Universitatea Tehnică a Moldovei

MODELE DE ASIGURARE A SECURITĂȚII ÎN CADRUL MINISTERULUI AFACERILOR INTERNE

Masterand:

Moghilda (Mitev) Constantin

Conducător:

lector universitar Putere Alexandru

Chişinău 2020

Ministerul Educaţiei, Culturii şi Cercetării
Universitatea Tehnică a Moldovei
Facultatea Calculatoare Informatică şi Microelectronică
Departamentul Ingineria Software şi Automatică

Admis la susţinere
Şef departament:
dr.conf.univ. Ion Fiodorov.
„27" decembrie 2019

MODELE DE ASIGURARE A SECURITĂȚII ÎN CADRUL MINISTERULUI AFACERILOR INTERNE

Teză de master în Securitate Informațională

Masterand: (Moghilda Constantin)
Conducător (Putere Alexandru)

Chişinău 2020

ADNOTARE

Prezenta lucrare cu tema: **"Modele de asigurare a securității în cadrul Ministerului Afacerilor Interne"** are menirea de a prezenta date cu privire la analiza standardelor și metodologiilor de securitate utilizate la elaborarea modelelor de asigurare a securității specifice Ministerului Afacerilor Interne. Prin studiul de faţă tindem să contribuim la micşorarea numărului de incidente de securitate printr-un cadru eficient de management al securității informației.

Teza de master este structurată în: întroducere, trei capitole, concluzie şi referinţe biografice și anexe.

Capitolul I este întitulat **Analiza modelelor de securitate informațională**. Este compus din trei puncte: 1) Conceptul de management al securității informației, 2) Metodologii de management al riscurilor la adresa securităţii informaţiilor și 3) Cadrul de management al securității informației în Republica Moldova.

Capitolul II este întitulat **Cadrul de management pentru arhitectura tic şi securitatea informației a MAI** și abordează: 1) Cadrul de management pentru arhitectura TIC a MAI și 2) Cadrul instituțional de management al securității informației pentru MAI.

Capitolul III este întitulat **Modele de asigurare a securității informaționale în cadrul MAI** în care sunt propuse următoarele modele de securitate: 1) Modelul privind gestionarea incidentelor de securitate a informației în cadrul MAI, 2) Modelul privind analiza și evaluarea riscurilor de securitate a informației și 3) Model tipizat pentru achiziția/dezvoltarea de sisteme informatice a MAI.

ANNOTATION

The present paper with the theme: **"Models of security assurance within the Ministry of Internal Affairs"** aims to present data on the analysis of security standards and methodologies used in the elaboration of the models of security assurance specific to the Ministry of Internal Affairs. Through this study we tend to contribute to reducing the number of security incidents through an efficient information security management framework.

The master's thesis is structured in: introduction, three chapters, conclusion and biographical references and annexes.

Chapter I is entitled **Analysis of Information Security Models**. It is composed of three points: 1) The concept of information security management, 2) Risk management methodologies for information security and 3) Information security management framework in the Republic of Moldova.

Chapter II is entitled **Management framework for ICT architecture and information security of the Ministry of Internal Affairs** and addresses: 1) Management framework for ICT architecture of the Ministry of Interior and 2) Institutional framework for information security management for the Ministry of Interior.

Chapter III is entitled **Information security assurance models within the Ministry of Internal Affairs**, in which the following security models are proposed: 1) Information security incident management model within the MIA, 2) Information security risk analysis and evaluation model, and 3) Typical model for the acquisition / development of information systems of the MIA.

CUPRINS

INTRODUCERE

Pe fiecare dintre palierele sociale, în fiecare dintre activităţile noastre zilnice operăm cu informaţii, informaţii al cărui nivel de sensibilitate variază în funcţie de prejudiciul pe care îl poate provoca compromiterea respectivei informaţii asupra individului sau organizaţiei căreia îi aparţine.

Organizaţiile, indiferent de tipul acestora, au început, tot mai mult, să conştientizeze rolul esenţial al informaţiilor în îndeplinirea obiectivelor propuse. Tendinţa de globalizare, internaţionalizare şi mondializarea crescândă a economiei impune un schimb permanent de informaţii cu alte organizaţii şi agenţii, în scopul obţinerii cunoştinţelor manageriale necesare asigurării competitivităţii şi eficienţei.

