

**MINISTERUL EDUCAȚIEI, CULTURII ȘI CERCETĂRII AL REPUBLICII
MOLDOVA**

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

**Admis la susținere
Șef de departament:
Fiodorov I. dr., conf.univ.**

„___” _____ 2021

Model de securitate al sistemului ‘1C:Enterprise’

Teză de master

Student: _____ Gribincea Dorin, SI-201M

**Conducător: _____ Beșliu Victor, dr., prof.
univ.**

Chișinău, 2022

Rezumat

Această teză de master a fost elaborată de studentul Gribincea Dorin, grupa SI-201M la tema "Model de securitate al sistemului '1C:Enterprise'". Structura tezei este alcătuită din Introducere, 3 capitole, concluzie și bibliografie.

Tematica acestei lucrări constă este actuală deoarece orice întreprindere are nevoie de un model de securitate pentru infrastructura 1C:Enterprise. Așadar, ca prototip finit al acestui studiu, se propune un model de securitate care încearcă să cuprindă cerințele de securitate ale sistemelor și aplicațiilor comerciale, punând accent pe consistența internă și externă a informațiilor. Este adaptabil și aplicabil mediului de afaceri și proceselor industriale. Restricțiile modelelor și regulile de certificare definesc categorii specifice de date și procese care formează fundamentul unei politici de integritate.

Obiectivele acestei lucrări de master au fost atinse cu succes, precum fundamentarea cunoștințelor în domeniul securității informaționale, modelul de securitate a fost creat pentru un sistem informațional care poate fi văzut ca având mai multe straturi ce reprezintă nivelurile de securitate ce înconjoară subiectul ce trebuie protejat. Fiecare nivel izolează subiectul și îl face mai dificil de accesat în alt mod decât în care a fost prevăzut.

Modelul de securitate are ca scop principal de a oferi o protecție fiabilă și rentabilă a infrastructurii 1C:Enterprise. La acest model se iau decizii cu privire la următoarele aspecte: mecanisme, mijloace și metode de protecție să utilizeze, mijloace tehnice sunt achiziționate și instalate, se realizează administrarea zi de zi, minorizarea sistemului de securitate a informațiilor în ansamblu și urmărirea și starea punctelor slabe, pregătirea inițială a personalului.

Studiind toate materiale necesare pot să demonstrez încă o dată că orice set de măsuri de securitate ar trebui să acopere toate etapele de implementare: dezvoltare, implementare, administrarea sistemului și măsuri organizatorice. În sistemele informaționale factorul uman este principala amenințare la adresa securității. Acest set de măsuri trebuie să fie rezonabil și echilibrat, nu are sens și este puțin probabil să se aloce suficiente fonduri pentru a organiza protecția, care depășește costul datelor în sine.

Conținutul acestei teze de master este alcătuit din 3 capitole bine structurate, în fiecare capitol am descris în detaliat cadrul general al protecției și securității a infrastructurii 1C, detectarea și analiza vulnerabilităților în infrastructura 1C și recomandări privind măsurile de protecție și securitate a infrastructurii 1C.

În concluzie această teză de master este un studiu amplu al securității informaționale pentru realizarea modelului de securitate, datorită acestui proiect am utilizat toate cunoștințele acumulate în ani de studii de master.

Abstract

This master's thesis was developed by student Gribincea Dorin, group SI-201M on the topic "The security model of ' 1C: Enterprise 'system". The structure of the thesis consists of Introduction, 3 chapters, conclusion and bibliography.

The topic of this paper is current because every enterprise needs a security model for the 1C: Enterprise infrastructure. Therefore, as a finished prototype of this study, a security model is proposed that seeks to encompass the security requirements of commercial systems and applications, emphasizing the internal and external consistency of the information. It is adaptable and applicable to the business environment and industrial processes. Model restrictions and certification rules define specific categories of data and processes that form the basis of an integrity policy.

The objectives of this master's thesis have been successfully achieved, such as substantiating knowledge in the field of information security, the security model was created for an information system that can be seen as having several layers representing the levels of security surrounding the subject to be protected. Each level isolates the subject and makes it more difficult to access than it was intended to be.

The main purpose of the security model is to provide reliable and cost-effective protection of the 1C: Enterprise infrastructure. This model makes decisions on the following aspects: mechanisms, means and methods of protection to use, technical means are purchased and installed, day-to-day administration, monitoring of the overall information security system and monitoring and status of weaknesses , initial staff training.

By studying all the necessary materials I can demonstrate once again that any set of security measures should cover all stages of implementation: development, implementation, system administration and organizational measures. In information systems, the human factor is the main security threat. This set of measures must be reasonable and balanced, does not make sense and it is unlikely that sufficient funds will be allocated to organize the protection, which exceeds the cost of the data itself.

