UNIVERSITATEA BABEŞ-BOLYAI CLUJ-NAPOCA
FACULTATEA DE ŞTIINȚE ECONOMICE ŞI GESTIUNEA AFACERILOR
CATEDRA DE INFORMATICĂ ECONOMICĂ

AUDITUL INFRASTRUCTURII IT FOLOSIND INTELIGENȚA ARTIFICIALĂ

~ Rezumat ~

Coordonator Ştiințiific: Prof. Univ. Dr. Nicolae Tomai
Drd. Ana-Maria Ghiran (Mureşan)

2011

Abstract

Auditul s-a constituit ca urmare a solicitărilor de a dispune de o evaluare obiectivă a modului în care managementul îşi desfăşoară activitatea. Dacă inițial era strict aplicat în domeniul financiar, ulterior prin abordarea sistematică şi riguroasă, s-a arătat eficient şi în alte domenii non financiare ce cuprind securitatea, performanța sistemelor informatice sau aspecte legate de mediu. Infrastructura IT s-a infiltrat în toate ramurile proceselor economice. Auditul Infrastructurii IT devine o necesitate în îmbunătățirea semnificativă a performanțelor proceselor de afaceri. Subiectul tratat este de însemnătate deosebită atât pe plan practic cât şi teoretic şi poate deschide numeroase oportunități aplicative şi în cercetare. În prezenta lucrare am încercat să atragem atenția asupra acestuia în preocupările auditorilor şi în special al celor din România. Pentru aceasta, am studiat care sunt metodele folosite în prezent pentru realizarea automatizată a auditului IT, descrierea acestora pentru a facilita realizarea practică a cât mai multor prototipuri - contribuții teoretice, iar prin modelul nou propus sperăm am reuşit să aducem şi o mică contribuție practică în acest domeniu.

Cuvinte cheie: *Auditul IT, auditul continuu, standarde de audit, agenți inteligenți, formalizarea cunoştintelor, ontologii*

Cuprins

1 Introducere

1.1 Preliminarii

Rolul auditorilor este din ce în ce mai însemnat în cadrul unei organizații prin contribuția pe care o aduc în sprijinirea procesului decizional.

Auditorul evaluează controalele implementate de către manageri şi va emite un raport. Dacă rolul unui manager este de a se încredința de aplicarea controalelor, un auditor va garanta modul în care sunt aplicate controalele, dacă sunt eficiente şi corespund scopului pentru care au fost definite [Gallegos 2008].

Pe plan mondial, conceptul de audit evoluează spre auditul continuuu şi auditul informatic.

Pe fondul creşterii aşteptărilor utilizatorilor ca informația să fie disponibilă în timp real, dar şi a faptului că noile tehnologii permit astfel de raportări (nu neapărat financiare) vor exista tot mai multe implementări ale conceptului de audit continuu.

Dacă auditul continuu va impune solicitări asupra modului de realizare a auditului (automatizat), pe de altă parte se va modifica şi obiectul evaluării, spre auditul IT, pe măsură ce deciziile manageriale sunt sprijinite din ce în ce mai mult de tehnologie.

Dacă anterior IT-ul a jucat un rol ambiguu în cadrul unei afaceri, oscilând între facilitarea procesului de afacere sau definirea acestuia, în funcție de cât de bine a fost integrat în scopurile şi strategiile companiei, în prezent se poate afirma cu convingere că IT-ul este parte componentă a oricărei organizații. Este clar că sistemele informatice au rol esențial în comunicațiile întreprinderii, contabilitate, producție, gestiunea lanțului de aprovizionare etc. IT-ul devine la fel de important atât în succesul sau câştigurile unei afaceri precum şi în pierderile acesteia.

Altfel spus, majoritatea organizațiilor în prezent sunt dependente de tehnologie, în principal de riscurile asociate acesteia, ceea ce se traduce prin necesitatea companiilor nu doar de a deține controlul asupra infrastructurii IT dar şi de a demonstra acest lucru sub forma unui raport de audit IT independent. În unele țări acesta este o recomandare în vederea realizării Guvernanței IT (IT Governance), ca parte a Guvernanței Corporatiste (Corporate Governance) sau este chiar o cerință legislativă pentru companiile ce acționează în domeniul public de ex. Sarbanes-Oxley Act – SOX [sox 2002] sau Health

Insurance Portability and Accountability Act - HIPAA [hip 1996] în SUA. Majoritatea țărilor din întreaga lume, printre care şi Romania, au adoptat legislație asemănătoare cu cea americană în ceea ce priveşte protecția datelor şi a informațiilor.

Astfel, IT-ul şi-a câştigat propria disciplină în audit fiind întâlnit sub diferite denumiri: Electronic Data Processing Audit - EDP Audit, Computer Information System Audit - CIS Audit, Information Technology Audit - IT Audit. Inițial acesta era utilizat doar pentru verificarea modului în care erau procesate datele financiare însă în timp, aria auditului IT s-a extins şi a trebuit să includă şi verificarea *modului* în care toate datele cu caracter sensibil sunt prelucrate, păstrate, comunicate.

1.2 Definirea problemei

În condițiile actuale, datorită suportului IT din ce în ce mai mare în cadrul unei organizații auditorii au nevoie de a evalua întregul sistem pentru a-şi fundamenta concluziile în ceea ce priveşte corectitudinea datelor furnizate de acesta.

Eficiența şi eficacitatea unui proces (IT, de management sau chiar de audit) sunt în general măsurate folosind metrici precum:

- timpul necesar pentru completarea procesului
- costul necesar executării
- calitatea sau procentajul de execuție corectă

Pentru obținerea unor rezultate bune a acestor metrici, procesele de afaceri în general şi cele IT în special au solicitat din ce în ce mai mult folosirea tehnologiei ceea ce a determinat gestionarea acestora tot cu ajutorul tehnologiei („using technology to manage technology" [ibm 2006]). Astfel, din momentul eliminării procedurilor manuale pentru gestionarea IT-ului, implicit s-a solicitat folosirea tehnologiei şi pentru realizarea auditului IT.

În prezent, există puține soluții pentru realizarea auditării în mod automatizat sau cu implicarea cât mai puțină a factorului uman şi din acest motiv considerăm că este o *problemă ce merită atenție*. Realizarea unei astfel de soluții ar avea o valoare practică deosebită.