Desigur, că creşterea importanţei acestei resurse a condus la escaladarea proporţională a potenţialului de ameninţare la adresa acesteia, fapt favorizat şi de vulnerabilităţile pe care le prezintă sistemele prin intermediul cărora se gestionează informaţiile.

În vederea stabilirii unor măsuri coerente, eficiente şi eficace de protecţie a informaţiilor, managementul securităţii informaţiilor a devenit parte integrantă a managementului organizaţiilor, indiferent dacă ne referim la organizaţii guvernamentale, private sau la organizaţii internaţionale.

În acest sens, nivelul de securitate care trebuie vizat pentru informaţii trebuie să fie în deplină corespondenţă cu valoarea informaţiilor şi cu prejudiciile pe care le poate genera utilizarea necorespunzătoare a acestora – dezvăluire, degradare sau lipsa disponibilităţii.

Totodată, măsurile de securitate trebuie să ţină cont de vulnerabilităţile mediului operaţional şi de climatul de ameninţare, care justifică aplicarea unui complex de măsuri. Acest fapt demonstrează că costurile aferente asigurării protecţiei împotriva ameninţărilor la adresa informaţiilor cresc, odată cu creşterea ameninţărilor şi a vulnerabilităţilor, de aceea, și necesită o justificare argumentată.

Un Sistem de Management al Securității Informației reprezintă un sistem de management bazat pe o abordare a riscurilor la care organizația este expusă și are drept scop de a stabili, implementa, opera, monitoriza, menține, revizui și îmbunătăți securitatea informației.

Analiza riscului la adresa securităţii informaţilor este un instrument puternic pe care managerii îl au la îndemână în procesul de adoptare a deciziilor cu privire la implementarea

unor sisteme eficiente de management al informaţiilor şi, în ultimă instanţă, în îndeplinirea misiunii organizaţiei. Ca parte a procesului de management al riscului, analiza riscului reprezintă implementarea sistematică a metodelor, tehnicilor şi practicilor de management pentru evaluarea contextului, identificarea şi analiza riscurilor, găsirea variantelor de răspuns care maximizează impactul pozitiv si minimizează impactul negativ al acestora, tratarea, monitorizarea şi comunicarea riscurilor la adresa securităţii informaţiilor şi a sistemelor prin intermediul cărora acestea sunt procesate, stocate sau transmise. Natura fluidă a mediului tehnologic impune, totodată, necesitatea de a revizui rezultatele analizei riscului la adresa securităţii informaţiilor, prin reluarea periodică a acestui proces.

Problema cercetării În contextul preocupărilor legate de protecția informației și a sistemelor TIC, cadrul intern stabilit pentru managementul securității informației a devenit o prioritate actuală prin aplicarea acestuia la nivel de MAI.

Scopul cercetării: Studierea metodelor de protecție a informației existente la nivel internațional și național prin elaborarea modelelor specifice Ministerului Afacerilor Interne.

Obiectul cercetării: Pentru performanța instituțională a MAI privind protejarea informației și gestiunii riscurilor asociate TIC, abordarea MAI să fie focusată pe implementarea cadrului de management al securității informației propuse.

CONCLUZII

Cadrul de management TIC și Securitatea informației al MAI a fost îmbunătățit în măsură importantă, nu și suficientă. Rezultate și beneficii cheie ce pot fi menționate:

- MAI are aprobate politici formale ce stabilesc consolidarea și centralizarea managementului TIC în cadrul instituției. Acest fapt oferă avantaje incontestabile din punct de vedere al alinierii TIC la necesitățile strategice ale MAI și investirea inteligentă în TIC;
- Sunt stabilite și aprobate formal reglementări cheie pe procesele de bază aferente TIC: managementul serviciilor TIC (focusat pe producerea și operarea serviciilor TIC calitative) și managementul securității informației (focusat pe conștientizarea și gestiunea riscurilor asociate TIC și securității informației);
- Sunt stabilite cerințe standard pentru securitatea informației și pentru sistemele informatice ale MAI. Acestea sunt aliniate atât la practicile bune, cât și la legislația aplicabilă, inclusiv pe domeniul protecției datelor personale;

