

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departamentul Telecomunicații și Sisteme Electronice

Admisă la susținere

Șefă departament:

Valentina TÎRȘU, conf.univ., dr.

_____ 2024

**Analiza amenințărilor cibernetice și strategiile de
protecție în sectorul telecomunicațiilor**

Teză de master

Studenta: Mămăligă Mihaela, gr. MMRT-221M

Conducător: Sava Lilia, conf.univ., dr.

Chișinău, 2024

ADNOTARE

Proiectul de master al studentei Mămăligă Mihaela cu tema „ Analiza amenințărilor cibernetice și strategiile de protecție în sectorul telecomunicațiilor” are următoarea structură: introducere, 3 capitole (fiecare dintre ele având paragrafe), concluzii și bibliografie.

Cuvinte cheie: Securitate cibernetică, vulnerabilități, criptare, strategii.

Scopul principal al acestei lucrări a fost analizarea amenințărilor și strategiilor de securitate cibernetică la care pot fi supuse rețelele fără fir din telecomunicații și aplicarea a 3 standarde diferite de securizare.

Obiectivele generale:

- Studiul amenințărilor de securitate cibernetică;
- Studiul soluțiilor de securizare a rețelelor fără fir
- Aplicarea a 3 metode de securizare
- Analiza rezultatelor primite;
- Studiul strategiilor de securitate cibernetică;
- Elaburarea unui ghid de dezvoltare a unei strategii de securitate cibernetică

Pentru elaborarea acestui proiect s-a utilizat software-ul de simulare Cisco Packet Tracer, în care s-au proiectat trei rețele fără fir diferite și au fost securizate împotriva atacurilor cibernetice cu ajutorul a 3 standarde și anume protocolul WEP, protocolul WPA2-PSK și protocolul WPA2-Enterprise. S-au utilizat aceste protocoale pentru a demonstra care dintre acestea este mai efektiv. Astfel, s-a ajuns la următoarea concluzie: standardul WEP este nesigur și deja este neutilizat, standardul WPA2-PSK este ușor de implementat, dar nu oferă cel mai înalt nivel de securitate, iar standardul WPA2-ENT oferă cea mai înaltă securitate, însă implementarea acestuia este mai complexă și costisitoare.

De asemenea, în acest proiect s-a elaborat și un ghid pentru dezvoltarea unei strategii de securitate cibernetică. Astfel, în acest ghid s-au enumerat și explicat pașii de elaborare a unei strategii.

ANNOTATION

The master's project of the student Mămăligă Mihaela with the theme "Analysis of cyber threats and protection strategies in the telecommunications sector" has the following structure: introduction, 3 chapters (each with paragraphs), conclusions and bibliography.

Keywords: Cyber security, vulnerabilities, encryption, strategies.

The main purpose of this paper was to analyze the cyber security threats and strategies that wireless telecommunication networks can be subjected to and to apply 3 different security standards.

General objectives:

- Study of cyber security threats;
- Study of wireless network security solutions;
- Application of 3 security methods;
- Analysis of the received results;
- Study of cyber security strategies;
- Elaboration of a guide for the development of a cyber security strategy.

Cisco Packet Tracer simulation software was used to develop this project, where three different wireless networks were designed and secured against cyber attacks using 3 standards namely WEP, WPA2-PSK and WPA2 -Enterprise. These protocols were used to demonstrate which one is more effective. Thus, the following conclusion was reached: the WEP standard is insecure and already unused, the WPA2-PSK standard is easy to implement, but does not provide the highest level of security, and the WPA2-ENT standard provides the highest security, but its implementation it is more complex and expensive.

This project also developed a guide for developing a cyber security strategy. Thus, in this guide the steps for developing a strategy have been listed and explained.

