MINISTERUL EDUCAŢIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Electronică și Telecomunicații

Departamentul Telecomunicații și Sisteme Electronice

Admis la susţinere

Şefa departament:

Tîrșu Valentina conf. Univ., dr.

_____

„_____” _____2024

Securitatea cibernetică în infrastructura de telecomunicații: amenințări, riscuri și soluții

Proiect/teză de licenţă

Student: **Șonțu Doru, IMTC-201**

Coordonator: **Țurcanu Tatiana conf. univ., dr.**

Consultant: **Grițco Maria asist. univ.**

Chişinău, 2024

ADNOTARE

Șonțu Doru

Tema: Securitatea cibernetica în infrastructura de telecomunicații: amenințări, riscuri și soluții .

Structura tezei cuprinde: introducerea, 3 capitole, bibliografie din 34 titluri, 76 pagini de bază.

Cuvinte cheie: Securitate cibernetică, amenințări, atacuri, riscuri, solutii.

Scopul și obiectivele lucrării: Scopul acestei teze este să exploreze și să analizeze amenințările cibernetice cu care se confruntă infrastructura de telecomunicații, să evalueze riscurile asociate și să identifice soluțiile și practicile optime pentru a le contracara eficient. Pentru a atinge acest obiectiv, vom examina în detaliu diversele tipuri de amenințări cibernetice, de la atacuri de tip DDoS și phishing la exploatarea vulnerabilităților de securitate. Vom investiga, de asemenea, impactul acestor amenințări asupra infrastructurii de telecomunicații și a utilizatorilor săi, inclusiv pierderile financiare, deteriorarea reputației și perturbările operaționale.

În plus, această teză va analiza soluțiile și practicile de securitate cibernetică disponibile pentru a contracara amenințările identificate. Vom explora tehnologiile și instrumentele de securitate utilizate pentru protejarea rețelelor de comunicații și a datelor transmise, precum și politici și proceduri adecvate pentru gestionarea riscurilor și pentru prevenirea incidentelor de securitate.

Prin investigarea profundă a acestor aspecte și propunerea unor strategii și soluții eficiente, această teză își propune să contribuie la înțelegerea și îmbunătățirea securității cibernetice în infrastructura de telecomunicații, promovând astfel stabilitatea și fiabilitatea serviciilor de comunicații critice pentru societatea modernă.

Lucrarea este inpărțită in 3 capitole:

Capitolul 1: Noțiuni Generale: Detaliază conceptele fundamentale ale securității cibernetice, analizând diferitele tipuri de vulnerabilități și riscuri:

- Vulnerabilități de sistem, aplicație, rețea și umane.
- Riscuri tehnice, erori umane, amenințări interne și pierderea/furtul de date.
- Amenințări precum malware, phishing, hacking, atacuri DoS/DDoS, atacuri asupra identității, ingineria socială și amenințările interne.

Sunt discutate și componentele esențiale ale securității cibernetice și soluțiile:

- Firewall-uri, criptarea datelor, autentificare puternică, sisteme de detecție/prevenire a intruziunilor, monitorizare și jurnalizare, actualizări de securitate, educație și conștientizare.

Capitolul 2: Amenințările: Analizează sursele comune de amenințări cibernetice și diferitele tipuri de atacuri:

- Atacuri malware (spyware, ransomware), phishing, man-in-the-middle, atacuri DoS și DDoS, atacuri de injecție.
- Examinarea detaliată a unor atacuri cibernetice notabile, cum ar fi atacurile asupra companiei de retail Target și atacul NotPetya.

Capitolul 3: Soluții de securitate: Capitolul descrie diverse tipuri și instrumente de securitate cibernetică:

- Securitatea Cloud, infrastructurii critice, prevenirea pierderii datelor (DLP), securitatea aplicațiilor, informațiilor, rețelei, utilizatorilor finali, operațională, punctelor terminale, site-urilor web, big data, blockchain, protecția împotriva atacurilor DDoS și bot-urilor, securitatea bazelor de date și a API-urilor.
- Instrumente de securitate cibernetică precum firewall-uri, software antivirus, servicii PKI, instrumente de monitorizare a securității rețelei, servicii MDR, testarea de penetrare, scanarea vulnerabilităților web și instruirea personalului.
- Cadrele de securitate cibernetică, componentele lor, nivelurile de implementare și profilele.

