Universitatea Tehnică a Moldovei

Instrument pentru gestionarea procesului de audit al securității TI

Tool for managing the IT security audit process

Student: **Bularga Mircea**

Conducător: **Cernei Valeriu**

Lector universitar

Chişinău, 2020

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

Admis la susținere
Şef departament:
Fiodorov Ion, dr. conf.univ
_____
„__”_____ 2020

Instrument pentru gestionarea procesului de audit al securității TI

Teză de master

Student: **Bularga Mircea**

Conducător: **Cernei Valeriu**
Lector universitar

Chişinău, 2020

Rezumat (Adnotarea)

Lucrarea de master „Instrument pentru gestionarea procesului de audit al securității TI” descrie importanța procesului de audit, etapele implicate în proces, precum și rolul instrumentelor utilizate în optimizarea și gestionarea calitativă a misiunilor de audit.

Rezultatele obținute în cadrul proiectului pot fi implementate în cadrul diferitor instituții care implică un departament de audit intern, precum și de companiile specializate pe audit extern și vor fi utilizate de către membrii echipelor implicate în misiuni de audit. Instrumentul în cauză, pe lingă asigurarea suportului și gestionarea procesului la diferitor etape de audit, include și unele instrumente pentru comunicare precum un client de mail și un chat intern. Pentru planificarea ședințelor și evenimentelor importante platforma este dotată și cu un calendar. În cazul inițierii unui misiuni de audit, pot fi selectați membrii potriviți pentru proiect prin analiza abilităților profesionale a fiecărui utilizator, prezente în compartimentul “Team”.

Cele mai importante elemente ale instrumentului, care au servit ca obiectiv de bază, sunt etapele de audit, generate automat la inițierea unui proiect nou. Astfel sunt definite cinci etape după cum urmează: planificarea, pregătirea planului de audit, executarea auditului, efectuarea auditului la fața locului și pregătirea raportului de audit. Fiecare etapă include alte sub etape și instrumente necesare care asigură suportul pentru gestionarea optimă a procesului. Instrumentele prezente oferă posibilitatea de identifica domeniile de audit, componentele și sincronizarea lor la diferite etape. Tot procesul se finisează cu pregătirea raportului, etapă în care sunt descrise domeniile, sunt documentate constatările identificate iar la final toată informația este inclusă într-un raport generat automat printr-un buton.

Teza este structurată în patru capitole. Primul capitol analizează procesul de audit IT, importanța, etapele și rolul lor. Proiectarea sistemului se descrie în capitolul doi, prin diagrame UML, care reprezintă detaliat funcționalul și capacitățile platformei. Tehnologiile și instrumentele utilizate în procesul de elaborare sunt descrise în capitolul trei. Tot aici sunt descrise și etapele parcurse pentru dezvoltarea proiectului. Capitolul patru poate fi considerat un ghid, în care sunt descrise posibilitățile instrumentului, cum are loc înregistrarea, inițierea unui proiect, parcurgea etapelor, pregătirea și generarea raportului, etc.

Abstract

The master's thesis "Tool for managing the IT security audit process" describes the importance of the audit process, the steps involved in the process, as well as the role of the tools used in optimizing and qualitatively managing audit missions.

The results obtained within the project can be implemented in different institutions involving an internal audit department, as well as by companies specialized in external audit and will be used by the members of the teams involved in audit missions. The tool, in addition to providing support and managing the process at different stages of the audit, also includes some communication tools such as a mail client and an internal chat. The platform is also equipped with a calendar for planning important meetings and events. In case of initiating an audit mission, the appropriate members for the project can be selected by analyzing the professional skills of each user, present in the “Team” section.

The most important elements of the instrument, which served as the basic objective, are the audit steps, automatically generated at the start of a new project. Thus, five stages are defined as follows: planning, preparation of the audit plan, execution of the audit, conducting the on-site audit and preparation of the audit report. Each step includes other necessary sub-steps and tools that provide support for optimal process management. The present tools offer the possibility to identify the audit areas, the components and their synchronization at different stages. The whole process ends with the preparation of the report, the stage in which the fields are described, the identified findings are documented and at the end all the information is included in a report generated automatically by a button.

The thesis is structured in four chapters. The first chapter analyzes the IT audit process, its importance, stages and role. The design of the system is described in chapter two, through UML diagrams, which represent in detail the functionality and capabilities of the platform. The technologies and tools used in the development process are described in Chapter Three. Also here are described the stages taken for the development of the project. Chapter four can be considered a guide, in which the possibilities of the instrument are described, how the registration takes place, the initiation of a project, the stages, the preparation and generation of the report, etc.

