UNIVERSITATEA TEHNICĂ A MOLDOVEI

PROIECTAREA ŞI IMPLEMENTAREA MODELULUI DE SECURITATE ÎN CADRUL CENTRELOR DE REACTIE LA INCIDENTE CIBERNETICE

Masterand:
Victor GOJA

Conducător:
conf. univ., dr. Rodica BULAI

Chişinău – 2020

Ministerul Educației Culturii si Cercetării al Republicii Moldova

Universitatea [illegible] a Moldovei

FACULTATEA Calculatoare, Informatică şi Microelectronică

Departamentullngineria software şi Automatică

Admis la susținere

Şef departament: conf. univ.,dr. Ion FIODOROV

„24" decembrie 2019

PROIECTAREA SI IMPLEMENTAREA MODELULUI DE SECURITATE IN CADRUL CENTRELOR DE REACTIE LA INCIDENTE CIBERNETICE

Teză de master în

Securitate informațională

Masterand: Victor GOJA

Conducător: lector univ. Rodica BULAI

Chişinău 2020

ADNOTARE

la teza de mastercu tema ”Proiectarea şi implementarea modelului de securitate în cadrul centrelor de răspuns la incidente cibernetice” a masterandului Victor GOJA

În teză sunt prezentate şi analizate date teoretice privind importanţa şi metodele de implementare a securității informaţionale şi cibernetice în mediul infrastructurilor critice de diferitenivele şi apartenenţe.

De asemenea, este caracterizat evoluţia riscurilor şi ameninţărilor cibernetice în spaţiul informaţional.

Se impune proiectarea unui Centru de reacţie la securitate cibernetică, pentru Ministerul Apărării şi structurile aferente acestuia, apt să detecteze şi să răspundă la incidentele cibernetice prin desfăşurarea activităților de cercetare, instruire și răspuns la incidente în domeniul apărării cibernetice.Studiile au demonstrat necesitatea implementării unei astfel de infrastructuri critice la nivel naţional şi guvernamental.

Teza de master cuprinde introducere, trei capitole, concluzii, bibliografie și referințe. Volumul lucrării este de 70 de pagini text de bază, 33 de tabele şi 10 figuri.

În teză au fost utilizate cuvinte-cheie, cum ar fi: securitate cibernetică, securitate informațională, vulnerabilitate, risc, ameninţări, testare, instrument, proces, sistem, resurse, protejare, aplicații, software, politici.

ANNOTATION

at master’s thesistitled as “Designing and implementing framework of the security within cyber incident response centers” master’s student Victor GOJA

In the thesis are presented and analyzed theoretical referenceon the importance and methods of implementing information and cyber security in the environment of critical infrastructures of different levels and memberships.Also is described the evolution of risks and cyber threats in the information space.

It `s being suggested to design a Cyber Security Reaction Center, for the Ministry of Defense and structures related to it, capable of detecting and responding to cyber incidents by conducting research, training and incident response activities in the cyber defense field. Studies have shown the need to implement such critical infrastructures at national and governmental level.

The master's thesis includes an introduction, three chapters, conclusions, bibliography and references. The volume of the paper is 70 pages of basic text, 33 tables and 10 figures.

The key words used in the thesis, were: cyber security, information security, vulnerability, risk, threats, testing, instrument, process, system, resources, protection, applications, software, policies.

CUPRINS

ÎNTODUCERE

Apărarea cibernetică este un domeniu relativ nou de preocupări pentru guverne și state independente. Răspândirea tehnologiilor și costul accesibil al instrumentelor și echipamentelor de comunicaţii şi informatică au transformat un număr impresionant de oameni în potențiali contrabandiști de informații. De când a apărut o piață în care informațiile sustrase pot fi tranzacționate, vânzările de informații au devenit o afacere profitabilă la nivel mondial.