CUPRINS

INTRODUCERE	8
1 CONCEPTE TEORETICE PRIVIND SECURITATEA CIBERNETICĂ ÎN TELECOMUNICAȚII	9
1.1. Generalități în securitatea cibernetică.....	9
1.2. Importanța securității cibernetică pentru companii.....	10
1.3. Amenințări de securitate cibernetică pentru un operator de telecomunicații.....	11
1.4. Principalele tipuri de amenințări cibernetică și modalități de a le atenua.....	13
1.5. Protejarea rețelelor și a datelor împotriva amenințărilor cibernetică.....	19
1.6. Beneficiile securității cibernetică în telecomunicații.....	20
2 ANALIZA METODELOR DE SECURIZARE A REȚELELOR DE TELECOMUNICAȚII	22
2.1. Securizarea rețelei utilizând protocolul WEP.....	22
2.2. Securizarea rețelei utilizând protocolul WPA2-PSK.....	24
2.3. Securizarea rețelei utilizând protocolul WPA2 RADIUS.....	25
2.4. Aplicarea metodelor de securizare.....	26
2.5. Avantajele și dezavantajele WEP, WPA2 PSK, WPA2 RADIUS.....	44
3 STRATEGII PRIVIND SECURITATEA REȚELELOR	46
3.1. Obiectivele și importanța strategiilor de securitate cibernetică.....	46
3.2. Strategii de securitate cibernetică.....	47
3.3. Ghid pentru dezvoltarea unei stragerii de securitate cibernetică.....	52
CONCLUZII	55
BIBLIOGRAFIE	57

INTRODUCERE

Securitatea cibernetică în telecomunicații reprezintă un domeniu esențial în era digitală actuală, în care infrastructurile și serviciile de comunicații electronice joacă un rol central în viața cotidiană și în funcționarea întreprinderilor și a guvernelor. Această disciplină se concentrează asupra protejării rețelelor de comunicații și a datelor împotriva accesului, utilizării și manipulării neautorizate, precum și a amenințărilor cibernetică în continuă evoluție.

Într-o lume în care tot mai multe informații și procese critice sunt digitalizate și transmise prin intermediul rețelelor de telecomunicații, securitatea cibernetică devine o prioritate crucială. Infrastructurile de telecomunicații trebuie să fie protejate împotriva unui spectru larg de amenințări, care pot varia de la atacuri comune, precum malware și phishing, până la atacuri sofisticate ale actorilor statali sau grupurilor de hackeri.

Scopul principal al acestei lucrări este analiza amenințărilor de securitate cibernetică cu scopul identificării strategiilor de securitate la care pot fi supuse rețelele fără fir din telecomunicații.

Principalele obiective ale acestei lucrări sunt:

- Studiul amenințărilor de securitate cibernetică;
- Studiul soluțiilor de securizare a rețelelor fără fir;
- Aplicarea a 3 metode de securizare;
- Analiza rezultatelor primite;
- Studiul strategiilor de securitate cibernetică;
- Elabărarea unui ghid de dezvoltare a unei strategii de securitate cibernetică.

Tema dată este una foarte actuală deoarece securitatea cibernetică în telecomunicații implică o gamă variată de strategii și tehnologii, cum ar fi criptarea datelor, firewall-urile, sistemele de detecție și prevenire a intruziunilor, gestionarea accesului, educația utilizatorilor și colaborarea între organizații și autorități. Este un domeniu în evoluție continuă, care necesită o adaptabilitate constantă pentru a ține pasul cu amenințările cibernetică din ce în ce mai sofisticate.

