MINISTERUL EDUCAŢIEI, CULTURII ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament:
Fiodorov Ion, conferențiar universitar, doctor în informatică

_____

„____”_____ 2021

Model de securitate cibernetică într-o companie de stat

Teză de master

Student: **Stoleru Dragoș, TIA-191M**

Conducător: **Zgureanu Aureliu, conf. univ., dr.**

Chişinău, 2021

REZUMAT

la teza de master „Model de securitate cibernetică într-o companie de stat”,

autor, Stoleru Dragoș, Chișinău, 2021

Structura tezei: teza cuprinde introducere, trei capitole, bibliografie cu 15 de referinte, este expusă pe 56 pagini text de bază.

Cuvintele-cheie: Securitate cibernetica, securitatea aplicatiei, securitatea la nivel de retea, securitatea asigurata de angajatii companiei, Sistemul Informatic Integrat Vamal, vulnerabilitati de securitate, atacatori, date criptate, date in clar, autentificare, autorizare.

Scopul lucrării constă în aducerea la cunostinta a vulnerabilitatilor actuale ale unui sistem cibernetic, analizarea si identificarea lor pe baza unui studiu de caz reprezentat de Sistemul Informatic Integrat Vamal si propunerea unei serii de implementari prezentate punctual pentru excluderea vulnerabilitatilor de securitate. Pentru a oferi o imagine de ansamblu mai clara, securitatea unei aplicatii a fost prezentata din trei puncte de vedere diferite: securitatea la nivelul aplicatiei, securitatea la nivelul retelei si securitatea asigurata de personalul companiei care utilizeaza sistemele, iar solutiile prezentate in studiul de caz au fost clasificate in acelasi mod.

Obiectivele generale:

- Studierea tipurilor de securitate cibernetica;
- Presupunerea unei implementari a platformei SIIV bazata pe date din bibliografii publice;
- Propunerea de solutii de implementare pentru vulnerabilitati si riscuri cibernetice actuale;

Metodele aplicate la elaborarea proiectului (lucrării). Pe parcursul lucrării, au fost folosite o gamă diversă de metode, precum: documentare, relatare, deducția, analiza, propuneri.

Documentarea teoretică a oferit informatii clare asupra ceea ce inseamna securitate ciberetica.

Rezultatele concrete obținute. S-au adus la cunostiinta modele actuale de securitate din trei planuri si anume: securitatea la nivelul aplicatiei, securitatea la nivelul retelei si securitatea asigurata de personalul companiei care utilizeaza sistemele. S-au propus o serie de solutii pentru a exclude vulnerabilitatile prezentate in partea de teorie a lucrarii.

Cea mai importanta etapa a lucrarii a reprezentat-o documentarea notiunilor teoretice si asimilarea lor astfel incat sa fie posibila o analiza si popunerea de solutii de implementare a securitatii asupra Sistemului Informatic Integrat Vamal.

Ultima etapă a lucrarii a reprezentat-o valorificarea informațiilor științifice acumulate la partea de documentare si analizarea lor pe Sistemul Informatic Integral Vamal si concluzionand cu solutii de evitare a breselor de securitate prdin cele trei planuri: securitatea la nivelul aplicatiei, securitatea la nivelul retelei si securitatea asigurata de personalul companiei care utilizeaza sistemele

SUMMARY

to the master's thesis " Cyber security model in a state-owned company", author Stoleru Dragos, Chişinău, 2021

Thesis structure: thesis cuprinde introducere, trei capitole, bibliografie with 15 references, este expusa pe 56 pagini text de base.

Keywords: Cyber security, application security, network level security, security provided by company employees, Integrated Customs Information System, security vulnerabilities, attackers, encrypted data, clear data, authentication, authorization.

The purpose of the study It consists in raising awareness of the current vulnerabilities of a cyber system, analyzing and identifying them based on a case study represented by the Integrated Customs Information System and proposing a series of latest technology implementations to exclude security vulnerabilities. To provide a clearer picture, the security of an application was presented from three different points of view: application-level security, network-level security, and security provided by company personnel using the systems, and the solutions presented in the case study have were classified in the same way.

General objectives:

- Studying the types of cyber security;
- Assuming an implementation of the SIIV platform based on data from public bibliographies;
- Proposing implementation solutions for current cyber vulnerabilities and risks;

Methods applied to the elaboration of the project (papers): During the work, they were used în a different range of methods documentation, reporting, deduction, analysis, proposals.