Atacurile cibernetice sunt îndreptate de obicei împotriva rețelelor dislocate şi mai puțin frecvente decât cele care vizează rețelele de infrastructură. Cu toate acestea, consecințele acestui tip de scurgeri de informații pot fi drastic severe pentru structurile de forţă a Republici Moldova.

Securitatea informațiilor a devenit o problemă mult mai importantă pentru majoritatea instituţiilor din întreaga lume. Aceste instituţii au înțeles, de asemenea, că o mai bună securitate nu poate fi obținută doar instalând un alt dispozitiv hardware de securitate precum un firewall sau un sistem de detectare a intruziunilor. Chiar și cel mai sigur sistem nu va oferi siguranță dacă din timp nu se va acţiona rapid în adresa incidentului.

Un centru de răspuns la incidente de securitate cibernetică (CRIC) este o entitate organizatorică concretă (adică, unul sau mai mulți membri) care are atribuția de a coordona și de a susține răspunsul la un eveniment sau incident de securitate a reţelelor. CRIC-urile pot fi create pentru state sau economii naționale, guverne, organizații comerciale, instituții de învățământ și chiar entități non-profit. Scopul unui CRIC este de a reduce la minimum și de a controla daunele rezultate din incidente, de a oferi îndrumări eficiente pentru activitățile de răspuns și recuperare și de a lucra pentru a preveni incidentele viitoare.

În condițiile gestionării informației ce necesită protecție și securitate sporită, modul de gestionare și control al externalizării serviciilor este un factor determinant în organizarea activităților aferente a tehnologiilor informaționale. Din această perspectivă, lipsa unei abordări manageriale a problemelor de securitate cibernetice reprezintă un factor de risc pentru asigurarea confidențialității informației și a securității componentelor sistemului informațional al instituțiilor.

Compromiterea securității informației poate afecta capacitatea de a oferi servicii, poate conduce la fraude sau distrugerea datelor, neonorarea clauzelor contractuale, divulgarea secretelor de stat și a informațiilor confidențiale, afectarea credibilității instituțiilor publice și a organizațiilor.

CONCLUZII

Apărarea cibernetică constituie o parte semnificativă din cadrul proceselor de gestionare a informaţiilor şi apărare naţională.Studiul a confirmat că gestionarea securității informațiilor şi managementul ameninţărilor cibernetice este o sarcină națională și nu o sarcină a instituţională. Lucrarea a arătat că securitatea obiectului, echipamentului nu este suficientă, trebuie să existe anumite centre de securitate pentru a face față provocări, riscurilor şi ameninţărilor invocate.

Literatura de cercetare şi analiză elucidează aceleași idei, există mai multe modele și cadre care vor ajuta organizațiile în gestionarea securității informațiilor și a riscurilor. Managementul nu este singurul element în securitatea informațiilor, comportamentul și cunoștințele despre riscuri sunt, de asemenea, necesare, ultimul urmează a fi efectuată de către specialiștii de securitate cibernetică din organizațiile care dețin aceste cunoştinţe.

Educația este necesară întregii organizații și nu doar specialiștii de securitate. Erorile umane reprezintă cel mai mare risc pentru securitatea informațiilor.Conştientizarea riscurilor de securitate a informațiilor la nivelul fiecărei organizații atrage atenția asupra securității informațiilor și poate fi mult mai eficientă decât formarea formală, care este foarte costisitoare.

În lucrarea mea am constatat că reacţia la incidente este unul dintre cei mai importanți factori în managementul securității. În ultimii ani au loc tot mai multe atacuri asupra utilizatorilor instituţiilor de profit. Acești utilizatori nu au capacitatea de a obține toate utilitățile pentru a stabili un mediu de gestionare a securității informațiilor și de gestionare a riscurilor. Infracțiunile organizate s-au văzut posibile prin obținerea controlului la computer și efectuarea de înregistrări atunci când utilizatorul este conectat în contul personal.