ANNOTATION

Șonțu Doru

Cybersecurity in Telecommunications Infrastructure: Threats, Risks, and Solutions.

The structure of the thesis includes: introduction, 3 chapters, bibliography with 34 titles, 76 main pages.

Keywords: Cybersecurity, threats, attacks, risks, solutions.

Purpose and objectives of the work: The purpose of this thesis is to explore and analyze the cyber threats facing telecommunications infrastructure, to assess the associated risks, and to identify optimal solutions and practices to counter them effectively. To achieve this objective, we will examine in detail the various types of cyber threats, from DDoS and phishing attacks to the exploitation of security vulnerabilities. We will also investigate the impact of these threats on telecommunications infrastructure and its users, including financial losses, reputational damage, and operational disruptions.

Additionally, this thesis will analyze the available cybersecurity solutions and practices to counter the identified threats. We will explore the technologies and security tools used to protect communication networks and transmitted data, as well as appropriate policies and procedures for risk management and preventing security incidents.

By thoroughly investigating these aspects and proposing effective strategies and solutions, this thesis aims to contribute to the understanding and improvement of cybersecurity in telecommunications infrastructure, thus promoting the stability and reliability of critical communication services for modern society.

The work is divided into 3 chapters:

Chapter 1: General Concepts: Details the fundamental concepts of cybersecurity, analyzing the different types of vulnerabilities and risks:

• System, application, network, and human vulnerabilities.

• Technical risks, human errors, internal threats, and data loss/theft.

• Threats such as malware, phishing, hacking, DoS/DDoS attacks, identity attacks, social engineering, and internal threats.

Essential components of cybersecurity and solutions are also discussed:

• Firewalls, data encryption, strong authentication, intrusion detection/prevention systems, monitoring and logging, security updates, education, and awareness.

Chapter 2: Threats: Analyzes common sources of cyber threats and various types of attacks:

• Malware attacks (spyware, ransomware), phishing, man-in-the-middle, DoS and DDoS attacks, injection attacks.

• Detailed examination of notable cyber attacks, such as the attacks on Target retail company and the NotPetya attack.

Chapter 3: Security Solutions: Describes various types and tools of cybersecurity:

• Cloud security, critical infrastructure, data loss prevention (DLP), application security, information security, network security, end-user security, operational security, endpoint security, website security, big data, blockchain, DDoS and bot protection, database, and API security.

• Cybersecurity tools such as firewalls, antivirus software, PKI services, network security monitoring tools, MDR services, penetration testing, web vulnerability scanning, and staff training.

• Cybersecurity frameworks, their components, implementation levels, and profiles.

Cuprins

INTRODUCERE

În epoca digitală în care trăim, infrastructura de telecomunicații reprezintă o coloană vertebrală a societății moderne, facilitând comunicarea instantanee și accesul la informații critice în timp real. Cu toate acestea, odată cu creșterea dependenței noastre de tehnologie și conectivitate online, amenințările cibernetice asupra acestei infrastructuri au devenit din ce în ce mai sofisticate și mai omniprezente. Aceste amenințări pot afecta nu doar integritatea și confidențialitatea datelor, ci și funcționarea corectă a serviciilor esențiale, punând în pericol securitatea națională și bunăstarea societății în ansamblu.

Scopul acestei teze este să exploreze și să analizeze amenințările cibernetice cu care se confruntă infrastructura de telecomunicații, să evalueze riscurile asociate și să identifice soluțiile și practicile optime pentru a le contracara eficient. Pentru a atinge acest obiectiv, vom examina în detaliu diversele tipuri de amenințări cibernetice, de la atacuri de tip DDoS și phishing la exploatarea vulnerabilităților de securitate. Vom investiga, de asemenea, impactul acestor amenințări asupra infrastructurii de telecomunicații și a utilizatorilor săi, inclusiv pierderile financiare, deteriorarea reputației și perturbările operaționale.

În plus, această teză va analiza soluțiile și practicile de securitate cibernetică disponibile pentru a contracara amenințările identificate. Vom explora tehnologiile și instrumentele de securitate utilizate pentru protejarea rețelelor de comunicații și a datelor transmise, precum și politici și proceduri adecvate pentru gestionarea riscurilor și pentru prevenirea incidentelor de securitate.

