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

Admis la susținere
Șef departamentTSE:
Sava Lilia, conf.univ.dr.
_____
"___" _____2023

Analiza și compararea metodelor de securizare în tehnologia Cloud.

Teză de Master

Student: **Svișcic Dumitru,**
gr. SISRC-211M

Coordonator: **Cerbu Olga,**
conf.univ.dr.

Chișinău, 2023

ADNOTAREA

Autor: Svișcic Dumitru, gr. SISRC-211M.

Tema: " Analiza și compararea metodelor de securizare în tehnologia Cloud. ".

Structura lucrării: lucrarea este compusă din coperta, pagina de titlu, avizul, adnotarea, introducere, capitolul 1, capitolul 2, capitolul 3, concluzie, bibliografie, anexe.

Cuvinte-cheie: cloud, algoritmi, riscuri, securitatea informației, amenințări, host, vmware.

Scopul lucrării: compararea metodelor de securizare în Cloud .

Obiectivele lucrării:

- Compararea metodelor de securizare în Clod.
- Analiza algoritmilor de evaluare a amenințărilor.
- Cercetarea procesului de control asupra riscurilor.
- Implementarea unui cloud securizat.
- Analiza eficacității cloudului.

Motodele aplicate la elaborarea lucrării: mașini virtuale VirtualBox.

Rezultatele obținute: a fost efectuată o conexiune sigură între user și cloud, au fost analizate nenumărate amenințări care pot apărea la adresa cloudului cât și userului și au fost propuse metode cât mai sigure de protecție.

ANNOTATION

Author: Svișcic Dumitru, gr. SISRC-211M.

Theme: " Analysis and comparison of security methods in Cloud technology. "

Structure of the paper: the paper consists of the cover, the title page, the specifications, the opinion, the annotation, the introduction, chapter 1, chapter 2, chapter 3, conclusion, bibliography, annexes.

Key-words: cloud, algorithms, risks, information security, threats, host, vmware.

The purpose of the paper: comparing cloud security methods.

Objectives of the paper:

• Comparison of security methods in Clod.

• Analysis of threat assessment algorithms.

• The creation of the network from the center of the risris.

• Implementation of a secure cloud.

• Cloud efficiency analysis.

Methods applied to the elaboration of the paper: VirtualBox virtual machines.

The results obtained: A secure connection between the user and the cloud was made, countless threats that can appear to the cloud and the user were analyzed and the safest protection methods were proposed.

Cuprins

INTRODUCERE

Cloud se referă la utilizarea unor servicii și resurse informatice prin intermediul unei rețele, de obicei Internetul. Aceste servicii și resurse pot include stocarea datelor, procesarea datelor, aplicații și servicii de comunicare. Cloud computing poate oferi o serie de avantaje, cum ar fi costuri mai reduse, flexibilitate și scalabilitate, dar implică și un anumit grad de riscuri legate de securitate. Securitatea cloud este importantă deoarece datele și aplicațiile sunt stocate și procesate în afara organizației, astfel încât acestea pot fi accesate de la orice dispozitiv cu conexiune la internet. Din acest motiv, este important să se acorde atenție protejării datelor și aplicațiilor împotriva accesului neautorizat, furtului sau distrugerii. Există mai multe modalități de a asigura securitatea în cloud, inclusiv prin utilizarea criptării pentru protejarea datelor în timpul transferului și stocării, prin utilizarea autentificării și autorizării pentru a controla accesul la date și aplicații, și prin monitorizarea continuă a activităților pentru a detecta orice activitate neobișnuită sau suspectă. Este important de a acorta atenție la alegerea furnizorului de servicii cloud și de a verifica dacă acesta oferă măsuri adecvate de securitate. De asemenea, este important să înțelegi responsabilitățile tale și ale furnizorului de servicii cloud în ceea ce privește protejarea datelor și aplicațiilor, precum și să ai planuri de acțiune în cazul în care apar probleme de securitate.