The theoretical documentation provided a clear picture about what cyber security means.

The concrete results obtained: The current security models from three levels were brought to light, namely: application-level security, network-level security and security provided by the company's staff using the systems. A number of solutions have been proposed to exclude the vulnerabilities presented in the theory part of the paper.

The most important stage of the paper was the documentation of the theoretical notions and their assimilation so that it is possible to analyze and propose solutions for implementing security on the Integrated Customs Information System.

The last stage of the paper was represented by applying the valuable technical information learned at the documentation part of the paper and security analysis on the Securitate Informatic Customs system bazed on: application level security, network level security and security provided by the staff of the company that uses the systems.

CUPRINS

INTRODUCERE

Având în vedere că fiecare dintre noi avem o viață socială în mediul online, este important ca aceasta să se supună anumitor reguli de igienă cibernetică. În cazul companiilor acest aspect este încă și mai important, întrucât este necesar să fie cât mai apărate împotriva unor eventuale atacuri cibernetice, deoarece, în caz contrar, pierderile suferite de către companii sunt mult mai mari decât în cazul persoanelor fizice.

În cazul societăților, un atac cibernetic ar conduce la pierderea datelor de ordin financiar, pierderi de informații cu caracter personal ale clienților, sau alte informații cu caracter specific al afacerilor, cum ar fi: întreruperea activității, imaginea eronată asupra societății la nivel național, scăderea imaginii pe plan național.

De ce sunt importante aceste noțiuni? De ce avem nevoie de Securitate cibernetică, ar putea fi considerată o întrebare mai mult sau mai puțin retorică. Am putea chiar, asemăna acest lucru cu nevoia de a avea o încuietoare la ușa casei noastre. Sigur că acest lucru este necesar, întrucât nu ne putem lăsa locuințele neîncuiate. Așadar, observăm că nu ne putem permite nici să ne lăsăm informațiile neprotejate din punct de vedere al unui posibil atac informatic.

Având în vedere că marea majoritate a afacerilor din zilele noatre au la bază o bază informatică, o componentă IT (un program de contabilitate în rețea, un program de depunere al declarațiilor în format online) și chiar și în cazul în care nu se folosește un program de contabilitate în rețea, tot se folosește un program prin care se depun declarații în format electronic.

Având în vedere că mai toate afacerile din ziua de astăzi au o componentă de IT care stochează şi procesează datele (la baza activităţii marii majorităţii a companiilor aflându-se o infrastructură informatică de mari sau de mici dimensiuni) iar acolo unde există o structură informatică, implicit există și un risc cibernetic. Ca atare, aproape toate afacerile din ziua de astăzi sunt supuse unor riscuri cibernetice, unor breşe de securitate informatică care pot avea repercusiuni majore.

Acest **risk assessment**, această conştientizare a riscurilor şi a nevoii de securizare este primul pas pe care îl putem pune în adoptarea unui comportament corect din punct de vedere al securităţii cibernetice. Investiţia ulterioară în soluţii de cyber security se face în funcţie de ceea ce are fiecare de protejat, respectiv evaluarea datelor protejate, a riscurilor cibernetice la care acestea pot fi expuse.

Lăsând la o parte conștiința fiecăruia în materie de protecție cibernetică, mai există și constrângeri de ordin legislativ, pe care vrem sau nu vrem trebuie să le adoptăm și să le punem în practică, așa după cum prevede Regulamentul GDPR sau Directiva NIS respective Legea nr. 362/2018.

Cum ne protejăm când vine vorba de Securitate cibernetică? Când discutăm despre securitate cibernetică, este necesar să luăm în calcul o serie de elemente necesare care nu țin cont neapărat de profilul companiei, de tipul de activitate sau de dimensiunile companiei sau de mărimea rețelei

informatice. Sunt patru mari probleme pe care trebuie să le rezolvăm pentru ne putea simți asigurați împotriva unui eventual atac cibernetic și anume:

•să conştientizăm ce date trebuiesc protejate, și acest lucru îl putem face răspunzând la întrebarea - **CE anume protejăm**;

•în al doilea rând răspundem la întrebarea CU CE program ne putem proteja (antivirus, firewall, software de back-up);

•în al treilea rând contează și personalul (oameni cu know-how) - **CU CINE protejăm**;

•procesele - **CUM protejăm**.