Cuprins

Introducere

Mediul și procesele IT sunt zilnic amenințate de către hackerii, virușii și viermii, impactul fiind simțit prin daunele financiare semnificative provocate companiilor. Pentru corporații, atenuarea pierderilor potențiale implică detectarea în timp util a problemelor, o comunicare eficientă și un plan de rezolvare. Din păcate, nu toate companiile își permit formarea unei echipele de securitate, iar în multe cazuri numărul de personal nu este suficient atunci când se gestionează securitatea pentru întreprinderi, rețele și sisteme mai mari. Organizațiile își dau seama că simpla achiziționare sau instalare a unui firewall sau a unui sistem de detectare a intruziunilor nu va proteja sistemele și activele companiei de atacurile externe. Ei își dau seama că securitatea întreprinderii nu este doar ai instalat și funcționează, iar cei care continuă să o trateze așa vor avea pierderi și mai mari și deseori catastrofale.

Ca soluții poate servi utilizarea programelor de securitate a informațiilor, cum ar fi o soluție de gestionare a evenimentelor de securitate, un serviciu externalizat de scanare a vulnerabilităților sau un furnizor de servicii de securitate. Soluțiile centralizate de gestionare a securității câștigă popularitate datorită capacității lor de a agrega, standardiza, analiza și raporta informațiile despre evenimentele de securitate într-un mod succint și în timp real, totul printr-o singură consolă centrală. Acestea se dovedesc valoroase pentru gestionarea și evaluarea fluxului de date pe toate dispozitivele de securitate instalate și pentru auditul continuu al controalelor de securitate. Lipsa capacităților de audit al controlului de securitate este echivalentă cu instalarea unei uși din oțel dar fără lacăt. O inspecție de asigurare va confirma că au fost îndeplinite condițiile pentru securitate, dar fără blocarea ușii, toate controalele sunt în zadar.

Organizațiile de securitate a informațiilor și organizațiile de audit au un scop comun, să verifice că informațiile critice pentru misiunile companiei sunt protejate în mod corespunzător de accesul neautorizat. Este un pas înțelept pentru echipa de securitate, în primele etape de planificare a unui proiect, să înainteze îndrumări de audit, ca exemplu să includă instalarea de firewall-uri și sisteme de detectare a intruziunilor. Acest lucru ajuta la asigurarea faptului că controalele rezultate vor fi implementate în mod corespunzător, atât din punct de vedere tehnic, cât și operațional, pentru a se asigura protecția, precum și pentru respectarea politicilor de securitate care guvernează programul general de securitate. Un audit al securității IT oferă o imagine clară a performanței controlului de securitate și permite organizațiilor să facă modificările și achizițiile necesare pentru a preveni un atac pe scară largă. Corporațiile fac investiții semnificative într-o mare varietate de produse de securitate, dar fără audit, este aproape imposibil să se obțină o imagine cuprinzătoare a eficienții sistemului de securitate. Auditul și monitorizarea controalelor de securitate verifică starea și administrarea produselor punctelor de securitate și oferă numeroase avantaje.

Procesul de audit al securității informaționale include mai multe etape standarde, precum: inițierea auditului, analiza documentelor, pregătirea auditului la fața locului, efectuarea auditului la fața locului, pregătirea, aprobarea și prezentarea raportului de audit. Fiecare din aceste etape la fel include mai multe procese, gestionarea cărora uneori devine puțin mai complexă din cauza numărului mare de informații acumulate și comunicarea instabilă dintre membrii echipei de audit.

Astfel după mai multe observații s-a ajuns la concluzia că implementarea unui instrument, precum o platformă web, pentru gestionarea centralizată a procesului de audit v-a fi foarte benefică pentru echipa care efectuează o misiune de audit. Respectiv proiectului de master are ca scop implementarea unei astfel de instrument care v-a genera un set de avantaje, fiecare membru în orice moment v-a putea face cunoștință cu starea proiectului, se vor utilizeze informația și materialele reutilizabile astfel economisindu-se timpul pentru crearea repetată, dar cel mai mare avantaj îl constituie faptul că nu se vor utiliza canale de comunicare externe pentru transmiterea informațiilor confidențiale ce fac parte din proiectul de audit precum și se v-a exclude stocarea informației date pe stațiile locale ale membrilor, care nu mereu pot fi controlate din punct de vedere al securității astfel devenind o sursă bună pentru compromiterea datelor confidențiale. Toate manipulările și comunicarea necesară urmează se fie efectuate pe o singură platformă, lucru ce permite sporirea controlului și securității mediului informatic.