BIBLIOGRAFIE

- 1 CYBER THREATS OUTREACH IN TELECOM. Guidelines for national Authorities and telecom providers on outreach to users about cyber threats. Martie 2022
- 2 Security in telecommunications and information technology (7th edition). An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications. 09/2020
- 3 Amro Mohamed, Eleanor Barlow. Creșterea preocupărilor de securitate în industria telecomunicațiilor. februarie 2021
- 4 Ludmila Peca, Dinu Țurcanu. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chișinău, Publisher „Tehnica-UTM”, 2022.
- 5 Dinu Țurcanu, Natalia Spinu, Serghei Popovici, Tatiana Țurcanu. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. Journal of Social Sciences, Vol. IV, no. 1 (2021), pp. 74 – 83.
- 6 Annual-Cyber-Threat-Report-ACSC. 2022
- 7 Draft Telecommunications Security Code of Practice. Department for Digital, Culture, Media and Sport. 2022
- 8 Nistiriuc Pavel, Țurcanu Tatiana, Chihai Andrei, Sava Lilia. Comunicații optice și securitatea lor. Partea II: Note de curs. Chișinău: Tehnica-UTM, 2023, 38 p., ISBN 978-9975-45-9.
- 9 IoT SECURITY GUIDELINES for Network Operators. GSM Association. 29 Februarie 2020
- 10 Ludmila Peca, Dinu Țurcanu. Network security: Practical examples solved to be introduced in network security. Chișinău, Publisher „Tehnica-UTM”, 2023, pp. 7-232.
- 11 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.
- 12 Telecomunicații și securitate cibernetică, Protejarea datelor în rețele. Disponibil: <https://utilitiesone.com/telecommunications-and-cybersecurity-protecting-data-on-networks>
- 13 Rina Țurcan, Dinu Țurcanu, Alexandru Ciubuc. The impact of Internet access on economic development. The 5th Economic International Conference „COMPETITIVENESS AND SUSTAINABLE DEVELOPMENT”, 2-3.11.2023. <https://doi.org/10.52326/csd2023.24>.
- 14 Dinu Țurcanu, Serghei Popovici, Tatiana Țurcanu. Digital signature: advantages, challenges and strategies,” Journal of Social Sciences, Vol. III, no. 4 (2020), pp. 62 - 72.

- 15 Cybersecurity in Telecom: Protecting Networks & Data from Cyber Threats. Disponibil: <https://skill-lync.com/blogs/technical-blogs/cse-cybersecurity-in-telecom-protecting-networks-data-from-cyber-threats>
- 16 Security in Telecom: 5 Current Cyber Threats and Solution. Disponibil: <https://www.infopulse.com/blog/security-telecom-threats-and-solutions>
- 17 Top Cybersecurity Threats in 2023. Disponibil: <https://onlinedegrees.sandiego.edu/top-cyber-security-threats/>
- 18 WHY IS CYBER SECURITY IMPORTANT FOR TELCO COMPANIES? Disponibil: <https://bilginc.com/en/blog/why-is-cyber-security-important-for-telco-companies-5550/>
- 19 Use of Cybersecurity in Telecom Industries. Disponibil: <https://insidetelecom.com/cybersecurity-in-telecom-industries/>
- 20 Securitatea cibernetică în industria telecomunicațiilor: 7 provocări cheie. Disponibil: <https://elnion.com/2023/04/28/cybersecurity-in-the-telecommunications-industry-7-key-challenges/>
- 21 Soluții de securitate pentru telecomunicații, Disponibil: <https://www.bitdefender.com/business/industry-solutions/telecommunications-cybersecurity.html>
- 22 Types of WPA2 Authentication. Disponibil: <https://www.cloudradius.com/types-of-wpa2-authentication/>
- 23 EVOLUTION OF WI-FI PROTECTED ACCESS: SECURITY CHALLENGES. Disponibil: https://hit.skku.edu/?page_id=2363
- 24 What is Wi-Fi Protected Access (WPA)? Disponibil: <https://www.zenarmor.com/docs/network-security-tutorials/what-is-wpa>
- 25 What is WPA2-PSK? Disponibil: <https://www.scaler.com/topics/cyber-security/wpa2-psk/>
- 26 How to Develop a Comprehensive Cybersecurity Strategy. Disponibil: <https://www.eccu.edu/blog/cybersecurity/how-to-develop-a-cyber-security-strategy/>
- 27 Cyber Security Strategies. Disponibil: https://www.tutorialspoint.com/information_security_cyber_law/cyber_security_strategies.htm