MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susținere

Șef departament: conf. univ., dr. Ion FIODOROV

_____

"___" _____ 2022

Centru Operațional de Securitate Cibernetică destinat companiilor mici și mijlocii

Teză de master

Student: **Andrian Cornei**

Conducător: **Bulai Rodica**
asistent univ.

Chișinău, 2022

ADNOTARE

Această lucrare este structurată pe trei capitole, fiecare cu câte trei și patru subcapitole. Capitolul unu urmărește studierea studierea problemelor de securitate informațională la nivel global asupra organizațiilor, efectul pandemiei COVID-19 asupra societății, atacurile cibernetice împotriva dispozitivelor mobile și IT, riscurile expunerii informațiilor în Cloud și importanța securizării acestora. Care sunt efectele lor asupra mediului de afaceri mic și mijlociu din Republica Moldova, care sunt probleme cu care se confruntă acestea, cum funcționează ele la moment și dacă sunt gata să facă față atacurilor cibernetice actuale, importanța conștientizării riscului la care sunt expuși utilizatorii de rând, obișnuițele lor de lucru, toate acestea finalizează primul capitol al lucrării.

Capitolul doi este o continuare a capitolului unu, esențial în a înțelege situația la care se află mediul de afaceri mic și mijlociu și necesitatea creării unui Centru Operațional de Securitate Cibernetică care să vină în ajutorul lor. Ce presupun Centrele Operaționale de Securitate la nivel global și tipurile acestuia, ce presupune deschiderea unui Centru Operațional de Securitate Cibernetică în R. Moldova și care ar fi rolul și impactul acestuia pentru organizațiile din Moldova, necesitatea deschiderii acestuia, tipurile de probleme și incidente pe care urmează să le rezolve, sunt doar o parte de informațiii care sunt descrise în capitolul doi al acestei lucrări.

Lucrarea este finalizată cu capitolul trei în care este prezentată viitoarea platformă interactivă de securitate "E-Security" care are ca și scop prezentarea celor trei direcții de activitate ale acesteia precum, centru de analiză și implementare a soluțiilor de securitate, centru de instruire privind securitatea informațională cât și un laborator de simulări a situațiilor de atac cibernetic.

ANNOTATION

This paper work is structured in three chapters, each with three and four subchapters. Chapter One examines the study of global information security issues on organizations, the effect of the COVID-19 pandemic on society, cyberattacks on mobile and IT devices, the risks of information exposure in the Cloud, and the importance of securing them. What are their effects on the small and medium business environment in the Republic of Moldova, what are the problems they face, how do they work at the moment and if they are ready to face the current cyberattacks, the importance of awareness of the risk to which ordinary users are exposed, their work habits, all of this are completing the first chapter of the paper.

Chapter two is a continuation of Chapter One, essential in understanding the situation of the small and medium business environment and the need to create a Cyber Security Operations Center to come to their aid. What do the Global Security Operations Centers entail and their types, what does the opening of a Cyber Security Operations Center in the Republic of Moldova entail and what would be its role and impact for Moldovan organizations, the need to open it, the types of problems and incidents that to solve them, are just some of the information that is described in chapter two of this paper.

The paper work is completed with chapter three in which is presented the future interactive security platform "E-Security" which aims to present its three directions of activity such as, center for analysis and implementation of security solutions, security training center information and a laboratory for simulating cyberattack situations.

CUPRINS

INTRODUCERE

Astăzi, datorită apariției internetului și a efectului globalizării, tehnologiile informaționale se dezvoltă foarte rapid iar acest lucru a făcut posibil dezvoltarea în același timp a atacurilor cibernetice la care sunt expuse riscului infrastructurile organizațiilor. Aceste riscuri au un impact direct asupra dezvoltării mediului de afaceri.

Această lucrare are ca și scop studierea problemelor de securitate informațională la nivel global asupra organizațiilor, efectul pandemiei COVID-19 asupra lor, cum dezvoltarea tehnologică le impactează. Care sunt efectele lor asupra mediului de afaceri mic și mijlociu din Republica Moldova, care sunt probleme cu care se confruntă acestea, cum funcționează ele la moment și dacă sunt gata atacurilor cibernetice actuale. Pentru o mai bună înțelegere și o analiză mai adâncă, a fost realizat un sondaj privind *"Evaluarea problemelor cibernetice și a securității informaționale la nivelul companiilor mici și mijlocii din Moldova"* în urma cărora s-a stabilit cele mai frecvente atacuri cibernetice întâlnite în cadrul organizațiilor, volumul atacurilor cibernetice în dependență de sectorul de business, topul atacurilor cibernetice începând cu perioada COVID-19 cu scopul de a înțelege schimbările care s-au produs la nivelul securității informaționale, care sunt cele mai des sisteme de protecție împotriva atacurilor cibernetice întâlnite și utilizate de către domeniul business, provocările la nivelul utilizării platformelor cloud și conștientizarea riscului la care sunt expuse, obișnuițele de lucru a angajaților și nivelul lor de conștientizare a riscului informațional prin dezvoltarea concepului de "Cyber hygiene". Aceste informații descrise în capitolul unu au fost esențiale în înțelegerea situației la care se află mediul de afaceri mic și mijlociu și necesitatea creerii unui Centru Operațional de Securitate Cibernetică care să vină în ajutorul lor.