Prin eliminarea procedurilor manuale se realizează atât creşterea eficienței în procesul de audit, cât şi eliminarea inacurateței ce poate să apară datorită unor erori

umane, a imposibilității de a lua în calcul toate informațiile sau chiar a subiectivității auditorului. Mai mult dacă prin metodele tradiționale de realizare a auditului IT, repetarea procesului era greu de luat în considerare, nu acelaşi lucru se poate spune despre folosirea automatizării în procesul de audit.

Inițial pentru automatizarea procesului de audit s-a avut în considerare eliminarea sarcinilor ce presupuneau activități monotone, laborioase.

Auditorii au început să folosească diverse tehnici de audit asistate de calculator Computer Assisted Audit Tools – CAATs care sunt diferite în funcție de tipul de audit în care sunt folosite. CAATs sunt definite ca fiind orice instrument sau metodă care implică folosirea calculatorului şi care permite auditorilor să-şi crească productivitatea în realizarea auditării [Gallegos 2008]. Definiția este foarte largă putând fi incluse în categoria CAATs atât editoarele simple de text cât şi sistemele expert, metode ce doar afişează date sau metode complexe de verificare a mai multor corelații [Gallegos 2008].

Instrumentele de audit în prezent ar trebui nu doar să sprijinine procesul de audit ci să realizeze cât mai mult din acesta („Use technology to actually audit as opposed to using technology to automate manual auditing procedures" comentariu al auditorilor parteneri grupului BigFour citat în [Searcy 2003]).

Chiar dacă există firme ce au realizat instrumente de audit şi toate firmele mari de audit le-au folosit pentru evaluarea riscurilor, a controalelor sau pentru audit în general, acestea nu sunt dispuse să dezvăluie realizările lor. Ca şi consecință, abordările acestora nu sunt supuse unui proces de revizuire ştiințifică putând ascunde anumite erori iar combinarea avantajelor ale diferitelor metode este greu de realizat deoarece nu sunt cunoscute. *Concluzionăm că este nevoie de eforturi ştiințifice în cadrul acestui domeniu.*

În urma analizării unor metode de audit informatic automatizate folosite în prezent, acestea realizează teste de conformață cu un anumit model de benchmark considerat bun.

Abordarea noastră se diferențiază de cele existente în domeniu şi descrise în capitolul 3 prin faptul că nu se realizează doar testul de conformanță ci şi o analiză preliminară în vederea determinării unui nivel de risc, care ulterior va fi folosit în construirea personalizată a modelului față de care se va realiza testul. Astfel abordarea noastră aduce o îmbunătățire calitativă a realizării auditării, rezultatele fiind mult mai

corecte deoarece au fost generate pentru fiecare situație în parte şi în plus se încadrează în modelul general de audit.

1.3 Obiectivele noastre

Ceea ce ne propunem să realizăm în această lucrare este ca pornind de la un model general pentru auditul informatic continuu să dezvoltăm o arhitectură proprie, care să contribuie la automatizarea procesului de audit. În implementarea acesteia vom folosi metodele şi tehnologiile "state of the art" din domeniu.

Prin prezenta lucrare, propunem realizarea acestor obiective prin următoarele abordări:

- prin delegarea sarcinilor de audit către agenții inteligenți
- prin descrierea semantică a cunoştințelor auditorilor prin intermediul ontologiilor
- aplicarea de către agenți a unor metode de raționare automate ce vor conduce la descoperirea de noi cunoştințe

Pornind de la cerințele auditorilor IT vom realiza un prototip care să verifice conformitatea cu cerințele funcționale şi nefuncționale exprimate în termeni abstracți, date de anumite coduri de bună practică. Pentru aceasta, vom propune o arhitectură generică a procesului de audit, vom furniza o modalitate de descriere a cunoştințelor auditorilor într-o ontologie, precum şi o exemplificare a funcționării pe probleme concrete de audit informatic.

1.4 Motivații

Motivațiile care ne-au condus pe parcursul realizării acestei teze pot fi împărțite în *motivații ale cercetării* şi *motivații pentru alegerea modului de abordare.*

Motivațiile cercetării decurg din problema supusă dezbaterii şi anume nevoia de a găsi o soluție care să aducă o contribuție cât de mică pentru realizarea automatizării procesului de audit IT.

Motivațiile pentru alegerea modului de abordare au rezultat din avantajele pe care le oferă metodologiile alese, care permit îndeplinirea în mare parte a cerințelor modelului propus. Astfel am identificat care sunt motivațiile pentru alegerea sistemelor multi-agent,

motivațiile pentru alegerea ontologiilor şi motivații pentru alegerea motoarelor de raționare.

Un sistem multi-agent va permite integrarea mai multor surse de cunoştințe Aceasta ce va duce la creşterea eficienței în procesul de audit prin obținerea aceloraşi rezultate într-un timp mult mai scurt, va obține o evaluare aproape în timp real şi va elimina posibilele erori umane.

O parte importantă a prototipului propus în această lucrare o constituie formalizarea expertizei unui auditor astfel încât aceste cunoştințe să poată fi construite separat de implementare şi refolosite ulterior. Acest deziderat poate fi uşor realizat cu ajutorul ontologiilor ce permit separarea cunoştințelor de modul lor de prelucrare.

Baza de cunoştințe descrisă într-o ontologie va trebui să includă extrem de multe concepte şi euristici aplicate de auditori şi în construcția acesteia pot colabora mai mulți experți. Din acest motiv este necesară o verificare a corectitudinii ontologiei. Ontologiile OWL-DL pot fi traduse într-o reprezentare a logicii descriptive, în acest fel se poate realiza o raționare automată asupra lor folosind un motor de raționare specific logicii descriptive. Un astfel de motor va realiza diverse sarcini de inferență precum deducerea superclaselor, a subclaselor, determinarea dacă o clasă este consistentă.

1.5 Organizarea tezei

Pentru început, în partea de introducere, am dat o scurtă prezentare a auditului şi care sunt tendințele actuale şi anume schimbările atât în ceea ce priveşte obiectul auditului (spre auditul IT) cât şi modul de realizare a acestuia (spre auditul continuu).