Concluzii

În urma efectuării tezei de master au fost analizat amănunțit etapele unui proces de audit al securității IT, s-au depistant avantajele, dezavantajele, tipurile și cele mai eficiente metode de organizare a unei misiuni de succes. Observînd unele amenințări de securitate cu care se confruntă companiile la moment s-a constat că beneficiile unui audit de securitate sunt enorme, deoarece prin constatarea și aplicarea tuturor recomandărilor înainte de auditor pot fi evitate pierderi financiare semnificative.

Astfel după mai multe observații și studii s-a luat decizia de implementare a unui instrument, precum o platformă web, pentru gestionarea centralizată a procesului de audit, lucru ce generează un set de beneficii pentru echipa care efectuează o misiune de audit. Sistemul a fost creat în totalitate utilizându-se limbajul de programare python și anume frameworkul Django, cu baza de date PostgreSQL.

La acest moment fiecare membru, accesând sistemul poate avea acces la un set de instrumente, precum clientul de mail, chatul, calendarul și poate vizualiza informația de profil a fiecărui membru al echipei. Un proiect nou poate fi inițiat de orișicare membru prezent în sistem. După inițierea proiectului și adăugarea informației necesare sunt generate etapele și instrumentele automatizate ce ușurează lucrul în cadrul unui audit.

Sistemul la acest moment încă se află la etapa de dezvoltare finală, care va fi urmată de etapa de testare și îmbunătățire continue.

Instrumentul generează un set de avantaje, fiecare membru în orice moment v-a putea face cunoștință cu starea proiectului, se vor utilizeze informația și materialele reutilizabile astfel economisindu-se timpul pentru crearea repetată, dar cel mai mare avantaj îl constituie faptul că nu se vor utiliza canale de comunicare externe pentru transmiterea informațiilor confidențiale ce fac parte din proiectul de audit precum și se v-a exclude stocarea informației date pe stațiile locale ale membrilor, care nu mereu pot fi controlate din punct de vedere al securității astfel devenind o sursă bună pentru compromiterea datelor confidențiale. Toate manipulările și comunicarea necesară urmează se fie efectuate pe o singură platformă, lucru ce permite sporirea controlului și securității mediului informatic.

Bibliografie

1. ScienceDirect: Cybersecurity investments in the supply chain: Coordination and a strategic attacker. Elsevier B.V., © 2020. [citat 16.09.2020]. Disponibil: https://www.sciencedirect.com/science/article /abs/pii/S037722171930757X
2. DNSstuff: Best Audit Management Software in 2020. SolarWinds Worldwide, © 2020. [citat 02.09. 2020]. Disponibil: https://www.dnsstuff. com/audit-management-software
3. Kaseya: Top 10 Cybersecurity Threats in 2020. [citat 13.09. 2020]. Kaseya Limited, © 2020. Disponibil: https://www.kaseya.com /blog/2020/04/15/top-10-cybersecurity-threats-in-2020/
4. I-sight: Cybersecurity Threats for 2020. [citat 02.09. 2020]. i-Sight by Customer Expressions, © 2020. Disponibil: https://i-sight.com/resources/11-cybersecurity-threats-for-2020-plus-5-solutions/
5. Alliancetechpartners: Enterprise Security Threats and Challenges in 2020. Alliance Technology Partners, © 2000-2020. [citat 02.12. 2020]. Disponibil: https://www.alliancetechpartners.com/top-enterprise-security-threats-and-challenges-in-2020/
6. ISACA: CISA® Review Manual 27th Edition
7. Netwrix: IT Security Audits: The Key to Success. Netwrix Corporation, © 2020. [citat 02.09. 2020]. Disponibil: https://blog.netwrix.com /2020/04/09/it-security-audit/
8. Tutorialspoint: UML – Overview. [citat 02.09. 2020]. Disponibil: https://www. tutorialspoint.com/uml/uml_ overview.htm
9. Sparxsystems: The Dynamic Model. Sparx Systems Pty Ltd., © 2000 - 2020 . [citat 02.09. 2020]. Disponibil: https://sparxsystems.com/resources/tutorials/uml /dynamic-model.html
10. Turbo-creative: Website Design Process. ALAN HUDGINS, © 2009-2018. [citat 02.09. 2020]. Disponibil: http://turbo-creative.com/website-design-process/
11. Amarinfotech: 5 Global Steps To Prepare Before Initializing Any Web Development Project. Amar Infotech. A Division Of Amar Technolabs Pvt Ltd, © 2009-2020. [citat 22.09. 2020]. Disponibil: https://www.amarinfotech.com/5-global-steps-for-web-development-project.html
12. Datacamp: Django Web Development in Python. [citat 02.10. 2020]. Disponibil: https://www.datacamp. com/community/tutorials/web-development-django