , 19 surse bibliografice, 53 pagini text de bază.

Capitolul I: În primul capitol am analizat domeniul general al securității cibernetice, cu referire la amenințări și vulnerabilități actuale, analiza obiectivelor și principiilor de elaborare a unei strategii naționale de securitate cibernetică reieșind din literatura de specialitate existentă.

Capitolul II: În cadrul capitolului doi, am analizat cadrul legislativ și normativ aferent securității cibernetice în Republică, am analizat și descris strategia națională de securitate cibernetică aplicată la moment pentru asigurarea până în 2024 a unui plan de acțiuni privind securitatea și totodată digitalizarea serviciilor. De asemenea am evaluat și descris actorii principali ce asigură guvernanța cibernetică națională ca mecanism complex de acțiune și oportunitățile și provocările cu care se confruntă statul la implementarea unui CERT național.

Capitolul III: Capitolul 3 conține o analiză a modelelor de guvernare cibernetică în Estonia, Israel și România. Acest studiu a permis identificarea unor machete de acțiuni generice aplicabile pentru orice stat în dorința lor de a consolida o guvernare cibernetică eficientă pentru viitor.

Capitolul IV: Capitolul 4 oferă un model de guvernare cibernetică posibilă pentru Republica Moldova reeșind din necesități, resurse disponibile și bune practici acumulate din analiza și sinteza unor modele preexistente în țările vecine. Acest capitol însumează eforturile de pe urma cercetării desfășurate în capitolele anterioare în scopul definirii unei guvernanțe viitoare mai eficiente pentru amenințările ce urmează.

Cuvinte-cheie: *guvernare cibernetică, vulnerabilități de securitate cibernetică, amenințări de securitate cibernetică, strategie națională, CERT.*

CONTENTS

INTRODUCTION

Today we are more connected than ever. The cyber sphere has expanded exponentially and technologies such as the cloud and IoT have made us more dependent on the internet. Being connected is a part of being competitive. This holds true for nations and businesses of all sizes and nature. Security has always been a huge concern for organizations. It was crucial even in the days of punch cards and manual filing of data in hard-copy format. A single lost file back in those days could cost a lot. Today, however, the stakes are even higher. With the increasing frequency of cyber-attacks, the cost has also taken a hike.

Recent reports reveal that the cost of a single cyber breach is around $84,000 to $148,000 for a small business. This doesn't even include the cost of remediation and recovery. Add the loss of customer trust, and the damage is irreparable. With a blow that huge, it is no surprise that 60 percent of these companies go out of business within six months after a cyber-attack. A single breach can prove fatal for your business, and therefore, prevention is the best strategy.

Trends like BYOD and IoT are becoming crucial for a productive environment. These disruptive technologies and trends bring numerous benefits — but since they involve connecting various devices to the network, they may also serve as entryways for hackers and attackers. These technologies may only prove effective in a secure environment. Without proper cybersecurity system and policies in place, potential network threats might multiply with the number of devices connected to the network.

Cybersecurity has become such a crucial concern that even the government has become more involved in the matter. Over the past year, numerous important regulations and legislation were passed, especially following the attacks on major corporate giants such as Facebook and Deloitte. Ironically, the latter is one of the leading cybersecurity consultants in the world. GDPR, introduced by the EU, is one of the prime examples of governments playing their role in fortifying cybersecurity. These regulations force businesses to take security more seriously and invest more time and money on securing data and systems.

Tighter regulations mean it will soon become impossible for any business to operate, let alone survive, without prioritizing cybersecurity. With an increasing number of cyber threats that are also becoming more sophisticated by the day, cybersecurity is the need of the hour. Any small business is just one breach away from a complete shutdown. And for a larger corporation, there is much more at stake than money.