Din punct de vedere al **costurilor**, doar în cazul conştientizării şi al tool-uri open-source putem discuta despre gratuitate, cu menţiunea că acestea din urmă vin cu limitări precum riscul stagnării dezvoltării la moment dat. În plus, această gratuitate în cazul instrumentelor utilizate pentru protejarea datelor devine irelevantă, atât timp cât apar costuri ce ţin de exploatarea lor sau de resursele umane calificate necesare pentru configurare şi operare. Limitările tool-urilor open-source sunt compensate, într-o oarecare măsură, de cele comerciale, însă şi în acest caz trebuie să realizăm că sunt necesare cunoştinţele specialiştilor din domeniu, ele neputând fi utilizate de oricine.

Primul capitol descrie bazele teoretice și necesitatea securității informaționale, standardele și riscurile din acest domeniu.

În al doilea capitol se descrie studiul de caz al sistemului integrat vamal si principiul de lucru al sistemului, denumirile tuturor ramurilor din acest sistem.

Al treilea capitol constă în aducerea la cunostinta a vulnerabilitatilor actuale ale unui sistem cibernetic, analizarea si identificarea lor pe baza unui studiu de caz reprezentat de Sistemul Informatic Integrat Vamal si propunerea unei serii de implementari prezentate punctual pentru excluderea vulnerabilitatilor de securitate.

Astfel, În concepția de informatizare a societății este necesar a prevedea orientarea tehnologiilor informaționale și a legislației corespunzătoare în vederea creării condițiilor pentru realizarea unui compromis acceptabil intre tendința de apărare a resurselor informaționale, fapt ce poate fi însoțit de limitarea drepturilor informaționale) și dorința de a obține cit mai multe drepturi și libertăți

BIBLIOGRAFIE:

1. Accesul la componentele sistemului informatic integrat vamal
   Disponibil: https://infotva.manager.ro/articole/legislatie/accesul-la-componentele-sistemului-informatic-integrat-vamal-siiv-11875.html
2. Conectare la sistemul informatic vamal
   Disponibil: https://www.vamaromana.eu/e-customs/ncts/conectare-la-sistemul-informatic
3. Modele si protocoale criptografice
   Disponibil: http://www.cs.ubbcluj.ro/~rlupsa/works/retele/retele-cripto.pdf
4. Algoritmul de criptare RSA
   Disponibil: https://www.securitatea-informatiilor.ro/solutii-de-securitate-informatica/algoritmul-de-criptografie-rsa/
5. Centru national de raspuns la incidente de Securitate cibernetica – Ghid pentru securizarea aplicatiilor si serviciilor web
   Disponibil: https://cert.ro/vezi/document/ghid-securizare-aplicatii-web
6. Despre Open Web Application Security Project
   Disponibil: https://www.owasp.org/index.php/About_The_Open_Web _Application_Security_Project
7. Noi orientări pentru scrierea codului securizat
   Disponibil: https://opensource.com/business/14/5/new-guidelineswriting-secure-code
8. Exploatare prin injectie SQL
   Disponibil: https://www.bitdefender.ro/consumer/support/answer/21619/
9. Cele 10 riscuri majore pentru securitatea app web
   Disponibil: https://www.checkmarx.com/glossary/owasp-top-10/
10. On Security of Web Applications Dr. Sabin-Corneliu BURAGA
    Disponibil: http://revistaie.ase.ro/content/34/Buraga.pdf
11. Securitatea aplicatiilor web. Cele mai intalnite vulnerabilitati/atacuri si metode de aparare impotriva lor
    Disponibil: https://www.worldit.info/articole/securitatea-aplicatiilor-web-a-cele-mai-intalnite-vulnerabilitatiatacuri-si-metode-de-aparare-impotriva-lor/
12. Vulnerabilitatea companiilor sta in fiecare angajat
    Disponibil: https://www2.deloitte.com/ro/ro/pages/risk/articles/vulnerabilitatea-companiilor-sta-in-fiecare-angajat.html
13. Securitatea la nivelul retelei si tipuri de atacuri

Disponibil:
https://www.researchgate.net/publication/277723629_Network_Security_and_Types_of_Attacks_in_Network

14. Securitatea la nivelul retelei. Definitie si metode
    Disponibil: https://www.csoonline.com/article/3285651/what-is-network-security-definition-methods-jobs-and-salaries.html
15. Aducerea la cunostinta a securitatii
    Disponibil: https://www.mimecast.com/content/what-is-security-awareness-training/