Universitatea Tehnică a Moldovei

Sistem pentru analiza riscurilor la transferul de date în cadrul unei rețele corporative

Student: **Cătălina ȚAPU**

Conducător: **Victor ABABII**

conf.univ., dr

Chişinău, 2022

ADNOTARE

la teza de master cu tema „Sistem pentru analiza riscurilor la transferul de date în cadrul unei rețele corporative” a masterandului grupa CRI-201M Cătălina ȚAPU.

Structura tezei cuprinde: introducere, trei capitole, concluzii, bibliografie și referințe,76 pagini de text de bază, 26 figuri.

Scopul lucrării: studiul și analiza provocărilor actuale prezente la transferul de date în cadrul unei rețele corporative, identificându-se atacurile, amenințările, vulnerabilitățile și riscurile, precum și aplicarea metodelor în vederea asigurării securității informaționale.

Printre **obiectivele** principale ale lucrării se enumeră analiza amenințărilor, riscurilor și vulnerabilităților la adresa rețelei corporative, studiul privind importanța instrumentelor și modelelor de asigurare a securității informaționale la transferul de date, precum și aplicarea metodei de asigurare a securității informaționale prin implementarea tehnologiei VPN și prin monitorizarea continuă a rețelei.

Capitolul I, **„Aspecte generale privind rețelele corporative”** cuprinde studiul teoretic privind conceptul de rețea informațională/rețea corporativă, avantajele și dezavantajele acestora. În acest capitol sunt evidențiate riscurile, amenințările și vulnerabilitățile la care sunt supuse rețelele sus menționate.

În Capitolul II, **„Metode și tehnici de asigurare a securității rețelei corporative”** sunt analizate și descrise instrumentele de securitate și enumerate modelele de securitate. La acest subiect am abordat problema de securitate destul de actuală atât la nivel național, cât și internațional prin prisma politicilor și standardelor de securitate informațională.

Capitolul III, **„Implementarea tehnologiei VPN pe baza protocoalelor Ipsec și OpenVPN prin routerul MikroTik”,** descrie realizarea unei reţele VPN cu ajutorul protocoalelor, precum OpenVPN, și pașii privind accesul securizat de la distanță la rețeaua corporativă.

Teza de masterat nu prezintă un produs finit. Lucrarea prezintă o bază solidă în abordarea securității comunicațiilor, un interes din punct de vedere al tehnologiei moderne de asigurare a transmite informații cu un înalt grad de confidențialitate. Abordarea teoretică este completată prin implementarea tehnologiilor astfel, ca la următoarea etapă, să se prevadă dezvoltarea, completarea cu noi funcționalități și îmbunătățiri încât, serviciile testate să fie integrate în interiorul unui sistem de comunicații și informatică complex.

Valoarea aplicativă a cercetării: se impune de a construi cu resurse tehnice optime sisteme de comunicații corporative eficiente, performante și stabile în conformitate cu standardele internaționale cu tendința ca transferul și păstrarea informației să ruleze doar în interiorul organizației. Materialele tezei pot constitui un suport pentru elaborarea unor lucrări ştiinţifice ulterioare, precum și cursuri de specializare în domeniul rețelelor corporative.

Cuvinte-cheie: rețea corporativă, securitatea rețelelor, firewall, VPN, OpenVPN, Mikrotik.

ANNOTATION

to the master thesis with the topic "System for risk analysis for data transfer within a corporate network" of the master student group CRI-201M Cătălina ȚAPU.

The structure of the thesis includes: introduction, three chapters, conclusions, bibliography and references, 76 pages of basic text, 26 figures.

Purpose of the paper: to study and analyze the current challenges present in the transfer of data within a corporate network, identifying attacks, threats, vulnerabilities and risks, as well as the application of methods to ensure information security.

The main objectives of the paper include the analysis of threats, risks and vulnerabilities to the corporate network, the study on the importance of tools and models to ensure information security in data transfer, and the application of the method of information security by implementing VPN technology and monitoring continuous network.

Chapter I, "General aspects of corporate networks", covers the study of the theory on the concept of information network / corporate network, their advantages and disadvantages. This chapter highlights the risks, threats and vulnerabilities to which the above-mentioned networks are subject.