Prin investigarea profundă a acestor aspecte și propunerea unor strategii și soluții eficiente, această teză își propune să contribuie la înțelegerea și îmbunătățirea securității cibernetice în infrastructura de telecomunicații, promovând astfel stabilitatea și fiabilitatea serviciilor de comunicații critice pentru societatea modernă.

BIBLIOGRAFIE

1. ADRIANA-MEDA UDROIU. Soluție de securitate aplicabilă sistemelor informatice integrate de management al activităților. Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București. In: Romanian Journal of Information Technology and Automatic Control, Vol. 30, No. 1, 101-110,. Accessed: 06.01.2024. Available:https://www.researchgate.net/publication/340361582_Solutie_de_securitate_aplicabila_sistemelor_informatice_integrate_de_management_al_activitatilor/fulltext/5e8dcc86a6fdcca789fe0936/Solutie-de-securitate-aplicabila-sistemelor-informatice-integrate-de-management-al-activitatilor.pdf
2. Ghidul securității cibernetice. 10.2019. Accessed: 06.01.2024. [Online]. Available:https://stisc.gov.md/sites/default/files/ghiduri/ghidul_securitatii_cibernetice_0.pdf
3. POLITICA DE SECURITATE PRIVIND PROTECŢIA DATELOR CU CARACTER PERSONAL LA PRELUCRAREA ACESTORA ÎN CADRUL SISTEMELOR INFORMAŢIONALE GESTIONATE DE UNIVERSITATEA DE STAT DIN MOLDOVA. USM. 28.04.2015. Accessed: 06.01.2024. [Online]. Available:https://usm.md/wp-content/uploads/POLITICA-DE-SECURITATE.pdf
4. CYBERSECURITY SOLUTIONS For Critical Operational Technologies. Pacific Northwest National Laboratory. Accessed: 06.01.2024. [Online]. Available:https://www.pnnl.gov/sites/default/files/media/file/DDST_0149_BROCH_GridCyberBooklet-DIGITAL5.pdf
5. P. SORIN EUGEN. SECURITATEA SISTEMELOR INFORMATICE. 2007. Accessed: 06.01.2024. [Online]. Available:https://cadredidactice.ub.ro/sorinpopa/files/2011/10/Curs_Securit_Sist_Inf.pdf
6. CCS146 – Securitatea Cibernetică – Securitatea Reţelelor şi a Sistemelor Informatice. 06.11.2021. Accessed: 05.01.2024. [Online]. Available:https://vdocumente.com/-site-ul-proiectului-analiza-asupra-metodelor-de-lucru-i-.html?page=1
7. Securitatea cibernetică: concepte, abordare. Accessed: 05.01.2024. [Online]. Available:https://staff.fmi.uvt.ro/~stelian.mihalas/sec_cib/cursuri/secCib.pdf
8. Securitate Cibernetica. Scribd. Accessed: 03.01.2024. [Online]. Available:https://www.scribd.com/document/510925283/securitate-cibernetica
9. TUNGGAL TYAS A. What is a Cyber Threat?. UpGuard. 17.08.2022. Accessed: 14.03.2024. [Online]. Available: https://www.upguard.com/blog/cyber-threat.
10. Cybersecurity Threats. imperva. Accesed: 15.03.2024. [Online]. Available:https://www.imperva.com/learn/application-security/cyber-security-threats/.