Pornind de la aceste noi cerințe în audit, am arătat necesitatea unei noi abordări şi care sunt obiectivele pe care ni le-am propus să le îndeplinim în această lucrare precum şi motivațiile care ne-au determinat în alegerea metodelor şi tehnologiilor folosite pentru implementarea acestora.

Teza este structurată pe două părți majore: prima va adresa *stadiul actual* şi va descrie detaliat auditul IT continuu, metodele folosite în prezent precum şi conceptele şi tehnologiile necesare pentru abordarea noastră, iar cea de-a doua se va concentra pe *contribuțiile* aduse prezentând arhitectura generală a sistemului pornind de la un model

propriu al procesului de audit IT şi un studiu de caz prin implementarea prototipului la nivelul auditării unui firewall.

Capitolul 2 Auditul IT continuu

2.1 Definirea conceptelor

2.1.1 Auditul IT

2.1.2 Auditul Continuu

2.1.3 Relația auditului cu mangementul

2.1.4 Auditul, Guvernarea Corporativă, Guvernarea IT

2.2 Riscul IT

2.2.1 Analiza riscurilor

2.2.2 Tratarea riscurilor

2.3 Controlul IT

2.3.1 Cadre de control

2.3.2 Controale ale securității informației şi modele de securitate

În acest capitol am încercat să clarificăm conceptele legate de auditul IT continuu precum şi a celor două componente majore ale acestuia. Am prezentat întâi ce se înțelege prin audit IT, audit al sistemului informatic şi audit al sistemului informațional. Am adaptat una din definiții pentru a clarifica domeniul la care facem referire în această teză şi anume auditul infrastructurii IT. În continuare am arătat rolul important pe care auditul îl are în cadrul unei organizații, ca instrument de sprijin al activității manageriale, prin oferirea de recomandări şi în general ca furnizor al unor asigurări pentru terțe părți în ceea ce priveşte modul de realizare a managementului, prin urmărirea principiilor de guvernanță corporativă.

În vederea realizării procesului de audit, se va evalua eficacitatea controalelor implementate de manageri. Pentru aceasta este important să se cunoască nivelul de risc pe care aceste controale trebuie să îl gestioneze. Astfel, auditorii vor realiza activități asemănătoare cu cele ale managerilor însă în mod separat, determinând un nivel de risc pentru elementul auditat şi identificând controalele potrivite pentru tratarea acestuia. În cadrul capitolului au fost detaliate metodele folosite pentru analiza riscului (atât calitative

cât şi cantitative) şi tratarea acestuia (micşorarea până la eliminarea lui sau acceptarea lui) precum şi cadrele de lucru folosite pentru implementarea unui sistem de control intern. S-a pus accentul pe riscul IT şi controlul IT.

Capitolul 3 Metodologii actuale de realizare a auditului IT continuu

3.1 Evaluarea vulnerabilităților

3.2 Testele de penetrare

3.3 Instrumente folosite de auditori

3.4 Particularități ale procesului de audit prezent

3.5 Abordări existente pentru automatizarea procesului de audit IT

3.5.1 SCAP - Security Content Automation Protocol

3.5.2 CAPEC - Common Attack Pattern Enumeration and Classification

În capitolul 3 am dorit a realiza o prezentare a abordărilor din domeniu pornind de la cele care deja sunt testate în practică spre cele teoretice care se constituie la momentul actual mai degrabă recomandări. Astfel, în *practica* auditului IT cele mai folosite metode sunt evaluarea vulnerabilităților şi testele de penetrare. Acestea determină nivelul de risc asupra unui element evaluat dar şi existența unor contramăsuri menite să micşoreze vulnerabilitățile în cauză. În ceea ce priveşte instrumentele folosite de auditorii IT, acestea sunt în general instrumente utilizate de managerii de sistem. *Cercetările* teoretice în audit oferă recomandări ce se referă la standardizarea şi formalizarea descrierilor de vulnerabilități, oferirea de nomenclaturi sub forma enumerațiilor. Aspectul predominant care a preocupat cercetarea teoretică este legat de securitate.

Capitolul 4 Metodologii folosite în abordarea noastră

4.1 Sisteme de extragere a informațiilor de management

4.1.1 Implementările existente

4.1.2 Către automatizarea procesului

4.2 Formalizarea cunoştințelor

4.2.1 Conceptul de ontologie

4.2.2 Limbaje pentru descrierea ontologiilor

Conținutul capitolul 4 este preponderent tehnic descriind tehnologiile folosite în abordarea noastră. Pentru început am analizat sistemele de extragere a informațiilor de management pentru a identifica varianta cea mai eficientă. În alegerea metodelor folosite în abordarea nostră s-a avut în vedere ca toate acestea să poată fi integrate împreună şi cu realizarea maximă a funcționalității. Mai mult, s-a urmărit adoptarea metodelor şi a tehnologiilor ce s-au dovedit în prezent a fi cele mai eficiente: ontologiile pentru descrierea formalizată a cunoştințelor, motoarele de raționare automată pentru generarea de noi cunoştințe, sistemele multi agent pentru distribuirea sarcinilor şi posibilitatea intercorelării informațiilor diferite, şi nu în ultimul rând sistemele de extragere a informațiilor de management.

Capitolul 5 Arhitectura generală propusă

În capitolul 5 am descris un model generic propriu pentru procesul de audit precum şi o arhitectură în mai multe straturi pentru implementarea acestui model cu ajutorul unui sistem multi agent. Cele patru nivele ale arhitecturii (nivelul utilizatorilor

umani, nivelul sistemului MAS, nivelul elementului gestionat, nivelul resurselor gestionate) au fost apoi detaliate în principal cu ajutorul cazurilor de utilizare. S-a trecut apoi la explicarea funcționalității sistemului începând cu inițializarea sistemului şi continuând cu utilizarea acestuia.

