MINISTERUL EDUCAŢIEI, CULTURII ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software şi Automatică

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

„____”_____2021

Asigurarea securităţii fluxului informaţional al operaţiunilor unei companii

Teză de master

Student: **Arpentin Maria, TIA-191M**

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

Chişinău,2021

ADNOTARE

Arpentin Maria. Asigurarea securităţii fluxului informaţional al operaţiunilor unei companii.

Chişinău,2021

Structura tezei: Lucrarea conţine adnotări în limba română şi engleză, cuprins, introducere, trei capitol, concluzii, bibliografie şi 45 pagini de text de bază.

Cuvinte-cheie: Securitate informaţională, informaţii sensibile, informaţii confidenţiale, ameninţări, riscuri, fraude, vulnerabilităţi, principia de Securitate, inginerie social.

Domeniul de studii: securitate informaţională

Scopul lucrării: studierea metodelor de protecţie a informaţiei şi a sistemelor informaţionale care o prelucrează, contra accesului neautorizat, divulgării, indisponibilităţii, modificării sau distrugerii.

Obiectivele lucrării: elaborarea de ghiduri ca parte componentă a programului de securitate a companiei, care ajută la protejarea confidenţialităţii informaţiilor, la asigurarea cerinţelor legale referitoare la securitatea datelor, protejarea datelor personale ale clienţilor şi protejarea sistemelor informaţionale ale companiei, în care are loc prelucrarea şi stocarea informaţiilor şi datelor.

Valoarea teoretică a lucrării: sunt descrise conceptele generale ce ţin de securitatea informaţiilor, ameninţări, vulnerabilităţi şi riscuri asociate, principii de securitate şi managementul acestora.

Valoarea aplicativă a lucrării: ca rezultat al cercetării teoretice, au fost elaborate două ghiduri privind manipularea informaţiilor confidenţiale şi evitarea trucurilor de inginerie socială. De asemenea a fost elaborat un ghid pentru angajaţii companii, de folosire a platformei de semnare a documentelor electronice Orange Sign. Participarea în revizuirea procedurii de semnare electronica a documentelor utilizînd serviciul mSign, şi anume clasificarea tipurilor de documente care sunt eligibile pentru semnarea prin intermediul portalului mSign.

ANNOTATION

Arpentin Maria. Ensuring the security of information flow of a company's operations.

Chişinău,2021

Thesis structure: the thesis contains annotations in Romanian and English, table of contents, introduction, 3 chapters, conclusions, bibliography, 45 pages of text.

Keywords: informational security, sensitive information, confidential information, threats, risks, fraud, vulnerabilities, security principles, social engineering.

Study domain: informational security.

Scope: study of methods of data protection and protection of information systems, which processes it, against unauthorized access, disclosure, unavailability, modification or destruction.

Objectives: elaboration of guides as part of company's security program, which helps protect information confidentiality, ensure legal requirements for data security, protect the customers personal data and protect the company's information systems, where the processing and storage of information and data takes place.

Theoretical value of the thesis: was described the general concepts related to information security, threats, vulnerabilities and associated risks, security principles and their management.

Practical value of the thesis: as a result of the theoretical research, two guidelines have been developed about handling of confidential information and the avoidance of social engineering. Also has been developed a guide for company's employees, to use the platform for signing electronic documents, Orange Sign. Participation in the review of the electronic document signing procedure using the mSign service, namely the classification of the types of documents that are eligible for signing through the mSign portal.

Cuprins

Introducere

Trecerea de la societatea industrial la societatea informaţională, dezvoltările în domeniul tehnologic, au contribuit la creşterea importanţei cunoaşterii producţiei, stocării, procesării şi partajării datelor. Anume progresul destul de rapid în tehnologia informaţiei a dus după sine numeroase schimbări, înepînd de la viaţa de zi cu zi a oamenilor, procesele de lucru a organizaţiilor, furnizarea de servicii , pînă la apariţia a noi domenii de expertiză şi profesii.