REFERENCES

1. Guide to developing a national cybersecurity strategy, ITU. [quoted 06.09.2021]. Available: https://www.itu.int/myitu/-/media/Publications/2018-Publications/BDT-2018/Guide-to-developing-a-national-cybersecurity-strategy---Strategic-engagement-in-cybersecurity.pdf;
2. National Cyber Security Strategy Good Practice Guide, ENISA. [quoted 08.09.2021]. Available: https://www.enisa.europa.eu/publications/ncss-good-practice-guide;
3. Michael POZNANSKY, Confronting cyber threats: Challenges and Opportunities. [quoted 14.09.2021]. Available: https://mwi.usma.edu/confronting-cyber-threats-challenges-and-opportunities/;
4. 2009/140/ec of the european parliament and of the council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services. [quoted 17.09.2021]. Available: https://eur-lex.europa.eu/lexuriserv/lexuriserv.do?Uri=OJ:L:2009:337:0037:0069:EN:PDF;
5. Low of Republic of Moldova Nr. 241 / 2007 Electronic Communications Directive. [quoted 05.10.2021]. Available: https://www.legis.md/cautare/getresults?Doc_id=112412&lang=ro#;
6. Government Decision No. 1141/ for the approval of the Regulation on the application of the electronic signature on electronic documents by the officials of legal entities under public law within their electronic circulation. [quoted 14.10.2021]. Available: https://www.legis.md/cautare/getresults?Doc_id=102490&lang=ro;
7. Parliament Decision No. 257/2018 on the approval of the Information Security Strategy of the Republic of Moldova for the years 2019–2024 and of the Action Plan for its implementation. [quoted 19.10.2021]. Available: https://www.legis.md/cautare/getresults?Doc_id=111979&lang=ro;
8. Ronald J. DEIBERT and Masashi CRETE-NISHIHATA, Global Governance.Vol. 18, No. 3 (July–Sept. 2012), pp. 339-361 (23 pages), Published By: Brill;
9. "Estonia takes the plunge". The Economist. June 26, 2014. Archived from the original on July 1, 2014. Retrieved February 2, 2015;
10. Toomas Hendrik ILVES, e-Estonia: The Making of An Information Age Society. [quoted 26.10.2021]. Available: https://www.worldbank.org/en/events/2014/05/20/e-estonia-the-making-of-an-information-age-society#3;
11. About e-Estonia briefing center. [quoted 29.10.2021]. Available: https://e-estonia.com/;

12. NIST Cybersecurity Framework Success Story Israeli National Cyber Directorate. [quoted 02.11.2021]. Available: https://www.nist.gov/system/files/documents/2020/07/23/Israeli%20National%20Cyber%20Directorate%20Success%20Story%20062920%20508.pdf;
13. Isaac KFIR , Israel's cyber ecosystem, Why the start-up nation eschews doctrines and silos when it comes to cybersecurity. [quoted 10.11.2021]. Available: https://www.policyforum.net/israels-cyber-ecosystem/;
14. About Israel National Cyber Directorate. [quoted 19.11.2021]. Available: https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page;
15. Jasper FREI , CYBERDEFENSE REPORT, Israel's National Cybersecurity and Cyberdefense Posture. [quoted 24.11.2021]. Available: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf;
16. Romania – EU Cybersecurity dashboard. [quoted 30.11.2021]. Available: https://cybersecurity.bsa.org/assets/pdfs/country_reports/cs_romania.pdf;
17. PRESS RELEASE, The Romanian Government has approved Emergency Ordinance no. 104 from 22nd of September 2021 for the establishment of the National Cyber Security Directorate, Bucharest, 27th of September 2021. [quoted 03.12.2021]. Available: https://dnsc.ro/vezi/document/dnsc-romanian-national-cyber-security-directorate-approved-by-government;
18. Romanian Cyber Security Journal. [quoted 07.09.2021]. Available: , https://rocys.ici.ro/;
19. About Romanian National Cyber Security Directorate. [quoted 07.12.2021]. Available: https://dnsc.ro/;