Capitolul 6 Studiu de caz

6.1 Problema auditării unui firewall

6.1.1 Particularități în evaluarea configurației firewall-urilor

6.1.2 Conflictele în cadrul aceleiaşi politici de securitate

6.1.3 Conflictele între politici de securitate diferite

6.2 Modelarea unei ontologii pentru reprezentarea cunoştințelor din domeniul firewall-urilor

6.3 Proiectarea de detaliu a sistemului

6.3.1 Inițializarea sistemului

6.3.2 Adunarea datelor inițiale

6.3.3 Afişarea interfeței grafice

6.3.4 Preluarea datelor de la utilizator

6.3.5 Stabilirea nivelului de risc

6.3.6 Verificarea controalelor existente

Ultimul capitol este un studiu de caz al auditării IT folosind arhitectura propusă. Am arătat de ce am ales firewallul, ca element exemplificativ şi anume datorită faptului că acoperă atât situația evaluării unui simplu element cât şi situația în care evaluarea este pentru un element ce se constituie ca şi control al altor elemente. În continuare am descris care sunt particularitățile şi provocările întâlnite în evaluarea firewallurilor şi cum sunt tratate în cercetările prezente. Problema conflictelor din cadrul politicilor de firewall a fost dezbătută pe larg în cercetările teoretice, însă foarte puține abordări cu ajutorul descrierilor ontologice datorită particularităților pe care le solicită exprimarea regulilor de acces din cadrul politicilor de firewall. În continuare am prezentat pe scurt o exemplificare proprie a modelării prin ontologie a cunoştințelor pentru evaluarea regulilor dintr-un firewall şi aplicarea unor raționamente pentru identificarea posibilelor

conflicte. Sperăm că am reuşit să arătăm prin ce se diferenţiază abordarea noastră de celelalte.

Concluzii

Prin prezenta lucrare am încercat să demonstrăm aplicabilitatea agenţilor inteligenţi în ceea ce priveşte auditul infrastructurii IT în vederea automatizării procesului şi eliminarea cât mai mult posibil a factorului uman.

Tema a fost selectată cu convingerea că trecerea către o abordare automatizată a realizării procesului de audit devine o necesitate clară a momentului.

Auditul a început să treacă de la o preocupare în mare parte a practicienilor către un subiect de cercetare, existând interes din ce în ce mai mult din partea domeniului educaţional. De asemenea, obiectul auditării a evoluat în prezent spre auditul IT.

Auditul, indiferent de forma pe care o îmbracă, se referă la evaluarea modului în care managementul implementează controale pentru a micşora riscurile. Astfel auditul IT va considera managementul tehnologiei informaţionale, adică a resurselor informatice şi a modului de organizare a acestora (a reţelei). „State of the art" în domeniul managementului IT se îndreaptă către automatizarea procesului. Automatizarea acestuia obligă implicit şi auditorul să adopte o soluţie pe măsură: dacă pentru gestionarea tehnologiei este necesară folosirea tehnologiei cu atât mai mult pentru a verifica acest mod de gestionare este nevoie de tehnologie.

Având două direcţii principale pentru automatizarea managementului reţelelor şi a resurselor IT care au reuşit să se impună de-a lungul timpului, una prin descrierea semantică ale politicilor ce trebuie aplicate şi alta prin aplicarea diverselor cunoştinţe din domeniul inteligenţei artificiale, considerăm că soluţia optimă este dată de combinarea acestor tehnici. Arhitectura propusă este bazată pe agenţi inteligenţi care sunt conduşi de modele ontologice ale politicilor stabilite la nivel de întreprindere şi care în plus ar putea oferi o asigurare în ceea ce priveşte conformitatea cu anumite politici stabilite în coduri de bună practică sau standarde de audit.

Prototipul realizat este în Jade care este platforma cel mai des folosită pentru realizarea de sisteme multi-agent. Cunoştinţele agenţilor sunt păstrate sub ontologiilor OWL în acest fel putând fi construite separat de implementarea agenţilor. Aceste

ontologii vor permite transformarea cerințelor primite de la utilizatorul uman (care sunt exprimate în limbaj abstract) în noțiuni concrete pe care un agent trebuie să le urmărească în informațiile interogate. De asemenea, ontologiile sunt necesare pentru a realiza operația inversă la returnarea rezultatului. Este posibil să fie necesară apelarea şi a altor ontologii în cazul în care se fac verificări de conformanță.

Agenții pot să acceseze informațiile din ontologie direct prin OWL API - ce permite şi adăugarea de cunoştințe în ontologie (agenții vor avea nevoie să îşi construiască un model propriu al realității). De asemenea, agenții pot să apeleze la un motor de inferență care le va permite să raționeze asupra cunoştințelor.

În prezent pentru a extrage informațiile de management din cadrul elementelor de rețea gestionate, necesare prototipului s-a apelat la protocolul SNMP, care este în continuare cel mai răspândit. Deşi în practică nu s-a putut renunța la acesta, majoritatea furnizorilor importanți de echipamente de rețea oferă concomitent şi posibilitatea de a accesa informațiile de management prin intermediul altor protocoale mult mai evoluate precum cele bazate pe servicii web (WS -Management). De exemplu, Microsoft oferă pentru managementul sistemelor Windows atât serviciul SNMP cât şi WMI – Windows Management Instrumentation. Astfel ca şi perspective ale cercetării trebuie avute în vedere modificările în ceea ce priveşte adoptarea altor protocoale de management în rețea.

În auditulul informatic, existența unor standardizări ale obiectivelor de control urmărite în cadrul unei afaceri permite formalizarea cu uşurință a acestora.

În cele din urmă, considerăm că se poate spune că evoluția tehnologiilor prezente permite adoptarea acestora către domenii considerate anterior specific umane, precum realizarea activităților de audit.

7.1 Contribuții personale

Teza de doctorat cu titlul „Auditul Infrastructurii IT folosind Inteligența Artificială” prezintă rezultatele cercetării realizate de autoare începând cu 2005 prin abordarea unei teme ce are influențe în multiple domenii. Prin modul în care a fost organizată prezenta lucrare s-a încercat păstrarea unui echilibru între descrierea stadiului actual şi descrierea contribuțiilor personale. În prima parte pentru detalierea conceptelor

s-a luat în considerare strict ceea ce a fost folosit ulterior în abordarea noastră şi de asemenea în partea de contribuții s-a urmărit pe cât posibil doar descrierea rezultatelor proprii - din acest motiv şi referințele bibliografice sunt mult mai puține.