Deficiențe aferente cadrului de management TIC al MAI ce persistă la data curentă:

- Politicile și reglementările aferente TIC, deși sunt aprobate, sunt insuficient aplicate și urmate de către toate instituțiile MAI. În continuare există o parte importantă a bugetelor TIC consumată distribuit și fără coordonare centralizată;
- Organigrama MAI pentru management TIC nu este pe deplin implementată. Nu sunt organizate funcții de coordonatori TIC în toate instituțiile subordonate MAI, ocupate de persoane cu pregătirea profesională potrivită. Acest fapt creează importante impedimente la colaborarea între STI, în calitate de subdiviziune TIC specializată a MAI și restul instituțiilor subordonate MAI, în calitate de beneficiari de servicii TIC centralizate și participanți la arhitectura TIC de scară largă a MAI;
- STI, în calitate de subdiviziune TIC specializată a MAI, este în proces de reorganizare și transformare. Acest fapt afectează progresul implementării practicelor bune pentru modelul de operare a serviciilor TIC prestate de STI. Persistă în continuare insuficiența oamenilor calificați.

BIBLIOGRAFIE

1. ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT, [citat 2019-09-15]. Disponibil pe Internet: https://www.iso.org/isoiec-27001-information-security.html
2. Rodica Bulai, Dumitru Ciorbă, Rostislav Călin, Andrei Poștaru, *Methodology and algorithm of information security risk management for local infrastructure*, Central and Eastern European e|Dem and e|Gov Days 2017 Budapest, Hungary, 3-4 mai 2017.
3. ISO/IEC 27005:2011. Информационная технология - Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности, [citat 2019-09-17]. Disponibil pe Internet: https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf
4. S. Yevseiev , O. Shmatko , N. Romashchenko, Methods of information systems protection, [citat 2019-11-15]. Disponibil pe Internet: https://CRAMM-Methodology-crosscutting-approach-to-risk-assessment_fig2_334314954
5. Henry Nnoli , Dale Lindskog , Pavol Zavarsky , Shaun Aghili , Ron Ruhl, The Governance of Corporate Forensics using COBIT, NIST and Increased Automated Forensic Approaches, [citat 2019-10-25]. Disponibil pe Internet: https://259647347_The_Governance_of_Corporate_Forensics_using_COBIT_NIST_and_Increased_Automated_Forensic_Approaches
6. Guide for Conducting Risk Assessments. National Institute of Standards and Technology, [citat 2019-10-26]. Disponibil pe Internet: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
7. Programul național de securitate cibernetică al Republicii Moldova pentru anii 2016 – 2020, aprobat prin Hotărîrea Guvernului nr. 811 din 29 octombrie 2015.
8. Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărîrea Guvernului nr. 201 din 28 martie 2017.
9. O R D I N nr.247 Cu privire la aplicarea practicilor de protecție a datelor cu caracter personal în cadrul implementării serviciilor de Tehnologia Informației și Comunicațiilor în cadrul MAI din 23 august 2016, mun. Chișinău.
10. O R D I N nr.243 Privind Sistemul de management al serviciilor de Tehnologia Informației și Comunicațiilor în cadrul MAI din 18 august 2017, mun. Chișinău.
11. O R D I N nr.244 Privind Sistemul de management al securității informației în cadrul MAI din 18 august 2018, mun. Chișinău.
12. O R D I N nr.374 Privind aprobarea procedurilor de raportare a incidentelor, analiza și evaluarea riscurilor de securitate a informației în cadrul MAI din 12 decembrie 2019, mun. Chișinău.
13. Strategia națională de ordine și securitate publică pentru anii 2017-2020 și a Planului de acțiuni privind implementarea acesteia (HG nr. 354 din 31.05.2017).
14. Strategia de dezvoltare a Poliției pentru anii 2016-2020 și a Planului de acțiuni privind implementarea acesteia (HG nr. 587 din 12.05.2016).