Un alt aspect important al securității în cloud este managementul riscurilor. Acest lucru poate include evaluarea continuă a riscurilor potențiale și implementarea de măsuri de mitigare a riscurilor pentru a proteja datele și aplicațiile. De exemplu, poți utilizarea de backup și recuperare pentru a proteja datele în cazul în care apar probleme de securitate sau de disponibilitate. Cantități mari de putere de calcul sunt necesare nu numai pentru întreprinderile industriale comerciale, ci și în domeniile educației și divertismentului. Prin urmare, problema necesității de a crea sisteme de prelucrare a datelor economice și eficiente devine din ce în ce mai acută. În deosebi după carantina, din cauza Covid 19, carea ne-a impus să efectuăm majoritatea lucrului la distanță. Prin accest fapt având nevoie de noi resurse în cloud.

În legătură cu dezvoltarea rapidă a tehnologiilor de acces fără fir, nevoia de a localiza un complex de facilități de procesare și stocare a informațiilor direct pe teritoriul organizației a dispărut, iar lucrul la distanță cu date a devenit posibil. Acest a aparit serviciilor cloud.

Până în prezent, cloud este una dintre cele mai promițătoare domenii pentru dezvoltarea tehnologiei informației și este considerată o alternativă la modurile tradiționale de lucru cu informația. Utilizarea structurii cloud vă permite să realizați posibilitatea lucrului de la distanță cu informații și

asigură obținerea unei disponibilitati ridicate și toleranță la erori.

Datorită dezvoltării active a acestei industrii, menținerea securității în timpul stocării și transmiterii datelor este una dintre principalele probleme atunci când se lucrează cu sisteme cloud, în special în ceea ce privește informațiile care conțin secrete comerciale sau alte informații protejate.

Prin urmare, scopul acestei lucrări este analiza și compararea metodelor de securitate în tehnologia Cloud și de a alege cele mai bune metode de protecție a datelor utilizatorilor utilizate în serviciile cloud.

Pentru a atinge acest obiectiv, este necesar să atingem următoarele obiective:

1. Analiza caracteristicilor construirii de servicii cloud;
2. Exlorarea amenințărilor de securitate în cloud;
3. Analiza problemelor securității informațiilor în tehnologiile cloud;
4. Analiza comparative a metodelor existente de protecție a informațiilor atunci când lucrez cu tehnologii cloud;
5. Implemantarea în practică a politicilor de securitate în cloud.

La scrierea acestei lucrări pot apărea dificultăți din cauza lipsei accesului gratuit la informații complete despre configurația și costul serviciilor oferite de furnizori.

CONCLUZIE

În prezent, instrumentele de cloud s-au răspândit în mod activ atât în rândul organizațiilor care au nevoie de putere de calcul suplimentară, cât și în rândul oamenilor obișnuiți care doresc să simplifice procesul de procesare și stocare a datelor. Dar, odată cu creșterea numărului de utilizatori, a crescut și numărul vulnerabilităților identificate în această metodă de procesare a datelor. Pentru minimizarea acestora am indeplinit obiectivele acestei lucrări:

1. Am analizat caracteristicilor construirii de servicii cloud;
2. Am exlorat amenințările de securitate în cloud;
3. Am analizat problemele securității informațiilor în tehnologiile cloud;
4. Am analizat comparative a metodelor existente de protecție a informațiilor atunci când lucrez cu tehnologii cloud;
5. Am implemantat în practică politici de securitate în cloud.

În funcție de nevoile clienților, sunt oferite mai multe modele de implementare a tehnologiilor cloud. Cel mai sigur dintre acestea este modelul de cloud privat, în timp ce cel mai vulnerabil este modelul de cloud public. Norii sunt, de asemenea, împărțiți pe modele de servicii. Fiecare dintre ele are avantajele și dezavantajele sale și este selectat de utilizator în funcție de obiectivele urmărite. Dintre clienții individuali, modelul de servicii SaaS este cel mai răspândit. În acest moment, tot mai multe companii își oferă aplicațiile pe baza acestui model. Dar, în același timp, acest serviciu de prelucrare a informațiilor este cel mai puțin sigur.

În conformitate cu sarcinile stabilite, în această lucrare au fost luate în considerare modelele de amenințări existente în cloud computing și au fost testate posibile măsuri de îmbunătățire a securității fișierelor utilizatorilor. Metodele de autentificare și de control al accesului nu au fost luate în considerare din cauza faptului că nu sunt disponibile pentru un utilizator obișnuit.