Principalele contribuții aduse prin această lucrare se referă la dezvoltarea unui model generic de audit pe baza căruia a fost ulterior implementat un prototip pentru realizarea auditării infrastructurii IT cât mai aproape de timpul real, a auditării continue.

O listă cu contribuțiile aduse prin această lucrare ar putea include:

- realizarea unor sinteze atât în domeniul auditului informatic cât şi a metodologiilor folosite în abordarea noastră
- propunerea unui model generic pentru procesul de audit IT
- elaborarea unei arhitecturi în mai multe straturi a unui sistem multi-agent pentru modelul propus
- am arătat modul în care o platformă mult-agent precum JADE poate fi implementată pentru a automatiza procesul de audit IT descris
- am arătat modul în care se pot descrie cunoştințele unui auditor prin ontologii
- am prezentat un studiu de caz care să implementeze modelul propus

7.2 Direcții viitoare de cercetare

Luând în considerare conținutul lucrării de față, putem afirma că cercetările în cadrul direcțiilor propuse sunt abia la început şi ne propunem o serie de îmbunătățiri şi dezvoltări viitoare:

- Realizarea mai multor tipuri de agenți pentru a cuprinde mai multe sarcini ale auditorului
- O asimilare mai bună a serviciilor publice de descriere a vulnerabilităților şi a amenințărilor
- Integrarea cu mai multe servicii de management a informațiilor precum cele bazate pe web-services
- Cercertări ale implicațiilor într-un mediu mobil sau cloud computing
- Integrarea în cadrul prototipului a unor metode de securizare

7.3 Diseminarea rezultatelor

Întreaga abordare propusă în această lucrare a fost discutată inițial în Simpozionului Doctoral din cadrul conferinței ESWC (European Semantic Web Conference) din 2006.

Contribuțiile aduse prin această lucrare au fost diseminate în principal prin prezentările la conferința BIS - Business Information Systems, în 2009 [Ghiran 2009], respectiv 2011 [Ghiran 2011], ambele cu publicare în Lecture Notes in Business Information Processing, seria specială Springer dedicată publicării rezultatelor din domeniul Informaticii Economice.

1) [Ghiran 2009] **Ana-Maria Ghiran (Mureşan)**, Gheorghe Cosmin Silaghi and Nicolae Tomai. Ontology Based Tools for Automating Integration and Validation of Firewall Rules. In BIS'09, pages 37-48, 2009

   În această lucrare am prezentat mare parte din implementarea studiului de caz, arătând cum pot fi identificate conflictele din cadrul politicilor de securitate dintr-un firewall cu ajutorul aplicării unor metode de raționare automată asupra descrierilor ontologice a cunoştințelor din domeniul respectiv.

2) [Ghiran 2011] **Ana-Maria Ghiran (Mureşan)**, Gheorghe Cosmin Silaghi and Nicolae Tomai. Deploying an Agent Platform to Automate the IT Infrastructure Auditing Process. In Proceedings of BIS'11, 2011

   Lucrarea prezintă modelul generic propus pentru realizarea automatizată a procesului de audit IT precum şi arhitectura în mai multe straturi bazată pe un sistem multi-agent. De asemenea, este inclusă o parte din modul în care o platformă multi-agent precum JADE poate fi implementată pentru realizarea arhitecturii propuse.

Pe lângă aceste publicații, activitatea de cercetare derulată pe tema doctoratului a mai fost concretizată:

3) [Ghiran 2010a] **Ana-Maria Ghiran (Mureşan) –** Network Management Framework Based on Intelligent Agents, Semantic Modeling and Web Services, The Second

În lucrare este prezentat un model şi o arhitectură incipientă al abordării noastre ce a stat la baza devoltării modelului şi a arhitecturii curente diseminate la articolul din acest an.

4) [Ghiran 2010b] **Ana-Maria Ghiran (Mureşan)**– Semantic Modeling for Autonomic Network Management, The Second International Conference Software, Services and Semantic Technologies,Varna, Bulgaria, 2010, ISBN 978-954-9526-71-4
   Articolul prezintă cerinţele pentru realizarea unui management autonom în reţea, ce stă la bazele realizării auditului autonom sau automatizat, precum şi posibilitatea formalizării cunoştinţelor prin ontologii.

5) [Ghiran 2007] **Ana-Maria Ghiran (Muresan)**, Monica Vancea – Risk Identification Method based on Ontology, in Proceedings of the International Conference Competitiveness and European Integration, 2007,Ed. Risoprint,ISBN 978-973-751-597-1
   Studiul se referă la evaluarea oportunităţii de a folosi ontologiile în partea de identificare a riscurilor.

7.4 Lista completă a lucrărilor

1. Tomai Nicolae, **Mureşan Ana-Maria** - Agent Technology in Wireless Networks, InfoBusiness 2006 – The International Conference on Business Information Systems, Ed. Universităţii Al. Ioan Cuza, Iaşi, ISBN: 978-973-703-207-2
2. Tomai Nicolae, **Mureşan Ana-Maria** – Cooperative Agents in Mobile Ad-Hoc Networks, Annals of the Tiberiu Popoviciu Seminar of Functional Equations Approximation and Convexity, Vol. 4, 2006, Mediamira Science Publisher, Cluj-Napoca, ISSN 1584-4536
3. **Mureşan Ana-Maria** – Intelligent Agents for Collaborative Work, Annals of the Tiberiu Popoviciu Seminar of Functional Equations Approximation and Convexity, Vol. 4, 2006, Mediamira Science Publisher, Cluj-Napoca, ISSN 1584-4536
4. **Mureşan Ana-Maria** – Technology Issues in Adopting Continuous Audit, Informatics in Knowledge Society, The Proceedings of the Eight International Conference on Informatics in Economy, may 2007, Ed. Economică, ISBN 978-973-594-921-1
5. Tomai Nicolae, **Mureşan Ana-Maria**, Mican Daniel – Wireless Network Design