Prin urmare, dacă se va înţelege importanţa apărării cibernetice, atunci abordarea actuală a managementului securității trebuie îmbunătățită - așa cum a afirmat (Frangopoulos, 2007), este necorespunzător utilizarea principiilor secolului al XIX-lea pentru a gestiona problemele secolului XXI.

BIBLIOGRAFIE

1. Hotărârea Guvernului Republicii Moldova cu privire la aprobarea Cerințelor minime obligatorii de securitate cibernetică: nr.201 din 28.03.2017. În *Monitorul Oficial al Republicii Moldova*. 2017, nr. 109-118, art. nr.: 277;

2. ISACA și RSA Conference, *Starea securității cibernetice: Implicații pentru 2015*, [accesat 18.11.2019]. Disponibil: http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

3. SM EN ISO/IEC 27001:2017, Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Cerinţe – Aprobat: 29.08.2017. – Chișinău: INSM, 2017. – 33 p. – Nepubl. Localizare: INSM (Chișinău);

4. https://www.cert.ro/pagini/ecsi-page[accesat pe 10.11.2019];

5. BROȘURA PROTECTIA INFRASTRUCTURILOR CRITICE [accesat pe 12.10.2019]Disponibil:https://www.sri.ro/upload/.pdf

6.https://doi.org/10.6028/NIST.CSWP.04162018 [accesat pe 5.11.2019]

7. Framework for Improving Critical Infrastructure Cyber security, Version 1.1, National Institute of Standards and Technology April, 2018

8. ISMS Implementation Guide v1.1 ATSEC information security corporation

9. Sistemul de management al securităţii informaţionale ISO/IEC 27001:2013. Algoritmul de implementare

10. http://en.wikipedia.org/wiki/SWOT_analysis [accesat pe 16.11.2019]

11.http://en.wikipedia.org/wiki/PEST_analysis [accesat pe 16.11.2019]

12. O abordare pas cu pas a modului de creare a unui CSIRT Produs final WP2006/5.1 (CERT-D1/D2)

13. Ghid Amenințări generice la adresa securității cibernetice CERT.RO

14. CELE MAI FRECVENTE AMENINŢĂRI CIBERNETICE ALE ANULUI 2019 [accesat pe 12.12.2019]Disponibil:https://stisc.gov.md/ro/content/

15. ENISA Threat Landscape 2012,

16. https://cert.ro/vezi/document/raport-alerte-primite-cert-ro-2013 [accesat pe 20.11.2019]

17. Studii de strategie și politici - SPOS 2017 - nr. 4 Institutul European din Romania.

18.Cybersecurity Cyber Crime Statistics Facts Trends [accesat pe 12.12.2019]Disponibil:https://www.comparitech.com/vpn/
/#Headline_cyber_crime_statistics_for_2018-2019

19. Insurance Information Institutehttps://www.iii.org/table-archive, [accesat pe 27.11.2019]

20. IC3 2018 Internet crime report

21. https://www.fm-magazine.com/news/2019/may/cybercrime-costs-201920981. [accesat pe 03.12.2019]

22. Ninth Annual Cost Of Cybercrime Study, ACCENTURY SECURITY.

23. EVOLUȚIA AMENINȚĂRILOR ÎN SPAȚIUL CIBERNETIC ROMÂNESC ÎN ANUL 2018

24. Cyber Security Awareness Campaigns: Why do they fail to change behavior?

25. Global Campaign to Raise Cyber security Awareness [accesat pe 08.12.2019]Disponibil:https://www.thegfce.com/initiatives/.

26. MANAGEMENTUL VULNERABILITĂŢILOR ŞI EVALUAREA RISCURILOR ÎN DOMENIUL SECURITĂŢII INFORMATICE [accesat pe 9.12.2019] Disponibil: https://www.todaysoftmag.ro/article/2357/

27. http://www.cert.org/csirts/services.html [accesat pe 5.11.2019]

28. https://safeatlast.co/blog/cybercrime-statistics/#gref