Ce presupun Centrele Operaționale de Securitate la nivel global și tipurile acestuia, ce presupune deschiderea unui Centru Operațional de Securitate Cibernetică în R. Moldova și care ar fi rolul și impactul acestuia pentru organizațiile din Moldova, necesitatea deschiderii acestuia, tipurile de probleme și incidente pe care urmează să le rezolve, sunt doar o parte de informațiii care sunt descrise în capitolul doi al acestei lucrări. Iar lista cu recomandări minime pe care ar trebui să le implementeze o companie, demonstrează utilitatea creării unui astfel de centru cât și importanța lui națională.

Lucrarea este finalizată cu capitolul trei în care este prezentată viitoare platformă interactivă de securitate "E-Security" care are ca și scop prezentarea celor trei direcții de activitate ale acesteia precum, centru de analiză și implementare a soluțiilor de Securitate, centru de instruire privind securitatea informațională cât și un laborator de simulări a situațiilor de atac cibernetic. Avantajul mare pe care îl va aduce platforma dată companiilor este că acestea vor putea apela la aceasta oricând, necătând la tipurile de probleme sau lacune de informații de securitate cu care se confrută acestea.

În concluzie pot afirma faptul că pe măsură ce atacurile cibernetice devin tot mai răspândite în întreaga lume, organizațiile comerciale trebuie să găsească modalități și soluții cât mai eficiente de a-și proteja infrastructura. Pe măsură ce multe atacuri sunt lansate împotriva unor sisteme specifice, contracararea acestor atacuri țintite devine tot mai dificilă. Iar această lucrarea vine să demonstreze odată, efectiv problemele cu care se confruntă acestea și ulterior necesitatea creării unui centru operațional de securitate cibernetică privat, și inclusiv realizarea unei platforme de securitate care să vină în ajutorul companiilor, să le maturizeze din punct de vedere a securității informaționale și să le ajute cu costuri minimale atunci când au nevoie.

REFERINȚE BIBLIOGRAFICE

Sondaje

1. [1] *Evaluarea problemelor cibernetice și a securității informaționale la nivelul companiilor, perioada ianuarie – septembrie 2021*, Sondaj realizat în baza răspunsurilor companiilor mici și mijlocii din R. Moldova Accesul la sondaj poate fi realizat prin accesarea acestui link: *https://forms.office.com/Pages/ResponsePage.aspx?id=GzmE0KJExUqO7V87RM0y-Pr8qA5rzOFJiMlFo1O3MmRUMDBINVdRTTU4Q1NJNEJIMUtHSUJFMTVXTy4u&wdLOR=c542DC48A-993F-4DB3-A8C4-F7F6B9F065BE*

Cărți și monografii

2. [12] BOLUN, Bolun, CIORB, Dumitru, ZGUREANU, Zgureanu, BULAI, Rodica, ROSTISLAV Călin, BODOGA Cristina, Informatics Security Assessment in the Republic of Moldova, în coautorat, *Journal of Engineering Science, Electronics and Computer Science, Computers and Information Technology, Vol. XXVII, no. 4 (2020), pp. 103 – 119*
3. [17] MITNICK, K. and SIMON, W., *The Art of Deception: Controlling the Human Element of Security*, Indianapolis (Wiley), 2002.
4. BULAI, Rodica, CIORBĂ, Dumitru, ȚURCANU, Dinu, *Education in Cybersecurity*, Central and Eastern European e|Dem and e|Gov Days 2019 Budapest, Hungary, 2-3 mai 2019
5. BRĂGARU, Tudor, *Dezvoltarea și implementarea sistemului de management al securității informației (în baza ISO/IEC 27001),* Chișinău, 2021.