6. **Ghiran (Mureşan) Ana-Maria**, Monica Vancea – Risk Identification Method based on Ontology, in Proceedings of the International Conference Competitiveness and European Integration, 2007, Ed. Risoprint, ISBN 978-973-751-597-1
7. Mican Daniel, Bologa Cristian Sorin**, Ghiran (Mureşan) Ana Maria,** Optimized Advertising Content Delivery, Annals Of The Tiberiu Popoviciu Seminar Of Functional Equations, Approximation And Convexity, Categ CNCSIS C, 6/1, 2008, P.230 - 240
8. **Ghiran (Mureşan) Ana-Maria,** Mican Daniel – Firewalls on Mobile Devices, The Ninth International Conference on Informatics in Economy, 2009, Ed. Economica, ASE, ISBN 978-606-505-178-2
9. **Ghiran (Mureşan) Ana Maria,** Silaghi Gheorghe-Cosmin, Tomai Nicolae**,** *Ontology-Based Tools for Automating Integration and Validation of Firewall Rules*, Business Information Systems 12th International Conference, BIS 2009, Poznan, Poland, 27-29 April, Proceedings, Springer Berlin Heidelberg, Editor: Witold Abramowicz, 978-3-642-01189-4, http://www.springerlink.com/content/p124578166010p14/?p=fd586ab81f154fe4bab507e706fdb65e&pi=4
10. **Ghiran (Mureşan) Ana-Maria** – Semantic Modeling for Autonomic Network Management, The Second International Conference Software, Services and Semantic Technologies,Varna, Bulgaria, 2010, ISBN 978-954-9526-71-4
11. **Ghiran (Mureşan) Ana-Maria –** Network Management Framework Based on Intelligent Agents, Semantic Modeling and Web Services, The Second Romanian Workshop on Mobile Business, Cluj-Napoca, 2010, Economy Informatics, Vol. 10, No1/2010
12. **Ghiran (Mureşan) Ana Maria,** Silaghi Gheorghe-Cosmin, Tomai Nicolae**,** *Deploying an Agent Platform to Automate the IT Infrastructure Auditing Process*, in Business Information Systems 14th International Conference, BIS 2011, Poznan, Poland, Proceedings, Springer Berlin Heidelberg, Editor: Witold Abramowicz
13. Breşfelean Vasile Paul, **Ghiran (Mureşan) Ana-Maria** Ontology Importance towards Enhancing Suggestions in a News Recommender System for a Financial Investor, to appear in Metadata and Semantics Research Conference Proceedings, MTSR 2011, Iymir, Turkey, Proceedings, Springer Berlin Heidelberg

Bibliografie

[1] [Andone 2005] Ioan Andone. Ontologiile şi modelarea informațională a întreprinderii. Analele Ştiințifice ale Universitatii "Al.I.Cuza", Secțiunea Ştiințe Economice, nr. 26, 2005. 83

[2] [Barnum 2010] Sean Barnum. Common Attack Pattern Enumeration and Classifcation CAPEC Schema Description. 2010. 69

[3] [Bellifemine 2007] Fabio Luigi Bellifemine, Giovanni Caire and Dominic Greenwood. Developing multi-agent systems with jade. Wiley, 2007. 100, 102, 103, 106, 107, 109

[4] [Bellifemine 2008a] Fabio Bellifemine, Giovanni Caire, Agostino Poggi and Giovanni Rimassa. JADE: A software framework for developing multi-agent applications. Lessons learned. Inf. Softw. Technol., vol. 50, pages 10-21, January 2008. 100

[5] [Bellifemine 2008b] Fabio Luigi Bellifemine, Giovanni Caire and Tiziana Trucco. Jade programmer's guide. Jade Documentation, 2008. 100, 101, 102, 103, 104, 105, 106, 107, 108, 110, 111, 170

[6] [Borst 1997] Willem Nico Borst. Construction of Engineering Ontologies for knowledge sharing and reuse. PhD thesis, University of Twente, Enschede, 1997. 82

[7] [Boutaba 2002] Raouf Boutaba and Jin Xiao. Network Management: State of the Art. In Communication Systems: The State of the Art (IFIP World Computer Congress)'02, pages 127-146, 2002. 74, 76

[8] [Buraga 2004] Sabin Corneliu Buraga. Semantic web, fundamente şi aplicatii. Matrix ROM, Bucureşti, 2004. 86

[9] [Burtescu 2004] Emil Burtescu. Securitatea datelor în sisteme informatice. Teza de doctorat, 2004. 28

[10] [Caire 2009] Giovanni Caire. Jade tutorial, jade programming for beginners. Jade Documentation, 2009. 101, 102, 104, 106, 109

[11] [Cis 2003] Internetworking technologies handbook, forth edition. Cisco Press, 2003. 74

[12] [Clark 2003] David D. Clark, Craig Partridge, J. Christopher Ramming and John T. Wroclawski. A knowledge plane for the internet. In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, SIGCOMM '03, pages 3-10, New York, NY, USA, 2003. ACM. 79, 81

[13] [Cob 2007] Cobit 4.1, versiunea în limba română. IT Governance Institute, 2007. vii, 21, 36, 37

[14] [Coderre 2005] David Coderre. Global technology audit guide, continuous auditing: Implications for assurance, monitoring and risk assessment. The Institute of Internal Auditors, 2005. vii, 2, 17, 18, 19

[15] [Damianou 2001] Nicodemos Damianou, Naranker Dulay, Emil Lupu and Morris Sloman. The Ponder Policy Specifcation Language. In Lecture Notes in Computer Science, pages 18-38. Springer-Verlag, 2001. 75

[16] [Davies 2006] John Davies, Rudi Studer and Paul Warren. Semantic web technologies: Trends and research in ontology-based systems. John Wiley & Sons, 2006. 82, 89, 91

[17] [Derbel 2009] Hajer Derbel, Nazim Agoulmine and Mikael Salaln. ANEMA: Autonomic network management architecture to support self-confguration and self-optimization in IP networks. Computer Networks, vol. 53, no. 3, pages 418 -430, 2009. 80, 81

[18] [Dobson 2006] Simon Dobson, Spyros Denazis, Antonio Fernandez, Dominique Gaiti, Erol Gelenbe, Fabio Massacci, Paddy Nixon, Fabrice Safre, Nikita Schmidt and Franco Zambonelli. A survey of autonomic communications. ACM Trans. Auton. Adapt. Syst., vol. 1, pages 223-259, December 2006. 81