Datorită dezvoltării rapide a infrastructurii cloud, ar trebui să ne așteptăm la apariția unor metode universale pentru asigurarea securității datelor în viitorul apropiat. Dar astăzi, nu este posibil să se evidențieze cea mai optimă metodă de protecție, deoarece trebuie aplicată o abordare individuală fiecărui tip de serviciu în conformitate cu obiectivele urmărite de clientul serviciilor cloud. Într-un final am creat un cloud provizoriu securizat, datorita masini virtuale, IaaS cere permite userilor de a menține datele în iguranță datorită evitări riscurilor fregvente la care se expune cloud.

Biblografie

1. Sen, J. Probleme de securitate și confidențialitate în cloud computing [resursă electronică]/J. Sen.
Mod acces: https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf /08.10.2022

2. Kumar, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey [Text] /R. Kumar, R. Goyal // Computer Science Review- Vol. 33. - P. 1-48.

3. Securitate și control organizațional în cloud: o abordare proactivă [Text] / K. Spanaki., Z.Gürgüç, C.Mulligan,E.Lupu// Information Technology & People

4. Dinu Ţurcanu, 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. Mod acces: https://ibn.idsi.md/sites/default/files/imag_file/JSS-1-2021_74-83_0.pdf

5. Scott, S. Securitatea eficientă necesită un control strâns asupra datelor și resurselor dumneavoastră.
Mod acces: https://cloudacademy.com/blog/aws-bastion-host-nat-instances-vpc-peering-security/

6. AWS security best practices [Electronic resource]. – Mod acces: https://aws.amazon.com/white-papers/aws-security-best-practices/-
7. Google cloud platform security best practices [Electronic resource]. – Mod acces: https://cloud.google.com/docs/enterprise/best-practices- for-enterprise-organizations
8. Cloud tip IaaS – Mod acces: https://docs.vmware.com/
9. Controlul accesului în sisteme informaționale – Mod acces: https://moodle.usm.md/pluginfile.php/234531/mod_resource/content/2/Controlul%20accesului%20in%20SI%20prez.pdf
10. Ghid securitatea in cloud – Mod acces: https://dnsc.ro/vezi/document/securitatea-in-cloud
11. Ludmila Peca, Dinu Ţurcanu. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chișinău, Publisher ,,Tehnica-UTM", 2022.
Mod acces: http://repository.utm.md/bitstream/handle/5014/20549/Computer-networks-Practical-examples-DS.pdf?sequence=1&isAllowed=y
12. Amenintari in clod – Mod acces: https://www.hqsolutions.ro/ro/suport-it-top-12-amenintari-cu-care-se-confrunta-organizatiile-cand-utilizeaza-servicii-de-tip-cloud-partea-iii/
13. Informatii privind securitatea clod - https://www.oracle.com/ro/a/ocom/docs/cloud/mission-of-the-cloud-centric-ciso-report.pdf
14. Metode de a proteja virtualizarea in cloud – Mod acces: https://www.dendrio.com/blog/5-moduri-de-a-ti-proteja-sistemele-virtualizate-din-cloud/
15. Conditii generale utilizarea conturilor – Mod acces: https://www.procreditbank.md/files/pdf/Conditii%20generale%20prestare%20servicii%20PF_%20clienti%20noi%2012.12.17.pdf
16. Ghid bune practici – Mod acces: https://stisc.gov.md/sites/default/files/ghiduri/ghid_securitatea_cibernetica_modificat.pdf

17. Autentificare cu mai multi factori – Mod acces: https://www.openvision.ro/blog/analize-it-securitate/autentificare-cu-mai-multi-factori-mfa-ce-este-si-de-ce-aveti-nevoie-de-ea/
18. Criptarea unitati bazate pe cloud – Mod acces: https://www.thefastcode.com/ro-ron/article/how-to-encrypt-your-cloud-based-drive-with-boxcryptor
19. Sisteme distribuite – Mod acces : https://staff.fmi.uvt.ro/~dana.petcu/distrib/TDS12-RO.pdf