In Chapter II, "Methods and Techniques for Ensuring Corporate Network Security," security tools are analyzed and described, and security models are listed. In this regard, we have addressed the current issue of security, both nationally and internationally, in terms of information security policies and standards.

Chapter III, "Implementing VPN technology based on Ipsec and OpenVPN protocols through the MikroTik router," describes how to build a VPN using protocols such as OpenVPN, and the steps to secure remote access to the corporate network.

The master's thesis does not present a finished product. The paper provides a solid basis for addressing communications security, an interest in modern technology to provide information with a high degree of confidentiality. The theoretical approach is complemented by the implementation of technologies so that, in the next stage, development, completion and new functionalities and improvements are provided, so that the tested services are integrated within a complex information and communication system.

The applicative value of the research: it is necessary to build with optimal technical resources systems of efficient, high-performance and stable corporate communications in line with international standards with the tendency to transfer and store information only within the organization. The materials of the thesis can be a support for the elaboration of further scientific papers as well specialization courses in the field of corporate networks.

Keywords: corporate network, network security, firewall, VPN, OpenVPN, Mikrotik.

CUPRINS:

INTRODUCERE

Actualmente, în noile condiții determinate ca urmare a dezvoltării tehnologiilor informaționale putem analiza transformarea spațiul cibernetic într-un mediu caracterizat de entuziasm și oportunități pede o parte și de provocări și nesiguranță pe de altă parte. Observăm o strânsă legătură între riscurile induse și măsurile de control ce trebuie implementate de instituții și organizații pentru rețelele de calculatoare la transferul de date.

Se cunoaște că spațiul informațional este în continuă creștere și dezvoltare, însă odată cu progresarea acestuia evoluează și pericolele, crește numărul vulnerabilităților nou descoperite, se intensifică pierderile de date. Se mai știe că instrumentele și metodele de realizare a atacurilor sunt larg răspândite, iar capacitățile tehnice și numărul utilizatorilor capabili de provocarea unui adevărat dezastru este în avansare.

Scopul general al acestei lucrări de cercetare îl reprezintă studiul și analiza provocărilor actuale prezente la transferul de date în cadrul unei rețele corporative, identificându-se atacurile, amenințările, vulnerabilitățile și riscurile, precum și aplicarea metodelor în vederea asigurării securității informaționale.

Afirmăm just că utilizarea rețelelor corporative duce la o comunicare îmbunătățită între angajații instituției, precum și clienții și furnizorii acesteia [23]. Rețelele reduc necesitatea ca oranizațiile să întrebuințeze alte forme de transfer de informații, cum ar fi telefonul sau poșta.

Suportul metodologic și teoretico-științific de cercetare asupra tezei este alcătuit dintr-o totalitate de metode: documentarea științifică (informarea, studierea documentelor, observarea), analiza și sinteza, statistica, generalizarea și sistematizarea, abstractizarea și modelarea teoretică, precum și interpretarea surselor bibliografice teoretice, comparația și interpretarea rezultatelor. Toate acestea au permis deschiderea noilor oportunități de abordare a unor idei și perspective a rețelelor informaționale, care propun soluții realiste și viabile în măsură să asigure transferul de date de la sursă la destinație fără abateri.

BIBLIOGRAFIE

1. https://olacom.ru/ro/ssd/korporativnye-informacionnye-sistemy-korporativnaya-set/ (accesat la 10.09.2021).

2. Autor OPREA Dumitru, Editura Polirom, Iaşi, 2003, "Protecţia şi securitatea informaţiilor" pag.27.

3. Ioan-Cosmin MIHAI (coordonator), Costel CIUCHI, Gabriel-Marius PETRICĂ "Provocări actuale în domeniul securității cibernetice - impact și contribuția României în domeniu", disponibilă online http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf

4. Masterand: Nechifor C. Francisca-Amalia Proiect „Cercetări privind securitatea datelor în sistemele informatice", București 2019.

5. I.C. Mihai, G. Petrică, Securitatea informațiilor. Ediția a II-a, îmbunătățită și adăugită, Editura Sitech, 2014.

6. L.Scripcariu, I. Bogdan, L. Nicolaescu „ Securitatea rețelelor de comunicații", Casa de Editură „ Venus" Iași 2008, pag 160.

7. BRAGARI Tatiana, Introducere în rețelele de calculatoare, http://www.afahc.ro/facultate/cursuri/retele_note_curs (Accesat la 10.09.2021).