[19] [Domingue 2009] John Domingue and Dieter Fensel. Problem solving methods in a global networked age. Artif. Intell. Eng. Des. Anal. Manuf., vol. 23, pages 373-390, 2009. 77

[20] [Gallegos 2008] Frederick Gallegos and Sandra Senft. Information technology control and audit, third edition. Auerbach Publications, 2008. 1, 5

[21] [Gavalas 2000] Damianos Gavalas, Dominic Greenwood, Mohammed Ghanbari and Mike OMahony. Advanced Network Monitoring Applications Based on Mobile/Intelligent Agent Technology. Computer Communications Journal, vol. 23, pages 720-730, 2000. 77

[22] [Gavalas 2009] Damianos Gavalas, George E. Tsekouras and Christos Anagnostopoulos. A mobile agent platform for distributed network and systems management. J. Syst. Softw., vol. 82, pages 355-371, February 2009. 76, 77, 132

[23] [Gheorghe 2006] Mirela Gheorghe. Guvernanța IT -Cheia optimizării unei afaceri. The Journal of the Faculty of Economics -Economic Science Series, vol. II, pages 1104-1107, 2006. 23

[24] [Ghiran 2009] Ana-Maria Ghiran, Gheorghe Cosmin Silaghi and Nicolae Tomai. Ontology-Based Tools for Automating Integration and Validation of Firewall Rules. In BIS'09, pages 37-48, 2009. vii, 10, 122, 146, 148, 153, 155

[25] [Ghiran 2010] Ana-Maria Ghiran. Semantic Modeling for Autonomic Network Management. In Proceedings of The Second International Conference on Software, Services and Semantic Technologies, S3T Conference, pages 15-26, 2010. 78, 122

[26] [Ghiran 2011] Ana-Maria Ghiran, Gheorghe Cosmin Silaghi and Nicolae Tomai. Deploying an Agent Platform to Automate the IT Infrastructure Auditing Process. In to appear in BIS'11, 2011. vii, 10, 121, 122, 123, 125, 126, 127, 128, 130, 131, 133, 137, 168

[27] [Ghita 2009] Marcel Ghiță, Cornelia Nicolau, Zaharica Florea-Ianc, Ion Peres, Ovidiu Constantin Bunget and Cristian Elian Peres. Guvernanţa corporativă şi auditul intern. Editura Mirton, 2009. 21, 22, 35, 36

[28] [Gouda 2007] Mohamed G. Gouda and Alex X. Liu. Structured firewall design. Computer Networks Journal, vol. 51, 2007. 147, 151, 152

[29] [Gruber 1993] Thomas R. Gruber. A translation approach to portable ontology specifcations. Knowl. Acquis., vol. 5, pages 199-220, June 1993. 82

[30] [GTA 2005] Global technology audit guide, information technology controls. The Institute of Internal Auditors, 2005. vii, 33, 36

[31] [Hamed 2006] Hazem Hamed and Ehab Al-shaer. Taxonomy of conficts in network security policies. In In IEEE Communications Magazine, pages 134-141, 2006. 147, 148, 151

[32] [Hebeler 2009] John Hebeler, Matthew Fisher, Ryan Blace, Andrew Perez Lopez and Mike Dean. Semantic web programming. John Wiley & Sons Inc., Chichester, West Sussex, Hoboken, NJ, 2009. 83

[33] [Hill 2003] Ernest Friedman Hill. Jess in action: Java rule-based systems. Manning Publications Co., Greenwich, CT, USA, 2003. 98

[34] [Hillson 2002] David Hillson. Extending the risk process to manage opportunities. International Journal of Project Management, vol. 20, no. 3, pages 235 -240, 2002. 24

[35] [hip 1996] The health insurance portability and accountability act. U.S. Government Printing Ofce, 1996. http://www.hipaa.org. 3

[36] [Horridge 2007] Matthew Horridge, Simon Jupp, Georgina Moulton, Alan Rector, Robert Stevens and Chris Wroe. A practical guide to building owl ontologies using protege 4 and co-ode tools, edition 1.1, technical report. The University of Manchester, 2007. 95, 96

[37] [Horrocks 2004] Ian Horrocks, Peter F. Patel-Schneider, Harold Boley, Said Tabet, Benjamin Grosof and Mike Dean. Swrl: A semantic web rule language combining owl and ruleml. W3C Member Submission, 2004. 96, 97

[38] [ibm 2006] An Architectural Blueprint for Autonomic Computing. IBM Autonomic Computing White Paper. June 2006. 4, 80, 81

[39] [ITG 2003] Board briefng on it governance, second edition. IT Governance Institute, 2003. 23

[40] [Jennings 2007] B. Jennings, S. van der Meer, S. Balasubramaniam, D. Botvich, M. O Foghlu, W. Donnelly and J. Strassner. Towards autonomic management of communications networks. Communications Magazine, IEEE, vol. 45, issue 10, pages 112-121, 2007. 79, 80, 81

[41] [Kephart 2007] Jefrey O. Kephart and Rajarshi Das. Achieving Self-Management via Utility Functions. IEEE Internet Computing, vol. 11, pages 40-48, January 2007. 81

[42] [MartinFlatin 1999] Jean-Philippe Martin-Flatin, Simon Znaty and Jean-Pierre

[43] [Martin 2008] R.A. Martin. Making security measurable and manageable. In Military Communications Conference, 2008. MILCOM 2008. IEEE, pages 1 -9, nov. 2008. 58, 59

[44] [Mell 2007] Peter Mell, Karen Scarfone and Sasha Romanosky. Cvss a complete guide to the common vulnerability scoring system, version 2.0. FIRST Forum of Incident Response and Security Teams, 2007. http://www.frst.org/cvss/cvss-guide.pdf. 66, 67, 68

[45] [Moeller 2010] Rober Moeller. It audit, control and security. John Wiley and Sons Inc, 2010. 37, 45

[46] [Munteanu 2001] Adrian Munteanu. Auditul sistemelor informationale contabile cadru general. Editura Polirom, 2001. 26, 28, 31

[47] [Munteanu 2005] Adrian Munteanu and Doina Fotache. Auditing Integrated Systems A Romanian Approach. In Proceedings of the International Workshop on Collaborative Support Systems in Business and Education. Risoprint, 2005. 2