11. HOORY L. ADITHAM K. LIVINGSTON Z. What Is A Cyber Attack? Definition, Types & Prevention. Forbes ADVISOR. 14.08.2023. Accessed: 15.03.2024. [Online]. Available:https://www.forbes.com/advisor/business/what-is-cyber-attack/.
12. Cyber Attack. imperva. Accessed: 16.03.2024. [Online]. Available: https://www.imperva.com/learn/application-security/cyber-attack/.
13. What Is Spyware, Who Can Be Attacked, and How Can You Prevent It?. Avast. Accesed: 16.03.2024. Available: https://www.avast.com/c-spyware.
14. What is phishing?. IBM. Accessed: 18.03.2024. [Online]. Available: https://www.ibm.com/topics/phishing.
15. What is a phishing attack?. Cloudfare. Accessed: 18.03.2024. [Online]. Available: https://www.cloudflare.com/learning/access-management/phishing-attack/.
16. Man-in-the-Middle Attack: Types and Examples. Fortinet. Accessed: 19.03.2024 [Online]. Available: https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack#:~:text=A%20man-in-the-middle%20%28MITM%29%20attack%20is%20a%20form%20of,entities%20in%20a%20communication%20channel%20to%20steal%20data.
17. SWINHOE D. Man-in-the-middle (MitM) attack definition and examples. CSO. 25.03.2022. Accessed: 19.03.2024. [Online]. Available: https://www.csoonline.com/article/566905/man-in-the-middle-attack-definition-and-examples.html.
18. TUNGGAL TYAS A. What Is a Man-in-the-Middle Attack? Prevention Tips and Guide. UpGuard. 25.10.2023. Accessed: 20.03.2024 [Online]. Available: https://www.upguard.com/blog/man-in-the-middle-attack#toc-4
19. RAFTER D. What are Denial of Service (DoS) attacks? DoS attacks explained. Norton. 15.03.2022. Accessed: 25.03.2024. [Online] https://us.norton.com/blog/emerging-threats/dos-attacks-explained.
20. What Is a DDoS Attack and How Does It Work?. CompTIA. Accessed: 26.03.2024. [Online]. Available: https://www.comptia.org/content/guides/what-is-a-ddos-attack-how-it-works.
21. What is a DDoS Attack? AWS. Accessed: 26.03.2024. [Online]. Available: https://aws.amazon.com/shield/ddos-attack-protection/.
22. DDos Attacks. imperva. Accessed: 27.03.2024. [Online]. Available: https://www.imperva.com/learn/ddos/ddos-attacks/.
23. What is ransomware?. IBM. Accesed: 29.04.2024. [Online]. Available: https://www.ibm.com/topics/ransomware.

24. NARANG S. Understanding the Ransomware Ecosystem: From Screen Lockers to Multimillion-Dollar Criminal Enterprise. Tenable. 22.06.2022. Accesed: 31.03.2024. [Online]. Available: https://www.tenable.com/blog/understanding-the-ransomware-ecosystem-screen-lockers-to-multimillion-dollar-criminal-enterprise.
25. GRAW M. What is ransomware and how does it work?. 05.09.2022. techradar. Accessed: 02.04.2024. [Online]. Available: https://www.techradar.com/features/what-is-ransomware-and-how-does-it-work.
26. What is ransomware? | Ransomware meaning. Cloudfare. Acccessed: 03.04.2024. [Online]. Available: https://www.cloudflare.com/learning/security/ransomware/what-is-ransomware/.
27. Ransomware. Malwarebytes. Accessed: 06.04.2024. [Online]. Available: https://www.malwarebytes.com/ransomware.
28. BHARDWAJ P. What Is Screen Locker Ransomware and How Can You Remove It?. 08.11.2022. MAKEUSEOF. Accessed: 06.04.2024. [Online]. Available: https://www.makeuseof.com/what-is-screen-locker-ransomware/#:~:text=Screen%20Locker%20is%20a%20duplicitous%20ransomware%20that%20locks,screen%20and%20prevents%20you%20from%20using%20your%20device.
29. WALDMAN A. 10 of the biggest cyber attacks of 2020. TechTarget. 05.01.2021. Accessed: 07.04.2024 [Online]. Available: https://www.techtarget.com/searchsecurity/news/252494362/10-of-the-biggest-cyber-attacks.
30. STEINBERG S. NEARY A. NEARY S. NEARY K. (2021) Target Cyber Attack: A Columbia University Case Study. Available: https://www.sipa.columbia.edu/sites/default/files/2022-11/Target%20Final.pdf.
31. STEINBERG S. NEARY A. NEARY S. NEARY K. (2021) NotPetya: A Columbia University Case Study. Available: https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf
32. KRASZANY C. (2020) Case Study: The NotPetya Campaign. In:Információ- és kiberbiztonság (pp.485-499). 01.2020. Retrieved from: https://www.researchgate.net/publication/353072644.
33. What Are Cybersecurity Solutions?. Akami. Accessed: 08.04.2024. [Online]. Available: https://www.akamai.com/glossary/what-are-cybersecurity-solutions.
34. PERWEJ Y., ABBAS Q., DIXIT PRATAP J., AKHTAR N. A Systematic Literature Review on the Cyber Security. In:International Journal of Scientific Research and Management (IJSRM) Volume 9(Issue 12):Pages 669 - 710, 12.2021, doi:10.18535/ijsrm/v9i12.ec04.