Din cauza ameninţărilor în schimbare, complexităţii şi eterogenităţii lor, nu mai este posibil să se ia în considerare diferite aspecte ale securităţii, independent una de cealaltă: sănătatea şi securitatea ocupaţională, securitatea fizică a activelor, securitatea mediului, securitatea reţelei şi a sistemei IT, precum şi informaţii mai generale despre securitate. Abordarea trebuie sa fie globală, atît în evaluarea cît şi în gestionarea şi controlul riscurilor. În acest sens, securitatea se încadrează firesc în abordarea corporativă de responsabilitate socială, care promovează creşterea responsabilă şi dezvoltarea durabilă.

Prin urmare, o politică de securitate globală acoperă toate domeniile de securitate. Ea are scopul de a controla efectele interdependenţei dintre aceste întrebări, în special cea de creare a propunerilor de servicii, de soluţionare a incidentelor sau de gestionare a crizelor. Aceasta este temelia unei abordări bazate pe îmbunătăţirea continuă a unui sistem de management de securitate. Intr-o epocă digitală, problema securităţii a devenit esenţială: securitatea datelor cu caracter personal, securitatea sistemelor utilizate pe piaţa afacerilor şi, în sfarşit, un alt aspect foarte important, interdependenţa între uzul profesional şi cel personal.

Dar dincolo de procesele indispensabile, vigilenţa, iluminismul, comportamentele noastre bine-informate, angajamentul fiecăruia dintre noi şi exemplele stabilite de manageri sunt factorii cheie în implementarea cu succes a politicii noastre de securitate globală. Acesta este un adevăr nu doar din punct de vedere a protecţiei, ci şi din punct de vedere pro-activ, pentru a profita de toate oportunităţile favorabile oferite de către o companie clienţilor săi.

Securitatea este afacerea tuturor, mai mult decît oricînd.

Lucrarea conţine adnotări în limba română şi engleză, cuprins, introducere, trei capitol, concluzii, bibliografie şi 45 pagini de text de bază, aplicate în domeniul de Securitate informaţională. S-au folosit aşa cuvinte ca cheie ca: Securitate informaţională, informaţii sensibile, informaţii confidenţiale, ameninţări, riscuri, fraude, vulnerabilităţi, principia de Securitate, inginerie social. Scopul propus pentru această lucrare este studierea metodelor de protecţie a informaţiei şi a sistemelor informaţionale care o prelucrează, contra accesului neautorizat, divulgării, indisponibilităţii, modificării sau distrugerii. Şi ca urmare obictivele de bază fiind elaborarea de ghiduri ca parte componentă a programului de securitate a

companiei, care ajută la protejarea confidenţialităţii informaţiilor, la asigurarea cerinţelor legale referitoare la securitatea datelor, protejarea datelor personale ale clienţilor şi protejarea sistemelor informaţionale ale companiei, în care are loc prelucrarea şi stocarea informaţiilor şi datelor.

Ca valoare teoretică sunt descrise conceptele generale ce ţin de securitatea informaţiilor, ameninţări, vulnerabilităţi şi riscuri asociate, principii de securitate şi managementul acestora.

Iar ca parte aplicativă au fost elaborate două ghiduri privind manipularea informaţiilor confidenţiale şi evitarea trucurilor de inginerie socială. De asemenea a fost elaborat un ghid pentru angajaţii companii, de folosire a platformei de semnare a documentelor electronice Orange Sign. Participarea în revizuirea procedurii de semnare electronica a documentelor utilizînd serviciul mSign, şi anume clasificarea tipurilor de documente care sunt eligibile pentru semnarea prin intermediul portalului mSign.

În capitolul 1 sunt descrise concepte generale ce ţin de securitatea informaţiilor, ameninţări, vulnerabilităţi şi riscuri asociate. De asemenea este descris managementul riscului şi managementul securităţii informaţiei.