Articole din reviste științifice

6. [8] INAKI, Aldasoro, FROST Jon, GAMBACORTA, Gambacorta, WHYTE David, BIS Bulletin, no. 37, *Covid-19 and cyber risk in the financial sector*, 2021.
7. [9] DataReportal, Hootsuite, & We Are Social, *Global digital overview*, Ianuarie 2021, https://datareportal.com/global-digital-overview
8. [14] DIMOV, I. *Security awareness statistics*, 29 august 2017, https://www.infosecinstitute.com/
9. [15] АНИСИМОВ, Александр, *Менеджмент в сфере информационной безопасности. Департамент информационной безопасности и работа с персоналом*, http://www.intuit.ru/studies/courses/563/419/lecture/9580?page=2

10. [16] BOLUN, Bolun, CIORB, Dumitru, BULAI, Rodica *Support of Education in Cybersecurity*, in The Pro Publico BonoJournal, https://folyoirat.ludovika.hu/index.php/ppb/, Hungary, 2021
11. [18] TRICIA A. H., *Cybersecurity Culture: The Root of the Problem*, https://www.uscybersecurity.net/cybersecurity-culture/
12. NABE, Cedric, Deloitte, *Impact of COVID-19 on Cybersecurity*, Ianuarie 2021, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html
13. MORGAN, S. *Healthcare industry to spend $125 billion on cybersecurity from 2020 to 2025*, 8 septembrie 2020, https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/
14. DE GROOT, Juliana, W*hat is a Security Operations Center (SOC)?*, 25 noiembrie 2020, https://digitalguardian.com/blog/what-security-operations-center-soc
15. KARAYMEH, Ashraf, *Next-Generation Security Operations Centers*, 4 martie 2021, https://home.kpmg/sa/en/home/insights/2021/03/next-generation-security-operations-centers.html
16. FIRCH, Jason, *10 Cyber Security Trends You Can't Ignore In 2021*, 29 aprilie 2021, https://purplesec.us/cyber-security-trends-2021/
17. JHONSON, Johna Till, *Cybersecurity & Risk Management*, https://nemertes.com/cybersecurity-risk-management/

Standarde, norme, ghiduri de utilizare

18. [19] HOTĂRÎRE Nr. 201 din 28-03-2017 privind aprobarea cerințelor minime obligatorii de securitate cibernetică https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro

Pagini WEB

19. [2] *Data Breach Investigations Report* https://www.verizon.com/business/resources/reports/dbir/
20. [3] *Staggering Phishing Statistics in 2020*, https://securityboulevard.com/2020/12/staggering-phishing-statistics-in-2020/
21. [4] Fior Market Research LLP, September 30, 2020, *Global healthcare cyber security market is expected to reach USD 33.65 billion by 2027*, https://www.globenewswire.com/news-release/2020/09/30/2101131/0/en/Global-Healthcare-Cyber-Security-Market-Is-Expected-to-Reach-USD-33-65-Billion-by-2027-Fior-Markets.html/
22. [5] *Healthcare data breaches: Insights and implications*, https://www.mdpi.com/2227-9032/8/2/133

23. [6] IBM Report: *Compromised Employee Accounts Led to Most Expensive Data Breaches Over Past Year* https://newsroom.ibm.com/2020-07-29-IBM-Report-Compromised-Employee-Accounts-Led-to-Most-Expensive-Data-Breaches-Over-Past-Year
24. [7] Deloitte *Navigating the cyber impacts of COVID-19* https://www2.deloitte.com/in/en/pages/risk/articles/in-ra-navigating-the-cyber-impacts-of-covid-19.html
25. [10] *Cybersecurity: Tendințe 2020,* https://www.electronica-azi.ro/2020/04/06/cybersecurity-tendinte-2020/
26. [11] *Current state of cybercrime* https://www.rsa.com/content/dam/en/white-paper/2019-current-state-of-cybercrime.pdf
27. [13] *The Key to Reducing Cybersecurity Risk* https://www.cyber-observer.com/key-to-reduce-cybersecurity-risk-with-cyber-observer/
28. TechTarget, *8 challenges every security operations center faces,* https://www.techtarget.com/searchsecurity/tip/8-challenges-every-security-operations-center-faces
29. Cyber Observer. *29 must-know cybersecurity statistics for 2020*, 8 martie 2020, https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/
30. ENISA, *Top ten cyber hygiene tips for SMEs during COVID-19 pandemic*, 2 iunie 2020, https://www.enisa.europa.eu/news/enisa-news/top-ten-cyber-hygiene-tips-for-smes-during-covid-19-pandemic
31. INTERPOL, *COVID-19 Cyberthreats*, 4 iunie 2020, https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats
32. MonsterCloud, *Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic*, August 2020, https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html