[48] [Nastase 2007] Pavel Nastase, Victoria Stanciu and Ali Eden. Auditul şi controlul sistemelor informationale. Editura Economica, 2007. 15, 16, 19, 23

[49] [Nikraz 2006] Magid Nikraz, Giovanni Caire and Parisa A. Bahri. A methodology for the development of multi-agent systems using the JADE platform. Comput. Syst. Sci. Eng., vol. 21, no. 2, 2006. 7

[50] [Noy 2001] Natalya F. Noy and Deborah L. McGuinness. Ontology Development 101: A Guide to Creating Your First Ontology. Rapport technique, Stanford Knowledge Systems Laboratory and Stanford Medical Informatics, 2001. 83, 84

[51] [Oprean 2002] Dumitru Oprean. Audit. Presa Universitara Clujeana, 2002. 1

[52] [Ova 2006] Introduction to oval language, version 5. MITRE Corporation, 2006. 63, 64

[53] [Ozier 2004] Will Ozier. Risk analysis and assessment, information security management handbook. Auerbach Publications, 2004. 24

[54] [Pranothi 2010] N. Pranothi and R. Hemavathy. A Survey of Network Device Configuration Audit Tools. Int. J. of Advanced Networking and Applications, vol. 02, issue 02, pages 532-538, 2010. 56, 58

[55] [Puliafto 2000] Antonio Puliafto and Orazio Tomarchio. Using Mobile Agents to implement flexible Network Management strategies. Computer Communication Journal, vol. 23, pages 708-719, 2000. 77

[56] [Quinn 2009] Stephen Quinn, David Waltermire, Christopher Johnson, Karren Scarfone and John Banghart. The technical specification for the security content automation protocol (scap), scap version

[57] NIST, 2009. http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf. 47, 61, 62, 64, 65

[58] [Rogers 2008] Russ Rogers. Nessus network auditing, second edition. Syngress Publishing, 2 edition, 2008. 48, 52, 54, 55, 57

[59] [Rothke 2004] Ben Rothke. How to perform a security review of a check-point firewall information security management handbook. Auerbach Publications, 2004. 142, 143, 144

[60] [Rughiniş 2010] Răzvan Rughiniş, Răzvan Deaconescu, Andrei Ciorba and Bogdan Doinea. Retele locale. Ed Printech, 2010. 25, 55

[61] [Scarfone 2009] Karen Scarfone and Paul Hofmann. Guidelines on firewalls and firewall policy. NIST, 2009. http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf. 141, 142

[62] [Schonwalder 2009] Jurgen Schonwalder, Marc Fouquet, Gabi Dreo Rodosek and Iris C. Hochstatter. Future internet = content + services + management. Comm. Mag., vol. 47, pages 27-33, July 2009. 77

[63] [Searcy 2003] DeWayne Searcy, Jon Woodroof and Bruce Behn. Continuous Audit: The Motivations, Benefits, Problems, and Challenges Identifed by Partners of a Big 4 Accounting Firm. Hawaii International Conference on System Sciences, vol. 7, page 210, 2003. 5, 17

[64] [Segaran 2009] Toby Segaran, Colin Evans, Jamie Taylor, Segaran Toby, Evans Colin and Taylor Jamie. Programming the semantic web. O'Reilly Media, Inc., 1st edition, 2009. 86

[65] [Siorpaes 2004] Katharina Siorpaes, Kathrin Prantner and Anna V. Zhdanova. Ontology instantiation, sw portal working draft, d13v0.2. DERI Semantic Web Portal Group, 2004. 92, 93, 94, 95

[66] [sox 2002] Sarbanes-oxley act of 2002. public law 107-204. U.S. Government Printing Ofce, 2002. http://www.gpo.gov/fdsys/pkg/PLA\-107publ204/content-detail.html. 3

[67] [SP80053 2009] Computer Security Division Publication SP800-53. Recommended security controls for federal information systems and organizations. NIST, 2009. 34, 146

[68] [Staab 2004] Stefen Staab and Rudi Studer. Handbook on ontologies (international handbooks on information systems). SpringerVerlag, 2004. 82

[69] [Stoneburner 2002] Gary Stoneburner, Alice Goguen and Alexis Feringa. Risk management guide for information technology systems. NIST, 2002. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf. 24, 25, 35, 127

[70] [Strassner 2006] John Strassner, Nazim Agoulmine and Elyes Lehtihet. FOCALE A Novel Autonomic Networking Architecture. In Latin American Autonomic Computing Symposium (LAACS), 2006. 79, 80

[71] [Studer 1998] Rudi Studer, V. Richard Benjamins and Dieter Fensel. Knowledge Engineering: Principles and Methods. Data and Knowledge Engineering, vol. 25, no. 12, pages

[72] [Trauşan-Matu 2003] Stefan Trausan-Matu. Inteligenţa artificială -suport curs. 2003. 8, 95

[73] [Uszok 2004] Andrzej Uszok, Jefrey M. Bradshaw, Matthew Johnson, Renia Jefers, Austin Tate, Jef Dalton and Stuart Aitken. KAoS Policy Management for Semantic Web Services. IEEE Intelligent Systems, vol. 19, pages 32-41, July 2004. 75

[74] [Vasarhelyi 2009] Miklos A. Vasarhelyi, Siripan Kuenkaikaew, James Littley and Katie Williams. Continuous Auditing technology adoption in leading internal audit organizations, working paper. 2009. 17

[75] [Verma 2008] Vijay K. Verma, Ramesh C. Joshi, Bin Xie and Dharma P. Agrawal. Combating the bloated state problem in mobile agents based network monitoring applications. Comput. Netw., vol. 52, pages 3218-3228, December 2008. 77

[76] [Wallin 2009] Stefan Wallin and Viktor Leijon. Telecom Network and Service Management: An Operator Survey. In MMNS'09, pages 15-26, 2009. 77

[77] [Watermire 2011] David Watermire and Karen Scarfone. Guide to using vulnerability naming schemes. NIST, 2011. http://csrc.nist.gov/publications/nistpubs/800-51-rev1/SP800-51rev1.pdf. 60, 61

[78] [Wooldridge 2009] Michael Wooldridge. An introduction to multiagent systems. second edition. John Wiley and Sons, 2009. 98