8. Autor OPREA Dumitru, Editura Polirom, Iaşi, 2003, "Protecţia şi securitatea informaţiilor" pag.79.

9. Autor MIHAI Ioan-Cosmin, Editura Dunărea de Jos Galați, 2007 „Securitatea sistemului informatic", pag .23-28.

10. Autor NECULCEA Vladislav Manual „Codul de practică al managementului securităţii informaţiilor" pag 19-25

11. GHID de securitate cibernetică pentru funcționarii publici. Elaborat de: Centrul de răspuns la incidente cibernetice CERT-GOV-MD din cadrul I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică" p.10

12. Autor ILIESCU Florin-Mihai Editura CISA, CISSP, Manual „Politica de Securitate a Informației" pag.7-9

13. Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, Jurnalul Oficial al Uniunii Europene, 19 iulie 2016.

14. Thomas Rid & Peter McBurney (2012) Cyber-Weapons, The RUSI Journal,17:1, pp. 6-13.

15. Ștefan-Victor NICOLAESCU, „Rețele virtuale dispersate", Editura Printech, București, 2011 pag. 38-39

16. John Bennet „Ce este un VPN? Ghidul începătorului" 18 aprilie 2020 Editura România pag. 24

17. https://wiki.merionet.ru/seti/61/struktura-korporativnoj-seti/ (Accesat la 12.09.2021)

18. https://life-prog.ru/1_14346_korporativnie-seti.html (Accesat la 09.09.2021)

19. Королев И.Д, Выявление уязвимостей информационных систем, Новосибирск: СибАК, 2016, P.11

20. https://newtravelers.ru/ro/poleznoe/korporativnye-seti-klassifikaciya-korporativnyh-setei-yavlyaetsya-li-korporativnaya-set-lokalnoi.html (Accesat la 10.09.2021)

21. Cod de bune practici pentru securitatea sistemelor informatice și de comunicații, p. 24, disponibil la https://cert.ro/ (Accesat la 10.09.2021)

22. Joseph Migga Kizza, Guide to computer network security. Fourth Edition, Ed. Springer, 2017.

23. Ryndin A., Khaustovich A. Proiectarea sistemelor informatice corporative / editura "Kvarta"

24. Kulgin M. " Tehnologiile rețelelor corporative&quot.

25. Valerii BUREC **“**ПРАКТИКУМ ПО ОБОРУДОВАНИЮ MIKROTIK 9 ИЮЛЬ 2018” pag. 154.

26. COLUN Tatiana “Securitatea sistemelor informatice - pilon de bază al siguranței informaționale” 2018 “ICTEI” Chisinau, 24—27 May pag.358

27. Kosarev V.P. Sisteme și rețele de calculatoare: Manual / Ed. V.P. Kosareva și L.V. Eremina.

28. Petriciuc Vasile „Organizarea managementului rețelelor informatice într-o instituție guvernamentală”, 2020

29. John COWLEY, "Communications and Networking". An Introduction, Ediția a 2-a, Editura "Springer" 2012. p.15

30. LEGEA Nr. 299 din 21.12.2017 privind aprobarea Concepției securității informaționale a Republicii Moldova Publicat: 16.02.2018 în Monitorul Oficial Nr. 48-57 art Nr.122.

31. LEGEA Nr. 241 din 15.11. 2007 cu privire la comunicațiile electronice Publicat : 14-03-2008 în Monitorul Oficial Nr. 51-54 art. 155.

32. HOTĂRÎRE privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 și a Planului de acțiuni pentru implementarea acesteia.

33. HOTĂRÎRE Nr. 134 din 19-07-2018 pentru aprobarea Strategiei naționale de apărare și a Planului de acțiuni privind implementarea Strategiei naționale de apărare pentru anii 2018–2022 Publicat: 03-08-2018 în Monitorul Oficial Nr. 285-294 art. 441.

34. Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, Hotărîrea Guvernului nr. 811 din 29 octombrie 2015, Monitorul Oficial nr. 306-310/905 din 13.11.2015.

35. Autor STĂNESCU Mihaela, Articol: Internetul sub amenințare: virușii informatici.

36. https://www.enisa.europa.eu (Accesat la 10.09.2021).

37. https://stisc.gov.md (Accesat la 10.09.2021).