În capitolul 2 sunt descrise prevederi generale de protecţie a datelor cu caracter personal, principii de securitate a datelor, de securitate IT şi securitate a activelor, de asemenea este descris şi riscul utilizării instrumentelor non-corporative şi auditul securităţii.

În capitolul 3 este descrisă partea aplicativă, adică ghidurile elaborate şi aportul meu personal la revizuirea procedurii de semnare electronică a documentelor prin intermediul portalului mSign.

BIBLOGRAFIE

1. Parlamentul European, Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, studiu pentru Comisia LIBE, septembrie2015. [citat 10.01.2021] Disponibil:https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf
2. ISO/IEC 27005:2018/ ISO/IEC 27001: 2005 Information technology — Security techniques — Information security risk management.
3. Chris Brook. What is a Data Classification Policy? [citat 12.03.2021] Disponibil: https://digitalguardian.com/blog/what-data-classification-policy
4. What is a Data Classification Policy and Why it's Important to Keep it Up to Date [citat 13.03.2021] Disponibil:https://securityboulevard.com/2020/11/what-is-a-data-classification-policy-and-why-its-important-to-keep-it-up-to-date/
5. Documente interne de guvernanţă a companiei Orange [citat 14.03.2021]
6. Information Security Management System (ISMS) [citat 16.03.2021] Disponibil: https://www.isms.online/information-security-management-system-isms/
7. Что такое современная система менеджмента информационной безопасности. Современные стандарты в области информационной безопасности, использующие концепцию управление рисками Цели и задачи исследования [citat 18.03.2021] Disponibil:https://johar.ru/war/chto-takoe-sovremennaya-sistema-menedzhmenta-informacionnoi-bezopasnosti/
8. Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risks [citat 19.03.2021] Disponibil:https://www.businesswire.com/news/home/20181115005665/en/Opus-Ponemon-Institute-Announce-Results-of-2018-Third-Party-Data-Risk-Study-59-of-Companies-Experienced-a-Third-Party-Data-Breach-Yet-Only-16-Say-They-Effectively-Mitigate-Third-Party-Risks
9. Ben Cole. risk management [citat 24.03.2021] Disponibil: https://searchcompliance.techtarget.com/definition/risk-management
10. The General Data Protection Regulation (GDPR). Security measures — ENISA Disponibil: https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/security-measures

11. Open-Source vs. Proprietary software [citat 05.05.2021] Disponibil:http://www.optimusinfo.com/downloads/white-paper/open-source-vs-proprietary-software-pros-and-cons.pdf
12. Aristide Bouix MSc. The risks of open-source software for corporate use [citat 05.05.2021] Disponibil:https://www.compact.nl/en/articles/the-risks-of-open-source-software-for-corporate-use/
13. Jinson Varghese. What is an IT Security Audit and How to Do It? [citat 29.04.2021] Disponibil: https://www.getastra.com/blog/security-audit/it-security-audit/
14. Republica Moldova PARLAMENTUL LEGE Nr. 171 din 06-07-1994 cu privire la secretul commercial
    Publicat : 10-11-1994 în Monitorul Oficial Nr. 13 art. 126
    Versiune în vigoare din data 20.07.2001 în baza modificărilor prin
    LP312-XV din 28.06.01, MO81-83/20.07.01 art.610 [citat 25.04.2021]
    Disponibil: https://www.legis.md/cautare/getResults?doc_id=64081&lang=ro
15. Republica Moldova PARLAMENTUL COD Nr. 1107 din 06-06-2002
    CODUL CIVIL AL REPUBLICII MOLDOVA
    Publicat : 22-06-2002 în Monitorul Oficial Nr. 82-86 art. 661
    Modernizarea Codului civil intră în vigoare la 01.03.2019
    MODIFICAT LP133 din 15.11.18, MO467-479/14.12.18 art.784; în vigoare 01.03.19 [citat 26.04.2021]
    Disponibil:https://www.legis.md/cautare/getResults?doc_id=110279&lang=ro