The content of this master's thesis consists of 3 well-structured chapters, in each chapter we have described in detail the general framework of protection and security of 1C infrastructure, detection and analysis of vulnerabilities in 1C infrastructure and recommendations on measures of protection and neglect of 1C infrastructure.

In conclusion, this master's thesis is an extensive study of information security for the realization of the security model, thanks to this project we used all the knowledge gained in years of master's studies.

CUPRINS

Introducere	8
1. Cadrul general al protecției și securității a infrastructurii 1C	9
1.1 Arhitectura platformei de întreprindere 1C:Enterprise.....	10
1.2 Componente de securitate ale infrastructurii 1C	16
1.3 Securitatea platformei 1C.....	19
1.4 Securitatea infrastructurii IT.....	21
1.5 Securitatea aplicațiilor web 1C.....	23
1.6 Securitatea ale serverului 1C-web.....	27
2. Detectarea și analiza vulnerabilităților în infrastructura 1C	29
2.1 Analiza vulnerabilităților în infrastructura 1C	30
2.2 Clasificarea vulnerabilităților în infrastructura 1C.....	32
2.3 Detectarea vulnerabilităților a infrastructurii 1C.....	35
2.4 Evaluarea vulnerabilităților a sistemului 1C	36
3. Recomandări privind măsurile de protecție și de securitate a infrastructurii 1C	39
3.1 Proiectarea securizată a infrastructurii 1C.....	40
3.2 Configurarea securizată a infrastructurii 1C.....	42
3.3 Controlul accesului, autentificarea și diferențierea corectă a drepturilor utilizatorilor	46
3.4 Criptarea datelor în infrastructura 1C.....	49
3.5 Backup și metode de recuperare a datelor din infrastructura 1C.....	52
Concluzie:	60
Bibliografie:	61

Introducere

În prezent problemele de securitate a informațiilor sunt în mod constant agravate de pătrunderea mijloacelor tehnice de prelucrare și transmitere a datelor în toate sferile societății, această problemă este deosebit de acută în domeniul sistemelor de contabilitate financiară.

Orice organizație are nevoie de protecție împotriva amenințărilor externe și interne, cum ar fi: pătrunderea unui virus informatic, defecțiunea echipamentului, ștergerea accidentală sau deliberată a informațiilor valoroase. Fiecare dintre pericolele enumerate este capabil să oprească activitatea companiei pentru o perioadă nedeterminată, ceea ce va atrage după sine pierderea clienților, neîndeplinirea obligațiilor și pierderea de profit. În plus, restabilirea capacității de lucru necesită adesea fonduri semnificative, în plus, instantaneu.

Pentru a asigura îndeplinirea tuturor acestor sarcini, este necesară construirea unei infrastructuri IT de înaltă calitate, care este un complex de sisteme interconectate, inclusiv produse software, politici de securitate a informațiilor, servicii de rețea și director, un sistem de backup și stocare a informațiilor, monitorizare și management și altele.

Modelul de securitate reprezintă o modalitate de formalizare a noțiunii de integritate a informației în contextul sistemelor de securitate informaționale. Modelul încearcă să cuprindă cerințele de securitate ale sistemelor și aplicațiilor comerciale, punând accent pe consistența internă și externă a informațiilor. Este adaptabil și aplicabil mediului de afaceri și proceselor industriale. Restricțiunile modelelor și regulile de certificare definesc categorii specifice de date și procese care formează fundamentul unei politici de integritate.

Modelul de securitate pentru un sistem informațional poate fi văzut ca având mai multe straturi ce reprezintă nivelurile de securitate ce înconjoară subiectul ce trebuie protejat. Fiecare nivel izolează subiectul și îl face mai dificil de accesat în alt mod decât în care a fost prevăzut.

Modelul de securitate are ca scop principal de a oferi o protecție fiabilă și rentabilă a infrastructurii IC:Enterprise. La acest model se iau decizii cu privire la următoarele aspecte: mecanisme, mijloace și metode de protecție să utilizeze, mijloace tehnice sunt achiziționate și instalate, se realizează administrarea zi de zi, monitorizarea sistemului de securitate a informațiilor în ansamblu și urmărirea și starea punctelor slabe, pregătirea inițială a personalului.

În sistemul IC:Enterprise, factorul uman este principala amenințare la adresa securității. Acest set de măsuri trebuie să fie rezonabil și echilibrat, deci nu are sens și este puțin probabil să se aloce suficiente fonduri pentru a organiza protecția, care depășește costul datelor în sine.

Într-o revizuire generală este imposibil să indicăm toate aspectele legate de securitate în infrastructura IC, dar am indicat toate măsurile de protecție care sunt actuale până în prezent

Bibliografie

1. Model de securitate , [citat 12.09.2021]. Disponibil: habr.com/ru/post/467269
2. Arhitectura platformei 1C: Enterprise, [citat 15.09.2021]. Disponibil: <https://v8.1c.ru/platforma/obzor-arkhitektury-platformy>
3. Platforma mobila 1C: Enterprise , [citat 20.09.2021]. Disponibil: <https://v8.1c.ru/platforma>
4. Construirea unei infrastructuri IT , [citat 23.09.2021]. Disponibil: <https://www.ibm.com/ru-ru/topics/infrastructure>
5. Schema infrastructurii a sistemului 1C:Enterprise , [citat 25.09.2021]. Disponibil: <https://www.ibm.com/ru-ru/topics/infrastructure>
6. Securitatea platformei 1C , [citat 28.09.2021]. Disponibil: <https://efsol.ru/articles/information-security-1c>
7. Securitatea infrastructurii IT , [citat 02.10.2021]. Disponibil: <https://acti.ru/resheniya-i-uslugi/informatcionnaia-bezopasnost/bezopasnost-it-infrastruktury>
8. Schema de conectare prin HTTP/HTTPS , [citat 2021]. Disponibil: <https://help-ru.tilda.cc>
9. Schema atacurilor asupra unei aplicații web , [citat 05.10.2021]. Disponibil: <https://v8.1c.ru>
10. Schema de conectare a clientului web 1C la server , [citat 07.10.2021]. Disponibil: <https://v8.1c.ru>
11. Schema de conectare a clientului web la router , [citat 08.10.2021]. Disponibil: <https://efsol.ru/articles/web-1s-secure.html>
12. Parametri și valorile pentru un server 1C , [citat 10.10.2021]. Disponibil: <https://infostart.ru/1c/articles/1119524>
13. Analiza vulnerabilităților în infrastructura 1C , [citat 12.10.2021]. Disponibil: <https://itglobal.com/ru-ru/company/glossary/analiz-uyazvimostej>
14. Securitatea aplicațiilor web 1C , [citat 15.10.2021]. Disponibil: <https://www.1c-bitrix.ru/products/cms/security>
15. Clasificarea vulnerabilităților , [citat 17.10.2021]. Disponibil: <https://studfile.net/preview>
16. Detectarea vulnerabilităților , [citat 18.10.2021]. Disponibil: <https://tirupati-tour-packages.com/ro>
17. Procesul de testare, analiză, evaluare și remediere , [citat 23.10.2021]. Disponibil: <https://www.laboratuar.com/ro/testler/hata-analiz-testleri>
18. Evaluarea vulnerabilităților a sistemului 1C , [citat 2021]. Disponibil: <https://www.researchgate.net/publicatio>
19. Tipuri de protecție a infrastructurii IT , [citat 25.10.2021]. Disponibil: <https://acti.ru/resheniya-i-uslugi/informatcionnaia-bezopasnost/bezopasnost-it-infrastruktury>
20. Proiectarea securizată a infrastructurii , [citat 28.10.2021]. Disponibil: <https://www.cisco.com>.

21. Configurarea securizată a infrastructurii 1C , [citat 30.10.2021]. Disponibil:<https://1c-dn.com>
22. Controlul accesului , [citat 01.11.2021]. Disponibil:<https://is1c.ru>
23. Restricții de acces, [citat 05.11.2021]. Disponibil: <https://programmist1s.ru/nastroyka-rls-ogranichenie-dostupa-na-urovne-zapisey-1s>
24. Rolurile pentru administrarea obiectelor , [citat 07.11.2021]. Disponibil: <https://wiseadvice-it.ru/o-kompanii/blog/articles/ogranichenie-prav-na-urovne-zapisi-1s-rls>
25. Criptarea datelor în timpul transmiterii între serverul de aplicații și MS SQL Server , [citat 08.11.2021]. Disponibil: <https://appcube.ru/ro>.
26. Model de criptare a datelor în infrastructura 1C , [citat 10.11.2021]. Disponibil: <https://appcube.ru/ro/1s-slishkom-slozhnyi>
27. Backup și metode de recuperare , [citat 12.11.2021]. Disponibil:<https://efsol.ru/articles/cloud-services.html>
28. Schimbul de date cu ajutorul serviciilor cloud , [citat 14.11.2021]. Disponibil:https://1c-dn.com/1c_enterprise
29. Scenarii de utilizare a tehnologiilor cloud 1C: Enterprise , [citat 15.11.2021]. Disponibil:https://1c-dn.com/1c_enterprise/cloud
30. Scenariul de utilizare a cloud-ului privat 1C , [citat 17.11.2021]. Disponibil:https://1c-dn.com/1c_enterprise/private
31. Scenariul de utilizare a cloud-ului corporativ 1C , [citat 18.11.2021]. Disponibil:https://1c-dn.com/1c_enterprise/corporate
32. Scenariu de utilizare a cloud-ului community 1C , [citat 25.11.2021]. Disponibil:https://1c-dn.com/1c_enterprise/community
33. Scenariu de utilizare a cloud-ului privat 1C , [citat 28.11.2021]. Disponibil: https://1c-dn.com/1c_enterprise/public